FortiWLM

User Guide

8.6.4

2022

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

Table of Contents

1 Introduction

The *FortiWLM Application Suite* is an intelligent management system that helps you to easily manage your wireless network. It shares a common administrator interface, making it easy to transition between the following applications:

- **FortiWLM (NM)—**is a web based application suite which manages controllers and access points mapped to the network to provide real-time data that enables centralized and remote monitoring of the network.
- **Service Assurance Manager (SAM)—**provides trouble-prevention capability that uses the FortiWLM FortiWLM infrastructure to perform end-to-end system tests, either on-demand or automatically at periodic configured intervals. SAM works by comparing a well-functioning network baseline metric to periodic tests. Once baseline network performance is established, any tests that deviate from the baseline can trigger automatic notification. Multiple tests can be configured with *Service Assurance Manager*.
- **Wireless Intrusions Prevention System (WIPS)—**Fortinet's WIPS provides complete wireless threat detection and mitigation into the wireless network infrastructure. It detects wireless intrusions using predefined and custom signatures on an integrated platform with other WLAN management applications.

Audience

This guide is intended for network administrators configuring and maintaining *Fortinet Services Appliance* such as the *SA250 or SA2000-VE.* The *Fortinet Services Appliance* such as the *SA250* will have *FortiWLM* pre-installed on it.

The SA2000-VE will not have NM pre-installed on it.

Other Sources of Information

Additional information is available in the following Fortinet publications and external references.

Related Publications

- *FortiWLM GUI (embedded) Online Help*
- *FortiWLM Release Notes*
- *Fortinet Services Appliance Installation Guide*
- *FortiWLM <Hardware> Quick Start Guides*

.

2 Getting Started

Setting up *FortiWLM Application Suite* for the first time involves:

1. Setting up the services appliance (For instructions on setting up SA250, see *Fortinet Services Appliance Installation Guide.* For instructions on setting up *SA2000VE*, see *"FortiWLM - Virtual Edition"* ***on page 499***)
2. Setting up *FortiWLM* via CLI (see *"Setting Up Services Appliance"* ***on page 27*** and *"Port Number Settings"* ***on page 30***.)
3. Installing a valid *FortiWLM and SAM* licenses (see *"Add a License"* ***on page 33***.)
4. Configuring any controllers to be managed by the services appliance (see *"Add Controllers to FortiWLM"* ***on page 263***.)
5. Configuring server backup settings (see *"Server Backup"* ***on page 33***.)

Follow through the sections below to complete the initial installation and configuration of *FortiWLM*.

Setting Up Services Appliance

The *FortiWLM* unit must be physically connected as described in the *Fortinet Services Appliance Installation Guide*. You will need the following items for software configuration:

- Run the **`setup`** command through the command line interface to configure the services appliance.
- List of IP addresses and passwords.
- Supported browsers is as mentioned below:
  - Internet Explorer 9 and later version (*All the pages of FortiWLM will load under normal browser settings. Compatibility View Settings are not supported*.)
    Note: The Internet Explorer version 11 displays floor maps only when they are uploaded in the *.gif* file format.
  - Mozilla Firefox 61.0.2
  - Google Chrome 68.0
  - Microsoft Edge (Windows 10)
  - Safari (MacOS) 11.0.3

Notes:

- SM is not available on the Firefox browser version 64.0.
- Due to the vulnerability fix, the floor maps do not load on IE version 11 for the following features. Convert floor maps/image into *.gif* file format and re-uploaded in *Operate* > *Map Management.*
  - Client Density (Monitor > Network Summary)
  - Station Location (Monitor > Stations)
  - Network Heat Maps (Monitor > Heat Maps)
  - Map Management (Operate > Map Management)
  - Locationing (Monitor > Locationing)
- Icons are not displayed for Physical and Logical Topology pages in Internet Explorer/Microsoft Edge browsers due to issues with these browsers - https://developer.microsoft.com/en-us/microsoft-edge/platform/issues/4320441/
- Pie charts in the AP Group dashboards are not positioned in the centre when viewed on the IE due to unsupported standard UI styles on the browser. This issue is observed on the following dashlets:
  - High Channel Utilization APs
  - High Retry APs
  - High Loss APs

1. Run the **`setup`** command through the command line interface. The **`setup`** command lists the following parameters of the services appliance to be configured:
   - host name
   - admin password
   - To configure networking, select the option **`yes`** to modify the network settings.

By default, the services appliance IP address is configured to DHCP.

   - Select the option **`yes`** to configure the *DHCP* Addressing and option **`no`** to configure the *Static* Addressing. The following parameters of the services appliance must be configured for static addressing:
     - IP address
     - netmask
     - default gateway (IP)
   - DNS server

- DNS domain
- Time zone settings
- Synchronize the time with the NTP (Network Time Protocol) server.

2. The system restarts.
3. After the services appliance restarts, use the **`show nms`** command to see the *IP address*.
4. Login to the WebUI using https: <IP address>. At the login prompt, enter a *User ID* and *Password*. By default, the *guest* and *admin* user IDs are pre-configured. Password is not required for guest login.
5. Create a signed server certificate using the instructions in the *Security Administration* of *NM*. (See *"Generate CSR on the FortiWLM"* ***on page 354***.)

Before performing set up, ensure you are running the latest version of the FortiWLM Application Suite. Contact Fortinet support for the latest version of FortiWLM Application Suite.

Browser Settings

The following configurations are described in this chapter:

Delete Caching

The dashboard updates are frequently ignored while using *FortiWLM Application*. To receive the dashboard updates, ensure to turn off the caching for the following browsers:

Browser	Steps to delete caching
Windows Internet Explorer	The following steps must be performed, to turn off caching in *Windows Internet Explorer*: **1.** Open the *Internet Explorer,* select *Tools* > *Internet Options*. **2.** In the *Internet Options* window, select the *General* tab. **3.** From the *Browsing History* section in the *General* tab, click the *Settings* button. **4.** On the *Temporary Internet Files and History Settings* window, select "*Every time I visit the webpage"* option. **5.** Click *OK*.

Browser	Steps to delete caching
Mozilla Firefox	The following steps must be performed, to turn off caching in *Firefox*: **1.** Open a *Firefox*. Click *Tools* > *Options.* **2.** Select the *Privacy* panel. **3.** In the *History* section, set *Firefox will:* to *Use custom settings for history*. **4.** Select the check box for Clear history when Firefox closes. **5.** Beside Clear history when Firefox closes, click the Settings button. The Settings for Clearing History window will open. **6.** On the Settings for Clearing History window, click the following items to be cleared: • Browsing History • Download History • Cookies • Cache • Active Logins **7.** Click *OK*. To stop *Firefox* from caching future data, select *ask me every time* from the *Keep Until:* parameter.
Google Chrome	The following steps must be performed, to turn off caching in *Google Chrome*: **1.** Click the *Chrome menu* on the browser toolbar. **2.** Select *Tools*. **3.** Select *Clear browsing data*. **4.** In the dialog that appears, select the check boxes for the types of information that you want to remove. **5.** Use the menu at the top to select the amount of data that you want to delete. Select *the beginning of time* to delete everything. **6.** Click *Clear browsing data*.

Port Number Settings

This section provides the details to *Network Configuration* required for,

- *"Configuring FortiWLM Settings"* ***on page 31***,

- *"Configuring Service Assurance Manager Settings"* ***on page 31*** and

Configuring FortiWLM Settings

Ensure the following ports must be open between *Controllers and Services Appliance*:

- UDP Port 5000, bi-directional
- Any SSH port, bi-directional (default port used is 22)
- TCP/UDP port 1194 for VPN discovery between the controller and *NM* server

Network Settings between Server and Browser

- The following ports are open between Server and Browser:
  - Port 443 for https
  - Port 80 for http
- Connect to *FortiWLM* by pointing a browser to the *Hostname/IP address* of the NM server or by providing a *Common Name* also known as *Fully Qualified Domain name* (FQDN) that is obtained while generating CSR. (See *"Generate CSR on the FortiWLM"* ***on page 354***.)
- Provide a login and password (admin/admin is default). Since the controllers are not added to the *FortiWLM*, the WebUI will not display any data.

Other Network Settings

Open SMTP Port 25.

Configuring Service Assurance Manager Settings

The following *Service Assurance Manager* port numbers must be enabled, if the hardware platform running *SAM Server* and *Controller /AP* is behind a firewall.

- UDP ports 9494, 9595, 9596, 9597 between APs and *SAM* server for *SAM* to work
- Along with the above UDP ports, enable 5000 + Max Controller ID (shown in the inventory of *FortiWLM*) for TCP/UDP test accordingly for Throughput tests to work.

SAM Installation Checklist

Sl No.	Question	Action
1	Are the APs *enabled* online, in L3 mode? Check on the controllers.	Check by clicking, *Operate* > *Inventory* > *Access Points*. Look at the column Connectivity Layer. Also check by typing the CLI command **`show ap`**
2	Are the required controllers listed in the *FortiWLM* inventory and online-active in the *FortiWLM*?	Check by clicking, *Operate* > *Inventory* > *Devices*.
3	The Release Notes reveals the version of the *FortiWLM* and *System Director* that is required. Are the controllers running a *SAM*-Supported build of *System Director*?	Check by clicking, *Operate* > *Inventory* > *Devices.*
4	Have two APs within the range? Are the two APs served with testing ESSIDs? Are the user credentials configured for *Radius* and *Captive Portal* based profiles on *SAM*?	Ensure all the APs are at a minimum signal strength of -70dbm Download ESS on servicing APs to ensure the connection of the *SAM* client. Configure the corresponding *User Name* and *Password* in *SAM* for ESS which are served by external authentication servers.
5	Is anything obstructing the APs and services appliance for UDP ports 9494, 9595, 9596,9597. This can be difficult to determine. The Ports 5000 to 5000+ max controller ID or port 5000 + controller ID for each controller in FortiWLM box must be enabled.	Cross verify the owners of all switches, routers, and firewalls between the boxes.
6	Is NAT disabled/enabled?	NAT is not supported.

Sl No.	Question	Action
7	Check if ICMP is successful between AP and *SAM* server.	The ICMP must be enabled in your network (particularly between the path of Server and AP).

Add a License

The services appliance box includes an *Entitlement Certificate* with a number that is needed to procure a license file. Locate the *Entitlement Certificate* and follow the instructions to configure your license:

1. Contact Fortinet support for your license.
2. When you receive an email with the license file, save the file to your local system.
3. Apply the *FortiWLM* license to your services appliance by following the below steps:
   - Select *Administration* > *Licensing*. In the *License* screen select the *Upload License* option and choose the license key file and click open.
   - Select *Upload* to upload the license key file. The file is uploaded and is displayed on the *License Details* section.

The *Upload* license file allows a single license file upload. Multiple license file upload in one upload operation/session is not permitted.

Server Backup

1. Configure the server, to automatically transfer the backup to a remote server. Refer *"Backup Administration"* ***on page 373***.
2. The nms-server provides an option to backup the database. The backup database is stored on the server in a pre-defined location (*/data/backup/nms*). The server backup performed can be moved between different nms-servers.
3. To configure the parameters, Refer to the *"FortiWLM Maintenance"* ***on page 260***.

Global Search and Notifications

The search function is available on top of all windows and screens. You can use the search function to search for inventory, alarms, events, configuration profiles, and stations that are a part of your E(z)RF Application Suite. You can enter a keyword to search across all categories or you can narrow your search results by selecting appropriate filters.

The notifications bell icon displayed on the FortiWLM GUI indicates the critical alarm notifications. When you click on an alarm notification to view the details, it is removed from the notifications list.

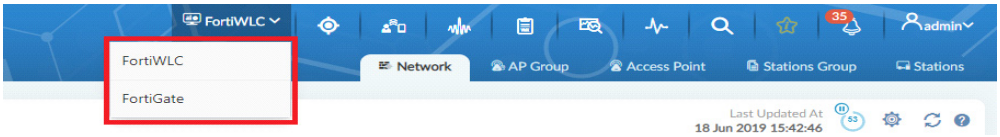
FortiWLC and FortiGate Controllers

FortiWLM enhances monitoring of integrated WiFi networks by supporting the monitoring of FortiGate controllers. You can select between the FortiWLC and FortiGate view by selecting the required option on the top bar of the GUI.

FortiWLM supports migration of 32-bit to 64-bit controllers. The 64-bit migration images are available to migrate the existing 32-bit FortiWLC-50D, FortiWLC-200D, and FortiWLC-500D hardware controllers to 64-bit. See *FortiWLC 8.6 Release Notes* for more information on upgrading to 64-bit FortiWLC.

Notes:

- FortiGate Controller data is now the default display mode of FortiWLM.
- Mixed deployment of FortiWLC and FortiGate controllers is supported.



You can add and manage the FortiWLC/FortiGate wireless controllers at *Operate* > *Inventory* > *Devices*. See section *"Inventory"* ***on page 274***.

FortiGate Configurations

The following must be configured on FortiGate to monitor using FortiWLM.

- [Station logs] The FortiAP profiles must be enabled with extensive info (*set ext-info-enable enable*).
  Note: This is not applicable on FortiGate 60D.
- [DPI statistics] Monitored features need to be enabled under *Application Control* in the FortiGate GUI.
- Rogue APs must be configured on FortiGate. Only active (online) rogue APs are displayed on FortiWLM.

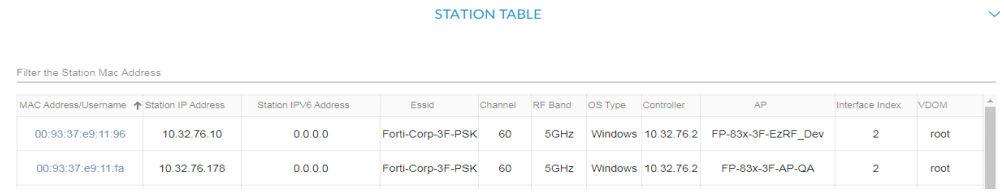
You can monitor and manage FortiGate controllers concurrently associated with APs and stations in a large scale setup. See the *FortiWLM 8.6.4 Release Notes* for more information.

FortiGate VDOM

Virtual Domains (VDOMs) are used to divide a FortiGate into two or more virtual units that function independently. VDOMs can provide separate security policies and, in NAT mode, completely separate configurations for routing and VPN services for each connected network.

For more information, see the FortiGate Documentation.

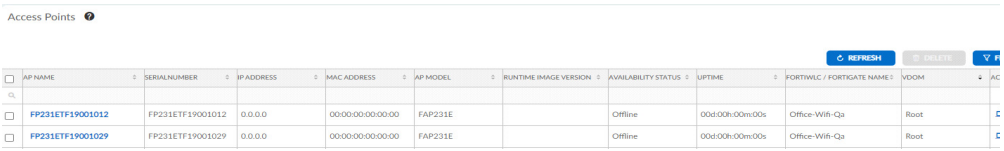
The VDOM is displayed in **Monitor > Overview > Network Summary (Stations).**


STATION TABLE

Filter the Station Mac Address

MAC Address/Username	Station IP Address	Station IPV6 Address	Essid	Channel	RF Band	OS Type	Controller	AP	Interface Index	VDOM
00:93:37:e9:11:96	10.32.76.10	0.0.0.0	Forti-Corp-3F-PSK	60	5GHz	Windows	10.32.76.2	FP-83x-3F-EzRF_Dev	2	root
00:93:37:e9:11:fa	10.32.76.178	0.0.0.0	Forti-Corp-3F-PSK	60	5GHz	Windows	10.32.76.2	FP-83x-3F-AP-QA	2	root

The VDOM is displayed in **Operate > Inventory > Access Points.**


Access Points

REFRESH DELETE

AP NAME	SERIALNUMBER	IP ADDRESS	MAC ADDRESS	AP MODEL	RUNTIME IMAGE VERSION	AVAILABILITY STATUS	UPTIME	FORTIWLC / FORTIGATE NAME	VDOM
FP231ETF19001012	FP231ETF19001012	0.0.0.0	00:00:00:00:00:00	FAP231E		Offline	00d:00h:00m:00s	Office-Wifi-Qa	Root
FP231ETF19001029	FP231ETF19001029	0.0.0.0	00:00:00:00:00:00	FAP231E		Offline	00d:00h:00m:00s	Office-Wifi-Qa	Root

IPV6 Support

All the hardware and virtual FortiWLM models support standard IPv6 address assignment. The FortiWLM GUI can be accessed over an IPv6 address. To access the FortiWLM GUI over an IPv6 address, enter the URL in the format*: https://[IPv6_address_of_FortiWLM]* in the browser, for example, *https://[2001:470:ecfb:45c:428d:5cff:fe5e:c588].* The GUI can be accessed over the HTTPS protocol.

The *show nms* or *show ip6* command on the console can be used to determine the IPv6 address details of the FortiWLM. All possible combinations of FortiWLM IPv6 address configuration are achieved using the *setup* command.

The following modes of IPv6 address acquisition methods are supported.

- ***Statically assigned addresses (global and/or link local scope)*** - You can statically configure one link local and one non link local (site local, unique local or global) scope address which persists across reboots. If you configure a static non-link-local address then DHCPv6 based address acquisition is disabled.

- ***DHCPv6*** - You can configure the FortiWLM to acquire an IPv6 address based on stateless or state full DHCPv6. Stateless DHCPv6 address acquisition is based on SLAAC.
- ***Auto configuration (all configuration from router advertisements)*** - The FortiWLM IPv6 address acquisition is based on the flags set in the router advertisement.

FortiWLM automatically acquires an IPV6 address using SLAAC based acquisition; always works in addition to the above methods.

3 Network Manager

Monitoring Network Manager

The dashboards provides a summary view of all WLAN statistics. The graphical representation of *Alarms, Controllers, Access Points, Stations,* and *Station by OS* type provides a glimpse of the wireless network, based on the current and historical data stored in the database. The aggregate global trend performance and the error rate for all controllers are recorded over a period of time.

The APs send the aggregated client data to the controller. *FortiWLM* gathers the controller data every ten minutes and stores it in database. The data is fetched from the database, when you access a particular dashboard. Every ten minutes, the raw data is compiled into summary charts and those statistics are displayed on the *Global Information Dashboard*.

Every ten minutes, these values are stored in the *FortiWLM* databases.

Parameter Name	Description / Data Type	Value Stored	Trend Dashboard	Longterm Trend Dashboard
Stations	# of associated stations	peak	Yes	Yes
Phones	# of registered phones	peak	Yes	Yes
Phone Calls	# of calls	average	Yes	Yes
Throughput	aggregated throughput	average	Yes	Yes
Rx Bytes	total bytes received	sum	-	Yes
Tx Bytes	total bytes transmitted	sum	-	

Parameter Name	Description / Data Type	Value Stored	Trend Dashboard	Longterm Trend Dashboard
Online Controllers	# of online controllers	minimum	-	Yes
Offline Controllers	# of offline controllers	peak	-	
Online APs	# of online APs	minimum	Yes	Yes
Offline APs	# of offline APs	peak	Yes	
Critical Alarms	# of critical alarms	peak	Yes	Yes
Major Alarms	# of major alarms	peak	-	
Minor Alarms	# of minor alarms	peak	-	
High Noise Radios	# of radios with high noise	NA. Instantaneous at the specific point in time	Yes	-
High Loss Radios	# of radios with high loss	NA. Instantaneous at the specific point in time	Yes	-
High Loss Stations	# of stations with high loss	NA. Instantaneous at the specific point in time	Yes	-
Low Signal Stations	# of stations with low signal	NA. Instantaneous at the specific point in time	Yes	-
Rogue APs	# of wired and wireless rogue APs	NA. Instantaneous at the specific point in time	Yes	-

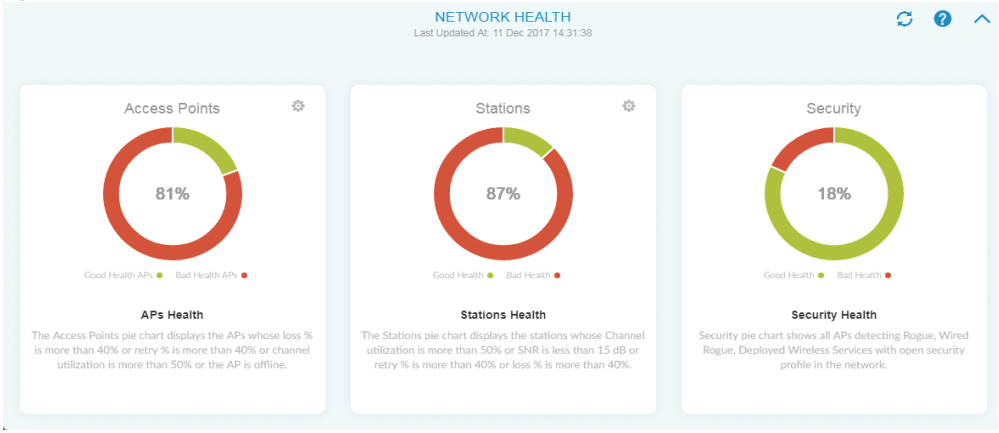
You can monitor data in the following set of dashboards:

- *"Overview Dashboards"* **on page 40**
- *"Client Exclusion View"* **on page 109**
- *"Trends Dashboards"* **on page 120**
- *"Topology"* **on page 135**

Network Health

The Network Health Dashboard monitors the devices in your wireless network and provides a health summary of the devices. The pie charts in this dashboard highlight the problematic devices/areas in the network by examining the statistics and behavior of stations and access points. You can identify the potential issues in the network using the data in this dashboard.

Figure 1: *Network Health*



Access Point

This chart displays the health of the APs in your network based on the Airtime Utilization (%), Loss (%), and Retries (%). You can configure the threshold in the Filter Criteria; the chart is updated to display data as per the filter criteria. The APs in good health are indicated in green and the APs in bad health are indicated in red. Hover over the chart in the respective areas to view the total number of APs in good health and the total number of APs in bad health.

By default, the AP is in bad health if the Loss (%) is more than 40%, or Retries (%) is more than 40%, or Channel Utilization is more than 50%, or if the AP is offline.

Clicking on this chart navigates you to the **AP Group** dashboard with the same filter options applied.

Stations

This chart displays the health of the stations in your network based on the Channel Utilization (%), Loss (%), Retries (%), and SNR (dB). You can configure the threshold in the Filter Criteria; the chart is updated to display data as per the filter criteria. The stations in good health are indicated in green and the stations in bad health are indicated in red. Hover over the chart in the respective areas to view the total number of stations in good health and the total number of stations in bad health.

By default, the station is in bad health if the SNR is less the 15dB, or Loss (%) is more than 40%, or Retries (%) is more than 40%, or Channel Utilization is more than 50%.

Clicking on this chart navigates you to the **Station Group** dashboard with the same filter options applied.

Security

This chart displays the security health based on rogue APs and deployed wireless services with open security profile in the network.

Hover over the chart in the respective areas to view the total number of APs in good health and the total number of APs in bad health.

Overview Dashboards

The *Overview* dashboards provide at-a-glance system information to the following dashboards available in the left panel of each page:

After upgrade to FortiWLM 8.4.0 or after a performing data backup and restore, partition (aggregation) tables are created in the database. **Data indexing** process symbol is displayed in the GUI. There might be a discrepancy in the older data displayed on the dashboards.

Navigate to *Monitor* > *Overview* on the FortiWLM GUI.

Network Summary

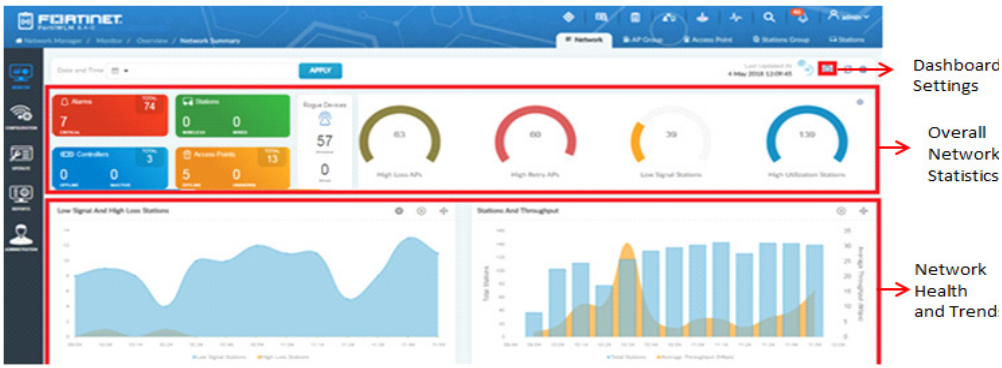
The **Network** dashboard gives statistics of the type of devices connected to the network and their performance. It provides a summary view of WLAN statistics, including network wide wireless controller and access point performance distribution. It gathers the data from all managed controllers and access points at specific intervals. The graphical representation of Controllers, Access Points, Stations, and Station by OS type provides a glimpse of the wireless network, based on the data that is fetched for the configured period of time.

Dashboard Organization

The Network dashboard is organized into the following areas:

- Dashboard Settings
- Overall Network Statistics
- Network Health and Trends

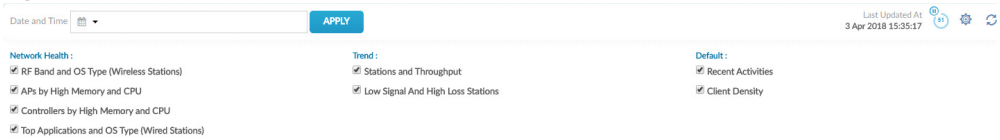
Figure 2: *Network Summary*



Dashboard Settings

The dashboard settings allow you to refine the widgets displayed on the dashboard panels. The filtering parameters of the dashboard analyze the statistics and behavior of the controllers, stations, and APs within the wireless network. It provides a graphical representation of the performance of these devices within the administrative scope of the logged in user.

Figure 3: *Dashboard Settings*



The dashboard is configured to generate data at a configured time interval. You can select the time interval from the **Date and Time** drop-down list or define a custom time range.

You can monitor the following network health parameters.

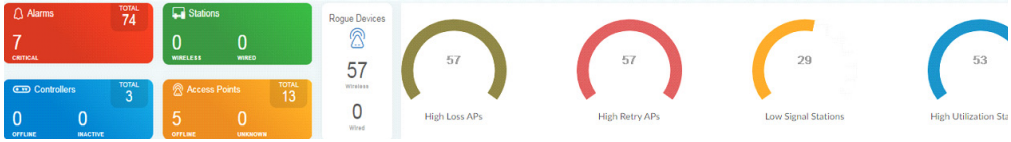
Filter By	Description
Network Health	• Stations • APs by High Memory and CPU • Controllers by High Memory and CPU • Top applications and OS Type (Wired Stations)

Trend	• Stations and Throughput • Low Signal And High Loss Stations • High Latency FortiGates (FortiGate only)
Default	• Recent Activities • Client Density

Overall Network Statistics

The statistics section of the Network dashboard provides the overall statistical details of Controllers, Access Points, Stations, and Alarms within the wireless network.

Figure 4: *Network Statistics*



Critical Alarms - Provides the total count of critical alarms raised. Click on the tab to view the detailed summary, displayed in a separate popup screen. The associated alarm information is displayed, *Date/Time, Alarm Name, Category, Fdn, Controller Id,* and *Message*.

Figure 5: *Critical Alarms*

CRITICAL ALARMS

Show 10 entries Search:

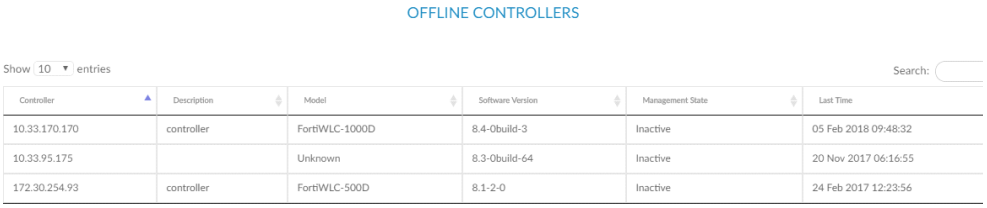
Date/Time	Alarm Name	Category	Fdn	Controller Id	Message
01 Feb 2018 10:54:21	AP Down	Access Point	SD-AP-51	13	AP [MAC address<00:0c:e6:3a:7d:90> IP<10.34.28.51>] is down
01 Feb 2018 14:06:42	AP Software Version Mismatch	Access Point	SD-AP-8	8	Firmware version <8.4-0dev-33> of AP [<42x_2F_Cafe_Entry> MAC address<00:0c:e6:36:89:80> IP<10.32.48.183>] doesn't match version in controller which is <8.4-0dev-39>
01 Feb 2018 17:06:22	AP Down	Access Point	SD-AP-32	13	AP [MAC address<00:0c:e6:3b:b4:90> IP<10.33.168.10>] is down
01 Feb 2018 20:28:42	AP Software Version Mismatch	Access Point	SD-AP-206	8	Firmware version of AP [<22x_3F_EzRF_Dev> MAC address<00:0c:e6:3a:7d:70> IP<10.32.48.191>] doesn't match version in controller which is <8.4-0dev-39>
01 Feb 2018 20:28:52	AP Software Version Mismatch	Access Point	SD-AP-203	8	Firmware version of AP [<22x_3F_Pioneer> MAC address<00:0c:e6:3a:6a:30> IP<10.32.48.192>] doesn't match version in controller which is <8.4-0dev-39>
01 Feb 2018 20:28:55	AP Software Version Mismatch	Access Point	SD-AP-209	8	Firmware version of AP [<22x_3F_HR_Admin> MAC address<00:0c:e6:3a:7d:b0> IP<10.32.48.189>] doesn't match version in controller which is <8.4-0dev-39>
01 Feb 2018 20:28:56	AP Software Version Mismatch	Access Point	SD-AP-208	8	Firmware version of AP [<22x_3F_IT_Bay> MAC address<00:0c:e6:3a:6b:50> IP<10.32.48.187>] doesn't match version in controller which is <8.4-0dev-39>

Stations – Provides the total count of stations connected to an AP. The associated station information is displayed, *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 VDOM (FortiGate Only).*

Figure 6: *Station*

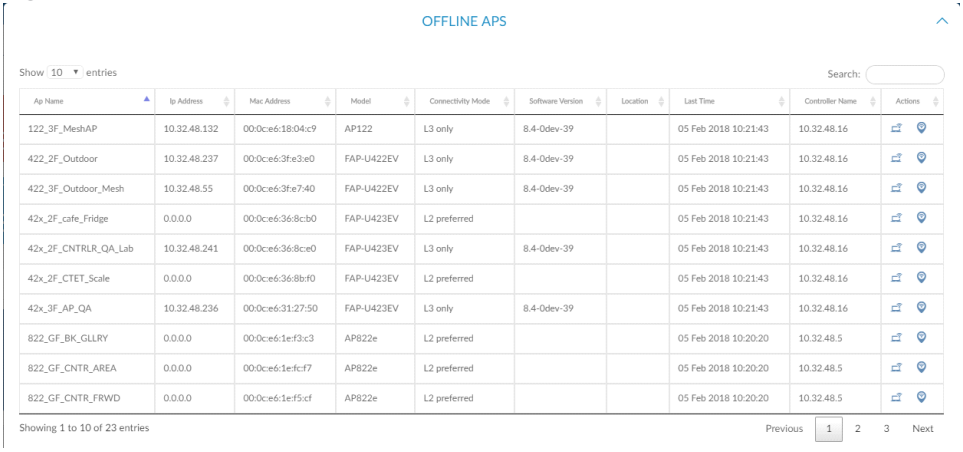
Offline/Inactive Controllers - Provides the total count of offline/inactive controllers. Click on the tab to view the detailed summary, displayed in a separate popup screen. The associated controller information is displayed, *Controller, Description, Model, Software Version, Management State,* and *Last Time*.

Figure 7: *Offline Controllers*



Offline/Unknown APs - Provides the total count of offline/unknown APs. Click on the tab to view the detailed summary, displayed in a separate popup screen. The associated AP information is displayed, *AP Name, IP Address, MAC Address, Model, Connectivity Mode, Software Version, Location, Last Time,* and *Controller Name*.

Figure 8: *Offline APs*



The dashboard provides filter criteria to configure the thresholds and apply them to the charts for obtaining statistics.

- **Rogue Devices** - Provides the total count of wired and wireless rogue devices (APs and stations) in the network. Click on the tabs to view the detailed summary, displayed in a separate popup screen. The associated rogue device information is displayed, *Controller Name, Rogue MAC Address, Rogue Type, BSSID, Channel, SSID, AP Reported, Date-Time,* and *Location*.
- **High Loss APs**: Provides the total count of APs in the network whose average loss percentage in greater than 40%. Clicking on the chart navigates to the **AP Groups** dashboard with the same filter applied.
- **High Retry APs**: Provides the total count of APs in the network whose average retry percentage is greater than 40%. Clicking on the chart navigates to the **AP Groups** dashboard with the same filter applied.
- **Low Signal Stations**: Provides the total count of stations whose average SNR is less than 15 dbm. Clicking on the chart navigates to the **Station Groups** dashboard with the same filter applied.
- **High Utilization Stations**: Provides the total count of stations in the network whose average airtime utilization is greater than 50%. Clicking on the chart navigates to the **Station Groups** dashboard with the same filters applied.

Network Health and Trends

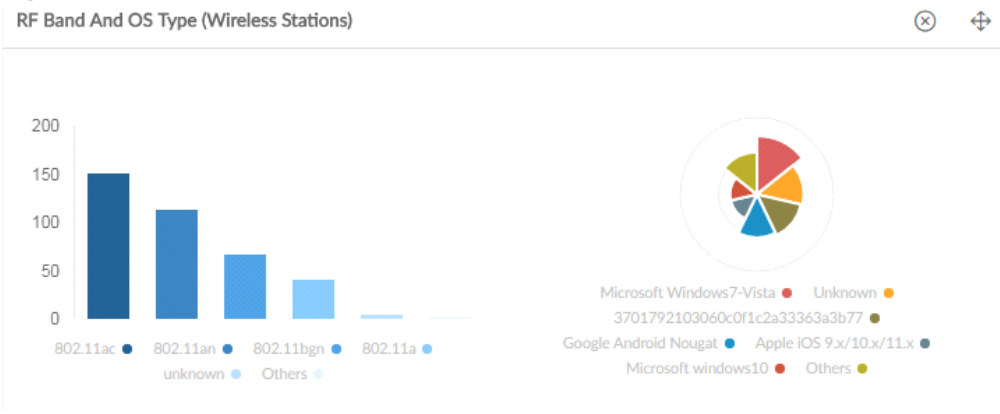
The dashboard panels displaying the health and trends of devices in your network are described in this section. The trend graphs display data for the last 10 minutes or 1 minute (based on the configured polling interval).

- RF Band and OS Type (Wireless Stations)
- Stations And Throughput
- Low Signal And High Loss Stations
- APs By High Memory And CPU
- Controllers By High Memory And CPU
- Top applications and OS Type (Wired Stations)
- Recent Activities
- Client Density Select Floor

RF Band and OS Type (Wireless Stations)

This panel provides the statistics for stations associated with each RF band and OS type.

Figure 9: *RF Band and OS Type*



Stations by RF Band - The Bar chart provides a graphical representation of stations for each RF type. Each vertical bar classifies the total number of stations connected to a particular RF type. For Example, a, b, bg, bgn, an, ac stations.

Each station type is represented in a unique color. Hover the mouse pointer over a graph to view the total number of stations connected to a particular RF type.

Stations	Description
802.11a	802.11a is a wireless standard that is implemented on 5GHz frequency range with a maximum data rate of 54Mbps.
802.11b	802.11b is a wireless standard that is implemented on 2.4GHz frequency range with a maximum data rate of 11Mbps.
802.11bg	802.11bg is a wireless standard that works on 2.4GHz frequency range with a maximum data rate of 54Mbps.
802.11bgn	802.11bgn is a wireless standard that is implemented on 2.4GHz and frequency range with a maximum data rate of 600Mbps.
802.11an	802.11an is a wireless standard that is implemented on 5GHz and frequency range with a maximum data rate of 600Mbps.
802.11ac	802.11ac is a wireless standard that is implemented on 5GHz and frequency range with a maximum data rate of 1Gbps.
Unknown	Unknown state is displayed when the system is unable to find the RF band of the station.

Hover over each bar to view the associated station count and click on the legend to view the associated station details, *Station MAC Address, Station IP Address, Station IPv6 Address, Essid, Channel, SNR, RF Band, OS Type, RX Rate, TX R*– The Pie chart provides a graphical

representation of stations for each OS type. Each slice classifies stations for each OS type. A maximum of 6 different OS types are plotted on the pie chart. Remaining OS types will be displayed under **Others** category.

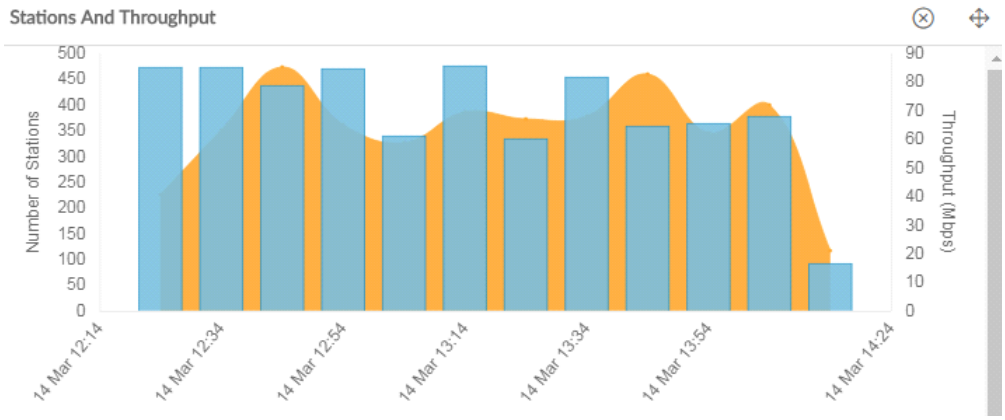
- This pie chart provides the station classification based on the OS type. For Example, Microsoft Windows7-Vista, Google Android Jellybean, Google Nougat, and so on.
- Each station type is represented in a unique color. Hover the mouse pointer over a graph to view total number of stations.
- Left click on each of the OS type to view a detailed summary of the stations connected to the controller by different OS Type.

Hover over each slice to view the associated station count and click on the legend to view the associated station details, *Station MAC Address, Station IP Address, Station IPv6 Address, Essid, Channel, SNR, RF Band, OS Type, RX Rate, TX Rate, Controller ID, AP ID,* and *Interface Index*.

Stations And Throughput

The **Stations And Throughput** chart displays a station's combined transmitted and received bytes during a 2 hour interval. The graph displays the aggregate number of wireless stations connected to the network and the average throughput (Mbps) at a 10 minutes or 1 minute interval (based on the configured polling interval).

Figure 10: *Stations and Throughput*

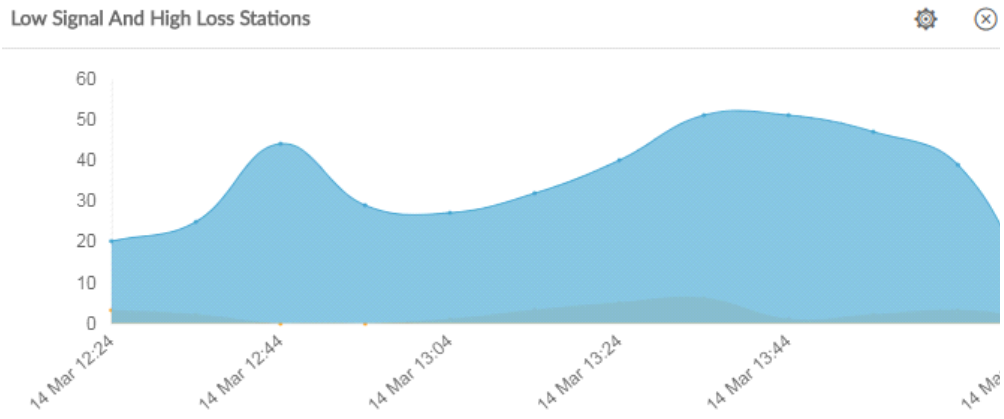


Each bar represents maximum stations connected and the average throughput during that interval. Hover the mouse over each bar to view the station count and throughput.

Low Signal And High Loss Stations

The **Low Signal And High Loss Stations** trend graph displays the total number of stations in the network facing low signal (SNR) and high loss at a 2 hour interval.

Figure 11: *Low Signal and High Loss Stations*

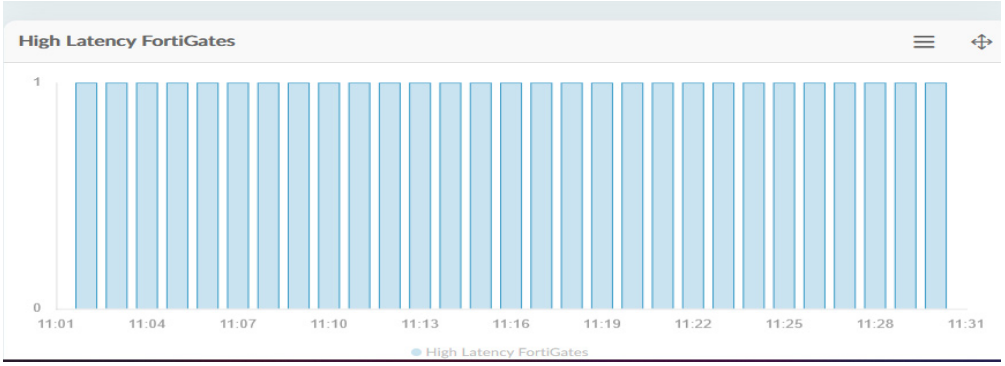


High Loss is defined as the percentage of 802.11 unicast packets transmitted for which no 802.11 Ack is received (> 40%).

Hover the mouse over each of the section, a summary of the high loss and low signal stations, as per the average loss % and average SNR configured in the filter criteria is displayed. The graph is plotted based on the configured filter criteria.

High Latency FortiGates (FortiGate only)

The high latency FortiGates panel displays the REST API query delays at different times. The purpose of this feature is to provide input to configure an optimum REST API timeout for FortiGate. See “Add Controllers to FortiWLM” on page 275.



APs By High Memory And CPU

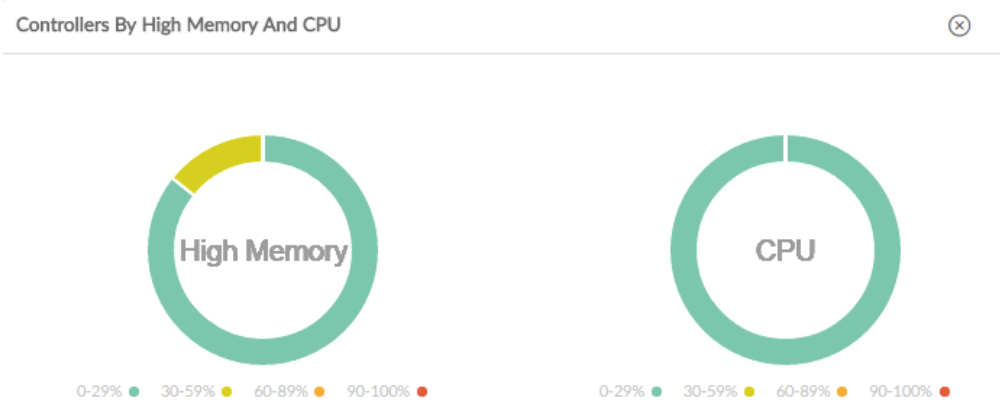
The **APs By High Memory And CPU** chart categorizes all the APs into different buckets of CPU and Memory utilization. Different buckets are 0-29%, 30-59%, 60-89% and 90-100%. Hover over each bucket in the chart to view the number of APs in the bucket.

Figure 12: *APs by High Memory and CPU Usage*

Controllers By High Memory And CPU

The **Controllers By High Memory And CPU** chart categorizes all the controllers into different buckets of CPU and Memory utilization. Different buckets are 0-29%, 30-59%, 60-89% and 90-100%. Hover over each bucket in the chart to view the number of controllers in the bucket..

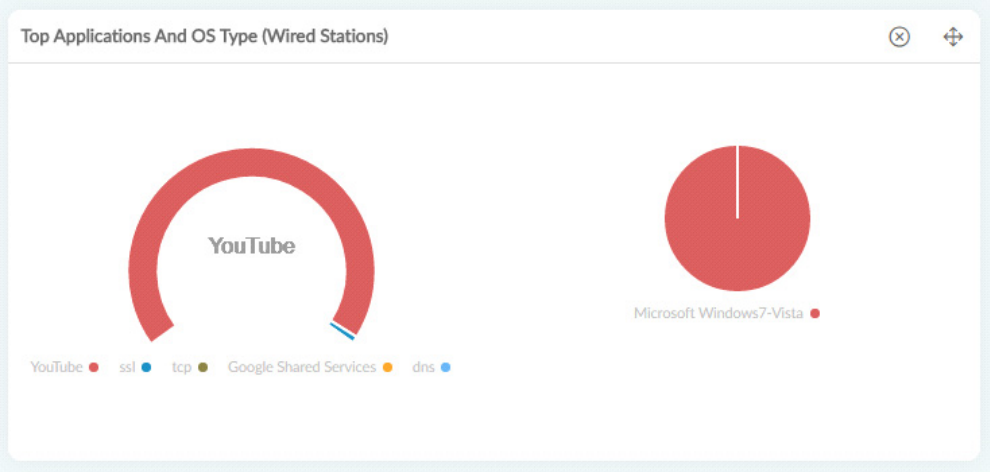
Figure 13: *Controllers by High Memory and CPU Usage*



Top applications and OS Type (Wired Stations)

This chart gives the summary of top 5 applications used in the network and also the highly used OS, for wired stations.

Figure 14: *Top Applications and OS*



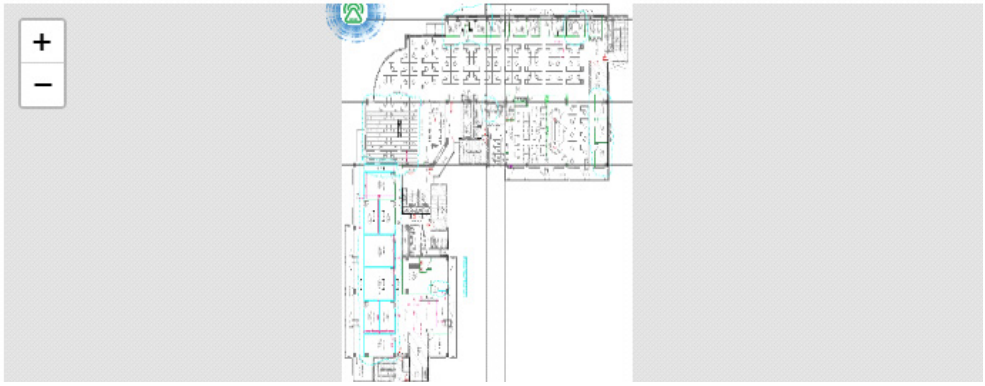
Recent Activities

The **Recent Activities** panel displays the last 40 user activities in the last 24 hours.

Client Density Select Floor

The **Client Density Select Floor** 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.

Figure 15: *Client Density*



You can 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.

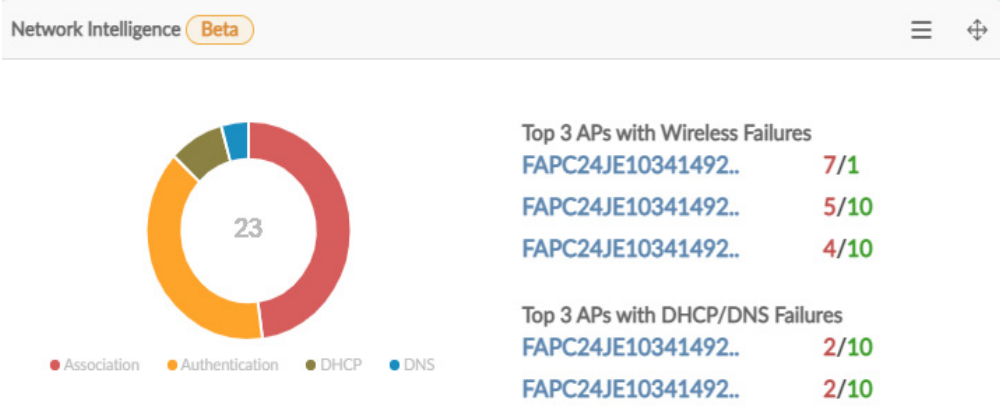
Note: APs that have clients associated with them will ONLY be displayed.

Click on an AP to view these details, *AP ID, AP Name, AP MAC, Controller,* and *Total Stations*. Additionally, you can zoom in and zoom out the maps.

Network Intelligence

The Network Intelligence panel provides a snapshot of FortiGate **ONLY** connectivity issues for specific durations. All station related wireless events from FortiGate are processed and classified into the following categories.

- Authentication failures
- Association failures
- DHCP failures
- DNS failures



Pie Chart

Failures detected up to 2 hours are presented as pie charts with success and failure event counts displayed along with the related station MAC address, reason, and remediation. The 4 failure categories are marked in different color.

- Top 3 APs with DHCP/DNS failures are listed.
- Top 3 APs with wireless failures are listed.

Click on each of these categories to view details.

Note: After a success event is generated, all previous failures are cleared.

Trend Graph

Failures detected for more than 2 hours are presented as trend graphs. The failure categoriesâ?? time and count are displayed along with the related station MAC address, reason, and remediation.

Click on each point in the graph to view the FortiGates with details.

AP Group

An **AP Group** is a coherent group of APs belonging to the same controller or different controllers placed in distinctive geographic locations. The AP group may consist of APs with different hardware model or APs from controllers having different FortiWLC versions. When an AP is added to a group, all the radios of the AP are also a part of this group.
The APs data within the selected AP group is used to create the AP Group dashboard. The data is generated based on configured time intervals (default is 2 hours for trend graphs widgets and 10 minutes or 1 minute (based on the configured polling interval) for other widgets) on the server. All the links or pop-up from this page and status bar display the current data.

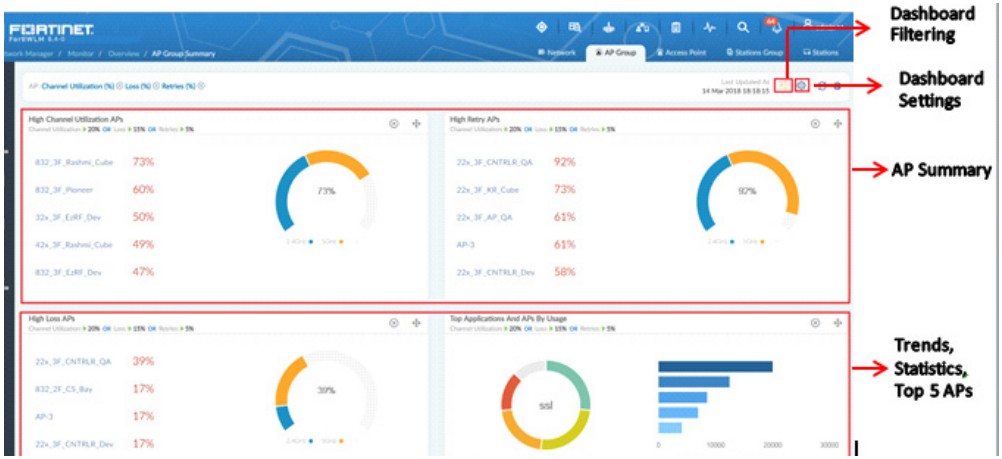
The AP Group Summary dashboard provides data from Trends, Statistics, and Top 5 APs.

Dashboard Organization

The AP Group dashboard is organized into the following areas:

- Dashboard Settings
- Dashboard Filtering
- Trends, Statistics, and Top 5 APs

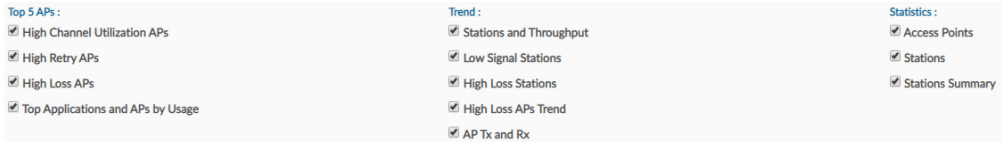
Figure 16: *Dashboard Organization*



Dashboard Settings

The dashboard settings allow you to refine the widgets displayed on the dashboard panels. It provides a graphical representation of the performance of these devices within the administrative scope of the logged in user. You can monitor the following network health parameters.

Figure 17:



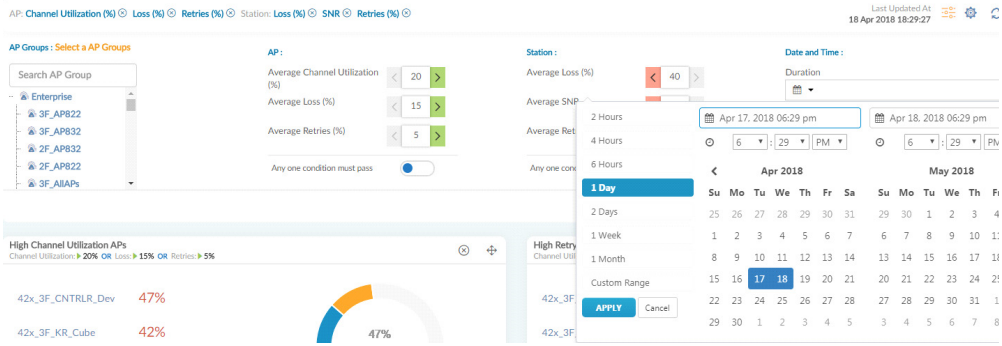
You can monitor the following AP Group parameters.

Filter By	Description
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 • High Loss Stations • High Loss APs Trend • AP Tx and Rx
Statistics	• Access Points • Stations

Dashboard Filtering

The monitoring parameters of the dashboard analyze the statistics and behavior of specific APs in the group and stations, based on the configured threshold values.

Figure 18: *Dashboard Filtering*



The dashboard generates data at a configured time interval. You can select the time interval from the Date and Time drop-down list or define a custom time range.

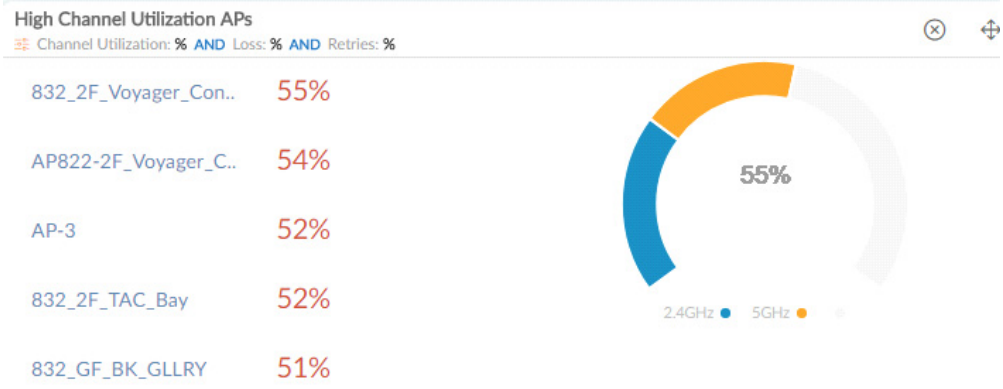
Trends, Statistics, and Top 5 APs

This section of the AP Group dashboard graphically represents the AP statistics and trends that belong to a selected AP group which are under administrative scope of your access settings. The trend graphs display data for the last 2 hours.

High Channel Utilization APs

Provides the top 5 APs whose average channel utilization % for the configured period of time (default is ten minutes) meets the filter criteria. The chart displays the name and the corresponding average channel utilization % of APs in the group for 2.4GHz and 5GHz bands.

Figure 19: *High Channel Utilization APs*

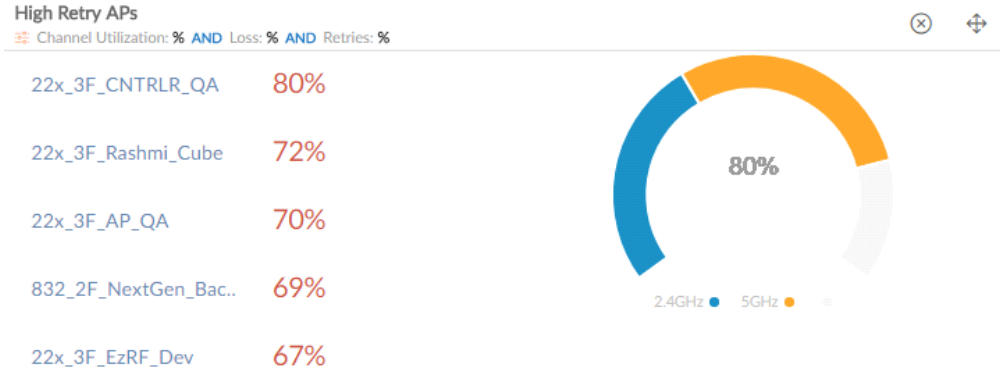


Clicking on the AP name navigates to the **Access Point** dashboard.

High Retry APs

Provides the 5 APs whose average retries % for the configured period of time (default is ten minutes) meets the filter criteria. The chart displays the name and the corresponding average retries % of APs in the group for 2.4GHz and 5GHz bands.

Figure 20: *High Retry APs*

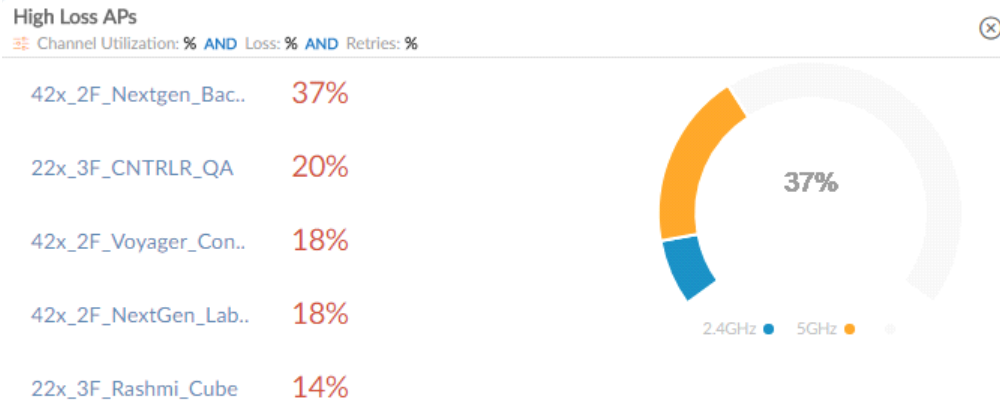


Clicking on the AP name navigates to the **Access Point** dashboard.

High Loss APs

Provides the 5 APs whose average loss % for the configured period of time (default is ten minutes) meets the filter criteria. The chart displays the name and the average loss % of APs in the group for 2.4GHz and 5GHz bands.

Figure 21: *High Loss APs*

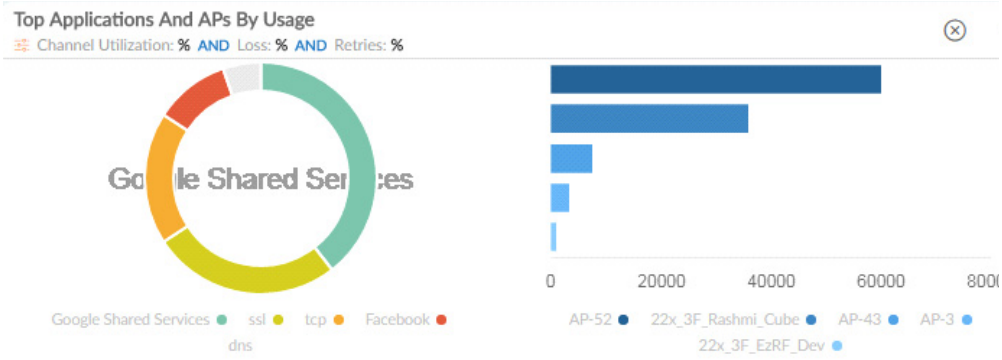


Clicking on the AP name navigates to the **Access Point** dashboard.

Top Applications And APs By Usage

This chart gives the summary of highly used applications within the selected AP Group and also top 5 APs with highest average throughput within the AP Group.

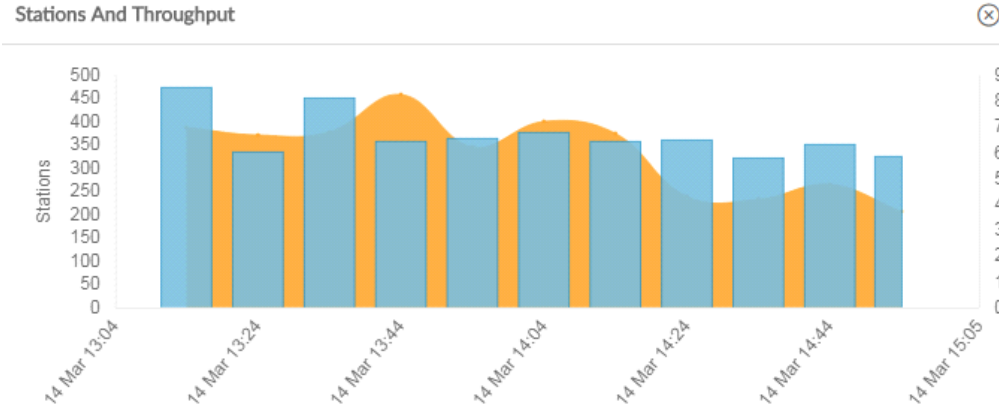
Figure 22: *Top Applications and APs- usage*



Stations and Throughput

The **Stations And Throughput** chart displays a station's combined transmitted and received bytes during a 2 hour interval. The graph displays the aggregate number of wireless stations connected to the APs within the selected AP Group and the average throughput (Mbps) at a given time.

Figure 23: *Stations and Throughput*

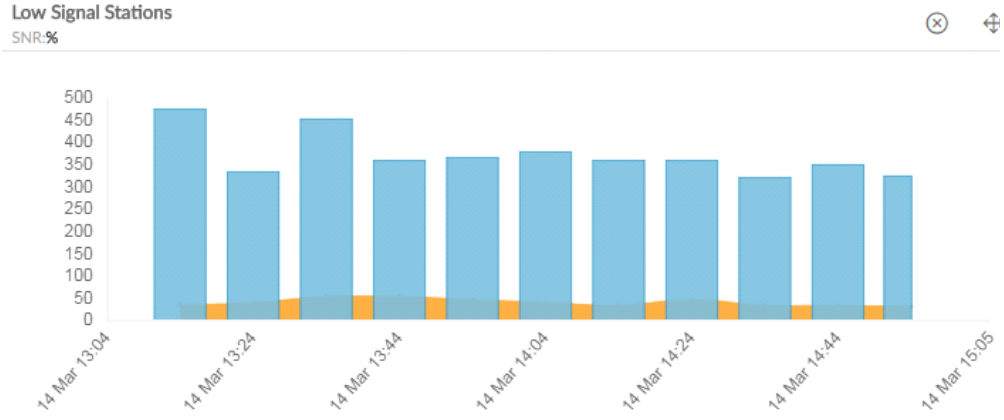


Each bar represents maximum stations connected and the aggregate throughput during that interval. Hover the mouse over each bar to view the station count and throughput.

Low Signal Stations

The **Low Signal Stations** trend graph displays the total number of stations in the network facing low signal (SNR). SNR is defined as the signal strength relative to background noise.

Figure 24: *Low Signal Stations*

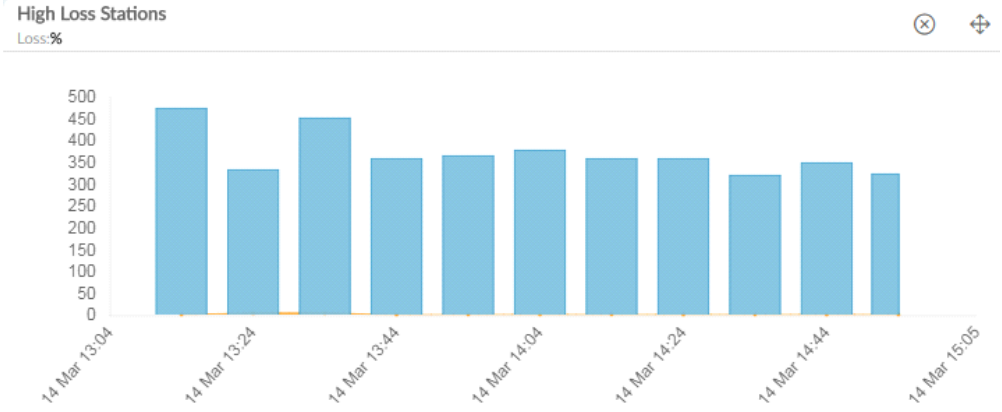


Hover the mouse over each of the bar, the maximum stations connected and the total number of low signal stations, as per the average SNR configured in the filter criteria during that interval are displayed. You can configure the threshold for low signal in the available filter options. The graph is plotted based on the configured filter criteria.

High Loss Stations

The **High Loss Stations** trend graph displays the total number of stations in the network facing high loss at a given point.

Figure 25: *High loss Stations*



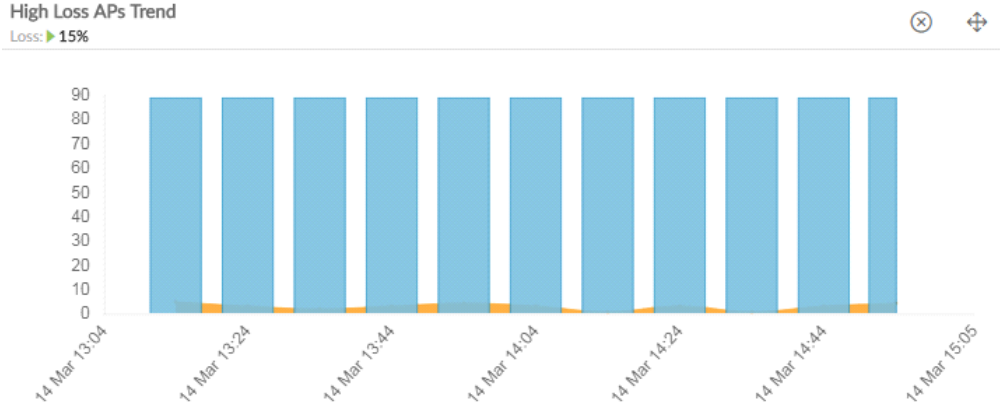
High Loss is defined as the percentage of 802.11 unicast packets transmitted for which no 802.11 Ack is received (> 40%). Hover the mouse over each of the section, the maximum stations connected and the total number of high loss stations, as per the average loss % configured in the filter criteria, during that interval are displayed.

The graph is plotted based on the configured filter criteria.

High Loss APs Trend

Provides the total count of APs in the network whose average loss percentage in greater than 40% within the AP group. Hover the mouse over each of the section, the maximum APs connected and the total number of high loss APs are displayed.

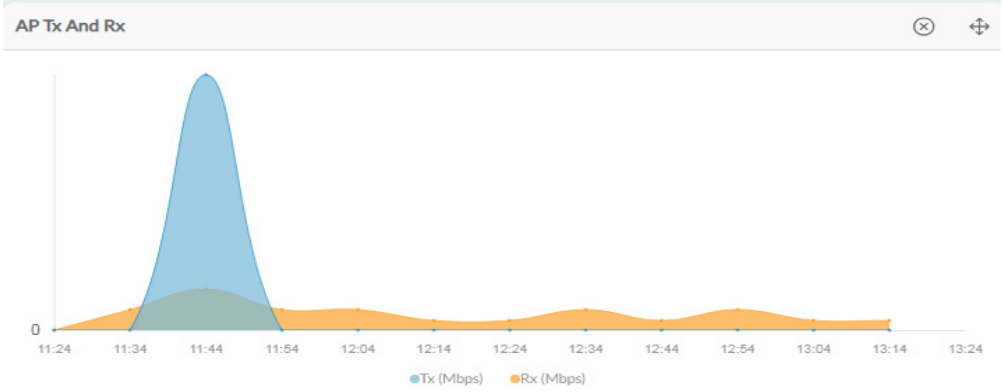
Figure 26: *High Loss APs Trend*



AP Tx and Rx

The **AP Tx and Rx** trend graph displays the average Tx and Rx utilization (Mbps) of the access point.

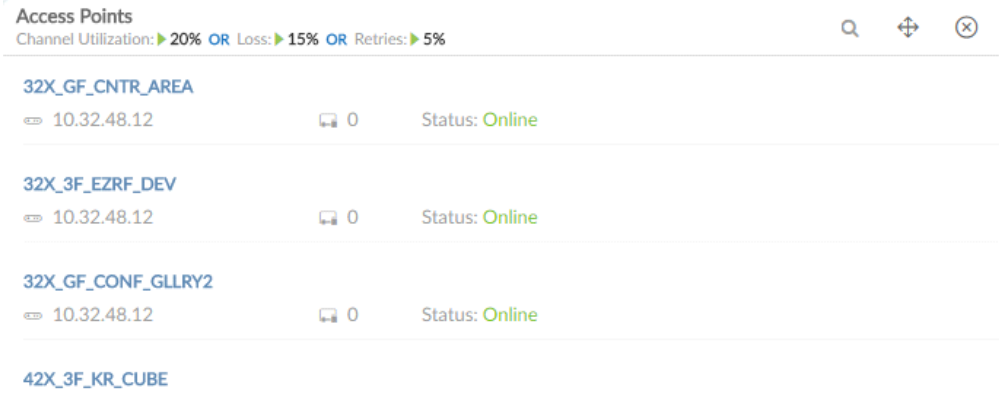
Figure 27: *AP Tx and Rx*



Access Points

The **Access Points** panel displays the details of all APs in the AP group that meet the filter criteria.

Figure 28: *Access Points*

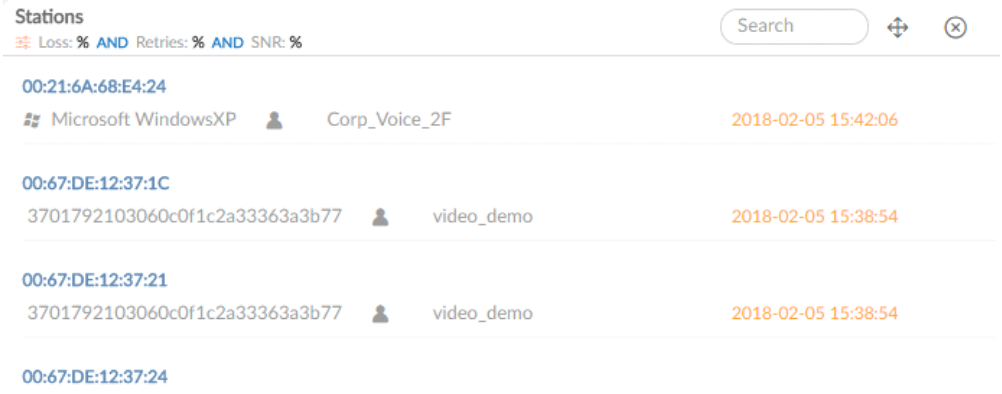


Clicking on the AP name navigates to the **Access Point** dashboard.

Stations

The **Stations** panel displays the details of all stations connected to each AP in the AP group that meet the filter criteria.

Figure 29: *Stations*

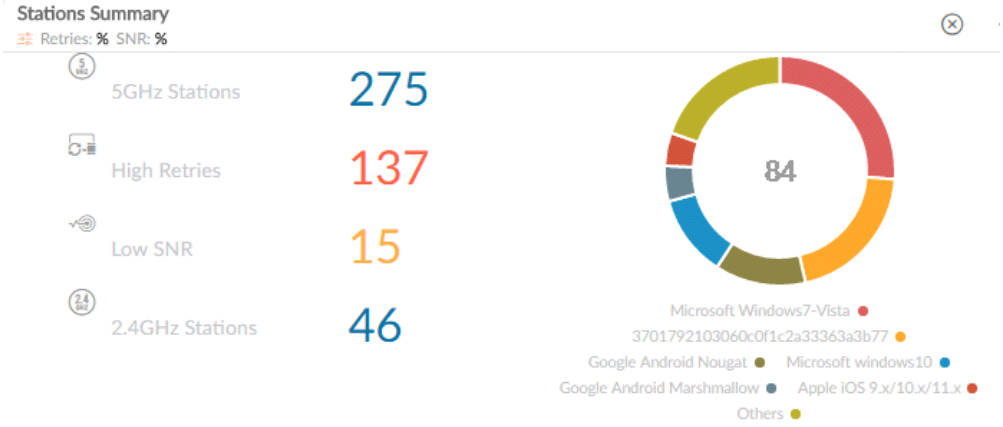


Clicking on the Station name navigates to the **Stations** dashboard.

Stations Summary

This panel displays the summary of all the stations connected to the access points in the group with the classification of stations by OS type. The total count of *5GHz Stations, 2.4GHz Stations, High Retries*, and *Low SNR* are displayed.

Figure 30: *Stations Summary*



Access Point

The **Access Point** Dashboard screen displays in-depth information about the AP activity. It provides the graphical representation of the Throughput, Station Count, Noise Level, Loss%, Channel Utilization%, and the health of stations connected to the selected access point which is connected to a controller managed by the FortiWLM. The trend result for each of the sta-

tions of the selected AP is displayed on the top portion of the window.
The data is generated based on configured time intervals ((default is 2 hours for trend graphs widgets and 10 minutes or 1 minute (based on the configured polling interval) for other widgets) on the server. All the links or pop-up from this page and status bar display the current data.

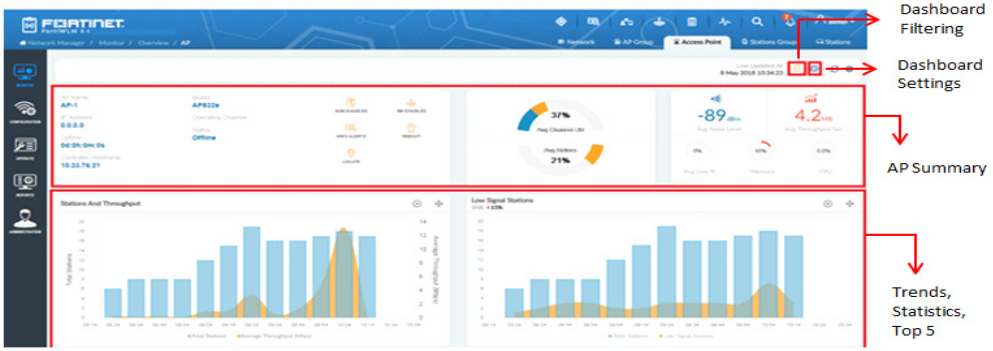
The AP Group Summary dashboard provides data from Trends, Statistics, and Top 5 APs.

Dashboard Organization

The Access Point dashboard is organized into the following areas:

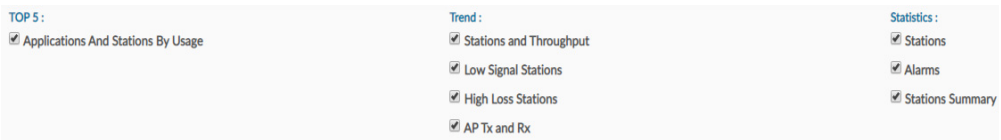
- Dashboard Filtering
- Dashboard Filtering
- Access Point Summary
- Trends, Statistics, and Top 5

Figure 31: *Dashboard Organization*



Dashboard Settings

The dashboard settings allow you to refine the results displayed on the dashboard panels. It provides a graphical representation of the performance of these devices within the administrative scope of the logged in user. You can monitor the following network health parameters.



You can monitor the following Access Point parameters.

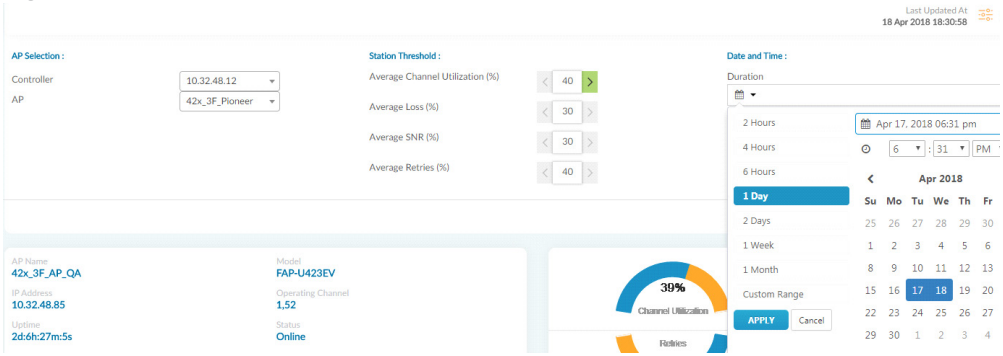
Filter By	Description
Top 5	Applications And Stations By Usage

Trend	• Stations and Throughput • Low Signal Stations • High Loss Stations • AP Tx and Rx
Statistics	• Stations • Alarms • Stations Summary

Dashboard Filtering

The filtering parameters of the dashboard analyze the statistics and behavior of specific APs and stations, based on the configured threshold values.

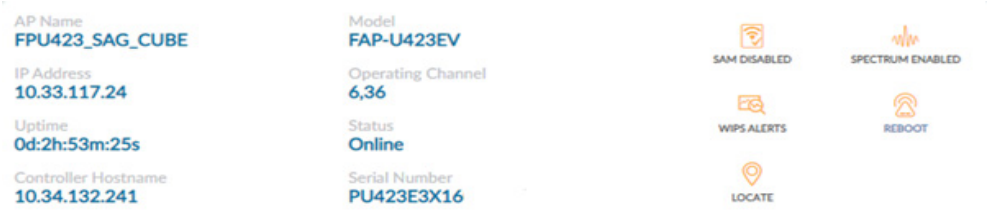
Figure 32: *Dashboard Filtering*



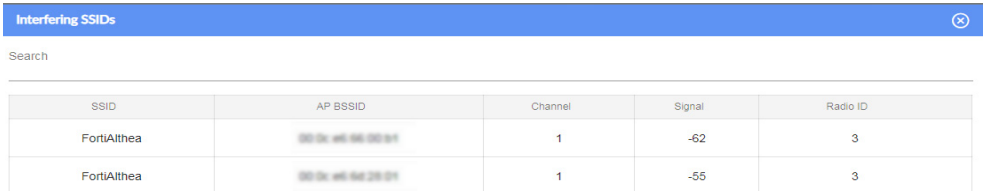
The dashboard generates data at a configured time interval. You can select the time interval from the Date and Time drop-down list or define a custom time range.

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.



- **SAM Enabled/Disabled**: This icon indicates if any SAM tests are running on the access point. The icon status is **SAM Enabled** if baseline or scheduled tests are running; click the icon to view the *Ongoing Tests* dashboard in SAM. Hover over this icon to view the access point's interface details on which SAM tests are running. The icon status is **SAM disabled** when no tests are running on the access point.
- **Spectrum Enabled/Disabled**: This icon indicates whether Spectrum Analyzer is enabled or disabled on the access point. The icon status is **Spectrum Enabled** if the AP radios are operating in the scan spectrum mode. The icon status is **Spectrum Disabled** if the AP radios are operating in the service/normal mode.
- **VLAN Probe**: Click this icon to configure VLAN probe on FortiGate controllers only.
- **Interfering SSIDs**: 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 (Managed FortiAP Profile). This is for FortiGate controllers only.



- **WIPS Alerts**: Click this icon to view the alerts raised by an access point when WIPS is configured, in the *Alerts* dashboard in WIPS. Hover over the icon to view the access points interface (1,2,3) details that are generated the alerts. This option is disabled if WIPS is not configured.
- **Reboot**: Click this icon to reboot an online access point only. This option is disabled if the access point is offline/unknown.
- **Locate**: Click this icon to view the location of an access point on the floor map. This option is disabled if the access point is not placed on the floor map.

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.

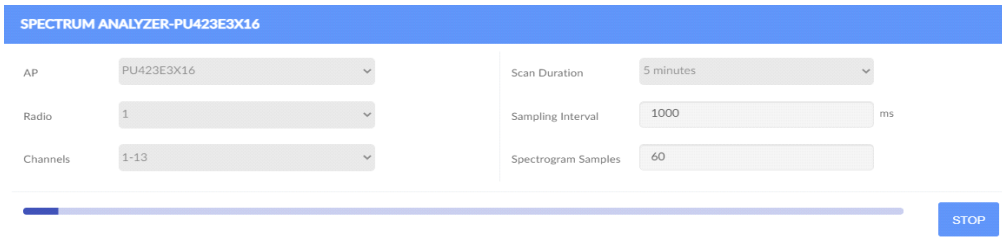
Select the channels to be scanned and configure. The spectrum analyzer result displays widgets with the type of interference, signal strength, impacted channels, and spectrum current utilization, start and end time and duration of the interference. It classifies non-WiFi interferences to easy identification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

Notes:

- FortiWLC: Spectrum Analyzer is supported only on FAP-U models with the radio configured in the *Scan Spectrum* mode.
- FortiGate: Spectrum Analyzer is supported on all AP models.
  - 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.

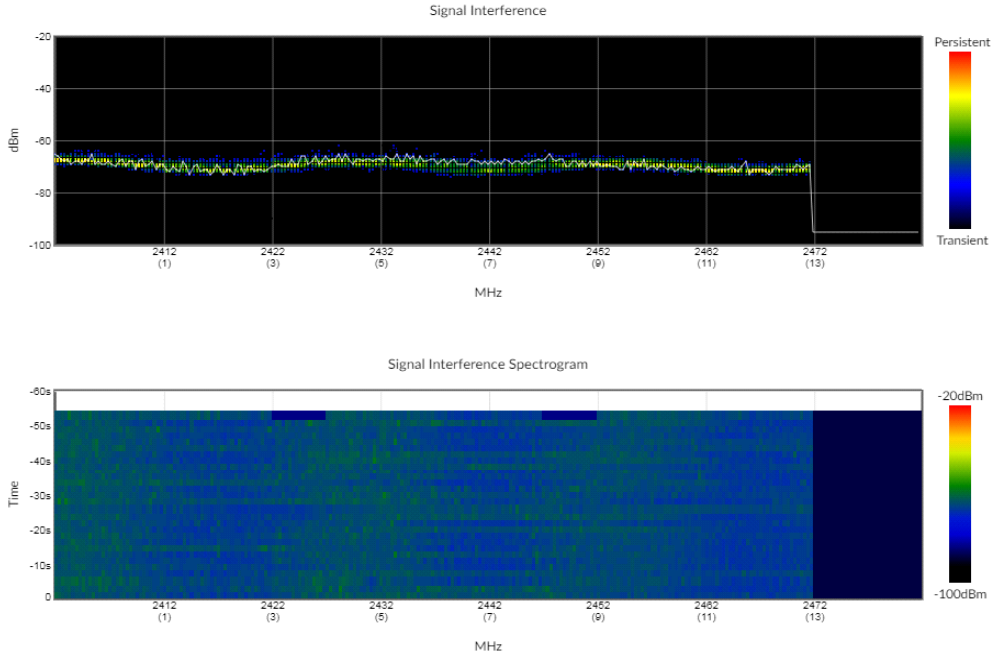
You can select the AP, Radio, and Channels to be scanned for interferences.

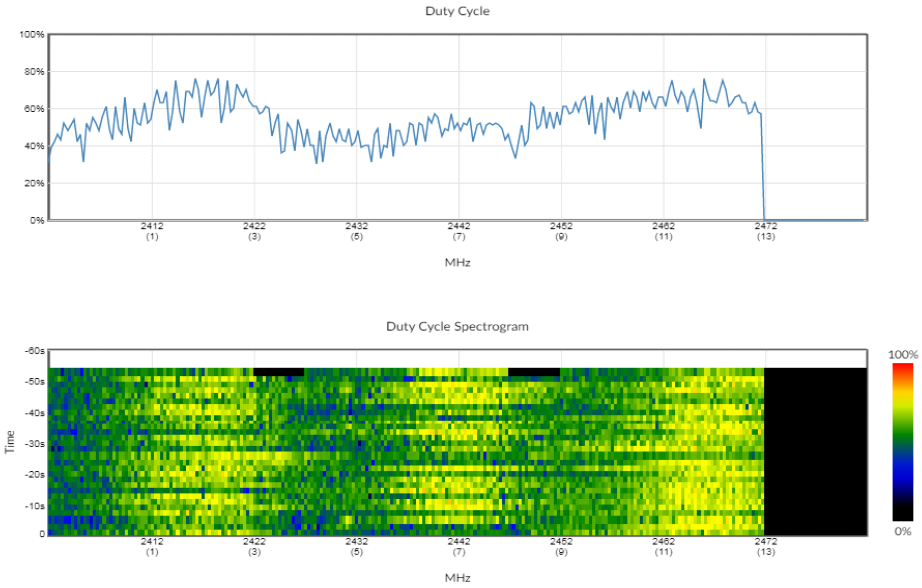
- The **Scan Duration** can be set to 1, 5, 30, 60 minutes or Infinite. When Infinite is selected the scan is performed till it is manually stopped.
- The **Sampling Interval** and the number of **Spectrogram Samples** cannot be modified.
- Select **Start** and the GUI periodically polls the spectrum analysis data based on the fixed sampling interval of 1000 milliseconds.



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/

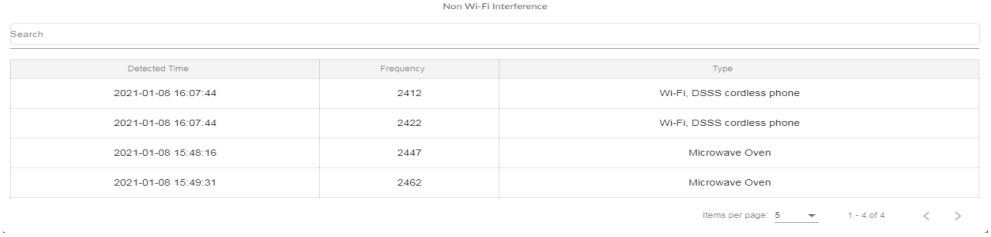
neighbouring AP is interfering, and the duty cycle spectrogram representing 60 such duty samples for each channel over a period of time.





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



VLAN Probe

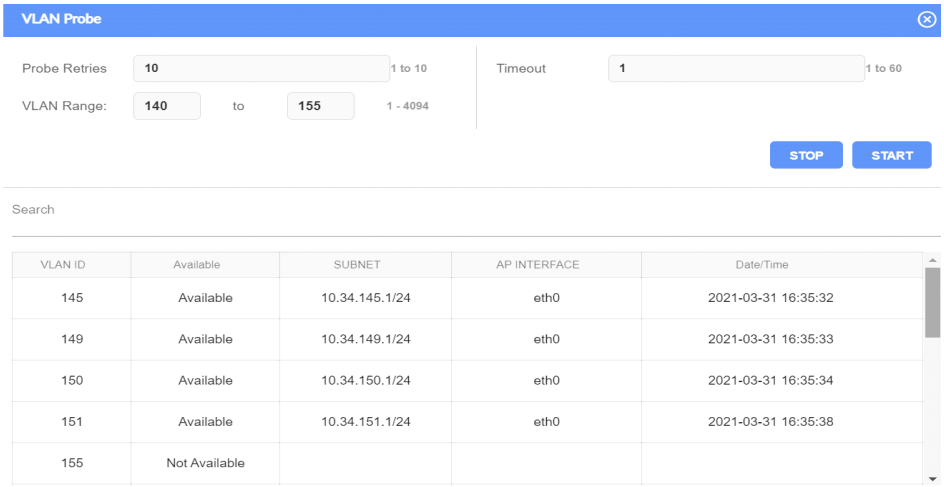
VLAN probe feature enables FortiAPs to probe connected VLANs and subnets. It sends DHCP probes from the FortiAP's Ethernet interface to specific VLANs on the wired interface

and returns information on their availability and subnet details. This helps diagnose and troubleshoot WiFi deployment issues.

Note: VLAN Probe is supported only on FortiGate controllers.

- **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.



Access Point Summary

These panels display the summary of the selected AP connected to the controller which is managed by the Network Manager.

Figure 33: *AP Summary*

A graphical representation of the average *Throughput,* average *Noise Level,* average *Loss%, Memory*, and *CPU* is displayed. The average *Retries%* and average *Channel Utilization%* for the 2.4GHz and 5GHz bands are also displayed. This data is displayed at configured time intervals, default is ten minutes.

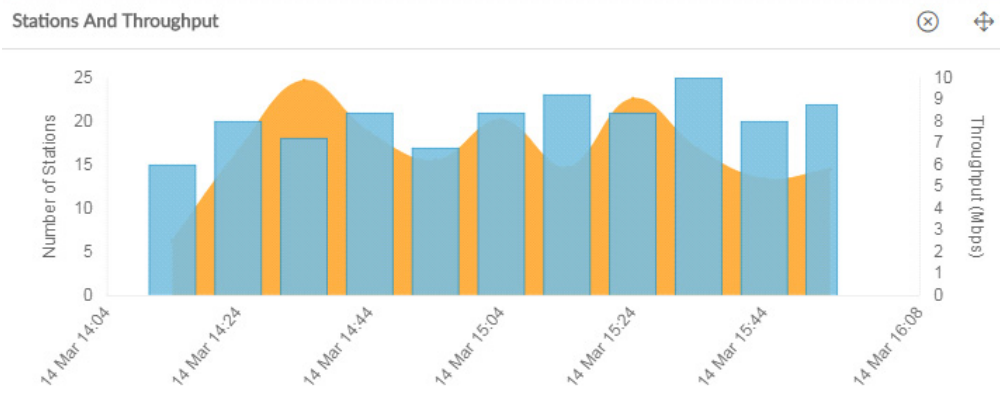
Trends, Statistics, and Top 5

This section of the Access Point dashboard graphically represents the AP statistics and trends that belong to the selected AP which are under administrative scope of your access settings. The trend graphs display data for the last 2 hours.

Stations and Throughput

The **Stations And Throughput** chart displays a station's combined transmitted and received bytes during a 2 hours interval. The graph displays the aggregate number of wireless stations connected to the selected AP and the average throughput (Mbps) at a given time.

Figure 34: *Stations and Throughput*

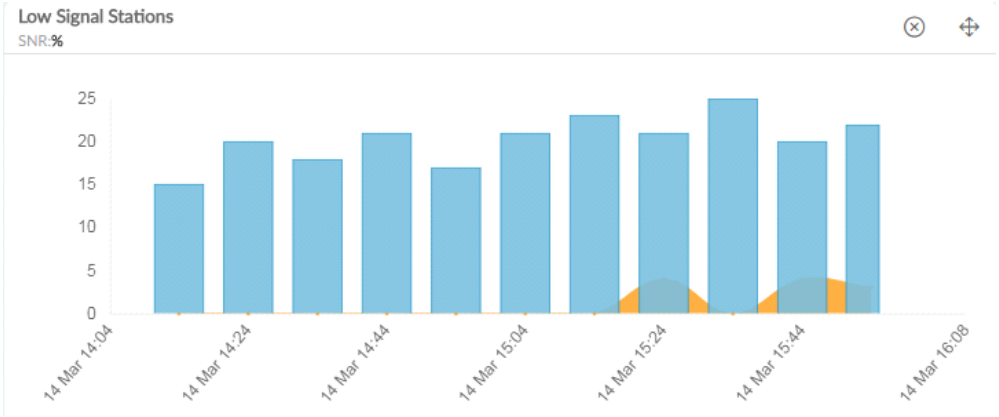


Each bar represents maximum stations connected and the average throughput during that interval. Hover the mouse over each bar to view the station count and throughput.

Low Signal Stations

The **Low Signal Stations** trend graph displays the total number of stations in the network facing low signal (SNR). SNR is defined as the signal strength relative to background noise.

Figure 35: *Low Signal Stations*



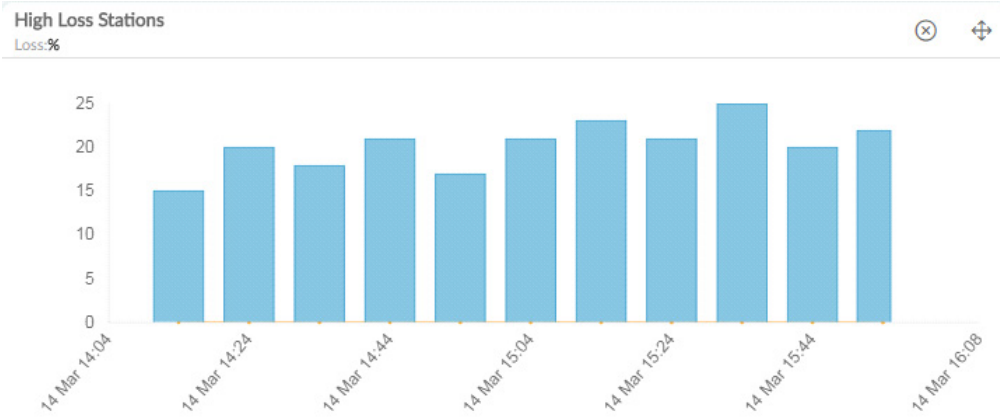
Hover the mouse over each of the bar, the maximum stations connected and the total number of low signal stations, as per the average SNR configured in the filter criteria during that interval are displayed. You can configure the threshold for low signal in the available filter options. The graph is plotted based on the configured filter criteria.

High Loss Stations

The **High Loss Stations** trend graph displays the total number of stations in the network facing high loss at a given point.

High Loss is defined as the percentage of 802.11 unicast packets transmitted for which no 802.11 Ack is received (> 40%). Hover the mouse over each of the section, the maximum stations connected and the total number of high loss stations, as per the average loss % configured in the filter criteria, during that interval are displayed.

Figure 36: *High Loss Stations*

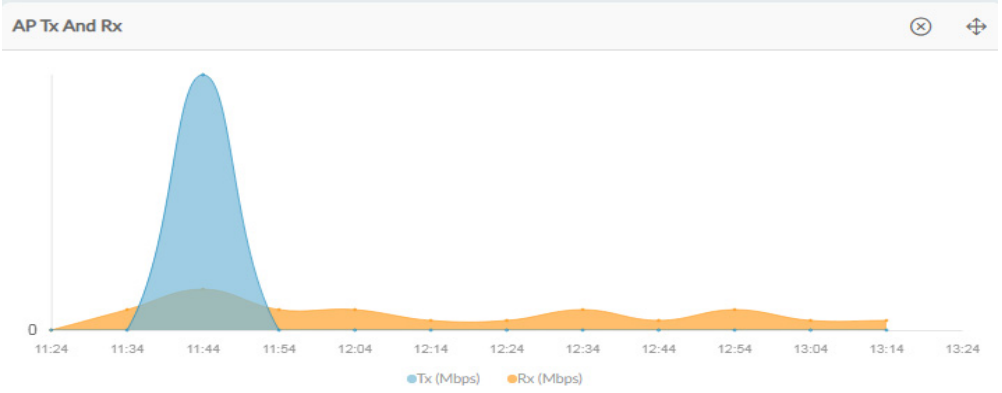


The graph is plotted based on the configured filter criteria.

AP Tx and Rx

The **AP Tx and Rx** trend graph displays the average Tx and Rx utilization (Mbps) of the access point.

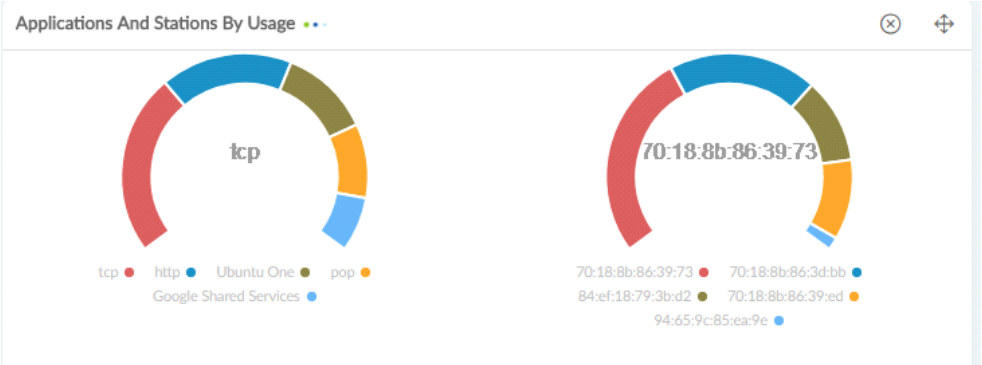
Figure 37: *AP TX and RX*



Applications And Stations By Usage

The **Applications And Stations By Usage** graph gives the summary of highly used applications by the selected AP and also top 5 stations with highest average bandwidth utilization.

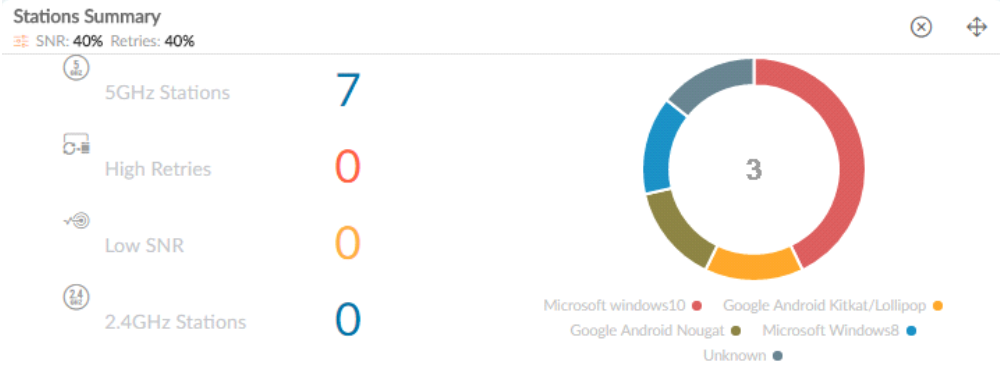
Figure 38: *Applications and Stations by Usage*



Stations Summary

This panel displays the summary of all the stations connected to the access point with the classification of stations by OS type. The total count of *5GHz Stations, 2.4GHz Stations, High Retries*, and *Low SNR* are displayed.

Figure 39: *Stations Summary*



Stations and Alarms

The **Alarms** panel displays the alarms reported on the AP and the **Stations** panel displays the total stations connected to the AP.

Station Group

This **Stations Group** dashboard screen displays the summary of all the stations within the station group. This dashboard provides status, activity, and health details of all stations in a station group.

The data is generated based on configured time intervals (default is 2 hours for trend graphs widgets and 10 minutes or 1 minute (based on the configured polling interval) for other widgets) on the server. Every station on the entire dashboard is click able which will navigate to station dashboard for the particular station.

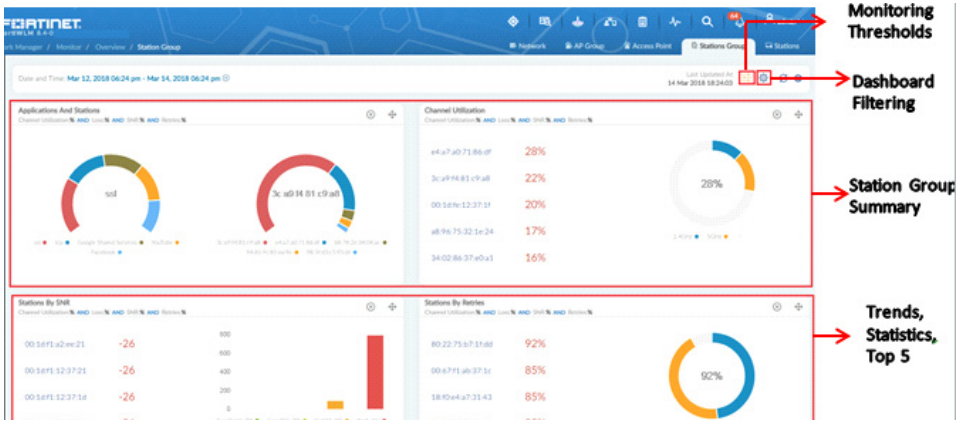
The Station Group Summary dashboard provides data from Trends, Statistics, and Top 5 Stations.

Dashboard Organization

The Station Group dashboard is organized into the following areas:

- Dashboard Settings
- Dashboard Filtering
- Trends, Statistics, and Top 5

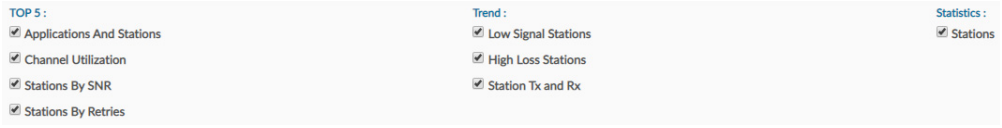
Figure 40: *Dashboard Organization*



Dashboard Settings

The dashboard settings allow you to refine the results displayed on the dashboard panels. It provides a graphical representation of the performance of these devices within the administrative scope of the logged in user.

Figure 41: *Dashboard Settings*



You can monitor the following Station Group parameters.

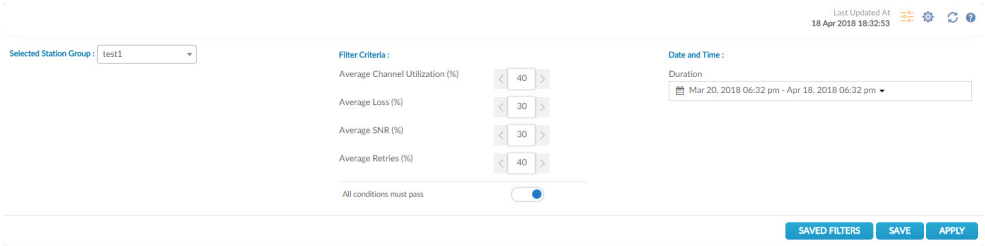
Filter By	Description

Top 5	• Applications And Stations • Channel Utilization • Stations By SNR • Stations By Retries
Trend	• Low Signal Stations • High Loss Stations • Station Tx and Rx
Statistics	• Stations

Dashboard Filtering

The filtering parameters of the dashboard analyse the statistics and behavior of specific stations, based on the configured threshold values.

Figure 42: *Dashboard Filtering*



The dashboard generates data at a configured time interval. You can select the time interval from the Date and Time drop-down list or define a custom time range.

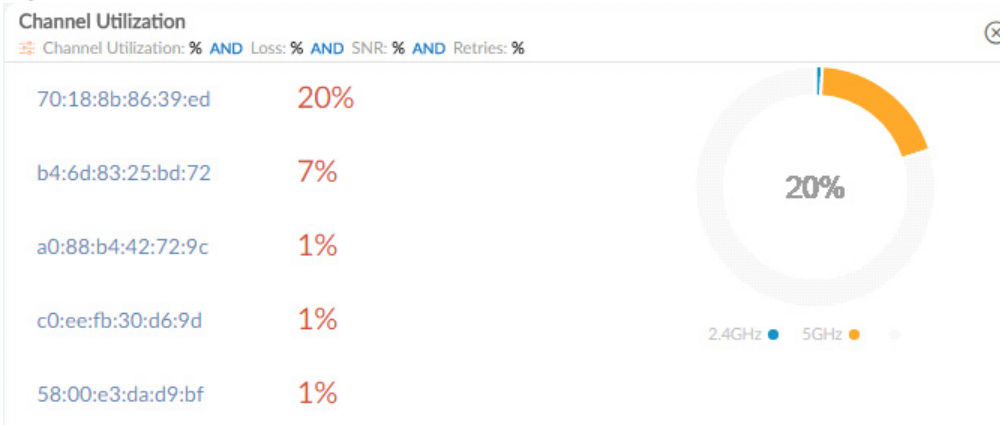
Trends, Statistics, and Top 5

This section of the Station Group dashboard graphically represents the station statistics and trends that belong to a selected Station group which are under administrative scope of your access settings. The trend graphs display data for the last 2 hours.

Channel Utilization

Provides the top 5 stations whose average channel utilization % for the configured period of time (default is ten minutes) meets the filter criteria. The chart displays the name and the corresponding average channel utilization % of stations in the group for 2.4GHz and 5GHz bands.

Figure 43: *Channel Utilization*

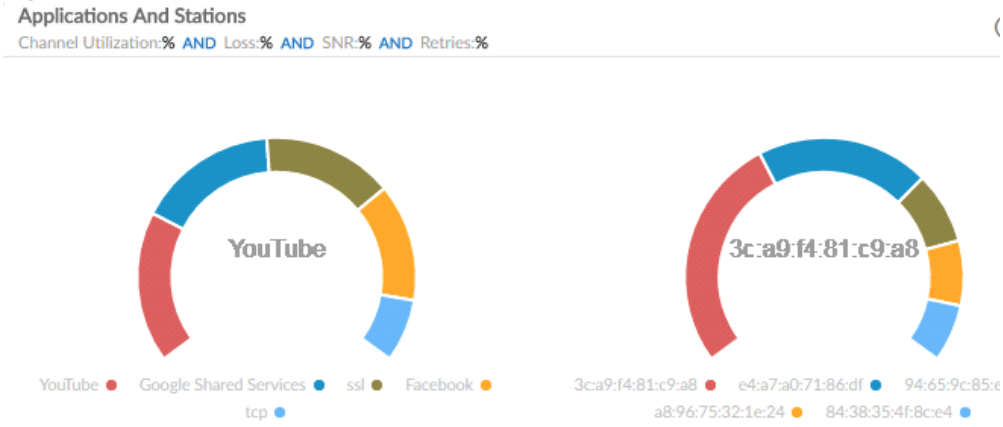


Clicking on the station name navigates to the **Stations** dashboard with the same filter applied.

Applications And Stations

This chart gives the summary of highly used applications and the associated stations within the selected station Group and also top 5 stations with highest average throughput within the station Group.

Figure 44: *Applications and Summary*

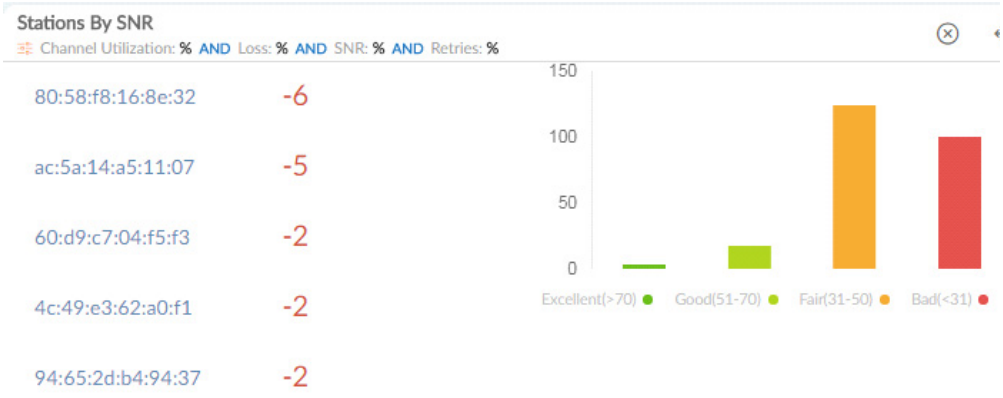


Stations By SNR

The **Stations By SNR** panel groups the stations based on the average SNR selected in the filter criteria and lists the top 5 stations within this group with lowest average SNR. The stations

are classified into *Excellent, Good, Fair*, and *Bad* categories based on the SNR. Hover over the bars to view the number of stations in each category.

Figure 45: *Stations by SNR*

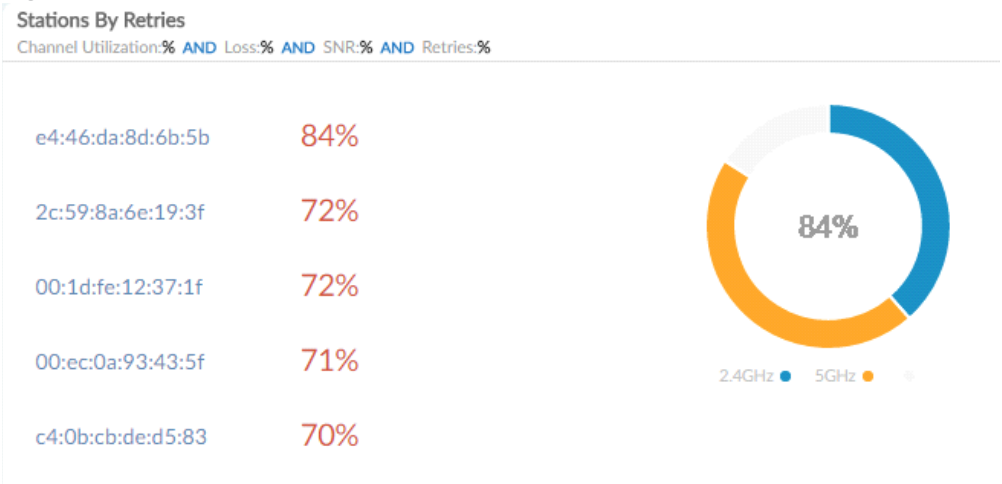


Clicking on the station name navigates to the **Stations** dashboard.

Stations By Retries

The **Stations By Retries** panel groups the stations based on the retries selected in the filter criteria and lists the top 5 stations within this group with highest average retries %. The chart displays the maximum retries % of stations in the group for 2.4GHz and 5GHz bands.

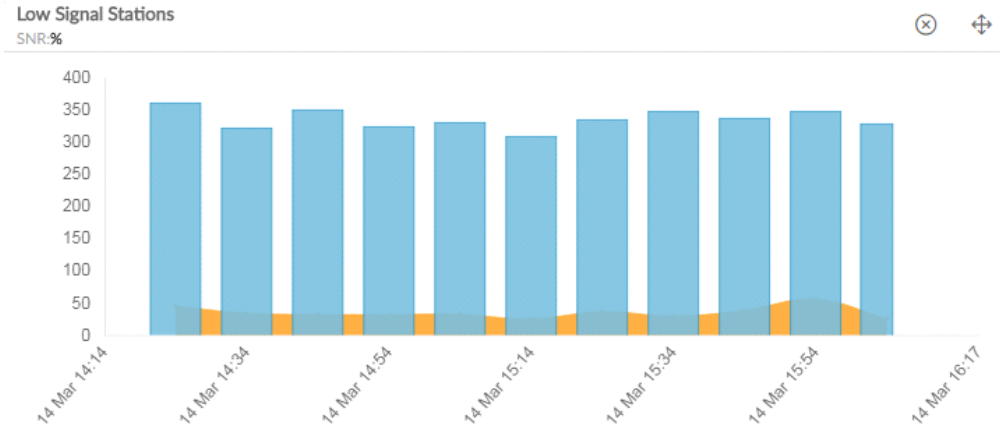
Figure 46: *Stations by Retries*



Low Signal Stations

The **Low Signal Stations** trend graph displays the total number of stations in the network facing low signal (SNR). SNR is defined as the signal strength relative to background noise.

Figure 47: *Low Signal Stations*

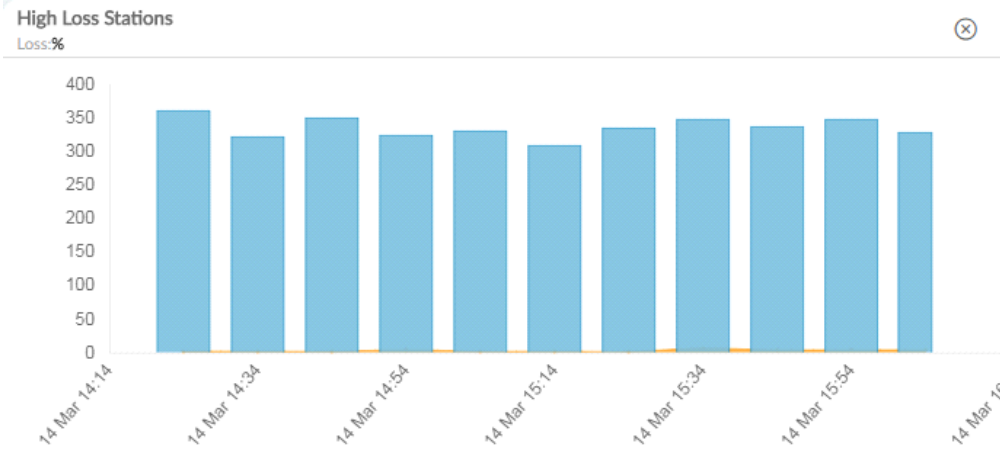


Hover the mouse over each of the bar, the maximum stations connected and the total number of low signal stations, as per the average SNR configured in the filter criteria, during that interval. The graph is plotted based on the configured filter criteria.

High Loss Stations

The **High Loss Stations** trend graph displays the total number of stations in the network facing high loss at a given point.

Figure 48: *High Loss Stations*



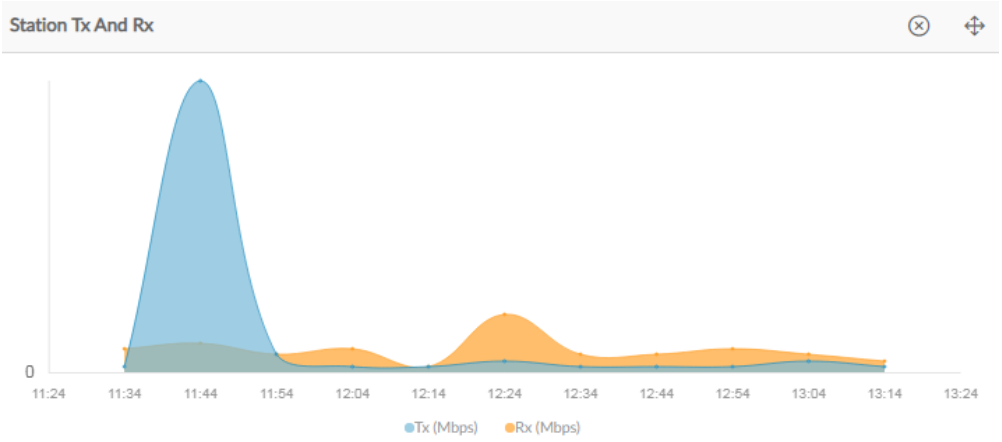
High Loss is defined as the percentage of 802.11 unicast packets transmitted for which no 802.11 Ack is received (> 40%). Hover the mouse over each of the section, the maximum stations connected and the total number of high loss stations, as per the average loss % configured in the filter criteria during that interval.

The graph is plotted based on the configured filter criteria.

Station Tx and Rx

The **Station Tx and Rx** trend graph displays the average Tx and Rx utilization (Mbps) of the station.

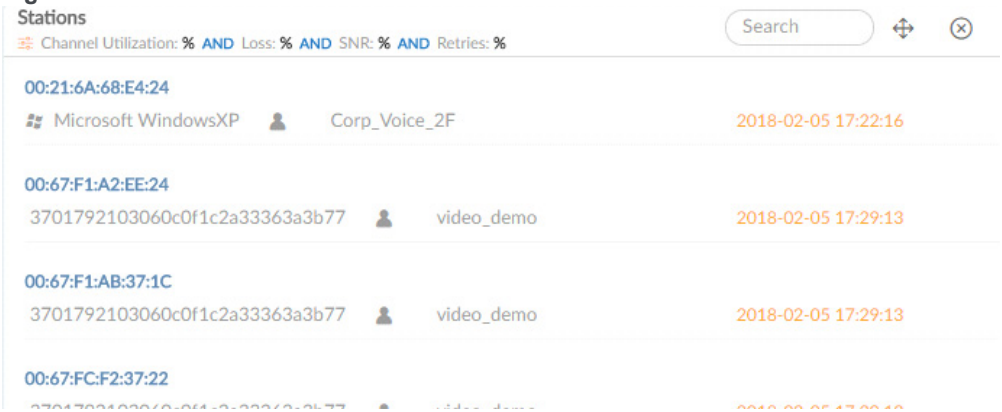
Figure 49: *Station Tx and Rx*



Stations

The **Stations** panel displays the details of all stations in the station group that meet the filter criteria.

Figure 50: *Stations*



Clicking on the Station name navigates to the **Stations** dashboard.

Stations

The **Stations** Dashboard screen displays in-depth information about the station activity. It provides the graphical representation of the Throughput, events, and the health of stations connected to the access points which are connected to a controller managed by the FortiWLM. The data is generated based on configured time intervals (default is 2 hours for trend graphs widgets and 10 minutes or 1 minute (based on the configured polling interval) for other wid-

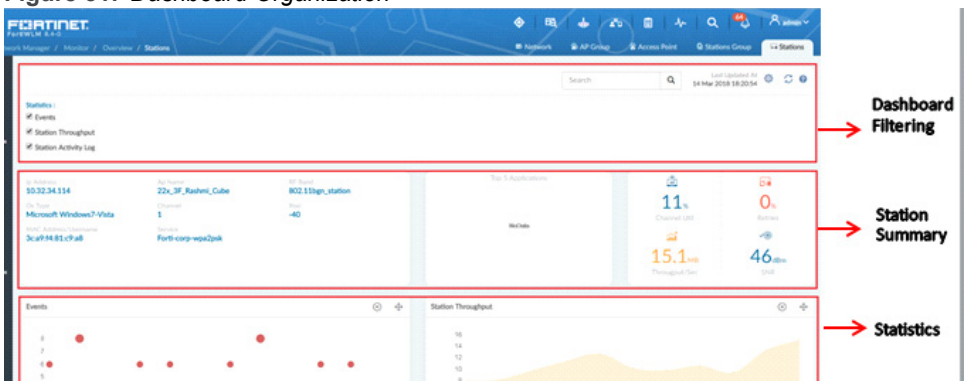
gets) on the server. All the links or pop-up from this page and status bar display the current data.

Dashboard Organization

The Access Point dashboard is organized into the following areas:

- Dashboard Settings
- Dashboard Filtering
- Station Summary
- Statistics

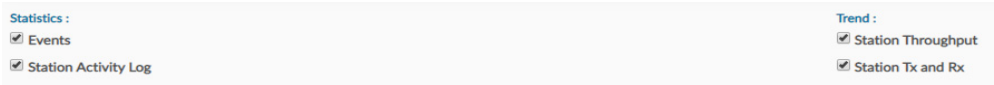
Figure 51: *Dashboard Organization*



Dashboard Settings

The dashboard settings allow you to refine the results displayed on the dashboard panels. It provides a graphical representation of the performance of these devices within the administrative scope of the logged in user. You can monitor the following network health parameters.

Figure 52: *Dashboard Settings*



You can monitor the following Station statistics.

- Events
- Station Throughput
- Station Activity Log
- Station Tx and Rx
- Station Location

Dashboard Filtering

The filtering parameters of the dashboard analyse the statistics and behaviour of specific stations associated with specific controllers, AP groups, and station groups based on the configured duration.

The dashboard generates data at a configured time interval. You can select the time interval from the Date and Time drop-down list or define a custom time range. Navigation to a different page retains the time duration setting.

Station Summary

These panels display the summary of the selected AP connected to the controller which is managed by the Network Manager.

Figure 53: *Stations Summary*

A graphical representation of the maximum *Throughput,* average *SNR%,* average *Retries%* and average *Channel Utilization%* for the 2.4GHz and 5GHz bands are displayed. This data is displayed for the last 10 minutes or 1 minute (based on the configured polling interval).

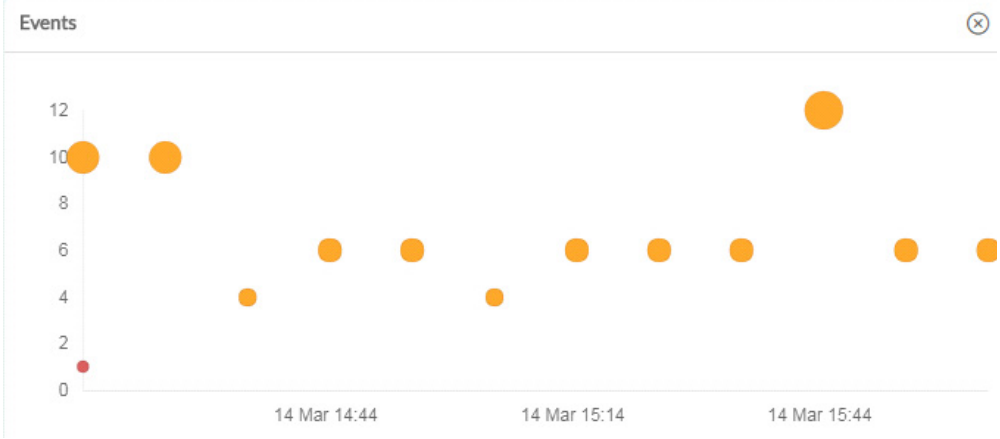
Statistics

This section of the Access Point dashboard graphically represents the AP statistics and trends that belong to the selected AP which are under administrative scope of your access settings.

Events

The 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.

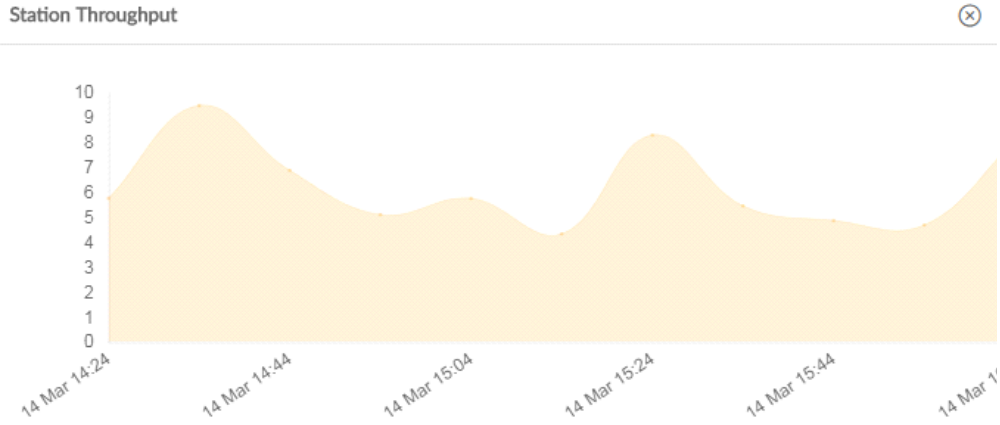
Figure 54: *Events*



Station Throughput

The **Stations Throughput** chart displays a station's combined transmitted and received bytes (Mbps) during the last 2 hours.

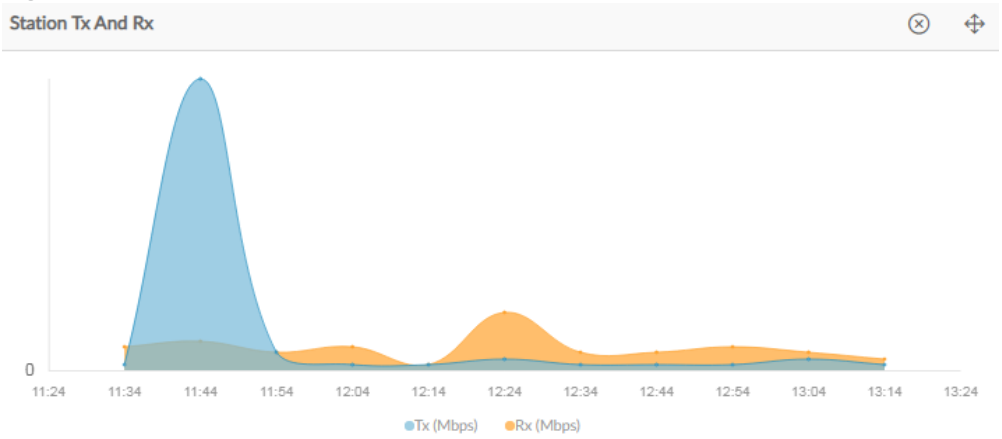
Figure 55: *Station Throughput*



Station Tx and Rx

The Station Tx and Rx trend graph displays the average Tx and Rx utilization (Mbps) of the station.

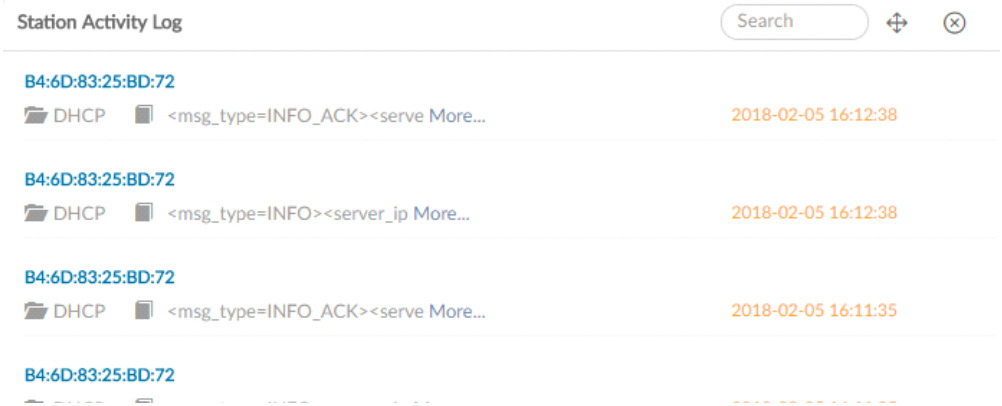
Figure 56: *Station Tx and Rx*



Station Activity Log

The **Station Activity Log** panel displays the station logs/activities of the selected station. This panel represents the station events of all stations. Most station events are updated almost immediately after the event occurs. The latest 40 events of the last 1 hour are available on the server.

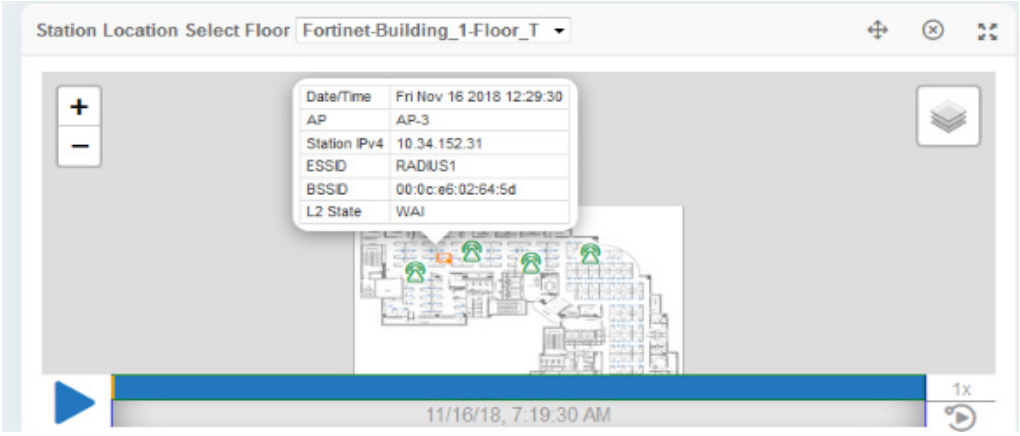
Figure 57: *Station Activity Log*



Station Location

The **Station Location** panel provides a graphical representation of the stations per floor. The floor map allows you to view the movement of the stations on a floor in the last 24 hours using the time-line view (with play and pause options). By default, the latest location of the station is displayed on the floor map.

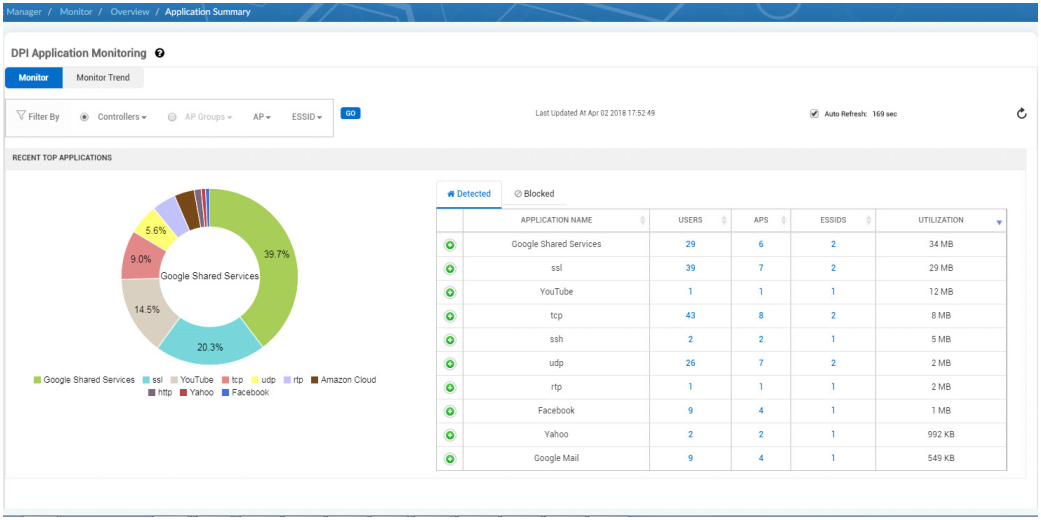
Note: This panel is available on the dashboard only when the location services are enabled.



Application Summary

You can monitor the traffic of top 10 applications used in your network. The Monitor > Overview > Application Summary dashboard provides detailed graph of top 10 applications.

Figure 58: *Application Visibility Dashboard*



The dashboard shows graphical display of traffic usage by Applications or Users (Clients).

- The *Pie chart* displays top 10 applications. Hover over pie slices to see traffic usage (in percentage) of an application.
- *Tabular data* with the list of top 10 applications. For each application, you can view the following:
  - Number clients using the application
  - Number of APs serving the clients using the application
  - Number of ESSID connected to clients using the application
  - Total traffic utilization in MB.
- The Blocked Statistics tab displays the list of blocked applications with the following details:
  - Number of users requesting these applications.
  - Number of APs the requests for access th these applications arrived.
- The *Trends* graph displays traffic usage in different intervals (2 hour, 1 day, 1 week, 1 month, and custom interval for a specified date range).

The trend graph data is maintained only for the last 30 days.

The application visibility dashboard allows you to monitor applications and stations based on the risk value associated with them. You can view pie charts grouping applications and users based on their risk values.

Select the *By Risk* tab to group applications and stations based on their risk values and usage information. Applications and users are assigned with these risk values; **low**, **elevated**, **medium**, **high**, and **critical**.

Note: The risk level cannot be defined for custom applications.

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 10 applications/users in that category along with their usage.

Channel Summary

This page contains detailed summary of channel utilization. The pie charts provides breakup of channel usage on 2.4 Ghz and 5 Ghz radios. For each of the radios, there are two pie charts.

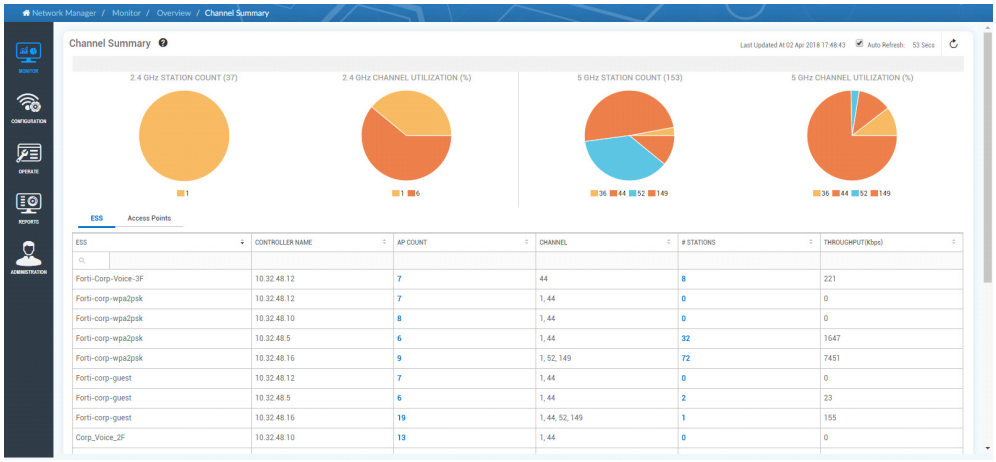
- Station Count - The number of stations connected to a specific channel in the radio.
- Channel Utilization - The total channel utilization (in percentage) of a channel in the radio.

NOTE: The icon below the pie-chart represents the channel number.

SSID and Access Points Tab

The SSID and Access Points tab provides 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.

Figure 59: *Channel Summary Dashboard*



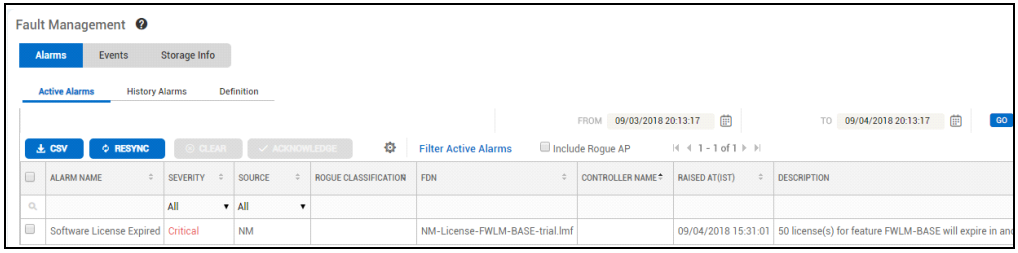
- SSID - The name of the SSID in your network.
- CONTROLLER NAME - The IP address of the controller that terminates the AP with this SSID.
- AP COUNT - The number of AP's broadcasting this SSID. Click on the hyperlinked number to view the following details about the AP.
  - AP NAME - The names of AP's 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 (%) -
  - RETRY (%) -
  - # STATIONS - Number of stations connected to this AP
  - THROUGHPUT (Kbps) - Total throughput of traffic passing through this AP
  - FLOOR MAP - Click the icon to get the physical location of the AP.
- 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.

Fault Management

The *Alarms and Events* interface is now available via a single dashboard as the *Fault Management.* The dashboard includes alarms and events for access points, controllers and *NM*. Fault management allows you to detect and notify faults encountered in the network.

Figure 60: *Fault Management*



The *Fault Management* screen is divided into the following tabs:

- *"Alarms"* **on page 86**
- *"Events"* **on page 92**
- *"Storage Info"* **on page 95**

Alarms

An *Alarm* is a notification of faults that occur over the course of time for an object. An alarm is either in *Active State* or *Cleared State*. When alarms are generated, you can either *Acknowledge* or *Clear the alarm* by simply checking the box alongside the desired alarm and clicking the appropriate button towards the bottom of the window. For an object, a new alarm cannot be raised until the old alarm is cleared. However, the same alarm on same object can be raised with different severity. During such scenarios, the new alarm will clear the old alarm.

- *Clear*—Moves the alarm from the *Active Alarms* table into the *Alarm History* table.
- *Acknowledge*—Marks the alarm as acknowledged in the *Acknowledged* column.

As seen in the figure above, the *Active Alarms* table provides several columns as described below:

Column	Description
Alarm Name	The name of the alarm triggered.

Column	Description

Severity	Displays the *Severity* of the alarm. The severity types are as follows:
	• Critical Alarms
	  • Critical Alarms are represented by *red* color and indicates the need for immediate action.
	  • Typical critical alarms are generated either when a controller or AP is down, or when a rogue AP is detected. The *Rogue* alarm is raised when the *Wired Rogue* is detected.
	• Major Alarms
	  • Major Alarms are represented by *orange* color and indicates the need for action when ever required.
	  • Typical major alarms are displayed due to *Authentication failure*.
	• Minor Alarms
	  • Minor Alarms are represented by *yellow* color and does not require any action.
	  • Typical minor alarms are displayed due to MIC errors.
	• Information Alarms
	  • Information Alarms are represented by *blue* color and is for information only. It does not require any action.

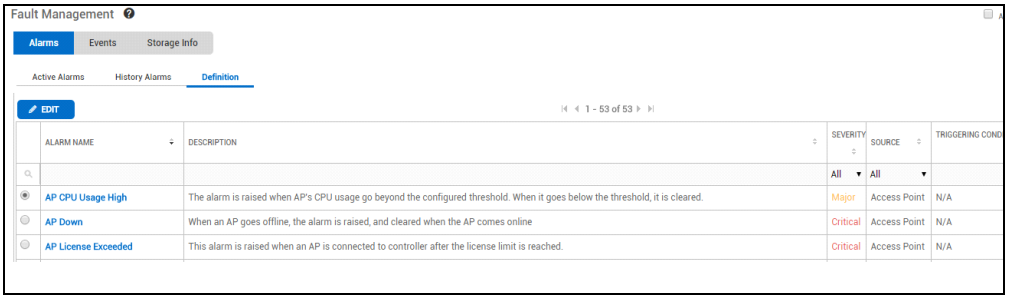
Source	Displays the Source name through which the alarm is raised. The following are the source names: • Controller • Access Point • NM

Column	Description
FDN (Full Distinguished Name)	The name of the device that triggered the alarm. Full Distinguished Name (FDN) identifies the name of the device that triggered the alarm. The abbreviations of *Fortinet Products* (SD, NM, SAM, WIPS and IDM) are prefixed as FDN followed by a connected dash also called as Relative Distinguished Names (RDN) and AP Identifier or ETH interface Identifier and Station MAC address. **Note**: The FDN received by SD applications are not supported by FortiWLM.
Controller	Displays the controller IP address.
Raised At	The date and time at which the alarm was triggered. **Note**: The time displayed will be in IST time zone. This can be modified by selecting the *Change Timezone* option.
Description	Detailed information regarding the alarm, including identifying device details.
Acknowledged	Indicates whether the alarm has been flagged as Acknowledged.
Actions	All the AP related alarms display the *AP Location* icon in the *Actions* column. Select the *Show AP Location* icon. The *AP Locator* screen is displayed. The *AP Locator* screen displays the selected AP located on the floor.

Modifying Alarm Definitions

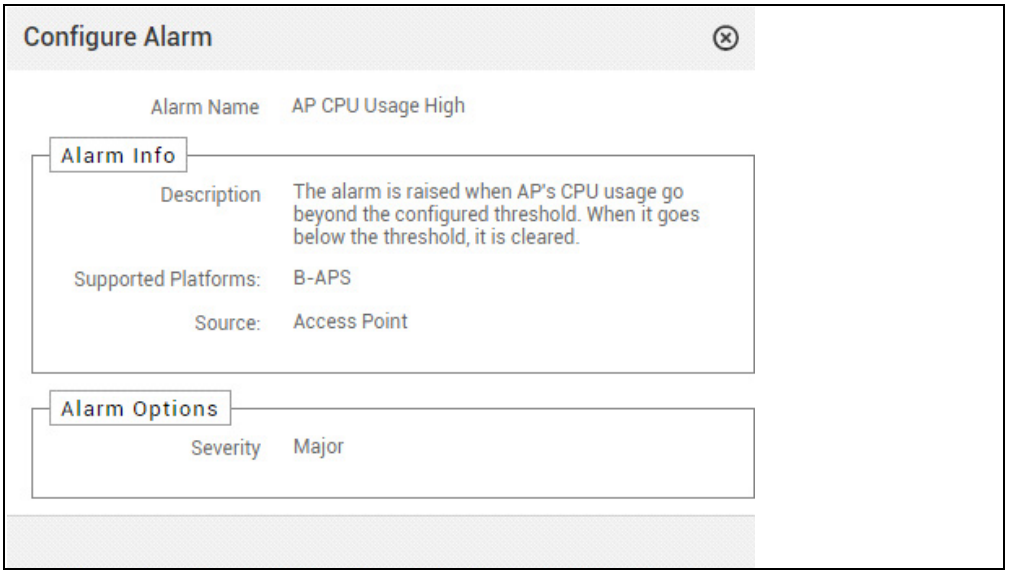
While *FortiWLM* provides a list of pre-configured alarms, you can also customize some of the attributes/triggering conditions for each of the alarm type. This can be performed via the *Alarms > Definition* tab.

Figure 61: *Alarm Definitions*



As shown above, each alarm comprises of a default predetermined *severity level, source, trigger condition, triggering threshold, SNMP,* and *syslog* but these values can be modified by selecting the desired *Alarm Name* followed by selecting the *Edit* option. The respective alarm details are displayed in the *Configure Alarm* window, as seen in *Figure 62 on* ***page 90***.

Figure 62: *Configure Alarm*



Modify the *Threshold Trigger Condition* and click *Save* when finished. If desired, you can click *Reload Default* to reset the alarms configuration to its original values.

The Threshold field's units will vary depending on the alarm selected—for example, when modifying *AP Memory Usage High*, the *Threshold* is measured in percentage of overall system memory (and defaults to 70%). However, in an alarm such as *Link Down*, no threshold is needed at all, as it is a binary alarm (i.e., it is triggered when a link to an AP goes down—there is no percentage involved).

Filter History Alarms

The *Filter History Alarms* allows you to filter alarms based on various parameters. Any of the following parameters can be selected from the *Filter History Alarms* popup. The table can be filtered using more than one parameter. For Example: You can filter alarms by providing the Alarm Name, FDN, and Source.

Column	Description
Alarm Name	Provide the alarm name.

Severity	Select the *Severity* of the alarm. The severity types are as follows:
	• Critical Alarms
	  • Critical Alarms are represented by *red* color and indicates the need for immediate action.
	  • Typical critical alarms are generated either when a controller or AP is down, or when a rogue AP is detected. The *Rogue* alarm is raised when the *Wired Rogue* is detected.
	• Major Alarms
	  • Major Alarms are represented by *orange* color and indicates the need for action when ever required.
	  • Typical major alarms are displayed due to *Authentication failure*.
	• Minor Alarms
	  • Minor Alarms are represented by *yellow* color and does not require any action.
	  • Typical minor alarms are displayed due to MIC errors.
	• Information Alarms
	  • Information Alarms are represented by *blue* color and is for information only. It does not require any action.

Source	Select the *Source* name through which the alarm is raised. The following are the source names: • Controller • Access Point • NM

Column	Description
FDN (Full Distinguished Name)	Provide the name of the device that triggered the alarm. Full Distinguished Name (FDN) identifies the name of the device that triggered the alarm. The abbreviations of *Fortinet Products* (SD, NM, SAM, WIPS and IDM) are prefixed as FDN followed by a connected dash also called as Relative Distinguished Names (RDN) and AP Identifier or ETH interface Identifier and Station MAC address. **Note**: The FDN received by SD applications are not supported by FortiWLM.
Controller	Provide the controller IP address.
Description	Provide a detailed information about the alarm raised followed by alarm cleared.
Acknowledged	Provide if the user has acknowledged the alarm raised. The options are Yes or No. The default is No.

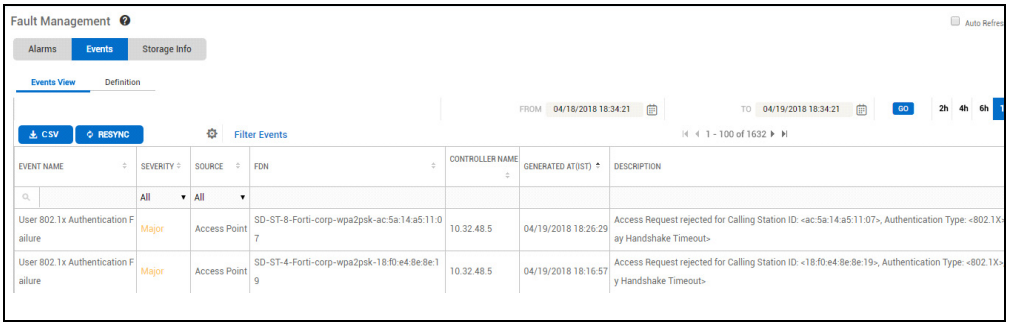
1. Select *Save* option to filter the history alarms with the parameters mentioned in the above table.
2. Select *Reset* option to reset all the fields mentioned in the above table.
3. Select *Cancel* to close the filter history alarms popup.

See the ***Fault Management*** screen in Online Help for detailed information on *configuring Alarms* and *Alarm definitions*.

Events

The *Events* are significant occurrences that take place on the E(z)RF-managed network. They are similar to alarms. The Event instances are generated based on a condition and can be generated multiple times. However, while alarms typically require some form of user intervention to resolve the problem, events simply provide an indication that a change has been made.

Figure 63: *Fault Management - Events*



The table below provides a brief description of the columns provided in the *Events* table.

Column	Description
Event Name	The name of the event triggered.
Severity	The severity level; can range from *Information, Minor, Major, Critical*.
Source	Displays the source name through which the event is raised. The following are the source names: • Controller • Access Point • NM
FDN	The name of the device that triggered the event. *Full Distinguished Name* (FDN) identifies the name of the device that triggered the event. The abbreviations of *Fortinet Products* (SD, NM, SAM, WIPS and IDM) are prefixed as FDN followed by a connected dash also called as Relative Distinguished Names (RDN) and AP Identifier or ETH interface Identifier and Station MAC address. **Note**: The FDN received by SD applications are not supported by FortiWLM.
Raised At	The date and time at which the event was triggered. **Note**: The time displayed will be in IST time zone. This can be modified by selecting the *Change Timezone* option.

Column	Description
Detail	Detailed information regarding the event, including identifying device details.

Modifying Event Definitions

While *FortiWLM* provides a list of pre-configured events, you can also customize some of the attributes/triggering conditions for each of the event type. This can be performed via the *Events* > *Definition* tab. Each event has a predetermined severity level, trigger condition, and threshold, but these values can be modified by selecting the desired *Event Name* followed by selecting the *Edit* option. The respective event details are displayed in the *Configure Event* window.

Modify the *Threshold Trigger Condition* and click *Save* when finished. If desired, you can click *Reload Default* to reset the event's configuration to its original values.

Filter Events

The *Filter Events* allows you to filter events based on various parameters. Any of the following parameters can be selected from the *Filter Events* popup. The table can be filtered using more than one parameter. For Example: You can filter alarms by providing the Event Name, FDN, and Source.

Column	Description
Event Name	Provide an event name.
Severity	Select the severity level; can range from *Information, Minor, Major, Critical*.
Source	Select the source name through which the event is raised. The following are the source names: • Controller • Access Point • NM

Column	Description
FDN	Provide the name of the device that triggered the event. *Full Distinguished Name* (FDN) identifies the name of the device that triggered the event. The abbreviations of *Fortinet Products* (SD, NM, SAM, WIPS and IDM) are prefixed as FDN followed by a connected dash also called as Relative Distinguished Names (RDN) and AP Identifier or ETH interface Identifier and Station MAC address. **Note**: The FDN received by SD applications are not supported by FortiWLM.
Controller	Provide the *Controller IP Address*.
Detail	Provide the complete or partial description about the event generated.

1. Select *Save* option to filter the events with the parameters mentioned in the above table.
2. Select *Reset* option to reset all the fields mentioned in the above table.
3. Select *Cancel* to close the filter events popup.

See the ***Fault Management*** screen in Online Help for detailed information on *configuring Events* and *Event definitions*.

Storage Info

The Storage Info displays the *Storage Configuration* details of the *Alarms* and *Events*.

- *"Events - Storage Configuration"* ***on page 95***
- *"History Alarms - Storage Configuration"* ***on page 96***

Events - Storage Configuration

The *Events - Storage* configuration displays the following details:

Field	Description
Storage Capacity	Displays the maximum number of Events that can be stored in the database. The maximum storage capacity is 4000000 rows.
Current Usage	Displays the current usage of *Events* storage in percentage

Field	Description
Purge Options	
Purge is a scheduled operation that allows you to delete records following a configurable predefined setting. The maximum number of records to store and the number of records to retain is configured in the database. Purge operation is enforced, once the database crosses the configured number of records. The most former record is deleted from the database.	
Number of events to keep after every purge	Displays the percentage of *Events* to be retained after purge.
Schedule Purge	Displays the scheduled time of purge for the *Events*. Select the desired time from the drop-down list.
Enable Auto System Purge	System will purge events once usage reaches 99%.

History Alarms - Storage Configuration

The *History Alarms - Storage* configuration displays the following details:

Field	Description
Storage Capacity	Displays the maximum number of Alarms that can be stored in the database. The maximum storage capacity is 2000000 rows.
Current Usage	Display current usage of historical alarm storage in percentage.
Purge Options	
Number of History Alarms to keep after every purge	Display percentage of historical alarm to retain after purge.
Schedule Purge	Displays the scheduled time of purge for the *History Alarms*. Select the desired time from the drop-down list.
Enable Auto System Purge	System will purge historical alarms once usage reaches 99%.

Heat Maps

The heat map allows you to verify the coverage and performance of your WLAN APs. You can also use the maps to visually locate APs sending alarms. Use the map editor to set up your site maps.

1. In the *Network Heat Maps* screen, select a *Location* from the menu on the left to see the corresponding map.
2. Hover the mouse pointer over the objects on the screen to see details. For example, for this throughput map, by hovering the mouse pointer on an AP icon displays the *Name, model, Mac Address, status of the AP* and *throughput value*. If you change the *Heat Map Type*, be sure to click *Refresh* icon.
3. In the *Network Heat Maps* screen select a floor. The following five types of heat maps can be viewed.

Throughput Heat Map

Throughput maps display the AP throughput over the area represented by the map. The APs on the map is differentiated by using different colors for the regions around APs corresponding to the AP throughput value. Move your mouse on an AP icon to display the following:

- Name
- AP Model
- MAC Address
- Status of the AP
- Throughput in Kbps.
- Right click an *AP* and select *Show Details* to view the *AP details* and *Station details*.
  - **AP details**: *AP ID, AP Name, AP MAC, AP IP Address, Controller, and Total Stations.*
  - **Station details**: *MAC Address, IP Address, Last Known Association, User name, Throughput, Loss%, RSSI, Airtime Utilization, L2 State, and L3 State*.
- Click the MAC address to view the *Station Trend Dashboard*.

Figure 64: *Throughput Heat Map*

The filtering option comprises of *All, 2.4 GHz [default], 5 GHz* and *selected* channels within the two bands.

Loss Heat Map

Loss maps show AP loss over the area represented by the map. The *Loss* maps differentiate APs on the map by using different colors for the regions around APs corresponding to the AP Loss% value. Move your mouse on an AP icon to display the following:

- Name
- AP Model
- MAC
- Status
- Loss(%)
- Right click an AP and select *Show Details* to view the *AP details* and *Station details*.
  - **AP details**: *AP ID, AP Name, AP MAC, AP IP Address, Controller, and Total Stations*
  - **Station details**: *MAC Address, IP Address, Last Known Association, User name, Throughput, Loss%, RSSI, Airtime Utilization, L2 State,* and *L3 State*.
- Click the MAC address to view the *Station Trend Dashboard*.

Figure 65: *Loss Heat Map*

The filtering option comprises of *All, 2.4 GHz [default], 5 GHz* and *selected* channels within the two bands.

Channel Utilization Heat Map

The *Channel Utilization* maps differentiate APs on the map by using different colors for the regions around APs corresponding to the AP channel utilization value. Move your mouse on an AP icon to display the following:

- Name
- AP Model
- MAC Address
- Status
- Channel Utilization (%)
- Right click an AP and select *Show Details* to view the *AP details* and *Station details*:
- **AP details**: *AP ID, AP Name, AP MAC, AP IP Address, Controller, and Total Stations.*
- **Station details**: *MAC Address, IP address, Last Known Association, User name, Throughput, Loss%, RSSI, Airtime Utilization, L2 State,* and *L3 State*.
- Click the MAC address to view the *Station Trend Dashboard*.

Figure 66: *Channel Utilization Heat Map*

The filtering option comprises of *All, 2.4 GHz [default], 5 GHz* and *selected* channels within the two bands.

Number of Stations Heat Map

The Number of Stations Heat Map, represents the low signals over the area represented by the map. The Number of Stations maps differentiate APs on the map by using different colors for the regions around APs corresponding to the number of stations per AP. Move your mouse on an AP icon to display the following:

- Name
- AP Model
- MAC Address
- Status of the AP
- Number of Stations
- Right click an AP and select *Show Details* to view the *AP details* and *Station details*:
  - **AP details**: *AP ID, AP Name, AP MAC, AP IP Address, Controller ID, and Total Stations.*
  - **Station details**: *MAC Address, IP Address, Last Known Association, User name, Throughput, Loss%, RSSI, Airtime Utilization, L2 State,* and *L3 State*.
- Click the MAC address to view the *Station Trend Dashboard*.

Figure 67: *Number of Stations Heat Map*

The filtering option comprises of *All, 2.4 GHz [default], 5 GHz* and *selected* channels within the two bands.

Signal Strength Heat Map

Signal strength heat map provides a distribution of signal quality over the floor map. The signal strength is represented in dBm and is divided into color buckets. The *Signal Strength* maps display the availability of signal over the area represented by the map. Select different cut-off values to view the signal coverage.

Figure 68: *Signal Strength Heat Map*

The signal strength heat map allows you to view the signals of all the APs on the floor. Due to this, the FortiWLM displays heat map for all APs irrespective of whether the logged in user has scope for those APs or not. This enables you to capture accurate signal value for all APs located on the floor

Select a location from the menu on the left to see the corresponding map. Move your mouse over the AP icon to display the following:

- AP Name
- AP Model
- AP MAC
- Status of the AP
- Signal Strength
- Right click an AP and select *Show Details* to view the *AP details* and *Station details*:
  - **AP details**: AP ID, AP Name, AP MAC, AP IP Address, Controller ID, and Total Stations.
  - **Station details**: *MAC Address, IP Address, Last Known Association, User name, Throughput, Loss%, RSSI, Airtime Utilization, L2 State,* and *L3 State*.
- Click the MAC address to view the *Station Trend Dashboard*.

The filtering option comprises of *All, 2.4 Hz [default], 5 GHz* and *selected* channels within the two bands.

With signal strength heat map having smooth transition in colors, the color at a given point may not exactly match with the bucket colors. For such cases, it should be interpreted as a value that is greater/lower than the nearest bucket color.

- **Coverage Cut Off**: Coverage cutoff [default being none] can be used to see the signal coverage region within the cutoff value specified. The cutoff range is from -42dBM to -90dBM.

In order to view the signal strength heat map of a floor, follow the steps:

- Ensure the APs are placed accurately through the map management feature.
- Click on the *Heat maps -> Floor*, select the RF band of choice, or the relevant channel.
- Choose a cutoff that is of interest.
- Click on *Refresh* icon.

Locationing

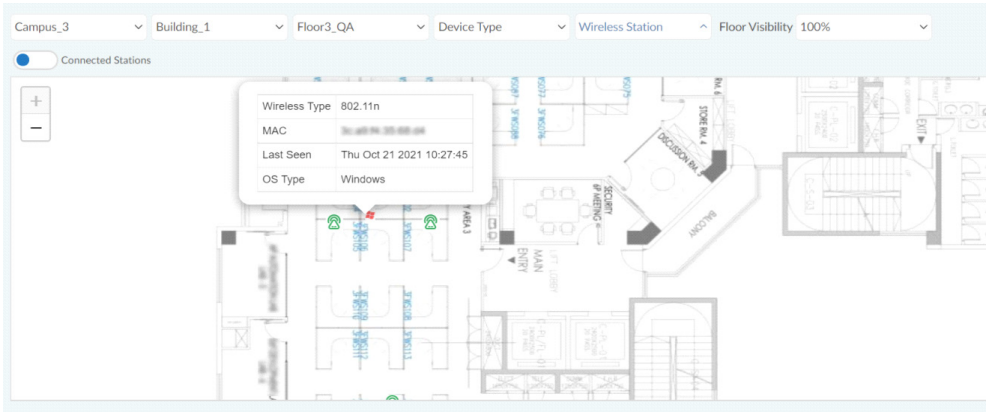
The locationing feature plots the current location of all stations on the floor map imported into the FortiWLM. FortiWLM plots the current location based on the location feed received from all controllers (which are in turn connected to APs) and does not display the movement of the stations.

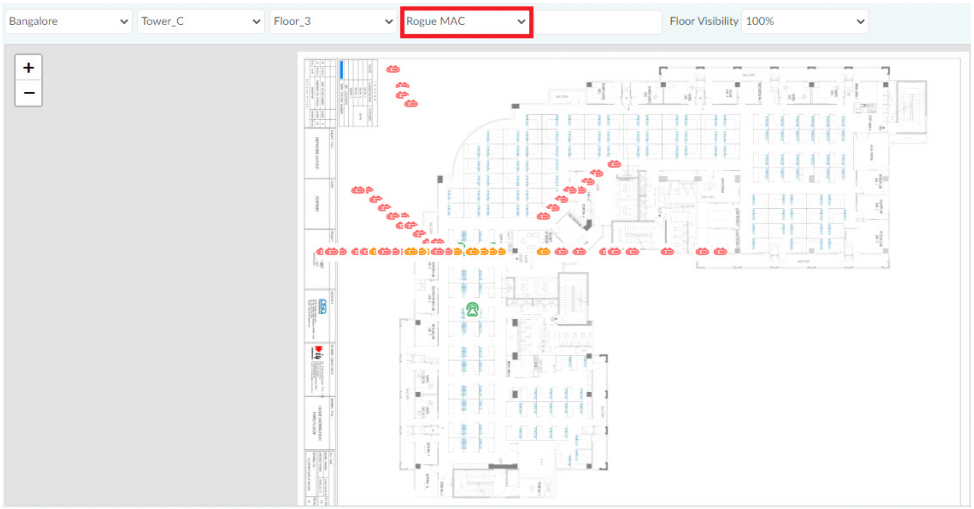
FortiGate

You can filter and view device locations based on the site, building, and floor. 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.





FortiWLC

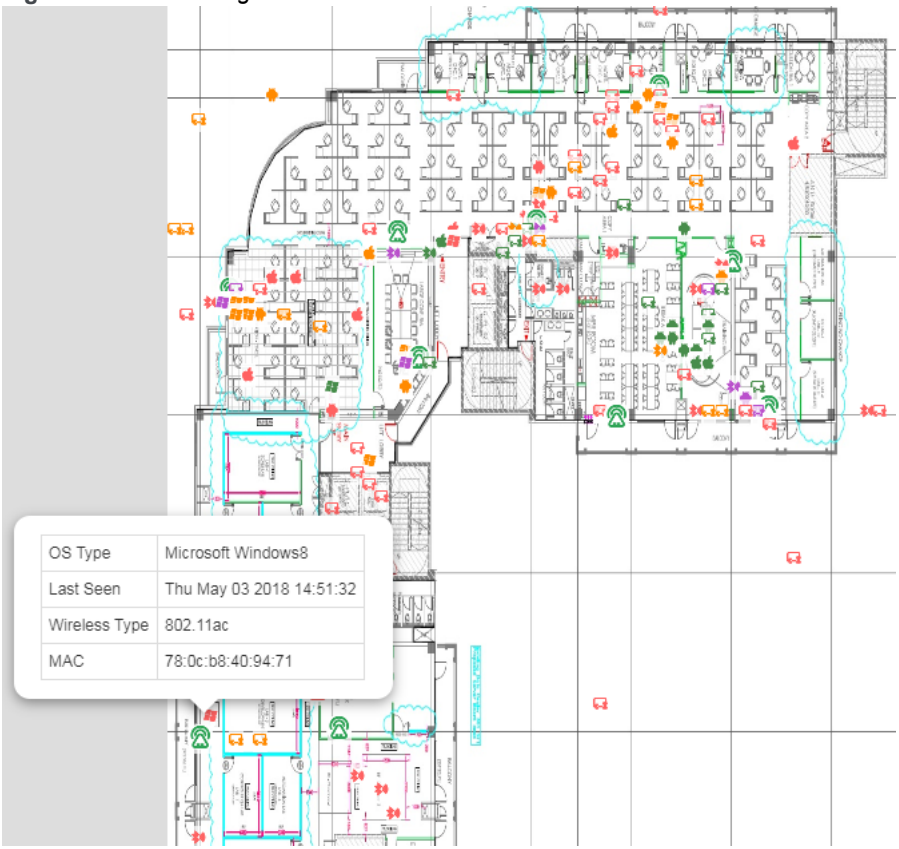
For FortiWLM to display the location data, a Location Services profile with the following configuration should be pushed to the controller. A default Location Services profile, *WLM_Locationing*, exists in FortiWLM with this configuration. You can enable and use the default profile.

- Report Format – Forti-Presence
- Project Name – FWLM

- Secret – The secret key displayed in *Administration* > *System Settings* > *Maintenance*.

Select the campus and the floor details to monitor the station locations. These filters can be applied, *Device Type, Wireless Type, OS Type*, and *Station MAC*. You can set the **Floor Visibility** and magnify the floor view.

Figure 69: *Locationing data*



Service Control

The *Service Control Summary* screen displays the list of services discovered in the network. By default, wireless services in all ESSIDs and all APs and wired services on VLAN 0 on the *NM* and controller's wired interface will be selected. To modify this, change the services that are discovered using *"Modifying Service Control Global Configuration"* ***on page 142***.

The *Service Control Summary* consists of the following sections:

1. **Statistics**: The Statistics section provides a graphical representation (pie chart) of the services discovered in the network. The area of each sector is proportional to the percent-

age of the number of services by each category against the total number of services. The following two types of services are graphically represented:

- **Services Chart**: The services chart provides the service types that are discovered in the network. The chart is color coded based on the service types.
- **Wired/Wireless Chart**: This chart is about the services discovered in the network based on the Wired or Wireless network. The chart is color coded based on the network type, Wired or Wireless.

Service Details: The Service Details section provides the information of the services that are discovered in the network. The *Controller, Service, Service Name, Service Type, Location, Node Name, Source Type,* and *Source* details are displayed in this section.

Mismatched APs

The APs are considered to be in *Mismatched* state when the radio or connectivity configuration present on the controller for the AP is not same as the radio or connectivity configuration which was applied from the *FortiWLM* for that AP. The sync status a modified AP is displayed as *Not in sync with Controller* on the *FortiWLM* server.

The *Mismatch APs* icon is available on the *FortiWLM* screen's *Status bar*, which when clicked is redirected to *APs Not In Sync With NMS Configuration* screen providing a list of APs with the configuration mismatch displayed along with the time stamp when the mismatch was detected.

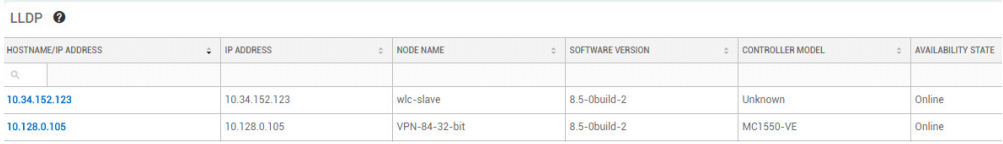
1. The *APs Not In Sync With NMS Configuration* screen is displayed providing the *Name, MAC Address, Device Group, Controller, Applied Template, Difference and Review Status* details along with the *Mismatch* details.
2. The Mismatch details wizard provides the mismatch configuration details of the AP Template (Radio Profile and Connectivity Profile).
3. The details displayed on the *Mismatch Details* wizard must be acknowledged by selecting the below options:
   - Reviewed/Acknowledged
   - Reviewed
4. Once the mismatch is acknowledged, the mismatch will be excluded from the count displayed on the *Status bar*. Select *Close*.

See the ***APs Not In Sync With NMS Configuration*** screen by selecting the *Mismatched APs* link in Online Help for a detailed information on *Mismatched APs* topic.

LLDP

Navigate to *Monitor* > *Overview* > *LLDP* to view the controller and access points' information along with their neighboring switch details. Click on the HOSTNAME/IP ADDRESS of the Controller to view the details.

Figure 70: *LLDP dashboard*



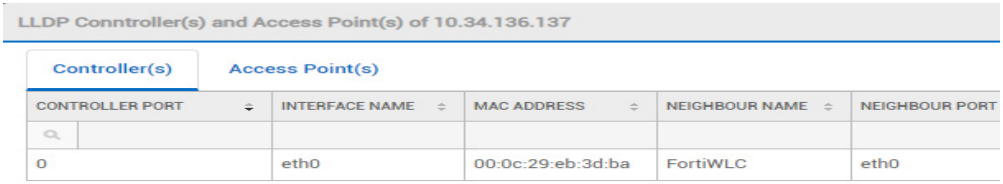
Field	Description
Hostname or IP Address	Displays the Controller’s Hostname or IP Address.
IP Address	Displays the Controller's IP Address.
Node Name	Displays the Hostname configured on the Controller.
Software Version	Displays the Controller’s runtime Software Version.
Controller Model	Displays the Controller's appliance hardware model such as MC4100 or MC3000.
Availability State	Indicates whether a controller is reachable or not from Network Manager. • **Online** indicates reachable • **Offline** indicates not-reachable • **Unmanaged** indicates not managed by Network Manager
Management State	Displays the monitoring state of the Controller. **Active** or **Inactive**.

Displays the controller and access points' information along with their neighboring switch details.

Click on the **HOSTNAME/IP ADDRESS** of the Controller to view the following details.

Controller (s)

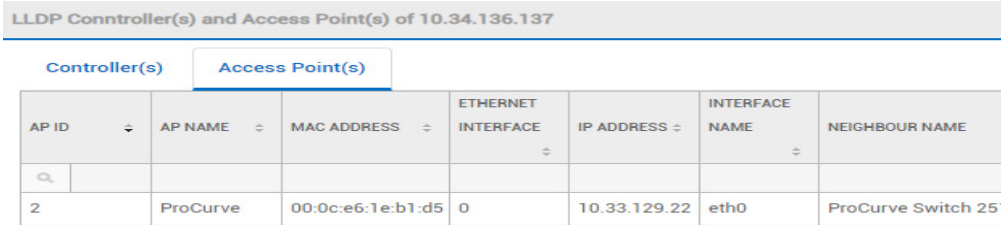
The following details are displayed for controllers**.**



Field	Description
Controller Port	Displays the port number of the Controller that receives and sends LLDP packets to the particular switch.
Interface Name	Displays the interface name of the Controller that receives and sends LLDP packets to the particular switch.
MAC Address	Displays the MAC address of the Controller.
Neighbour Name	Displays the neighboring switch with which the Controller exchanges LLDP information.
Neighbour Port	Displays the port of the neighboring switch that is connected to the Controller.
Neighbour IP Address	Displays the IP address of the neighboring switch that is connected to the Controller.
TTL	Displays the Time-To-Live (TTL) of the LLDP packets.
Timestamp	Displays the time of the last exchange of LLDP information between the controller and the switch.

Access Point (s)

The following details are displayed for access points.



Field	Description
AP Name	Displays the name of the access point.

Field	Description
MAC Address	Displays the MAC address of the access point.
IP Address	Displays the IP address of the access point.
Interface Name	Displays the interface name of the access point that receives and sends LLDP packets to the particular switch.
Neighbour Name	Displays the neighboring switch with which the access point exchanges LLDP information.
Neighbour Port	Displays the port of the neighboring switch that is connected to the access point.
Neighbour IP Address	Displays the IP address of the neighboring switch that is connected to the access point.
TTL	Displays the Time-To-Live (TTL) of the LLDP packets.
Timestamp	Displays the time of the last exchange of LLDP information between the access point and the switch.

Multiple PSK Stations

The users authenticated with a PSK, will have their details cached here. The associated client station MAC Address, IP address, ESS ID, associated group name and user name, and the timestamp of the last station update are displayed. If the PSK profile is removed from the Security Profile or is deleted, then the PSK profile cache is also deleted. The cache is not added for MAC bound PSK profile.

Figure 71: *Multiple PSK stations*

Client Exclusion View

This page monitors the clients blocked as per the configured client exclusion policy.

The MAC Address of the blocked client, the controller name, the exclusion reason, and the time remaining for the client to be blocked are displayed.

Detailed Dashboards

The *Detailed Dashboard* provides at-a-glance system information to the following dashboards available towards the left panel of each page:

- *"Controller"* ***on page 110***
- *"AP"* ***on page 111***

- *"Nplus1"* **on page 112**
- *"Stations"* **on page 117**

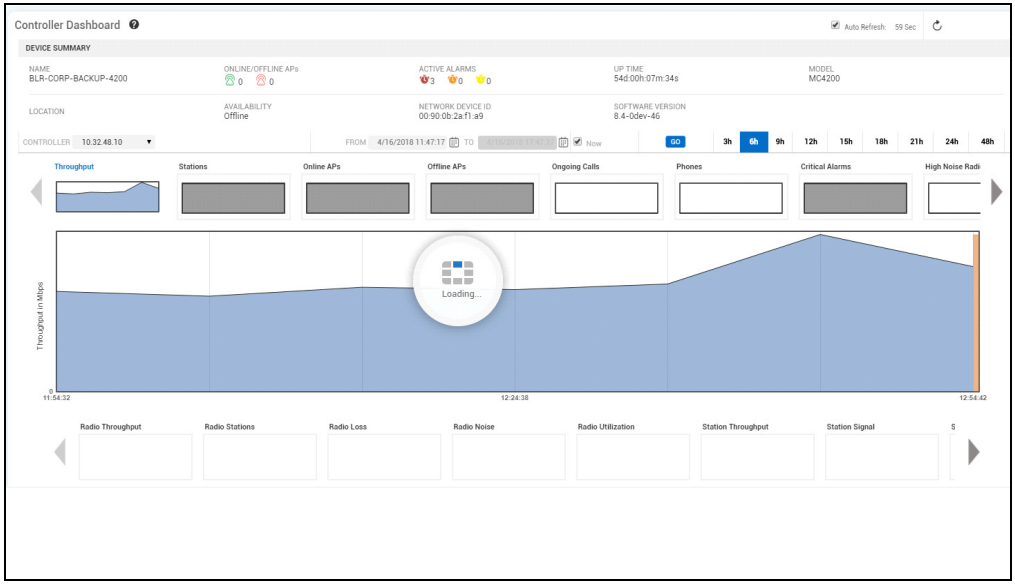
Navigate to *Monitor* > *Detailed Dashboard*.

Controller

The *Controller Dashboard* screen displays an in-depth information about the controller's activity. It provides the graphical representation of the *Throughput Trend, Stations, Online APs, Offline APs, Ongoing Calls, Registered Phones, Critical Alarms, High-Noise Radios, High-Loss Radios, High-Loss Stations, Low-Signal Stations,* and *Rogue APs* of the selected controllers that are managed by *FortiWLM*. The results for the controller are displayed in the upper graphs and results per radio is displayed in the lower set of graphs.

1. In the *Controller Dashboard* screen, select a controller IP address from the *Controller Selection* drop-down list. The details such as *name, location, availability status, the number of online or offline APs connected, the alarms raised,* and *other details* for the selected controller is displayed.

Figure 72: *Controller Dashboard*



2. The *Controller Dashboard* screen provides the graphical representation of the *Throughput Trend, Stations, Online APs, Offline APs, Ongoing Calls, Registered Phones, Critical Alarms, High-Noise Radios, High-Loss Radios, High-Loss Stations, Low-Signal Stations,* and *Rogue APs* of the selected controllers that are managed by *FortiWLM*.
3. The upper graphs display the results for the controller or trend graphs for the selected controller. *Click* a smaller upper graph to see a larger version displayed in the middle of the screen.

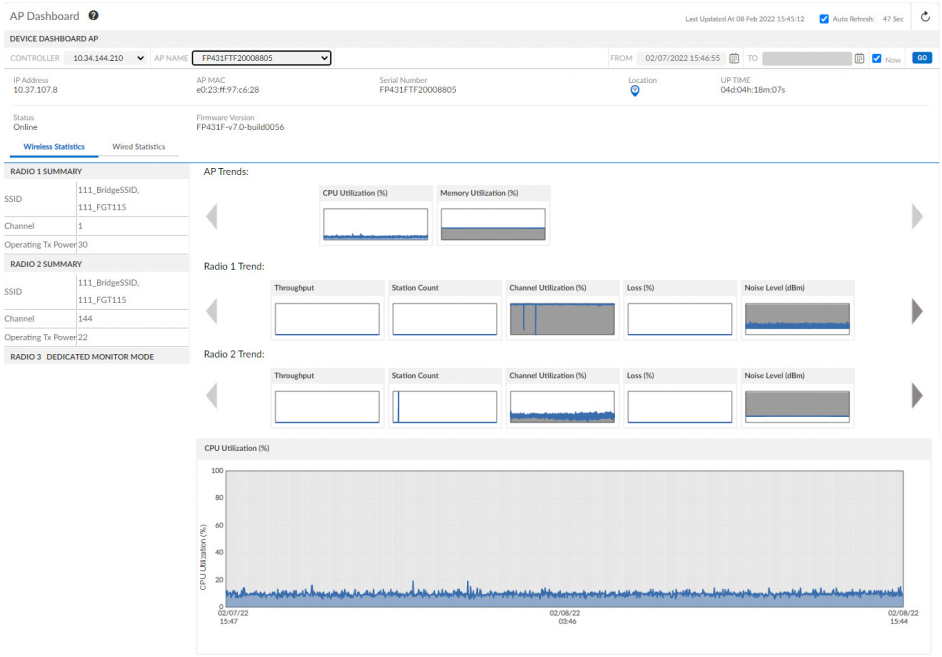
4. The lower graphs are distribution state graphs for a respective parameter at a given time. *Click* a smaller lower graph to see a larger version displayed in the middle of the screen.
5. The trends based on controller selection is monitored by selecting the trend duration. The time period can be modified from 1 to 48 hours by selecting the Trend Interval or by selecting the "*From*" and "*To*" duration of time.

See the ***Controller Dashboard*** screen in Online Help for detailed information on *the Controller Trends* and *Distribution Trends*.

AP

The *AP Dashboard* screen displays an in-depth information about the AP activity. It provides the graphical representation of the *Throughput, Stations, Noise Level, Loss%,* and *Channel Utilization%* for each of the radio on AP connected to the controller which is managed by *FortiWLM*. The results for the radio on AP is graphically displayed on the top portion of the window and *Trends Per radio* in the lower portion of the window.

Figure 73: *AP Dashboard*



1. In the *AP Dashboard* screen, select a controller IP address from the *Controller* drop-down list. The controller selection provides the list of APs located on the selected controller.
2. Select an *AP* from the *AP Name* drop-down list.
3. Select the time period by selecting the "*From*" and "*To*" duration of time. The time interval cannot be more than 1 day. Select the *Refresh* icon.

4. The results for the radio on AP is displayed in the graphs on the top portion of the window and *Trends Per radio* in the lower portion of the window.
5. The number of *Radios* displayed varies from one AP to Other. To illustrate, If the AP is Teton, a third set of graphs are displayed.

The following fields are applicable only for FortiGate controllers.

- **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.

See the ***AP Dashboard*** screen in Online Help for detailed information on *the AP Trends*.

Nplus1

The Nplus1 clusters allow a standby Nplus1 secondary controller in the same subnet to monitor and failover more than one primary controller.

A set of primary controllers and a standby secondary controller are configured via static IP addressing to reside in the same subnet, and are considered to be an N+1 cluster. The standby secondary monitors the availability of the primary controllers in the cluster by receiving advertisement messages sent by the primarys over a well known UDP port at expected intervals. If five successive advertisements are not received, the standby secondary changes state to an active secondary, assumes the IP address of the failed primary, and takes over operations for the failed primary. Because the standby secondary already has a copy of the primary's latest saved configuration, all configured services continue with a short pause while the secondary switches from standby to active state.

While in the active secondary role, the secondary controller's cluster monitoring activities are put on hold until the failed primary rejoins the cluster. An active secondary detects the restart of a primary through ARP (Address Resolution Protocol). When the active secondary is aware of the primary's return (via the advertisement message) it relinquishes the primary's IP address and then returns to the standby state. The now-passive secondary will not fail over for the same primary until a WTR (Wait to Restore) is completed.

If it is necessary for the failed primary to be off-line for a lengthy interval, the administrator can manually set the active secondary back to the standby secondary, thereby ensuring the standby secondary is able to failover for another primary.

In most cases with a cluster of N+1 Primarys, the APs all have to be in L3 Connectivity mode, but if you only have one Primary and one Secondary unit (N=1) the APs can be in L2 connec-

tivity mode. In this case, while the Primary unit is active the Secondary unit will not take AP registration so the AP will always go to the correct controller.

FortiWLM monitors the overall health of the cluster by looking at the *Primary to Secondary* transitions. You can add secondary controllers in the *FortiWLM* and view the primarys for the *Nplus1 cluster* to monitor the events related to primary or secondary transition.

Notes:

- On a FortiWLC-3000D controller, if the fail-over and fall-back happen within 10 minutes, FortiWLM does not detect the Nplus1 state.
- In case of an Nplus1 cluster, note the following points:
  - After the Nplus1 cluster formation is complete, it takes a maximum of 10 minutes to get discovered in FortiWLM.
  - If the secondary and primary controllers are to work as standalone, then backup the FortiWLM configuration, double delete the controller and add it again from the controller inventory in FortiWLM, so that the controller can be successfully managed.

The controller is configured to *Primary* or *Secondary* through the *System Director* CLI. *FortiWLM* allows you to add the configured secondary and primary controllers to the nms-server. This is achieved by navigating to, *Operate* > *Inventory* > *Devices* > *Add* icon.

To view the Nplus1 state of the selected controller, navigate to *Controllers* > *Select a controller* > *Click on View Details* > *Nplus1 State* option.

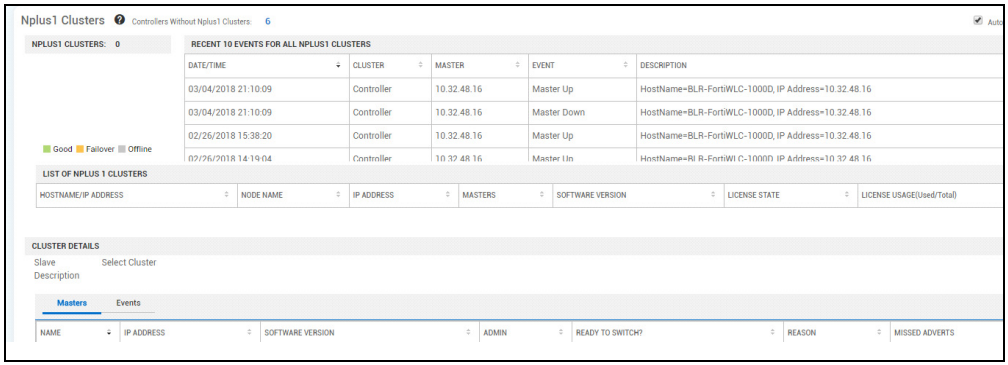
You can upgrade the *Nplus1 clusters* by selecting the *Upgrade Group* as *Nplus1 Clusters* in the *Current Upgrades* screen (*Operate* > *Software Image Management* > *Current Upgrades* > *Add icon* > *Upgrade Group)*.

Secondary controllers cannot be registered to a service profile. The status is displayed as *Sync Failed* when registered to a secondary controller.

The *Nplus1 Clusters* screen in the *Monitor* menu allows you to view the history of transitions for the Nplus1 cluster.

1. Navigate to *Monitor* > *Detailed Dashboard* > *Nplus1*.

Figure 74: *Nplus1 Clusters*



2. The *Nplus1 Clusters* screen is divided into the following four sections:
   - Nplus1 Clusters section
   - Recent 10 events for all Nplus1 Clusters
   - List of Nplus1 Clusters
   - Cluster Details

Nplus1 Clusters section

This section provides the graphical representation of the *Good*, *Failover* and *Offline* clusters in pie-chart. Further details of each cluster are displayed by hovering the mouse pointer over each block.

- **Good Clusters**: These are *Passive Secondary Controllers* where, the *secondary controller* is ready to take control over the *primary controller*. The *Good Clusters* are represented in *Green* color in the pie chart.
- **Failover Clusters**: These are *Active Secondary Controllers* where, the *secondary controller* takes control over the failed primary *controller.* The *Failover Clusters* are represented in *Yellow* color in the pie chart.
- **Offline Clusters**: These are *Secondary Controllers* which are neither *Active* nor *Passive*. When the primary controller goes down, there is no *secondary controller* to take control over the *primary controller*. The *Offline Clusters* are represented in *Red* color in the pie chart.

Recent 10 events for all Nplus1 Clusters

This section displays the recent Nplus1 related events for all the clusters in the nms-server. It provides the details of the Primary controller. The primary details are as follows:

Field	Description
Date/Time	Displays the date/time at which the event occurred.

Field	Description
Cluster	Displays the cluster to which the notification belongs to.
Primary	Displays the IP address of the primary controller.
Event	Displays the event of the primary controller, if the primary controller is down or up.
Description	Displays the event description.

List of Nplus1 Clusters

This section provides the list of clusters added in the *FortiWLM* server. It displays the *Good, Failover and Offline* clusters. Select any one of the *Nplus1 cluster* type (*Good, Failover or Offline Clusters*) from the *Nplus1 Clusters* section (graph), the list of Nplus1 Clusters heading is modified to the selected type of cluster as per the selection.

Field	Description
Host Name/IP Address	Displays the host name of the secondary controller. Select a host name link, the details are displayed in the *Cluster Details* section. See*"Cluster Details"* ***on page 115***.
Node Name	Displays the name of the secondary controller.
IP Address	Displays the IP address of the secondary controller.
Primarys	Displays the number of primary controllers in the cluster.
Software Version	Displays the software version of the secondary controller.
Wait To Restore	Displays the *Wait to Restore* countdown timer that is used to count down before the *Standby secondary* can again take over the role of a *Primary* unit it recently relinquished.
Primary Timeout	Displays the timeout of the primary controller.
License State	Displays the licensed state of the *Secondary Controller*. The types are as follows: • Licensed • Unlicensed
License Usage (Used/ Total)	Displays the total number of the Nplus1 licenses and the number of licenses used on the secondary controller.

Cluster Details

The *Cluster Details* section displays the Host Name of the selected secondary controller from the *List of Nplus1* table along with the description that can be modified by the *Edit* selection. The *Primarys* and *Events* of the secondary are viewed by selecting any secondary controller from the *List of Nplus1 Clusters* table.

Primarys Tab

Select any secondary controller from the *List of Nplus1* table to view the Primarys of the selected secondary. The following fields are displayed:

Field	Description
Name	Displays the host name of the primary controller.
IP Address	Displays the static IP address assigned to the primary controller.
Software Version	Displays the software version of the primary controller.
Admin	Displays the status of Nplus1 clusters on the primary: • *Enable*—Nplus1 clusters have been enabled on the Primary Controller. • *Disable*—Nplus1 clusters have been disabled on the Primary Controller.
Switch	The ability of the secondary to assume the active secondary for the primary: • *Yes*—Secondary and primary model/*FortiWLM* version number is compatible. • *No*—Secondary and primary model/*FortiWLM* version number are incompatible or the administrator has disabled Nplus1 on the primary.
Reason	If *Switch* is *No*, describes why switch cannot be made: • *Down*: The primary has been disabled by the user. • *No Access*: The passive secondary was not able to access the primary because it did not receive a copy of the configuration. This is a rare message that occurs if show nplus1 is executed almost immediately after adding a controller.
Missed Adverts	Displays the number of consecutively missed (not received) advertisements (a maximum of 5 triggers a failover if the Switch field is *Yes*).

Events Tab

Select any secondary from the *List of Nplus1* table to view the *Events* of the selected secondary. The following fields are displayed:

Field	Description
Date/Time	The date and time at which the event occurred.
Primary	Displays the device name.
Description	Displays the Event description.

Status Bar

The *Status Bar* displays the Icons for the following Nplus1 Clusters with a tool tip label:

- Good Clusters
- Failover Clusters
- Offline Clusters

Select one of the above mentioned *Nplus1 Clusters* icon, a summary of the selected *Nplus1 Cluster* is displayed in a separate window as a pop-up screen. The *Nplus1 Clusters* screen and the status bar use the same aggregated data. All the links or pop-up from this page and status bar display the current data.

Stations

The *Stations* dashboard displays the performance trends for a specific station. An intuitive graphical display of the *throughput, signal strength, loss, and airtime utilization trends* are plotted for the selected station. The station history can be viewed and exported in CSV format (comma separated values) by selecting the *CSV* option. The event types are filtered either based on the station event type or by selecting the controller, event severity, event Id, and MAC address. The *Station Activity* comprises of the below mentioned dashboards:

- *"Station Trend Dashboard"* **on page 117**
- *"Station Activity Log"* **on page 331**

Station Trend Dashboard

The *Station Trend Dashboard* displays a variety of performance trends for a specific station or all stations for a specific controller. The graphs on the station trend dashboard require a MAC address or the user name. If you don't know the MAC address, use the *Search* function (*Operate >Tools > Search*) to find a station by entering keywords related to that station. Copy the MAC address and use it as input for this *Station Trend Dashboard*.

To see information for an individual station, follow these steps:

1. Click *Monitor* > *Detailed Dashboard* > *Station*.

2. In the *Station Trend Dashboard* screen, obtain a *Station Key* by selecting the *Select Station* option. The IP address of the selected *Station* is displayed as the *Station Key.*
3. Provide a *Start Time* and *End Time* in the format 01/08/2009 09:14:51 (the date followed by time in the format hh:mm:ss). Optionally, use a calendar to select the date and time. To use the current time, check *Now*. Note that the start and end times cannot be more than 24 hours apart. followed by selecting the *Refresh* option.
4. The following sections are displayed.

Charts

Station Throughput Chart

The *Station Throughput* chart displays stations combined transmitted and received bytes during a 1 minute/10 minute interval. The date, time and value for that point is viewed by hovering the mouse pointer over the respective section in graph. Right-click and select *Show Details* to view the Throughput details.

Signal Strength Chart

The *Signal Strength* chart displays the signal strength (dBm) for this station in the time period indicated. The date, time and value for that point is viewed by hovering the mouse pointer over the respective section in graph. The chart is updated approximately every 1 minute/10 minutes. Right-click and select *Show Details* to view the Signal Strength details.

Loss% Chart

The *Loss%* chart displays the station's transmit loss percentage for all unicast data frames. The date, time and value for that point is viewed by hovering the mouse pointer over the respective section in graph. The chart is updated approximately every 1minute/10 minutes. Right-click and select *Show Details* to view the Loss% details.

Airtime Utilization Chart

The *Airtime Utilization* chart displays station airtime utilization in percentage. The date, time and value for that point is viewed by hovering the mouse pointer over the respective section in graph. The chart is updated approximately every 1 minute/10 minutes. Right-click and select *Show Details* to view the *Airtime Utilization* details.

Station Information

The Station Information provides the *MAC Address, IPv4 Address, IPv6Address, User Name, Station Type, OUI Name, Device Type, OS Type, Radio Type, Data Rate, Service Name, AP ID, AP Name,* and *Controller* details of the selected station.

802.11 Session

The *802.11 Session* is available for controller version 5.2 and higher versions. Each 802.11 Session is generated by events such as association, disassociation and hand offs. The 802.11 Session table provides the details of the Session duration and bytes transmitted during session. The 802.11 session details can be viewed in CSV format (comma separated values.) by selecting the *CSV* option.

Station History

The history of events accomplished through *FortiWLM* for the selected station along with the *Date/Time, Duration, Controller, AP ID, AP Name, Radio, Station IP4, Station IPv6, User Name,* and *SSID* for the selected station can be viewed in this section. The Heat maps with the actual AP statistics retrieved from the controller is viewed by selecting the *Go to Visualization* option. The station history can be viewed in CSV format (comma separated values) by selecting the *CSV* option. The *Show AP Location* displays the selected AP located on the floor.

The station history contains the complete history of sessions recorded for the chosen station in the station dashboard. This data is **not limited** to the time-range selected in the dashboard.

Station Activity Log

The *Station Activity Log* on the *Station Trend Dashboard* screen represents the station events only for the selected station. It displays the most recent 10,000 station events within the interval of one week. Once the number reaches 10,000, additional events are not listed. If additional events are important for troubleshooting, refine the time 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 can be filtered based on the event type. The station history can be viewed and exported in CSV format (comma separated values) by selecting the *CSV* option. The event types are filtered based on the station event type.

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

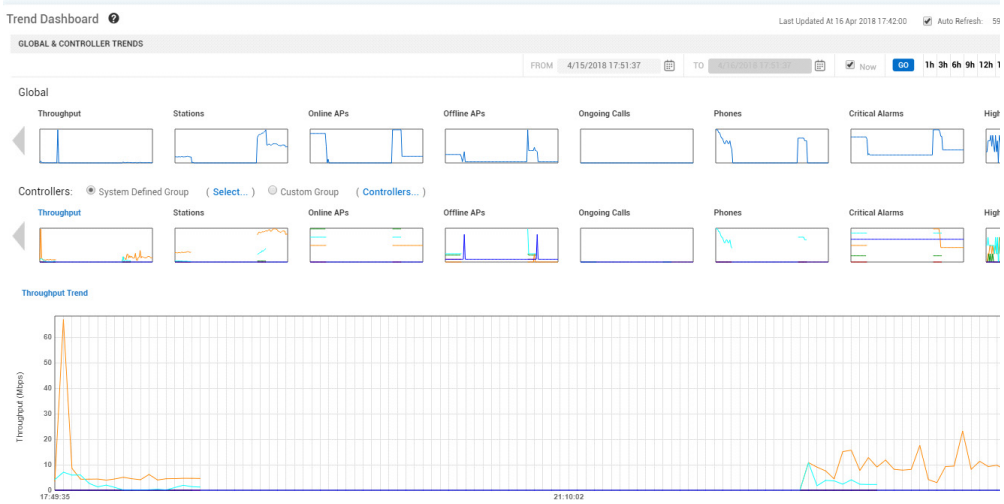
Trends Dashboards

Trend Dashboard provides you the aggregate global trend performance and controller error rates over a period of time. *FortiWLM* collects statistics from a controller every ten minutes 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.

Trends

The global trends and trends per controller are graphically represented in 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 information about the controller trend graph is plotted for past 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.

Figure 75: *Trend Dashboard*

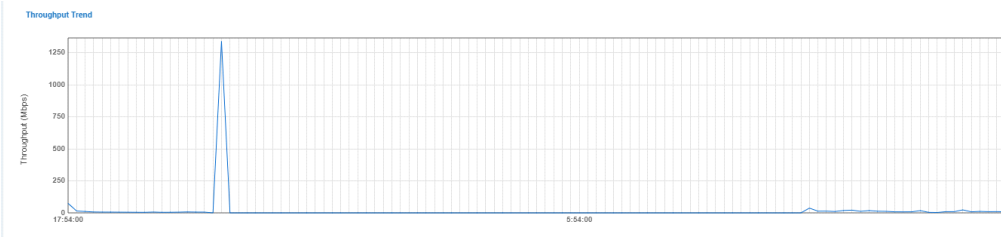


Throughput Trend Graph

Select the small Throughput graph to see a larger version displayed in the middle of the screen.

The default *Throughput Trend* graph illustrates the throughput trend for the network (upper graph) and individual controllers (lower graph). The lower graphs are trends for selected controllers; the objective here is to compare relative performance of up to five controllers.

Figure 76: *Throughput Trend Graph*

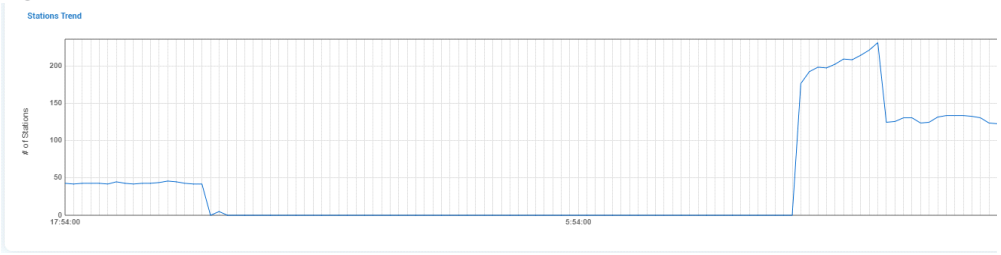


Station Trend Graph

Select the small *Stations Graph* to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

The lower graphs displays station trends for selected controllers; the *Station Trend Graph* showcases the number of stations on up to five controllers.

Figure 77: *Station Trend Graph*

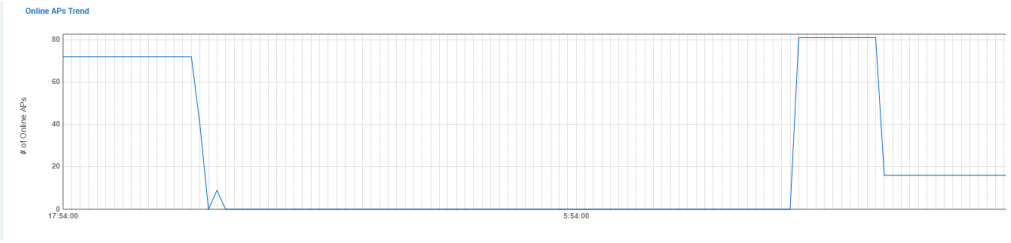


Online AP Trend Graph

Select the small *Online AP* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

The upper graph represents the number of online APs on all controllers currently managed by *FortiWLM* that are up and running. The lower graphs are *Online AP Trends* for selected controllers; the objective here is to compare the number of online APs for up to five controllers.

Figure 78: *Online AP Trend Graph*

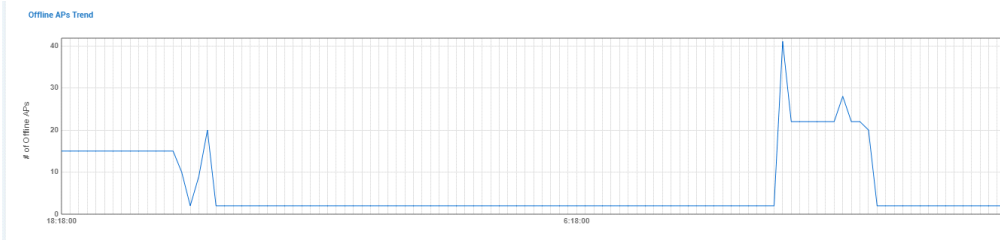


Offline AP Trend Graph

Select the small *Offline AP* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

The upper graph represents the trend for APs on all controllers managed by *FortiWLM* that are not running. The lower graphs are *Offline AP Trends* for selected controllers; the objective here is to compare the number of offline APs on up to five controllers.

Figure 79: *Offline AP Trend Graph*

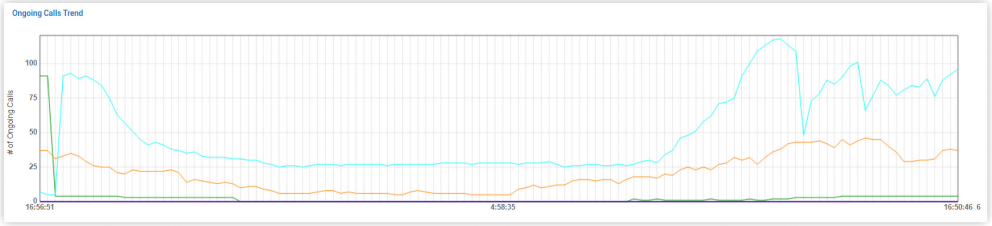


Ongoing Calls Trend Graph

Select the small *Ongoing Calls* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

For the upper graph, all ongoing calls are counted on every controller currently managed by *FortiWLM*. The lower *Ongoing Calls Trend* graph represents calls for up to five selected controllers; the objective here is to compare the number of ongoing calls on these controllers.

Figure 80: *Ongoing Calls Trend Graph*

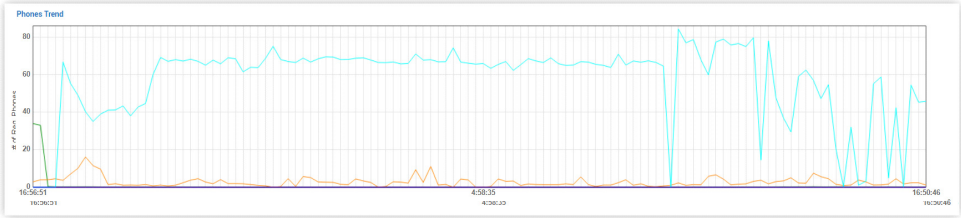


Phones Trend Graph

Select the small *Phones* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

The phones associated to any of the APs or controllers managed by the *FortiWLM*. The upper graph shows the trend for all registered phones for all controllers. The lower *Phones Trend* graph represents phones for up to five selected controllers; the objective here is to compare the number of phones on these controllers.

Figure 81: *Registered Phones Trend Graph*

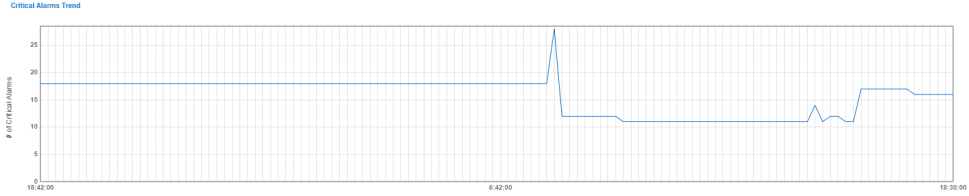


Critical Alarms Trend Graph

Select the small *Alarms* graph to see a larger version displayed in the middle screen. By default, the *Throughput* graph is displayed which cannot be modified.

The upper graph shows the trend for all alarms on all controllers in a line chart. The lower *Critical Alarms Trend* graph represents alarms for up to five selected controllers; the objective here is to compare critical alarm count on these controllers. Typical examples of critical alarms are AP Down and Rogue AP Detected.

Figure 82: *Critical Alarms Trend Graph*

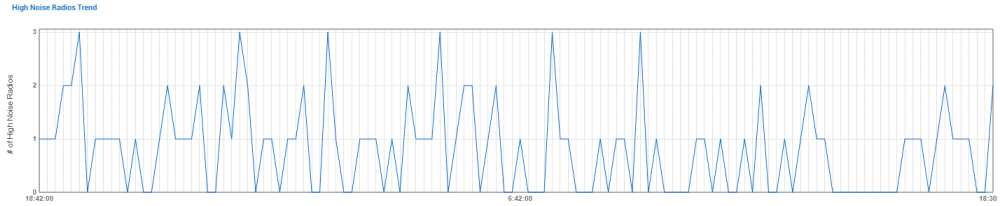


High Noise Radios Trend Graph

Select the small *High Noise Radios* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

The *High Noise Radio Trend* graph displays the aggregate number of radios experiencing noise greater than threshold (-70 dBm).

Figure 83: *High Noise Radios Trend Graph*

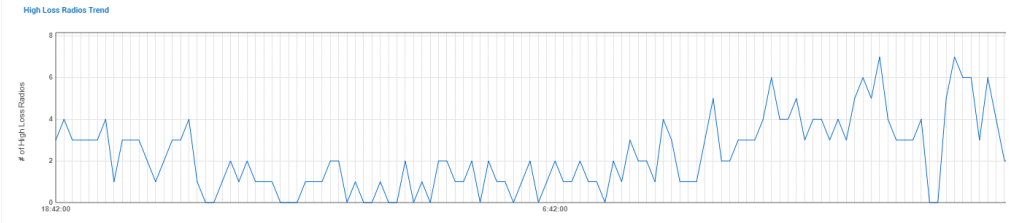


High Loss Radios Trend Graph

Select the small *High Loss Radios* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

The *High Loss Radios Trend* graph displays the aggregate number of radios experiencing loss greater than the threshold (50%). You cannot modify the threshold at this time.

Figure 84: *High Loss Radios Trend Graph*

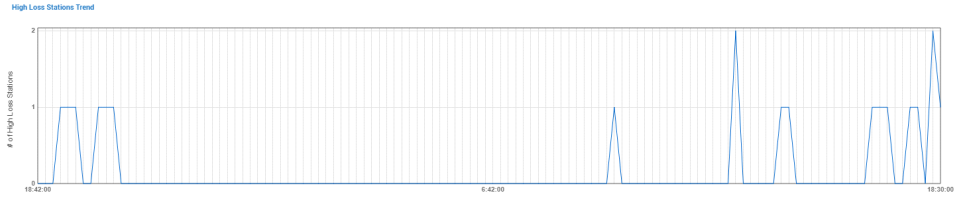


High Loss Stations Trend Graph

Select the small *High Loss Stations* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

The *High Loss Stations Trend* graph displays the aggregate number of high-loss stations for each three minute period. High loss is defined as 50%.

Figure 85: *High Loss Stations Trend Graph*

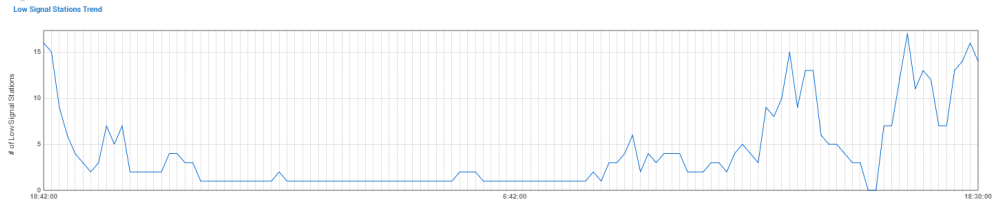


Low Signal Stations Trend Graph

Select the small *Low Signal Stations* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

The *Low Signal Stations Trend* graph displays the aggregate number of radios on all controllers that are experiencing loss greater than the threshold (50%). You cannot change thresholds at this time.

Figure 86: *Low Signal Stations Trend Graph*

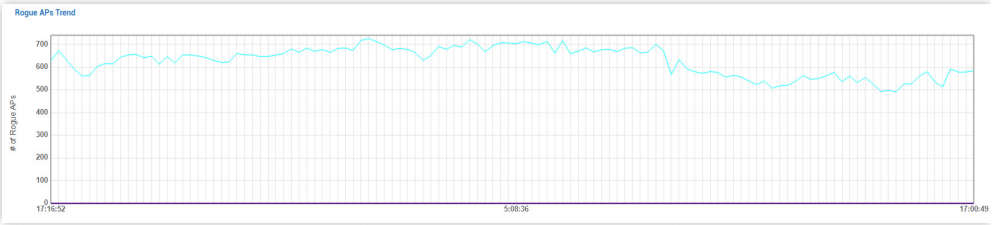


Rogue APs Trend Graph

Select the small *Rogue APs* graph to see a larger version displayed in the middle screen. By default, the Throughput graph is displayed which cannot be modified.

The *Rogue AP Trend* graph represents the classification of controllers into ten groups based on number of rogue APs detected on each controller.

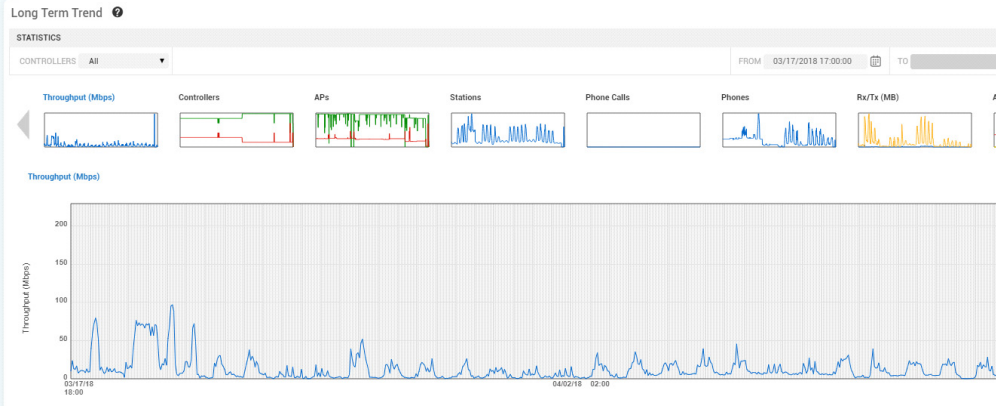
Figure 87: *Rogue APs Trend Graph*



Long Term Trend

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

Figure 88: *Long Term Trend Dashboard*



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 one hour for either all controllers or for one particular controller is displayed. The Long Term Trend data stored in the *FortiWLM* database cannot be modified. The *FortiWLM* summarizes the data in three predefined sample periods as follows:

- **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* > *System Settings* > *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.

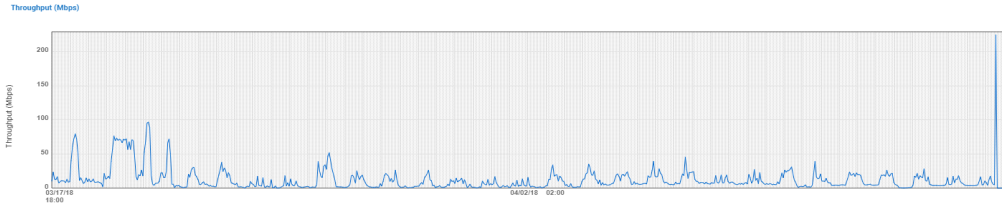
The long-term trend graphs display up to 12 months of data for either the selected controller or all controllers available to the user group.

Throughput

The *Throughput* graph represents the total number of controllers' throughput aggregated.

Right click and select *Show Details* on the Throughput graph to view the details of Throughput.

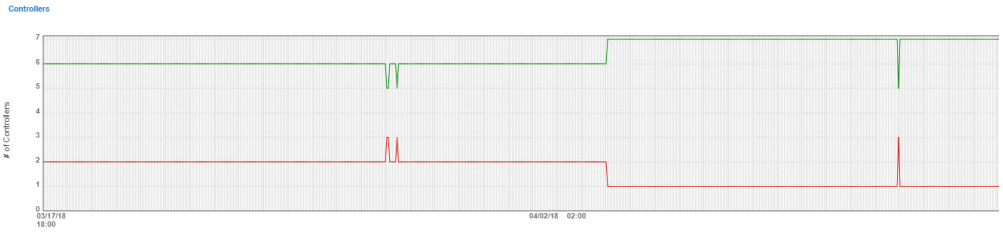
Figure 89: *Throughput long term trend graph*



Controllers

The *Controllers* graph represents total number of polled controllers. Both *online* (green) and *offline* (red) controllers can be viewed.

Figure 90: *Controllers long term trend graph*



The number of managed controllers in the controllers graph can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of online and offline controllers.

APs

The *APs* graph represents the total number of APs present on the polled controllers. Both online (green) and offline (red) APs can be viewed.

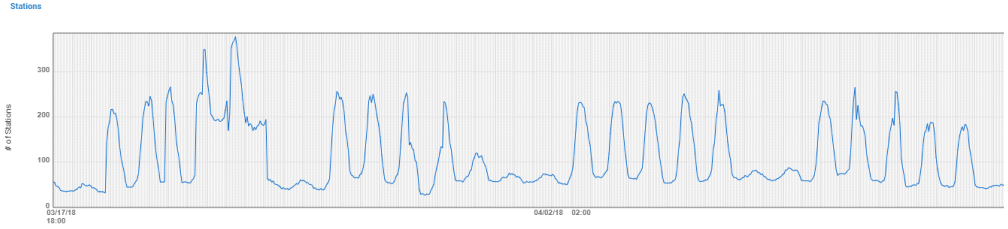
Figure 91: *APs long term trend graph*

The number of APs present on the managed controllers in the APs graph can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of the online and offline APs.

Stations

The *Stations* graph represents the total number of stations associated to *FortiWLM* controllers for the selected time period.

Figure 92: *Stations long term trend graph*

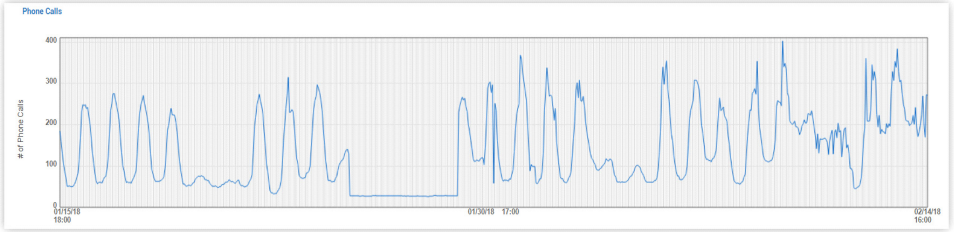


The number of stations in the Stations graph can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of the stations associated.

Phone Calls

The *Phone Calls* graph represents the aggregate number of all the current wireless phone calls.

Figure 93: *Phone Calls long term trend graph*

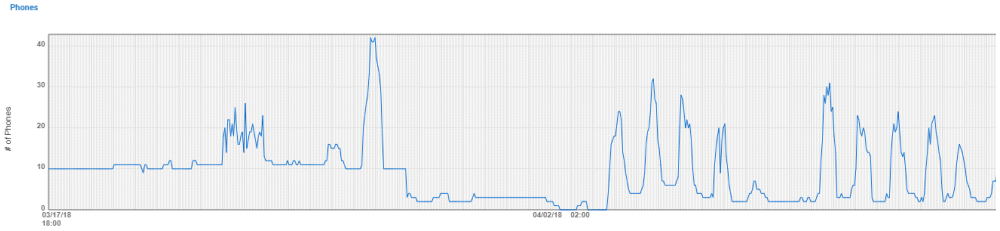


The number of *Phone Calls* in the *Phone Calls* graph can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of the number of all the current wireless phone calls.

Phones

The *Phones* graph represents the aggregate number of all current registered phones. A phone is considered registered when it has been recognized by the network.

Figure 94: *Phones long term trend graph*

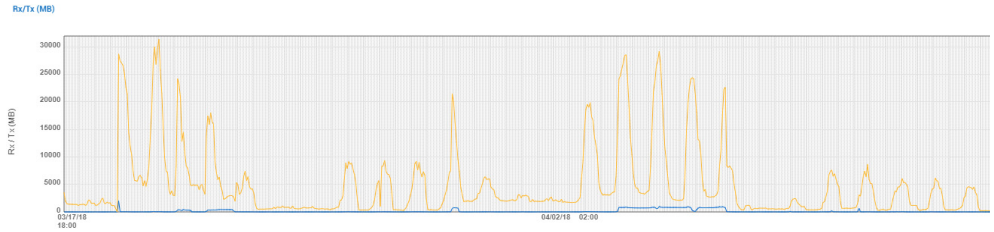


The number of registered *Phone* in the *Phone* graph can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of the registered phones.

Rx/Tx

The *Receive data and Transmit data (Rx/Tx)* graph represents the data transferred in bytes.

Figure 95: *Receive data and Transmit data (Rx/Tx) long term trend graph*

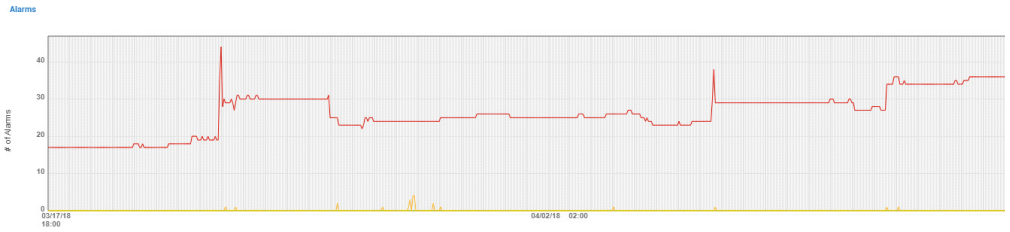


The number of Receive data and Transmit data (in bytes) can be viewed by hovering the mouse pointer over the graph. Right click and select *Show Details* to view the details of the data transferred in bytes.

Alarms

The *Alarms* graph represents the aggregate number of all alarms on all polled controllers. The *critical* alarms are displayed in red color, *major* alarms in orange color and *minor* alarms in yellow color.

Figure 96: *Alarms long term trend graph*

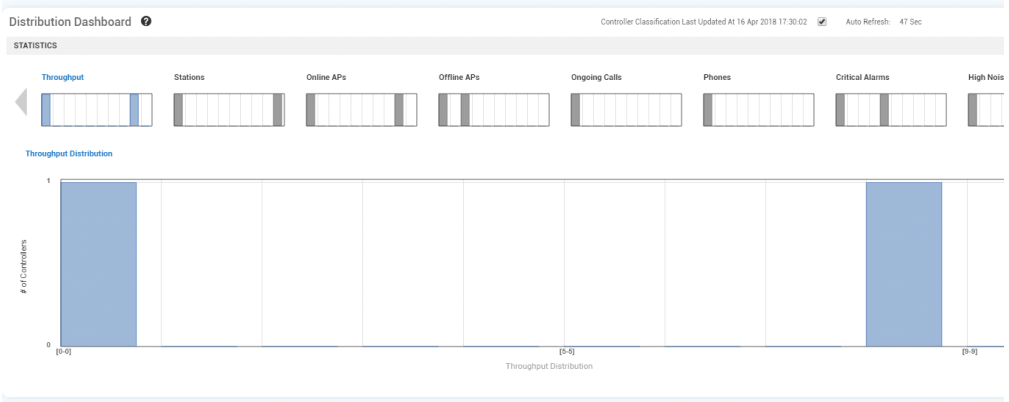


Hover the mouse pointer over a graph to view the number of the *Critical, Major,* and *Minor* alarms. Right click and select *Show Details* to view the details of the *Critical, Major and Minor* alarms.

Distribution

The *Distribution Dashboard* displays data for the entire configured network on one chart; it displays the global graphs with available detailed breakdown of information. This graphing section of the distribution dashboard reflects the distribution of *throughput, stations, online and offline APs, phones and, phone calls, alarms, noise, loss,* and *signals*. Each of these graphs is the collection of data for each topic, divided into ten bars per graph. To have these graphs automatically refresh every minute, *enable auto-refresh*.

Figure 97: *Distribution Dashboard*



To interpret one of the 10 sections of a graph, move the mouse over a bar on the graph. The data range for the selected section with the number of controllers/stations that fall within in that data range is displayed. Perform a right-click on the graph and select *Show Details* to view the individual data for each graph.

In short, hover the mouse pointer over a graph to view further information. Right-click on the graphs, provides a drop-down list of available actions for that graph.

Throughput Distribution Graph

Click the small *Throughput* graph to see a larger version displayed in the middle of the screen. This graph represents the distribution of each controller's throughput over the range of the controller with the lowest throughput and the controller with the highest throughput. Throughput is graphed with integers and fractional values are rounded down. For example, if throughput is 10.5, it is counted in bar 9-10 (assuming bars are 9-10,11-12 and so on). For example, the first bar could represent 1-10 Mbps, the second bar 11-20 Mbps, and the third 21-30Mbps. Two controllers could be operating 1-10 Mbps, three at 11-20, and two at 21-30Mbps.This is a simple way to scale network size.

Hover the mouse pointer over a bar to see the range included in that particular bar. To see throughput details for each controller, right-click on a throughput graph (either the large or small version) and select *Show Details*. Throughput details for each controller are displayed in Mbps.

Stations Distribution Graph

Click the small *Stations* graph to see a larger version displayed in the middle of the screen. This graph shows the distribution of wireless stations across the network managed by FortiWLM. The leftmost bars represent controllers supporting the fewest wireless stations and the right-most bars represent stations supporting the most wireless stations.

Online APs Distribution Graph

Click the small *Online APs* graph to see a larger version displayed in the middle of the screen. The graph represents the distribution of online APs on all controllers currently managed by FortiWLM that are up and running. This graph represents the number of APs on all controllers currently managed by FortiWLM that are up and running. The leftmost bars represent controllers supporting the fewest wireless stations and the right-most bars represent stations supporting the most wireless stations.

Offline APs Distribution Graph

Click the small *Offline APs* graph to see a larger version displayed in the middle of the screen. The graph represents the distribution for APs on all controllers managed by FortiWLM that are not running.

Ongoing Calls Distribution Graph

Click either small *Ongoing Calls* graph to see a larger version displayed in the middle of the screen. All ongoing calls are counted on every controller currently managed by FortiWLM, then that data is divided into 10 bars on this graph. Hover the pointer over a bar to see the data range included in that particular bar. To see details for each bar in the distribution, right-click an *ongoing call graph* (either the large or small version) and select *Show Details*. The details for each number of bars per controller are displayed.

Phones Distribution Graph

Click the small *Phones Distribution* graph to see a larger version displayed in the middle of the screen. Phones are connected to the wireless network that are either making

calls at this time or not (same as associated phones). It represents the classification of controllers into ten groups based on number of wireless phones on the controller.

Critical Alarms Distribution Graph

Click a smaller *Alarms Distribution* graph to see a larger version displayed in the middle of the screen. The graph shows the distribution for all alarms on all controllers. Critical Alarms is marked as critical when the corresponding Notification Filter is created. This chart represents the classification of controllers into ten groups based on the number of critical alarms on the controller. Examples of critical alarms are *AP Down* and *Rogue AP Detected*.

High-Noise Radios Distribution Graph

This graph displays the distribution of radio noise. Click the small *High-Noise Radios* graph to see a larger version displayed in the middle of the screen. This graph shows the number of controllers whose noise value is greater than a set threshold (default is >= -70). Noise is defined as either random noise with no coherence or coherent noise introduced by the devices mechanism or processing. Noise level is calculated in each controller and represents the

noise floor. No averaging method is used here and the noise level and noise floor are the same. The noise floor is represented in dBm which is a negative value.

High-Loss Radios Distribution Graph

This graph displays the distribution of radio loss. Click the small *High-Loss Radios* graph to see a larger version displayed in the middle of the screen. The graph shows the radio interface loss distribution for all radios on all controllers. Interface loss is defined as the percentage of 802.11 unicast packets transmitted for which no 802.11 Ack is received. The graph represents the number of controllers whose loss value is greater than a set threshold (default is >= 50%). Interface Loss for a controller is the sum of Interface Loss of all APs. This graph represents the distribution of packet loss across all controllers over the last two minutes. Similarly to the Throughput graph, each bar represents a range of loss and how many controllers fall within that range. The network is performing best when most controllers are in the leftmost columns. There is a variable kept for each controller and so the transmit loss percentage for all unicast data frames is calculated for each controller using the formula Loss Percentage = Ack Fail Count / (successful frames + Ack Fail Count) * 100 (%).

High-Loss Stations Distribution Graph

This graph displays the distribution of station loss. Click the smaller *High-Loss Stations* graph to see a larger version displayed in the middle of the screen. The graph represents the number of controllers with stations whose loss value is higher than a set threshold (default is >= 50%). Station loss is defined as the percentage of 802.11 unicast packets transmitted for which no 802.11 Ack is received. This graph represents the distribution of packet loss across all stations over the last two minutes. Similar to the Throughput graph, each bar represents a range of loss and how many stations fall within that range. The network is performing best when most stations are in the leftmost columns. There is a variable kept for each station and so the transmit loss percentage for all unicast data frames is calculated for each station using the below formula:

Loss Percentage = Ack Fail Count / (successful frames + Ack Fail Count) * 100 (%).

Low-Signal Stations Distribution Graph

Click the smaller *Low-Signal Stations* graph to see a larger version displayed in the middle of the screen. The graph displays the signal distribution for stations on all controllers combined. This graph represents the number of controllers whose stations' RSSI value is less than a set threshold (default is <-80). Received Signal Strength Indication (RSSI) is a measurement of the power present in a received radio signal, aggregated across the entire network. The value reported is the measured signal strength in dBm averaged over 3 seconds.

Rogue APs Distribution Graph

This graph displays the distribution for rogue APs which are distributed on all network managed controllers. Click the smaller *Rogue APs* graph to see a larger version displayed in the

middle of the screen. The rogue APs are calculated for the entire network (all controllers) and divided into 10 bars on this graph.

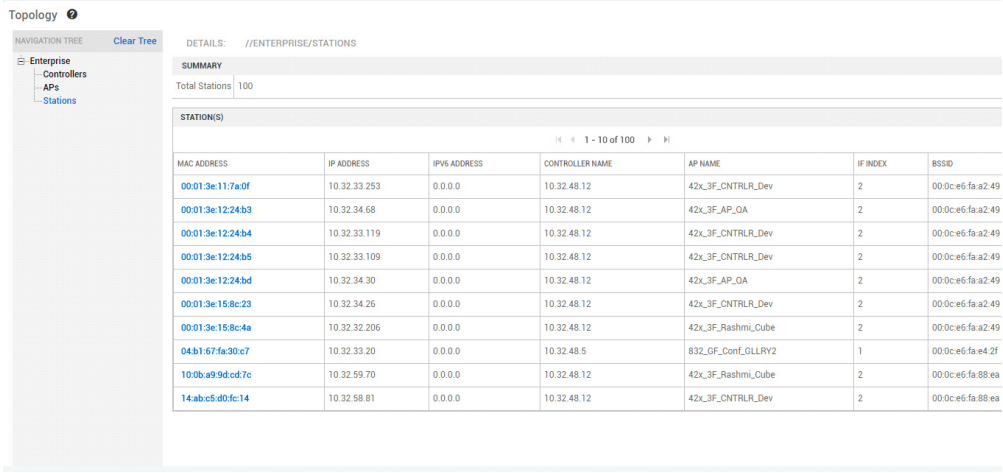
Another option is to display Rogue-AP related messages by clicking *Search* > providing the Keyword “rogue” > selecting *Alarms* > clicking *Search*.

5.

Topology

Topology is a tree that illustrates the logical placement of hardware devices. The hardware devices include *controllers, APs, and Stations*. Double-click *Stations* to see the following information for each client.

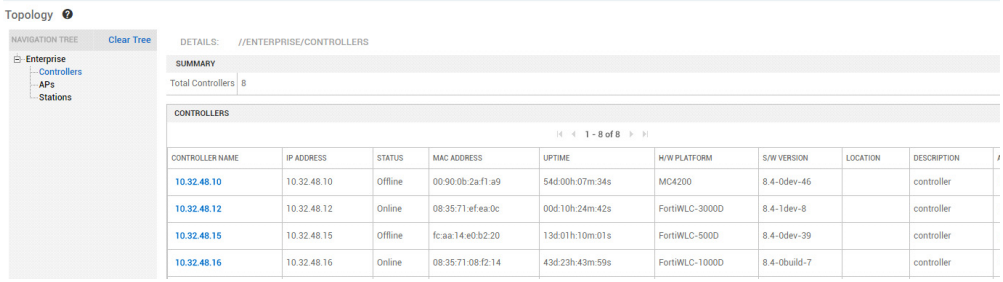
Figure 98: *Station Topology*



Controllers

Select *Controllers* from the tree. The following sections are displayed:

Figure 99: *Station Topology - Controllers*



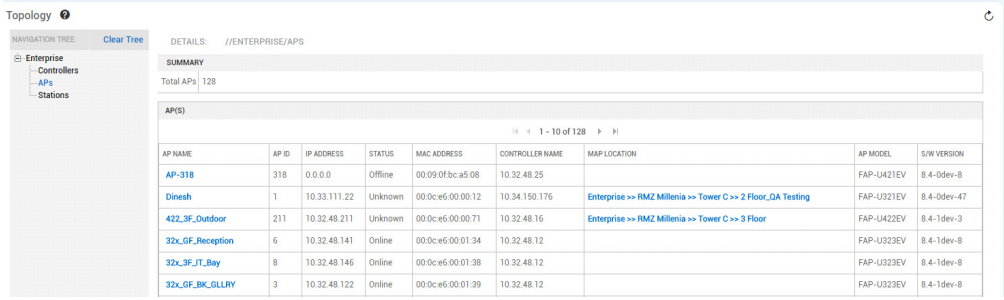
- **Summary**: Displays the total number of controllers.
- **Controllers**: Displays the list of controllers managed by *FortiWLM* in a tabular format. The controllers table provides the following details:

Field	Description
Hostname	Displays the controller's Hostname or IP Address. Select the hyper link of the controller's IP address. The selected controller's IP address gets included to the controllers tree.
IP Address	Displays the controller's IP Address.
Status	Displays the controller's status whether Online or Offline.
Serial#	Displays the serial number of the controller.
Uptime	Displays the controller's uptime.
H/W Platform	Displays the hardware platform associated to the controller.
S/W Version	Displays the software version of the controller.
Location	Displays the location of the controller.
Description	Displays the description provided for the controller.
Controller UI	Select the hyper link of the controller, the selected controller is displayed.

Access Points

Select the APs from the tree. The following sections are displayed:

Figure 100: *Station Topology - APs*



Summary: Displays the details of the selected AP managed by *FortiWLM* in a tabular format. The AP table provides the following details:

Field	Description
AP Name	Displays the *AP Name*. Select the hyper link of the *AP Name*. The selected AP name address gets included to the AP tree.
AP ID	Displays the *AP ID* to which the station was associated at the time of the event.
IP Address	Displays the controller's IP Address. **Note**: For APs connected through L2 to a controller, the IP address displayed is 0.0.0.0 For Teton APs, the information for three radios are displayed.
Status	Displays the AP status whether *Online* or *Offline*.
Serial#	Displays the serial number of the AP.
Controller Hostname	Displays the controller's Hostname.
Map Location	Displays the *Map Location*. Select the hyper link of the map location. The *Map Management* screen is displayed.
AP Model	Displays the AP Model.
S/W Version	Displays the software version of the AP.

Interface: The Interface table provides the following details:

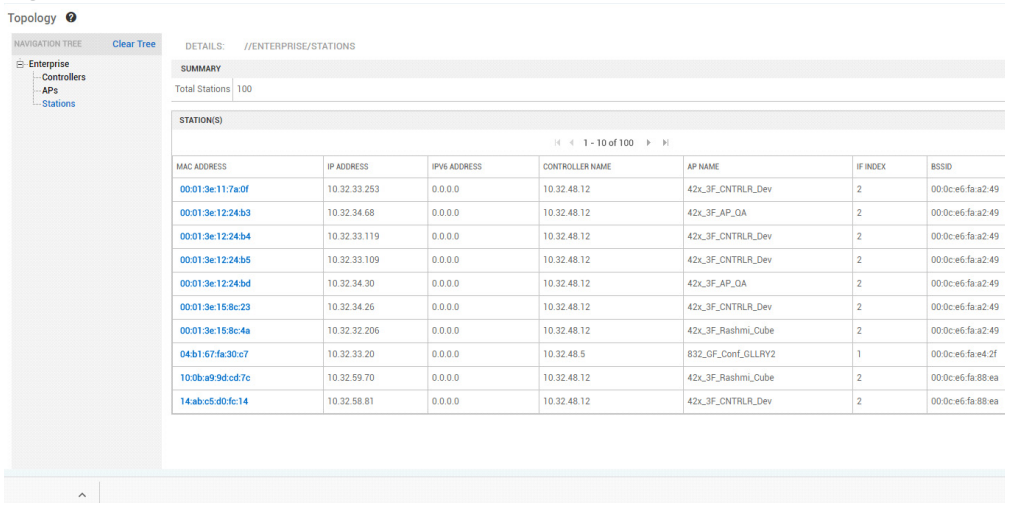
Field	Description
IF Index	Displays the Interface Index number. • Select the hyper link of the Interface Index. • The selected Interface is added to the Interface tree. • A summary of the Interface Index is displayed, depicting the stations connected to the selected Interface.
Serial#	Displays the Serial number of the AP.
AP Name	Displays the AP Name.
Channel	Displays the Channel number.

Stations

Select the *Stations* from the tree. The following sections are displayed:

Summary: Displays the total number of stations.

Figure 101: *Station Topology*



Station: Displays the list of *Stations* managed by *FortiWLM* in a tabular format. The Station table provides the following details:

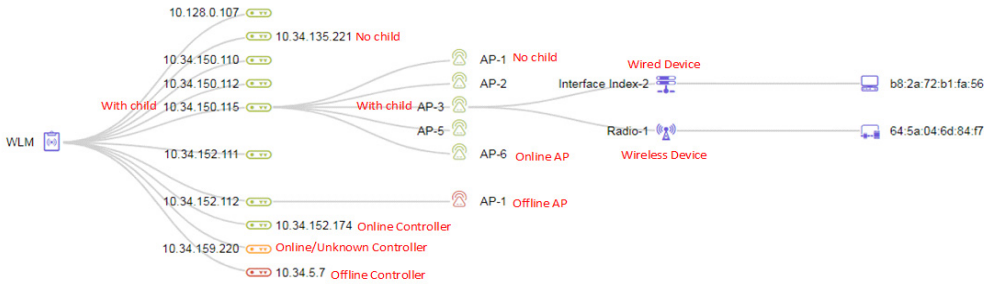
Field	Description
MAC Address	Displays the station *MAC Address*. Select the hyper link of the MAC Address. The selected *MAC Address* gets included to the station's tree.
IP Address	Displays the controller's IP address.
Controller Hostname	Displays the controller's hostname.
AP Name	Displays the AP name.
IF Index	Displays the IF index.
BSSID	Displays the BSSID of the associated station.

Physical Topology

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

You can filter and view selective devices, the filter options available are controllers, APs, the device OS and MAC Address.

The collapsible/expandable hierarchy of devices in the physical topology is **controller ~ AP ~ radio ~ station**; each of the devices displayed is clickable to display the next level of hierarchy. Hover over the device name to obtain additional information.



- The status of the controllers and APs is marked using a color legend.
  - **Green**: Online and active
  - **Orange**: Online and unknown (unmanaged)
  - **Red**: Offline
- The wired and wireless stations are illustrated with icons.
- If the controller and AP name is on the right of the specific icon, it implies that the device has no child associated with it in the hierarchy.

Logical Topology

The logical topology provides a visualization/illustration of the logical placement 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 logical topology is representational; you cannot perform any operations on this page.

You can filter and view selective entities, the filter options available are ESS, VLANs, and the device MAC Address.

The collapsible/expandable hierarchy of entities in the logical topology is **wireless service ~ ESS ~ VLAN ~ station**; each of the entities displayed is clickable to display the next level of hierarchy.

Note: The physical and logical network topology views differ based on the browser, *Internet Explorer & Microsoft Edge* **VS** *Chrome, Firefox, and Safari*.

Configuring Network Manager

You can use *FortiWLM* to manage multiple *FortiWLC*. One of the major features of *NM* is the ability to create a controller configuration from *FortiWLM* and download it to one or more managed controllers. These controller configurations are owned by the *nms* - server and cannot be altered by the controllers using them.

This chapter describes creating and applying controller configurations.

The *NM* can download the controller configuration to one or all managed controllers. If you modify the controller configuration, all controllers using it are automatically updated with those modifications. The configuration of controllers is managed by *FortiWLM* via a *Wireless Service Profile, AP Template,* and *Service Control*.

You can configure the network manager on the following parameters:

- *"Device Management"* ***on page 141***
- *"Design-Features"* ***on page 153***
- *"Importing Controller Configuration"* ***on page 186***
- *"Templates"* ***on page 188***

Device Management

Service Control

Fortinet's *Service Control* feature is designed to allow clients in the enterprise network to access and communicate with devices that are advertising service via a protocol such as Bonjour. *FortiWLM* manages multiple controllers and AP groups. The *NM* has the ability to create global settings for the *services*, *create policy templates*, and *create global controller configuration*. One of the major features of this product is the ability to create a *Global Controller Configuration* from *NM* and download it to one or more managed controllers. These *Global Controller Configurations* are owned by *NM* (nms-server) and cannot be altered by the controllers using them. *NM* can download a *Global Controller Configuration* to one or all managed controllers. If you change a *Global Controller Configuration*, all controllers using it are automatically updated with those changes.

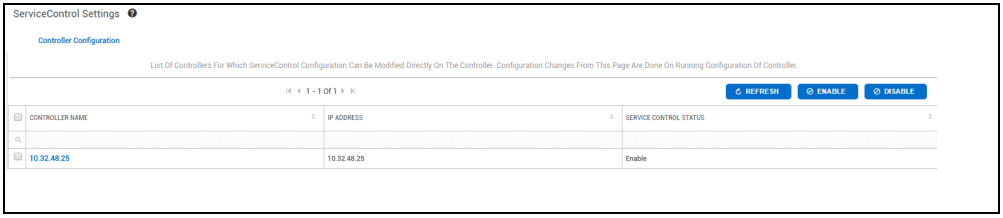
The limitation for Bonjour-enabled devices is that they were largely designed for small-scale use; however, they are growing increasingly prevalent in the enterprise-level environment. The nature of the service makes scaling for larger deployments challenging because the wireless traffic communications for these protocols cannot travel across various subnets; as such, users on VLAN1 will be unable to access a device operating on VLAN2 (for example).

Service Control addresses this problem by providing a framework by which Fortinet will direct traffic from clients on different subnets over to the Bonjour-capable devices (and vice versa), allowing seamless communication between the two. Additionally, you can specify which services should be available to specific users, SSIDs, or VLANs, allowing a fine control to be exercised over the deployment.

To enable Service Control:

1. Navigate to *Configure* > *Device Center* > *Service Control*. By default, you land on the *Service Control Settings*.

Figure 102: *Service Control Settings*



2. Click the *Global Settings* tab.
3. Check *Enable Service Control*. The page will automatically refresh. Refer to the sections below for configuration instructions.

Modifying Service Control Global Configuration

Once Service Control has been enabled, the *Global Settings* tab displays two new tables:

- *Discovery Criteria:* The discovery criteria allows you to specify the types of services that may be discovered. By default, all *AppleTV* and *Printer* services configured in the system will be set for discovery across all SSIDs and APs and on Controller native VLAN by controller on the wired side. To modify this, click the pencil icon under the Services column to access the *Discovery Criteria* dialog.
- *Advanced Options*: The Advanced Options will allow you to specify the IP addresses to block the bonjour services.

Figure 103: *Service Control Settings - Global Settings*

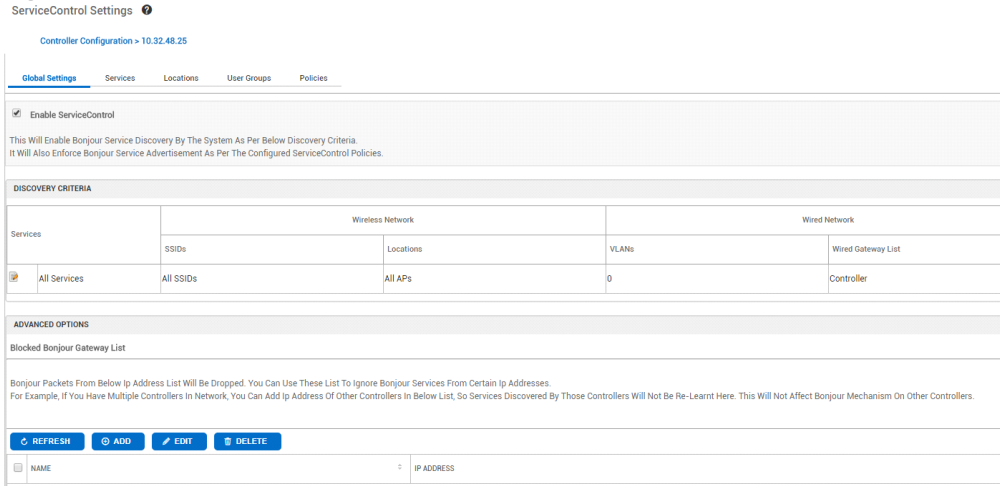
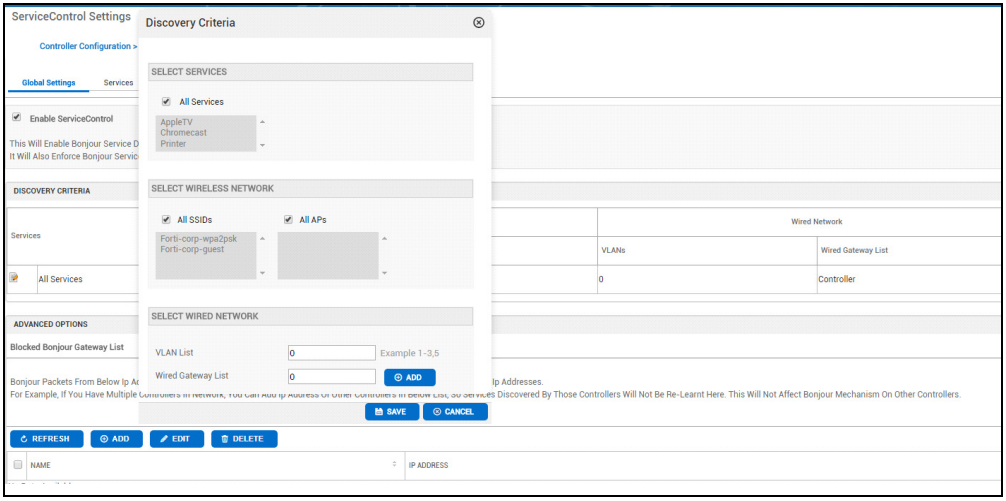


Figure 104: *Discovery Criteria*



1. As shown above, the *All Services* box is checked, ensuring that all configured services will automatically be detected by the system. Uncheck this box and select the desired service(s) if you wish to restrict the types of services provided.
2. The *Select Wireless Network* section allows you to customize which SSIDs/APs can access the services; by default, all of them are permitted.

3. The *Select Wired Network* section controls how wired devices access the services; enter the VLAN(s) that should be allowed access. To add wired gateways, click the **Add** button and specify the desired options from the resulting list of devices.

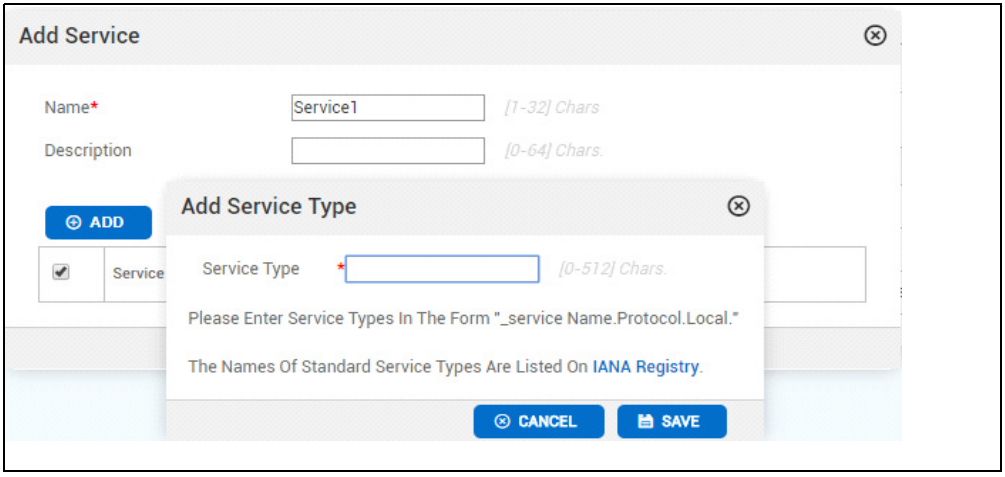
For Controller to detect services on a tagged VLAN (say VLAN XX), Controller should have a VLAN profile VLAN XX (configured VLAN).

4. Click *Save* to save your changes.

Adding or Removing Services

The Services tab allows you to modify the services that may be detected via Service Control; by default, several services are pre-configured in the system. However, you can expand this list by clicking the *Add* button to create a new service.

Figure 105: *Add Service*



Fill in the required fields as described below:

- **Name**—Enter a name for the service
- **Description**—Enter a brief description
- **Service Type**—Enter the service type string(s). If multiple entries are needed, enter them one at a time, clicking **Add** after each one. They will display in the *Added Service Types table.*

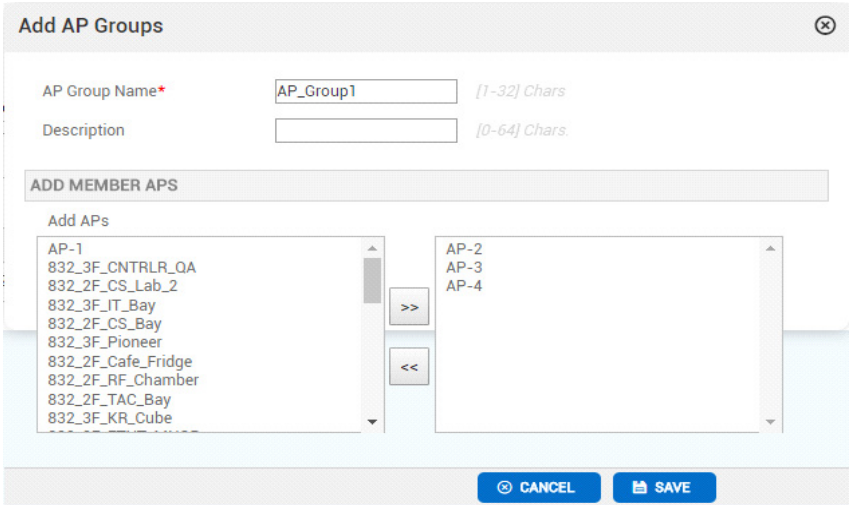
To remove an added service, verify the box alongside it and click *Delete*.

- Click *Save* to save the new service.

Configuring Locations

The *Locations* tab allows you to specify locations where services should be advertised; by default, no locations are configured, so click *Add* to create one.

Figure 106: *Add Location*



A Location consists of three main components: the location's name, description, and member APs. Enter the *Name* and *Description* in the fields provided, then select the AP(s) that belong to the desired location from the drop-down list. Click the button pointing to the right to add the selected AP(s) to the new location.

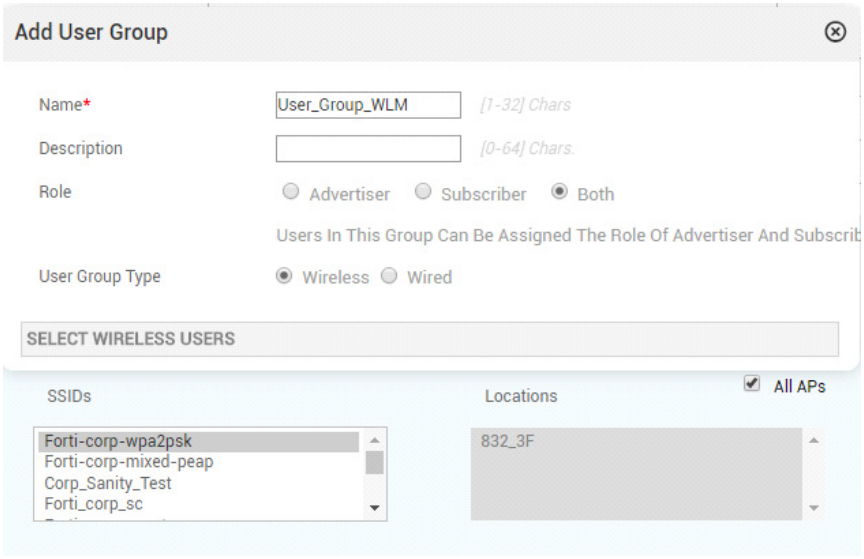
Click *Save*, to view the new location in the *Location Table*. The AP(s) specified in the location definition will now provide access to the service.

Creating User Groups

User Groups segregates Subscriber and Advertisers under a group. User Groups define which users/Advertisers (grouped by either VLAN for wired clients or SSID/Location for wireless) can access the advertised service or advertise the services.

By default, there is no User Group.

Figure 107: *Add User Group*



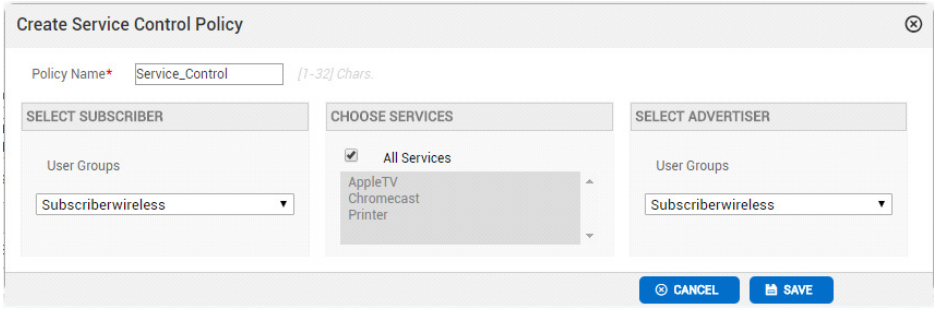
A *User Group* consists of four main components: the group's *name, description, Role, User Group Type,* and *SSIDs*. These fields will allow you to customize which users can access the defined services.

1. Enter the *Name* and *Description* in the fields provided.
2. Select one of the Role for the user group. The options is Advertiser, Subscriber, or Both.
3. Select the *User Group Type*. The options is *Wireless or Wired*.
4. If you have selected *Wireless* user group type, then *Select Wireless Section*. From the *Select Wireless Users* section, select the *SSIDs* that should be allowed access. To select multiple options, click and drag across them. Ctrl+click to select or de-select items individually.
5. If you have selected *Wired* user group type, then the *Select Wired Users* section. Enter the VLAN(s) that should be allowed to access advertised services.
6. Click *Save* to create the group. The devices contained within the group's parameters will now be able to access the advertised services.

Defining Service Control Policies

Service Control policies determine which user groups can access specific advertised services. Thus, the policies table allows you to define routes between the subscriber (i.e., the device that seeks the service) and the advertiser (i.e., the device that provides access to the service).

Figure 108: *Create Service Control Policy*



1. From the *Policies* tab, click *Add* to access the *Create Service Control Policy* window.
2. Enter a name for the policy to be created in the *Policy Name* field.
3. Enter the description of the policy.
4. Use the *Select Subscriber* drop-down to specify the group that should be granted access.
5. Select the desired services from the drop-down list supplied in the *Choose Services* section. Note that if all services should be included, simply verify the *All services* box.
6. Finally, use the *Select Advertiser* drop-down to select the group that supplies access to the services.

Click *Save* to save the new policy.

Roaming Across Controllers

Clients can roam between access points connected to two different controllers in same subnet or different subnets. System director allows you to specify static or dynamic roaming.

Things to consider before enabling RAC

- IP PREFIX validation has to be OFF in the RAC enabled ESS profile.
- RAC can be enabled on more than one ESSID
- If any parameter of an ESSID profile is changed, then RCA must be stopped and the changes made in the ESSID must be updated to all controllers in the roaming domain.
- Ensure that the controller IP is reachable before adding its IP address to the roaming domain.

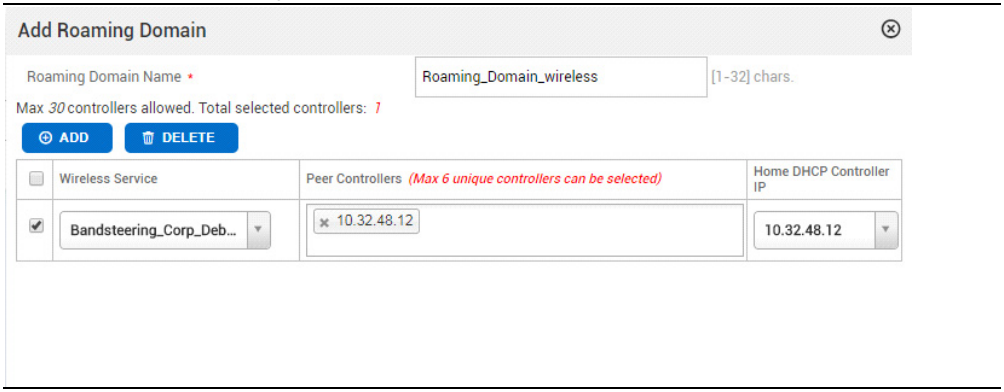
In **static DHCP home** configuration, you specify one of the controllers (in the roaming domain) as the home controller. A client associating with any controller in the roaming domain will receive IP address from this home controller. Once a controller is set has home, it applies to all the native VLAN, configured VLAN and dynamic VLAN configurations of that controller as per the "tunnel interface type" set in in the ESS profile.

In **dynamic DHCP home** configuration, a client associating with a controller for the first will continue to receive IP address from that controller. This controller will be the home controller for the client. To allow dynamic roaming, set the home controller IP address as 0.0.0.0.

When RAC is stopped all the existing clients are forcefully de-authenticated and forced to reconnect. Irrespective of the client has roamed or not, this process is applied on all clients in the roaming domain.

To configure RAC in FortiWLM, do the following:

1. Specify a Mobility Domain Name
2. Select an ESSID profile (Wireless Service)
3. Select member controllers attached to that ESSID profile. You can select a maximum of 6 controllers are member controllers
4. Select a Home DHCP IP: The IP address of the home controller in the roaming domain. All the DHCP packets from the visiting client will be forwarded to this home controller and will be delivered locally in home.



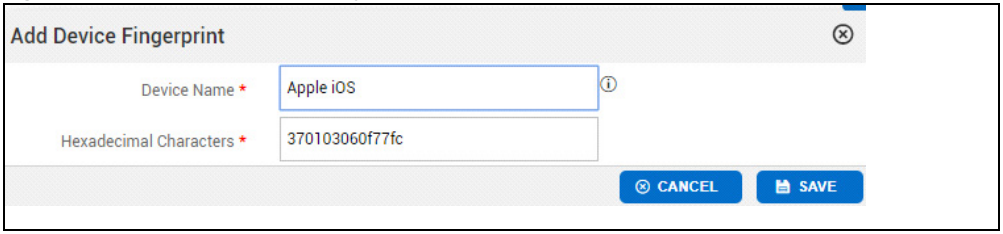
5. Now, click the PUSH icon to push this this profile to selected controllers.

Device Fingerprinting

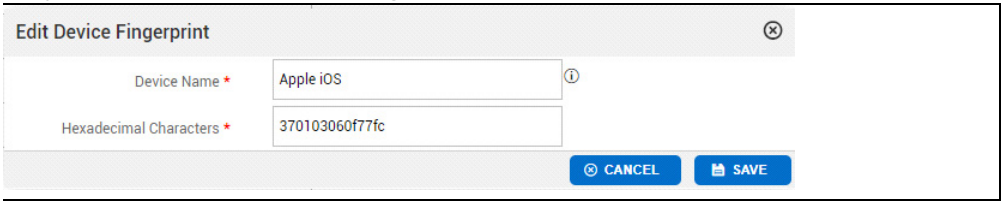
You can manage device OS fingerprinting options (configuration and monitoring) from the WebUI. The options include:

- Adding a new device OS type
- Importing Device OS type list
- Export device OS type list
- Editing an existing device OS type
- Deleting an existing device OS type

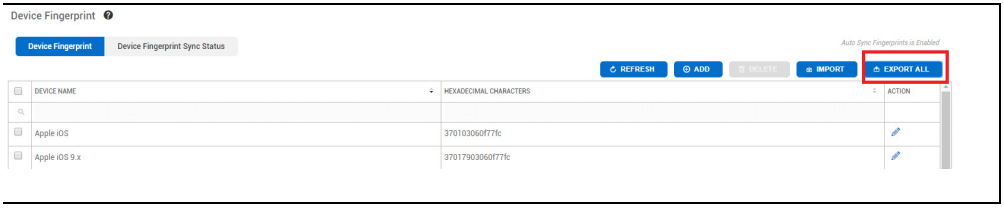
Add a new device OS type: Click the add icon and enter the device name and the corresponding hexadecimal value of its OS type.



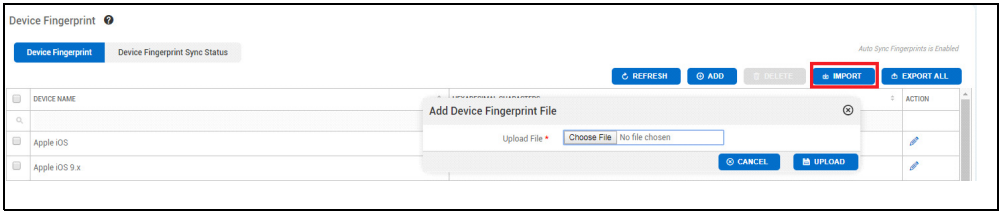
Edit an existing device OS type: Click the edit icon in the action column of corresponding the entry to be modified and made changes.



Export entries: Click the export icon to export full or selected list of entries to a text file. This can then be imported to another server. To export specific entries, select the checkbox against the entries and click the export icon.



Import new entries: To import new entries, click the import item and browse to the location that has the text file and click the UPLOAD button.



Delete entries: To delete an entry, select the checkbox of the entry and click the trash can icon.

Duplicate entries are observed in the following cases:

- If a device OS type was edited when one of the managed controllers (previously synced with entries) is offline, re-sync will result in duplicate entries.
- Reset of device fingerprints from WLM after syncing with few edits.

Simplified Config Deployment

This is a step by step wizard to easily create wireless configuration and deploy them to your controllers. This configuration assistant allows you to easily create and deploy wireless configuration on controllers with minimum effort by avoiding bulky configurations.

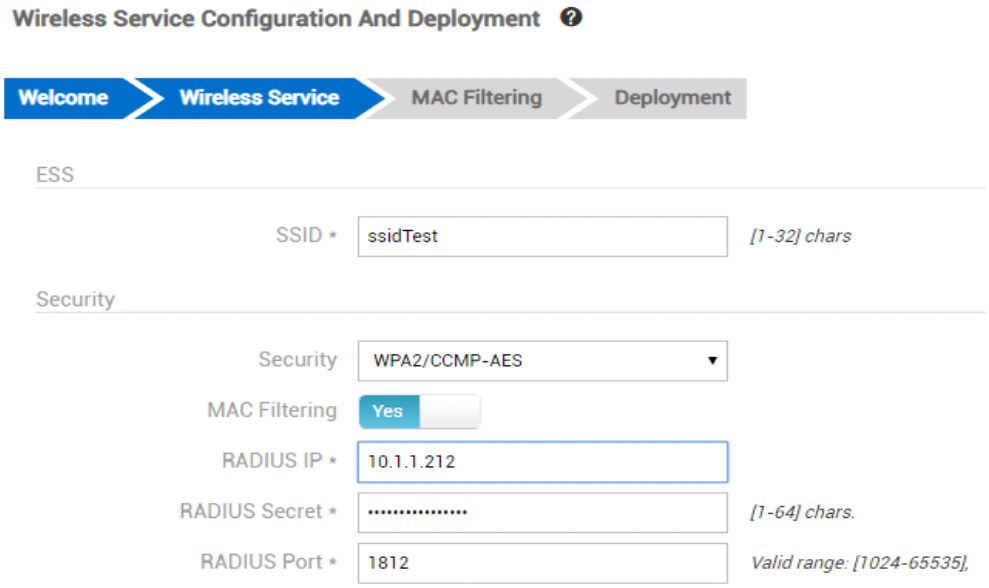
- Basic ESS and security profile configurations
- MAC filtering settings
- Wireless service deployment on controllers, AP groups, and radio groups

Navigate to *Configure* > *Deploy* > *Config Assist.*

To understand the configuration options in detail, refer to the help available in the respective configuration pages.

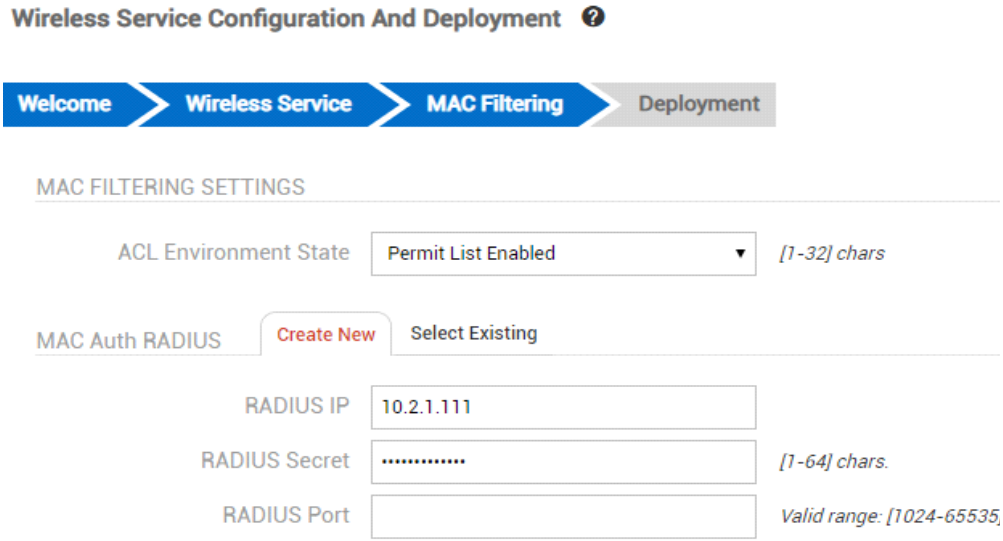
1. Click *Next* on the optional welcome page of the configuration wizard. To skip this page in further configurations, select Don't display the Welcome page again.
2. Enter a name for the wireless network (*SSID*).
3. Select the *Security Mode* and update the subsequent fields. The security options are grouped logically; when you select a specific security protocol, the page is refreshed to display fields that accept parameters for that security protocol.
   Enable *MAC Filtering* for the security profile and click *Next* to configure the filtering options.

Figure 109: *Wireless Service configuration*



4. Select the *ACL Environment* to create rules to allow or deny access based on the MAC address. The supported options are, *Disabled*, *Permit List Enabled,* and *Permit List Disabled*.
   Note: When the ACL Environment is disabled, configuring the MAC authentication RADIUS server is mandatory.
   Configure a RADIUS profile for MAC authentication. You can *Select Existing* RADIUS profile or create a new one. To create a new one, configure the following:
   - The IP address of the RADIUS server.
   - The shared secret for the RADIUS server.
   - The port that the RADIUS server uses for authentication.

Figure 110: *MAC Filtering configuration*



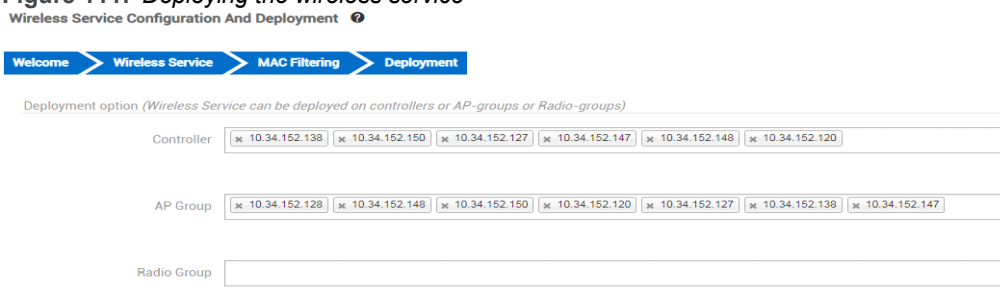
After the ESS and security configurations are complete, you can deploy the wireless service on controllers, AP groups, and radio groups. Click on each of these options to add/modify existing controllers, AP groups, or radio groups. You can add new controllers and groups.

Note: VPN and PAT controllers cannot be discovered from this deployment page.

- Select *Add Controller* and enter the controller hostname/IP address, the user Id, and the encrypted password for the controller.
- Select *Add AP Group* and enter a unique name and description, select the group type and the usage type.
- Select *Add Radio Group* and enter a unique name and description for the radio group and add the members.

Click *Finish* and you are directed to the wireless Service Profile page to view the configured profiles and their deployment status. You can modify the created profiles if required.

Figure 111: *Deploying the wireless service*



Design-Features

Application Visibility

Fortinet WLM allows you to monitor and/or block traffic based on applications used by clients in your network. By default, FortiWLM allows all application traffic and monitoring data is shown as cumulative value of all usage.

The application visibility feature in FortWLM allows you to do the following:

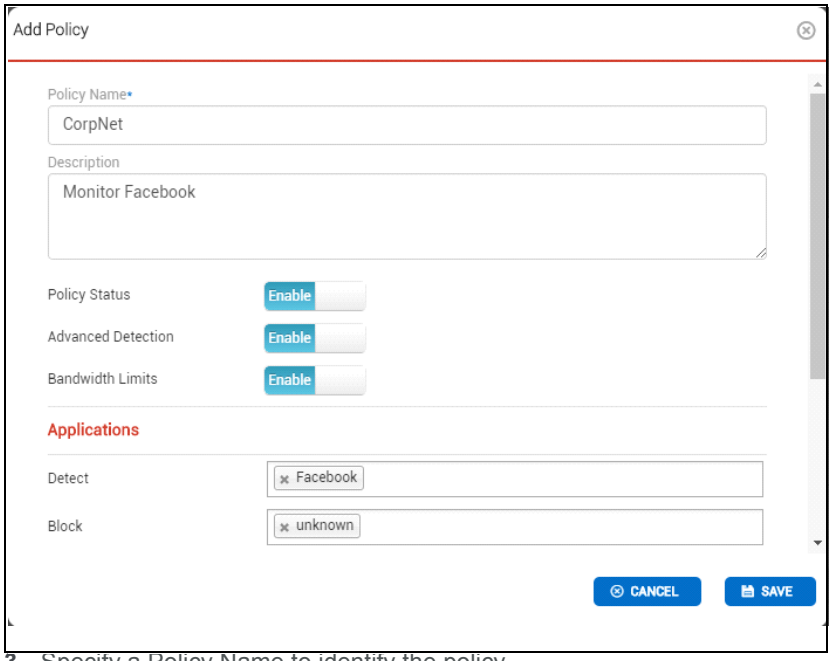
- Monitor application traffic
- Block applications
- Create and push policies to controller
- Control bandwidth usage (Bandwidth Throttling)
- Modify priority of application traffic using DSCP values. (DSCP Marking)
- View blocked statistics (Blocked Stats)

To monitor or block applications, you must create application visibility policies. Application visibility will take effect only after the policies are pushed to the controller.

To create a policy, do the following:

1. In the FortiWLM WebUI, go to *Configure* > *Design-Features* > *Application Visibility* to view the DPI Global Configuration page.
2. Policies are defined in the Policy and System Applications section of the page. Click the + icon to create policies in the Add Policy settings window. Enter the following details to create a policy rule:

Figure 112: *Add DPI Policy*

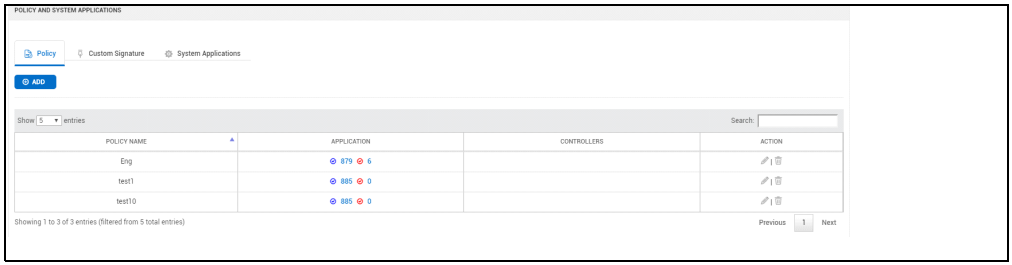


3. Specify a Policy Name to identify the policy
4. Provide Description for the policy.
5. Toggle the Profile Status switch to Enable
6. To add applications for monitor or to block, click either the Detect text box or Block text to view the list of supported application and select the required application. To add more than one application click on the textbox again after adding an application.
7. Select the controller to select the required ESSID and click SAVE to add the policy.

A single policy can be used to monitor and detect applications.

8. After the policy is added, it is listed in the Policy and System Applications section. For each policy, this section shows the number of applications being monitored (blue color) and blocked (in red color).

Figure 113: *DPI Policy Listing*



DSCP Marking

DSCP value is selectable field that can be used to assign various levels of precedence to network traffic. By default, traffic packets contained an EF value and with the introduction of DSCP you can now change the priority bit from EF to a DSCP value.

Valid DSCP value strings

- af11
- af12
- af13
- af21
- af22
- af23
- af31
- af32
- af33
- af41
- af42
- af43
- cs0
- cs1
- cs2
- cs3
- cs4
- cs5
- cs6
- cs7
- no

- ef

For more details about DSCP values, see: https://tools.ietf.org/html/rfc4594

When a DSCP value is applied to application traffic, this value and the associate priority is maintained till the next node in the traffic. If the traffic carrying the DSCP value encounters a QoS aware switch, then the DSCP value maybe overridden by a QoS value specified by the switch.

Bandwidth Throttling

You can now enforce and allocation maximum bandwidth usage limits for individual applications.

To enable bandwidth throttling and mark DSCP value, Go to *Configure* > *Design-Features* > *Application Visibility* > *Policy.*

1. Enable policy
2. Enable Bandwidth limits

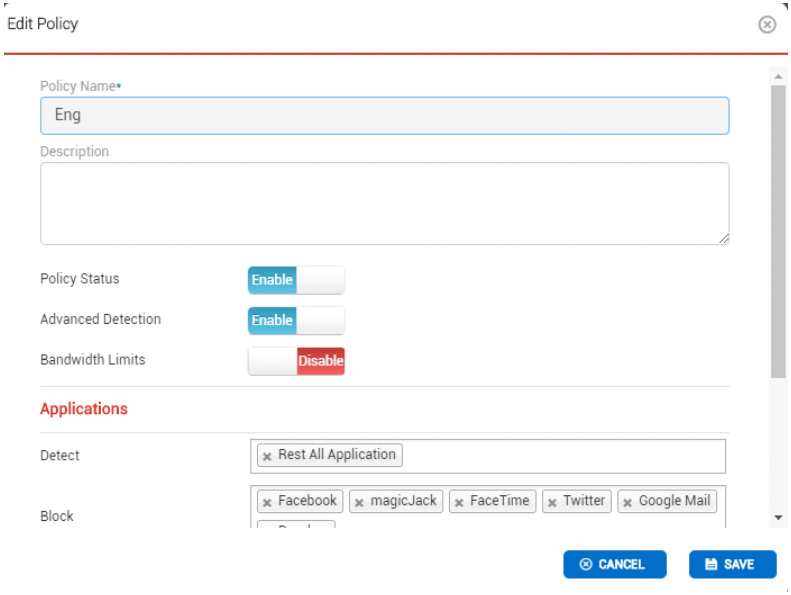
	Minimum	Maximum
Client	150 kbps	1 Gbps
ESSID / Port Profile	150 kbps	12 Gbps

3. Select applications.
4. You can specify maximum limits per client and per SSID
5. In the DSCP Marking column, select the DSCP value.

Blocked Statistics

The application visibility dashboard is enhanced to display visual statistics of blocked traffic. The following screenshots illustrates blocked statistics for blocked applications (Facebook, YouTube, and Skype)

Create a policy



View blocked Statistics

To view blocked statistics, go to *M.onitori*> *Overview* > *Application Summary* > *Blocked tab*

Wireless Service Profiles

A wireless service profile is a set of configurations created on the *NM* server that is applied to a controller to create the service on the controller. A service profile consists of *ESS Profile, Security Profile, RADIUS Profile, and Tunnel (GRE/VLAN) Profile*. The ESS and security profiles are common across multiple controllers, the *RADIUS Profiles* can be common or controller specific and the *Tunnel Profiles* are configured per controller basis.

All complete service profiles are registered to controllers or AP groups. A service profile is said to be *complete* only if the configurations for the required fields in the profile with the dependent configuration profiles are complete and the profile is effective on saving or registering on to the controller. The service profile is said to be *incomplete* if the configurations for the required fields in the profile along with the dependent configuration profiles are incomplete. Incomplete service profiles will not be registered to a controller but will be saved in the database. The incomplete profile can be completed by providing the input data for all the missing fields and then can be registered to a controller or an AP Group.

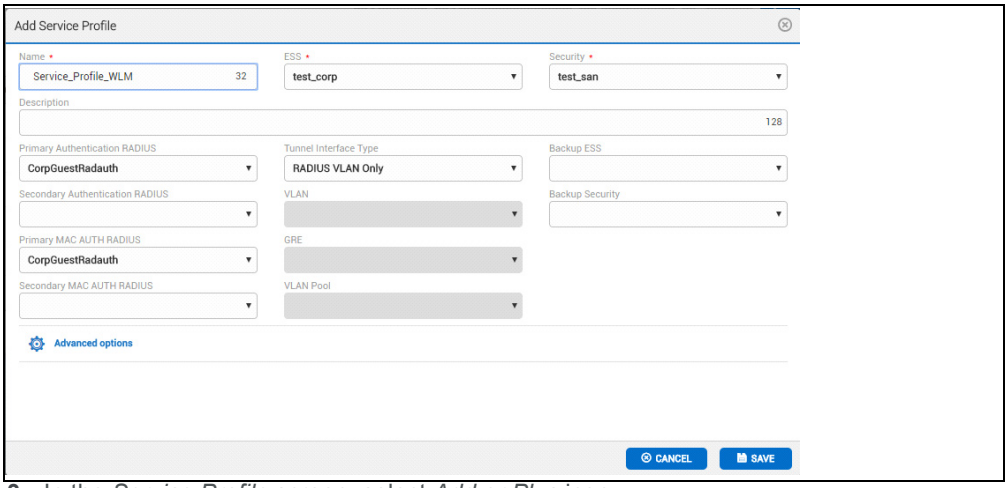
While selecting a profile you can select one of the existing profiles that were individually created (*Configure* > *Templates* > *ESS, Security, RADIUS, VLAN or GRE*) or provide a name of

the non-existent profile and create the named profile at later point of time. Once the named profile is created, the service profile is applied to the registered controllers.

Add a Service Profile in FortiWLM

1. Navigate to *Configure* > *Design-Features* > *Wireless Service*.
2. The *Service Profile* screen displays a list of service profiles to which a Controller or an AP Group can be registered.

Figure 114: *Service Profile - Add*



3. In the *Service Profile* screen, select *Add or Plus* icon.
4. The *Service Profile - Add* screen allows you to select existing *ESS Profile, Security Profile, RADIUS Profile, and Tunnel (GRE/VLAN) Profile* to associate with the service profile. By default, the service profile is associated with the ESS and security profiles named default.
5. In the *Name* field, type the name of the service profile. The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.
6. In the *Description* field, provide a description for the service profile. The description can be up to 128 characters long and can contain spaces and special characters (for example, Service Profile - ESS Profile).
7. In the *ESS Profile* field, type a new ESS profile name or select an existing ESS profile from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths:
   Configure > *Design-Features* > *Wireless Service* > *Service Profile* > *ESS Profile*
   Configure > *Templates* > *ESS* > *Select a ESS Profile* > *Edit option*
   The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.
8. In the *ESS Profile for Overflow* field, type the ESS profile for overflow name or select an existing ESS profile for overflow from the drop-down list. This field is applicable for all

AP300 or AP400 model. This works by having the two ESS profiles share an SSID so they can seamlessly move clients back and forth as needed.

9. In the *Security Profile* field, type the security profile name or select an existing security profile from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths:
   Configure > *Design-Features* > *Wireless Service* > *Service Profile* > *Security Profile*
   Configure > *Templates* > *Security* > *Select a Security Profile* > *Edit option*
   The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.
   ESS profiles and Security profiles can be configured either from *FortiWLM* or from the controller. You can tell where a profile was configured by checking the read-only from the controller, by selecting *Configure* > *Templates* > *ESS* and look at the field *Owner*. A controller configuration owned by *FortiWLM* has the owner listed as *nms-server*.
10. The *RADIUS* is AAA protocol (authentication, authorization and accounting) server that comprises of the user names and passwords of all the users to authenticate a client. *RADIUS Profiles* can be either common to all controllers or specific to one controller.
    - *Common RADIUS profiles* are created by navigating to,
      Configure > *Design-Features* > *Wireless Service* > *Choose a Service Profile* > *Select Edit option* > *Service Profile - Update screen*.
      In the *Primary Authentication Radius* field, type the data for the following fields to create common RADIUS profiles.
      - Primary Authentication
      - Secondary Authentication
      - Primary Accounting
      - Secondary Accounting
      - Primary MAC AUTH RADIUS
      - Secondary MAC AUTH RADIUS
        The above names can be up to 16 alphanumeric characters long with no spaces. This is an optional field.
    - *Controller specific RADIUS profiles* are created by navigating to,
      - *Configure* > *Design-Features* > *Wireless Service* > *Choose a Service Profile* > *Select Edit option* > *Service Profile - Update screen* Choose the Radius Profile tab, select Primary Authentication tab > Select the *Add or plus* icon to add Individual Controller Radius Configuration.
      - *Configure* > *Templates* > *Radius* > *Radius Profile screen* Select the *Add or plus* icon to add Individual Controller Radius Configuration. Controller specific RADIUS profiles can be configured either from *FortiWLM* or from the controller. You can tell where a profile was configured by checking the read-only from the controller, by selecting *Configure* > *Templates* > *Radius* > *Radius Profile screen* and look at the field *Owner*. A controller configuration owned by *FortiWLM* has the owner listed as *nms-server*.

11. In the *Tunnel Interface Type*, select a tunnel interface type from the drop-down list. The following are the options:
    - *No Tunnel*: No tunnel is associated with this service profile.
    - *Configured VLAN Only*: A configured VLAN only is listed in the following VLAN Name list is associated with this service profile.
    - *Radius VLAN Only*: The VLAN is assigned by the RADIUS server via the RADIUS attribute Tunnel Id. Use RADIUS VLAN Only when clients authenticate via 802.1x/WPA/WPA2 or MAC Filtering.
    - Radius and Configured VLAN: Both configured VLAN and RADIUS VLAN are associated with this service profile.
    - GRE: Specifies a GRE Tunnel configuration.

    This is an optional field.
12. If you have selected the *Tunnel Interface Type* as *Configured VLAN Only*, *Radius VLAN Only*, and *Radius and Configured VLAN*, type a *VLAN Profile* name or select an existing *VLAN Profile* name from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths:
    Configure > Design-Features > Wireless Service > Service Profile > Edit > Service Profile - Update > VLAN Profile
    Configure > Templates > VLAN > Add
    The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.
13. If you have selected the *Tunnel Interface Type* as *GRE*, type a *GRE Profile* name or select an existing *GRE Profile* name from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths:
    Configure > Design-Features > Wireless Service > Service Profile > GRE Profile
    Configure > Templates > GRE > Add
    The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.

The VLAN and GRE profiles cannot be edited once they are synchronized to a controller.

14. Complete the *Service Profile* and select *Save* option. The service profile with the set of *ESS Profile, Security Profile, RADIUS, and Tunnel Profiles (GRE/VLAN)* are displayed on the *Service Profile* screen.

See the ***Service Profile - Add*** screen (*Configure > Design-Features > Wireless Service > Add*) in Online Help for detailed information on *Service Profile - Add* topic.

The ESS profile and security profile are default profiles across multiple controllers where as the *RADIUS and Tunnel Profiles (GRE/VLAN)* are configured per controller basis.

Cloning Wireless Profile

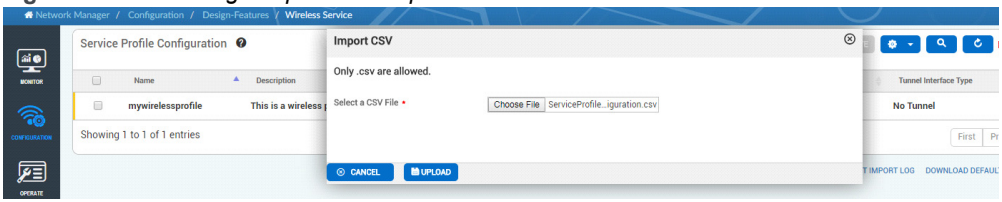
You can now clone a wireless service profile instead of creating a duplicate manually. All profiles (except VLAN and GRE) in the service profiles is cloned. For detailed information, see the online help for Service Profile.

Importing Wireless Profiles

FortiWLM supports importing a Service Profile (*.csv) from your local drive and uploading it to FortiWLM.

1. Navigate to **Configure > Design-Features > Wireless Service**.
2. Click  to import the.*csv* file.
3. Browse to the file saved on your local drive and click **Upload**.

Figure 115: *Selecting the profile to import*



Complete the Registration of a Service Profile in FortiWLM

You are allowed to register or unregister controllers or AP groups to a *Service Profile*. Registering a controller allows *NM* to apply the complete configuration of the *Service Profile* to the selected controller. Similarly, unregistering the controller deletes configuration from the controller of the selected service profile. A service profile with the set of *ESS Profile, Security Profile, RADIUS Profile, and Tunnel (GRE/VLAN) Profile* must be registered to a controller or an AP group.

To complete the registration of a service profile, follow the below steps:

1. Navigate to *Configure > Design-Features > Wireless Service*.
2. The *Service Profile* screen displays a list of service profiles to which a Controller or an AP Group can be registered.
3. Select a check box of the *Service Profile* and select *Edit*. The following tabs are displayed:
   - Service Profile
   - Registration
   - ESS Profile

- Security Profile

4. Select the *Registration* tab. The *Service Profile - Registration* screen displays a list of controllers and AP groups registered to that particular service profile. The *Service Profile - Registration* screen provides the following details:
   - *Registered Member*: Displays the host name or IP address of the registered member.
   - *Member Type*: Displays if the member type is a controller or AP group.
   - *Auto-Sync*: Displays if the Auto-Sync is *On* or *Off*.
   - *Last Sync Time*: Displays the last sync time of the service profile to the registered controller or an AP group.
   - *Sync Status*: Displays the sync status of the service profile to the registered controller or an AP group. The following are the types:
     - *In-Sync*: The service profile status is displayed as *In-Sync* for the profiles with *Auto-sync* as *On* and are successfully applied to all APs or Controllers.
     - Sync Pending: All the incomplete service profiles display the Status as *Sync-Pending*.
     - *Failed*: The service profile status is displayed as *Failed* if the controllers are in the *Deleted* or the controllers are *not managed* or the controllers are in the *Unlicensed* state. If the controller registered to the service profile is unregistered, all the profiles on that controller belonging to the service profile is deleted from the *Registration* table.
   - Sync Details: Displays the reason for the controller or AP group that failed to sync.
   - Controller Group Name: The Controller group the Service profile is registered to.
   - Nodename: The name of the Controller.

Secondary controllers cannot be registered to a service profile. The status is displayed as *Sync Failed* when registered to a secondary controller.

You will be able to perform the following actions on the *Service Profile - Registration* screen:

- **Auto-Sync**:
  - Select the *Edit* option for a Controller or an AP Group.
  - Select the *Auto-Sync* to *On* in the Registration-Update screen. The option *On* enables the service profile to synchronize any modified data to the registered controller or an AP group. If any of the profiles within the *Service Profile* is modified, the modified profile is automatically synchronized to the registered controller only when the *Auto-sync* is set to *On*
- **Register**: Select the service profile and register to a controller, AP, or an AP Group.
- **Unregister**: Select controllers or AP groups check box and select the *Unregister* option. The following are the scenarios:

- Unregistering a service from the AP group deletes the services from all the APs within the group.
- When the service is registered to both AP group and controllers, by unregistering a service from the controller will delete the services only on the APs which are not part of the registered AP group.
- If the controller is not online at the time of service un-registration, the services will be unregistered for the APs after the controller comes online.
- All the service profiles get unregistered from the AP group, when an AP Group is deleted.
- When a service profile is deleted, the services will be unregistered from all the APs within the AP group to which the service is registered.
- When the controller is deleted from the inventory, the APs corresponding to the controller will not be deleted from the AP group. But the services will be deleted on those APs.

- **Force Sync**: You can perform the necessary modifications on failed APs and allow to perform a *Force Sync*.

See the ***Service Profile - Registration*** screen (*Configure* > *Design-Features* > *Wireless Service* > *Edit*) in Online Help for detailed information on *Service Profile - Registration* topic.

Verify if a Controller is using NM or a Controller Configuration

There are three options to determine whether a controller is using a *FortiWLM* configuration or Controller configuration.

The first option to determine which controllers are using a service profile in the *FortiWLM* is by following these steps:

1. Navigate to *Configure* > *Design-Features* > *Wireless Service*. The *Service Profile* screen provides a list of service profiles to which a controller or an AP group can be registered.
2. Choose a *Service Profile* and select *Edit.* The following tabs are displayed:
   - Service Profile
   - ESS Profile
   - Security Profile
3. Select the *Deploy* tab, the list of controllers, AP groups, and Radio groups registered to the Service Profiles is displayed.

The second option to determine which controllers are using a service profile in *FortiWLM* is to view a controller's current profiles by following these steps:

1. Navigate to *Configure* > *Device Center* > *Configuration View*. The *Controllers View* screen displays a list of controllers to which the profiles are applied.
2. Choose a controller from the *Controllers View* screen and select *View*.

3. The *Controller View* tab with each profile tab (*ESS Profile, Security Profile, RADIUS Profile, VLAN Profile,* and *GRE Profile*) is displayed. The profiles applied on the controller from *FortiWLM* are indicated here.

You cannot perform any modifications from here.

The third option to determine the controller configuration is by viewing the controller (SD) itself. From the controller, click *Configure* > *Templates* > *ESS* and look at the field *Owner*. A controller configuration owned by *FortiWLM* has the owner listed as *nms-server*.

Port Profiles

You can now create port profile and push them to available ports in access points managed by FortiWLM. Single Port Profile can be applied only to APs of a single controller, if the profile contains VLAN and/or Radius profile. To apply same port profile to multiple controllers create required VLAN and/or Radius profiles with the same name for all the controllers and select it during Port profile creation

To use this feature, do the following:

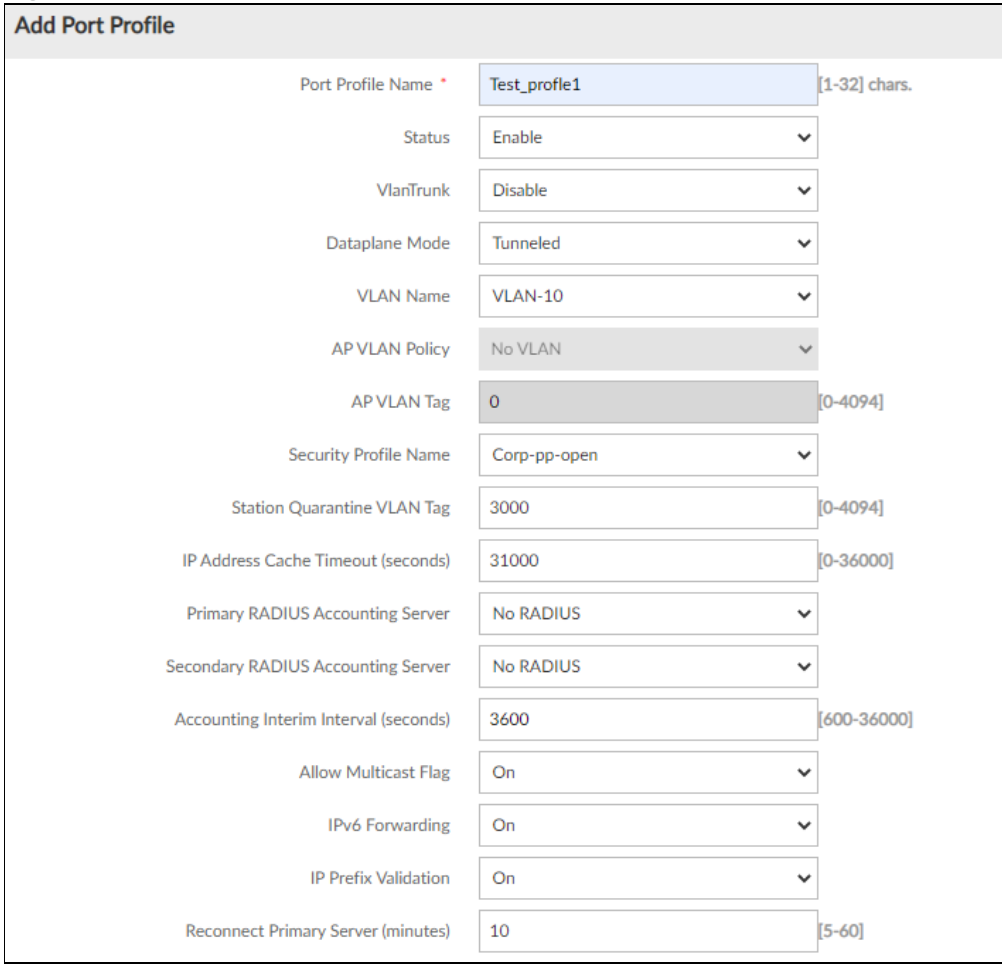
Create Port Profile (to include security profile in a port profile, create the security profile before creating port profile)

Push the port profile to available ports.

Creating a Port Profile

To create a port profile, go to *Configure* > *Design-Features* > *Port Profile* and click the add icon to create a port profile.

Figure 116: *Adding Port profile*



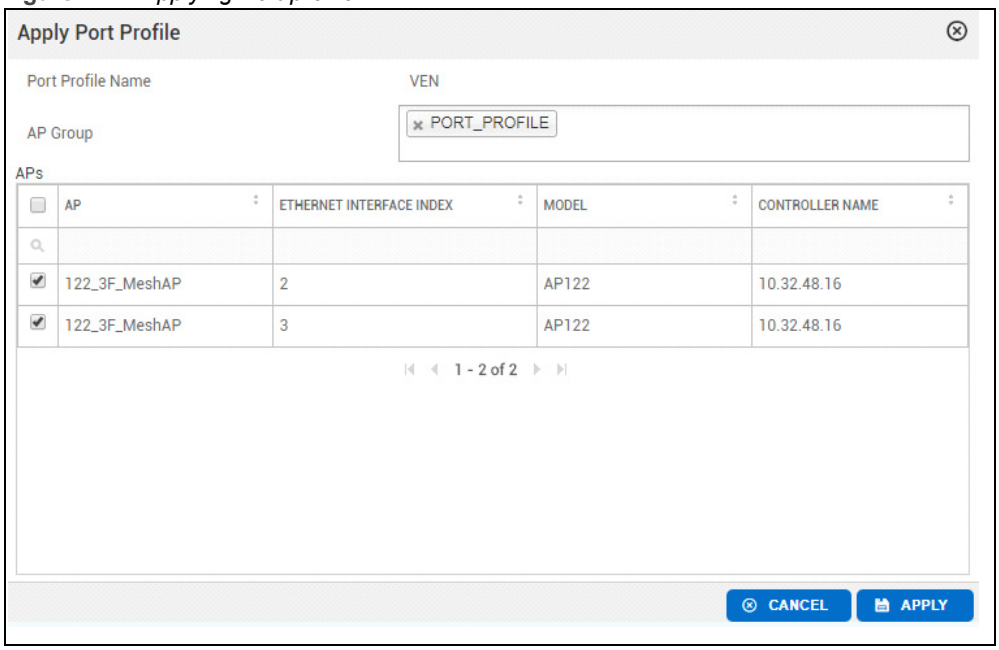
- Port Profile Name: Enter a name for the profile.
- Status: Enable/Disable, Select whether the profile should be enabled or disabled.
- VLAN Trunk: Select Enable to enable trunk mode for the port.
- Dataplane Mode: Can be set to Tunneled or Bridged.
- VLAN Name: This field is used only if the Dataplane Mode is set to Tunneled operation. Identifies the name of the VLAN on which the profile is configured.
- AP VLAN Policy: This field is toggled when the profile is configured for Bridged operation. This tag is an integer from 0 to 4094 that identifies the AP's VLAN.
- AP VLAN Tag: Specify the VLAN tag.

- Security Profile Name: Select an existing security profile. To include a security profile, you must create a security profile before creating the port profile.
- Station Quarantine VLAN tag: This field specifies the VLAN Tag to be assigned to associated quarantined stations. The valid range is 0 - 4094.
- IP Address Cache Timeout (seconds): Configure this field for wireless disabled clients residing behind a wireless bridge that might get disconnected when roaming. The IP address of such clients is retained for the configured cache timeout period and if the reconnection occurs within this period then the client connectivity is not impacted. This field supports both IPv4 and IPv6 addresses. The valid range is 0 - 36000 seconds.
- Primary RADIUS Accounting Server
- Secondary RADIUS Accounting Server
- Accounting Interim Interval (seconds)3600 [600-36000]
- Allow Multicast Flag: Toggles multicast traffic on or off on the port.
- IPv6 Bridging: Specifies whether bridging for IPv6 devices is On or Off.
- IP Prefix Validation: Available only in tunneled mode.

Push the Port Profile

Click the push icon to view the Apply Port Profile pop-up. Select the available ports and click the APPLY button.

Figure 117: *Applying Port profile*



Auto Radio Resource Provisioning (ARRP)

ARRP is a mechanism that allows auto selection of channels for optimum use with respect to a given RF environment. By default, in a native cell the administrator manually allocates channels. By enabling ARRP, each AP scans all channels and provides the scan details to the controller. The controller uses this information to select and allocate the best available channel per radio. You can perform ARRP configurations for interface 1 and 2 channels and select channels for ARRP participation from the custom channels list. This is supported on FortiWLC 8.6.0.

FortiWLM now allows registration of a maximum of 1024 ARRP profiles to AP groups. This is supported only on FortiWLC version 8.6.2 and greater.

You can configure ARRP settings on **Radio1** and **Radio2**.

By default, this feature is disabled.

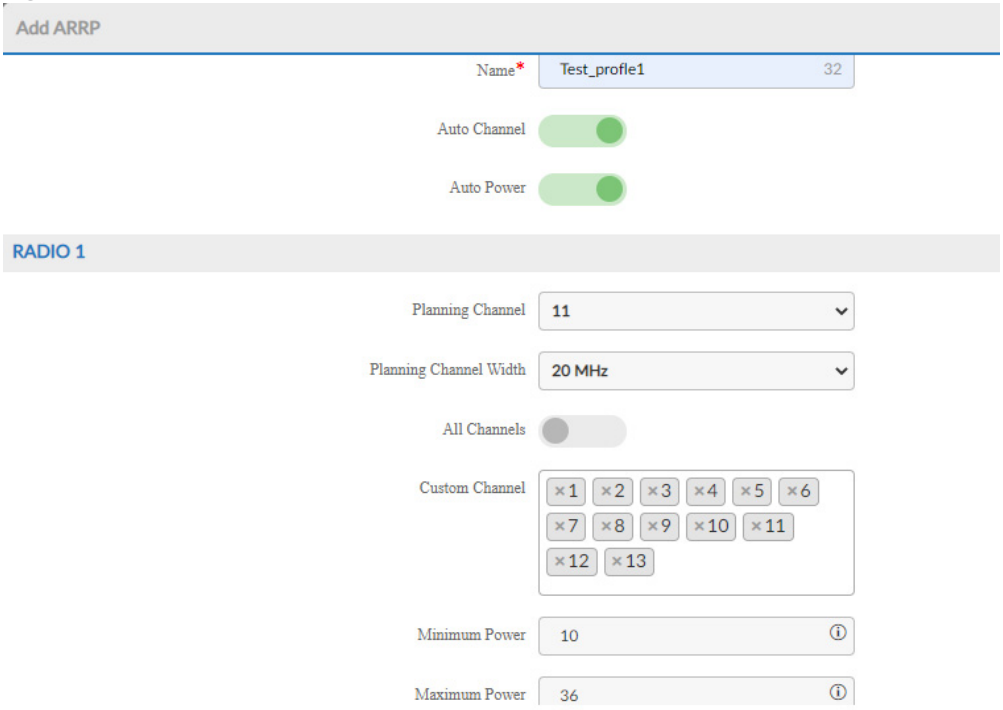
- Supported only on 11ac/ax APs.
- Once enabled, the virtual cell is not available for 11ac APs.
- Non-11ac/ax APs continue to work as configured and will not be affected by auto channel feature.

If the ARRP is disabled, all 11ac APs will reboot to default channels.

Configuring ARRP

To configure ARRP across one or more controllers, create an ARRP profile with required settings and push this profile to one or more controllers.

Figure 118: *Adding ARRP profile*



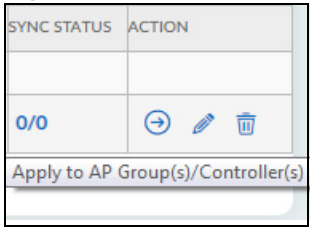
- Auto Power: The auto power functionality is applied only after channel allocation irrespective of when the auto power option was enabled. When enabled, the controller will determine the optimum power level between neighbouring (by channel) 11ac APs. The auto power option can be enabled and applied only when ARRP is enabled.
- Planning Channel: Once enabled, the respective radios of all APs are set to the channels selected for radio 1 and radio 2. In the above screenshot, the planning channel is set to 11 /20MHz for radio 1 and 48/20MHz for radio 2. Based on the report received by all APs, the controller allocates the optimum channel. DFS channels are not available to be set as planning channel
- Planning Channel Width: Select the planning channel width. The supported options are 20MHz, 40MHz Extension Channel Above, and 40MHz Extension Channel Below. For radio 2, additional options of 80MHz and 160MHz are supported.
- All Channels: All channels are selected for planning. This is enabled by default when Auto Channel is enabled.

- Custom Channel: Based on the planning channel width, the custom channels can be configured for the radios. All channels are available when the planning channel width is 20MHz.
  Note: The above mentioned Minimum Power and Maximum Power while using Auto Power, Planning Channel Width, and Custom Channel are supported with FortiWLC 8.6.0 and above.
- Freeze: The option is applied after the initial planning phase. When this option is disabled, the 11ac APs perform periodic scan (at the end of every minute) on their allocated channels. This is used to determine the quality of the channel. If the quality of the channel crosses the threshold limit (based on three consecutive scans), it sends a request for change of channel. If enabled, the periodic scan is disabled and the 11ac APs remain in allocated channels irrespective of the channel quality. If this option is disabled, the radio interface settings cannot be modified.
- Timer State and Timer: This option is available only when the Freeze option is disabled. To avoid frequent channel change, you can set the channel scan interval to happen at the end of 15 minutes. By default the timer interval is set to 15 minutes and maximum is 3600 minutes. When enabled, the APs start their channel quality scan at the end of 15th minute and continue to scan at the end of every minute for 10 minutes. Based on the data gathered during this period channel change may happen. At the end of the 10 minute of the scan, the channel scanning is disabled for the next 15 minutes.
- DFS: By default scanning and allocation of DFS channel is disabled during the planning phase. If enabled, the APs can scan DFS channels and they can be allocated DFS channels. DFS option must be selected when ARRP is enabled. Enabling DFS after enabling ARRP will require re-planning of channel allocation for all APs.
  Note: DFS option must be selected when the Auto RF is enabled. Enabling DFS after enabling Auto RF will require re-planning of channel allocation for all APs.
- Neighbour RSSI Threshold: Set the minimum RSSI value for the neighbouring APs. The default is -85dbm and the valid range is -95dbm to -30dbm.
- REPLAN: This option is used if a new AP is added to an AP group or controller or if the ARRP profile is edited after initial planning.

Push ARRP Profiles

Click the profile push icon to push the profile to 1 or more managed controllers.

Figure 119: *Push the ARRP profile to controllers*



Other options :

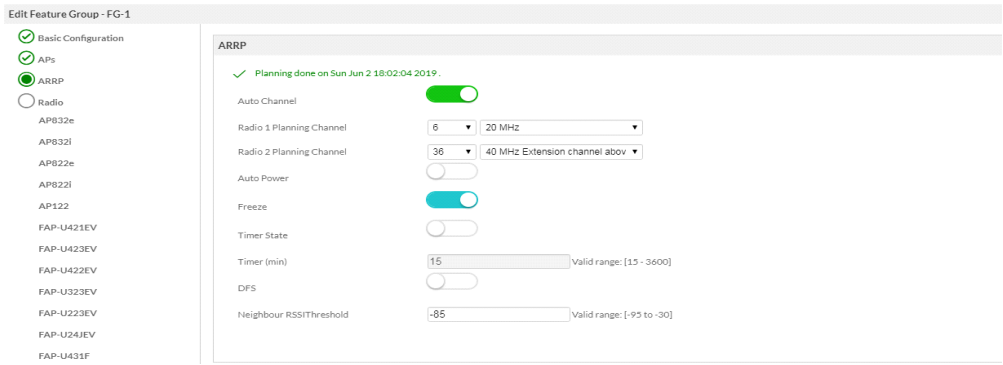
- Apply: Click the force apply icon to push the profile again to the controllers or to specific static AP Groups.
- Replan: Click the replan icon to restart ARRP planning.

ARRP Planning Status

The ARRP planning status on this page displays the date and time when the planning was done and a list of overlapping APs (APs sharing channels with their neighbours).

Click **View Sync Status** in the **Sync Status** column of an ARRP profile registered to controller or AP group, the **Registered Controller(s)/AP Group(s) Details** screen is displayed.

Note: This feature is supported only on FortiWLC 8.5.2 and above.



Limitations

If disabled, existing vCell profiles will be pushed to all 11ac APs irrespective of whether the AP was part of the vCell profile before auto channel feature was enabled. Native cell profiles will remain unchanged.

Rogue AP Detection

You can create a allow-list of APs that will perform rogue detection. Other APs that are not added to this allow-list will not scan for rogue AP/clients.

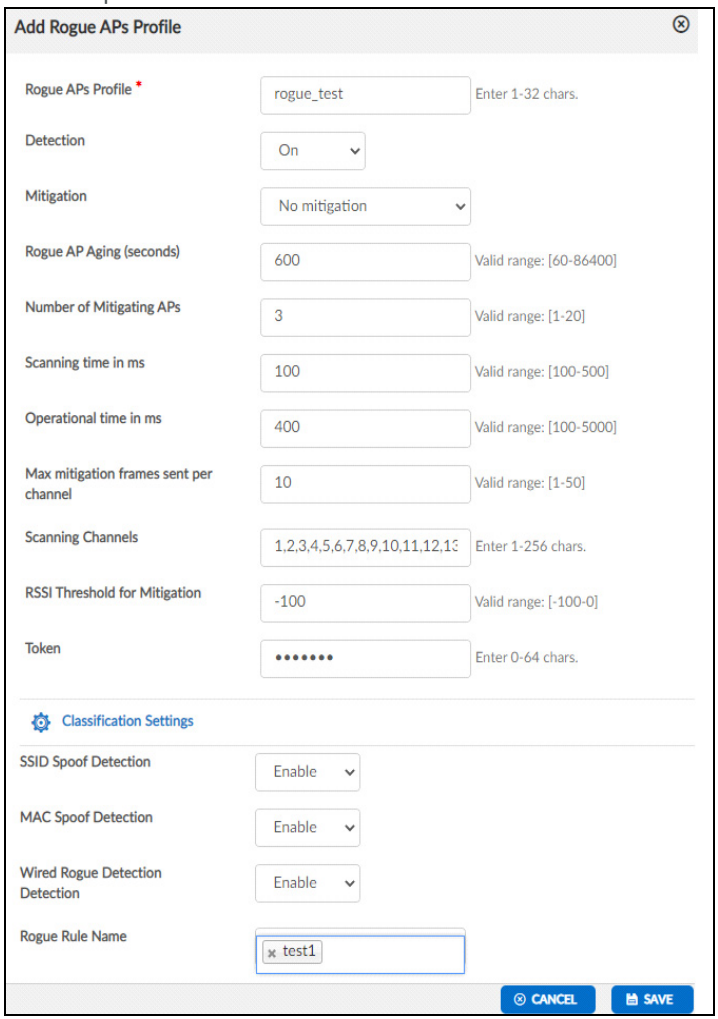
The rogue detection feature is available only if the global option for rogue detection is enabled.

If you have upgraded from an older (pre 8.1 build), all APs in the network are added to the Allowed APs list. You must manually remove from the AP list and keep or add AP required for rogue AP detection.

To configure an AP for rogue detection,

Go to *Configure* > *Design-Features* > *Rogue APs.*

Create a profile and ensure that Detection is set to ON.



- Enter a name for the profile
- In the **Detection** list, select one of the following: On: Enables scanning for rogue APs. Off: Disables rogue detection.
- In the **Mitigation** list, select one of the following:
  - *No mitigation*: No rogue AP mitigation is performed.
  - *Block all BSSIDs that are not in the ACL*: Enables rogue AP mitigation of all detected BSSIDs that are not specified as authorized in the Allowed APs list.

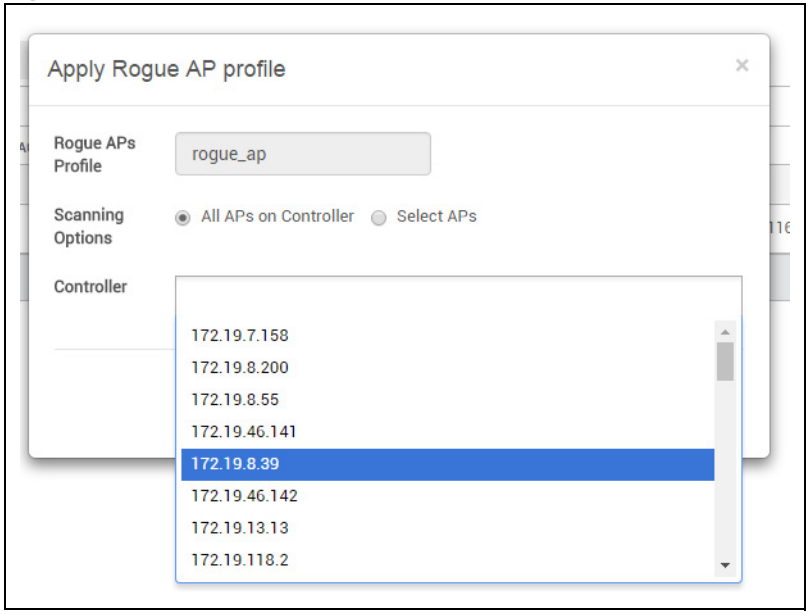
- *Block only BSSIDs in blocked list*: Enables rogue AP mitigation only for the BSSIDs that are listed in the Blocked APs list.

- In the **Rogue AP Aging** box, type the amount of time that passes before the rogue AP alarm is cleared if the controller no longer detects the rogue. The value can be from 60 through 86,400 seconds.
- In the **Number of Mitigating APs** text box, enter the number of APs (from 1 to 20) that will perform scanning and mitigation of rogue APs. Usually, you won't want to exceed 3 APs to avoid the mitigation from one AP interfering with another one.
- In the **Scanning time in ms** text box, enter the amount of time Mitigating APs will scan the scanning channels for rogue APs. This can be from 100 to 500 milliseconds.
- In the **Operational time in ms** text box, enter the amount of time Mitigating APs will spend in operational mode on the home channel. This can be from 100 to 5000 milliseconds.
- In the **Max mitigation frames sent per channel** text box, enter the maximum number of mitigation frames that will be sent to the detected rogue AP. This can be from 1 to 50 deauth frames.
- In the **Scanning Channels** text box, enter the list of channels that will be scanned for rogue APs. Use a comma separated list from 0 to 256 characters. The complete set of default channels are 1,2,3,4,5,6,7,8,9,10,11,36,40,44,48,52,56,60,64,149,153,157,161,165.
- In the **RSSI Threshold for Mitigation** text box, enter the minimum threshold level over which stations are mitigated. The range of valid values is from to -100 to 0.
- In the **Token** text box, enter a unique token string broadcast as a part of the beacons for identification of rogue and friendly APs.
- In the **Classification Settings** text box, configure the following detection mechanisms for rogue APs.
  - *SSID Spoof Detection* - SSID spoofing involves rogue access points beaconing same SSID name as a FortiWLC managed AP.
  - *MAC Spoof Detection* - In a MAC spoofing attack, rogue access points beacon same BSSID as a known managed AP, attracting clients and resources to connect to the fake network/SSID for exploiting data.
    In the case of SSID and MAC spoofing events, clients connected to the rogue APs are de-authenticated and valid notifications are raised about the presence of rogue APs.
    Note: SSID and MAC spoofing detection is only for wireless clients.
  - *Wired Rogue Detection* - Rogue APs and stations connected to the wired network.
  - In the **Rogue Rule Name** text box, select the name of rule rogue classification rule.

Click **OK**.

Click the push profile icon to push this profile. There are two ways to push the profile. When you select controllers running SD 8.0 or older version, the rogue detection profile is pushed to all APs.

Figure 120: *Applying a rogue profile*



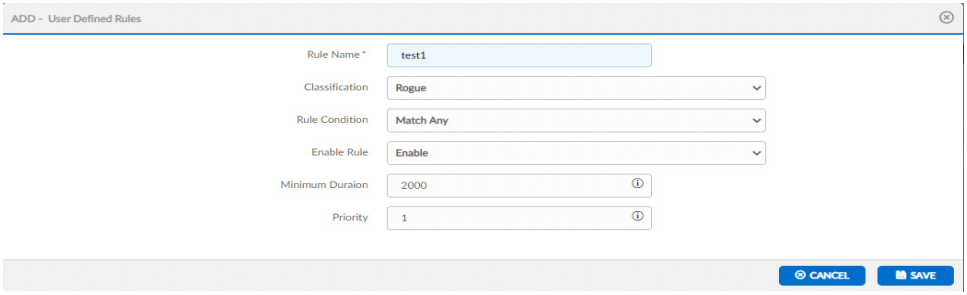
To select specific APs in the network, click Select APs to view APs running 8.1 release.

Rogue Classification Settings

The rogue access points detected by the controller are categorized as rogue and friendly based on specific rules that you configure. You can configure multiple rules; these rules are assigned different priorities. When a rogue access point is detected its attributes (ESSID, RSSI, Security mode, and discovered by APs count) are matched against the configured rules and its classification type is defined by the matching rule with highest priority.

The **Basic Configuration** for a user defined rule includes the following.

1. In the **Classification Settings** tab, select **Add**. The **Add User Defined Rule** screen is displayed.

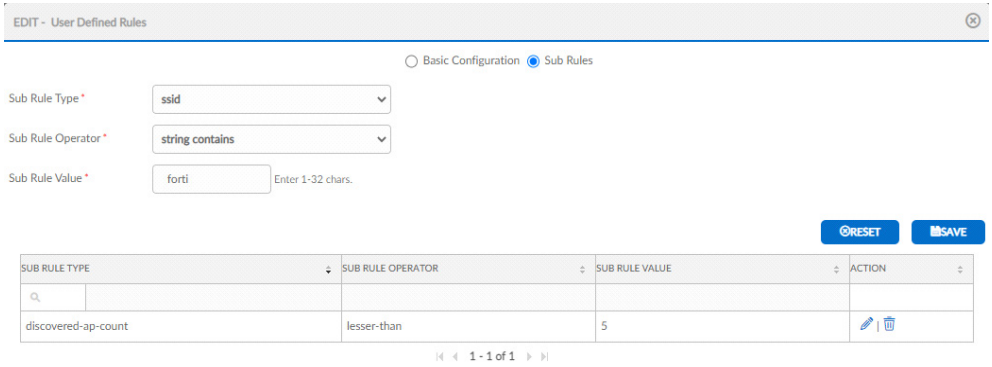


2. Provide the details for the following parameters. You can create multiple Rogue Classification rules.

   - **Rule Name:**: Unique name for this rogue classification rule.
   - **Classification**: The classification of the rogue access point, whether rogue and friendly, based on matching the configured rule.
   - **Rule Condition:** Select any of these conditions to apply.
     - o**Match Any** - If the rogue access point matches a single rule of the many configured rules, then the classification is successful and the access point is marked as per the classification type.
     - o**Match All** - If the rogue access point matches all the configured rules only then the classification is successful and the access point is marked as per the classification type.
   - **Enable Rule**: To enable or disable the rogue classification rule.
   - **Minimum Duration:** The minimum amount of time the AP is heard on air, for the rule to be applied.
   - **Priority**: Allows configuring the priority of the rogue classification rule.

3. Click **Save**. The rogue classification rule is created.

You can configure multiple **Sub-Rules** for a user defined rule. To create a sub-rule, click on the edit icon and the **User Defined Sub Rules** screen is displayed. Select **Add**; the **Sub Rule** screen is displayed. Provide the details for the following parameters.



Note: A maximum of 8 sub-rules are supported for each user defined rule.

Sub Rule Type	Sub Rule Operator	Sub Rule Value (Examples)
ssid	• string contains • string matches • string is not • string starts-with	string contains: SSID containing forti is friendly.
rssi	• lesser than • greater than	number greater than: Any unknown BSS with an RSSI greater than 50 is rogue. **Note:** The valid range is 0 to -100.
discovered-ap-count	• lesser than • greater than	number greater than: Any unknown BSS detected by more than 1 AP is rogue. **Note:** The valid range is 1 to 10.
ssid-encryption	• Enable • Disable	Disable: SSID encryption disabled.

You can perform the following additional operations on the configured rogue classification settings.

- **Delete** – Select the rule and click **Delete** or the delete icon.

- **Edit** - Select the rule and click the edit icon. You can modify the basic configuration and the sub rules.
- **Reset** – Resets configuration to default values.

AP Template

An AP Template comprises of a *Connectivity Profile* and *Radio Profiles* applied to *Device Administration group* which is one of the classified form of AP Group. A *Connectivity Profile* comprises of the AP configuration parameters related to Network Connectivity. A Radio profile comprises of the configuration parameters which is applied on the wireless interface of the AP. Profiles can be created and applied to a set/group of APs from the *NM* server. Each Radio Profile can be configured individually via the controller or NM.

The *FortiWLM* provides the mechanism to set radio properties and connectivity properties for a set of APs. These radio and connectivity properties are applied to a group of APs from the *NM* server. The user groups having configuration permissions can only create, modify, and delete templates.

The *Device Administration* group which is one of the classified form of AP Group (refer *"AP Group Inventory"* ***on page 279*** for further information on AP Groups) is applied to the device settings such as Radio and Connectivity Profiles.

When a AP Template is applied to *Device Administration group*, the Radio Profiles and Connectivity Profiles which are a part of the AP Template will be downloaded on all APs in the Device Administration group.

An AP Template cannot consist of two radio profiles for the same interface.

Before creating the AP Template, independent *Radio Profile* and *Connectivity Profile* must be created. These Radio and Connectivity profiles are applied to the AP Template.

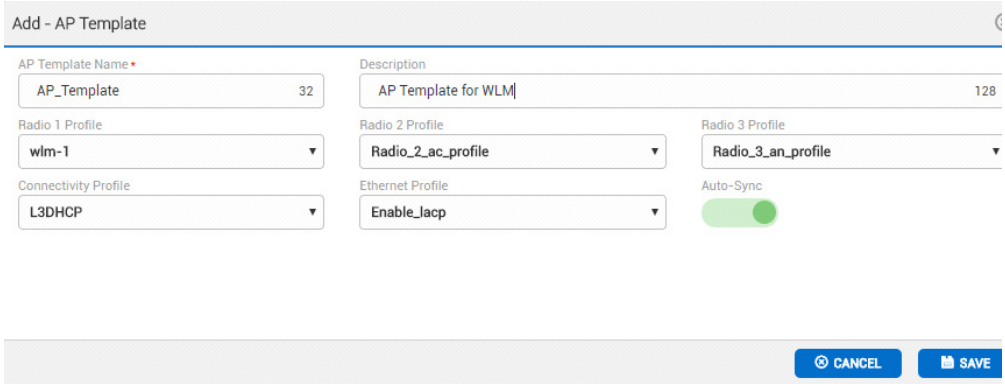
To create independent *Radio Profile* and *Connectivity Profile*. Navigate to *Configure* > *Templates* > *Radio Profile and Connectivity Profile*. See *"AP Init Scripts"* ***on page 179*** and *"Connectivity Profile"* ***on page 179***.

Creating and Applying an AP Template

To create a AP Template, follow these steps:

1. Navigate to *Configure* > *Design-Features* > *AP Template*.
2. In the *AP Template* screen, select the Add option. The *AP Template - Add* screen is displayed.

Figure 121: *AP Template - Add*



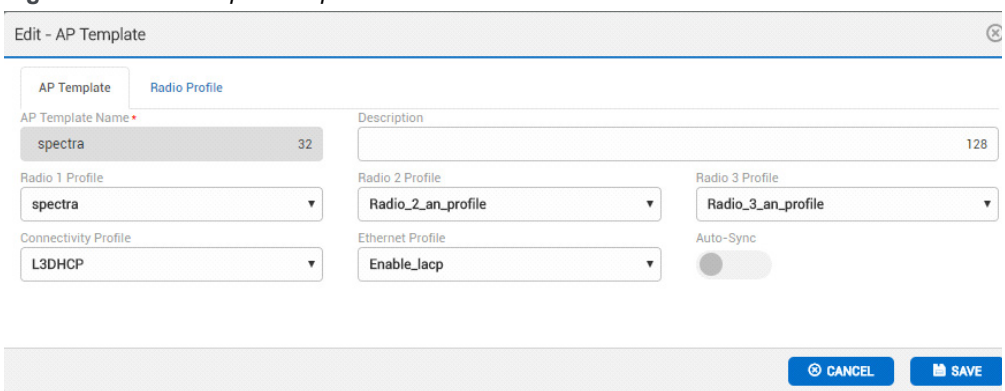
3. In the *AP Template - Add* screen, provide the details for *Name and Description*
4. Select the *Radio Profile, Connectivity Profile and Auto-Sync* options from the drop-down list. To add independent Radio, Connectivity, and Ethernet profiles, See *"AP Init Scripts"* ***on page 179*** and *"Connectivity Profile"* ***on page 179***.
5. Select *Save*. The new AP Template is included and is displayed on the *AP Template* screen.

See the ***AP Template*** screen in Online Help for detailed information on *AP Template* topic.

Updating an AP Template

1. Navigate to *Configure* > *Design-Features* > *AP Template*.
2. In the *AP Template* screen, select an *AP Template* and select *Edit.*
   The *AP Template - Update* screen is displayed.

Figure 122: *AP Template - Update*



3. The *AP Template - Update* screen displays the following tabs:

AP Template

- The AP Template - Update screen provides the *Description*, *Radio Profile, Connectivity Profile and Auto-Sync* options that can be modified.

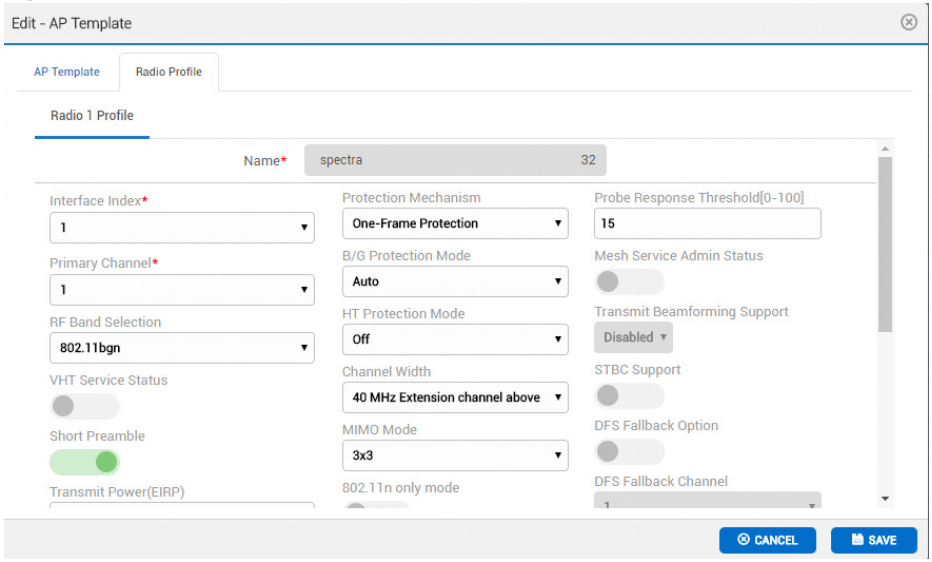
Registered Device Groups

- The *AP Template - Registered Device* Groups screen displays a list of the *Device Groups* registered to the *AP Template.* Only the *Device Administration group* which is one classified form of an AP Group can be registered to the AP Template.
- The Registered profiles can be *Force-synced*. The following are the types of Sync status:
  - *In-Sync*: The In-Sync status is displayed if the AP Templates are successfully applied to all Device Groups.
  - *Sync Pending*: The Sync Pending status is displayed, when the auto-sync flag for the AP Template is off and the current version of the AP Template is different from the synced version of the AP Template.
  - *In sync with another template*: The In sync with another template status is applicable for nested AP Groups. Where one main group and a sub group are registered to different AP Templates. While viewing the sync details of the Main Group, the sync status for all APs under the sub group is displayed as In Sync with Other Template as the sub group is registered to another AP Template.
  - *Failed*: The Failed status is displayed if the AP Template is synced to the Device Groups.

Radio Profile

The *Radio Profile* screen allows you to view the details of the *Radio Profile* applied to the respective AP Template.

Figure 123: *AP Template - Radio Profile*



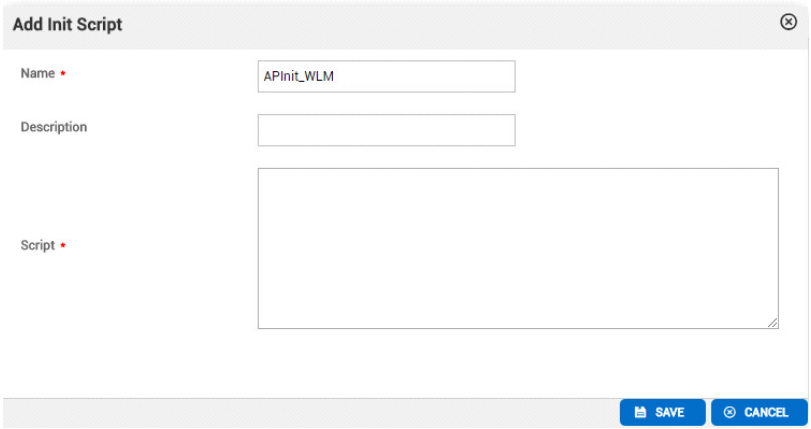
Connectivity Profile

The *Connectivity Profile* screen allows you to view the details of the Connectivity Profile applied to the respective AP Template.

AP Init Scripts

You can now load AP specific scripts files (for example, AP boot scripts) via FortiWLM and push them to controller APs or AP Groups. The default page shows the list of all scripts and options to push the script to controller APs/AP Groups, edit scripts, import Scripts, and export the script file to be used externally.

To add a new script, click the ADD button. In the pop-up box, enter a name for the script and provide the script.



Alternatively, you can load AP Init scripts by importing script files (*.scr), by clicking the IMPORT button.

WIPS Configuration

The Wireless Intrusion Prevention System (WIPS) configuration profile created on FortiWLM enables the WIPS management system to detect intrusions in your network by configuring profiles with signatures to analyze data packets, and synchronizing the profile to the controller. The WIPS configuration screen lists the existing profiles with the configured parameters and the synchronization status of the profile.

Navigate to *Configure* > *Design-Features* > *WIPS Configuration*.

The **Sync Status** displays the total number of controllers to which the profile is pushed and number of controllers on which profile is successfully synchronized. Click on the **Sync Status** to view the controller and synchronization details.

The following actions can be performed on the **WIPS Configuration** screen:

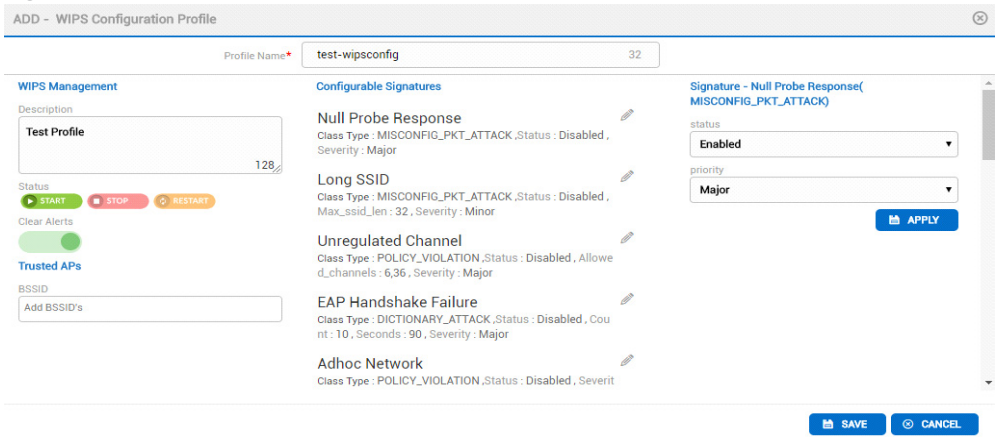
Name of the Action	Description
Add	**Add** allows to add a **WIPS Configuration Profile**.
Apply	**Apply** allows to apply a **WIPS Configuration Profile** to specific Controllers. Click on the apply icon and select the controllers to apply the profile to.
Delete	**Delete** allows deleting a **WIPS Configuration Profile**. Select the **Delete** option, the **WIPS Configuration Profile** gets delete.

Name of the Action	Description
Edit	**Edit** allows editing a **WIPS Configuration Profile**. Select the **Edit** option and modify the **WIPS Configuration Profile** as required. The name of the profile cannot be modified.
Status	**Status** allows modifying the current status of the WIPS service; start, stop, and restart.

Adding WIPS Configuration Profile

In the **WIPS Configuration Profile** screen, select **Add**. The **ADD - WIPS Configuration Profile** screen is displayed.

Figure 124: *Adding a WIPS configuration profile*



Provide the details for the following parameters. You can create multiple profiles.

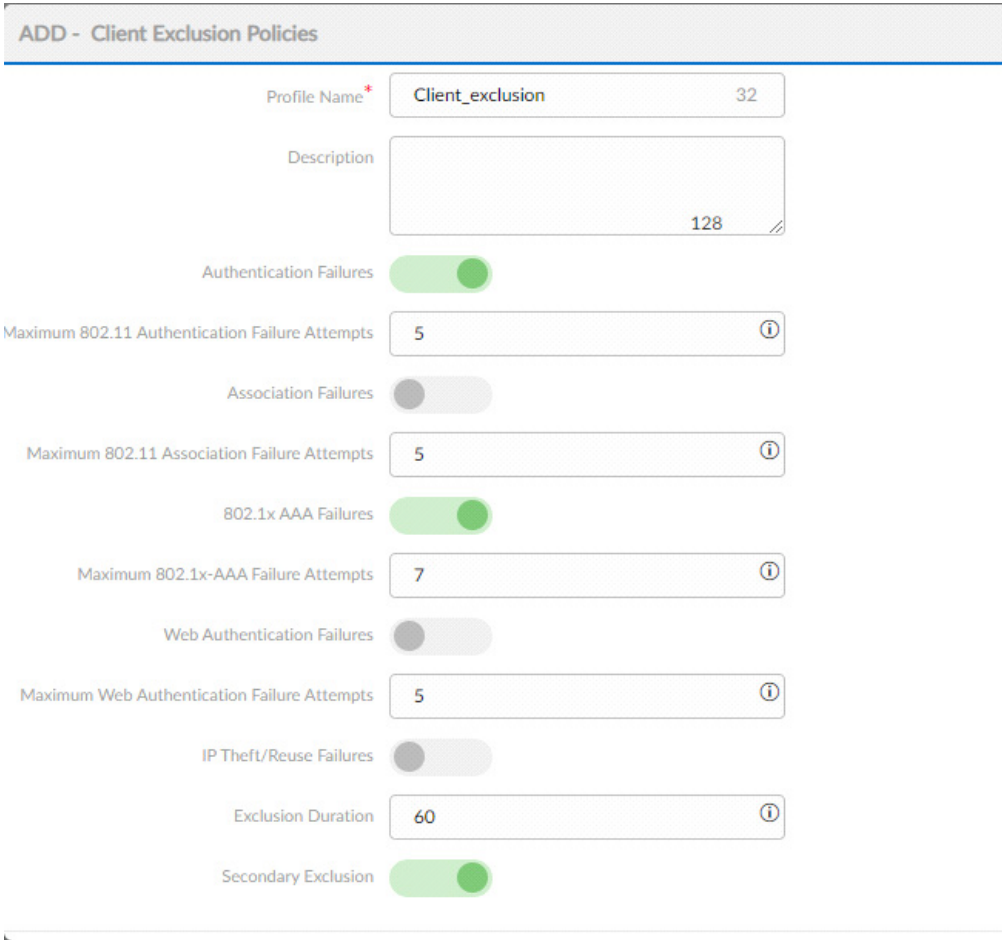
Field	Description
Name	Unique name for this WIPS Configuration Profile. The supported range is 1-32 alphanumeric characters.
WIPS Management	• **Description** – Enter a unique description for the WIPS configuration profile. The supported range is 128. • **Status** – To get started with intrusion detection, enable WIPS service by clicking **Start**. You can stop and restart the service as required. • **Clear Alerts** – Enable this option to clear all WIPS alert data generated previously.

Field	Description
Trusted APs	These are access points that are not monitored by the WIPS service, for example, access points that will always be present because your networks share the same airspace and you don't want to be constantly alerted that your neighbors have access points. To prevent this, create a list of trusted APs. Enter the **BSSID**.
Configurable Signatures	Signatures detect attacks on the wireless infrastructure by analyzing the wireless packets flowing in the network. Click the edit icon for a signature and modify the following values: • **Priority** – Severity of the signature. It can be set to one of the following: **Critical**, **Major** or **Minor**. • **Status** – Status of the signature. A signature status can be **Enabled** or **Disabled**. When a signature is disabled, no alerts are raised if an attack matches that particular signature. Note that by default, upon initial installation all predefined signatures are disabled. Users can enable the alerts desired and leave the remainder alone.

Click **Save**. The WIPS Configuration Profile is created.

Client Exclusion Policies

WIPS monitors clients based on specific parameters configured in the client exclusion policy; clients detected with a suspicious pattern based on the configured parameters in the policy are deemed malicious and blocked.



In the **Configuration** tab, enable the following monitoring events for clients, based on your requirement and configure the maximum number of failures wherever applicable. Occurrence of the configured maximum number of failures of a certain event within 60 seconds results in blocking that client from connecting to the network.

- Authentication Failures
- Association Failures
- 802.1x AAA Failures
- Web Authentication Failures
- IP Theft/Reuse Failures

The default value for the maximum number of failures for all configurable parameters is 5 and the valid range is 3 – 10. The client is blocked for the configured **Exclusion Duration;** default value is 60 seconds**.**

Enable **Secondary Exclusion** to monitor client activity after the **Exclusion Duration** is over. Client is monitored for 5 minutes and is blocked indefinitely if it is excluded more than 3 times for any of the failures; the client remains blocked until it is manually unblocked. When unblocked, the monitoring status of this client is deleted and the next failure is considered the first incidence.

Navigate to **Configure > Design-Features > Client Exclusion Policies**.

Custom Captive Portal

You can create custom Captive Portal login pages with your own logos and credentials. A maximum of four sets of custom Captive Portal login pages can be created; referred to as Captive Portal 1 through 4. Each set has 6 files, but you can only create customized pages for the main login page, the remaining HTML pages are the default.

Click on **Download Default File** to download the Fortinet default files and use the customizable login page as template, giving the altered HTML page a new name. Use unique names for all customized HTML pages for different captive portals. The custom captive portal screen lists the existing profiles with the configured parameters and the synchronization status of the profile.

The **Controller Sync Status** displays the total number of controllers to which the profile is pushed and number of controllers on which profile is successfully synchronized. Click on the **Controller Sync Status** to view the controller and synchronization details. The custom captive portal profile can be applied to multiple controllers; when applied it overrides any custom captive portal configuration on the controller.

Navigate to *Configure > Design-Features > Custom Captive Portal*.

The following actions can be performed on the **Custom Captive Portal** screen:

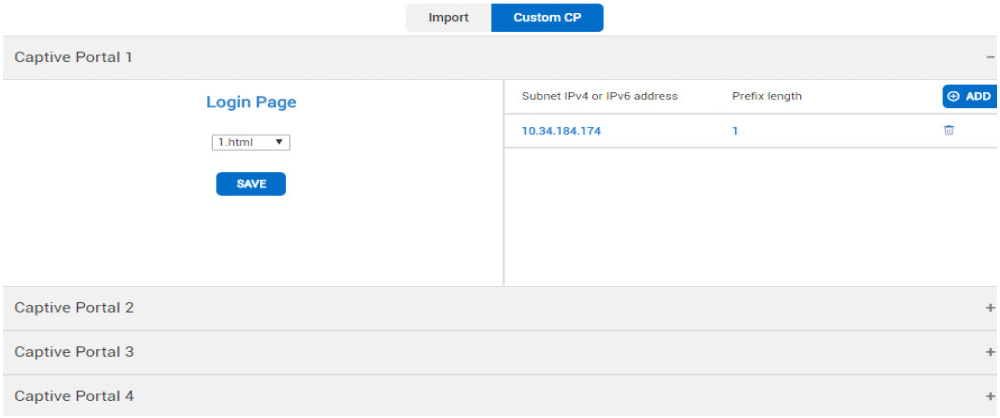
Name of the Action	Description
Add	**Add** allows to add a **Custom Captive Portal Profile**.
Apply	**Apply** allows to apply a **Custom Captive Portal Profile** to specific Controllers. Click on the apply icon and select the controllers to apply the profile to. The applied profile overrides any existing custom captive portal settings on the controller.

Name of the Action	Description
Delete	**Delete** allows deleting a **Custom Captive Portal Profile**. Select the **Delete** option, the **Custom Captive Portal Profile** gets deleted.
Edit	**Edit** allows editing a **Custom Captive Portal Profile**. Select the **Edit** option and modify the **Custom Captive Portal Profile** as required. The name of the profile cannot be modified.

Adding Custom Captive Portal Profile

In the **Custom Captive Portal** screen, select **Add**. The **Add Custom Captive Portal** screen is displayed.

Figure 125: *Add a custom captive portal profile*



Provide the details for the following parameters. You can create multiple profiles.

Field	Description
Name	Unique name for this Custom Captive Portal Profile. The supported range is 1-32 alphanumeric characters.
Import	Import the customized login page (default filename is *loginformWebAuth.html*). The supported file types are CSS, JavaScript, HTML, and graphics up to 50K each in the formats GIF, JPG, PNG, BMP. Import all new customized Captive Portal files one by one.

Field	Description
Custom CP	Select the imported customized **Login Page** for Captive Portal 1 and click **Save**. Provide at least one subnet location by clicking **Add**, enter the **Subnet IP address (IPv6/IPv4)** and the **Prefix length**. The valid range is 1-31 for an IPv4 address and 1-127 for an IPv6 address. Click the save icon. Users logging in from the added subnet will see Captive Portal 1. You can add multiple subnets. Configure Custom Captive Portals 2 ~ 4 similarly.

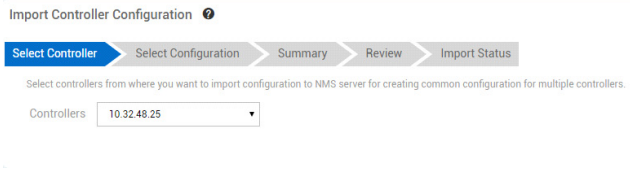
Importing Controller Configuration

The *Import Controller Configuration* in *FortiWLM* assists you to import controller configuration to nms-server for creating a common configuration across multiple controllers. A controller configuration with the available *ESS Profiles* are selected and imported, by performing the actions in the following sequential order:

1. Select *Configure* > *Import From Controller Configure* > *Import*. The *Import Controller Configuration* screen displays the following sequence of steps:

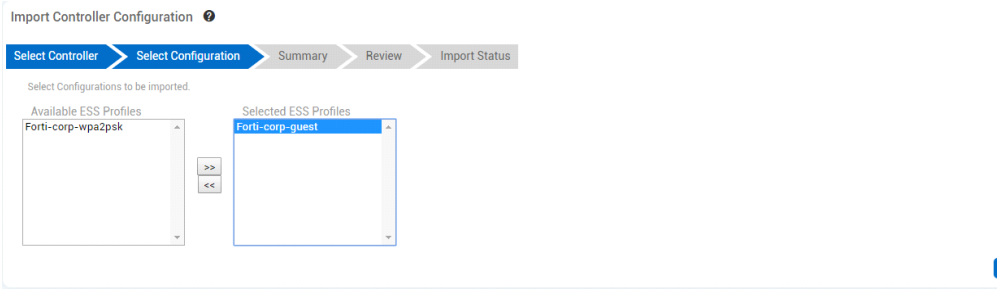
- ***Select Controller***: The *Select Controller* allows you to import configuration to NMS for creating common configuration for multiple controllers.
  - Select a *Controller* from the drop-down list. Click *Next* to navigate to the *Select Configuration* tab.

Figure 126: *Select Controller*



- ***Select Configuration***: The *Select Configuration* screen displays a list of available *ESS Profiles*.
  - Select the *ESS Profile* from the *Available ESS Profiles* list and click the *Forward* button. To select multiple options, click and drag across them. Ctrl+click to select or de-select items individually.

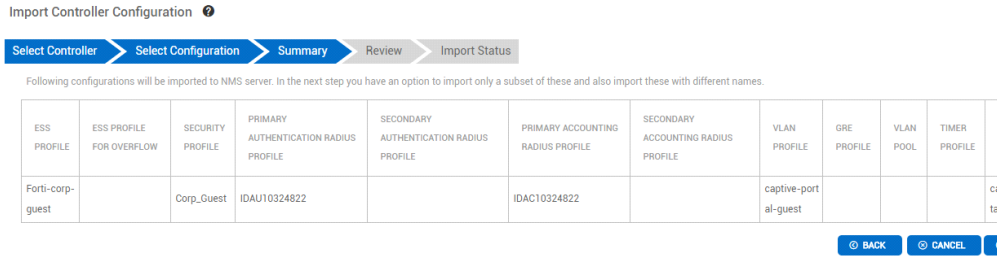
Figure 127: *Select Configuration*



- Click *Next* to navigate to the *Summary* tab.
- Select *Back* to navigate to the *Select Controller* screen.

- ***Summary***: The *Summary* screen displays a summary of selections performed in the *Select Controller* and *Select Configuration* screens.

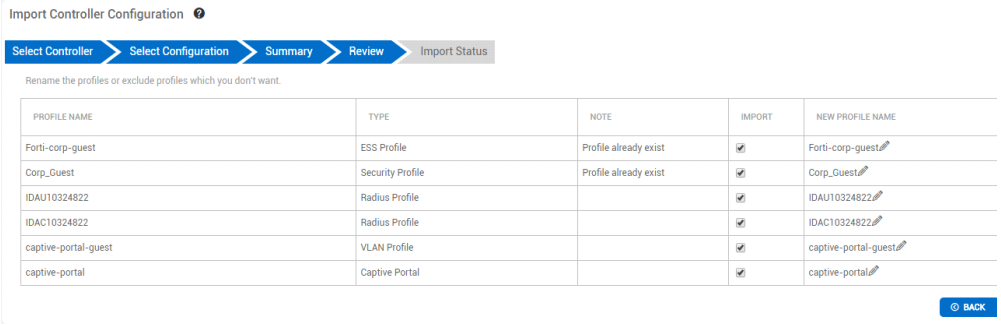
Figure 128: *Summary*



- Click *Next* to navigate to the *Review* tab.
- Select *Back* to navigate to the *Select Configuration* screen.

- ***Review***: The *Review* screen allows you to modify the summary of selections performed in the *Select Controller* and *Select Configuration* screens.

Figure 129: *Review*



- ***Import Status***:
  Click *Import*. The *Import Status* screen displays the status of the profiles that was selected to import.

Templates

FortiWLM allows you to create a common configuration for multiple controllers. A controller configuration comprising of multiple profiles (*ESS Profile, Security Profile, RADIUS Profile, and Tunnel (GRE/VLAN) Profile)* is created and downloaded to one or more managed *controllers* or *AP Groups*. These multiple profiles support a wide variety of connection requirements which enhances the wireless security.

ESS

A basic service set (BSS) is the basic building block of an IEEE 802.11 wireless LAN; one access point together with all associated clients is called a BSS. The BSSs can create coverage in small offices and homes, but they cannot provide network coverage to larger areas. 802.11 allows wireless networks of arbitrarily large size to be created by linking BSSs into an extended service set (ESS). An ESS is created by chaining BSSs together with a backbone network. An AP acquires its clients by broadcasting its name (SSID) which is picked up by clients within range. Clients can then respond, establishing a connection. It is legitimate for multiple access points to share the same SSID if they provide access to the same network as part of an Extended Service Set (ESS).

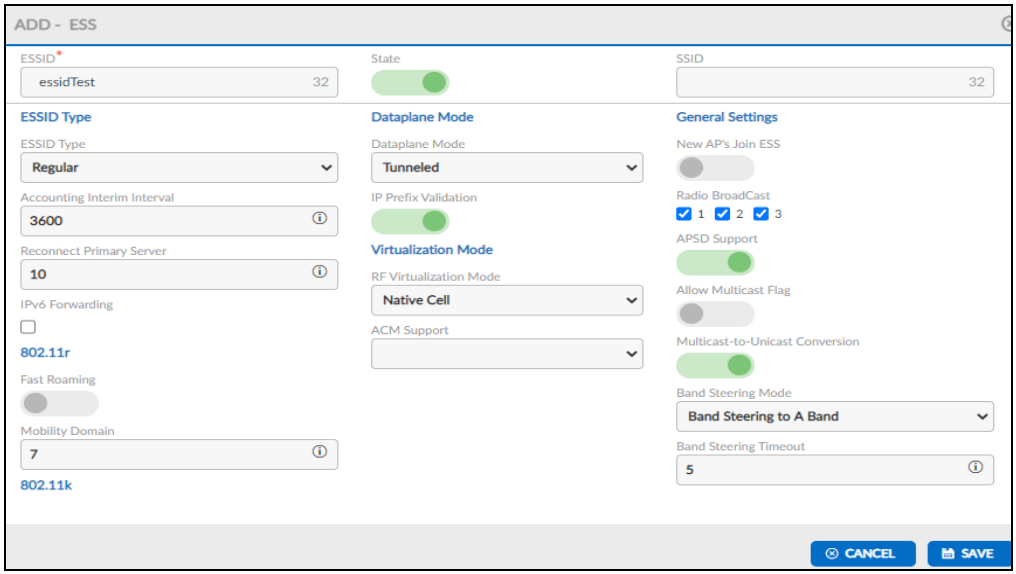
The ESS profiles can be configured either from FortiWLM or from the controller. To add an ESS from the *NM* web UI, follow these steps:

1. Navigate to *Configure* > *Design-Features* > *Wireless Service*. The *Service Profile* screen displays a list of Service profiles to which a Controller or an AP Group can be registered.
2. Choose a *Service Profile* and select *Edit.* The following tabs are displayed:
   - Service Profile
   - Registration
   - ESS Profile

- Security Profile

3. Select the *ESS Profile* tab, the *Service Profile - ESS Profile* screen is displayed.

Figure 130: *Service Profile - ESS Profile*



4. In the *Enable/Disable* drop-down list, select one of the following:
   - *Enable*: ESS Profile created is enabled.
   - *Disable*: ESS Profile created is Disabled.
5. In the *Accounting Interim Interval* field, type the time (in seconds) that elapses between accounting information updates for RADIUS authentication. If a RADIUS accounting server is enabled, the controller sends an interim accounting record to the RADIUS server at the interval specified. Accounting records are only sent to the RADIUS server for clients that authenticate using 802.1x. The interval can be from 600 through 36,000 seconds (10 minutes through 10 hours). The default value is 3,600 seconds (1 hour). You can disable the Accounting Interim Interval by configuring a value of 0.
6. Beacon Interval sets the rate at which beacons are transmitted. Setting the beacon interval to a higher value decreases the frequency of unicasts and broadcasts sent by the access point. If the power-save feature is enabled on clients that are connected to access points, clients “wake up” less if fewer unicasts and broadcasts are sent, which conserves the battery life for the clients. In the Beacon Interval field, type the interval (in ms) at which beacons are transmitted. The beacon interval must be between 20 through 1000 milliseconds. For AP300/AP400 and AP1000, beacon interval is a multiple of 20, from 20 to 1000ms. If your WLAN consists mostly of Wi-Fi phones, and you have a low number of ESSIDs configured (for example, one or two), Fortinet recommends setting the beacon interval to 100.
   Note: The beacon interval cannot be configured for FAP-U models.

7. In the SSID Broadcast drop-down list, select one of the following:
   - *On*: SSID is included in the beacons transmitted.
   - *Off*: SSID is not included in the beacons transmitted. Also Probe Responses will are not sent in response to Probe Requests that do not specify an SSID.
   - *2.4GHz only*: SSID is included in the 2.4GHz beacons transmitted.
   - *5GHz only*: SSID is included in the 5GHz beacons transmitted.
8. In the Bridging area, verify any of these bridging options:
   - *AirFortress*: FortressTech Layer 2 bridging and encryption with Fortress Technology AirFortress gateway.
   - *IPv6*: Configures bridging Internet version 6 addresses. IPv6 via tunneling mode has these limitations:
     - No dynamic VLAN
     - No multiple ESSID mapping to same VLAN
     - No support for IPv6 filtering
     - No IPv6 IGMP snooping
   - *AppleTalk*: configures bridging to AppleTalk networks on this ESS.
9. By default, access points that join the ESS profile and have the same channel form a Virtual Cell. In the *New APs Join ESS* profile drop-down list, select one of the following:
   - *On*: (default) Access points automatically join an ESS profile and are configured with its parameters.
   - *Off*: Prevents access points from automatically joining an ESS profile. The user is now allowed to add multiple interfaces on the ESS Profile screen.
10. **Radio Broadcast** - Select the radio interface index for deployment/broadcast. This option is available only when **New AP's Join ESS** is disabled. By default, all three interfaces are enabled; you can choose to enable any of these interfaces.
11. In the *Allow Multicast Flag* drop-down list, optionally enable multicasting (on). Only enable multicasting if you need to use a multicast application. Enabling multicasting causes all multicast packets on the air side to appear on the wired side, and all multicast packets on the wired side to appear on the air side.
    Multicasting is a technique frequently used for the delivery of streaming media, such as video, to a group of destinations simultaneously. Instead of sending a copy of the stream to each client, clients share one copy of the information, reducing the load on the network. Multicasting is an advanced feature and can cause subtle changes in your network. By default, multicasting is disabled and should be enabled only for specific circumstances.
    - On: Enables multicasting. Enable multicasting only if you need to use a multicast application. Enabling multicasting causes all multicast packets on the air side to appear on the wired side, and all multicast packets on the wired side to appear on the air side.

- Off: Disables multicasting.

Multicasting is allowed only when an ESS profile has a one-to-one mapping with the default VLAN for this ESS profile; no other ESS profile uses the same VLAN; and security rules associated with this ESS profile do not redirect traffic to another VLAN. Multicasting is an advanced feature. Enabling multicasting in the Fortinet WLAN System can cause subtle changes in your network. Contact Fortinet Technical Support before enabling multicasting.

12. In the *Isolate Wireless to Wireless Traffic* drop-down list, optionally enable the Isolate wireless to wireless traffic (on). This is enabled to prevent two wireless stations operating on the same L2 domain from communicating directly with each other. This is not a common requirement, but can be necessary for some security policies. Set the option to On if your network requires this. This option is supported in both the tunnel and bridge mode.
13. In the *Silent Client Polling* drop-down list, optionally enable the silent client polling (on).
    - *On*: Enables tracking information to be sent between the Controller and the APs and between the AP and a phone that is not in a call or during power save. This feature keeps the system appraised of a client phone location if the client moves between APs while the phone is inactive.
    - *Off*: Disables silent client polling.
14. In the *Multiple IP per Station* drop-down list, optionally enable the multiple IP per station (on).
15. In the Multicast-to-Unicast Conversion optionally enable the conversion (on) select one of the following:
    - On: Enables multicast-to-unicast conversion. Enabling this conversion allows multicast packets to be converted to unicast packets and deliver it all the clients.
    - Off: Disables multicast-to-unicast conversion. The multicast packets will be delivered as multicast packets to the clients.
16. In the *RF Virtualization Mode* drop-down list select the user to specify the type of virtualization used by the specified ESS profile. The option for selections are as follows:
    - Virtual Cell:
    - Virtual Port: This option is not supported on Wave 1 and Wave 2 APs.
    - Native Cell: This option disables virtualization on the ESS and is the default setting for all APs.
17. *802.11r*: Enable 802.11r and specify to allow fast roaming for 802.11r clients between the available access points. Fast roaming does not support inter-controller roaming.
18. *802.11k*: Enable 802.11k to calculate 802.11k neighbor and radio measurement reports.
19. *802.11v*: Enable 802.11v standards for wireless networks, which provide several enhancements for network management such as network assisted roaming and power saving. Network assisted roaming allows the wireless network to send requests to associated clients, recommending better APs to associate with while roaming. This is beneficial for both load balancing and in guiding clients with poor connectivity.
    Network assisted power saving allows configuring an idle period for devices ensures that

they remain connected to APs without receiving any frames from them. This helps in reduced power consumption and improved battery life. The following fields are defined by the 802.11v standard.
Note: 802.11k and ARRP must be enabled to use 802.11v capabilities.

- Enable **BSS Transition Management** to allow the roaming client to initiate a BSS transition query to the associated AP for a candidate list of other APs it can re-associate with, the associated AP responds with a BSS transition request containing the requested AP list. The AP can also send an unsolicited BSS transition request to the client. The client can accept the request and re-associate with the suggested APs or it can reject the request and continue its association with the current AP.
- Enable the **Max Idle Service** to configure the amount of time that an AP keeps a connected client associated without receiving any frames from it, that is, this value configures the maximum time a client remains idle without transmitting any frames to the AP. When the idle period is configured, the clients are not required to send repeated keep-alive messages to the AP and remain in the sleep mode for a longer duration, thereby saving battery power. After this period the AP disassociates with the client.
- Specify the **Client Idle Timeout** duration for the enabled Max Idle Period. The valid range is 60 - 3600 seconds and the default is 400 seconds.
- Enable the **Direct Multicast Service** to allow the AP to transmit the requested multicast traffic as unicast frames. This enables the client to receive the multicast packets ignored while in the sleep mode. Also, the client receives the packets faster by enabling the radio for a shorter duration as the unicast frames are transmitted at a greater wireless link rate. This saves battery power.

20. *ACM Support:* This is available in *Native Cell* and *Virtual Cell* mode. Enable this option to support Ascom and Spectralink certificate complaint phones.
The *ACM Voice* and *ACM Video* determine the bandwidth that is allocated to the voice calls. Of the maximum calls configured per radio, 70% of the bandwidth is allocated to the voice and video mediums. The control messages before the initiation of the call uses the video medium and once the call is established the voice medium is used.

21. In the *WMM Support* drop-down list, select one of the following:

- *On*: Enables Wifi Multimedia (WMM) Enhanced Distribution Channel Access (EDCA) for QoS priority scheduling and Automatic Power Save Delivery (APSD) for improvements over the 802.11 legacy power management. WMM is on by default.
- *Off*: Disables WMM.

22. In the *APSD Support* drop-down list (*Advanced WMM Power Save*), select one of the following:

- *On*: Data packets for power save mode clients are buffered and delivered based on the trigger provided by the client. This feature saves more power and provides longer lifetime for batteries than the legacy power save mode (TIM method).
- *Off*: No U-APSD support

23. In the *DTIM Period* text box, type the number of beacon intervals that elapse before broadcast frames stored in buffers are sent. This value is transmitted in the DTIM period

field of beacon frames. The DTIM period can be a value from 1 through 255. The default DTIM period is 1. Setting the DTIM period to a higher value decreases the frequency of broadcasts sent by the access point. If power save is enabled on clients that are connected to access points, clients "wake up" less if fewer broadcasts are sent, which conserves battery life for the clients. Only the behavior of clients currently in power-save mode is affected by the DTIM period value. Because broadcasts are generally wasteful of air resources, the Fortinet WLAN has devised some mechanisms that mitigate broadcasts either with proxy services or with more efficient, limited unicasts. As an example, ARP Layer 2 broadcasts received by the wired side are not relayed to all wireless clients. Instead, the Forti WLC maintains a list of IP-MAC address mappings for all wireless clients and replies with proxy-ARP on behalf of the client.

24. In the *Dataplane Mode* drop-down list, select the type of AP/Controller configuration:

- *Tunneled*: The default connection between controllers and APs, where data and control packets are passed.
- *Bridged*: (formerly Remote AP mode) Bridged mode ESS profiles are supported by AP300s. In bridged mode, data packets are not passed to the controller; only control plane packets are passed to the controller. This setting determines the type of traffic that is passed between the controller and an AP. By default, tunneled mode is active where a controller and an AP are connected with a data tunnel so that data from a mobile station is tunneled to the controller from the AP and vise versa. When bridged mode is configured, an AP can be installed and managed at a location separated from the controller by a WAN or ISP, for example a satellite office. The controller monitors the remote APs through a keep-alive signal. Remote APs can exchange control information, including authentication and accounting information, with the controller but are unable to exchange data. Remote APs can exchange data with other APs within their subnet. Because remote APs cannot exchange dataplane traffic (including DHCP) with the controller, these System Director features are not available for Remote AP configuration: Virtual Cell, VLAN, Captive Portal, L3 Mobility, and QoS. A VLAN tag can be configured for a Bridged mode profile (see below) and then multiple profiles can be associated to that VLAN tag.

25. The *AP VLAN Policy* is selected for the *Bridged dataplane* mode. The following are the types of AP VLAN Policy that can be selected from the drop-down list.

- No VLAN
- Static VLAN
- RADIUS VLAN Only
- RADIUS and Static VLAN

26. The AP VLAN Tag can be selected only if the *AP VLAN Policy* is selected as *Static VLAN* or *RADIUS and Static VLAN.* This VLAN tag value is configured in the controller's VLAN profile and is used for tagging client traffic (for the ESSIDs with dataplane mode bridged) using 802.1q VLAN. AP VLAN Tag is a number between zero and 4094. This is a mandatory field.

27. In the *Enable APVLAN priority* drop-down list optionally set the Enable APVLAN priority on or off.

- *On*: AP disregards the DSCP value in the IP header of a packet.
- *Off*: AP honors the DSCP values in the IP header of a packet. AP converts the DSCP value in the IP header to appropriate WMM queues. This feature works only for downstream packets and only for ESSID with dataplane mode as bridged.

28. The Band steering mode balances multi-band capable clients by assigning bands to clients based on their capabilities. In the Band steering mode drop-down list optionally set the following Band Steering Mode options:

- *Band Steering to A band*: Infrastructure attempts to steer all A-Capable wireless clients to the 5 GHz band when they connect to this ESS.
- *Band Steering to N band*: Infrastructure attempts to steer all N-Capable wireless client that are also A-Capable to the 5GHz band when they connect to this ESS. Infrastructure also attempts to steer non N-Capable wireless clients to the 2.4 GHz band.
- Band Steering Disabled

29. In the *Band Steering Timeout* text box, optionally provide the number between 1-65535. *Band Steering Timeout* is the number of seconds that assignment for a steered client is blocked on the forbidden band while it is unassociated.

30. In the *Expedited Forward Override* drop-down list, optionally enable override (on). The *Expedited Forward Override* option is implemented to Override the DSCP value of Expedited Forwarding to Class Selector CS6 in the IP-Header of the Voice Packet sent by WLAN Phones. This feature is specific to AP300 and is disabled by Default.

- The SSID Broadcast Preference is specific to address the CISCO phone connectivity issues. It consists of three options as follows:
- *Disable*: Configuring the parameter to "Disable" makes the AP not to advertise the SSID string in the beacon.
- *Always*: Configuring the parameter to "Always" enables the AP to advertise the SSID on the beacons always. This must not be configured unless recommended.
- *Till-Association*: This is the default option. Configuring the parameter to "Till Association" enables the AP to advertise the SSID in the beacons till the association stage of the client and disable the SSID broadcast in the later part of connectivity. This parameter is preferable to configure for certain versions of phones which resolve connectivity issues in the Virtual Port mode. Once the station is associated, AP433 stop broadcasting SSID string and the users are allowed to configure SSID broadcast, per ESS, from the FortiWLC GUI or CLI.

31. In the *Enable Countermeasure* list, select whether to enable or disable MIC Countermeasures:

- *On*: (The default) Countermeasures are helpful if an AP encounters two consecutive MIC errors from the same client within a 60 second period. The AP will disassociate all clients from the ESSID where the errors originated and does not allow any clients to connect for 60 seconds. This prevents an MIC attack.
- *Off*: Countermeasures should only be turned off temporarily with this option while the network administrator identifies and then resolves the source of a MIC error.

32. Multicast MAC Transparency feature enables MAC transparency for tunneled multicast, which is needed for some clients to receive multicast packets. Multicasting is an advanced feature and can cause subtle changes in your network. By default, multicasting is disabled. Optionally enable *Multicast MAC*:
    - *On*: All downstream multicast packets will have the MAC address of the streaming station.
    - *Off*: Default - all downstream multicast packets will have the MAC address of the controller.
33. In the *Supported and Base Transmit Rates* for each of the modes, enable or disable rates as needed.
34. To provide faster connection to a phone moving in and out of a coverage area, select the specific **Voice Client Type**.
    - *Spectralink*: This phone type is used only for certification. It changes the minimum and maximum contention window parameters on an ESSID basis for supporting the calls along with FTP data.
    - *Ascom*: The clients probing to ESSID with Ascom, get a probe response when the station is assigned to the radio.
    - *None*: The clients probing to ESSID with None, get a probe response whether the client is assigned to the radio or not.
35. The MCS index values determine the likely data rate of your WiFi connection using 11ax access points ONLY. Up to 4 spatial streams are allowed in the 2G and 5G bands. Configure the supported and base MCS index values in **AX 2G High Efficiency Settings/AX 5G High Efficiency Settings**.
    Setting the base rate specifies the mandatory rates that all connecting clients must support when connecting to the access point.
    Setting the supported rate specifies the rates at which clients can connect to an access point to transmit data provided the clients and the access points support the rate.
    If **None** is specified for all streams then 11ax capable clients connect as 11ac clients.

See the ***FortiWLC Configuration Guide***, for detailed information on *ESS Profiles*.

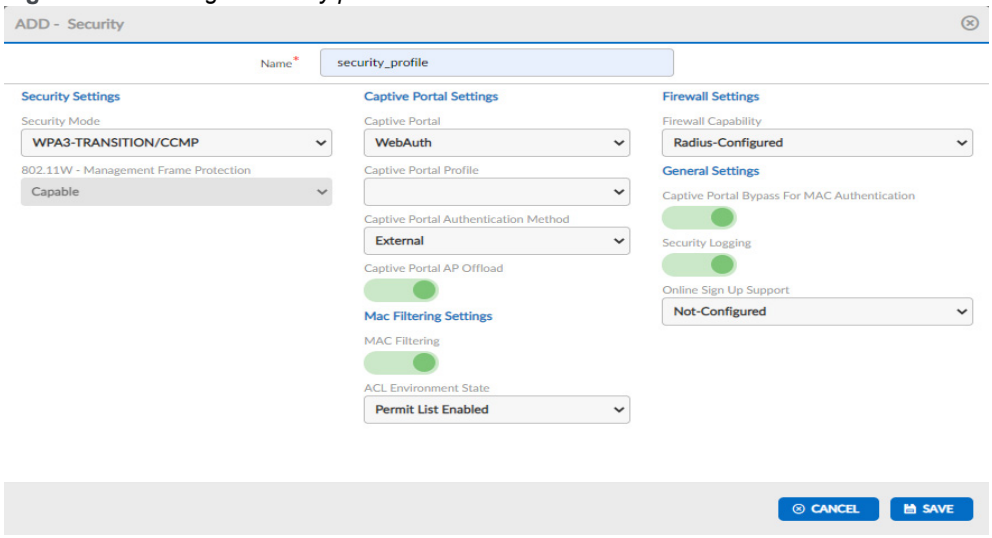
Security

As the networks of the world have united into a single, globe-spanning behemoth, security has taken on new importance. Wireless LANs were once the bane of security-conscious networking organizations, but newer tools make it easier to build networks with significant security protections. In addition to traditional security issues such as traffic separation between user groups and maintaining appropriate access privileges, wireless networks present new challenges, like rogue access points and unauthorized clients.

The Security profiles can be configured either from FortiWLM or from the controller. The security options is enforced by creating security profiles that are assigned to a service profile. As such, they can be tailored to the services and the structure (virtual LAN, Virtual Cell, etc.)

offered by the ESSID and propagated to the associated APs. You can tell where a profile was configured by checking the read-only field *Owner* (*Configure* > *Design-Features* > *Wireless Service* > *ESS*); the *Owner* is either *nms-server* or *controller*. Each service profile must be associated with ESS and security profiles.

Figure 131: *Adding a Security profile*



To add a security from the web UI, follow these steps:

1. Navigate to *Configure* > *Design-Features* > *Wireless Service*. The *Service Profile* screen displays a list of Service profiles to which a Controller or an AP Group can be registered.
2. Choose a *Service Profile* and select *Edit.* The following tabs are displayed:
   - Service Profile
   - Registration
   - ESS Profile
   - Security Profile
3. Select the *Security Profile* tab, the *Service Profile - Security Profile* screen provides a list of parameters that define how security is handled within a service profile. With security profiles, you can define the Layer 2 security method, including the cipher suite, static WEP key entries and key index position, and other parameters. The various security profiles you create allow you to support multiple authentication and encryption methods within the same *NM* infrastructure.
4. Individual *Security Profiles* can also be created by clicking *Configure* > *Templates* > *Security* > *Add*. The *Security Profile - Add* screen allows you to create a new security profile and complete the profile by providing data in all fields. This security profile will not be linked to any configuration yet, but will be available to one or all configurations that you

create in the future. The Security that you create this way will appear in the drop-down box labeled Security for all configurations.

5. In the *L2 Modes Allowed* area, select one of the following *Layer 2* security modes:
   - *Clear*: The WLAN does not require authentication or encryption, and the WLAN does not secure client traffic. This is the default setting.
   - *802.1x*: Can provide 802.1X authentication and WEP64 or WEP128 encryption.
   - *Static WEP keys*: Requires that stations use a WEP key.
   - *WPA*: Requires 802.1X Radius server authentication with one of the EAP types. Radius profiles are configured in the Service Profile.
   - *WPA-PSK*: Uses the TKIP encryption and requires a Pre-shared key.
   - *WPA2*: Requires 802.1x Radius server authentication with one of the EAP types. Radius profiles are configured in the Service Profile.
   - *WPA2-PSK*: Uses the CCMP-AES encryption and requires a Pre-shared key.
   - *WPA3-SAE/CCMP-AES*: Uses the Simultaneous Authentication of Equals (SAE) encryption method and requires a pre-shared key.
   - *WPA2-WPA3/CCMP-AES*: Uses the CCMP-AES and SAE encryption methods and requires a pre-shared key.
   - *WPA3/CCMP*: Security profile using CCMP encryption method.
   - *WPA3-Transition/CCMP*: Security profile with mixed mode of authentication (WPA2&WPA3) using CCMP encryption method.
   - *MIXED*: Allows both WPA and WPA2 clients using a single security profile.
   - *MIXED PSK*: Allows pre-shared key clients to use a single security profile.
   - *WAI*: Security profile using WAPI certificate mode.
   - *WAI PSK*: Security profile using WAI with a pre-shared key. This key can be in either alphanumeric or hex format, and must be between 8 to 64 characters.

Security profiles with L2 Mode 802.1x/WPA/?WPA2/MIXED only requires Radius profile. The Radius profile specified in the service profile will be synced to the controller only if the security profile comprises of 802.1x/WPA/?WPA2/MIXED L2 Modes.

Note: WPA3 support is available only with FortiWLC 8.5.1 and above.

6. In the *Data Encrypt* area, select one of the following (available choices are determined by the L2 Mode selected in the previous step):
   - *WEP64*: A 64-bit WEP key is used to encrypt packets.
   - *WEP128*: A 128-bit WEP key is used to encrypt packets.
   - *TKIP*: Encryption algorithm used with
   - *CCMP-AES*: A 128-bit block key is used to encrypt packets with WPA2.

- *CCMP/TKIP*: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol replaces both TKIP, the mandatory protocol in WPA, and WEP, the earlier, non-secure protocol.
- *WPI-SMS4*: The encryption algorithm used for encrypting and decrypting messages in WAI-enabled profiles.
  If you select *WEP64* or *WEP128*, you need to specify a WEP key in the next step. If you specify *TKIP* for *WPA-PSK* or *CCMP-AES* for *WPA2-PSK*, set a pre-shared key.

7. In the *WEP Key* text box, specify a WEP key. If you selected *Static WEP Keys* option, you need to specify a WEP key in hexadecimal or text string format. A WEP64 key must be 5 octets long, which you can specify as 10 hexadecimal digits (the hexadecimal string must be preceded with 0x) or 5 printable alphanumeric characters (the! character cannot be used). For example, 0x619B947A3D is a valid hexadecimal value, and wpass is a valid alphanumeric string. A WEP128 key must be 13 octets long, which you can specify as 26 hexadecimal digits (the hexadecimal string must be preceded with 0x) or 13 printable alphanumeric characters (the ! character cannot be used). For example, 0xB58CE2C2C75D73B298A36CDA6A is a valid hexadecimal value, and mypass8Word71 is a valid alphanumeric string.
8. In the *Static WEP Key Index* text box, type the index number to be used with the WEP key for encryption and decryption. A station can have up to four static WEP keys configured. The static WEP key index must be an integer between 1 through 4 (although internal mapping is performed to handle wireless clients that use 0 through 3 assignments).
9. In the *Re-Key Period* text box, type the duration that the key is valid. Specify a value from 0 to 65,535 seconds. The default re-key value is zero (0). Specifying 0 indicates that re-keying is disabled, which means that the key is valid for the entire session, regardless of the duration.
10. In the *BKSA Caching Period* text box, enter the desired period for which the BKSA value will be cached (in seconds). Note that this field is only used in WAPI configurations, and will otherwise be disabled. Specify a value from 0 to 65,535 seconds. The default caching period value is 43200.
11. In the *Captive Portal* drop-down list, select one of the following:
    - *Disabled*: Disables the Captive Portal.
    - *WebAuth*: Enables a WebAuth Captive Portal for users to log into. This feature can be set for all L2 Mode selections.
12. Captive portal profiles allows you to create individual captive portal profiles with distinct configuration settings. Such captive portal profiles can be mapped to security profiles for fine control over captive portal user access. A captive portal profile is created from the *Configure* > *Templates* > *Captive Portal* page.

NOTE: Captive Portal profile can be enabled only if at least one Captive Profile is created.

13. If you want to use a third-party Captive Portal solution from a company such as Bradford, Avenda, or CloudPath change the value for *Captive Portal Authentication Method* to *external*.

14. Enabling *Captive Portal AP Offload* allows URL redirection to be offloaded to the APs, thereby, reducing the load on the controller and allowing more concurrent captive portal authentication requests to be handled. This option is disabled by default.
15. If 802.1x is to be used, in the *802.1X Network Initiation* drop-down list, select one of the following:
    - *On*: The controller initiates 802.1X authentication by sending an EAP-REQUEST packet to the client. By default, this feature is enabled.
    - *Off*: The client sends an EAP-START packet to the controller to initiate 802.1X authentication. If you select this option, the controller cannot initiate 802.1X authentication.
16. If the *Static WEP Key* mode to be used, in the *Shared Key Authentication* list, select one of the following:
    - *On*: Allows 802.1x shared key authentication.
    - *Off*: Uses Open authentication. By default, this feature is off.
17. IIn the *Psk Profile Name* drop-down, select the secured PSK profile to be mapped to the Security profile. In the *Pre-shared Key* text box, enter the key if WPA2-PSK or WPA3 was selected as the security mode. The key can be from 8 to 63 ASCII characters or 64 hex characters (hex keys must use the prefix "0x" or the key will not work).
18. In the *Group Keying Interval* text box, enter the time in seconds for the interval before a new group key is distributed.
19. In the PMK Caching list, select one of the following:
    - On: PMK caching is allowed.
    - Off: PMK caching is not allowed.
20. **Session Timeout(min)**: Configures the timeout for 802.1x active session. The default is 480 minutes and the valid range is 0-1440 minutes.
    Note: The session timeout value obtained from the RADIUS server takes precedence.
21. **Idle Timeout(min)**: Configures the timeout for 802.1x idle session. The default is 60 minutes and the valid range is 0-1440 minutes. After the timeout, client requests for re-authentication.
    Note: You can configure 802.1x session and idle timeout between the access point and wireless clients only for RADIUS/Enterprise security modes.
22. **EAP Timeout(second)**: Configures the EAP authentication timeout between the access point and the wireless clients. The default is 5 seconds and the valid range is 1-30 seconds.
23. **EAP Retries**: The maximum number of retries before EAP timeout. The default is 3 retries and the valid range is 1-3 retries. After the timeout, authentication fails and the client tries to reconnect as per the configured EAP retries.
    Note: You can configure EAP timeout and retries between the access point and wireless clients only for RADIUS/Enterprise security modes.
24. In the *Key Rotation* drop-down list, select whether to enable or disable this feature.
25. Indicate the *Backend Auth Server timeout* from zero milliseconds to 65535 milliseconds (about 1 minute, 5 seconds)

26. In the *Reauthentication* drop-down list, select one of the following:
    - *On*: Controller honors and enforces the "Session-timeout" Radius attribute that may be present in a Radius Access-Accept packet. Use this option if the Session-timeout attribute is used to require stations to re-authenticate to the network (802.1X) at a specified period. If "Session-timeout" is not used, there is no reason to enable re-authentication.
    - *Off*: Disables re-authentication for this security profile.
27. In the *MAC Filtering* drop-down list, select one of the following:
    - *On*: Enables MAC Filtering for this security profile.
    - *Off*: Disables MAC Filtering for this security profile.

    Enabling Per ESS MAC Filtering
    - In the *Configure* > *Design-Features* > *Wireless Service* page, specify the Primary Authentication RADIUS and the Primary MAC AUTH RADIUS and click the Save button. This will create the RADIUS profile tabs
    - In the RADIUS profile tab, configure Primary authentication and Mac Filtering Primary.
    - In the Security profile, ensure that the MAC Filtering is ON.

Configure Primary authentication before configuring Mac Filtering Primary parameters.

28. In the ACL Environment State, select one of the following:
    - Disabled: The local ACL list is not used for MAC filtering.
    - Permit List Enabled: Only the MAC address in this list is allowed.
    - Deny List Enabled: Only the MAC address in this list is blocked.
29. In the *Firewall Capability* drop-down list, select one of the following:
    - *Configured*: The controller defines the policy through configuration of the Firewall Filter-ID.
    - *Radius-configured*: The Radius server provides the policy after successful 802.1X authentication of the user. This option requires the Radius server have the filter-id configured. If this is not configured, the firewall capability is not guaranteed.
    - *None*: Disables the Firewall Capability for this security profile.
30. In the *Firewall Filter ID* text box, enter the firewall filter-id that is used for this security profile. The filter-id is an alphanumeric value that defines the firewall policy to be used on the controller, when the firewall capability is set to configured. For example, 1.
31. In the *Security Logging* drop-down list, select one of the following:
    - On: Enables logging of security-related messages for this security profile.
    - Off: Disables logging of security-related messages for this security profile.

32. In the *Passthrough Firewall Filter ID* text box, enter a firewall filter ID. The filter ID is an alphanumeric value that defines the firewall policy to be used on the controller for a Captive Portal-enabled client that has no authentication.
33. Configure *802.11W - Management Frame Protection*.
    - *Required* allows only those devices to associate with the SSID that support 802.11w and prevents devices that do not support 802.11w from associating.
    - *Capable* allows devices that do not support 802.11w along with those that support 802.11w to associate with the SSID and use the 802.11w features.
    - *Disable* disables the usage of 802.11w management protection frames.
34. *Tunnel Termination* allows you to perform configuration on per-security profile basis. Select one of the following in the *Tunnel Termination* drop-down list.
    - *PEAP*: PEAP (Protected Extensible Authentication Protocol) is a version of EAP, the authentication protocol used in wireless networks and Point-to-Point connections. It is designed to provide more secure authentication for 802.11 WLANs (wireless local area networks) that support 802.1X port access control. It authenticates the server with a public key certificate and carries the authentication in a secure Transport Layer Security (TLS)
    - *TTLS*: TTLS (Tunneled Transport Layer Security) is a proposed wireless security protocol.

When Tunnel Termination is enabled, Fortinet's default certificate is used. In this case, the certificate must be "trusted" on the wireless client end in order for authentication to be successful. Refer to Security Certificates for details on how to import a certificate.

When PEAP/TTLS is configured on the RADIUS server, PEAP/TTLS termination should be disabled.

See the ***Configuring Security*** chapter of the ***FortiWLC Configuration Guide***, for detailed information on *Security Profiles*.

Multiple PSK

The multiple Pre-shared key (PSK) is a shared secret method added to the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) encryption methods for WPA/WPA2 authentication. The secured PSK feature allows generation of unique pre-shared encryption keys for each wireless user (the valid range for the number of clients is 0-10. A value of 0 means that a single PSK can be used by any number of clients). The clients are authenticated and allowed access to the network based on the verification of these keys.

Multiple keys can be generated, distributed, and managed across different clients. A maximum of 256 secured PSK profiles can be created per controller with a maximum of 16k keys. These keys can be generated for one profile or be distributed across profiles. Only one PSK profile is associated with one ESS profile.

Each PSK profile is created based on the key generation method, whether manual or automatic. Once the authentication key is generated, e mails can be triggered to send the PSK information to the user. Note that e mails can be triggered successfully only when SMTP is configured. These keys are valid till their configured timeout period. You can create multiple VLAN groups, multiple groups can be assigned to each PSK profile.

VLAN support is available for multiple PSK in both bridge (except FAP-U43xF) and tunnel modes.

Note: Multiple PSK is supported on FortiWLC 8.5 and above.

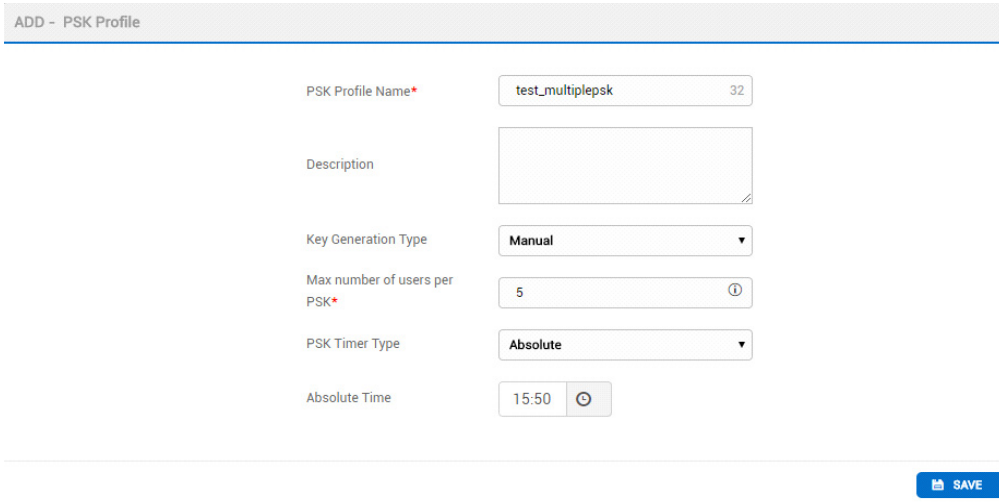
Configure the PSK profile in the **Security** profile to link it to the ESS profile. FortiWLC-1000D and 3000D support 256 security profiles; all other controller models support 64 security profiles.

Navigate to *Configure* > *Templates* > *Multiple PSK*, the following details about the multiple PSK profiles are displayed.

Field	Description
Hostname	Displays the controller's Hostname or IP Address. Select the hyper link of the controller's IP address. The selected controller's IP address gets included to the controllers tree.
Psk Profile Name	A unique name for the secured PSK profile.
Description	The description associated with the secured PSK profile.
Key Generation Type	The method of key generation, whether **Manual** or **Automatic**.
Max Number of Users per psk	Maximum number of clients per PSK. A value of 0 means that a single PSK can be used by any number of users.
PSK Timer Type	The timer for the expiry of a PSK profile. The timer can be None, Absolute, or Periodic. None indicates an infinite time period for the PSK profile.
Service Start Time/ Service End Time	The start and end time for the PSK profile validity.
Absolute Time	The expiry time for the PSK profile.

Adding a Multiple PSK Profile

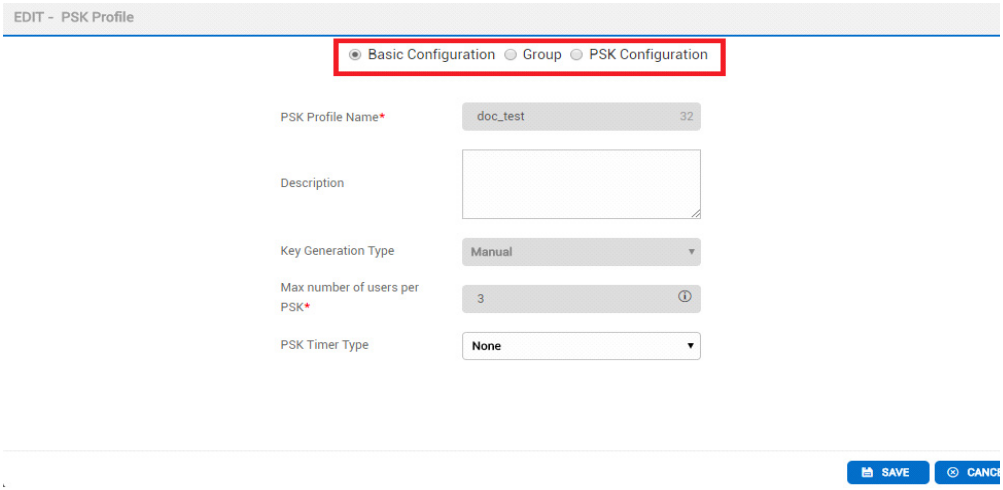
Click **Add** to create a PSK profile and provide the following configuration details and click **Save.**



Parameter	Description
Psk Profile Name	A unique name for the PSK profile. Valid range is 1-32 characters.
Description	The description associated with the PSK profile.
Key Generation Type	The method of key generation, whether **Manual** or **Automatic**.
Max Number of Users per psk	Maximum number of clients per PSK. Valid range is 0-10 clients and the default is 1. A value of 0 means that a single PSK can be used by any number of users.
PSK Timer Type	The timer for the expiry of a PSK profile. The timer can be **None**, **Absolute**, or **Periodic**. An absolute timer sets a single expiry time and starts immediately after the PSK profile creation. A periodic timer sets a start and end time for the PSK profile. The PSK profile is valid only till the timeout. None indicates an infinite time period for the PSK profile.
Service Start Time/ Service End Time	The start and end time for the PSK profile validity.
Absolute Time	The expiry time for the PSK profile.
Periodic Time	The time period for the PSK profile.
Psk Profile Name	A unique name for the PSK profile. Valid range is 1-32 characters.

Editing Multiple PSK Profile

Select an existing PSK profile and click the edit icon. A PSK profile can be modified based on these parameters.



Parameter	Description
Basic Configuration	Displays the PSK profile configurations. Update the **PSK Timer Type**, if required.

Groups	To add a new VLAN group, click Add and specify the following:
	• **Group Name** – A unique name for the group.
	• **Tunnel Interface Type** – Select the following:
	  • **No VLAN** – No VLAN is associated with this group.
	  • **Configured VLAN** – A configured VLAN is associated with this group. Specify the VLAN profile tag in **PSK VLAN TAG**.
	  • **Configured VLAN Pool** – A configured VLAN pool is associated with this group. Specify the **VLAN Pool Name**.

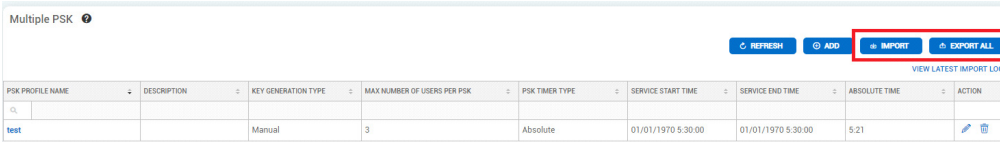
Parameter	Description
PSK Configuration	Based on the key generation method specified while creating the profile, configure the PSK key. If manual key is to be created, enter the following details: • **User Name** – A unique user name. Valid range is 1-24 characters. • **PSK key** – A unique authentication key. Valid length is 8-10 alphanumeric characters. • **Email** – The e mail ID to receive the notification for the generated key. • **Group** – The group to be assigned to the PSK profile. • **MAC Binding** – Enables MAC-IP address binding for the client. Specify the **MAC Address**. If automatic key is configured, enter the following details: • **User Prefix** – A unique user name. Valid range is 1-24 characters. • **No of PSKs** – The number of PSK keys to be generated. Valid range is 1-16000K. • **PSK length** – The length of the PSK key to be generated. The valid range is 8-10 alphanumeric characters. • **Email** – The e mail ID to receive the notification for the generated key. • **Group** – The group to be assigned to the PSK profile. • **MAC Binding** – Enables MAC-IP address binding for the client. Specify the **MAC Address**.

Deleting Multiple PSK Profile

Select an existing PSK profile and click the delete icon. The PSK profile is deleted.

Importing /Exporting Multiple PSK Profiles

You can export the multiple PSK profiles to your local system and import profile information into FortiWLM. Click **Export ALL** to export all existing PSK profiles' information in the *.csv* format on your system.



The multiple PSK profile information can be imported in the *.csv* format. The following fields are required to import the profile information.

- Basic Configuration
  - Profile Name
  - Description
  - Key Generation Type
  - Max Number of Users per psk
  - PSK Timer Type
  - Service Start Time
  - Service End Time
  - AbsoluteTime
- Groups
  - Profile Name
  - Group Name
  - Tunnel Interface Type
  - VLAN Pool Name
  - VLAN Profile
- PSK Configuration
  - Profile Name
  - User Name
  - PSK Key
  - Email ID
  - Group Name
  - MAC Binding
  - MAC Address

Note: Insert an empty row after every table so that the configuration is imported and applied correctly.

RADIUS

RADIUS (Remote Authentication Dial-In User Service) enables you to use up to three servers (one primary server and one or two backups) and maintain separate authentication and accounting for each RADIUS server employed. For authentication, this allows a different password for each user instead of having to rely on maintaining and distributing switch-specific passwords to all users. For accounting, this can help you track network resource usage.

If you have a RADIUS accounting server in your network, you can configure the controller to act as a RADIUS client, allowing the controller to send accounting records to the RADIUS accounting server. The controller sends accounting records either for clients who enter the wireless network as 802.1X authorized users or for the clients that are Captive Portal authenticated.

When using RADIUS accounting, set up a separate RADIUS profile for the RADIUS accounting server and point the *Service Profile* to that RADIUS profile. So, for example, you could have a RADIUS profile called radiusprofile1 that uses UDP port 1645 or 1812 (the two standard ports for RADIUS authentication) and your service profiles would point to radiusprofile1. To support RADIUS accounting, configure a new RADIUS profile (like radiusprofile1_acct) even if the RADIUS accounting server is the same as the RADIUS authentication server. Set its IP and key appropriately and set its port to the correct RADIUS accounting port (1646, 1813 for example). Then point *Service Profiles* to this new RADIUS profile radiusprofile1_acct.

The *RADIUS Profiles* can be either be *common* to all controllers or *specific* to one controller. *Common RADIUS* profiles apply to all controllers registered to a service profile. A *controller-specific* RADIUS profile, is specific to one controller. If both the types of RADIUS profiles are on a controller, the controller-specific RADIUS profile takes precedence over a common RADIUS profile. If you want to use a common RADIUS profile instead of controller-specific, delete the controller-specific RADIUS profile.

Remote RADIUS Server

Network deployments with remote sites that are physically away from their head-quarter (or primary data center -DC) can use remote RADIUS server in each of the remote sites for local authentication purposes.

In a typical scenario, a RADIUS server is usually co-located in the DC. Remote sites that required AAA services to authenticate their local clients use the RADIUS server in the DC. This in most cases introduces among other issues high latency between the remote site and its DC. Deploying a RADIUS server within a remote site alleviates this problem and allows remotes sites or branches to use their local AAA services (RADIUS) and not rely on the DC.

Before you Begin

Points to note before you begin deploying a remote RADIUS server:

1. Ensure that the Controller and the site AP communication time is less than RADIUS time-out.
2. Provision for at least one AP that can be configured as a relay AP.
3. Only Fortinet 11ac APs (AP122, AP822, AP832, and OAP832) in L3-mode can be configured as a relay AP.
4. In case of WAN survivability, no new 802.1x radius clients will be able to join, until relay AP rediscovers the controller.
5. Remote radius profile configurations are not supported in the common radius profile creation.

How It Works

This feature provides local authentication (.1x, Captive Profile, and mac-filtering) services using a RADIUS server set up in the remote site. In addition to the RADIUS server, the remote site must also configure a Fortinet 11ac AP as a relay AP. The remote RADIUS profile can be created using FortiWLM's WebUI (*Configure* > *Templates* > *RADIUS*). A remote RADIUS profile works like a regular profile and can be used as primary and secondary RADIUS auth and accounting servers.

High latency between the remote site and DC can cause client disconnections and sluggish network experience.

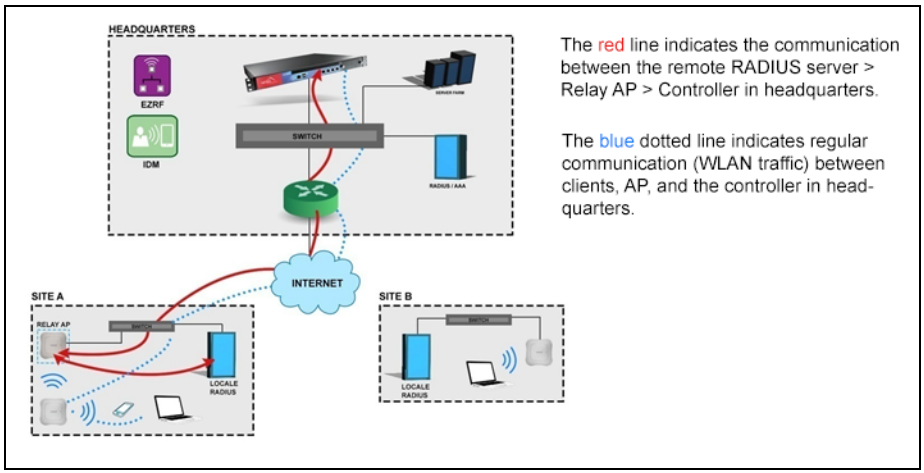
About Relay AP

The relay AP primarily is used for communicating between the RADIUS server (in the remote site) and the controller in the head-quarters.

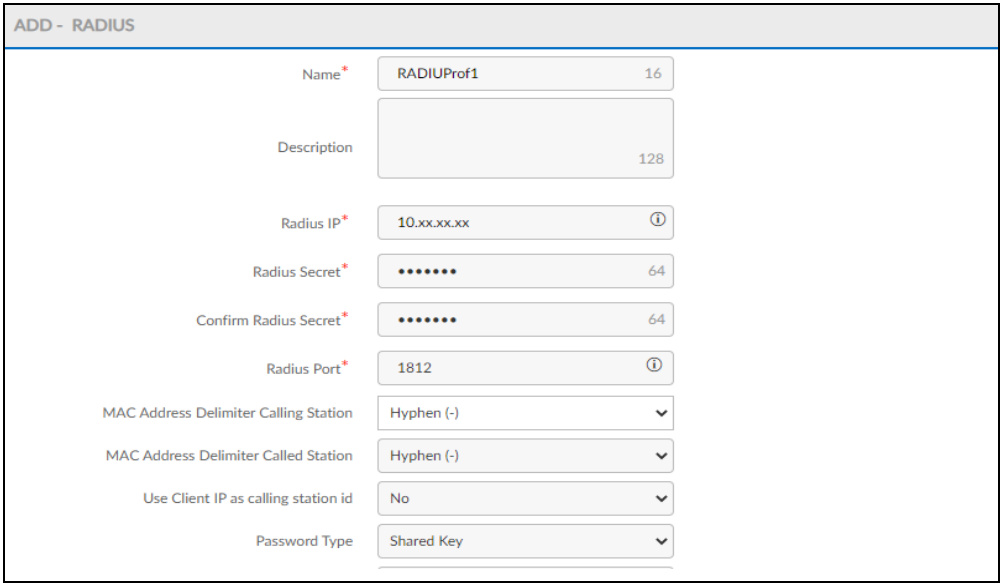
An AP is set as a relay AP only when it is assigned in the RAIDUS profile. Once an AP is assigned as a relay AP It is recommended that you do not overload the relay AP with client WLAN services. This can result in communication issues between the relay AP and DC. For regular client WLAN services, we recommend the use of a different Fortinet access point.

For a remote RAIDUS profile, you cannot configure a secondary relay AP. However, for resilience purposes, we recommend configuring an alternate (backup) RADIUS profile and assigning another AP as a relay AP to this backup RAIDUS profile. In the security profile, set this RADIUS profile as the secondary RADIUS server.

The following figure illustrates a simple scenario with local RADIUS deployment



While creating the RADIUS profile in the FortiWLM (*Configure* > *Templates* > *RADIUS*), enable Remote RADIUS Server and select a Relay AP.



To complete the *RADIUS Profile*, follow these steps:

1. *Common RADIUS profiles* are created by navigating to, *Configure* > *Design-Features* > *Wireless Service* > *Choose a Service Profile* > *Select Edit option* > *Service Profile - Update screen*. If you don't see a *RADIUS Profile* tab, then the

selected service profile does not have one configured. Provide the data for the following fields:

- Primary Authentication
- Secondary Authentication
- Primary Accounting
- Secondary Accounting
- Primary MAC Auth RADIUS
- Secondary MAC Auth RADIUS

The RADIUS created using the above method appears in the drop-down list is the labeled as RADIUS for all configurations. The above names can be up to 16 alphanumeric characters long with no spaces. This is an optional field.

2. Provide the information for the following fields in the *Primary Authentication* and *Secondary Authentication* tabs:
   - In the *Description* text box, provide some description about the RADIUS profile. A maximum of 128 characters of text can be added.
   - In the *RADIUS IP* text boxes, add the IP address (IPv4/IPv6) of the RADIUS server.
   - In the *RADIUS Secret* text box, add the shared secret that is configured for the RADIUS server. The key can be a maximum of 64 characters.
   - In the *RADIUS Port* text box, change the default port for authentication servers, 1812, to another port if the RADIUS server uses a non-default port or if the configuration is for a RADIUS accounting server, which uses port 1813 by default.
   - In the *MAC Address Delimiter Calling Station* and *MAC Address Delimiter Called Station* drop-down list, select the delimiter used on the RADIUS server to separate MAC addresses.
     - *None* - No delimiter is used.
     - *Hyphen (-)* - A hyphen is used to delimit the fields (xx-yy-zz-aa-bb-cc)
     - *Single Hyphen (-)* - Only one hyphen is used to delimit fields (xxyyzz-aabbcc)
     - *Colon (:)* - A colon is used to delimit fields (xx:yy:zz:aa:bb:cc)
   - Enable **Use Client IP as calling station id** to use the wireless client IP address as the calling station ID. When enabled the MAC address delimiter need not be specified.
   - In the *Password Type* drop-down list, select the type of password to be used for clients:
     - Shared Key--Uses the RADIUS secret that is configured.
     - MAC Address--Uses the client's MAC Address.
   - The **Called-Station-ID Type** determines the information that is sent to the RADIUS server in the Called-Station-ID attribute of the Access-Request message.
     - **Default**--This attribute stores the controller /WLAN MAC address
     - **MACAddress**--This attribute stores the controller /WLAN MAC address.

- **MACAddress:SSID**--This attribute stores controller/WLAN MAC address and the SSID to which the client connects.
- **APMACAddress**--This attribute stores the access point MAC address.
- **APMACAddress:SSID**--This attribute stores the access point MAC address and the SSID to which the client connects.
- **APName**--This attribute stores the name of the access point configured on the controller.
- **APName:SSID**--This attribute stores the name of the access point configured on the controller and the SSID to which the client connects.
- **APLocation**--This attribute stores the location details of the access point configured on the controller.
- **APGroup**--This attribute stores the access point group details configured on the controller.
- **AP IP**--This attribute stores the IP address of the access point.
- **VLAN**--This attribute stores the VLAN tag associated with the ESSID from where the RADIUS request originates.

- [IPv6 only] The **NAS IP** address to be used in RADIUS access requests. When configuring a controller to use a RADIUS server, the controller interface has multiple IP addresses, select the IP address included in the RADIUS configuration. However, if the NAS IP is not specified, any of the controller IPv6 interface addresses is used instead.
- Configure the Network Access Server Identifier (**NAS Identifier**) to report the source of the RADIUS access request. This allows the RADIUS server to select a policy for that request. You can configure the NAS identifier for each security profile.
  The controller sends the NAS ID to the RADIUS through an authentication request to classify users to different groups. This allows the RADIUS server to send a customized authentication response.
  While creating a RADIUS security profile you can configure the **NAS Identifier**; valid range is 0-128 characters.

3. Accounting records are sent for the duration of a client session, which is identified by a unique session ID. You can configure a RADIUS profile for the primary accounting RADIUS server and another profile for a secondary accounting RADIUS server, which serves as a backup should the primary server be offline. The switch to the backup RADIUS server works as follows. After 30 seconds of unsuccessful Primary RADIUS server access, the secondary RADIUS server becomes the default. The actual attempt that made it switch is discarded and the next RADIUS access that occurs goes to the Secondary RADIUS server. After about fifteen minutes, access reverts to the Primary RADIUS Server.
   Provide the information for the following fields in the *Primary Accounting* and *Secondary Accounting* tabs:
   - In the *Description* text box, provide some description about the RADIUS profile. A maximum of 128 characters of text can be added.
   - In the *RADIUS IP* text boxes, add the IP address of the RADIUS server.

- In the *RADIUS Secret* text box, add the shared secret that is configured for the RADIUS server. The key can be a maximum of 64 characters.
- In the *RADIUS Port* text box, change the default port for authentication servers, 1812, to another port if the RADIUS server uses a non-default port or if the configuration is for a RADIUS accounting server, which uses port 1813 by default.
- In the *MAC Address Delimiter Calling Station* and *MAC Address Delimiter Called Station* drop-down list, select the delimiter used on the RADIUS server to separate MAC addresses.
  - *None* - No delimiter is used.
  - *Hyphen (-)* - A hyphen is used to delimit the fields (xx-yy-zz-aa-bb-cc)
  - *Single Hyphen (-)* - Only one hyphen is used to delimit fields (xxyyzz-aabbcc)
  - *Colon (:)* - A colon is used to delimit fields (xx:yy:zz:aa:bb:cc)
- Enable **Use Client IP as calling station id** to use the wireless client IP address as the calling station ID. When enabled the MAC address delimiter need not be specified.
- The **Called-Station-ID Type** determines the information that is sent to the RADIUS server in the Called-Station-ID attribute of the Access-Request message.
  - **Default**--This attribute stores the controller /WLAN MAC address
  - **MACAddress**--This attribute stores the controller /WLAN MAC address.
  - **MACAddress:SSID**--This attribute stores controller/WLAN MAC address and the SSID to which the client connects.
  - **APMACAddress**--This attribute stores the access point MAC address.
  - **APMACAddress:SSID**--This attribute stores the access point MAC address and the SSID to which the client connects.
  - **APName**--This attribute stores the name of the access point configured on the controller.
  - **APName:SSID**--This attribute stores the name of the access point configured on the controller and the SSID to which the client connects.
  - **APLocation**--This attribute stores the location details of the access point configured on the controller.
  - **APGroup**--This attribute stores the access point group details configured on the controller.
  - **AP IP**--This attribute stores the IP address of the access point.
  - **VLAN**--This attribute stores the VLAN tag associated with the ESSID from where the RADIUS request originates.
- [IPv6 only] The **NAS IP** address to be used in RADIUS access requests. When configuring a controller to use a RADIUS server, the controller interface has multiple IP addresses, select the IP address included in the RADIUS configuration. However, if the NAS IP is not specified, any of the controller IPv6 interface addresses is used instead.
- In the *Password Type* drop-down list, select the type of password to be used for clients:

- Shared Key--Uses the RADIUS secret that is configured.
- MAC Address--Uses the client's MAC Address.

4. *MAC Filtering options are specified in the MAC Filtering Primary and MAC Filtering Secondary tabs:*
5. *Controller specific RADIUS profiles* are created by navigating to, *Configure* > *Design-Features* > *Wireless Service* > *Choose a Service Profile* > *Select Edit option* > *Service Profile - Update screen* > Choose the Radius Profile tab > Select Primary Authentication tab > Select the *Add or plus* icon to add individual controller radius configuration.
6. *Configure* > *Templates* > *Radius* > *Radius Profile screen* > Select the *Add or plus* icon to add individual controller radius configuration. Controller specific RADIUS profiles can be configured either from *FortiWLM* or from the controller. You can tell where a profile was configured by checking the read-only from the controller, by selecting the Wireless *Service profile - Security* and *RADIUS* tabs and look at the field *Owner*. A controller configuration owned by *FortiWLM* has the owner listed as *nms-server*.
7. Provide the information for the following fields in the *Radius Profile - Add* screen:
   - In the *RADIUS Profile Name*, provide a name for the controller specific RADIUS profile. A maximum of 16 characters of text can be added.
   - In the *Description* text box, provide some description about the RADIUS profile. A maximum of 128 characters of text can be added.
   - In the *RADIUS IP* text boxes, add the IP address of the RADIUS server.
   - In the *RADIUS Secret* text box, add the shared secret that is configured for the RADIUS server. The key can be a maximum of 64 characters.
   - In the *RADIUS Port* text box, change the default port for authentication servers, 1812, to another port if the RADIUS server uses a non-default port or if the configuration is for a RADIUS accounting server, which uses port 1813 by default.
   - In the *MAC Address Delimiter Calling Station* and *MAC Address Delimiter Called Station* drop-down list, select the delimiter used on the RADIUS server to separate MAC addresses.
     - *None* - No delimiter is used.
     - *Hyphen (-)* - A hyphen is used to delimit the fields (xx-yy-zz-aa-bb-cc)
     - *Single Hyphen (-)* - Only one hyphen is used to delimit fields (xxyyzz-aabbcc)
     - *Colon (:)* - A colon is used to delimit fields (xx:yy:zz:aa:bb:cc)
   - Enable **Use Client IP as calling station id** to use the wireless client IP address as the calling station ID. When enabled the MAC address delimiter need not be specified.
   - In the *Password Type* drop-down list, select the type of password to be used for clients:
     - Shared Key--Uses the RADIUS secret that is configured.
     - MAC Address--Uses the client's MAC Address.

- The **Called-Station-ID Type** determines the information that is sent to the RADIUS server in the Called-Station-ID attribute of the Access-Request message.
  - **Default**--This attribute stores the controller /WLAN MAC address
  - **MACAddress**--This attribute stores the controller /WLAN MAC address.
  - **MACAddress:SSID**--This attribute stores controller/WLAN MAC address and the SSID to which the client connects.
  - **APMACAddress**--This attribute stores the access point MAC address.
  - **APMACAddress:SSID**--This attribute stores the access point MAC address and the SSID to which the client connects.
  - **APName**--This attribute stores the name of the access point configured on the controller.
  - **APName:SSID**--This attribute stores the name of the access point configured on the controller and the SSID to which the client connects.
  - **APLocation**--This attribute stores the location details of the access point configured on the controller.
  - **APGroup**--This attribute stores the access point group details configured on the controller.
  - **AP IP**--This attribute stores the IP address of the access point.
  - **VLAN**--This attribute stores the VLAN tag associated with the ESSID from where the RADIUS request originates.
- [IPv6 only] The **NAS IP** address to be used in RADIUS access requests. When configuring a controller to use a RADIUS server, the controller interface has multiple IP addresses, select the IP address included in the RADIUS configuration. However, if the NAS IP is not specified, any of the controller IPv6 interface addresses is used instead.
- In the *Controller Name* drop-down list, select a controller IP address to which you want the RADIUS profile to be mapped.

See the ***Authentication*** chapter of the ***Controller Configuration Guide***, for detailed information on *RADIUS Profiles*.

Captive Portal

The captive portal profiles feature that allows you to create individual captive portal profiles with distinct configuration settings. Such captive portal profiles can be mapped to security profiles for fine control over captive portal user access.

A captive portal profile is created from the **Configure > Templates** > **Captive Portal** page. Profile created in this page can be applied to a security profile.

NOTE: Captive Portal profile can be enabled only if at least one Captive Profile is created.

Social Authentication Support in Captive Portal

The captive portal authentication process now supports Fortinet Presence as an external CP authentication server that allows users to authentication using social media accounts like Facebook or Gmail OAuth.

Supported APs: AP122, AP822, AP832, OAP832, FAP-U421, and FAP-U423.

Before proceeding, note the following:

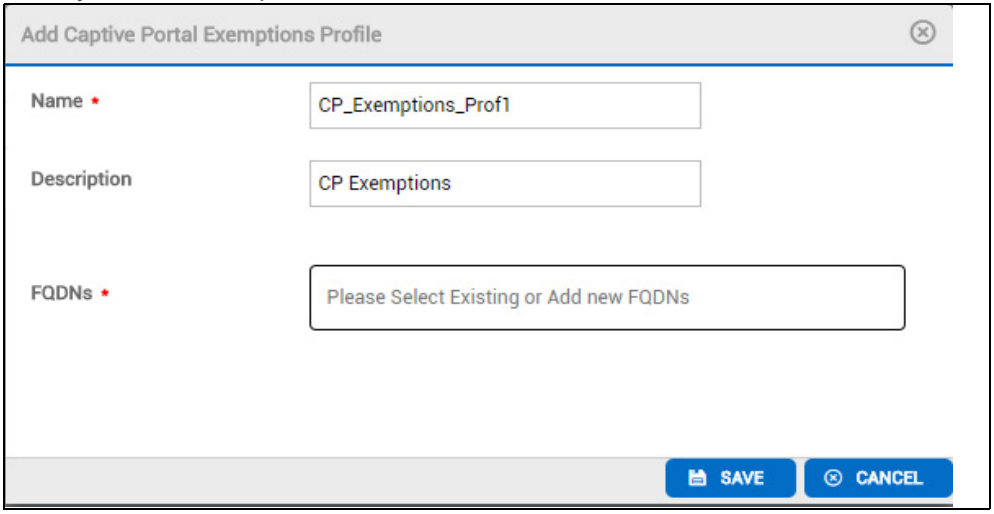
- Enable location service in the controller (See Configuring FortiPresence API section in the FortiWLC (SD) configuration guide for more details).
- Assign the AP in the data analytics store.
- Not supported in "Bridge mode"

To enable social authentication support, do the following:

Create Captive Portal Exemptions Profile

To enable social login, create a profile with the list of exempted URLs and in the captive portal profile and select FortiPresence as the external authentication server.

1. Go to *Configure* > *Templates* > *Captive Portal Exemptions*.
2. Click the Add (+) button to create a profile with the list of URLs that will be allowed for social authentications. To add multiple URL to a profile, enter a space after each URL entry. You can add up to 32 URLs.

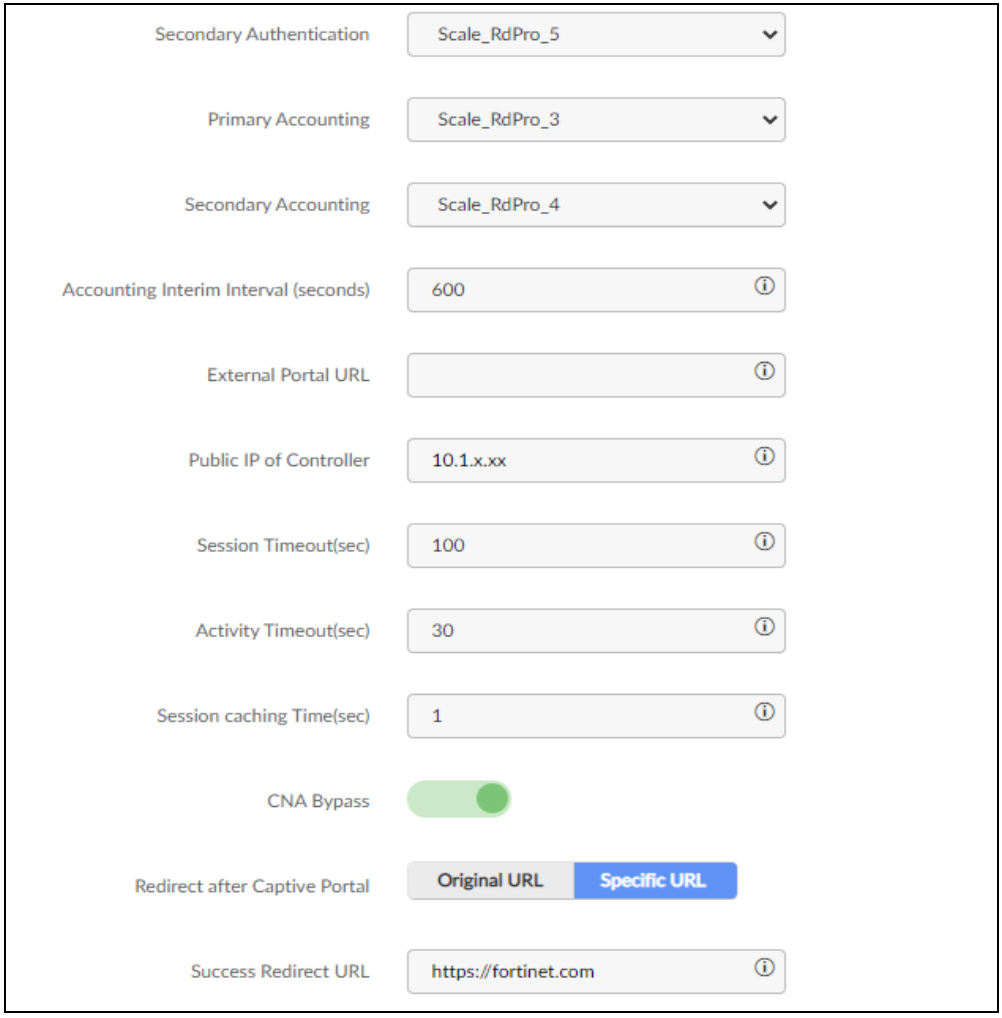


For each profile, ensure that you add **socialwifi.fortipresence.com** (inclusive of the 32 URLs) as part of the FQDN list. This is mandatory for clients to access Social Wi-Fi login page.

Configure Captive Portal Profile to use Fortinet Presence

1. Go to *Configure* > *Templates* > *Captive Portal*.
2. Create a captive portal profile with local/radius/local and radius as authentication type
   - If Authentication type is Local, then create a guest user profile with a username and password and register the profile to controller or create guest users in the controller.
   - If Authentication type is RADIUS, then in that RADIUS server, create a user with a username and password.

Make the following changes to External Portal Settings:



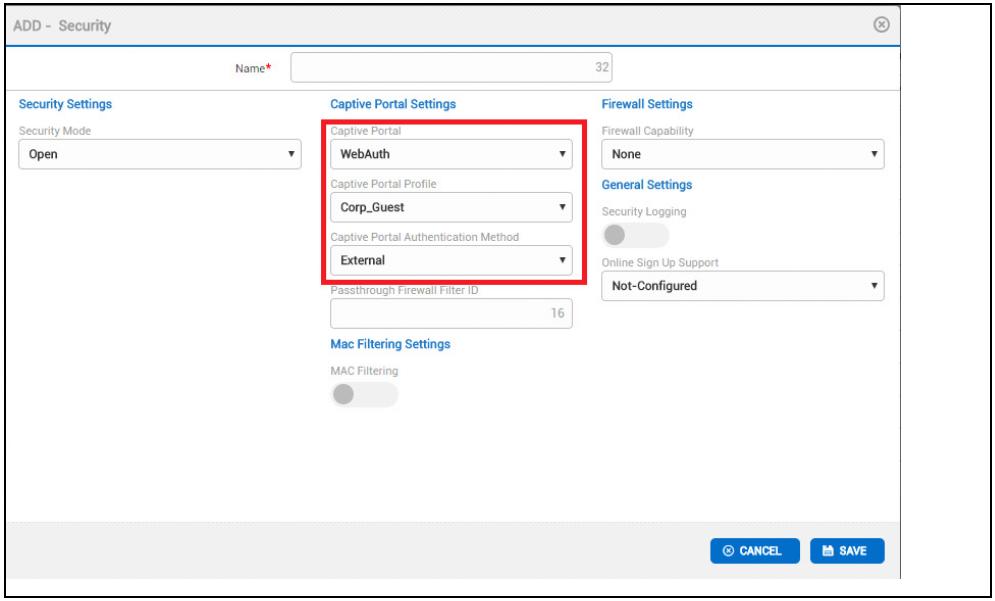
3. Enter the URL (IPv4/IPv6) of the external captive portal server. This is used if you set Captive Portal Authentication Method as External in the security profile. Enter the **http://socialwifi.fortipresence.com/wifi.html?login** URL (1) in the external portal URL.
4. **Public IP of Controller**: Enter the IP address (IPv4/IPv6) of the external captive portal server.
5. **Session Timeout(sec):**If a client session lasts this long (0-1440 minutes), ask the client to reauthenticate. By default, 0 is set, which is no timeout.
6. **Activity Timeout(sec)**:If a client is idle for this many minutes (0-60), ask the client to reauthenticate. By default, 0 is set, which is no timeout.

7. **Session caching Timeout(sec)** Valid range: [1-1440]: If the client leaves the network and rejoins within this time, reauth is not required.
8. **CNA Bypass**: Enable this to disable authentication pop up displayed on Apple iOS and Android devices.
9. **Redirect after Captive Portal:** Configure the website redirection options after successful login into the captive portal. Select **Original URL** to redirect to the initial URL browsed before Captive Portal authentication. Select **Specific URL** to redirect to the URL specified in **Success Redirect URL** after successful Captive Portal authentication.
10. **Captive Portal External Server Type**: Select the external server, Fortinet-Connect or Fortinet-Presence.
11. **Captive Portal Exemption**: Select the Captive Portal Exemption Profile associated with the external server type.

Note: This feature is supported only on FortiWLC 8.5.2 and above.

Enable this captive portal profile in security and ESS profiles

Enable the captive portal profile in the security profile and map the security profile in the ESS Profile. In the security profile, make the following changes to the CAPTIVE PORTAL SETTINGS section:



VLAN

A virtual local area network (VLAN) is a broadcast domain that can span across wired or wireless LAN segments. Each VLAN is a separate logical network. Several VLANs can coexist within any given network, logically segmenting traffic by organization or function. In this way,

all systems used by a given organization can be interconnected independent of physical location. This has the benefit of limiting the broadcast domain and increasing security. VLANs can be configured in software, which enhances their flexibility. VLANs operate at the data link layer (OSI Layer 2), however, they are often configured to map directly to an IP network, or subnet, at the network layer (OSI Layer 3). You can create up to 512 VLANs.

IEEE 802.1Q is the predominant protocol used to tag traffic with VLAN identifiers. VLAN1 is called the default or native VLAN. It cannot be deleted, and all traffic on it is untagged. A trunk port is a network connection that aggregates multiple VLANs or tags, and is typically used between two switches or between a switch and a router. VLAN membership can be port-based, MAC-based, protocol-based, or authentication-based when used in conjunction with the 802.1x protocol. Used in conjunction with multiple ESSIDs, VLANs support multiple wireless networks on a single Access Point using either a one-to-one mapping of ESSID to VLAN, or mapping multiple ESSIDs to one VLAN. By assigning a security profile to a VLAN, the security requirements can be fine-tuned based on the use of the VLAN, providing wire-like security or better on a wireless network.

VLANs can be configured/owned either by *FortiWLM* or by a controller. You can tell where a profile was configured by checking the read-only field *Owner*; the *Owner* is either *nms-server* or *controller*. All *nms-server* VLAN profiles cannot be modified on the controller. In order to map a service profile to a VLAN, follow the below steps:

1. Select *Configure* > *Design-Features* > *Wireless Service* > *Choose a Service Profile* > *Select Edit option* > *Service Profile - Update* screen.
2. In the *Service Profile - Update* screen, Select the *Tunnel Interface Type* from the drop-down list. The following are the options:
   - *No Tunnel*: No tunnel is associated with this service profile.
   - *Configured VLAN Only*: A configured VLAN only is listed in the following VLAN Name list is associated with this service profile.
   - *Radius VLAN Only*: The VLAN is assigned by the RADIUS server via the RADIUS attribute Tunnel Id. Use RADIUS VLAN Only when clients authenticate via 802.1x/WPA/WPA2 or MAC Filtering.
   - Radius and Configured VLAN: Both configured VLAN and RADIUS VLAN are associated with this service profile.
   - GRE: Specifies a GRE Tunnel configuration.

   This is an optional field.
3. If you have selected the *Tunnel Interface Type* as *Configured VLAN Only*, *Radius VLAN Only*, and *Radius and Configured VLAN*, type a *VLAN Profile* name or select an existing *VLAN Profile* name from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths:
   Configure > *Design-Features* > *Wireless Service* > *Service Profile* > *Edit* > *Service Profile - Update* > provide a name in the *VLAN Profile* text box or select the existing *VLAN Profile*.

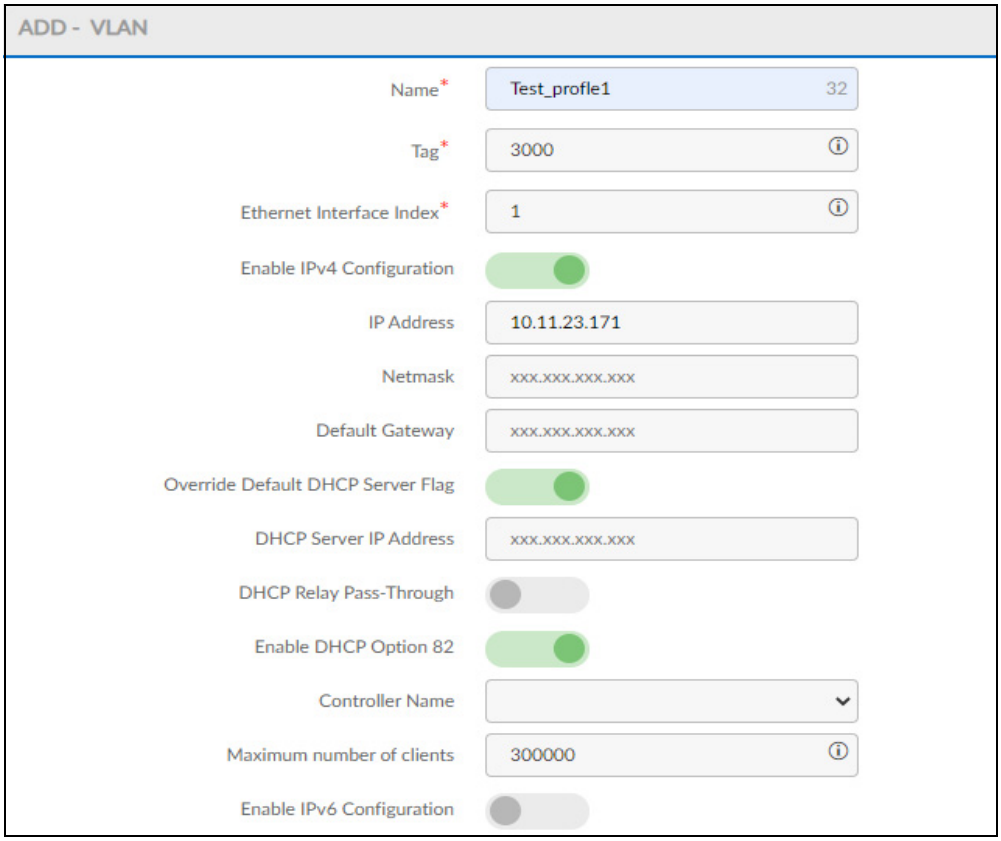
The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.

4. Select the *VLAN Profile* tab, click the *Add or plus* icon to add individual controller VLAN configuration. The controller specific VLAN profiles can be configured either from *FortiWLM* or from the controller. You can tell where a profile was configured by checking the read-only from the controller, by selecting *Configure* > *Templates* > *VLAN* and look at the field *Owner*. A controller configuration owned by *FortiWLM* has the owner listed as *nms-server*.
5. To add individual VLAN profiles, select *Configure* > *Templates* > *VLAN* > *Add*. Provide the information for the following fields in the *VLAN Profile - Add* screen:
   - Provide a *VLAN Profile Name* up to 32 alphanumeric characters long without spaces for the VLAN Profile Name. This is a required field.
   - In the *TAG* text box, either type the VLAN tag or select the VLAN tag. The VLAN tag is an integer in the range of 1 through 4,094. This is a mandatory field.
   - In the *Ethernet Interface Index* text box, enter the number of the interface (1 or 2; the second interface is an optional configuration).
   - In the *IP Address* text boxes, type the IPv4 address. The IP address must match the IP address of the default gateway configured in wireless clients.
   - In the *Netmask* text boxes, type the subnet mask of the IP address. The subnet mask must match the subnet mask of the default gateway configured in wireless clients.
   - In the *IP Address of the Default Gateway* text boxes, type the default gateway's IPv4 address. This IP address is the default gateway used by the controller to route traffic from clients using this VLAN.
   - In the *Override Default DHCP Server Flag* drop-down list, select one of the following options:
     - *On*: Enable use of specified DHCP server (see step 8 rather than the global DHCP server configured for the controller.
     - *Off*: Disable usage of specified DHCP server and return to using global DHCP server configured for the controller.
   - In the *DHCP Server IP Address* text boxes, type the IPv4 address of the DHCP relay server.
   - In the *DHCP Relay Pass-Through* drop-down list, select one of the following options:
     - *On*: Enable use of the pass-through DHCP server feature (default setting).
     - *Off*: Disable usage of the pass-through DHCP server feature. If the DHCP server is set to the default IP address of 127.0.0.1, DHCP packets pass through without modification. No DHCP relay function is performed. Instead, the packet is copied as is. This mode of operation is the default for a fresh system.
   - In the *Controller Name* drop-down list, select a controller IP address.
   - In the *Maximum number of clients* field enter the maximum number of IPv4 clients supported in this VLAN, if this VLAN tag is used in a VLAN pool.

- To add a VLAN Profile with IPv6 configuration, update the following fields.
  - *IPv6 Address*: Type a valid IPv6 address belonging to this VLAN.
  - *IPv6 Prefix*: Type the IPv6 address prefix.
  - I*Pv6 Address of the Default Gateway*: Type the default gateway's IPv6 address. This IP address is the default gateway used by the controller to route traffic from clients using this VLAN.
  - *Override Default DHCPv6 Server Flag*
    On: Enable use of specified DHCP server (rather than the global DHCP server configured for the controller.
    Off: Disable use of specified DHCP server and use the global DHCP server configured for the controller.
  - *DHCP Server IPv6 Address*: Type the IPv6 address of the DHCP relay server.
  - *DHCP Relay Pass-Through*
    On: Enable use of the pass-through DHCP server feature (default setting).
    Off: Disable use of the pass-through DHCP server feature.
  - *Maximum number of IPv6 clients*: The maximum number of IPv6 clients supported in this VLAN, if this VLAN tag is used in a VLAN pool.
  - *Fwd IPV6 MLD Report*: Enable to forward the Multicast Listener Discovery (MLD) report.

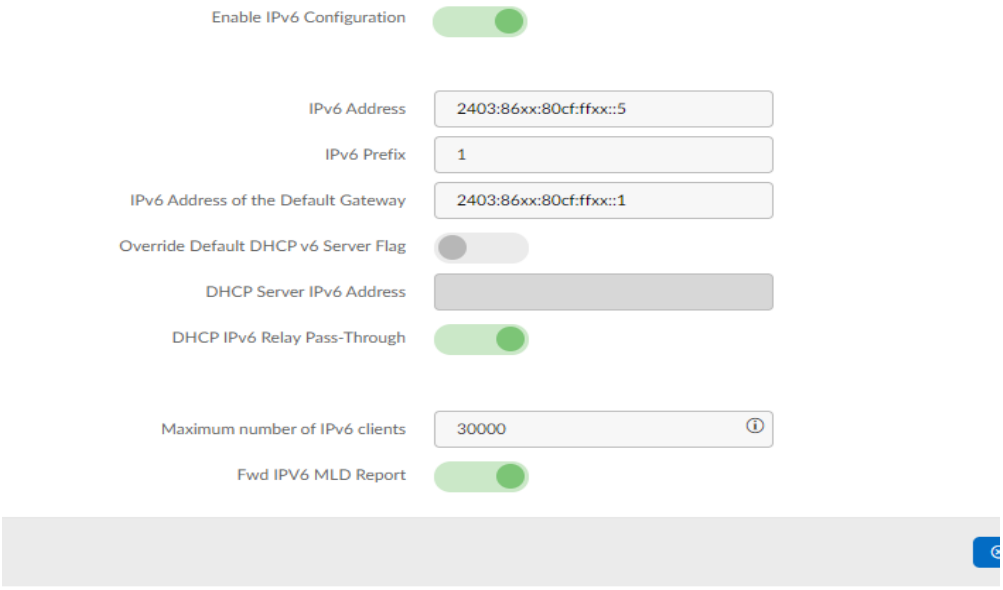
6. When this option is enabled, the controller acts as a DHCP relay agent to avoid DHCP client requests from untrusted sources. This secures the network where DHCP is used to allocate network addresses. The controller adds the DHCP option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server. By default, this option is disabled. This feature is supported with FortiWLC 8.6.0 and above.
   Note: DHCP Relay Pass-Through should be disabled for the controller to act as the DHCP relay agent.
7. Select *Save*. The VLAN Profile is created and displayed on the VLAN Profile screen.

Figure 132: *Service Profile - VLAN Profile - Add*



VLAN profiles cannot be edited once they are synchronized to a controller.

Figure 133: *VLAN IPv6 configuration*



Modify the Existing VLAN Profile

All *VLAN Profiles* are edited differently, depending on whether or not they are synced to a controller. To edit a unsynced *VLAN Profile*,

1. Navigate to *Configure* > *Design-Features* > *Wireless Service*. The *Service Profile* screen displays a list of service profiles to which a Controller or an AP Group can be registered.
2. Choose a *Service Profile* and select *Edit.*
3. Select the *VLAN Profile* tab, the *Service Profile - VLAN Profile Add* screen is displayed.
4. Perform the modifications on the *Service Profile - VLAN Profile* screen and select *Save*. Updating a synced *VLAN Profile* is more complicated and can be done with two methods, as described below.

Edit a Synced VLAN by un-registering Controllers

To edit a VLAN synced to controllers, follow these steps:

1. Navigate to *Configure* > *Design-Features* > *Wireless Service*. The *Service Profile* screen displays a list of service profiles to which a Controller or an AP Group can be registered.
2. Choose a *Service Profile* and select *Edit.* Un-register the controller(s) from all service profiles where this *VLAN Profile* is used
3. Choose a service profile where VLAN is used and select a *Registration* tab.
4. Select the existing profile and click Unregister.
5. Change the *VLAN Profile* by clicking *Configure* > *Templates* > *VLAN, selecting a VLAN Profile* > *Edit* > *making the changes* > *Save*.

6. Re-register the controller to all service profiles where this *VLAN Profile* is used by clicking *Configure* > *Design-Features* > *Wireless Service* > select a service profile where this VLAN is used > *Registration tab* > *select the controller* > *Save*.

Edit a Synced VLAN by Editing Service Profiles

To edit a VLAN synced to controllers, follow these steps:

1. Edit all the service profiles where this VLAN is used by clicking *Configure* > *Design-Features* > *Wireless Service* selecting a profile where VLAN is used > *Edit* > changing Tunnel Interface Type to No Tunnel > OK.
2. Change the *VLAN Profile* by clicking *Configure* > *Templates* > *VLAN, selecting a VLAN Profile* > *Edit* > *making the changes* > *Save*.
3. Re-edit all the service profiles you changed in step 1 by clicking *Configure* > *Design-Features* > *Wireless Service* > selecting a profile > *Edit* > changing Tunnel Interface Type to the earlier value (Configured VLAN only or RADIUS VLAN only or Configured VLAN or GRE) > Save.

See the ***Configuring VLANs*** chapter of the ***Controller Configuration Guide***, for detailed information on *RADIUS Profiles*.

VLAN POOL

To reduce big broadcast or risking a chance of running out of address space, you can now enable VLAN pooling in a wireless service profile.

VLAN pooling essentially allows administrators to create a named alias using a subset of VLANs thereby creating a pool of address. By enabling VLAN pool, you can now associate a client/device to a specific VLAN. This allows you to effectively manage your network by monitoring appropriate or specific VLANs pools.

VLAN pool profiles can also be created while configuring a wireless service profile (*Configure* > *Design-Features* > *Wireless Service*).

VLAN Pool is available only in tunnelled mode.

Features of VLAN Pool

- You can associate up to 16 VLANs to a pool
- You can specify the maximum number of clients that can be associated to a VLAN.
- The client/device behavior does not change after it is associated to a VLAN in a pool.

- If a VLAN is removed from a VLAN pool, clients/devices connected to the VLAN will continue to be associated to the VLAN. However, if the clients disconnect and reconnect, their VLAN will change.

Creating a VLAN Pool

1. In the *Configure* > *Templates* > *VLAN* page, create a VLAN.
2. Go to *Configure* > *Templates* > *VLAN Pool* page, create a VLAN pool and specify the VLAN tag as mentioned in step 1.
3. In the *Configure* > *Design-Features* > *Wireless Service* page:
   - Select **Tunnel Type Interface** as VLAN Pool

Select the VLAN Pool Profile.

Timer

You can schedule the availability of an ESS based on pre-define time intervals. By default, ESS profiles are always ON and available to clients/devices. By adding a timer, you can control the availability of an ESS profile based on pre-defined times during a day or across multiple days.

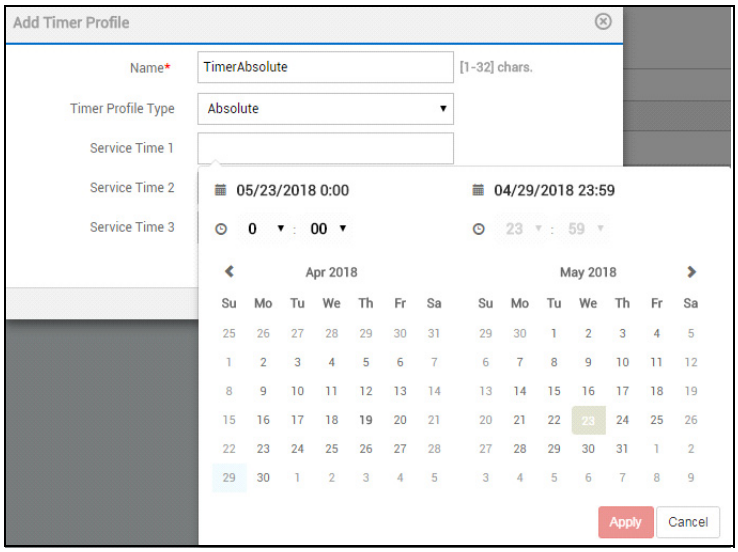
To create a time based ESS profile, you must first create a timer profile and then associate the timer profile to the ESS profile.

Creating a Timer Profile

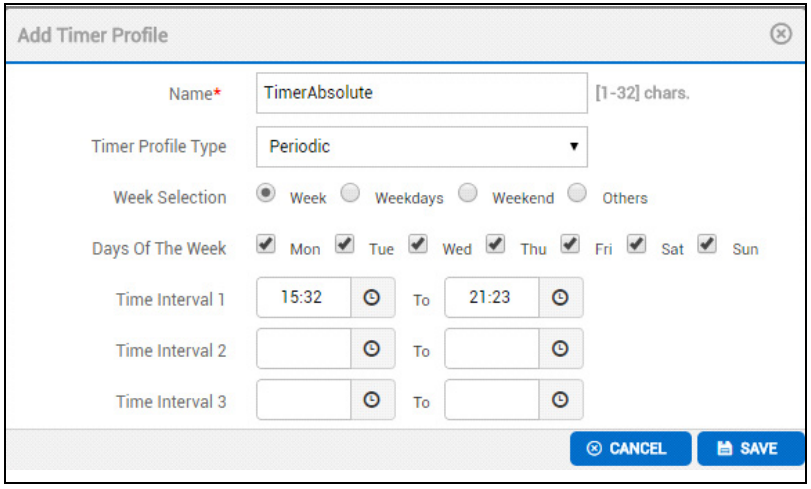
You can create timer profile using WebUI or CLI.

Using WebUI

1. Go to *Configure* > *Templates* > *Timer* and click the + button.
2. In the Add Timer Profile window, enter Timer Profile Name and select Timer Type:



- **Absolute** timer profiles can enable and disable ESS visibility for time durations across multiple days. You can create up to 3 specific start and end time per timer profile. To enter start of the end time, click the Date picker box.
- **Periodic** timer profiles are a set of start and end timestamp that can be applied across multiple days of a week. To create a period timer profile, enter the time in hh:mm format. Where hh, represent hours in 2-digits and mm represent minutes in 2-digits. This figure illustrates a timer profile that will be applied on Sunday, Monday, Tuesday, and Thursday from 15:32 (3.32 PM).



Alternatively, while creating a wireless service, specify a name for the Timer profile before you click the Save button. After you click the Save button, additional tabs are opened to configure the timer-profiles.

GRE

The GRE tunneling provides packet isolation from one endpoint to another, encapsulated within an IP tunnel to separate user traffic. GRE tunneling provides an option to segregate users' traffic by allowing a service profile to be tied to a GRE profile. This provides an alternative to VLANs for segregating traffic.

GRE tunneling is accomplished by creating routable tunnel endpoints that operate on top of existing physical and/or other logical endpoints. The tunnels behave as virtual point-to-point links that have two endpoints identified by the tunnel source and tunnel destination addresses at each endpoint. By design, GRE tunnels connect A to B and provide a clear data path between them. This data path is not secure. To ensure the data security, GRE uses *Internet Protocol Security* on the tunnels. These tunnels data is routed by the system to the GRE endpoint using routes established in the route table; therefore each data packet traveling over the GRE tunnel gets routed through the system twice.

The routes can be manually established or dynamically learned using routing protocols such as RIP or OSPF. Once a data packet is received by the GRE endpoint, it is encapsulated in a GRE header and routed again using the endpoint configuration destination address of the tunnel.

GRE can be configured/owned either by *FortiWLM* or by a controller. You can tell where a profile was configured by checking the read-only field *Owner*; the *Owner* is either *nms-server* or *controller*. All *nms-server* GRE profiles cannot be modified on the controller. In order to map a service profile to a GRE, follow the below steps:

Note: GRE configuration supports both IPv4 and IPv6 addresses.

1. Select *Configure* > *Design-Features* > *Wireless Service* > *Choose a Service Profile* > *Select Edit option* > *Service Profile - Update* screen.
2. In the *Service Profile - Update* screen, Select the *Tunnel Interface Type* from the drop-down list. The following are the options:
   - *No Tunnel*: No tunnel is associated with this service profile.
   - *Configured VLAN Only*: A configured VLAN only is listed in the following VLAN Name list is associated with this service profile.
   - *Radius VLAN Only*: The VLAN is assigned by the RADIUS server via the RADIUS attribute Tunnel Id. Use RADIUS VLAN Only when clients authenticate via 802.1x/WPA/WPA2 or MAC Filtering.

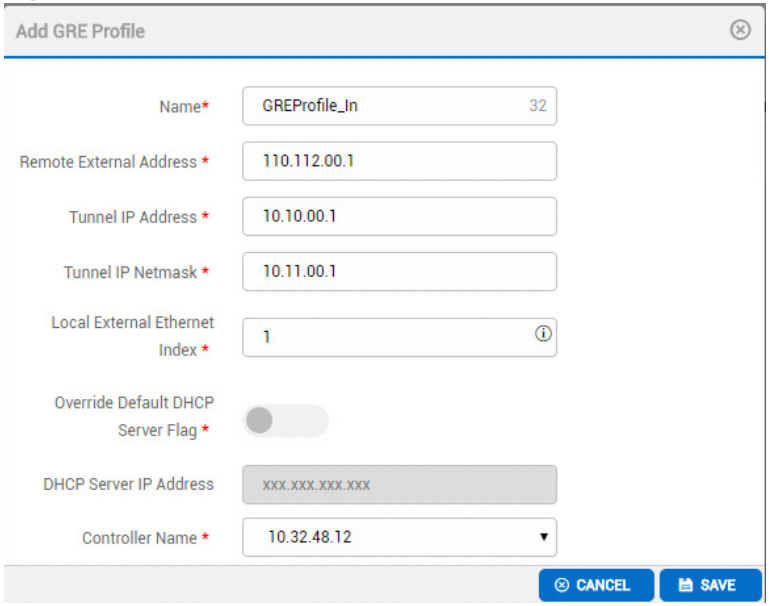
- Radius and Configured VLAN: Both configured VLAN and RADIUS VLAN are associated with this service profile.
- GRE: Specifies a GRE Tunnel configuration.

This is an optional field.

3. If you have selected the *Tunnel Interface Type* as *GRE*, type a *GRE Profile* name or select an existing *GRE Profile* name from the drop-down list. You can provide the name of the profile now and complete it later by navigating to the below paths: *Configure* > *Design-Features* > *Wireless Service* > *Service Profile* > *Edit* > *Service Profile - Update* > provide a name in the *GRE Profile* text box or select the existing *GRE Profile.* The name can be up to 32 alphanumeric characters long with no spaces. This is a mandatory field.
4. Select the *GRE Profile* tab, click the *Add or plus* icon to add individual controller GRE configuration. The controller specific GRE profiles can be configured either from *FortiWLM* or from the controller. You can tell where a profile was configured by checking the read-only from the controller, by selecting *Configure* > *Security* > *VLAN* and look at the field *Owner*. A controller configuration owned by *FortiWLM* has the owner listed as *nms-server*.
5. To add individual GRE profiles, select *Configure* > *Templates* > *VLAN* > *Add*. Provide the information for the following fields in the *VLAN Profile - Add* screen:
   - In the
   - In the *Remote External Address* text boxes, type the IP address of the remote end of the GRE tunnel.
   - In the *Tunnel IP Address* text boxes, type the IP address for the local end of the GRE tunnel.
   - In the *Tunnel IP Netmask* text boxes, type the IP address.
   - In the *Local External FastEthernet Index* text box, type the interface ID (1 or 2; interface 2 requires configuration) of the *FastEthernet* interface that the tunnel will use.
   - In the *Override Default DHCP Server Flag* drop-down list, select the following options:
     - *On*: Enable use of specified DHCP server rather than the global DHCP server configured for the controller.
     - *Off*: Disable usage of specified DHCP server and return to using global DHCP server configured for the controller.
   - In the *DHCP Server IP Address* text boxes, type the IP address of the DHCP relay server.
   - In the *Controller Name* drop-down list, select a controller IP address.
6. Select *Save*. The *GRE Profile* is created and displayed on the *GRE Profile* screen.

GRE profiles cannot be edited once they are synchronized to a controller.

Figure 134: *Service Profile - GRE Profile - Add*



See the ***Service Profile - GRE Profile*** screen (*Configure* > *Design-Features* > *Wireless Service* > *Edit* > *GRE Profile*) or the ***GRE Profile - Add*** screen (*Configure* > *Templates* > *Security* > *Add* > *GRE Profile - Add*) in Online Help for detailed information on *Security Profile* topic.

Modify the Existing GRE Profile

GRE profiles are edited differently, depending on whether or not they are synced to a controller. To edit an unsynced GRE profile,

1. Navigate to *Configure* > *Design-Features* > *Wireless Service*. The *Service Profile* screen is displayed, providing a list of service profiles to which a Controller or an AP Group can be registered.
2. Choose a *Service Profile* and select *Edit.*
3. Select the *GRE Profile* tab.
4. In the *Service Profile - GRE Profile* screen, select a GRE Profile and click *Edit*. Perform the modifications and select *Save*.
   Updating a synced GRE profile is more complicated and can be done with two methods, as described below.

Edit a Synced GRE Profile by un-registering Controllers

To edit a GRE synced to controllers, follow these steps:

1. Un-register the controller(s) from all service profiles where this GRE profile is used by clicking *Configure* > *Design-Features* > *Wireless Service* select a service profile where GRE is used. In the Registration tab, select the controller and unregister.
2. Change the GRE profile by clicking *Configure* > *Templates* > *GRE*, selecting a GRE profile, edit the profile and click **Save**.
3. Re-register the controller to all service profiles where this GRE profile is used by clicking *Configure* > *Design-Features* > *Wireless Service* > select a service profile where GRE is used > Registration tab > Register > select the controller > Save.

Edit a Synced GRE Profile by Editing Service Profiles

To edit a GRE synced to controllers, follow these steps:

1. Edit all the service profiles where this GRE is used by clicking *Configure* > *Design-Features* > *Wireless Service* > selecting a profile where GRE is used > Edit > changing Tunnel Interface Type to No Tunnel > Save.
2. Change the GRE profile by clicking *Configure* > *Templates* > *GRE*, selecting a GRE profile > Edit > making the changes > Save.
3. Re-edit all the service profiles you changed in step 1 by clicking *Configure* > *Design-Features* > *Wireless Service* > selecting a profile > Edit > changing Tunnel Interface Type to the earlier value (Configured VLAN only or RADIUS VLAN only or Configured VLAN or GRE) > Save.

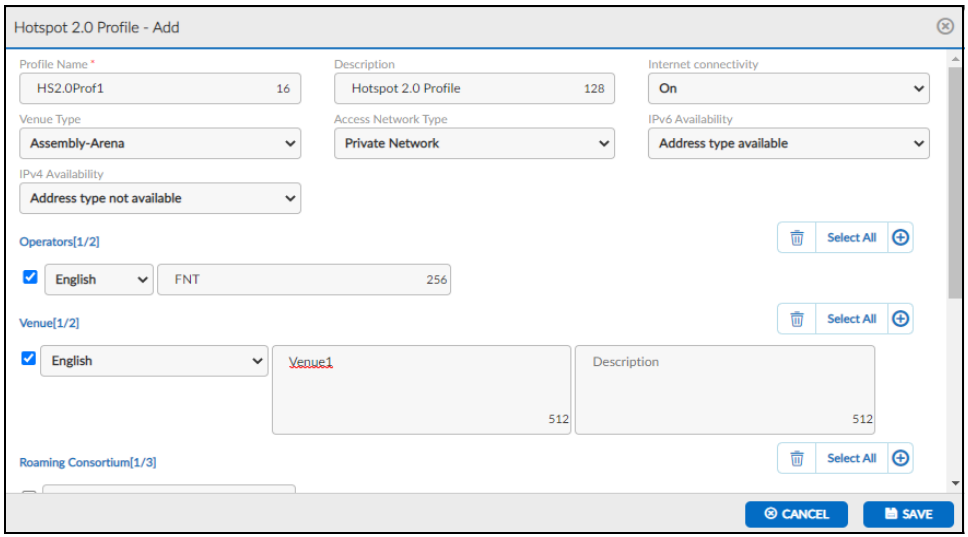
See the ***Configure GRE Tunnels*** in the ***Configuring Security*** chapter of the ***Controller Configuration Guide***, for detailed information on *GRE Profiles*.

Hotspot 2.0

Hotspot 2.0 is a specification by the Wi-Fi Alliance that specifies a framework for seamless roaming between WiFi networks and Cellular networks. The specification is based on the IEEE802.11u standard; a Generic Advertisement Service (GAS) that provides over-the-air transportation for frames of higher layer advertisements between stations APs and external information servers. This feature will allow users to configure hotspot profiles that can (optionally) be connected to existing ESS Profiles as desired. An ESS-profile connected to a hotspot profile will advertise 802.11u capabilities in its beacons.

Adding a Hotspot 2.0 Profile

The Hotspot Profiles can be created from the *Configure* > *Templates* > *Hotspot 2.0* page. By default, the page shows the following details about a Hotspot profile.



- **Hotspot Profile Name** - Displays the name of the Hotspot Profile.
- **Description** - Displays the Description provided for the Hotspot profile.
- **Venue Type** - Displays the Venue Type and Description.
- **Access Network Type** - Select the Access Network Type from the list. The default selection is displayed as Private Network. The types are as follows:
  - Private Network
  - Private Network with Guest Access
  - Chargeable Public Network
  - Free Public Network
  - Personal Device Network
  - Emergency Services Only Network
  - Test or Experimental Network
  - Wildcard Network
- **Internet connectivity -** Enable to advertise whether internet connectivity is available or not at the AP from beacons and probe responses.
- **IPv6 Availability** - Select the IPv6 Availability from the list. The default selection is displayed as Address type not available. The types are as follows:
  - Address type available
  - Address type not available
  - Availability of the Address type not known

- **IPv4 Availability** - Select the IPv4 Availability from the list. The default selection is displayed as Address type not available. The types are as follows:
  - Address type available
  - Address type not available
  - Availability of the Address type not known
  - Port-restricted IPv4 address available
  - Single NATed private IPv4 address available
  - Double NATed private IPv4 address available
  - Port-restricted IPv4 address and single NATed IPv4 address available
  - Port-restricted IPv4 address and double NATed IPv4 address available
- **Roaming Consortium** - Enter the roaming ORG ID for the Hotspot profile. The valid range is 0-10 characters.
- **Operators** - Enter multiple network operators. Select a language and enter a name. The valid range is 0 - 256 characters.
- **Venue** - Enter multiple hotspot venues. Select a language and enter a name. The valid range is 0 - 256 characters.
- **3GPP Cell Network** - Provide the following details:
  - Country code of the operator.
  - Provide the 3GPP Cell Network MCC. The default value is displayed is 0. The Valid range is [0-999].
  - Provide the 3GPP Cell Network MNC. The default value is displayed is 0. The Valid range is [0-999].
- **Domain Name** - Provide the Domain Name. The valid range is [0-128] chars.
- **NAI Realm from 1-10** - Provide the NAI Realm [1-10] from the list. The valid range is [0-50] chars.
- **NAI Realm Auth Method from 1-10** - Select the NAI Realm Auth Method [1-10] from the list. The valid range is [0-50] chars. The types are as follows:
  - EAP TLS Certificate
  - EAP TTLS MSCHAPv2 Username/Password
  - EAP SIM
  - EAP AKA
  - EAP AKA`
- **Advanced Settings** - Provide the following configuration details for advanced settings:
  - HESSID - An AP's Homogenous ESS Identifier (HESSSID), which is that device's MAC address in colon-separated hexadecimal format.
  - GTK Per Station - Enables the Group Temporal Key (GTK) to be assigned per station.

- Gas Come Back Flag - Enables the Generic Advertisement Service (GAS) comeback request/response option.
- Gas Come back Delay (millisecs) - At the end of the GAS comeback delay interval, the client can attempt to retrieve the query response using the comeback request action frame.
- ASRA Flag - Enable the Additional Step Required for Access (ASRA) to indicate that the network requires one more step for access.
- Authentication type - Configure the network authentication type required as per ASRA. Supported values are, Acceptance of terms and conditions, On line enrolment supported, http/https redirection, and DNS redirection.
- Redirect URL - Specify the Redirect URL in case of http/https redirection and DNS Redirection.

- **WAN Metrics** - Provide the following configuration details for WAN metrics:
  - Link Status State - Select the status of the WAN link.
  - Symmetric Link - Enable symmetric bandwidth.
  - At Capacity - Select whether the WAN link is at capacity and no additional mobile devices will be allowed to associate with the AP.
  - Down Link speed/Up Link speed - The WAN Backhaul link for current downlink/uplink speed in KBPS.
  - Down Link load/Up Link load - The current percentage load of the downlink/uplink connection, measured over an interval the duration of which is reported by the Load Measurement Duration.
  - Load Measurement Duration - The duration over which the downlink/uplink load is measured in KBPS.
  - Connection CapabilityThe Connection Capability enables filtering of protocols, allowing or restricting traffic on some protocols and ports. A set of system defined protocols as listed. Additionally, you can also create rules for custom protocols.
- **QoS Map** - Create a Quality of Service (QoS) policy by configuring the following DSCP ranges and DSCP exceptions.
  - DSCP Ranges - For a given DSCP range, specify the User Priority (valid range: 0 -7), DSCP High Priority (valid range: 0 - 255), and DSCP Low Priority (valid range: 0-255).
  - DSCP Exceptions - For a given DSCP exception, specify the User Priority (valid range: 0 -7) and the DSCP Value (valid range: 0 - 255).
- **OSU Settings** - The Online Sign Up (OSU) Service settings configures one or more Hotspot providers offering OSU service.
  - Online Sign Up Support - Select to enable OSU.
  - OSEN Enable - Enable OSU Server-only authenticated layer-2 Encryption Network (OSEN) to indicate that the hotspot uses a OSEN network type. This network provisions clients using the OSU functionality.

- OSU/OSEN ESSID - Specify the OSU ESSID.
- OSU Server URL - Specify the URL of the OSU server.
- OSU NAI - Specify the OSU NAI for authentication.

Click Settings to configure the OSU provider settings.

- OSU Provider Friendly Names
- OSU Provider Icons
- OSU Provider Method - Select one of the OSU provider provisioning methods, OMA-DM or SOAP-XML.
- OSU Provider Description - The description of the OSU Provider.

- The following third party configurations are supported.
  - SVR Device Type
  - SVR Device Model Number
  - Aggregation AAA
  - BW Class
  - Venue Id

Select **OK**. The Hotspot Profile is added and displayed on the Hotspot Profile screen.

The following operations ca be performed on the Hotspot 2.0 profile.

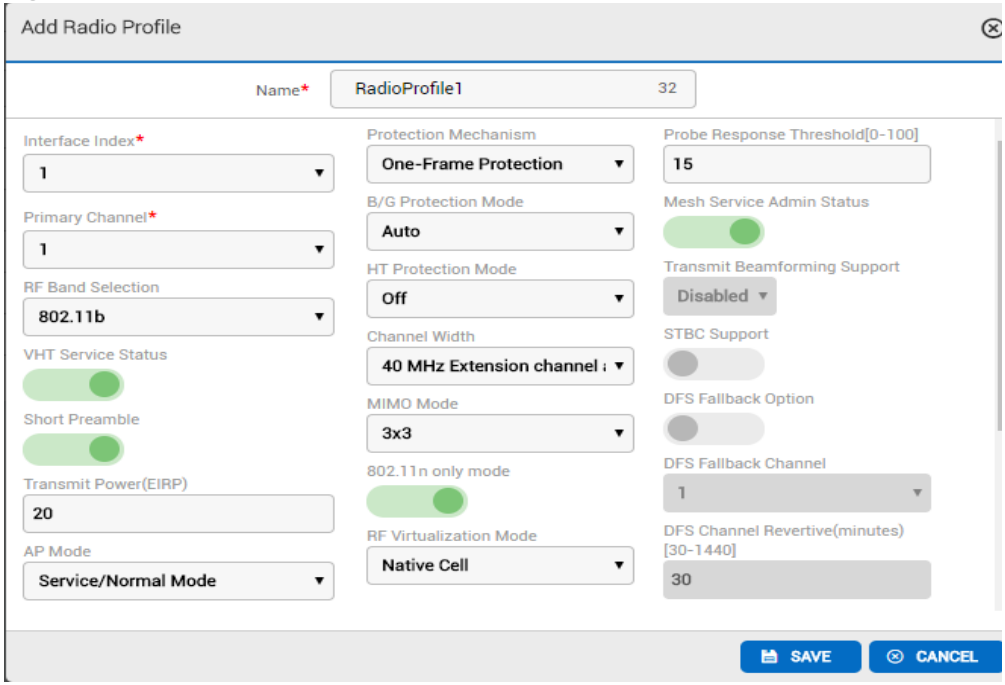
- **Delete** - Select a Hotspot Profile and click **Delete**. The selected Hotspot Profile gets deleted from the Hotspot Profile screen.
- **Edit** - Select a Hotspot Profile and click **Edit**.
- **View** - Allows to view the details of the Hotspot Profile. Select a Hotspot Profile and click **View**.

Radio

An AP comprises of either two or three radios. Each Radio Profile can be configured individually via the controller or *NM*. A radio profile comprises of the configuration parameters which is applied on the wireless interface of the AP. To create independent radio profiles, follow these steps:

1. Navigate to *Configure* > *Templates* > *Radio* > *Add*.
2. In the *Radio Profile - Add* screen, provide the details for *Radio Profile Name*, *Interface Index*, *Primary Channel, RF Band Selection, Short Preamble, Transmit Power High (dBm), AP Mode, Protection Mechanism, Protection Mode, Channel Width, MIMO Mode (MIMO mode is not supported in 8.3 release)* and other options.

Figure 135: *Radio Profile - Add*



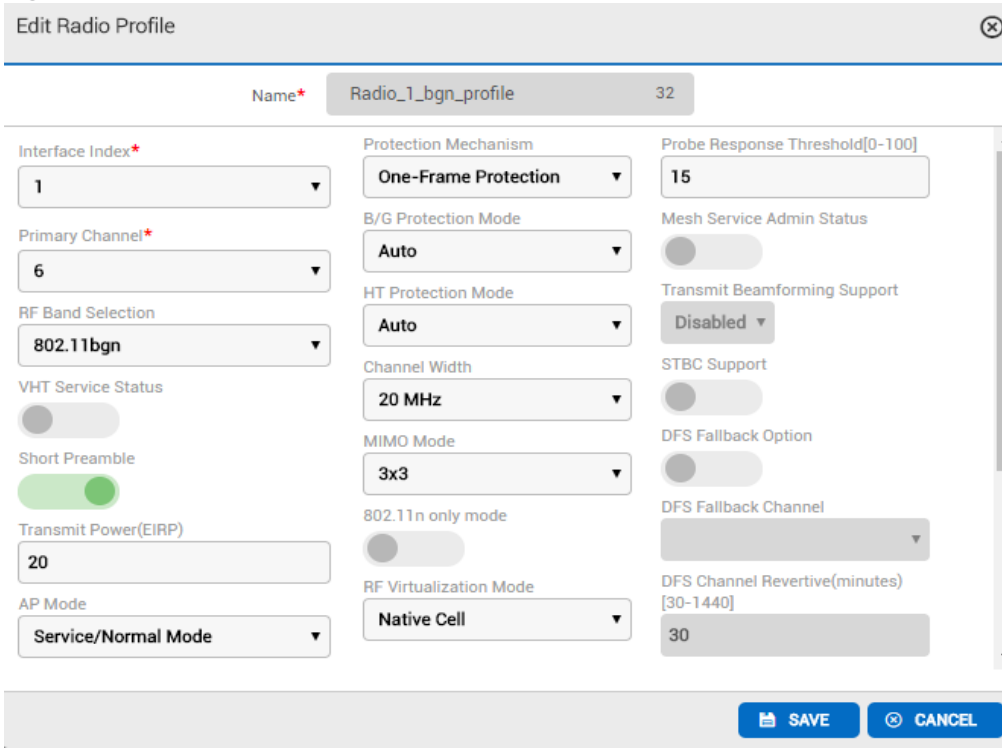
3. Select *Save*. The new *Radio Profile* is included and is displayed on the *Radio Profile* screen.

See the ***Radio Profile - Add*** screen in the Online Help for detailed information on *Radio Profile* topic.

Update the Radio Profile

1. Navigate to *Configure > Templates > Radio > select a radio profile by selecting a check box > Edit*
2. In the *Radio Profile - Update* screen, modify the *Primary Channel, RF Band Selection, Short Preamble, Transmit Power High (dBm), AP Mode, Protection Mechanism, Protection Mode, Channel Width, MIMO Mode* and other options.

Figure 136: *Radio Profile - Update*



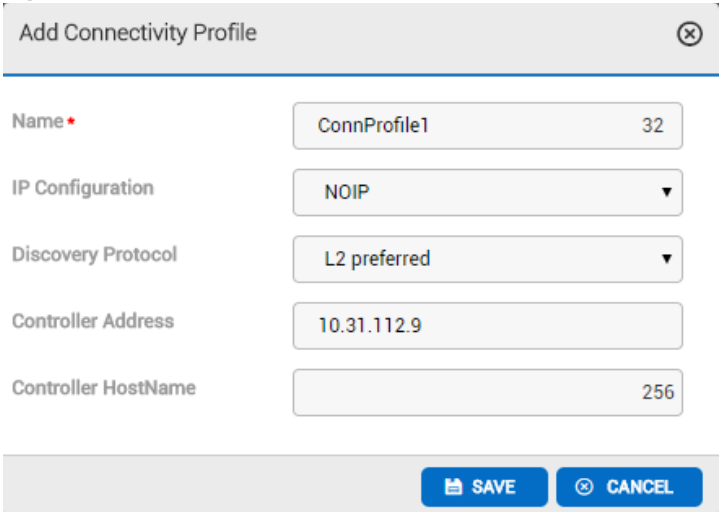
3. Select *Save*. The updated Radio Profile is included and is displayed on the *Radio Profile* screen.
   See the ***Radio Profile - Update*** screen in the Online Help for detailed information on *Radio Profile* topic.

Connectivity

A *Connectivity Profile* comprises of AP configuration parameters related to Network Connectivity. Profiles can be created and applied to a set/group of APs from the *NM* server. To create independent Connectivity profiles, follow these steps:

1. Navigate to *Configure* > *Templates* > *Connectivity* > *Add*.
2. In the *Connectivity Profile - Add* screen, provide the details for *Connectivity Profile Name, IP Configuration, Discovery Protocol, Controller Address and Controller Host Name box.*

Figure 137: *Connectivity Profile - Add*



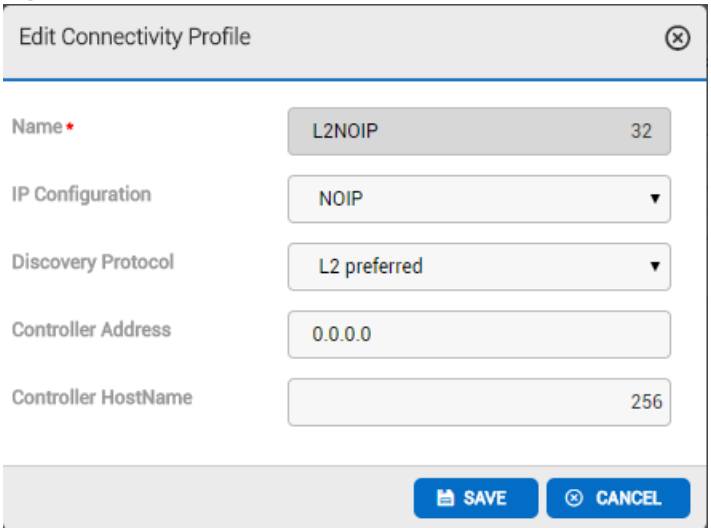
3. Select *Save*. The new Connectivity Profile is included and is displayed on the *Connectivity Profile* screen.

See the ***Connectivity Profile - Add*** screen in Online Help for detailed information on *Connectivity Profile* topic.

Update the Connectivity Profile

1. Navigate to *Configure* > *Templates* > *Connectivity* > *select a Connectivity Profile by selecting a check box* > *Edit option*.
2. In the *Connectivity Profile - Update* screen, modify the *Connectivity Profile Name, IP Configuration, Discovery Protocol, Controller Address and Controller Host Name box*.

Figure 138: *Connectivity Profile - Update*



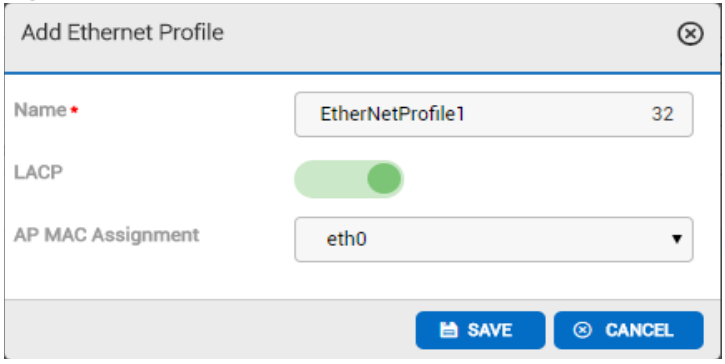
3. Select *Save*. The updated Connectivity Profile is included and is displayed on the *Connectivity Profile* screen.

See the *Connectivity Profile - Update* screen in Online Help for detailed information on *Connectivity Profile* topic.

Ethernet

An Ethernet Profile allows you to configure LACP settings which can be applied via an AP template.

Figure 139: *Add New Ethernet Profile*



To create an Ethernet profile:

1. Go to *Configure* > *Templates* > *Ethernet* and click the '+' icon on the page.

2. In the **Ethernet Profile - Add** page, enter a name to identify the profile and select option to enable LACP.
3. Select the AP MAC assignment from the drop-down list.
4. Click **SAVE**.

To apply an Ethernet profile to an AP, the profile must be added to an AP template.

1. Go to *Configure* > *Design-Features* > *AP Template* and select an AP template.
2. In the **AP Template: <*template-name*> - Update** page, select the Ethernet Profile from the drop-down list and click **SAVE**.

DHCP

Configure a DHCP server that can be operated directly from the controller. This configuration is ideal for relatively small deployments that do not require a separate server to handle DHCP duties. This can be particularly useful for deployments that require a DHCP sever for a separate VLAN (such as one used for a guest network) but also would prefer not to allow that traffic to impact the corporate DHCP server.

Creating a DHCP Server

The controller can have multiple different DHCP servers configured on it at any given time. A DHCP server can be associated to only one VLAN. The steps below can be repeated in order to configure different DHCP servers for separate VLANs or Virtual Interface Profiles as needed.

You can now create DHCP configurations from FortiWLM and deploy them to controllers. The default DHCP configuration page, *Configure* > *Templates* > *DHCP*, lists all online controllers with the IP address. To create DHCP configuration for a controller, select the controller and click the arrow button in the Action column.

Figure 140: *DHCP servers*

In the resultant page, click **DHCP server** and then click the **Add** button.

Figure 141: *DHCP IPv4 configuration*

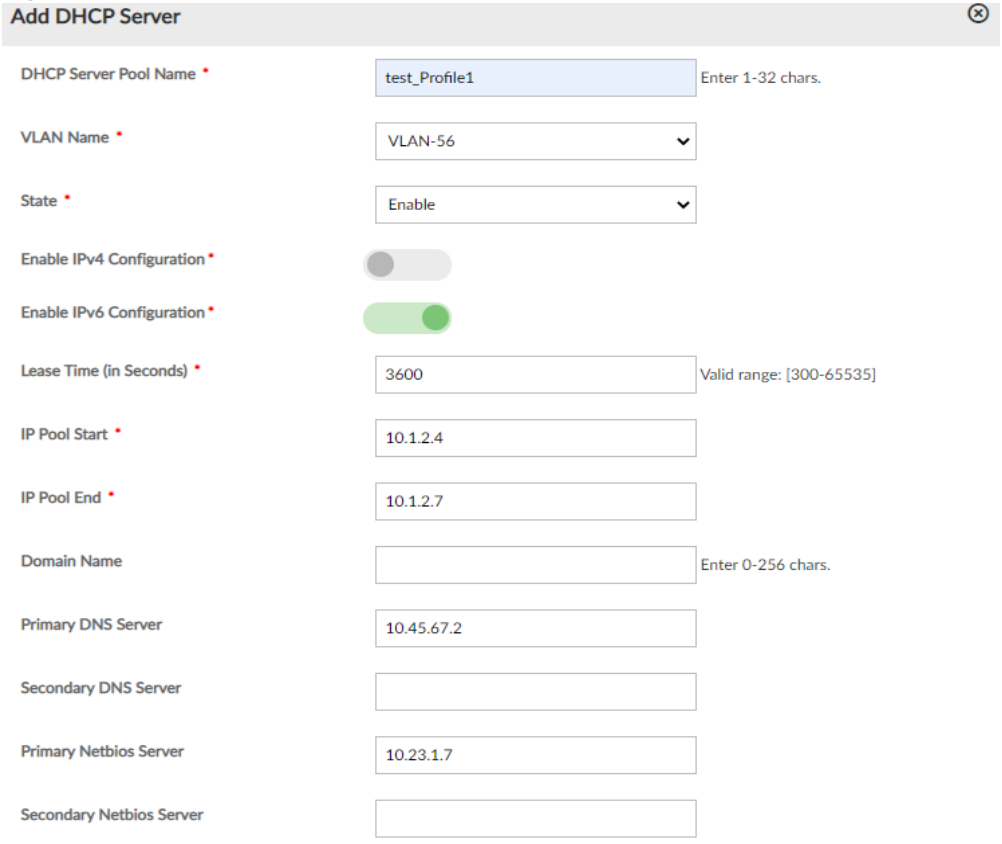
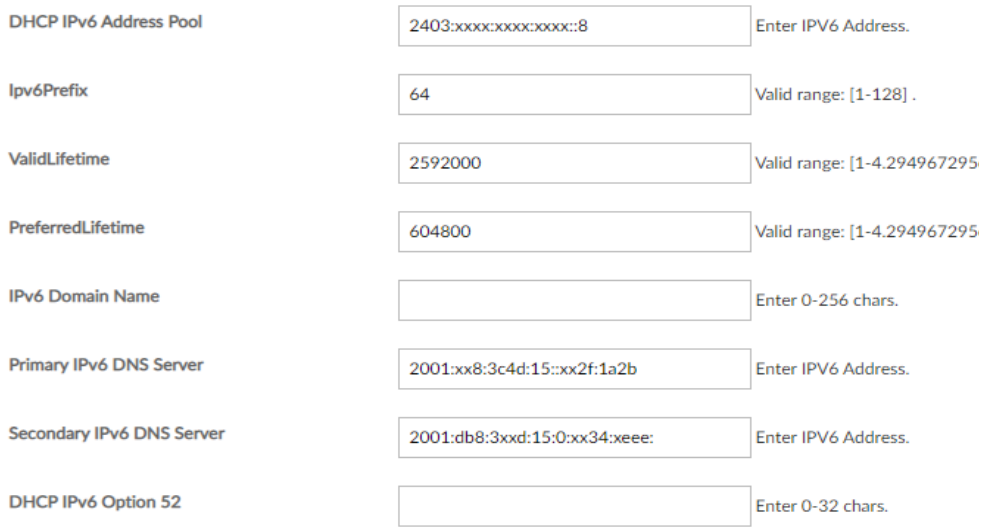


Figure 142: *DHCP IPv6 configuration*



The following table describes the DHCP server information provided. Note that the table will only be displayed after at least one DHCP server entry has been created.

Option	Description
DHCP Server Pool Name	Enter a name to be ascribed to the DHCP Server.
VLAN Name	This drop-down list allows you to select a VLAN to which the server should be applied. Note that this is only available if the controller is operating in Layer 2 routing mode.
State	Set to Enabled in order to activate the DHCP server, Disabled to deactivate it.
Lease Time	The duration of IP leases that are assigned by the DHCP server. This value is displayed in seconds.
IP Pool Start/End	The start and end IP addresses of the IP pool that may be assigned by the DHCP server.
Domain Name	The domain on which the DHCP server will be active.

Option	Description
Primary/Secondary DNS Server	The primary and secondary DNS servers to be used by the DHCP server.
Primary/Secondary Netbios Server	The primary and secondary Netbios servers to be used by the DHCP server.
DHCP Option 43	Option 43 allows you to manually specify the primary and secondary controllers to be used by the server. Enter the primary and secondary controller IP addresses (separated by a comma) in this field.
DHCP IPv6 Address Pool	The IPv6 addresses that the DHCP server assigns.
IPv6Prefix	The IPv6 address prefix. The valid range is 1 -128.
ValidLifetime	The duration that an IP address remains in the valid state and can be used for new or existing communications. When the valid-lifetime expires, the address becomes invalid and can no longer be used. **Note**: The value of PreferredLifetime must be less than the ValidLife-time when configured together.
PreferredLifetime	The duration that a valid IP address is in the preferred state and can be used without any constraints. When the preferred-lifetime expires, the address is deprecated. The default is 604800 seconds.
IPv6 Domain Name	The IPv6 Domain name for the DHCP server.
Secondary DNS Server/Secondary IPv6 DNS Server	The primary IPv6 DNS server used and secondary server in case the primary is unreachable.
DHCP IPv6 Option 52	Configure Option 52 on the DHCP server in an IPv6 deployment.

Additionally, select the configured DHCP server and click **Delete** to delete the server, click **Settings** to reconfigure the server, and click **View Details** to view a summary of the server configurations.

Mesh

The Mesh configuration page lists all online controllers. To create a mesh configuration on a controller, click the arrow button in the Action column.

In the resultant page, click the **Add** button to create the Mesh configuration.The *Configure* > *Templates* > *Mesh* table describes the current mesh configuration. Note that the table will only be displayed after at least one Mesh network has been created.

- Name: Enter a name for the mesh profile.
- Description: Enter a brief description for the profile (e.g., its location).
- Pre-shared Key: Enter an encryption key for mesh communications. This key will be shared automatically between APs that have been added to the mesh profile; the user will not be required to input it manually later on. This key must be between 8 and 63 characters.
- Admin Mode: Setting this field to Enable activates the mesh profile. If the profile needs to be disabled for any reason, set this field to Disable.
- PlugNPlay Status: This option allows APs to be added to the mesh by eliminating the the need to have them wired connected during mesh configuration.

Deleting the Mesh profile
Select the mesh profile and click **Delete**.

Reconfigure a Mesh profile
Select the mesh profile and click **Settings**. Modify the configuration as required.

Review additional Mesh information
Select the server and click **View Details**. The resulting page displays a quick summary of the mesh configuration.

VPN Configuration

FortiWLM supports configuring access points to connect to the controller via the Virtual Private Network (VPN), allowing a secure remote wireless connection.

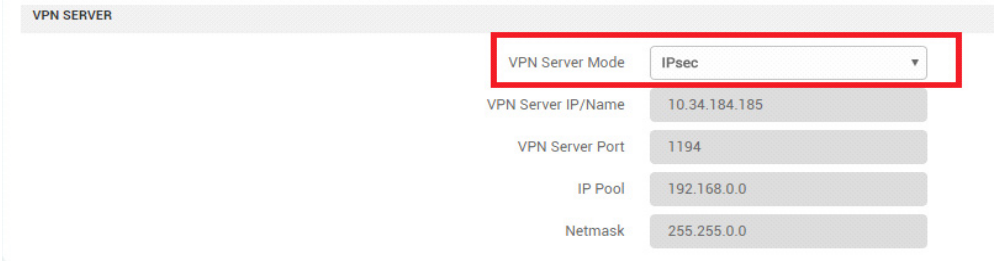
In order to configure an access point for VPN support, it must first be connected to the network so that it can be populated into the controller AP table. The access point's secure VPN connection requires the use of a security certificate. Ensure that the certificates are configured.

In addition to OpenVPN (SSL), the **IPSec** mode is also supported while configuring VPN. This mode enables encryption of all traffic between the AP and controller (both the control and data path).

Note: [VPN with NPlus1] Configure the VPN client before configuring NPlus1 in secondary controller.

Navigate to *Configure* > *Templates* > *VPN Configuration*

Figure 143: *.Configure the VPN server mode*



To configure VPN, click the **Action** icon for a specific controller and update the following parameters.

Field	Description
VPN Server Mode	Select the VPN server encryption mode. • **None** – This is the default option selected for the access point. No encryption is applied. • **IPSec** – This mode enables encryption of all traffic between the AP and controller (both the control and data path). • **OpenVPN** Update the following fields only when the server mode is **OpenVPN**.
VPN Server IP/ Name	Enter an IP address or DNS name to be used by the VPN server.
VPN Server Port	Enter the port to be used for VPN communications. This is the port on which the VPN server is waiting for the incoming request. The valid range is between 0 - 65535. The default is 1194.
IP Pool	Enter the IP range that can be used by the VPN server (in standard 255.255.255.255 (notation). It is the range of IP address from which the tunnel IP is assigned. The default is 192.168.0.0. **Note:** Ensure that the IP from which you are accessing the controller (i.e., your current machine's IP address) is not included in this range. If it is, your local connection will be terminated once VPN is enabled.
Netmask	Enter the netmask for the VPN server (in standard 255.255.255.255 notation). The default is 255.255.255.0.

VPN APs

Prior to using any access points for VPN, the VPN server must be enabled and access points must be added to the VPN table. In order to activate VPN for an access point, an x.509 certificate must be installed on it. This table displays which access points are ready for VPN and allows you to easily install a certificate for those that are needed.

To activate VPN for an access point, select it and click **Activate**.

Field	Description
AP ID	The identification number assigned to the access point.
AP Name	The name assigned to the access point.
MAC Address	The access point's MAC address.
Operational State	Enabled (if the access point is active and connected) or Disabled (if the access point is disconnected or deactivated).
Availability Status	Online (if the access point is active and connected) or Offline (if the access point is disconnected or deactivated).
AP Model	The access point model.
Certificate Status	In order to permit VPN operation, selected access points must have a security certificate installed on them. If this certificate is not present, this column indicates by displaying appropriate message. For example, Not-Installed is displayed in the absence of a certificate, Unknown is displayed when the certificate status cannot be obtained due to access point connectivity issues.
VPN Validation	Indicates whether a certificate is present on the access point or not. If not, the Certificates Not Available message appears, indicating that a certificate must be installed.
Action Required	If a certificate is not present for an access point, this column prompts you to upload a certificate from FortiWLC.

VPN Status

The VPN Status table displays all active VPN access points.

Field	Description
AP ID	The identification number assigned to the access point.
AP Name	The name assigned to the access point.
MAC Address	The access point's MAC address.
VPN Connectivity Status	Displays whether the AP is actively connected via VPN.
VPN Authentication status	Displays whether the AP is authenticated via VPN connection.
Real IP Address	The IP address that is visible externally.
VPN IP Address	The private IP address used by the access point. This is not visible externally.

To delete VPN access, select the access point and click **Remove**.

Beacon Services

Fortinet Beacon Services use iBeacon to allow mobile application (iOS and Android devices) to receive signals from beacons in the physical world to deliver hyper-contextual content to users based on location. Bluetooth Low Energy (BLE) is the wireless personal area network technology used for transmitting data over short distances. Broadly, the Beacon Service requires a Bluetooth based iBeacon device to broadcast signals and a mobile application to receive these signals once it comes in the configured proximity. You can now create multiple Beacon Service profiles and map APs to a specific profile.

The Beacon services are available by default in FAP U421EV, FAP U423EV, FAP U321EV and FAP U323EV. For other non-wave2 APs, you will need Bluetooth adapters (For example: Broadcom USB Class 2 Bluetooth 4.0 Dongle, CSR 4.0 Bluetooth Dongle and Iogear Bluetooth 4.0 USB Micro Adapter GBU521). Ensure that Bluetooth adapters support Bluetooth version 4.0 or above.

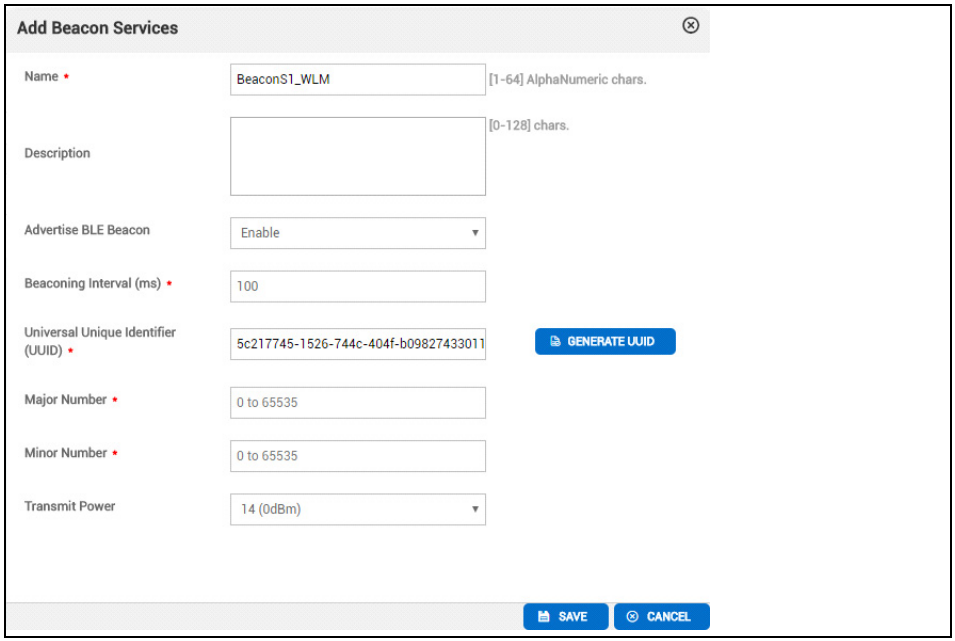
Note:
Access points must be connected to 802.3at power supply.

On upgrading the FortiWLM from a previous version to the latest, the existing Beacon profiles in FortiWLM are unregistered from the Controller.

You can perform the following operations to manage the Beacon Services. Navigate to *Configure > Templates > Beacon Services.*

Adding Beacon Services Profiles

This option allows you to add a **Beacon Service**. You can create multiple Beacon Service profiles and also map APs to a specific profile.
APs part of a profile send iBeacons that will help advertise hyperlocal content to users in context to their location.



- **Name** – Unique name for this **Beacon Service** profile. The supported range is 1-64 alphanumeric characters.
- **Description** – A description of the created Beacon Service. The supported range is 0-128 characters.
- **Advertise BLE Beacon** – Enables the BLE beacons to advertise packets received by devices. These packets determine the location of the device with respect to the Beacon.
- **Beaconing Interval (ms)** – Select the time interval at which the Beacons transmit signals to associated devices, that is, this sets the rate at which beacons advertise packets. Setting

the beacon interval to a higher value decreases the frequency of unicasts and broadcasts sent by the AP. The supported range is 100-1000 milliseconds.

- **Universal Unique Identifier (UUID)** – Click **Generate UUID**, to receive a UUID that is specific to the beacon. The purpose of the ID is to distinguish iBeacons in your network from all other beacons in other networks not monitored by you.
- **Major Number** – This number is assigned to some beacons in a network and is used to distinguish this subset of beacons within a larger group of beacons. For example, beacons within a particular geographic area can have the same major number. The supported range is 0 to 65535.
- **Minor Number** – This number is assigned to identify individual beacons. For example, each beacon in a group of beacons with the same major number, will have a unique minor number. The supported range is 0 to 65535.
- Transmit Power – Select a power level for the beacon's transmit signal. The higher the power, the greater will be the range of your signal. The supported range is 0 (-29 dBm) to 15 (4dBm).

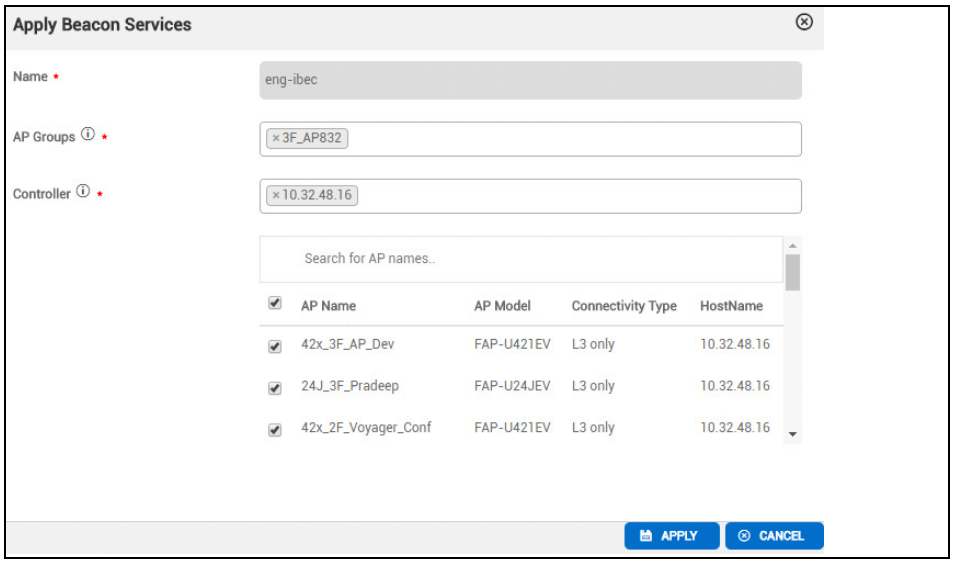
Enabling Beacon Services Profiles

Select the Beacon Services profile and click  in the **Action** column to enable the profile.

Applying Beacon Services Profiles to APs

Select the **Beacon Services** profile and click  in the **Action** column to apply the profile to specific APs. You can apply the profile to all APs of a Controller or to specific APs. These are the supported options:

- **AP Groups** - Select a group from the drop-down list. The profile is pushed only to the APs in the AP Group.
- **Controller** - Select the Controller from the drop-down list and select the supported APs. The profile is pushed to the selected APs.



Note: Controller versions 8.3.0 and above are supported. The list of APs is available only in FortiWLM 8.3.3 and later.

Editing Beacon Services Profiles

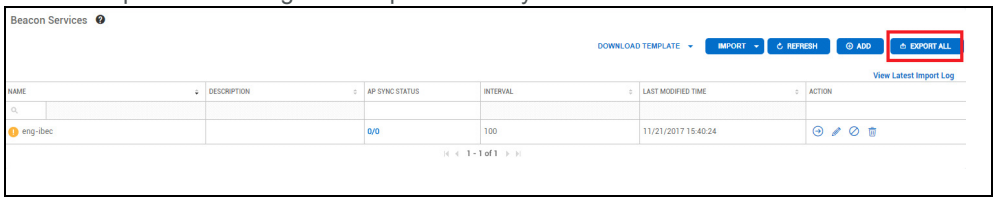
Select the Beacon Services profile and click in the Action column to edit the values for an existing profile.

Deleting Beacon Services Profile

Select the **Beacon Services** profile and click in the **Action** column to delete the profile.

Exporting Beacon Services Profiles

You can export the existing Beacon profiles into your local drive.



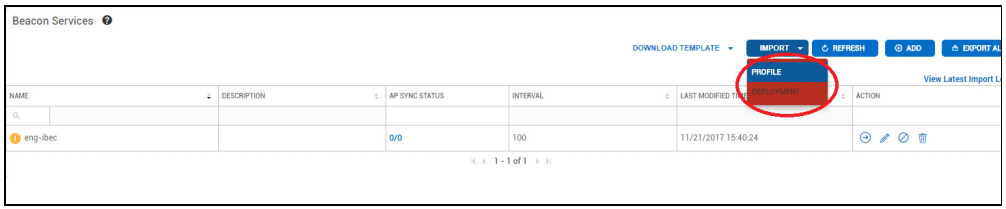
Note:

The **Export All** option exports the Beacon profiles, but does not export the associated APs.

Importing Beacon Services Profiles

You can load Beacon Services profiles by importing files (*.csv) from your local drive.

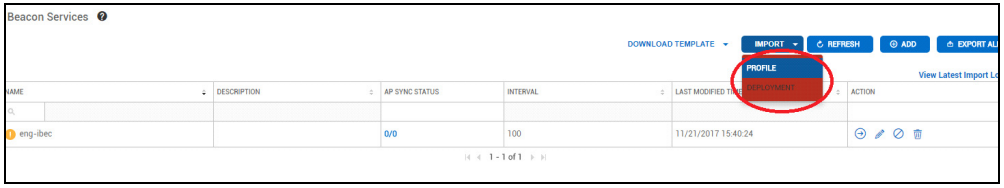
Use the **Download Template** option to download the default **Profile** and **Deployment** templates.



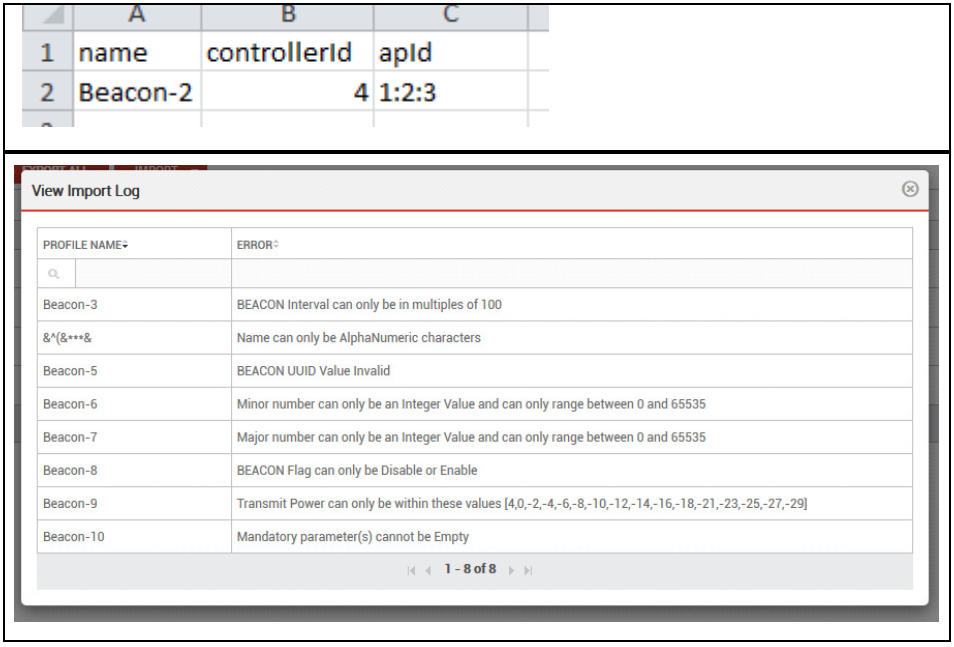
Edit and save these templates.

	A	B	C	D	E	F	G	H
1	name	uniqueidentifier	interval	minornumber	majornumber	descr	blebeacon	transmitpower
2	Beacon-3	545f4426-2896-0785-2c75-97d178e2a613	400	45	56		Enable	-18

Click **Import** and browse to the saved *.csv template file (**Profile** or **Deployment**).



In case of errors, view the import logs using the **View Latest Import Log** option for error details.



	A	B	C
1	name	controllerId	apId
2	Beacon-2	4	1:2:3

View Import Log

PROFILE NAME	ERROR
Beacon-3	BEACON Interval can only be in multiples of 100
&^(&***&	Name can only be AlphaNumeric characters
Beacon-5	BEACON UUID Value Invalid
Beacon-6	Minor number can only be an Integer Value and can only range between 0 and 65535
Beacon-7	Major number can only be an Integer Value and can only range between 0 and 65535
Beacon-8	BEACON Flag can only be Disable or Enable
Beacon-9	Transmit Power can only be within these values [4,0,-2,-4,-6,-8,-10,-12,-14,-16,-18,-21,-23,-25,-27,-29]
Beacon-10	Mandatory parameter(s) cannot be Empty

1 - 8 of 8

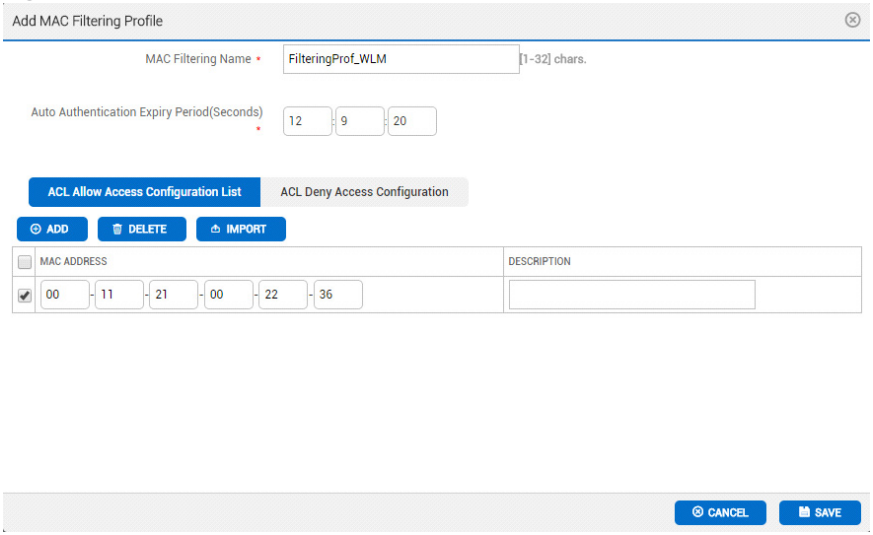
Select the **Apply Beacon Services** option to apply these to the APs.

MAC Filtering

MAC filtering controls a user station's access to the WLAN by permitting or denying access based on specific MAC addresses. A MAC address is unique to each IEEE 802-compliant networking device. In 802.11 wireless networks, network access can be controlled by permitting or denying a specific station MAC address, assigned to its wireless NIC card, from attempting to access the WLAN.

For more information on MAC Filtering, refer to the *FortiWLC Configuration Guide*.

Figure 144: *Add a MAC Filtering profile*



The Wireless LAN System provides MAC filtering using the following methods:

- **ACL Allow Access Configuration List**, which limits access to only those MAC addresses on the permit list
- **ACL Deny Access Configuration**, which specifically disallows access to those addresses (clients) on the deny list

To import a list of MAC addresses to permit, create a text file listing all the MAC addresses, and import the text file. When creating the text file to be imported, only include one MAC address, in hexadecimal format (***xx***:***xx***:***xx***:***xx***:***xx***:***xx***), per line. For example, the contents of a text file to be imported might look like the following:

```
00:04:23:87:89:71
   00:06:25:a7:e9:11
   00:07:e9:15:69:40
   00:0c:30:be:f8:19
   00:0c:e6:09:46:64
   00:0c:e6:12:07:41
```

To set up a Deny MAC Filtering List, enable the ACL deny state and then either configure a Deny ACL or import a Deny ACL.

A Deny ACL takes precedence over RADIUS Server access, so you can use it to immediately deny access to a station or deny-list certain clients (for example, if they have a virus or are attacking other devices).

To import a list of MAC addresses to deny, create a text file listing all the MAC addresses, and import the text file. When creating the text file to be imported, only include one MAC address, in hexadecimal format (***xx***:***xx***:***xx***:***xx***:***xx***:***xx***), per line. For example, the contents of a text file to be imported might look like the following:

```
00:04:23:87:89:71
   00:06:25:a7:e9:11
   00:07:e9:15:69:40
   00:0c:30:be:f8:19
   00:0c:e6:09:46:64
   00:0c:e6:12:07:41
```

Note:
Active connections do not get disconnected if the ACL environment is changed from Permit to Deny. However, during successive connection the MAC entry is filtered against deny or permit list.

QoS

Quality of Service rules evaluate and prioritize network traffic types. For example, you can prioritize phone calls (VoIP) or prioritize traffic from a certain department (group, VLANs) in a company.

You can configure the following QoS rules and push them to controllers

Global Parameters and Marking Management Packets

Value configured as global parameters and for Marking Management Packets will take precedence over values configured from FortiWLC-SD. When pushed to controller, these values will override the controller values and will be replaced with the parameters configured from FortiWLM.

Global Parameters

1. On/Off: Use this field to toggle whether the global QoS parameters should be enabled. By default, this is set to **On**.
2. Admission Control: Configures how new traffic requests will be handled; by default, this is set to **Admit All**, allowing all traffic to be processed. When set to **Request Pending**, new requests will be on hold until bandwidth resources are available, while **Reject Request** will reject new requests when bandwidth is insufficient.
3. Drop Policy: Specifies whether the drop policy should be configured for **Head** or **Tail**. When set to **Head**, backlogged traffic will be dropped from the head of the queue when the buffer reaches its capacity, while setting it to **Tail** will drop traffic from the tail of the queue.
4. Maximum Calls Per AP: This field specifies the maximum number of calls to be permitted on an individual AP. On a per-call basis, and can range from 0-256.

5. Maximum Calls Per Interference Region: This field specifies the maximum number of calls to be permitted in each interference region present. On a per-call basis, and can range from 0-256.
6. Maximum Stations Per Radio: This field specifies the maximum number of stations to be supported by a single AP radio. On a per-station basis, and can range from 0-128.
7. Maximum Stations Per BSSID: This field specifies the maximum number of stations to be supported by a single BSSID. On a per-station basis, and can range from 0-1023.
8. Native Load Balance Overflow: Setting this option to **On** allows new stations to join the network beyond the maximum allowed per radio in a round-robin fashion. This allows the user to permit for periodic spikes in association traffic and balances the new stations evenly across the deployment. By default, this is set to **Off**.
9. Maximum Calls Per BSSID: This field specifies the maximum number of calls to be supported by a single BSSID. On a per-call basis, and can range from 0-1023
10. CAC Deauth: If set to **On**, this configures the system to send a deauthentication packet to a device attempting to start a call on an AP or BSSID that is currently overloaded with existing call traffic. By default, this is set to **Off**.
11. Station Assignment Aging Time: Specifies the amount of time an assigned station can be idle before being dropped. Measured in seconds, and can range from 5-2000.
12. SIP Idle Timeout: Specifies the amount of time a SIP call can be idle before it is disconnected. Measured in seconds, and can range from 5-3600.
13. Default Time-to-Live: The Time-to-Live (TTL) setting specifies how long a packet is buffered before it may be dropped. Measured in seconds, and can range from 0-65535.
14. UDP Time-to-Live: This TTL setting specifies the duration for UDP-specific traffic. Measured in seconds, and can range from 0-65535.
15. TCP Time-to-Live: This TTL setting specifies the duration for TCP-specific traffic. Measured in seconds, and can range from 0-65535.
16. Bandwidth Scaling: This toggle allows the user to manually constrain the bandwidth used if desired. Measured as a percentage, and can range from 1-100.

Marking Management Packets

You can apply Differentiated Services Code Point (DSCP) values to management traffic.

DSCP value is selectable field that can be used to assign various levels of precedence to network traffic. By default, traffic packets contained an EF value and with the introduction of DSCP you can now change the priority bit from EF to DSCP value. Management traffic between the following can be assigned DSCP values:

- AP to Controller
- Controller to AP
- Controller to Network Manager

Select the DSCP values for each traffic and click the **Save** button.

QoS and Firewall Rules & QoS Codec Rules

These rules start with ID 6000 to differentiate them from FortiWLC-SD rules. In FortiWLM you can combine multiple rules into a profile and push them to controllers.

QoS and Firewall Rule

1. In the ID field, type a unique numeric identifier for the QoS rule. The valid range is from 0 to 6000.
2. In the Destination IP fields, type the destination IP address (IPv4/IPv6) to be used as criteria for matching the QoS rule. The destination IP address is used with the destination subnet mask to determine matching.
3. In the Destination Netmask fields, type the subnet mask or the destination IP address.
4. In the Destination Port field, type the TCP or UDP port to be used as criteria for matching the QoS rule. To specify any port, type 0 (zero).
5. In the Source IP fields, type the source IP address (IPv4/IPv6) to be used as the criteria for matching the QoS rule. The source IP address is used with the source subnet mask to determine matching.
6. In the Source Netmask fields, type the subnet mask for the source IP address.
7. In the Source Port field, type the TCP or UDP port to be used as criteria for matching the QoS rule. To specify any port, type 0 (zero).
8. In the Network Protocol field, type the protocol number of the flow protocol for the QoS rule. The protocol number can be a number 0 through 255. The protocol number of TCP is 6, and the protocol number for UDP is 17. For a list of protocol numbers, see http://www.iana.org/assignments/protocol-numbers.
   If you are also using a QoS protocol detector, you must match the network protocol with the type of QoS protocol. Use the following network protocol and QoS protocol matches:
   - UDP: SIP
   - TCP: H.323 or SIP
9. In the Firewall Filter ID field, enter the filter-ID to be used (per-user or per-ESS), if Policy Enforcement Module configuration is enabled (optional feature). This ID must be between 1 and 16 alphanumeric characters.
10. In the Packet minimum length field, specify the size of the minimum packet length needed to match the rule. (Valid range: 0-1500.)
11. In the Packet maximum length field, specify the size of the maximum packet length needed to match the rule. (Valid range: 0-1500.)
12. In the QoS Protocol dropdown list, select one of the following:
    - SIP
    - H.323
    - Other
    - None

For capture rules, the QoS protocol determines which QoS protocol detector automatically derives the resources needed for the flow (implicitly). Select Other if you want to specify the resource requirements for matched flows explicitly. The QoS protocol value is ignored for non-capture rules.

13. In the Average Packet rate box, type the average flow packet rate. The rate can be from 0 through 200 packets/second.
14. In the Action list, select the action the rule specifies:
    - Forward: A flow is given an explicit resource request, bypassing the QoS protocol detector and regardless of whether a QoS protocol was specified.
    - Capture: The system, using a QoS protocol detector, analyzes the flow for its resource requirements.
    - Drop: The flow is dropped.
15. In the Token Bucket Rate box, type the rate (in Kbps or Mbps, depending on the option checked) at which tokens are placed into an imaginary token bucket. Each flow has its own bucket, to which tokens are added at a fixed rate. To send a packet, the system must remove the number of tokens equal to the size of the packet from the bucket. If there are not enough tokens, the system waits until enough tokens are in the bucket.
16. In the Priority box, type the priority at which the flow is placed in a best-effort queue. Packets in a higher priority best-effort queue are transmitted by access points before packets in lower-priority queues, but after packets for reserved flows.
    Priority can be a value from 0 through 8, with 0 specifying no priority and 8 specifying the highest priority. The default value is 0. If you enable priority (specify a non-zero value), you cannot specify an average packet rate or token bucket rate.
17. In the Traffic Control list, select one of the following:
    - On
    - Off
    - For all types of flows (explicit, detected, and best-effort), selecting On for traffic control restricts the flow to the rate you specified. Packets above that rate are dropped.
18. In the DiffServ Codepoint list, select the appropriate DiffServ setting, if applicable.
19. In the QoS Rule Logging list, select whether to enable or disable logging activity for this QoS rule:
    - On
    - Off
20. In the QoS Rule Logging Frequency field, change the default collection interval in which packets related to this rule are logged, if QoS Logging is enabled. The interval must be a number between 30 and 60 (seconds).
21. Match Checkbox: For any field with the corresponding Match checkbox selected, the action mentioned in the ACTION field is performed on the matched packets. If the match checkbox is not checked, packets with any value are matched regardless of the data in the field and the action mentioned in the ACTION field is not performed on the packets.

22. Flow Class Checkbox: Flow Class options are relevant only for Flow Control rules (rules with Traffic Control enabled and Token Bucket Rate specified) and Firewall rules. This is typically rate limiting. When Flow Class is checked for a field, if a packet has matched a rule (either Flow Control or Firewall types), these fields are stored in the Flow Class entry. A Flow Class entry is used by the system for aggregating a set of flows so that they can be subjected to similar behavior, be it dropping the packets, or rate limiting them.
    For example, if a rule has a Src IP address of 0.0.0.0 and the Flow Class box checked, and Token Bucket Rate set to 10 kbytes/sec, all packets passing through the system must match this rule, and each flow will be allowed a maximum throughput of 10000 bytes/sec. If the rule were to have Src IP address of 10.0.0.10 and the Flow Class box checked, with a Token Bucket Rate of 10 kbytes/sec, all packets coming from a machine with IP address 10.0.0.10, must match this rule, and the cumulative throughput allowed for this machine shall be no more than 10000bytes/sec.
23. To add the QoS rule, click **Save**.

QoS Codec Rules

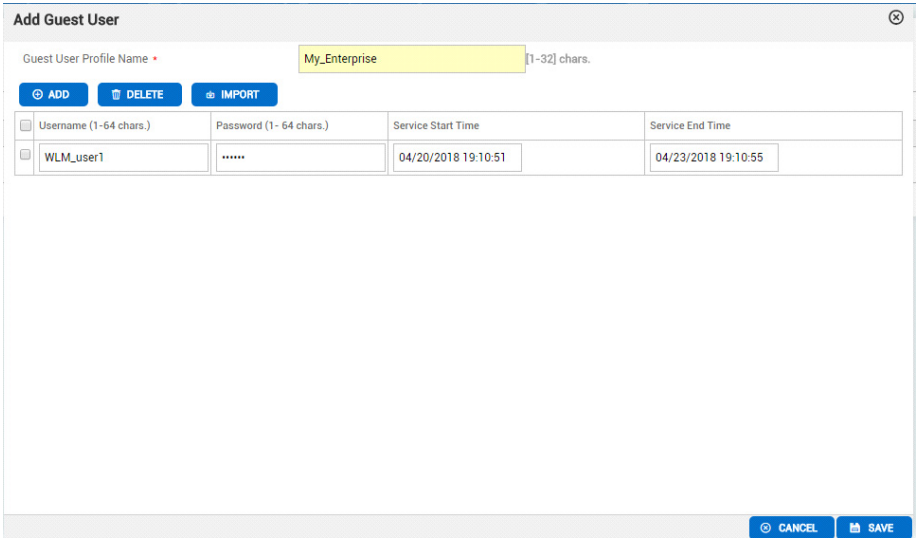
1. In the ID box, type an integer (0-6000) for the QoS Codec rule.
2. In the Codec list, select the Codec type.
3. In the Token Bucket Rate box, type the token bucket rate. The valid value range is 0 to 1,000,000 bytes/second.
4. In the Token Bucket Size box, type the token bucket size. The valid value range is from 0 to 16,000 bytes.
5. In the Peak Rate box, type the traffic peak rate. The valid value range is 0 to 1,000,000 bytes/second.
6. In the Maximum Packet Size box, type the maximum packet size. The valid value range is 0 to 1,500 bytes.
7. In the Minimum Policed Unit box, type the minimum number of policed units. The valid value range is 0 to 1,500 bytes.
8. In the Reservation Rate box, type the reservation rate. The valid value range is 0 to 1,000,000 bytes/second. The default value is 0 bytes/second.
9. In the Reservation Slack box, type the reservation slack. The valid value range is 0 to 1,000,000 microseconds.
10. In the Packet Rate box, type the packet rate. The valid value range is 0 to 200 packets/second.
11. In the QoS Protocol list, select which QoS protocol detector is used to derive resources needed for the flow.
    - SIP
    - H.323

To add the QoS Codec rule, click **Save**.

Guest Users

You can add profiles with a list of guest users that can connect via captive portal based as per the rule defined for the guest user profile.

The guest user profile specifies the total time that the guest users can be connected to your network.



To create a guest user profile, navigate to *Configure* > *Templates* > *Guest Users* and click the **ADD** button and update the following:

- Guest User Profile Name
- Username and Password for this user.
- Specify the time limit for the user to be connected to your network in Service Start Time and Service End Time.

Click **Save** to complete the process.

Now, assign the guest user profile to a controller. Select the required guest user profile and click the apply arrow icon to specify the controller IP address.

Location 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 in your network.

For non-wave2 APs, you will need Bluetooth adapters (for example: *Broadcom USB Class 2 Bluetooth 4.0 Dongle, CSR 4.0 Buletooth Dongle, Iogear Bluetooth 4.0 USB Micro Adapter GBU521*). Ensure that Bluetooth adapters support Bluetooth version 4.0 or above.
NOTE:

- Access points must be connected to 802.3at power supply.
- After upgrading to 8.5.0 from pre-8.4.1, disable and enable the location service profile, in case the location service is running.

Location Services Profiles (FortiWLC)

A default Location Services profile, *WLM_Locationing*, exists in FortiWLM with this configuration. You can enable and use the default profile.

- Report Format – Forti-Presence
- Project Name – FWLM
- Secret – The secret key displayed in *Administration* > *System Settings* > *Maintenance*.

Note:

In a HA setup, by default the primary server IP address is configured as the **Server IP Address.** Modify this to the VRRP IP address before enabling the default profile.

Fortinet recommends that you create a **new** location services profile with the following configuration:

- Location Services Feed: **Enable**
- Report Format: **Forti-Presence**
- Project Name: **FWLM**
- Secret: The secret key displayed in **Administration > System Settings > Maintenance.**
- Source Type: **ALL** or **WIFI**
- Server IP Address: FortiWLM IP address (VRRP IP address in case of HA)
- Server Port: **4013**
- Report Interval: **5**

Notes:

- For any modifications to the location services profile to be pushed successfully to the controller, disable and enable the modified profile.
- Only **Forti-Presence** report format is supported.

Figure 145: *Location Service profiles*

The following actions can be performed on the **Location Services** screen:

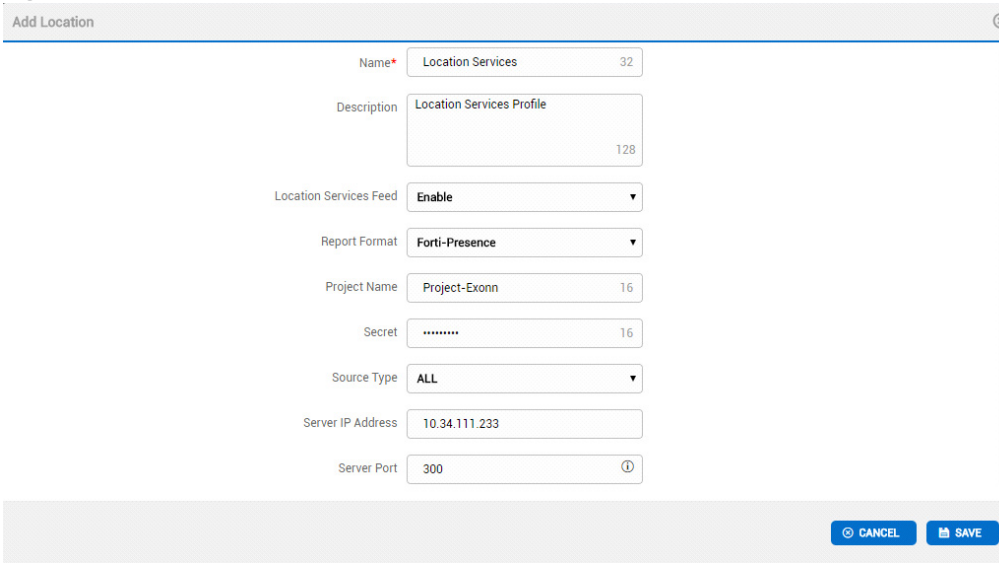
Action	Description
Add	**Add** allows to add a **Location Services Profile**.
Apply	**Apply** allows to apply a **Location Services Profile** to specific Controllers.
Edit	**Edit** allows to edit a **Location Services Profile**.
Enable/Disable	**This option** allows you to enable/disable a **Location Services Profile**. A disabled profile is not deleted and can be enabled again.
Delete	**Delete** allows deleting a **Location Services Profile**.

Adding Location Services Profile

Perform the steps in this section to add a new location service profile.

1. Navigate to **Configure > Templates > Location Services**. The **Location Services** screen is displayed.
2. Select **Add**. The **ADD - Location Services** screen is displayed.
3. Provide the details for the following parameters. You can create multiple location service profiles.

Figure 146: *Add a Location Service*



Field	Description
Name	Unique name for this Location Service. The supported range is 1-32 alphanumeric characters.
Location Services Feed	Enables the location feed to capture related data.
Report Format	Select the report format, **Legacy** or **Forti-Presence**. • Use the Forti-Presence option to send data supported by the Forti-Presence server. You will be required to set up and configure the Forti-Presence server to process the BLE/WiFi data received from the controller. When Forti-Presence is selected, enter the **Project Name** (name for this location service) and the **Secret Key** for this location service. • Use the Legacy option to send data to any other 3rd party location server.
Server Source	Enter the souce of the location server feed, **BLE**, **WiFi** or **ALL**.
Server IP Address	Enter the IP address of the location server. The location server must have capabilities to parse and display BLE/WiFi data received from the FortiWLC.

Field	Description
Server Port	Enter the port of the location server.
Report Interval	Enter the time interval at which data is sent to the location server.

Click **Save**. The Location Service profile is created.

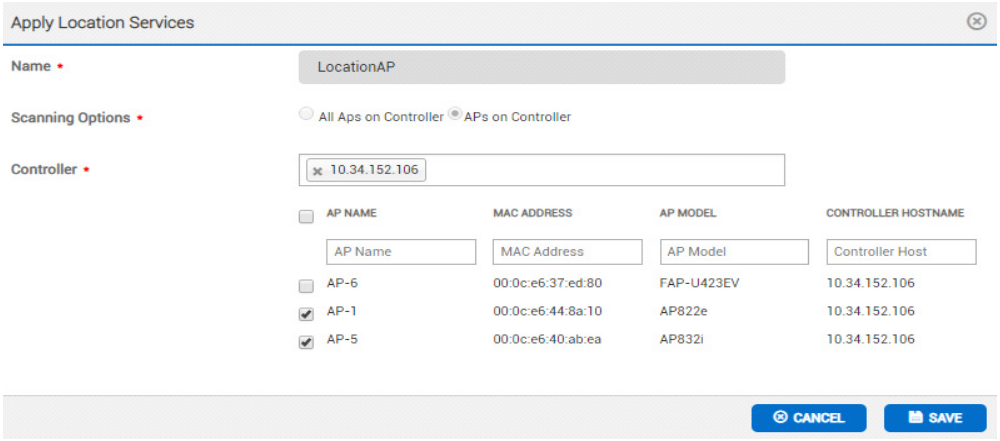
Applying Location Services Profile

Select the Location service profile and click  to apply to all APs of a Controller or to specific APs.

APs on Controller – This scanning option is supported only on FortiWLC 8.5. When this option is selected the **Controller** drop down list displays only 8.5 controllers. Select the controller(s) and the list of APs on each controller is displayed, select the required APs to apply the location services profile to.

All APs on Controller – This scanning option is supported all versions of FortiWLC (including FortiWLC 8.5). When this option is selected the **Controller** drop down list displays all controllers. Select the controller(s) to apply the location services profile to all APs of the selected controller(s).

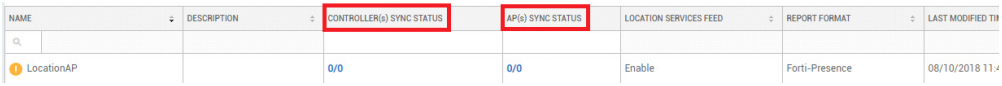
Figure 147: *Apply a Location Service profile*



Note:

- 11ac APs are only listed when FortiWLC 8.5 is selected (both Online/Offline).
- Both Controller level and AP level sync status is displayed on the Location Services page.

Figure 148: *Controller/AP sync status*



Click the **Force Apply** icon to push the profile again to the controllers.

Editing Location Services Profile

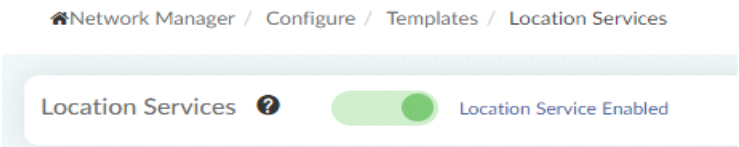
Perform the steps in this section to edit an existing location service profile.

1. Select **Configure > Templates > Location Services**.
2. The **Location Services** screen is displayed.
3. Select **Edit**. The **Edit - Location Services** screen is displayed.
4. Modify the fields as required. For field descriptions see *"Adding Location Services Profile" on page 260*.

Click **Save**. The Location Service profile is modified.

Location Services Profiles (FortiGate)

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



- Configure the WIDS profile for the AP radio.
- 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: **4013**
  - 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.

AP Packet Capture

The FortiWLM supports packet sniffing from access points to handle wireless network security issues and forward the capture packet dumps to any required destination IP and Port.

You can capture packets over the air from access points while the AP continues to operate normally. Once packets are captured, you can see packet captures in real time or save them to a file for offline analysis. AP packet capture can be used when WIPS is configured on the access points for intrusion detection/prevention. You can forward packet captures from APs directly to external devices without storing packets locally on the controller. This eliminates the restriction on the file size of the packet capture (you are not limited by controller memory) and also allows the captured information to be stored and archived externally.

AP Packet Capture profiles

Use the FortiWLM to configure packet capture profiles to start or stop packet capture for clients.

The following actions can be performed on the **AP Packet Capture** screen:

Action	Description
Add	**Add** allows to add an **AP Packet Capture Profile**.
Apply	**Apply** allows to apply an **AP Packet Capture Profile** to specific APs and Controllers.
Edit	Edit allows editing an AP Packet Capture Profile.
Enable/Disable	These options allow you to enable or disable an **AP Packet Capture Profile**. A disabled profile is not deleted and can be enabled again.
Delete	**Delete** allows deleting an **AP Packet Capture Profile**. Select the **Delete** option and the **AP Packet Capture Profile** gets deleted from the **AP Packet Capture Profile** screen.

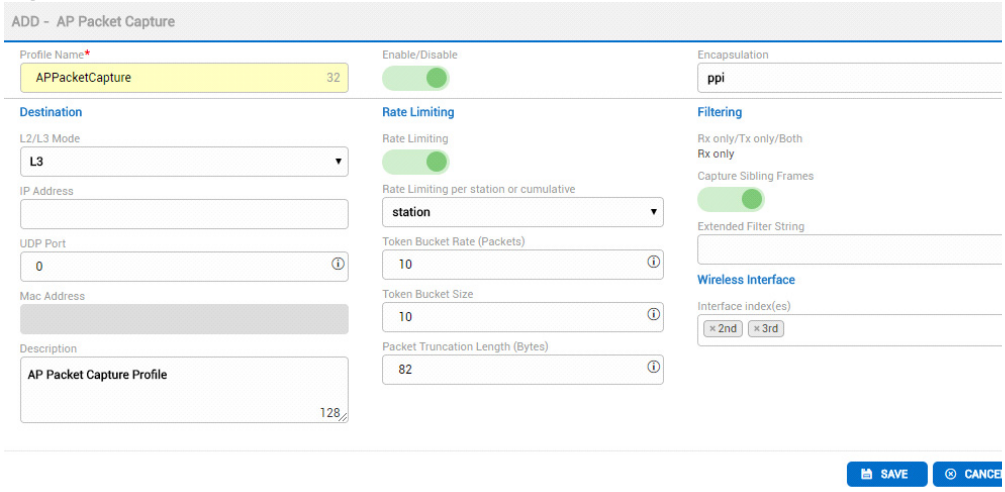
Adding AP Packet Capture Profile

Perform the steps in this section to add a new AP packet capture profile.

1. Navigate to **Configure > Templates > AP Packet Capture**.

2. In the **AP Packet Capture Profile** screen, select **Add**. The **ADD - AP Packet Capture** screen is displayed.

Figure 149: *Add a Packet Capture Profile*



3. Provide the details for the following parameters. You can create multiple packet capture profiles.

Field	Description
Profile Name	Unique name for this Packet Capture profile. The supported range is 1-32 alphanumeric characters.
Enable/Disable	Enables the current packet capture profile.
Encapsulation	Select the encapsulation format, PPI or Legacy.
Destination	**L2/L3 Mode**: Select the transmit mode to layer2 or layer3 for the current packet capture profile. This information is used by the AP when forwarding packets to the destination using either L2 or L3 mode as specified. Enter the destination **IP Address** and **UDP Port**, or the **MAC Address** based on the selected mode.

Field	Description
Rate limiting	This option enables the rate limit for the current packet capture profile. The packet capture is rate limited to per-station or cumulative for the current packet capture profile. If set to station, rate limiting is done per station and if set to Cumulative, rate limiting is done per AP. If rate limiting is enabled, the rate in the token-bucket-rate is used to forward the packets. The AP forwards the maximum packets per second configured in the token bucket rate. • **Token Bucket Rate**: Sets the token bucket rate for the current packet capture profile. Token-bucket-rate regulates the (non-zero) number of packets forwarded to the destination at a per-second rate, the token-bucket-rate value tells the APs the maximum number of packets they can forward per second. The token-bucket-rate value should always be lower than token-bucket-size. • **Token Bucket Size:** Sets the depth of the bucket where the wireless packets are stored and then forwarded to the destination. This should be a non-zero value and greater than token-bucket-rate. • **Packet Truncation Length (Bytes):** Sets the length of packets that APs forward to a hardware device. APs reduce the length of all packets to this value before forwarding the packet to the hardware destination.
Filtering	Sets traffic intrusion detection for the current packet capture profile to received traffic, sent traffic or both. The default is rx only. • Enable **Capture Sibling Frames** to capture frames sent by other APs in the network to be captured. For example, if you did not have a device to monitor what packets an AP was receiving, you could direct a second AP to listen to packets being sent to its sibling. • If required, specify the **Extended Filter String**. The supported range in 1-32 characters. • **Wireless Interface** - Sets an interface list for capture.

Click **Save**. The AP Packet Capture Profile is created.

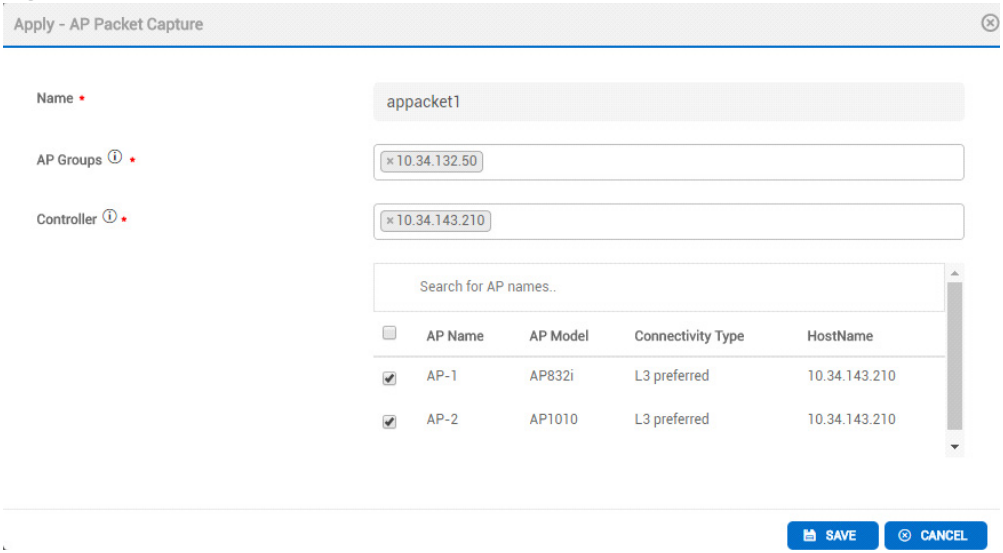
Applying AP Packet Capture Profile

Select the Packet Capture profile to apply to all APs of a Controller or to specific APs. These are the supported options.

- **AP Groups** - Select a group from the drop-down list. The profile is pushed only to the APs in the AP Group.

- **Controller** - Select the Controller from the drop-down list and select the supported APs. The profile is pushed to the selected APs.

Figure 150: *Apply an AP Packet Capture profile*



Editing AP Packet Capture Profile

In the **AP Packet Capture Profile** screen, select **Edit**. The **EDIT - AP Packet Capture** screen is displayed.

Edit the parameters. as required. For parameter descriptions, see *"Adding AP Packet Capture Profile"* ***on page 264***.

Click **Save**. The AP Packet Capture Profile is modified.

LLDP Discovery

The Link-Layer Discovery Protocol (LLDP) is a layer-2 neighbor discovery protocol that allows network devices to advertise specific information about themselves to other devices on the network and receive information from them. LLDP neighbor discovery by both controllers and access points is supported. LLDP-capable devices transmit information in type, length, and value (TLV) messages to neighboring devices. Devices advertise information such as chassis ID, port ID and description, system name and description, system capabilities, and management IP addresses.

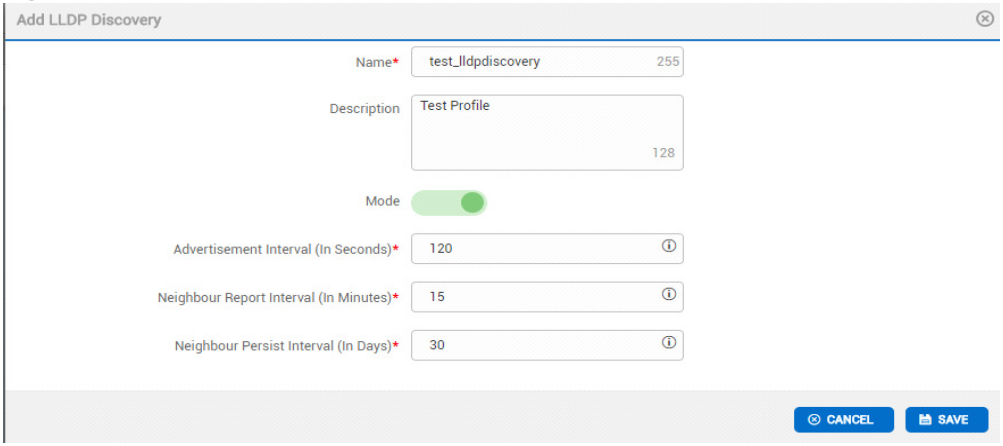
Note: LLDP discovery is supported on FortiWLC 8.5 and above.

This protocol is supported on all controller models and 11ac access points. This feature facilitates efficient network management by being aware of its neighbors and also locating defunct

access points in the network. The controller and access points advertise LLDP information periodically to their neighboring switches at a configured interval of time. The controller maintains a database of LLDP information received from its neighboring switches. The access points send LLDP information about the neighbouring switch along with its own details to the controller periodically at a configured reporting interval of time. This information from the access points is also stored on the controller database. The Controller persists the stored information in its database for a configured period of time and then discards it.

Navigate to *Configure* > *Templates* > *LLDP Discovery*.

Figure 151: *Adding LLDP profile*



Notes:

- LLDP discovery is supported only on 11ac APs.
- LLDP discovery is NOT supported on Mesh APs.
- In an N+1 setup, the active controller sends/received LLDP messages from the switch connected to it.
- Prior to enabling LLDP discovery, ensure that LLDP is enabled globally or in each port of the neighboring switches.

The following actions can be performed on the **LLDP Discovery** screen:

Field	Description
Add	**Add** allows to add an **LLDP Discovery Profile**. Enable the LLDP neighbour discovery **Mode** to configure the controller and access points to start the neighbour discovery process. Enter a unique **Name** and **Description** for the profile. • **Advertisement Interval(in seconds)** - Specifies the frequency at which LLDP (packets) advertisements are sent by the controller and the access points. The valid range is 30-120 seconds. Default is 120 seconds. • **Neighbor Report Interval(in minutes)** - Specifies the frequency at which the access points send information about the neighboring switch to the controllers. The valid range is 10-30 minutes. Default is 15 minutes. • **Neighbor Persist Interval(in days)** - Specifies the number of days the neighbor information is held in the controller database, before it is discarded. The valid range is 30-365 days. Default is 30 days.
Apply	**Apply** allows to apply an **LLDP Discovery Profile** to specific Controllers. One LLDP profile can be pushed to multiple controllers.
Edit	**Edit** allows editing the selected **LLDP Discovery Profile**.
Delete	**Delete** allows deleting an **LLDP Discovery Profile**. Select the **Delete** option, the **LLDP Discovery Profile** gets deleted.

CLI Template

The CLI Template configuration is a set of sub-profiles containing FortiWLC (controller) CLI commands to run on multiple selected controllers. CLI Templates can be created for all configuration commands supported on FortiWLC (controller), except *show* commands.

Once you create a CLI Template and deploy it on the controller FortiWLC runs the commands.

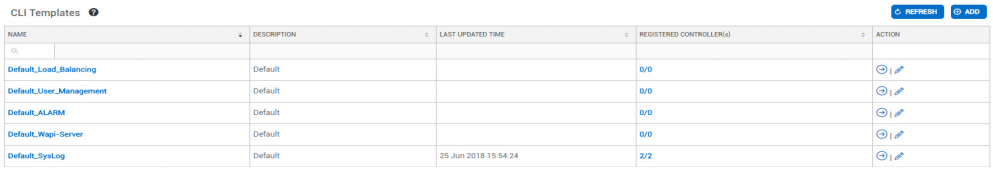
Default templates are provided with a list of CLI commands for the following. You are required to update the parameter values in these default templates.

- User Management
- Load Balancing
- WAPI Server
- Syslog

- Alarms

Navigate to *Configure* > *Templates* > *CLI Templates*.

Figure 152: *CLI templates listed*



The **Registered Controllers** displays the total number of controllers to which the CLI template is pushed and number of controllers on which CLI template is successfully synchronized. Click on the **Registered Controllers** to view the controller and synchronization details.

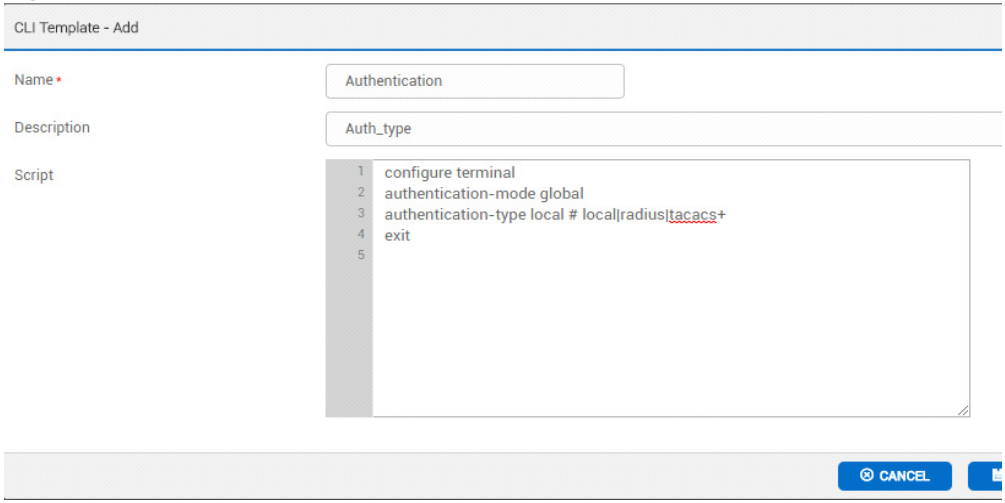
The following actions can be performed on the **CLI Template** screen:

Field	Description
Add	**Add** allows to add a **CLI Template**.
Apply	**Apply** allows to apply a **CLI Template** to specific Controllers. Click on the apply icon and select the controllers to apply the CLI template to.
Delete	**Delete** allows deleting a **CLI Template**. Select the **Delete** option, the **CLI Template** gets delete.
Edit	**Edit** allows editing a **CLI Template**. Select the **Edit** option and modify the **CLI Template** as required. The name of the CLI template cannot be modified.

Adding CLI Template Profile

1. In the **CLI Template** screen, select **Add**. The **CLI Template - Add** screen is displayed.
2. Provide the details for the following parameters. You can create multiple profiles.

Figure 153: *Adding a CLI template*



Configure the following fields to create a CLI template.

Field	Description
Name	Unique name for this CLI Template profile.
Description	A unique description for the CLI template profile.
Script	Add the CLI commands, one line contains one command and special symbol # as a comment. For example: **`configure terminal`** **`authentication-mode global`** **`authentication-type local # local|radius|tacacs+`** **`exit`** Where: • authentication-mode global is one command. • authentication-type local # local|radius|tacacs+ command has a comment, only authentication-type local will be executed on the controller, the remaining command is considered as a comment. • exit is one command.

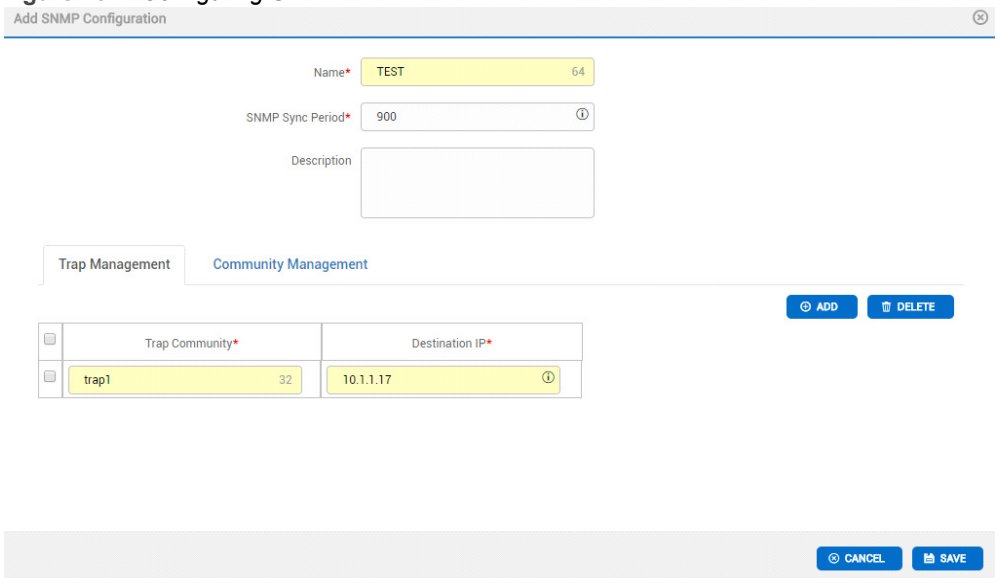
Click **Save**. The CLI Template Profile is created.

SNMP

SNMP configuration allows managing event notification and device statistics of all connected devices. SNMP configuration profile in FortiWLM consists of sub profiles, namely, **Community Management** and **Trap Management**, each Community and Trap Management feature can be configured with the same name but different client IP address. The SNMP configuration screen lists the existing profiles with the configured parameters and the synchronization status of the profile.

Navigate to *Configure > Templates > SNMP*.

Figure 154: *Configuring SNMP*



The **Profile Sync Status** displays the total number of sub-profiles synchronized to the controllers number of controllers on which sub-profiles are successfully synchronized. The **Sync Status** displays the number of controllers on which the profiles are successfully synchronized. Click on the **Sync Status** and the **Profile Sync Status** to view the controller, profiles, sub-profiles, and synchronization details.

The following actions can be performed on the **SNMP Configuration** screen:

Field	Description
Add	**Add** allows to add a **SNMP Configuration Profile**. • **Name** - A unique name of the SNMP configuration profile. The supported range is 1-64. • **SNMP Sync Period** - The period at which the SNMP configuration profile is synchronized to the controller. The valid range is 300 – 1500 seconds. • **Description** - A unique description of the SNMP configuration profile. • **Trap Management** - See **Trap Management.** • **Community Management** – See **Community Management.**
Apply	**Apply** allows to apply an **SNMP Configuration Profile** to specific Controllers. Click on the apply icon and select the controllers to apply the profile to.
Delete	**Delete** allows deleting an **SNMP Configuration Profile**. Select the **Delete** option, the **SNMP Configuration Profile** gets deleted. • Prior to deleting an SNMP profile, you need to delete its sub-profiles and unregister it from the controller. • Prior to deleting an SNMP sub-profile, you need to unregister it from the controller.
Edit	**Edit** allows editing an **SNMP Configuration Profile**. Select the **Edit** option and modify the **SNMP Configuration Profile** as required. The name of the profile cannot be modified.

SNMP Trap Management

Specify the SNMP trap information and add the trap.

1. In the **Trap Community** field, type the name of the SNMP community. The name can be up to 32 alphanumeric characters long. Do not include spaces or special characters in the name. The SNMP community acts as a password to authenticate messages sent between the SNMP server and SNMP client.
   Note: The SNMP community string is transmitted in clear text.
2. In the **Destination IP** field, type the IP address (IPv4 or IPv6) of the SNMP trap receiver that is listening for SNMP traps generated by the controller. To disable this feature, use 0.0.0.0.
3. To add the SNMP trap, click **Save**.

SNMP Community Management

Specify the SNMP community information and add the community.

1. In the **SNMP Community** field, type the name of the SNMP community. The name can be up to 32 alphanumeric characters long. Do not include spaces or special characters in the name. The SNMP community acts as a password to authenticate messages sent between the SNMP server and SNMP client.
   Note: The SNMP community string is transmitted in clear text.
2. In the **Client IP** field, type the IP address (IPv4 or IPv6) of the SNMP client. To specify a wildcard value, use 0.0.0.0.
3. In the **Privilege** list, select one of the following:
   - **read-only** - Allows read-only access to the MIB.
   - **read-write** - Allows read-write access to the MIB.

To add the SNMP community, click **Save**.

Management Operations

This section describes the various management methods for network manager.

- *"Inventory"* ***on page 274***
- *"Grouping"* ***on page 306***
- *"Configuration Archive"* ***on page 315***
- *"Software Image Management"* ***on page 320***
- *"Tools"* ***on page 327***
- *"Map Management"* ***on page 334***

Inventory

The *Inventory* allows you to

- Discover and manage controllers—*"Devices"* ***on page 274***
- Manage APs—*"Access Points"* ***on page 292***
- Discover third party devices—*"Switches"* ***on page 302***

Devices

FortiWLM manages multiple controllers (FortiWLC and FortiGate) and access points. You can create configurations from *FortiWLM* and download it to one or more managed controllers and monitor them as well. If you modify all controllers using FortiWLM, they are automatically updated with those modifications.These are owned by NMS and cannot be altered by the controllers using them.

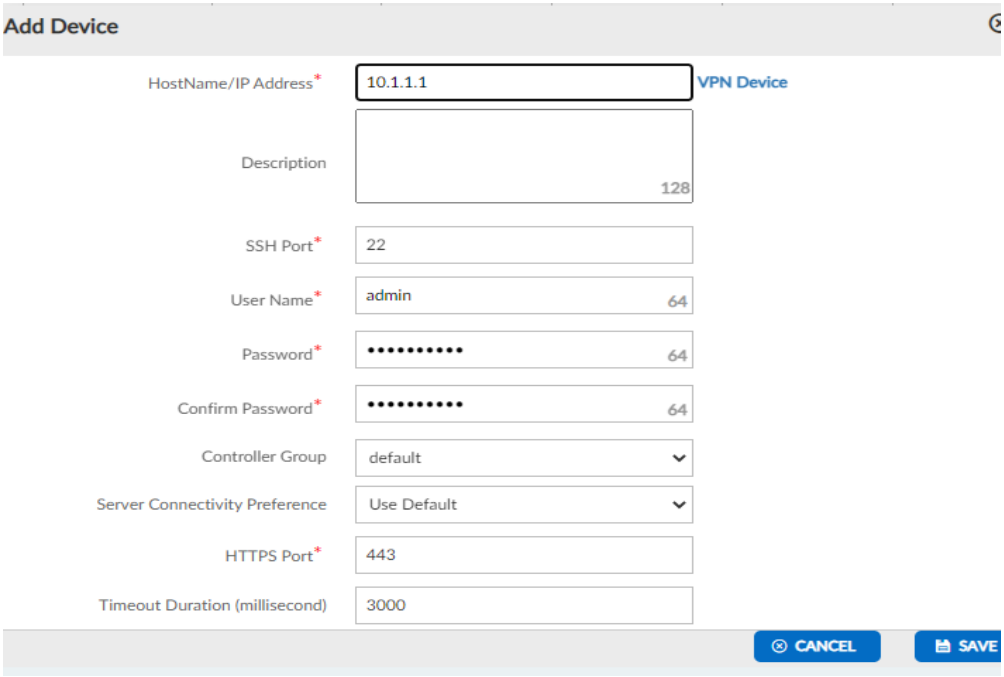
This chapter describes creating and applying configurations.

Add Controllers to FortiWLM

To add a controller to the *NM* inventory using a supported release, do the following:

1. Navigate to *Operate* > *Inventory* > *Devices*.
2. In the *Controllers* screen, select the *Add* icon. Provide the following details.

Figure 155: *Add a Controller*



3. In the *Controllers - Add* screen, provide the mandatory *Hostname/IP Address, User, and Password* details.

- **Hostname/IP Address**: Type the controller's IP address or name.
- **SSH Port**: Type the SSH port number. The controller can be added with the user defined port number.
- **User**: Type a user ID for the controller.
- **Password**: Type an encrypted password for the controller.
- **Controller Group Name**: Select a controller group name from the drop-down list. Controllers mapped to NM can be grouped. For further information to group controllers, refer to *"Controller Groups"* ***on page 306***.

- **Server Connectivity Preference**: Select the *Server Connectivity Preference*. The options are as follows:
  - **User Default**: This option is selected if the controller is in the same sub-network (Not behind NAT).
  - **User Server Public IP**: This option is selected to configure the public *IP Address* in *Administration* > *System Settings* > *Server Details* >*Public IP Address* screen.
  - **Specify Address**: This option is selected if the controller is behind NAT. The server IP address, which is reachable from controller, must be specified in the *Server IP Address* field.
  - **VPN Server IP Address**: This option is selected
- **Auto Save Configuration**: This option enables the automatic saving of updates to the Controller configuration.
- **Server IP Address**: Type the Server IP Address.This option is enabled, only if you want to specify an IP address by selecting the *Specify Address* check box in the *Server Connectivity Preference*.
- **HTTPS Port:** Specify the HTTPS port to be used.
- **[FortiGate Only] Timeout Duration (millisecond)** - Specify the timeout duration in milliseconds. This is the FortiGate REST API timeout value. The default value is 3000 milliseconds.

4. Select *Save*.
5. The controller is included and is displayed on the *Controllers* screen.

Modify Controllers

To modify a controller, do the following:

1. Navigate to *Operate* > *Inventory* > *Devices*.
2. In the *Controllers* screen, select a controller by clicking the check box and select the *Edit* option.
3. In the *Controller Inventory Details - Update* screen modify the following fields:
   - **Hostname/IP Address**: Modify the controller's IP address or name.
   - **SSH Port**: Modify the SSH port number. The controller can be added with the user defined port number.
   - **User**: Modify the user ID for the controller.
   - **Password**: Modify the encrypted password for the controller.

- **Management Administrative State**: Modify the *Management Administrative State*. The possible values are *Managed, Deleted, Maintenance,* or *Unlicensed*.

License violation message is displayed, when the number of APs exceed the number of Licenses. A grace period of 30 days is provided. After the grace period, the *Management Administrative State* is modified from the default *Managed* state to *Unlicensed*. The *Management Administrative State* is automatically modified to *Managed* after you upgrade the License.

- **Controller Group Name**: Modify the controller group name by selecting a different group name from the drop-down list.
- **Server Connectivity Preference**: Modify the *Server Connectivity Preference* by selecting one of the following options:
  - **User Default**: This option is selected if the controller is in the same sub-network (Not behind NAT).
  - **User Server Public IP**: This option is selected to configure the public *IP Address* in *Administration >System Settings > Server Details >Public IP Address* screen.
  - **Specify Address**: This option is selected if the controller is behind NAT. The server IP address, which is reachable from controller, must be specified in the *Server IP Address* field.
  - **VPN Server IP Address**: This option is selected.
- **Auto Save Configuration**: This option enables the automatic saving of updates to the Controller configuration.
- **Server IP Address**: Modify the *Server IP Address*.This option is enabled, only if you want to specify an IP address by selecting the *Specify Address* check box in the *Server Connectivity Preference*.
- **HTTPS Port**: Modify the HTTPS port number.

4. In the *Controller Inventory Details - Update* screen *view* the following fields:
   - **Communication IP Address**: Displays the controller's IP address.
   - **Network Device Id**: Displays the *Network Device Id* of the controller.
   - **Node Name**: Displays the *hostname* configured on the controller.
   - **Description**: Displays the description provided on the controller.
   - **Location**: Displays the location information configured on the controller.
   - **Contact**: Displays the contact information configured on the controller.
   - **Software Version**: Displays the controller's runtime software version.
   - **Controller Model**: Displays the controller's appliance hardware model such as MC4100 or MC3000.
   - **Availability State**: Indicates whether a controller is reachable or not from *FortiWLM*.
     - Online indicates reachable
     - Offline indicates not-reachable.

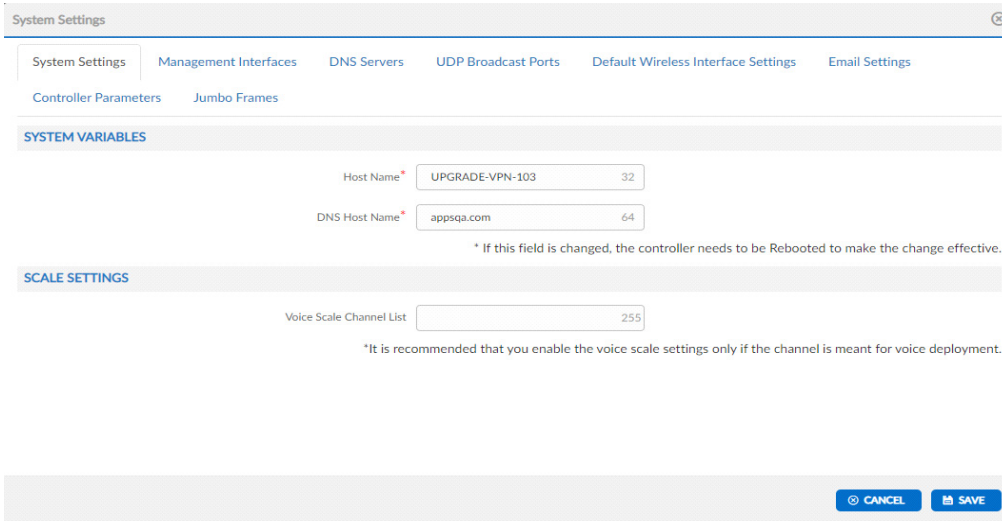
- **Management State**: Displays the monitoring state of the controller. *Active or Inactive*.
- **Management Server Message**: Displays the management server message.
- **N+1 State**: Displays the *N+1 State*. The possible ones are
  - Not Configured
  - Primary
  - Active Secondary
  - Active
  - Unknown.
- **Uptime**: Displays the Controller's current uptime in days, hours, minutes, and seconds.

System Settings

Use this page to modify the system settings. In the **Controller** screen, select a controller and click the system settings icon. The **System Settings** page is displayed. Update the configuration parameters as required.

Note:
System settings cannot be configured for offline controllers.

Figure 156: *Configuring system settings*



System Variables

Field	Description
Host Name	Enter the hostname of the controller. A maximum of 32 characters can be used. The hostname cannot consist entirely of integers, such as 1234 or 1.2.3.4. By default, the hostname is set to "default."
DNS Host Name	Enter the domain name that will be used with DNS. A maximum of 64 characters can be used.

Scale Settings

Voice scale settings are recommended if your deployment requires more than 3 concurrent calls to be handled per AP. The voice scale settings are enabled for an operating channel (per radio). When enabled, all AP's or SSIDs operating in that channel enhances voice call service. To enable, enter a channel number in the **Voice Scale Channel List** field and click **Save**.

Note:
Enable the voice scale settings only if the channel is meant for voice deployment. After enabling voice scale, the voice calls in that channel take priority over data traffic and therefore there will be a noticeable reduction of throughput in data traffic.

Management Interface

When the controller is set up, generally using the setup script, one controller IP address is assigned to the first Ethernet interface. An additional Ethernet interface can be configured to act as a redundant interface, or as a second active interface. When two Ethernet interfaces are configured, it is referred to as a Dual Ethernet configuration. You can add, modify, and delete **Physical Interfaces**, **VALN Interfaces**, and **Static Route**.

Physical Interfaces

To add a physical interface, click Add and update the following:

Field	Description
Interface Number	Controller Interface ID. The index can only be 1 or 2.
Assignment Type	Static IP address assigned - For the Static option, configure the Controller IP address manually. The following are the Static options displayed: • IP Address - IPv4 address of the interface. • Netmask - Subnet mask for the interface. • Gateway Address - Gateway IP address for the interface. DHCP - The controller procures the IP address from the DHCP server. The user must ensure that a DHCP server is reachable. Interface Mode - The interface mode, Active or Redundant

VLAN Interfaces

VLAN Interfaces allow you to specify VLANs that are to be used specifically for Management traffic on the network. Using this functionality, you can isolate management traffic from the rest of the network and route it specifically to the devices for which it is intended.

To add a VLAN interface, click **Add** and update the following:

Field	Description
VLAN Name	The name of the VLAN.
Interface Number	The physical interface number to be used. Management VLANs must utilize Interface number 1, so this field cannot be modified.
Tag	Tag name for the VLAN interface
IP Address	The IP address to be used by the VLAN.
Netmask	The NetMask for the VLAN.

Field	Description
Default Gateway	The gateway to be used by the VLAN.
Assignment Type	Management VLANs can only be implemented on static IP addresses, so this field cannot be changed.
Interface Mode	Management VLANs can only operate on Active interfaces, so this field cannot be changed.

Static Route

Static routes allow the system administrator to manually define the adapters that are permitted access to configured subnets. This is of particular use in smaller deployments where only a few routes are needed, or in larger ones where certain subnets must be kept separate from each other. Static routing can also be advantageous in that it doesn't require the processing power that dynamic routes (in which the network router automatically determines the best delivery path for packets) can.

To add a static route, click **Add** and update the following:

Field	Description
Static Route Name	A descriptive name for the route. Note that this must be between 1 and 16 characters in length.
IP Address/Subnet	The subnet for which the route provides access. This is typically in the xxx.xxx.xxx.0 format.
Subnet Mask	The subnet mask for the route. This is typically in the 255.255.255.0 format.
Interface Name	The name of the interface used for the route.

DNS Servers

Use this page to configure DNS Servers for the system. After DNS servers have been added, when needed, the system will connect to the first DNS server if it is able to; otherwise, it will go on to the next one until it finds one that is working. To add a DNS server, click **Add** and enter the DNS server name. Click **Save**. To delete a DNS server, click the delete icon to remove the server entry.

UDP Broadcast Ports

The upstream and downstream UDP broadcast ports can be configured for the Tunnel Mode and the Bridge Mode. The configured set of UDP ports are inspected for a broadcast destina-

tion address, and if received, are sent upstream or downstream onto the wireless interfaces. To delete a port, select it and click **Delete**.

To add the UDP ports, click **Add.**

1. **Mode** - Select the mode to configure the UPD ports; tunneld or bridged.
2. **Ports** - Check Upstream Ports, if you want to add upstream port or check Downstream Ports, if you want to add downstream port.
3. **UDP Port Number** - Enter the port number. Port numbers can range from 1 to 65,535 and a maximum of 8 upstream/downstream ports can be configured.

Click **Save**.

Default Wireless Interface Settings

The following table describes the information found in the Default Wireless Interface Settings table. Click on the edit icon to modify these.

Field	Description
IfIndex	The interface index number assigned to the interface. The interface index number cannot be modified.
Channel	The channel on which the interface is currently operating.
Channel Width	The operating channel width for the interface.

Email Settings

The following table describes the configuration of mail servers to send automated emails. The SMTP servers are used for email notification.

Field	Description
Sender Email	Enter the email address to receive emails from, for example, fortinet@example.com. Valid range is 1-254 characters.
Domain	Enter the domain name of the email address configured above, for example, example.com. Valid range is 1-254 characters.
Mail Server with Port	Enter the SMTP server to be used for email notification along with the port that the SMTP server uses separated by a colon (:), for example, smtp.example.com:port. Valid range is 1-254 characters.
Host Name	Enter the Hostname of the configured SMTP Server. Valid range is 1-254 characters.

Field	Description
SMTP User	Enter the login username for the SMTP server to be used. Valid range is 1-254 characters.
SMTP Password	Enter the password for the SMTP login username configured in the previous step.

Controller Parameters

You can reconfigure an existing controller. The following parameters can be configured.

Global Controller Parameters

Use this page to configure the controller. You can also review controller information.

To configure global controller parameters:

1. In the Description box, type a description for the controller. The description is for information only. The description can be up to 256 characters long.
2. In the Location box, type the location of the controller. The location is for information only. The location can be up to 127 characters long.
3. In the Contact box, type the name of the contact person or group for the controller. The contact is for information only. The contact name can be up to 127 characters long.
4. In the Automatic AP Upgrade list, select one of the following:
   - **On**: Ensures the AP image is automatically upgraded to the same level as the controller when an AP joins the WLAN. This is the default setting.
   - **Off**: Disables the Automatic AP Upgrade feature. APs must be upgraded manually.
5. In the DHCP Server boxes, type the IP address to which 802.11 client DHCP requests are forwarded.
6. In the Statistics Polling Period box, type the amount of time that elapses before the controller polls for information (for example, the number of packets passed or dropped), and as a result, refreshes the Web UI page with updated information. The value can be from 5 to 65,535 seconds. Specifying a value of zero (0) disables polling. The default is 60 seconds.
7. In the Audit Polling Period box, type the amount of time that elapses before the controller collects information about access points. The value can be from 5 to 65,535 seconds. Specifying a value of zero (0) disables auditing.
8. In the Default AP Init Script box, type the name of the default initialization script to be run for access points that have no script specified. Do not include an absolute path when specifying the script. A maximum of 64 characters is allowed. The script must already be located in /opt/(^)CompanyInPathname(^)/ATS/scripts for the script to be used.
9. In the DHCP Relay Passthrough, select one of the following:

- **On**: Enables the DHCP Passthrough; the default setting where DHCP packets are passed through the controller unchanged. With this option, you must configure DHCP relay on any routers between the 802.11 clients and the DHCP server. With this setting, the DHCP Server IP address field in Step 6. is ignored.
- **Off**: Disables the DHCP Passthrough. With this setting, DHCP relay is performed to the DHCP Server specified in Step 6.

10. When **DHCP Option 82** is enabled, the controller acts as a DHCP relay agent to avoid DHCP client requests from untrusted sources. This secures the network where DHCP is used to allocate network addresses. The controller adds the DHCP option 82 information to DHCP requests from clients before forwarding the requests to the DHCP server. By default, this option is disabled. This feature is supported with FortiWLC 8.6.0 and above. **Note:** The **DHCP Relay PassThrough** should be disabled for the controller to act as the DHCP relay agent.
11. Select the DHCP option 82 remote ID field format as **AP-MAC** or **AP-MAC-SSID**.
12. In the Management by wireless stations list, select one of the following:
    - **On**: (Default) Allow wireless stations to change the controller configuration
    - **Off**: Block management changes to the controller by wireless stations and allow only wired connection changes
13. In the Controller Index field, if the Personal AP feature is to be used, enter a number from 0 to 31 to represent a unique identifier for this controller; otherwise leave at 0. Also, remember to select Per Station BSSID for the Virtual Cell Type option in the ESS Profile configuration.
14. In Station Aging Out period, indicate the number of minutes of inactivity that causes a station to time out.
15. In the Roaming Domain State list, select one of the following:
    - **Disable**: (Default) The controller does not support the roaming domain state.
    - **Enable**: Enables the roaming domain state in the controller.
16. Click **OK**.

The following table lists the additional controller information that is available when the **Show Detail Info** link is clicked. Click **Refresh** to see updated information.

Field	Description
Controller ID	Numeric identifier of the controller.
Host Name	Hostname of the controller.
Uptime	Amount of time the controller has been up (in days:hours:minutes:seconds format).

Field	Description
Operational State	Operational state of the controller: • Enabled • Disabled
Availability Status	Availability of the controller: • Online • Offline
Alarm State	Most current pending alarm with the highest severity: • No Alarm • Minor • Major • Critical
Virtual IP Address	IP address of the controller.
Virtual Netmask	Subnet mask for the controller.
Default Gateway	Default gateway address used by the controller.
Software Version	Software version running on the controller.
Network Device ID	Controller MAC address.
System ID	Unique system identifier.
Controller Model	Model type of controller.
Region Setting	Region where controller is deployed.
Country Setting	Country where controller is deployed.
Manufacturing Serial Number	Lists the serial number for the controller.
FastPath Mode	FastPath Mode set for the controller: • **On**: (Default) Accelerates the rate that packets move through the Ethernet interface, based on identification of an IP packet stream. When FastPath is enabled, the beginning of the IP packet stream is processed by the controller, and all subsequent packets of the same stream are forwarded according to the disposition of the initial packets, without being processed by the controller. This offloads a significant amount of processing from the controller. • **Off**: Disables FastPath Mode. This should be the case when the capture-packets command is to be run, as the two are incompatible.

Field	Description
Bonding Mode	Bonding Mode set for the controller: • **Single**: Combines all Gigabyte Ethernet ports into one port for accelerated throughput. • **Dual**: Combines Gigabyte Ethernet ports into two ports.
Layer3 Routing Mode	Layer3 Routing Mode set for the controller: • **On**: Enables the Layer3 Routing mode. • **Off**: (Default) Disables the Layer3 Routing mode.

Controller Network Configuration Parameters

Use this page to do one of the following:

- **Enabling data fastpath forwarding** - Enable or disable hardware fastpath. By default its is Enabled.
- **Bonding Mode** - Enable Single or Dual Bonding for link aggregation or link redundancy.
- **Enabling 10 Gig module card** - Enable 10G interface, available only for MC4200, MC6000, FortiWLC-500D, FortiWLC-1000D and FortiWLC-3000D.

Mobility Configuration Parameters

Use this page to configure the controller mobility configuration parameters.

1. The Topology Information Update is useful for troubleshooting and collecting debug information. It is recommended that you enable this feature only if you need to collect troubleshooting and debug information. Select one of the following options:
   - **On**: Enable the topology information update in the Controller.
   - **Off**: Disable the topology information update. This is the default setting.
2. Enter the Associated Station Max Idle Period value. The default value is 2000 and the valid range is 30-86400.

IPv6 Configuration Parameters

Use this page to configure the controller IPv6 configuration parameters.

In the Neighbor Discovery Optimization, select one of the following:

- **On**: Enable the IPv6 neighbor discovery optimization.
- **Off**: Disable the IPv6 neighbor discovery optimization.

Jumbo Frames

An Ethernet frame is classified as Jumbo when its size exceeds the standard Maximum Transmission Unit (MTU) of 1500 bytes. Jumbo frames are supported only on 11ac APs.

Field	Description
Enable Jumbo Frames	Select to configure the MTU for Jumbo frames.
Jumbo frames MTU	The MTU configures the largest size of the Ethernet frame (in bytes) that a network can transmit. Any packet larger than the configured MTU is fragmented into smaller packets for transmission. The valid range is 1500 - 4500 bytes; default is 4500 bytes when Jumbo frames are enabled.

Notes:

- For wireless clients, Jumbo frames are NOT supported; aggregation is supported in the tunnel mode only. Wireless payload is aggregated into jumbo frames to improve the system throughput.
- Jumbo Frames are available only with FortiWLC 8.5.1 and above.

Configure Jumbo frames from the controller only when the MTU values are to be more than 4500 bytes. You can configure Jumbo MTU for access points using FortiWLC.

Controller Reboot/Password Change

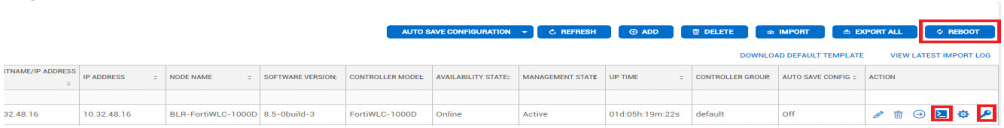
Reboot a Controller

This option allows you to reboot ONLINE controller(s) only; select one or multiple controllers and click **Reboot**. Confirm reboot when prompted.

Change Password

This option allows you to modify the controller password only for ONLINE and ACTIVE controllers only. Click the change password icon and provide the current and new passwords; click **Save.**

Figure 157: *Controller reboot and password change*

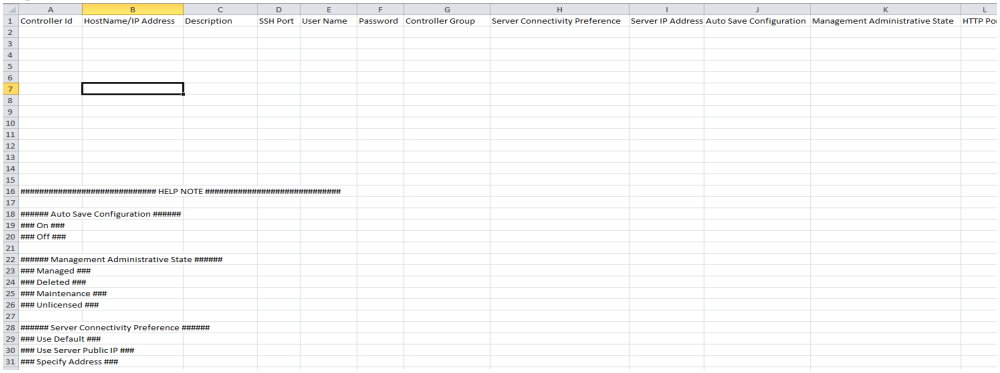


Import Controllers to Inventory

You can add Controllers into Inventory by importing files (*.CSV).

Click **Download Default Template** to download the default template to add a Controller.

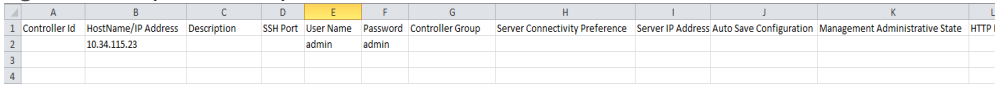
Figure 158: *Default Template*



	A	B	C	D	E	F	G	H	I	J	K	L
1	Controller Id	HostName/IP Address	Description	SSH Port	User Name	Password	Controller Group	Server Connectivity Preference	Server IP Address	Auto Save Configuration	Management Administrative State	HTTP Po
2												
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												
13												
14												
15												
16	########## HELP NOTE ##########											
17												
18	###### Auto Save Configuration ######											
19	### On ###											
20	### Off ###											
21												
22	###### Management Administrative State ######											
23	### Managed ###											
24	### Deleted ###											
25	### Maintenance ###											
26	### Unlicensed ###											
27												
28	###### Server Connectivity Preference ######											
29	### Use Default ###											
30	### Use Server Public IP ###											
31	### Specify Address ###											

Edit and save the template. The HostName, User Name, and Password are mandatory fields. Modifying the Controller ID will not take effect as the reset of the fields are identified with the Controller ID.

Figure 159: *Updated Template*

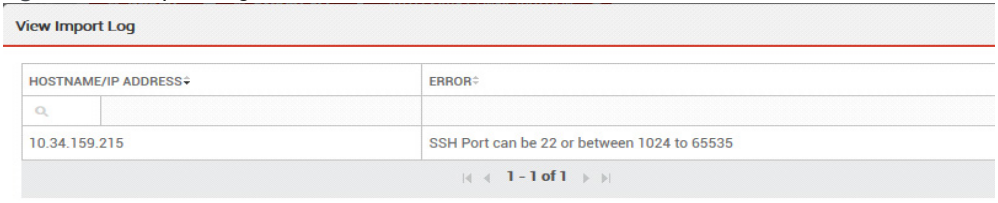


	A	B	C	D	E	F	G	H	I	J	K	L
1	Controller Id	HostName/IP Address	Description	SSH Port	User Name	Password	Controller Group	Server Connectivity Preference	Server IP Address	Auto Save Configuration	Management Administrative State	HTTP
2		10.34.115.23			admin	admin						
3												
4												

Click **Import** and browse to the saved *.csv template file. Click **Upload**.

In case of errors, view the import logs using the **View Latest Import Log** option for error details.

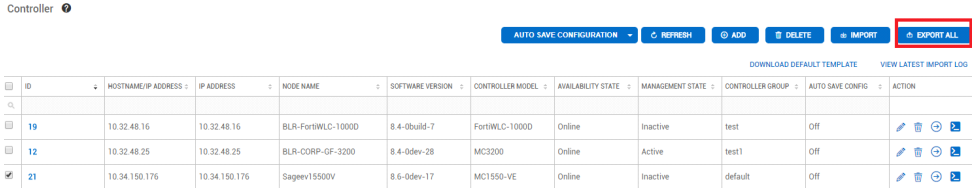
Figure 160: *Import Log*



Export Controllers from Inventory

You to export the existing Controllers to your local drive.

Figure 161: *Export Controllers*



Note:

The **Export All** option does not export the Controller password.

The exported Controller.csv can be edited and imported

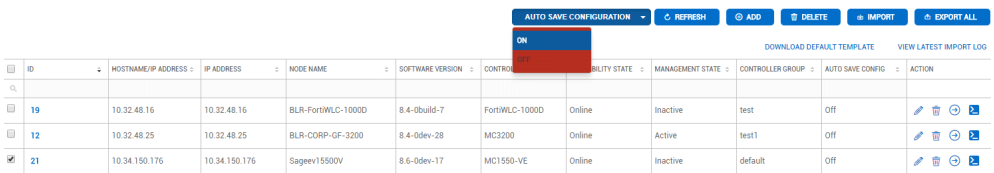
Figure 162: *Exported Controller CSV*

	A	B	C	D	E	F	G	H	I	J	K	L
1	Controller Id	HostName/IP Address	Description	SSH Port	User Name	Password	Controller Group	Server Connectivity Preference	Server IP Address	Auto Save Configuration	Management Administrative State	HTTP Port
2	7	10.33.115.28		22	admin		default	Use Default	0.0.0.0	On	Managed	443
3	4	10.34.133.230		22	admin		default	Use Default	0.0.0.0	Off	Managed	443
4	3	10.33.115.23		22	admin		default	Use Default	0.0.0.0	Off	Managed	443
5												

Auto Save Controller Configuration

To automatically save Controller configuration updates, select one or multiple Controllers and set the **Auto Save Configuration** to **On**.

Figure 163: *Auto Save Configuration*



To disable automatically saving the Controller configuration, set the **Auto Save Configuration** to **OFF**.

The **Auto Save Config** column is updated.

Access Points

1. Navigate to *Operate* > *Inventory* > *Devices*.
2. In the *Controllers* screen, select a controller by clicking the check box and select the *Edit* option.
3. Select the *Access Points* tab. The *Access Points* screen displays a list of APs mapped to the selected controller.

4. In the *Access Points* screen, select a access point by clicking the check box and select the *View Details* option.

5. In the *Access Points - Details* screen you can view the following fields:

Field	Description
Controller ID	Displays the controller Id to which the AP is mapped.
AP ID	Displays the AP ID.
Serial Number	Displays the serial number of AP, which is always the Ethernet MAC address.
Uptime	Displays the uptime of AP.
Location	Displays the location of the AP.
Building	Displays the building name where the AP is located in.
Floor	Displays the floor name where the AP is located.
Contact	Displays the person or organization responsible for the access point.
Discovery Protocol	Displays the discovery protocol.
Connectivity Layer	Displays the Network layer through which the access point is connected to the controller: • L2: Access point is in the same subnet as controller. • L3: Access point is in a different subnet from controller and connected to controller through a router.
Management Administrative State	Displays the management administrative state if managed, deleted, maintenance, or unlicensed.
Operational State	Displays the operational state is enabled or disabled.
Availability Status	Displays if the controller is reachable or not from FortiWLM. • Online indicates reachable • Offline indicates not-reachable.
Path MTU	Displays the configured Path MTU for the access point.
AP Model	Displays the AP model number.
Runtime Image Version	Displays the version of the operating system image on the access point. This version should always match the software version for the controller.
Boot Image Version	Displays the version of the ROM boot image on the access point.
FPGA Version	Displays the version of the FPGA chip on the access point (not supported for AP150, RS4000, OAP180, or AP300).

Field	Description
AP Role	Displays the role which the AP plays in the WLAN. The following are the AP role types: • **Access**: Access point is operating as a standard, wired AP. • **Wireless**: Access Point is part of the Enterprise Mesh configuration, providing wireless access services to 802.11/bg clients and backhaul services on the 802.11/a link. • **Gateway**: Access point is part of the Enterprise Mesh configuration, providing the link between the wired and wireless service.
Parent MAC Address	Specifies the MAC address of the parent AP when Enterprise Mesh is configured.

6. Select *Back* to go back to the *Access Points* screen.

Access Points

All FortiWLC run *System Director*, (the Fortinet operating system) that centrally manages and monitors access points (APs). System Director provides a centralized management system accessed from either the web UI or a *Command Line Interface* (CLI) for monitoring, configuration, and troubleshooting the system. The *FortiWLM* manages multiple *FortiWLC*. One of the major features of this product is the ability to create a global from *FortiWLM* and download it to one or more managed controllers. These global s are owned by E(z)RF server and cannot be altered by the controllers using them. The *FortiWLM* supports controllers running on a *Fortinet Services Appliance* hardware device or on a virtualized environment based on VMware.

How AP Discovery Works

There are three types of access point discovery:

- Layer 2 only—Access point is in same subnet as controller.
- Layer 2 preferred—Access point sends broadcasts to find the controller by trying Layer 2 discovery first. If the access point gets no response, it tries Layer 3 discovery.
- Layer 3 preferred—Access point send broadcasts to find the controller by trying Layer 3 discovery first. If the access point gets no response, it tries Layer 2 discovery.

For Layer 2 and Layer 3 discovery, the access point cycles between Layer 2 and Layer 3 until it finds the controller. The access point waits 16 seconds before cycling between Layer 2 and Layer 3.

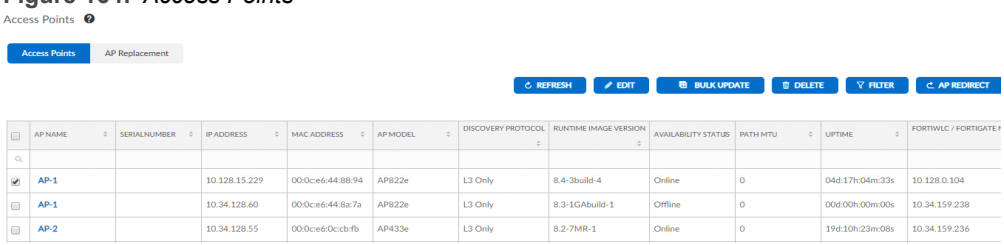
An access point obtains its own IP address from DHCP (the default method), or you can assign a static IP address. After the access point has an IP address, it must find the controller. By default, when using Layer 3 discovery, the access point obtains the controller's IP address by using DNS and querying for hostname "*wlan-controller*." This presumes the DNS server knows the domain name where the controller is located. The domain name can be entered via the AP configuration or it can be obtained from the DHCP server, but without it, a Layer 3-configured AP will fail to find a controller. Alternately, you can configure the AP to point directly to the controller's IP address (if the controller has a static IP configuration).

Once the access point obtains the controller IP address, it sends broadcast messages using UDP port 9393. After the controller acknowledges the messages, a link is formed between the AP and the controller.

Access Points tab

1. Navigate to *Operate* > *Inventory* > *Access Points*. The *Access Points* screen provides you a list of online and offline APs that are managed by the controllers.
2. You can perform the following actions on the *Access Points* screen.
   - **View**:
     - Select the *AP Name* hyper link.
     - The *Access Points* details, *AP Group Membership*, *Wireless Interface*, and *Connectivity* details of the selected AP is displayed.
   - **Filter**: Select the *Filter* option. The *Location Filter* allows you to filter the APs by the *Campus, Building, and Floor*.
   - **Delete APs**: The Offline APs can be deleted from the NM AP inventory. The selected APs can be deleted from inventory and geographical map assignment and clears any outstanding alarms related to the AP. It also releases respective licenses, if any. The delete option, does not delete the historical statistics collected on the serve.
   - **Edit**: You will be able to edit the *Administrative State* from *managed* to *maintenance*.
   - **Show AP Dashboard**: Select the *Show AP Dashboard* icon to view the details of the selected AP. The AP Dashboard screen displays an in-depth information about the AP activity. It provides you a 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.
   - **Show AP Location**: Select the *Show AP Location* icon, to view the location of the selected AP in the enterprise, campus, building, and floor.

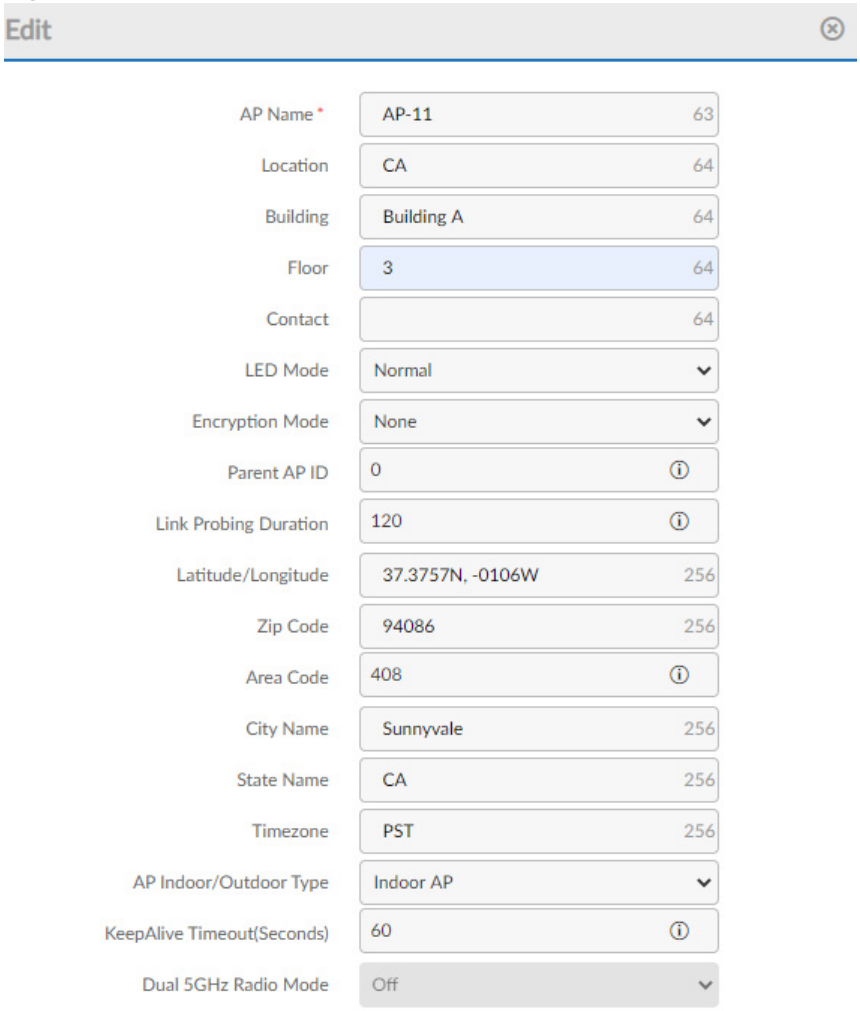
Figure 164: *Access Points*



Edit Access Points

The AP configuration can be edited from the FortiWLM AP inventory.In the Access Points screen, select an access point and click the edit icon. The Edit page is displayed. Update the configuration parameters as required.

Figure 165: *Editing access points*



Note: Access points belonging to offline controllers cannot be edited.

Field	Description
AP Name	You can modify the name of the access point. The required name can be 1-63 alphanumeric characters long, and can contain spaces. You cannot change the serial number.
Administrative State	Specify the administrative state of the access point as Managed or Maintenance.
Location	Type the location of the access point. The location is for information only and can be 1-64 alphanumeric characters long and contain spaces (for example, San Jose).
Building	Type the name of the building where the access point is located. The building description is for information only and can be 1-64 alphanumeric characters long and contain spaces (for example, building 1).
Floor	Type the floor where the access point is located. The floor description is for information only and can be 1-64 alphanumeric characters long and contain spaces (for example, first floor).
Contact	Type the name of the contact person or group for the access point. This is an alphanumeric string from 1-64 characters long and may contain spaces (for example, Chris Smith).
LED Mode	This is to help the administrator identify a running access point from the lights on the access point itself. The LED Mode light is the Status LED. In the LED Mode list, select one of the following: • **Normal** - The LED Status light is controlled by the Controller. • **Dark** - Dark means that all LED's (except the power LED) are off. • **NodeId** - LED with a long yellow light, followed by a series of short green lights. The number of short green lights is equal to the number of the AP ID module 10. Therefore, for AP IDs 4, 14, and 24, the NodeID mode will blink with a long yellow light followed by 4 short green lights. For AP IDs 7, 17, and 27, the NodeID mode will blink with a long yellow light followed by 7 green lights. Using this mode will help to the system administrator identify an AP from other APs in the system. Not supported on AP300. • **Blink** - The LED Mode (Status) light blinks off and on. The blink behavior is different for each AP.

Field	Description
Dataplane Encryption	This mode enables encryption only for the data path. • **On** - The AP-Controller link is encrypted. • **Off** - The AP-Controller link is unencrypted (default).
Parent AP ID	For the optional Enterprise Mesh configuration, specify a numeric identifier from 0-9999. In a mesh configuration, a wireless AP is directed to look for a signal from a Parent AP, which provides the wireless AP with its backhaul connectivity. Several APs can be assigned the same Parent AP ID. Several APs can be assigned the same Parent AP ID.
Link Probing Duration	Specify the duration of time (from 1 to 32000 minutes), that bridged APs wait before rebooting when the controller link is broken. This setting is used in bridged AP configurations to prevent AP reboots when the connectivity to the remote controller is lost. The default is 120.
Geo location parameters	While adding an access point you can specify its geographical location. The following location based attributes can be configured. • Latitude/Longitude - Coordinates separated by commas. • Zip Code • Area Code • City Name • State Name • Timezone
AP Indoor/Outdoor Type	Indicate whether this is an Indoor AP or an Outdoor AP.
KeepAlive Timeout(Seconds)	Specify the duration for Keep Alive Timeout (min 1 to max 1800 seconds). If an AP does not receive the Keep Alive message from the Controller, it will wait for this time period. After the time period, the AP starts rediscovery for a new controller. Default time period is 20 seconds. High value of KeepAlive Timeout is suggested for Remote APs (bridged profiles) with frequent downtime of WAN link. This will help in avoiding frequent AP reboots.

Field	Description
PathMTU State	The Path MTU discovery enables FortiWLC to determine the maximum transmission unit size on the network path between AP and controller; the packets sent conform to the MTU along the path, avoiding fragmentation and improving the network performance. **Note**: Path MTU discovery happens only between AP and Controller; the Path MTU is not discovered between controller and any external device like the RADIUS server or FortiWLM. Path MTU discovery works only for L3 APs and is enabled by default; you cannot disable it. The path MTU is discovered dynamically only when the AP is discovered/re-discovered. For example, if IPSec tunnel is configured between the AP and controller, Path MTU of 1438 bytes is set. Any update in the path MTU due to network changes (modification of MTU settings in L3 switch or router between AP and controller) does not take effect automatically/periodically; you are required to reboot the AP. Due to specific network requirements or the path MTU discovered by FortiWLC not being optimum, you can configure a value for path MTU. Select **Configured**, the Path MTU option is enabled.
PathMTU	The valid range is 1006 to 1500 bytes; the default is 1500 bytes. You are required to reboot the AP for the configured Path MTU to take effect.
Dual 5GHz Radio Mode	This is applicable only on FAP-U43xF access points and is disabled by default. When enabled, two radio interfaces of the access point can operate on the 5GHz band; This table describes the default configurations the radios operate with when this option is enabled/disabled. See **Dual 5GHz Radio Mode Configuration** below for configuration details. **Note:** The AP reboots whenever the Dual 5GHz Radio Mode is changed - enabled/disabled**.**

Dual 5GHz Radio Mode Configuration

When enabled/disabled, the radios operate with the default configurations described in this table

Dual 5GHz Radio Mode	Interface 1	Interface 2	Interface 3
Disabled (Default)	[Service Mode] • 2.4 GHz • 4x4 MIMO • 802.11ax_2g RF band	[Service Mode] • 5 GHz • 4x4 MIMO • 802.11ax_5g RF band	[Scan Spectrum Mode] • 2.4/5GHz • 2x2 MIMO • 802.11ac RF band
Enabled	[Service Mode] • 2.4 GHz • 2x2 MIMO • 802.11bgn RF band **OR** [Scan Spectrum Mode] • 2.4/5GHz • 2x2 MIMO • 802.11bgn RF band	[Service Mode] • 5 GHz • 4x4 MIMO • 802.11ax_5g RF band • Low band operating in channels 36 – 64.	[Service Mode] • 5 GHz • 4x4 MIMO • 802.11ax_5g RF band • High band operating in channels 100 – 165

Click **Save**. The following table describes access point information that is available if you click the **Detail Info** link.

Field	Description
AP Init Script	The name of the initialization script that the access point runs when booted.
Uptime	The amount of time the access point has been up.
Operational State	The access point state, Enabled or Disabled.
Availability Status	The access point availability, Online or Offline.
Alarm State	The highest value of the state of recently received alarms.
Boot Image Version	The version of the ROM boot image on the access point.
FPGA Version	The version of the FPGA chip on the access point.

Field	Description
Runtime Image Version	The version of the operating system image on the access point. This version should always match the software version for the controller.
Connectivity Layer	The network layer through which the access point is connected to the controller: • **L2** - Access point is in the same subnet as controller. • **L3** - Access point is in a different subnet from controller and connected to controller through a router.
Parent MAC Address	The MAC address of the Parent AP when Enterprise Mesh is configured.
AP IP Address for L3	The IP address of the access point when connected over L3.
AP Model	The AP model (for example, AP832, OAP832).
Hardware Revision	The version of the AP (for example, Rev 1, Rev 2).
VLAN Name	The associated VLAN name.
AP Hardware Serial Number	The serial number of the AP hardware.
Ap Group Id	The AP group number the access point is associated with.
Feature Group Id	The feature group number the access point is associated with.
Operating Mode	The current operating mode of the access point.

The bulk update function updates a group of selected APs. Select the APs that you want changed, then click **Bulk Update**. Make changes to the settings on the **Bulk Update** page and then, when you click **Save**, the selected APs are updated.

Update the following fields that will be propagated to the selected APs.

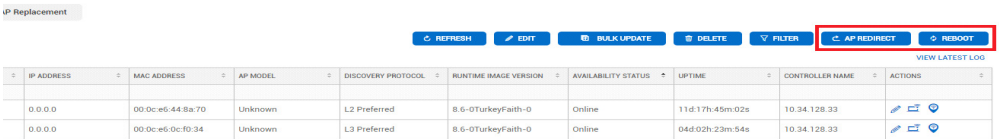
- Location
- Building
- Floor
- Contact
- LED Mode
- Link Probing Duration
- Power Supply Types
- KeepAlive Timeout(Seconds)

Access Point Redirect/Reboot

AP Redirect: This option allows you to redirect ONLINE L3 AP(s) only to a new controller; select the AP(s) and click **AP Redirect**. Select the IP address of the existing controller or enter the IP address of the new controller. Click **Save**.

Reboot: This option allows you to reboot ONLINE AP(s) only; select one or multiple APs and click **Reboot**. Confirm reboot when prompted.

Figure 166: *Access point reboot and redirect*



AP Replacement

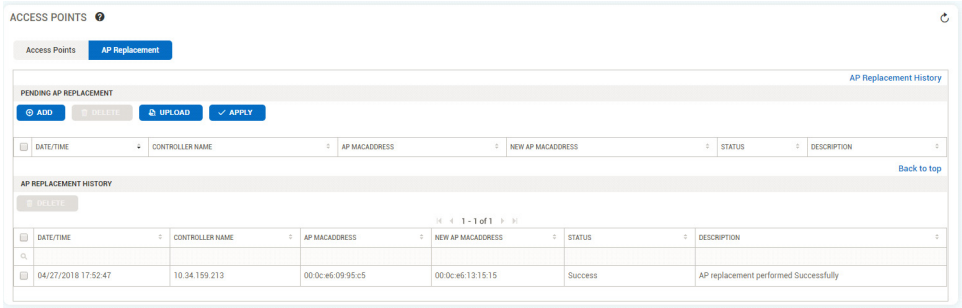
The *AP Replacement* allows you to replace a single AP or multiple APs from *NM*. The replacement of APs may be due to RMA or network upgrades such as replacement of all AP150's with AP 300's.The APs, when replaced on a controller is updated on *NM* also.

During the controller reboot, the AP replacement entries pushed from NM are preserved only if running-config is saved to startup-config.

The AP replacement screen is divided into the following sections:

- Pending AP Replacement (See *"Pending AP Replacement"* ***on page 301***)
- AP replacement History (See *"AP Replacement History"* ***on page 302***)

Figure 167: *AP Replacement*



Pending AP Replacement

The following actions can be performed on the Pending AP Replacement (See *Figure 167 on* ***page 301***) section:

- ***View the list of replaced APs***: You can view a list of the replaced APs from the *AP Replacement History* option.
- ***Add option for AP replacement***:
  - The *Add* icon allows you to select APs for replacement. An AP pair is replaced only if you possess access to the selected AP to be replaced.
  - A validation of the AP pair's MAC addresses is performed in the AP Replacement table, before the replacement.
  - For a new AP on *NM*, the *controller Id* and the *APID* is verified against the old AP.
  - The new AP is pushed to the controller for AP replacement. If the AP replacement is unsuccessful on the controller, the entry is deleted on the *NM* also. Upon successful completion, you are notified with the successful operation message.
  - The AP Replacement view will provide you a list the newly added AP pairs and the Replacement status is displayed as *Replaced*.
  - If the Replacement is awaiting physical replacement of the equipment, the status is displayed as *Replacement Pending*. The status is modified to *Replaced* once the replaced AP is online on the *NM*.
- ***Upload a list of APs to be replaced through a CSV report***: Multiple APs are replaced by selecting this option. A list of AP names are separated by coma separated values and saved in the CSV format on the local hard drive. The CSV file is uploaded to the *NM* server and the back end script validates the entries and creates entries in AP Replacement table. The CSV report consists of the *AP MAC-Address* and the *New AP MAC-Address*.
- ***Delete an AP pair from the list***: The deletion of the AP pair on the AP Replacement table, not only deletes the AP pair on the *NM* but also deletes the AP pair on the controller, if the affected controller appears online. The AP Replacement delete operation fails, if the Status of the selected AP Replacement entry is *Pending* and the Status of the Controller is *Offline*. The AP Replacement Status is displayed as *Delete Failed*.

AP Replacement History

The *AP Replacement History* table provides you a complete history of the APs replaced with the details like *Date/Time, Controller, AP MAC Address, New AP MAC Address, Status, and Description*. Select an AP and select *Delete* on the *AP Replacement History* table, to delete the history of the AP. Only three months old data is deleted from the AP Replacement History table. See *Figure 167 on* ***page 301***.

Switches

Switches use the SNMP protocol for fault management and REST for configuration and statistics.

- The FortiSwitch uses SNMP and REST credentials for detecting the wired rogues.

- Third party switches use only SNMP credentials for detecting wired rogues.

The Switches displays list of switches managed by the Network Manager. The list displays the following information.

Navigate to *Operate* > *Inventory* > *Switches*..

Field	Description
Host Name / IP Address	Displays the Host Name or the IP address of the Switch.
Model	Displays the Model number of the switch.
Status	Displays the Status of the switch.

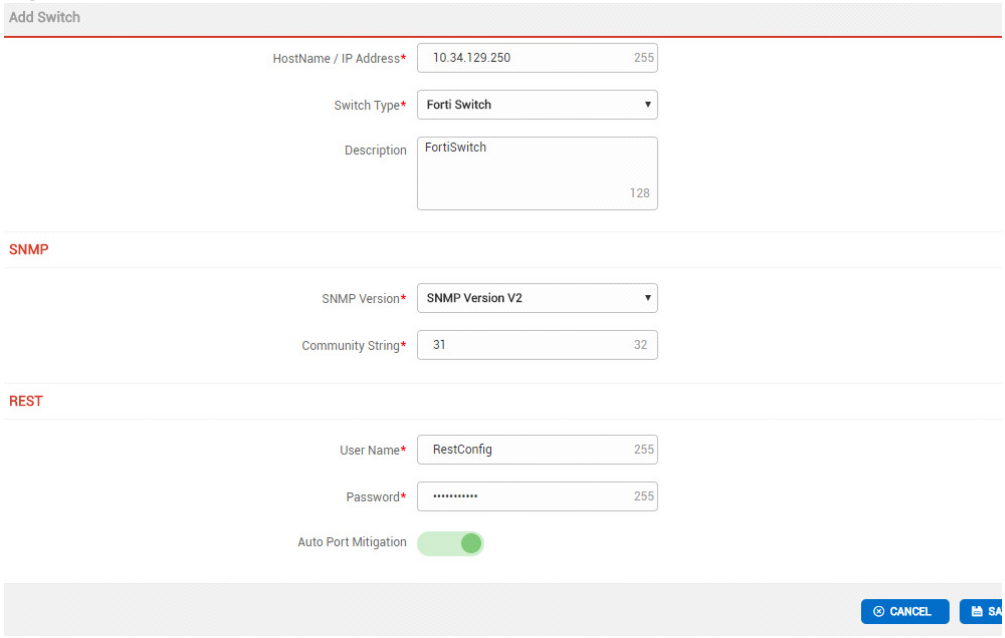
The following actions can be performed on the Switches screen:

Name	Actions
Refresh	Click **Refresh** icon to refresh the Switches screen.
Add	Click **Add** icon. The **Switches - Add screen** is displayed.
Delete	Select a check box of the Switch and click **Delete** to delete a Switch.
Edit	Select a check box of the Switch and click **Edit**.

Add Switches

1. Click **Add** icon. The **Switch - Add** screen is displayed.

Figure 168: *Add a Switch*



2. On the **Switch - Add** screen, enter the following required fields:

Field	Description
Hostname/IP Address	Enter the Hostname or the IP address for the switch in the **Hostname/IP Address** field. This is a required field and you can enter 1-255 characters.
Switch Type	Select the switch type, **Forti Switch** or **Others** (third party switches).

Field	Description

SNMP Version	Select one of the SNMP Version from the below list:
	SNMP Version V2
	Indicates that the switch is using the SNMP version. By selecting SNMP Version V2 from the list, the below mentioned fields are displayed.
	• Enter the **SNMP Community String** for the switch and you can enter 1-32 characters.
	SNMP Version V3
	Indicates that the switch is using the SNMP version 3. By selecting **SNMP Version V3** from the list, the below mentioned fields are displayed.
	• Enter the **Username** for the switch. This is a required field and you can enter 1-255 characters.
	• Select one of the **Authentication Protocol** from the below list:
	  • **No Authentication**
	  • **SHA (Secure Hash Algorithm)** - indicates that the switch is using secure hash algorithm protocol.
	  • **MD5 (Message Digest Algorithm 5)** - indicates that the switch is using message digest algorithm 5 protocol.
	• Enter the **Authentication String**. This is a required field and you can enter 1-255 characters.
	• Select one of the **Privacy Protocol** from the below list:
	  • **No Privacy**
	  • **DES** - indicates that the switch is using DES privacy protocol.
	  • **AES** - indicates that the switch is using AES privacy protocol.
	• Enter the **Privacy String**. This is a required field and you can enter 1-255 characters.

REST	Enter the **UserName** and **Password** for the switch. This is a required field and you can enter 1-255 characters. Enable **Auto Port Mitigation** to block the port for AP mitigation when WLM detects a rouge AP connected to the FortiSwitch.

3. Click **Save**.

Edit Switches

1. Select the check box of the switch and click **Edit** button. The **Switches - Update** screen is displayed.
2. On the **Switches - Update** screen, modify the fields as required. See *"Add Switches" **on page 303***.
3. Click **Save**. The modified Switch details for the selected switch is displayed on the **Switches** screen.

Grouping

The *Controllers* and *APs* are grouped for monitoring and configuration purpose. The groups are assigned to a user group. The following screens in the Inventory allows you to group controllers and APs:

- *"Controller Groups" **on page 306***
- *"AP Groups" **on page 308***

Controller Groups

The controllers can be grouped and assigned to a user group. Each controller can belong to one controller group only; if a controller is added to a second group, it is automatically removed from the previous group. However, controller groups can be assigned to multiple user groups.

Users can also be grouped and assigned group privileges from the web UI of *FortiWLM*. Only users with administration capability can modify a user group; *Administrators* can assign one or all permissions to their own user group.

A Controller group can be created using a set of controllers belonging to a particular user or user group. This allows the users belonging to the user group to have access to those controllers. For example, the controller drop-down list on the various dashboards display the controllers assigned to the current user group. The user must have inventory access permissions, to add, delete, view, or move controllers from one controller group to other.

Both controller groups and user groups are included in a backup.

If you do not set up controller groups, all controllers remain assigned to the controller group named *Default*. The controller group named *Default* can always be changed by the two permanent user groups named *Superuser* and *Default* user. The two permanent user groups, *Default* and *Superuser*, cannot be deleted.

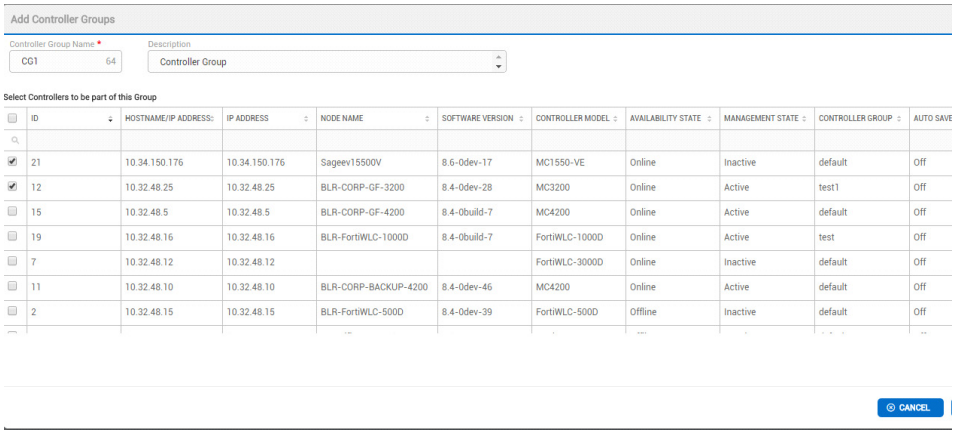
Add a Controller Group

Only users having *Inventory* access permissions will be able to add a group, delete a group or move controllers from one group to the other. If you add a controller that already belongs to a

group, the controller is removed from the old group and added to the new one. To create a controller group and add controllers to it, follow these steps:

1. Create the controller group by clicking *Operate* > *Grouping* > *Controller Groups* > *Add*.
2. In the *Controller Group - Add* screen provide a *Group Name* and optional *Description*. This is all that is required to create the group. You can click *Save* now if you wish.

Figure 169: *Controller Groups - Add*



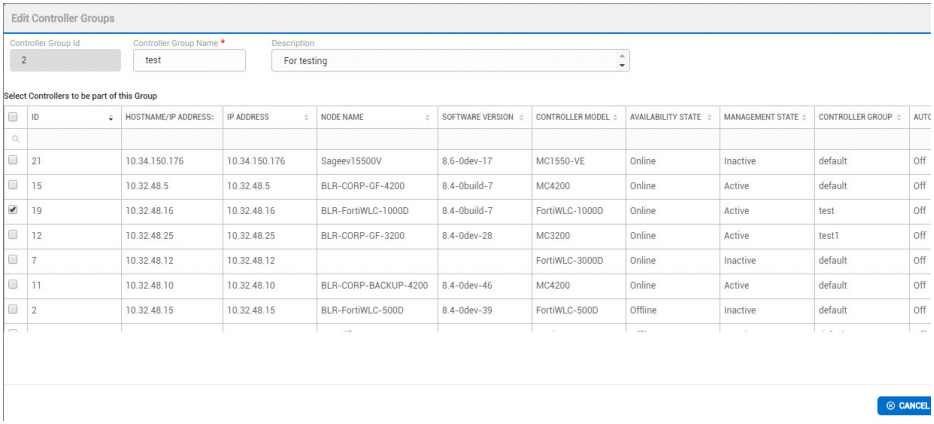
3. Optionally, add controllers to the group by clicking *Add*. A list of controllers present in the Inventory is displayed. Select one of the listed controllers - all of them are working with *FortiWLM* and click *OK*. The new controller is added to the list of controller groups.
4. Each *Controller Group* is assigned to a *Group Id*. The *Default* group comprises of the Group Id as 1.
5. To use the controller group, associate it with one or more user groups. To do this, see either *Add a User Group* or *Modify a User Group*.

Modify a Controller Group

Only users having *Inventory* access permissions will be able to add a group, delete a group or move controllers from one group to the other. (See *"User Group Access Capabilities"* ***on page 357*** for details on assigning permissions for Inventory access.) To modify a controller group, follow these steps:

1. Navigate to *Operate* > *Grouping* > *Controller Groups* > *select a controller group* > *Edit.*
2. In the *Controller Groups - Update* screen, modify the *Group Name, Description*, and add or delete controllers if required. If you delete controllers from a group, they are automatically reassigned to the group *Default*.

Figure 170: *Controller Groups - Update*



Delete a Controller Group

Only users having *Inventory* access permissions will be able to add a group, delete a group or move controllers from one group to the other. (See *"User Group Access Capabilities"* ***on page 357*** for details on assigning permissions for Inventory access.) The *Controller Groups* which consists of controllers within the group cannot be deleted. Remove all controllers from a group before deleting the groups.

To delete an empty controller group, follow these steps:

1. Navigate to *Operate* > *Grouping* > *Controller Groups*.
2. In the *Controller Groups* screen, select one or more check boxes corresponding to controller groups.
3. Click *Delete*. The selected controller is deleted from the *Controller Groups* screen.

AP Groups

The *AP Groups* screen displays a list of AP Groups. An *AP Group* is a hierarchical representation of all the APs assigned to the selected group to which the user has scope. The AP Groups screen allows you to create an AP group and assign APs to the group created. The APs within the selected AP Group is used to create *AP Group Dashboard* data, which is generated every 5 minutes on the server. See *"AP Group Summary"* ***on page 214***.

The AP Groups are classified into the following types:

- ***Monitoring and Service Configuration***: The *Monitoring and Service Configuration* group is identical to that of an AP Group to which the Service Profile is applied.
- ***Device Administration***: The *Device Administration* group, a specialized AP Group which applied to the device settings such as *Radio* and *Connectivity Profiles* (See *"Radio Profile"* ***on page 178*** and *"Connectivity Profile"* ***on page 179***.) This group has a restriction that an

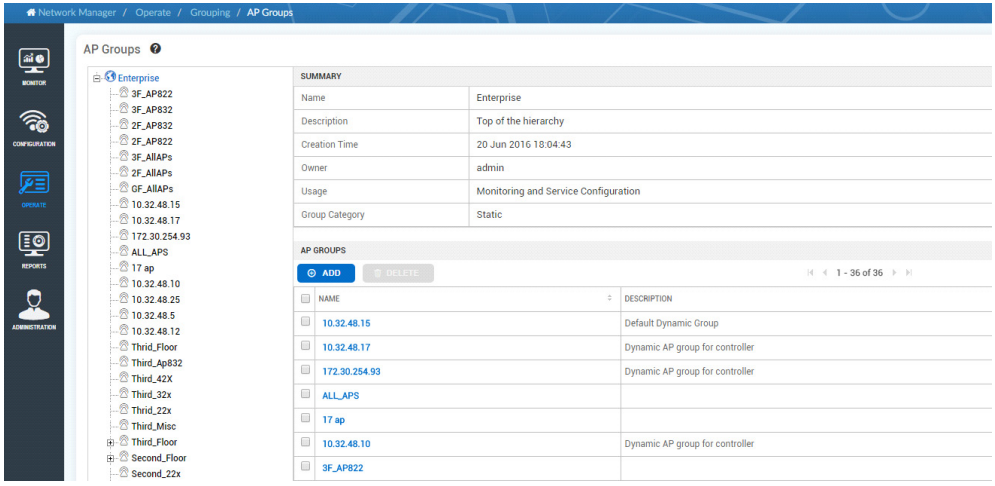
AP can belong to only one *Device Administration* group. This restriction prevents multiple device configurations getting applied from different groups.

An AP group may belong to multiple AP Groups. It can be created by using APs on the same controller or by using APs from multiple controllers. It may consist of APs of different hardware model, or APs from controllers running different system director versions.

The *AP Groups* screen displays the following sections:

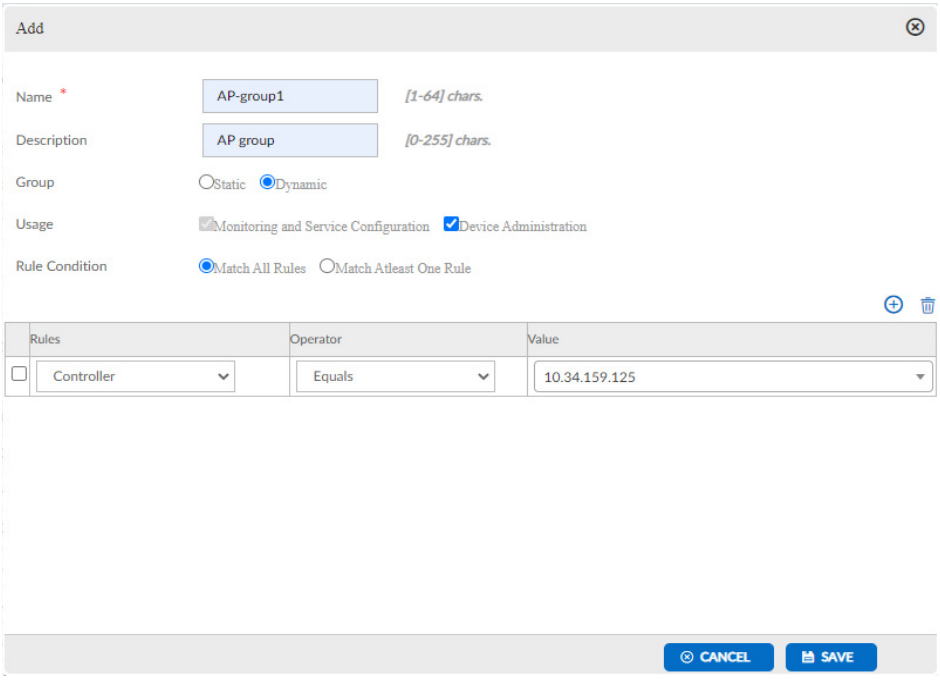
- **Hierarchical view of AP Groups**: Displays the *AP Groups, Subgroups* and *APs* of the Controller as a hierarchy. Each AP Group displays several subgroups. Select icon to view the AP Groups, Subgroups and APs of the Controller.
- **Summary**: Provides the details like *AP Name, Description, Last Updated Time, Owner,* and *Usage details*.
- **Member Sub Groups**: Provides the list of *Sub Groups* under the selected *AP Group*. A sub group can be added or deleted by selecting the respective options.
- **Member APs**: Provides a list of APs, under each *Sub Group* of the selected AP Group.

Figure 171: *AP Groups*



Monitoring and Service Configuration

By default, APs connected to a controllers are added into an AP group. This is done based on the controllers IP address. This is also called the default dynamic AP group. The default group cannot be modified or deleted and APs in that group cannot be removed. Dynamic groups are available only for service and monitoring and cannot be used for device administration.



Note:

- An AP can exist in more than one dynamic groups.
- A dynamic group can be created inside a static group.
- Any modification to the rule will affect the APs in the group.

To create custom dynamic groups, you can set rules using AND or OR conditions. The APs can be set to a dynamic group if all rules match or if at least one rules matches. The following filter are available to create rules:

- Controller IP address
- Location
- Building
- Floor
- Discovery Type (L2 or L3)
- AP Model
- Software Version
- AP Description
- Parent MAC Address

- Indoor / Outdoor APs

Device Administration

The dynamic AP group allows access points to be added dynamically to an AP group. The access point belongs only to the first Device Administration AP group that matches the first rule. If it is already a part of another static/dynamic Device Administration AP group, then it is not added to any other dynamic Device Administration AP group even if it matches the rule.

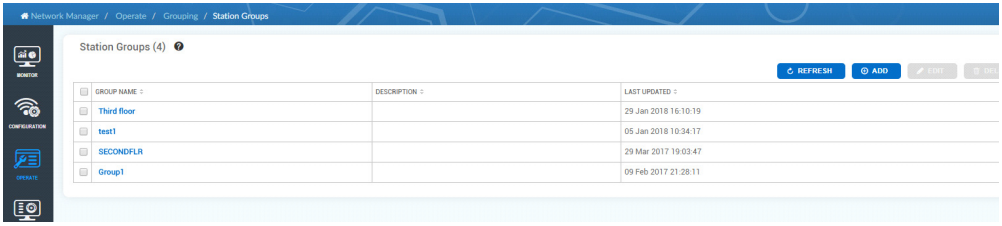
Click **Force Reexecte Rules** to forcefully re-run all the defined rules. This regroups the AP into the relevant dynamic group (first Device Administration AP group that matches the first rule). Click V**iew Recent Logs** to view the AP group and relevant error details.

Station Groups

The stations are logically grouped based on *Station Device 3 bytes MAC Prefix or Station MAC Address*. The stations are grouped to generate station group based reports by selecting the *scope* as *Station Groups* on the *Create Reports* screen.

1. Click *Operate* > *Grouping* > *Station Groups*. The *Station Groups* screen is displayed.

Figure 172: *Station Groups*



2. The *Station Groups* screen displays a list of all *Station Groups*. Each **Station Group** displays the *Group Name, Description,* and *Last Updated* details.
3. You can perform the following actions on the *Station Groups* screen by selecting the respective options:
   - Add Station Group
   - Edit Station Group
   - Delete Station Group

Add Station Group

The *Add* option allows you to create a *Station Group* by selecting individual stations. The stations are grouped by selecting a list of *MAC Addresses* or by selecting the *MAC Prefixes*.

1. Click *Add* in the *Station Groups* screen.
2. In the *Station Groups-Add* scresen you are allowed to create a station group by adding a list of *MAC Addresses* and *MAC Prefixes*.

3. Select *Save*. The new station group is created and displayed on the *Station Groups* screen.

Edit Station Group

The *Edit* option allows you to edit a *Station Group*. Some more stations can be included to the existing group by selecting a list of *MAC Addresses* or by selecting the *MAC Prefixes*.

Delete Station Group

The *Delete* option allows you to delete a *Station Group* from the *Station Groups* screen.

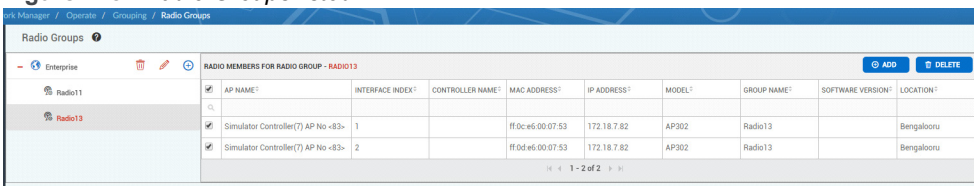
Radio Groups

A Radio group is a static logical group of AP radios across controllers. Radio groups are used for monitoring and configuration purposes. A Radio can belong to multiple Radio groups. You can deploy wireless services on particular Radios of the AP by selecting the Radio groups created. When deployed, services are deployed only on the AP Radios which are part of the Radio group.

When a new member is added to the Radio group, all the services deployed on the group are deployed on the new member as well.
When an AP or controller is deleted, corresponding radios of APs/Controllers are deleted from radio groups.

You can create multiple sub groups within a Radio group. FortiWLM provides an hierarchical representation of the radio groups and sub groups. Hover the mouse over the Radio group to view the name, time of the last update, and owner.

Figure 173: *Radio Groups listed*



You can perform the following actions on the **Radio groups**.

Action	Description
Add	**Add** allows to add a **Radio group**.

Action	Description
Edit	**Edit** allows to edit a **Radio group**.
Delete	**Delete** allows to delete a **Radio group**. Perform the following actions to delete a **Radio group**: • Select a **Radio group** and click the delete icon. • The selected **Radio group** gets deleted from the **Radio group** screen.

You can perform the following actions on **Radio group members**.

Action	Description
Add	**Add** allows you to add Radios to an existing **Radio group**.
Delete	**Delete** allows to delete members from a **Radio group**. Perform the following actions to delete a **Radio group** member: • Select a **Radio group** member and click **Delete**. • The selected member gets deleted from the **Radio group**.

Adding Radio Groups

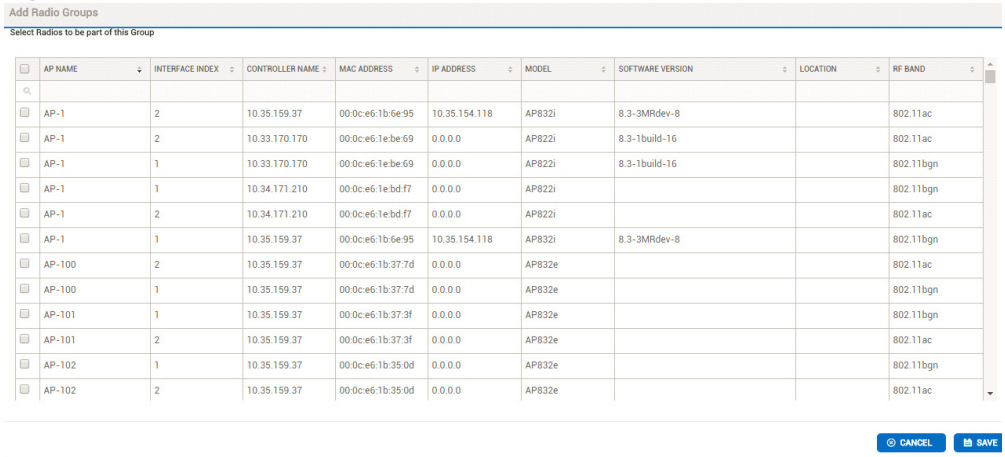
Perform the steps in this section to add a new radio group.

1. Navigate to **Operate > Grouping > Radio Groups**.
2. The **Radio Groups** screen is displayed.
3. Click  . The **Add Radio Groups** screen is displayed.
4. Enter a unique **Radio Group Name** and select the APs to be added to the group.

Note:

- Same members can be added in multiple radio groups.
- Sub groups can be created within a radio group.

Figure 174: *Add a Radio Group*



5. Click **Save**. The Radio group is created.

Editing Radio Groups

Perform the steps in this section to edit an existing radio group.

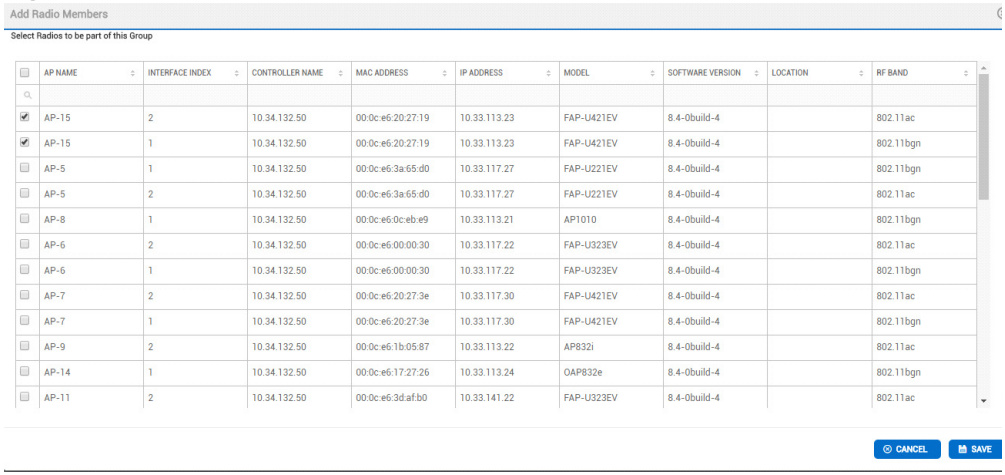
1. Navigate to **Operate > Grouping > Radio Groups**. The **Radio Groups** screen is displayed.
2. Select the Radio Group to be edited and click  . The **Edit Radio Groups** screen is displayed.
3. Modify the Radio group as required and click **Save**.

Adding Radio Group Members

Perform the steps in this section to add members to an existing radio group.

1. Navigate to **Operate > Grouping > Radio Groups**. The **Radio Groups** screen is displayed.
2. Select a radio group and click **Add**. The **Add Radio Members** screen is displayed.
3. Select the APs to be added to the group.

Figure 175: *Add Radio Group members*



4. Click **Save**. The members are added to the Radio group.

Configuration Archive

The *Configuration Archive* allows you to take periodic and manual *backups* of the *sys, startup* and *running configurations* for all online and managed controllers mapped to the *FortiWLM* application. It also allows you to *import* the controller configuration to nms-server for creating common configuration across multiple controllers.

- *"Backup Controller Configuration"* ***on page 315***
- *"Importing Controller Configuration"* ***on page 186***

Backup Controller Configuration

The **BACKUP NOW** tab allows you to store the backup data in the text format (P**lain Backup**) or encrypted format (**Encrypted Backup**). You are required to configure an encryption key of 16 hexadecimal characters (**Set Encryption Key**) to store the backup data in an encrypted format.

The details of the backup is as follows:

- The configuration backup can either be manual or scheduled.
- The scheduled configuration backup frequency is fixed to weekly.
- The weekly frequency remains unchanged. However, the user can configure the day of the week and the time of the day for scheduling the weekly configuration backup activity.
- The time scheduled is the server's local time with the default time as 1.00 A.M Sunday.
- The manual backup creation is based on the role. A user having the configuration capability and scope on particular controller will be able to take the backup of controller configuration.

In a manual backup, the user is provided with an option to add the list of controllers. Both startup and running configurations backup is taken for the controllers in the list.

- In a scenario of the scheduled backup failure, the backup activity for failed controllers is reinitiated every hour till the backup is successful.
- All the manual configuration backups are archived by default.
- The deletion of the selected controller from the inventory deletes all the backup data of the related controller.

Notes:

- Plain and encrypted sys-config backup option is supported on FortiWLC 8.5.2 and above.
- Encrypted sys-config backup is supported for on FortiWLC 8.5 and 8.5.1.
- Plain sys-config backup is supported on FortiWLC pre-8.5.0.

This section provides instructions for backing up the controller configuration database. You can manually initiate a backup or schedule regular backups through the *FortiWLM* user interface.

- *"Performing a Manual Backup"* ***on page 316***
- *"Scheduling Automatic Backups"* ***on page 374***

Controller Configuration backups will not be taken for *Secondary* controllers.

Performing a Manual Backup

The manual backup creation is based on the role. Only the users possessing configuration capability and scope on a particular controller is allowed to take the controller configuration backup. To back up of the controller configuration database, follow these steps:

1. Log into FortiWLM user interface.
2. Choose *Operate* > *Config Archive* > *Controller Config Backup* to display the *Controller Configuration Backup* screen.
3. The *Controller Configuration Backup* screen summarizes the host name, software version, last backup, number of backups, and log information of each of the controller mapped to the nm server. The *Config Type* displays the configuration types. The types are as follows:
   - sys configuration
   - startup configuration
   - running configurations

Figure 176: *Controller Configuration Backup*

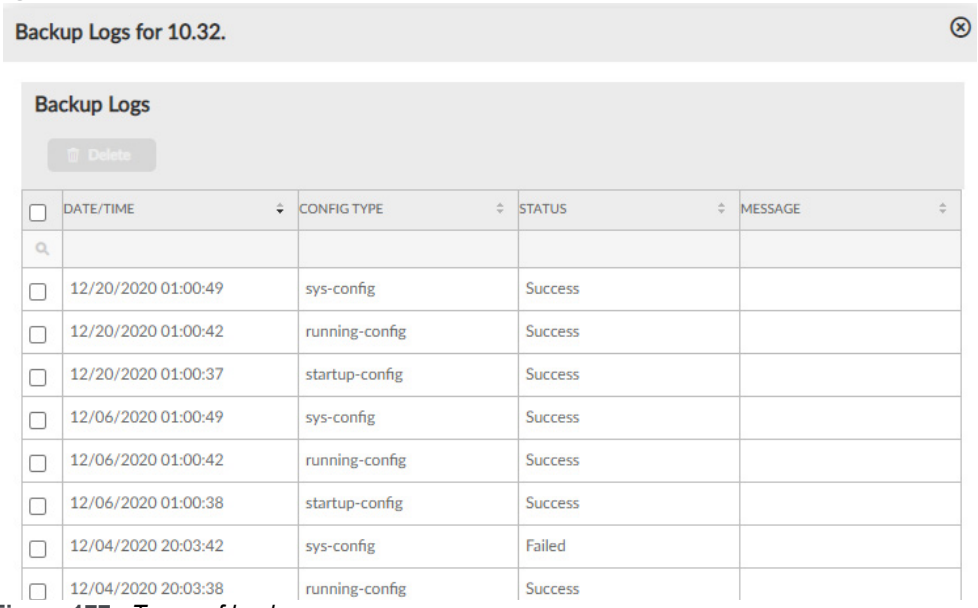
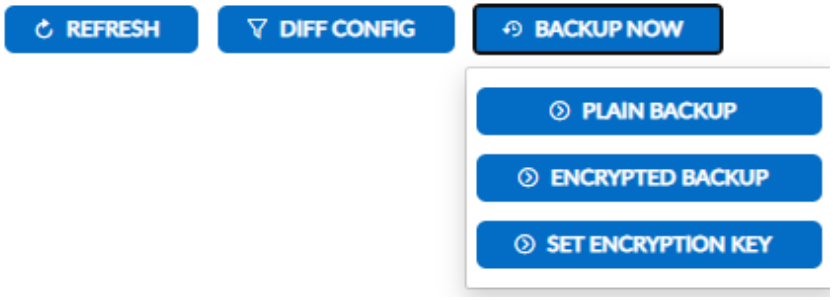


Figure 177: *Types of backup*



4. To view the backup details or to perform backup for a selected controller, select the *Controller* link. You can capture periodic backups for all online and managed controllers. The following are the different configurations that can be captured:
   - sys configuration
   - startup configuration
   - running configurations
5. The *Backup History* wizard provides you a complete history of the backup performed for a selected controller with the *Date/Time, Archive, Software Version, Config type, and Description* details. You can perform the following actions on the *Backup History* wizard.

- *Delete*: This option allows you to delete the selected controller configuration backup from the hard disk of the service appliance.

The deletion of the selected controller from the inventory deletes the complete backup data of the related controller.

- *Archive*: This option allows you to archive the selected controller configuration backup on the hard disk of the service appliance.

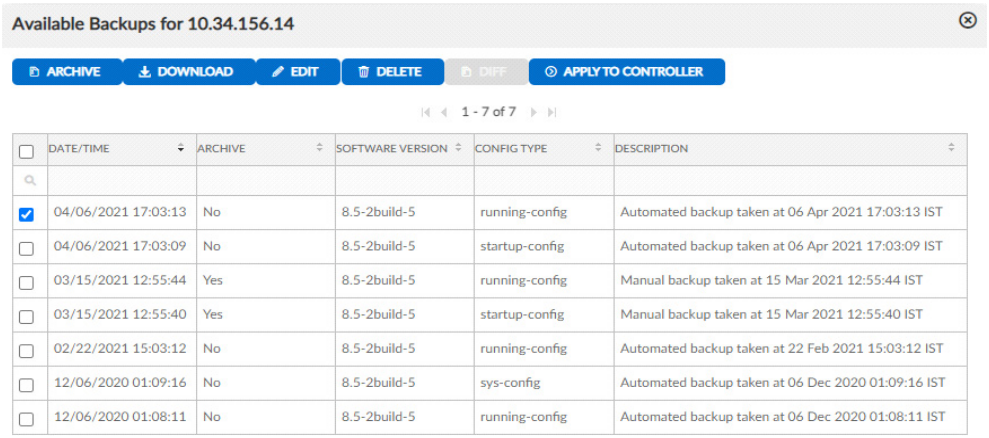
All the manual configuration backups are archived by default.

- *Download*: This option allows you to download and save the selected controller configuration backup on the computer hard disk in *text* format.
- *Edit*: This option allows you to edit the description of the selected controller configuration backup.
- *Diff*: This option allows you to view differences between two selected configuration types.
- *Apply*: This option allows you to apply running-config to startup-config and vice versa, and to apply sys-config to sys-config of the controller.

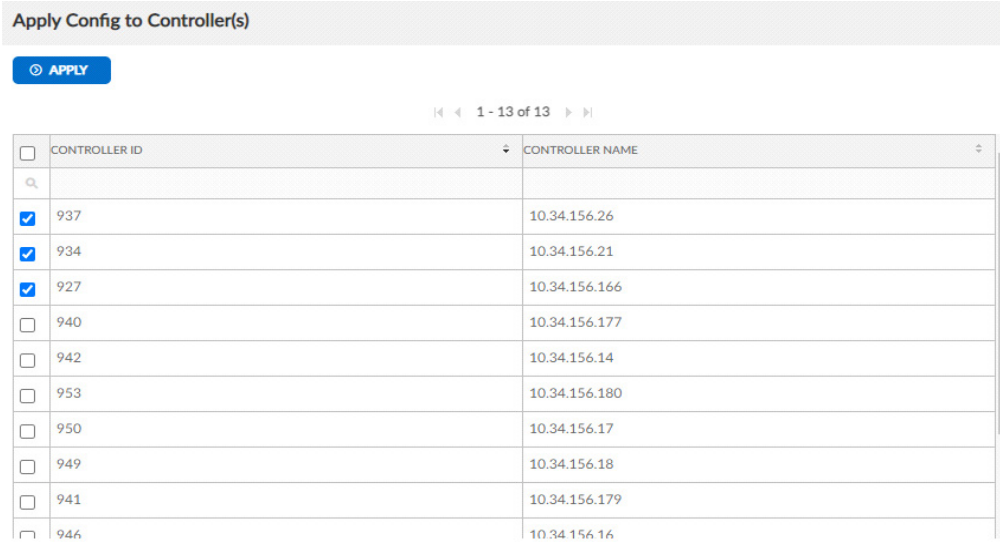
6. Select the *Detail* link to view the complete history of the backup for the selected controller. The *Backup History* wizard is displayed providing the *Date/Time* of the backup performed along with the *Config Type* and the *Status* of the backup, if failed or passed.

Applying Configuration Backup

The controller configuration backup can be restored to multiple controllers.



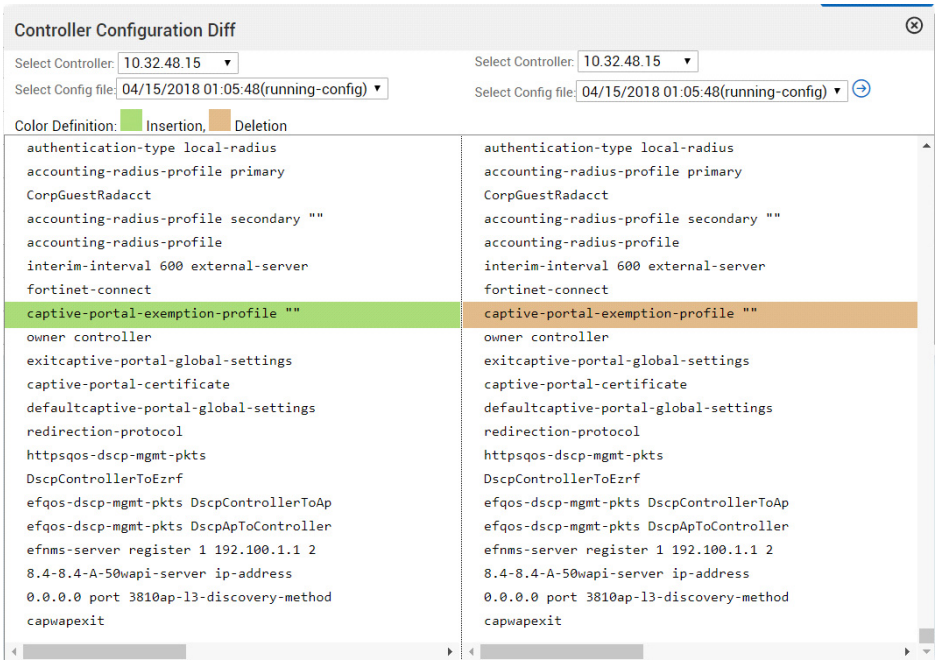
Apply to Controller: This option allows you to apply running-config to startup-config and vice versa, and to apply sys-config to sys-config of the controller. Clicking this option displays the list of available controllers with the **Controller ID** and **Controller Name**. Select one or multiple controllers and click **Apply.**



Controller Configuration Difference

You can view differences between startup and running configuration of the same controller or two different controllers and apply running-config to startup-config or startup-config to run-

ning-config. Select the Controllers and the configuration files to be compared and click **Diff Config**.



Software Image Management

You can upgrade multiple controllers from FortiWLM. All the controllers can be selected for upgrade but the actual upgrade is performed in batches of eight controllers at a time.

You must have Inventory capability to upgrade controllers. Both real-time and scheduled upgrades are supported. We recommend you to perform a backup before performing the upgrade. All the Fortinet images can be upgraded and distributed, including private builds, even though they may not be supported by *FortiWLM* for other features.

Use this same process to downgrade controllers.

Controllers running version 4.0 and above version can be upgraded to higher version and downgraded to lower version.

Images

FortiWLM can maintain up to 25 images. To *add, edit, or delete* an image in *FortiWLM*, follow these steps:

1. Navigate to *Operate* > *Software Image Management* > *Images*.
2. In the *Images* screen, select *Add* icon, to add additional images. Browse for the image file, and click *Save*.
   FortiWLM 8.5 supports both *.fwlm* and *.tar* file formats. For future releases, only *.fwlm* will be supported for upgrade and patch installations.

Figure 178: *Images*

3. To modify the description of an existing image, select an image, click *Edit*, perform the changes, and click *Save*.
4. To delete the existing image, select an image, click *Delete*, and click *Save*.

Upgrade Management

The *Current Upgrades* screen provides you the details of the controller upgrades that are in progress and in completed state during the last one hour. Individual *Controllers or Nplus1* controllers are upgraded here. It allows you to perform controller upgrade and keep track of the controllers that are in the process of getting upgraded.

To apply an image to controllers, follow these steps:

1. Navigate to *Operate* > *Software Image Management* > *Upgrade Management*..s
2. The *Current Upgrade* screen displays a list of *Primary, Secondary and Individual Controllers* for which the upgrade process is initiated. The following are the details:

Field	Description
Host name	Displays the *Host Name* of the controller.
Image Name	Displays the *Image* to be upgraded.
Upgrade Group	Displays the *Upgrade Group* of the controller. The two types are as follows: • Individual controllers • Nplus1 Clusters
Upgrade Type	Displays the *Upgrade Type* of the controller. The two types are as follows: • Controller • Access Points and controller • Feature • Patch-Controller

Field	Description
Phase	Displays the phase of the controller.
Status	Displays the *status* of the controller. The four types are as follows: • **In Progress** - The controller is *In Progress* for up gradation. • **Pending** - The controller is still pending for up gradation. • **Success** - The controller has successfully upgraded. • **Failed** - The controller has failed to upgrade. In Nplus1 upgrade, • **Success** indicates a successful upgrade of the controller with the right image and start the Nplus1 server. • **Failed** indicates a failure in upgrade of the controller with the right image and failed to start Nplus1 server.
Error	Displays the *Error* message during the failure of the controller upgrade.
Upgrade Details	Displays the *Upgrade Details* of the secondary controller. Select the *Detail* link to view the *Log Details*. The *Secondary Log* file displays the information about the secondary and high level information about the primarys.
Upgrade Progress	Displays the cluster *Upgrade Progress* of the secondary controller. The initial upgrade is progressed by the secondary controller followed by the primary controllers.

Select a *Secondary Controller*, the respective *Primary Controllers* can be viewed below the selected secondary controllers.

3. You can perform the following actions on the *Current Upgrades* screen:

- Expand All
  - Select *Expand All* option.
  - You can view the complete details of the secondary controllers and primary controller.
- Collapse All
  - Select *Collapse All* option.
  - The details of the secondary controllers and primary controller is compressed.
- Add
  - Select the *Add* icon. This option allows you to upgrade a controller

- In the *Select Controllers/Nplus1 Clusters to upgrade* screen you can view the following details of individual controllers and nplus1 cluster controllers.

Field	Description
Image Name	Select the *Image* to be upgraded.
Upgrade Group	Select the *Upgrade Group* of the Controller. The two types are as follows: • **Individual Controllers**: The *Individual Controllers* displays the list of Individual controllers listed on the *FortiWLM* server. • **Nplus1 Clusters**: The *Nplus1 Clusters* displays a list of *Secondary Controllers* and *Primary Controllers* that are located on the *FortiWLM* server. Select a *Secondary Controller*, the respective *Primary Controllers* can be viewed below the selected Secondary Controllers.
Upgrade Type	Select an *Upgrade Type* from the drop-down list as follows: • **Controller**: This is equivalent to the command *upgrade controller*. It upgrades the controller. • **Access Points and Controller**: This is the equivalent to the command *upgrade system*. It upgrades the *APs* and *controller*.
Schedule Upgrade	You can schedule controller upgrades to happen at different times and with different images. Select **Later** and then use the date picker icon to select the date and time. If you select Later, you have the option to **copy the image** to the controller but perform the installation process at a later scheduled time.

  - Click *Save* to proceed. The recently added *Select Controllers* or *Nplus1 Clusters* is displayed on the *Current Upgrades* screen.
- Delete
  - In the *Current Upgrades* screen, select one or more controllers from the drop-down list and click on *Delete*.
  - The selected controllers are deleted.
  - For *Nplus1*, the delete function, deletes the *Secondary and the Primary Controllers*.

The upgrade status older than one hour is available under *Operate* > *Software Image Management* > *Upgrade History*.

Scheduled Upgrade

You can schedule controller upgrades, controller patch upgrades, and nplus1 controller upgrades to happen at different times and with different images. To schedule controller

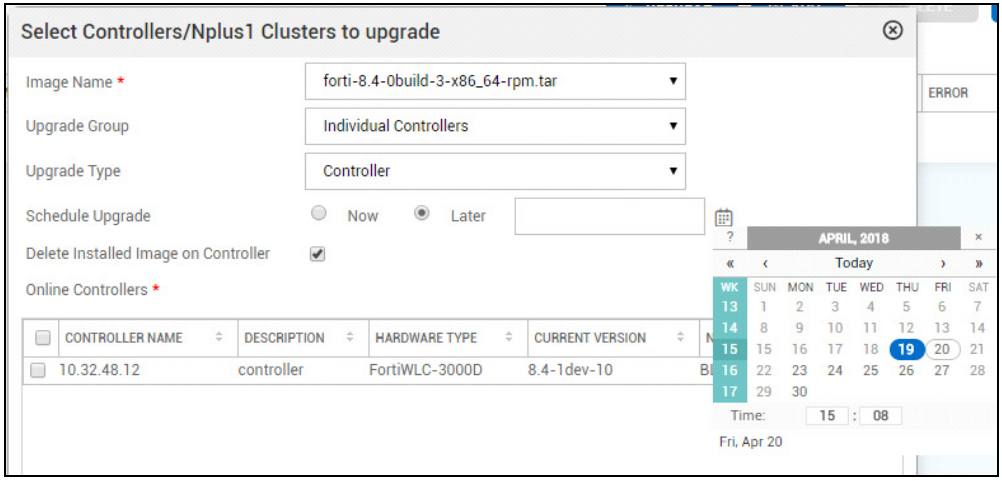
upgrades, go to *Operate* > *Software Image Management* > *Upgrade Management* and click the add icon to create a new upgrade schedule.

About Scheduler

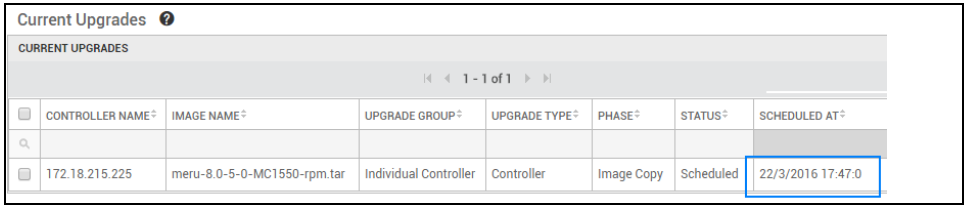
The upgrade scheduler allows you to:

- Create a single upgrade schedule for upgrading all controllers or all controllers and access points at a scheduled time with the same image.
- Create individual upgrade schedule to upgrade a controller with a specific image and at a specific time.
- Reschedule an already scheduled upgrade or a failed upgrade.

Create an Upgrade Schedule



Configured Upgrade Schedules



Reschedule Upgrades

To reschedule, select a controller and click the Reschedule Button.

Patches

The **Patches** screen allows you to manage and track the patches applied to controllers. The patch details and management options are displayed for each online controller.

Select the controller and click **Submit**.

Field	Description
Patch Name	The name of the patch currently installed on the selected controller.
Controller Name	The IP address of the controller the patch is installed on.
Version	The version of the installed patch.
Revertable	Specifies whether the patch is revertable or not.
Installed Date	The date and time stamp when the patch was installed on the controller
Size	The size of the patch installed on the controller.
Currently Installed	The current installation status of the patch, whether installed or not.
Currently Installed	The following actions can be prformed on the selected patch: • **Uninstall**: Select this option to uninstall the patch from the controller. • **Delete**: Select this option to delete the patch from the controller. **Patch History**: Select this option to view the history of the patch on the controller.

Upgrade History

You can view the complete history of *successfully* upgraded controllers and *failed* controllers.

Field	Description
Start Time	Displays the upgrade start time.
End Time	Displays the upgrade end time.
User	Displays the controller user name.
Controller	Displays the controller host name.
Previous Version	Displays the previous version of the controller before upgrade.
Next Version	Displays the next version of the controller after upgrade.
Upgrade Group	Displays the upgrade group of the secondary controller. The two types are as follows: • **Individual Controllers**: Displays a list of controllers selected for upgrade on the nms-server. • **Nplus1 Clusters**: Displays a list of secondary controllers and primary controllers that are located on the nms-server.
Upgrade Type	Displays the upgrade type. The two types are as follows: • **Controller**: This is equivalent to the controller upgrade command. It upgrades the controller. • **Access Points and Controller**: This is equivalent to the command upgrade system. It upgrades the Access Points and Controller.
Phase	Displays the different phases of the controller upgrade. Following are the types: • Image copy • Upgrade APs • Upgrade controller • Upgrade complete
Status	Displays the status of the controller. Following are the types: • **Success** - The controller is successfully upgraded. • **Failed** - The controller has failed to upgrade.

Field	Description
Error	Displays the error message of the only during the failure of the controller upgrade.
Upgrade Details	Displays the upgrade details of the controllers. Select the *Detail* link to view the *Log Details*. In the Nplus1 setup, the secondary log file displays a detailed information about the secondary and high level information about the primarys.

Deleting Upgrade History

You can delete a controller upgrade history by clicking the check box and select the *Delete* option.

Figure 179: *Upgrade History*

Upgrade Limitations

When an environment has an Nplus1 cluster with two different models (example: MC4200 and MC4200V combination), these controllers are not listed while trying to upgrade them from FortiWLM. When you select MC4200/MC4200V image in Upgrade management, it is not listed in either under cluster (since it is has two different models) or under individual controllers (since it is a cluster).

Tools

The *Tools* menu provides a *Search* and *Topology* options. The *Search function* allows you to explore for keywords appearing in data for *Reports, Inventory, Alarms, Configuration, and/or Stations*, including partial keyword search and advanced event filtering. The *Topology* provides at-a-glance system information and the logical placements of the hardware devices.

Search

Operate > Tools > Search

The search function is available on top of all windows and screens. You can use the search function to search for inventory, alarms, events, configuration profiles, and stations that are a part of your E(z)RF Application Suite. You can enter a keyword to search across all categories or you can narrow your search results by selecting appropriate filters as listed in the following table.

Filters	Descriptions and Options	Search Output
Inventory	You can search for all inventories that are currently connected or part of your E(z)RF deployment. Inventories are controllers and access points. To search for a controller or an access point, check the inventory option, type a keyword in the search text box, and select the *Search* option.	You can view a list of controllers with access points mapped to the selected controller that are connected to *FortiWLM* with the following details: • **Controllers**: The following controller details are displayed Controller Name, IP Address, Description, MAC Address, Model, Software Version, Availability Status, Administrative State, Location, and Controller Group. • **Access Points**: The following access points details are displayed: AP ID, AP Name, MAC Address, H/W model, Software Version, IP Address, Connectivity Preference, Location, Building, Controller, Availability Status, and AP Group.

Filters	Descriptions and Options	Search Output

		• You are allowed to navigate to the following screens, to view the controller or the controller mapped to the access point:
		  • Connect (Connects to the controller)
		  • Inventory Details (Navigates to the *Controllers* screen in *Operate* > *Inventory* > *Devices*)
		  • View Controller Dashboard (Navigates to the *Controller Dashboard* screen in *Monitor* > *Detailed Dashboard* > *Controller*)
		• Inventory Details (Navigates to the *Access Points* screen *in Operate* > *Inventory* > *Access Points*)
		• Topology (Navigates to the *Topology* screen in *Monitor* > *Topology*)
		• View AP Dashboard (Navigates to the *AP Dashboard* screen in *Monitor* > *Detailed Dashboard* > *AP*)
		• View Map Location (Navigates to the *AP Locator* screen in *Monitor* > *Overview* > *Heat Maps*)

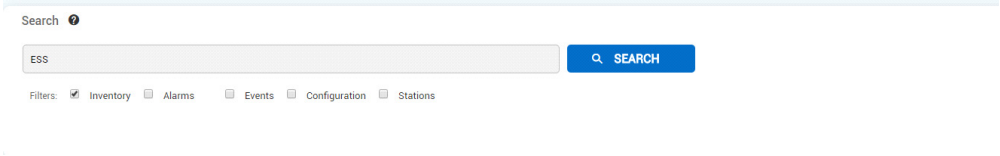
Alarms	You can search for all alarms that are notified by *FortiWLM*. To search for an alarm, check the alarm option, type a keyword in the search text box, and select the *Search* option. Narrow your search results by searching with *Active Alarms* or *History Alarms*.	You can view a list of alarms on FDN, notified by the *FortiWLM* with the following alarm details: FDN, Controller, Source, Alarm Name, Severity, Description, and Raised At. You are allowed to navigate to the Fault Management screen (*Monitor* > *Overview* > *Fault Management*) by selecting the View alarms link.

Filters	Descriptions and Options	Search Output
Events	You can search for all events that occur on the *E(z)RF Network Manger*. To search for an event, check the events option, type a keyword in the search text box, and select the *Search* option.	You can view a list of events that occur in *FortiWLM* with the following event details: Event Name, Severity, Source, FDN, Controller, Generated At, Description, Authentication Type, and Reason.

Configuration	You can search for all types wireless service profiles or individual profiles, users and user groups that are currently connected or part of your *FortiWLM*.
	Configuration includes *Profiles* and *Administration*.
	To search for a wireless service profiles or individual profiles, users and user groups, check the configuration option, type a keyword in the search text box, and select the Search option.
		• Profiles:
		  • You can view a list of wireless service profiles or individual profiles (ESS, Security, GRE, VLAN, RADIUS, RADIO, and Connectivity) with the respective SSID's and L2 Modes Allowed.
		  • You are allowed to navigate and view the respective wireless service profiles or individual profiles (ESS, Security, GRE, VLAN, RADIUS, RADIO, and Connectivity) by selecting the *View* link.
		• Users and User Groups:
		  • You can view a list of Users and User Groups with the following user details:
		User ID, User Name, User Group Id, User Description, Email Address, and Contact Details.
		  • You can navigate to the User screen (*Administration > User Administration > Users*) or the *User Groups* screen (*Administration > User Administration > User Groups*) by selecting the *View Users* and *View User Groups* link.

Filters	Descriptions and Options	Search Output
Stations	You can search for all stations connected to *FortiWLM*. To search for a station, check the stations option, type a keyword in the search text box, and select the *Search* option. Narrow your search results by searching with *Advanced Stations Filter*.	You can view a list of stations that are connected to *FortiWLM* with the following station details: MAC Address, AP ID, IPV4 Address, IPV6, BSSID, VLAN Name, ESS Name, User, Radio Type, and At Time. You are allowed to navigate to the Station Trend Dashboard screen (*Monitor* > *Detailed Dashboard* > *Stations*) by selecting the *View Station Dashboard* link.

Figure 180: *Search*

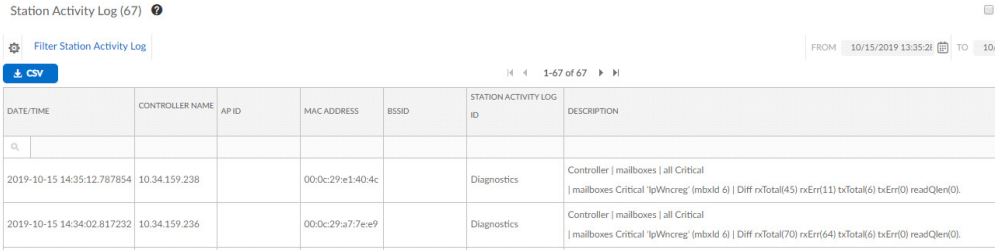


See the ***Search*** screen (*Operate* > *Tools* > *Search*) in Online Help for the details on search options.

Station Activity Log

The *Station Activity Log* represents the station events of all stations within the selected time 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 station history can be viewed and exported in CSV format (comma separated values) by selecting the *CSV* option. The event types are filtered by selecting the controller, event severity, event Id, and MAC address.

Figure 181: *Station Activity Log*



The *Station Activity Log* was called as *Event Viewer*, prior to the 4.0-6-0 release.

See the ***Station Activity Log*** screen (*Monitor* > *Detailed Dashboards* > *Stations)* in Online Help for the Station Log details.

System Log

The *System Log View* provides the log details of all the operations performed on NM. By default the syslog viewer displays messages from the last hour. If there are no messages in the past hour, the syslog window does not display any entries. The search for the logs can be performed in *Ascending* or *Descending* order. The system log *Date/Time, Application, Mnemonic, Priority, User, User Group, and Message* details are displayed. The *User* and *User Group* columns are displayed only if *Show All Columns* option is checked.

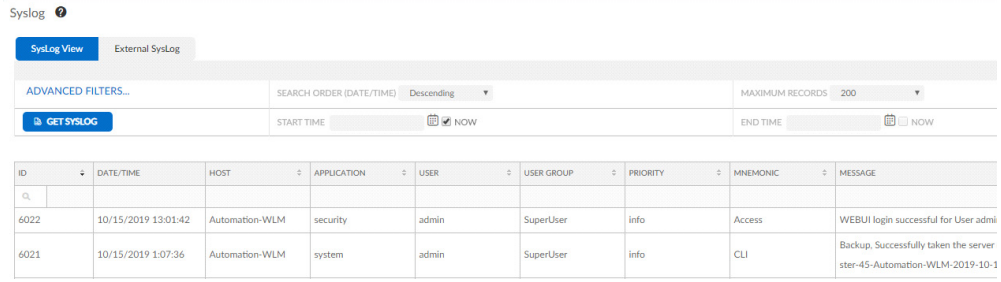
Any configuration changes done on the controller are reported in the FortiWLM syslog only when the FortiWLM IP address is registered to the controller as the syslog host. This is done using the Syslog CLI template (*Configure* > *Templates* > *CLI Template*) or the controller CLI mode.

Note: For Controllers discovered as VPN, FortiWLM VPN IP address must be registered with the controller.

View the *FortiWLM* logs by following these steps:

1. Navigate to *Operate* > *Tools* > *Syslog*. The Syslog View screen is displayed.

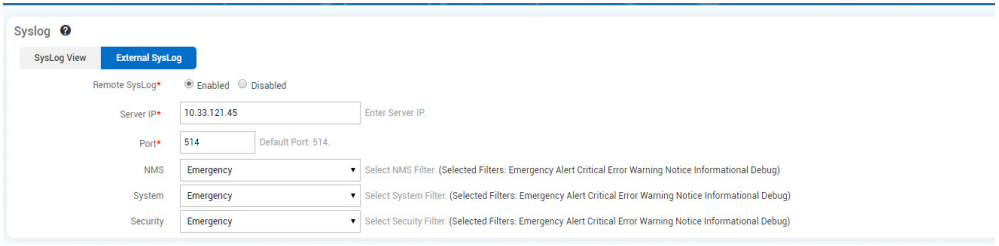
Figure 182: *Syslog View*



2. Modify the search order from *Ascending* to *Descending*.
3. Select the maximum number of records to display, 200, 500, 1000 or 2000.
4. Configure a *Start Time* and *End Time*.
5. Optionally, reduce the log results by adding a search filter.
   - Click *Advanced Filters > Add Filter.*
   - Select a *Filter ID, Operation* and *Filter Value*.
   - Click Close.
6. Click *Get Syslog*.

Export Syslog to External Server

Syslog from a FortiWLM device can be exported to an external syslog server. To export to an external server, configure the server details the type of logs to be exported.



Enter the following details:

- Select **Enable** to allow exporting the syslogs to an external syslog server.
- **Server IP**: The IP address of the external syslog server.
- **Port**: The port at which the external syslog server will accept incoming connection from FortiWLM.

- **NMS**, **System**, and **Security**: Select the type of logs from each of the category that will be sent to the external syslog server.

Syslog messages are raised during the following few scenarios:

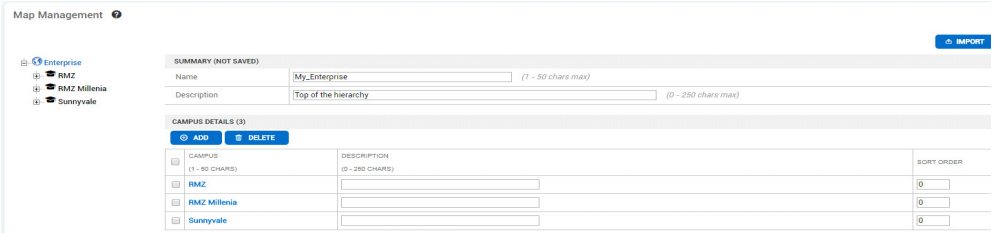
- When a new license file is uploaded.
- When a license file is removed.
- When the APs from the maps are removed during license enforcement.
- When the controller is marked as Unlicensed/Managed in case of license violation.
- When the CA certificates are imported, exported or deleted.
- When the server certificates are imported, exported, applied or deleted.
- When you create a CSR and export the CSR requests.

See the ***Syslog*** screen (*Operate* > *Tools* > *Syslog*) in Online Help for detailed information on *Syslog View* topic.

Map Management

You can create maps to track your APs visually. Maps must accurately represent the physical layout of the site and be as close to scale as possible. We suggest using a separate map for each floor in multi-level buildings and images based on accurate architectural drawings. Crop the map of each floor to remove any extra space and save it as a PNG, JPEG, BMP, or GIF file, no larger than 2MB adding the map to NM.

Figure 183: *Map Management*



There are multiple tasks required to set up a working map:

- Import a graphic map of the floor - *"Importing a Map Image"* ***on page 335***
- Add a new campus to FortiWLM -*"Add a Campus, Building, and Floor to the Map"* ***on page 337***
- Add a building
- Add a floor
- Place AP icons on the map to depict the WLAN network topology. *"Add APs, Floor APs and Landmarks to Maps"* ***on page 337***

- View the map - *"Viewing Maps"* ***on page 338***

Importing a Map Image

Complete the following steps to import a topology map:

1. If the Map Management screen is not displayed, click *Operate* > *Maps* > *Map Management*.
2. Select a floor.
3. Click *Change Image* in the Image Map section.
4. Select *Image Type* as *Floor* and *Operation* as *Upload*. Select the *Image File* by using the browse tab and click on Upload.

Next, add controllers and APs to the map.

Importing a Floor Map

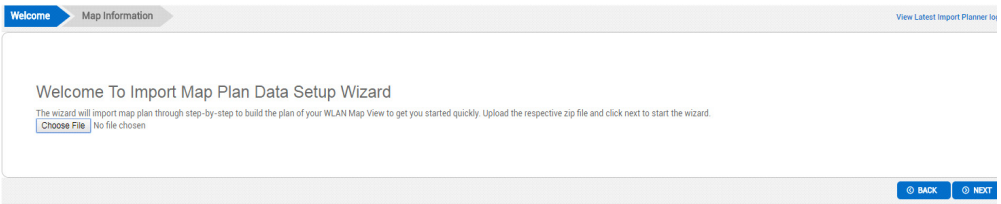
FotiWLM supports importing a floor map plan created on and exported from the FortiPlanner. Once the floor plan is created in the FortiPlanner, select **Export** in the project menu. The floor map to be imported is a *.zip* file.

Note:
Only exported *.zip* files from the FortiPlanner can be imported. Contact the Customer Support to obtain the relevant version of the FortiPlanner.

For more information on creating floor plans on the FortiPlanner, see the *FortiPlanner User Guide*.

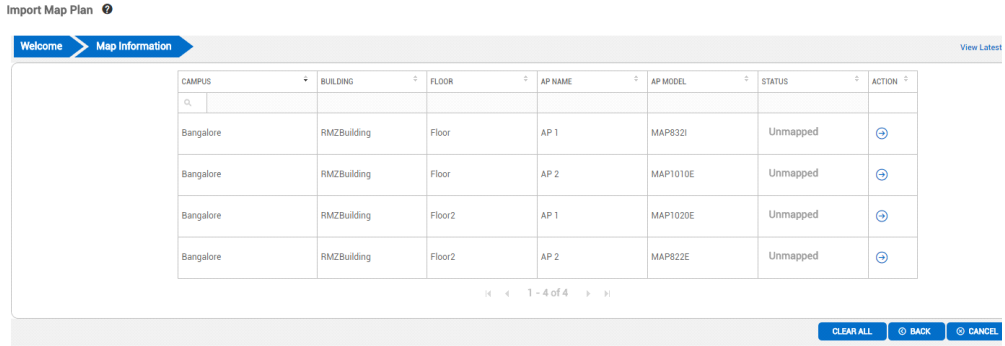
1. Navigate to **Operate > Maps > Map Management > Import.**
2. Click **Import**, the **Import Map Plan** screen is displayed.

Figure 184: *Import a floor map*



3. Browse to the *.zip* file on your system and click **Next**. A summary of map information is displayed.

Figure 185: *Map unassigned APs*



4. Map the unassigned APs and click **Finish**.
5. The planner for each campus is displayed. On the **Map Management** screen, you can add and delete floors in the map and manage the APs on each floor of the campus.

Figure 186: *Manage the imported map*

In case of errors importing the map, click **View Latest Import Planner logs**, to view the error logs.

You can perform the following operations on each floor:

- **Add APs** - Select the APs to be added to the floor map.
- **Floor APs** - Select the APs to be deleted from the floor map.
- **Landmarks** - Add or delete landmarks on the floor map.
- **Change Image** - Upload a new image or delete an existing image from the floor map.

Click **Save** to save changes to the map.

Add a Campus, Building, and Floor to the Map

Create a new location (campus, building, floor) in the enterprise by following these steps:

1. Click *Operate* > *Maps* >*Map Management*. All current maps are displayed on the *Map Management* page.
2. A new campus can only be added to the top level, *Enterprise*, which is the default. In the *Campus Details* section, click *Add*.
3. Provide a *name, description,* and *sort order* for the *campus*.
4. Click *Save Changes*.
5. In the left pane, double click the name of the new campus you just created.
6. Select the *Buildings* icon. In the *Building Details* pop-up, click *Add*.
7. Provide a *name, description* and *sort order* for the building.
8. Click *Save Changes*.
9. In the left pane, double click the name of the new building you just created.
10. In the *Floor Details* section, click *Add*.
11. Provide a *floor name, length, width, metric,* and *sort order* for the floor.
12. Click *Save Changes*.

Next, import a map image (see below).

Add APs, Floor APs and Landmarks to Maps

Once a map image has been imported, add the APs to create the network map of your site. The icons should be placed on the map as close as possible to the actual physical location of the APs.

To add detail to a map, follow these steps:

1. If the *Map Management* screen is not displayed, click *Operate* > *Maps* > *Map Management*.
2. Select a floor by its heading it in the left column.
3. You should see a map of the floor. If the floor does not yet have a corresponding map, complete the steps to *"Importing a Map Image"* ***on page 335***.
4. Optionally, alter the map using the options *Show Map* and *Show Scale* in the *Image Map* section.
5. Click *Add APs*, on the *AP selection* pop-up, select the APs to add from the drop-down list, then click *Save*. The selected AP appears on the map; drag it into position.
6. Add landmarks to the map by clicking *Landmarks* > *Add*.
7. Click *Save Changes*.

Viewing Maps

You can simply view the placement of APs on a map or you can view the *Heat Maps* using the following five attributes of those APs:

- Throughput
- Loss
- Channel Utilization
- Number of Stations
- Signal Strength

Heat map coloring depends on the distance between APs and selected attribute (throughput, loss, channel utilization, or stations) for all the APs on the floor. If there's only one AP on the floor, the entire floor will show the same coverage. View maps by following these steps:

1. Click *Monitor* > *Overview* > *Heat Maps*.
2. Select a *floor*. The map displays.
3. Optionally, alter the map using the options *Floor Visibility* or *Show Heat Map.*
4. Limit the map by clicking *Select Channels*, selecting channels, and then clicking *Save Changes*.
5. After any changes, click on *Refresh* icon.

RF Planner

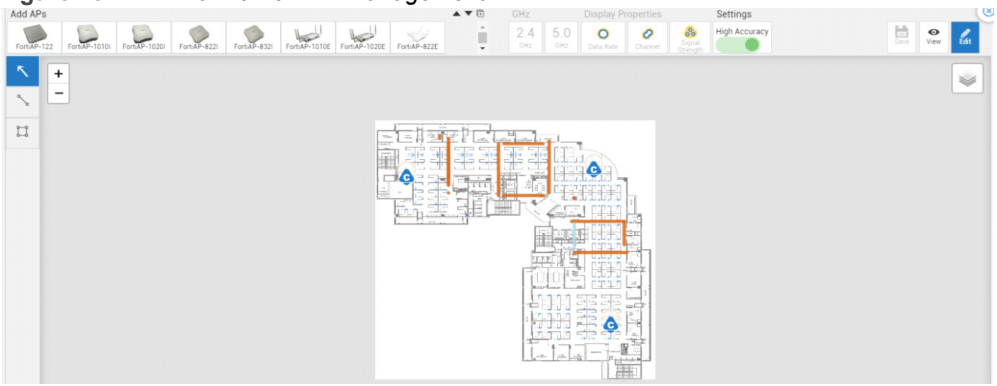
The RF planner allows you to plan for new access points, areas, and obstacles (walls, shafts etc.). The RF planner enables AP placement and drawing walls/columns, and is available in the **View** and **Edit** modes.

Add the required access points on the floor map and generate a heat map predicting the expected signal strength throughout the coverage area. You can change the placement of your APs based on the predicted signal strength and try out different placements for the APs prior to installing them on the premises. Hence, the RF planner allows you the following:

- Draw a floor plan of the coverage area.
- Place APs on your floor plan.
- Run heat maps to predict signal strength.

Navigate to *Operate* > *Maps* > *Map Management* > *RF Planner*.

Figure 187: *RF Planner for AP management*



You can add the required access points on the floor map and edit their configuration. Widgets are provided to draw walls and columns on the floor map.

View mode – The floor map displays the coverage pattern, data rate, channel, and signal strength of the access points. Select the 2.4GHz or 5GHz frequency to view the access point details.

Edit mode – New access points can be added/edited.

Drag the required access point from the **Add APs** panel and place it on the floor map. Right-click on an access point and edit the following configuration:

- Access point transmission power in dBm
- Access point channel
- Access point orientation
- **Ceiling**, **Wall**, and **Desk**
- Access point placement direction (in angles)

Widgets are provided to draw walls and columns on the floor map. Select the required widget and draw the wall or column on the map. A column is a closed drawing with four walls and a wall is demarcated as lines. Right-click on the created walls and columns to specify the composition/material used to construct them. Each material has a different attenuation value.

Administering Network Manager

The *System Administration* allows you to view and configure the following:

- *"User Preference"* ***on page 340***
- *"Licensing"* ***on page 344***
- *"Security"* ***on page 347***

- *"User Administration"* **on page 351**
- *"System Settings"* **on page 354**
- *"WLM Upgrade"* **on page 384**

User Preference

FortiWLM manages and monitors the performance of controllers. The *Notification* option allows you to notify when any NM managed controller goes down. The notification system identifies the alarm corresponding to the controller down condition and forwards the alarm to the user through email. A *notification profile* is set up to indicate the recipients for notification. A n*otification filter* is provided to indicate the type of error that triggers notification. To notify via email, set up an *SMTP Server* description. You can schedule email notification to occur regularly or you can send email only when a certain event occurs.

Set Up Email Notification

Complete these four tasks to set up email notification:

- Create a *User on Email,* See *"Create a User on Email"* **on page 362**
- Configure a *Mail Server* for *Notification*, See *"Configure a Mail Server for Notification"* **on page 362**
- Add a *Notification Profile*, See *"SNMP"* **on page 363**
- Add a *FortiWLM Notification Filter*, See *"Add a Notification Filter"* **on page 341**

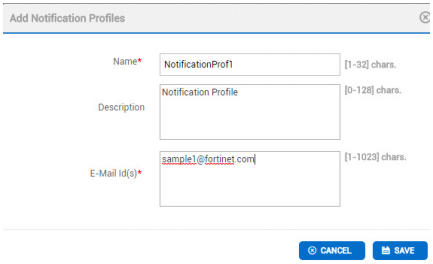
Add a Notification Profile

A notification profile comprises of a list of email Ids to indicate the error that triggers notification. The profile is created and referenced in *FortiWLM* notification filter or from an application that works with *FortiWLM*, for example *SAM*. You can associate multiple notifications to a single profile when you set up email notification using the notification filter. The filters discovers the names of profiles and displays them in a drop-down list during configuration.

To configure a FortiWLM notification profile, follow these steps:

1. Navigate to *Administration* > *User Preference* > *Notification Profiles* > *Add.*

Figure 188: *Notification Configuration - Add*



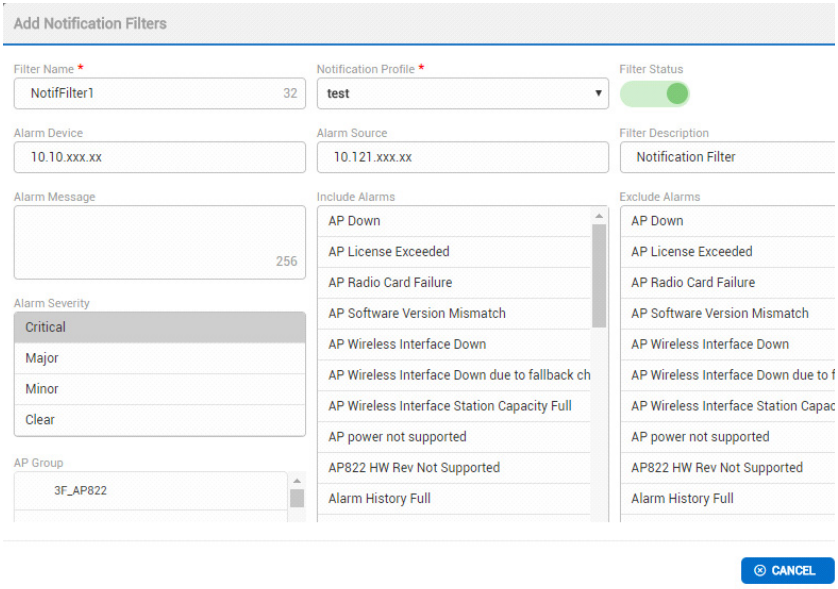
2. In the *Notification Configuration - Add* screen, enter a notification name such as *Critical_Alarm_Messages*.
3. Provide a description for the notification.
4. Provide the email addresses (up to 1024 characters). The following are the methods:
   - List each email address on a new line, such as:
     sandy@fortinet.com
     mike@fortinet.com
   - Separate the email addresses with commas such as: sandy@fortinet.com, mike@fortinet.com
5. Click *Save*.
6. You can associate multiple notifications to a single profile when you set up email notification using the notification filter.
7. The existing Notification Profiles can be modified and deleted. The profiles that are used by the filter cannot be deleted, an error message is thrown while deletion.

Add a Notification Filter

A notification filter specifies which alarms trigger notification. For example, if you select critical in the filter, only critical alarms will trigger notification. You can configure the notification filter and send the weekly report. To configure a filter, follow these steps:

1. Navigate to *Administration* > *User Preference* > *Notification Filters* > *Add.*
2. In *Notification Filters - Add* screen, provide the *Filter Name, Filter Description, Notification Profile,* and *Filter Status*. See *Figure 189 on* ***page 342***.

Figure 189: *Notification Filters - Add*



3. Configure the *Notification Filter* with one or more *Notification Filter Types* listed below. If you select multiple criterion, the alarm should meet all requirements for notification to be sent. For example, if you want only critical alarms from one particular controller, set both *Alarm Severity* and *Alarm Source* as the controller host name.

- **Alarm Severity** – Set this filter based on alarm severity. The values are *Critical, Major, Minor* and *clear*.
- **Alarm Severity Change** – Set notification to trigger when an alarm clears. The values are *Critical to Clear, Major to Clear,* and *Minor to Clear*.
- **Include Alarms** – Set this filter based on the alarms that occur. All the alarms are listed for this field and you can include multiple alarms in one filter set. The available alarms are:
  - AP CPU Usage High
  - AP Down
  - AP Memory Usage High
  - AP Radio Card Failure
  - AP Wireless Interface Down
  - AP Wireless Interface Down due to fallback channel not found
  - AP Wireless Interface Station Capacity Full
  - Controller CPU Usage High
  - Controller down
  - Controller Memory Usage High

- Controller unreachable
- DHCP Address Pool Exhausted
- Fan Module Failure (not supported on FortiWLM-100D))
- Link Down
- Primary Down
- Power Module Failure
- RADIUS Server Failed
- RAID status
- Rogue AP Detected
- Software License Expired
- Software License Violated
- System High Temperature
- Wired Rogue Detected

For detailed information on *configuring Alarms* and *Alarm definitions*, see the ***Fault Management*** screen (*Monitor > Overview > Fault Management*) in *Online Help*.

- **Exclude Alarms** – Exclude these alarms from the filter. All the alarms (see list above) are listed for this field and you can exclude alarms in one filter set. You cannot both include and exclude the same alarm.
- **Alarm Message** – Set the filter based on the substring to be matched in the Alarm message (the filtering is not case sensitive).
- **Alarm Source** – Set this filter based on the controller device that triggered the alarm. Provide an IP address or hostname for a controller.
- **Alarm Device** – Set this filter based on the source of the AP/device that triggered the alarm. The filter criterion enables you to filter the alarms based on the device on which the alarm is raised. For example, if AP MAC is provided, the alarms for the AP MAC are filtered.
- **AP Groups** - Select the AP Groups option, the Select AP Groups screen is displayed. Select an AP Group from the hierarchy and click *Save*. The selected AP Group is displayed in the AP Groups section. Each of the AP group consists of APs. A notification message is triggered, for the alarms raised for the APs within the AP Group.

4. Click *Save*.

There is AND operation across Filter Types and OR operation within the Filter Type. For example, if you want to receive all the critical alarms except Rogue alarms, configure the notification filter like this. Include Alarm severity - Critical and exclude Rogue Alarm type from the Exclude Alarms type list. On the other hand, if you want to receive any of the alarms (Critical or Major or Minor, or Clear) set the notification filter to include the “alarm severity” Critical or Major or Minor or Clear.

5. The Notification filters can be modified and deleted.

Licensing

The Licensing infrastructure is within *FortiWLM* and is applicable to the entire services appliance. The *FortiWLM* implements the license enforcement based on the AP count.

The *License* screen allows you to import a feature license key file for *NM* and its features installed on services appliance. You can request for *NM* license and upload it using *NM* web UI. A separate license key file is required for each feature that requires a license for operation. For instructions on procuring the license key file, see the *"Add a License"* ***on page 33***. Only one file can be selected and uploaded at a time. The Licensing Manager resumes whenever E(z)RF server restarts after a shutdown.

License Recovery and Backup

Licenses are a part of the server backup.

Licensing and Upgrade

The licensing is applicable after server reboots post the upgrade process. It is recommended to upload the license files before the upgrade. If licenses are not available after upgrade, APs will be marked unlicensed and the server is switched to a time limited validity. License (FortiWLM-NM-BASE) is required to monitor and manage controllers through *FortiWLM*. The License must be upgraded before it expires. The license expiry alarm is raised by the *FortiWLM* 30 days before its expiry. The License Violation message is displayed in the following scenarios:

- When the number of APs exceeds the number of licenses available for EZRF-NM-BASE feature.
- When the license for EZRF-NM-BASE feature has expired.

A grace period of 30 days is provided, during which the system functions normally. After the grace period, the controllers which does not have the required number of licenses for APs are marked as *Unlicensed* and will not be monitored by the *FortiWLM*. After licenses are added, the unlicensed controllers are automatically monitored by the Network Manger.

To access the Licensing through the NM web UI, perform the following steps:

1. Navigate to *Administration* > *Licensing*. See *Figure on* ***page 345***.
2. The *License* screen displays two sections as follows:

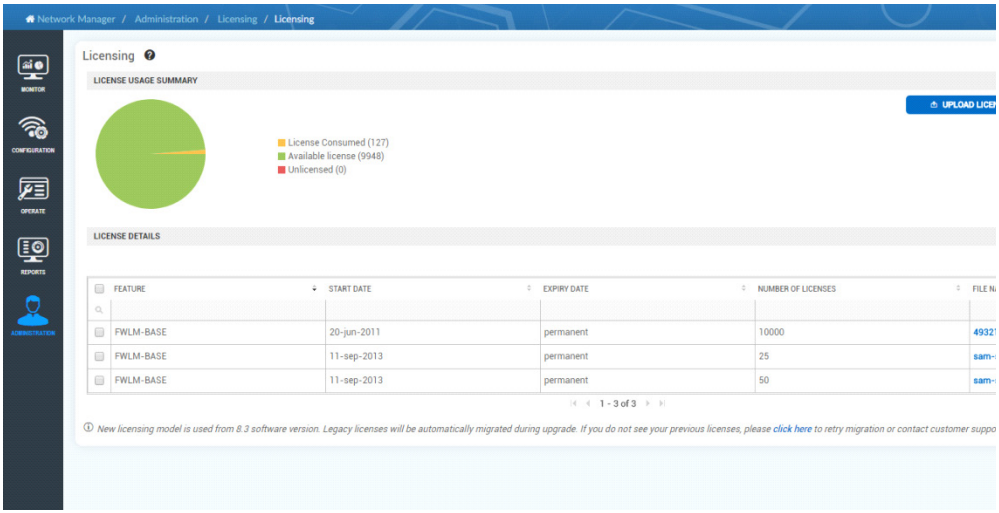
- *"License Usage Summary"* ***on page 345***
- *"License Details"* ***on page 346***

License Usage Summary

The *License Usage Summary* section provides a graphical representation of the License usage for *EZRF-NM-VISUALIZE, EzRF-NM-BASE and SAM*. The following graphs provide the visual representation of license usage.

- **License Consumed** - The number of used licenses is represented in YELLOW color.
- **Available licenses** - The number of unused licenses is represented in GREEN color.
- **Unlicensed** - The number of unlicensed licenses is represented in RED color.

Figure 190: *License Usage Summary*



The *License Usage Summary* section also provides the following links:

Request License

- Select *Request License* link to view the complete information of the license. The license information provides the following details:
  - **Serial Number** - Displays the manufacturer serial number.
  - **License Entitlement/Certificate ID** - Displays the License Entitlement number or the Certificate ID.
  - **System ID** - Displays the ID of the System.

The System ID is displayed only for SA200 and SA2000 services appliance.

- **VENDOR_STRING** - Displays the 32 digit hexadecimal ID of the system.

The VENDOR_STRING is displayed only for the SA2000-VE platform.

- **Feature Name** - Displays the name of the feature (*EZRF-NM-BASE and SAM and so on*) being licensed.
- **Number of licenses** - Displays the total number of licenses issued.
- **License Duration -** Displays the duration of the license (Permanent or Trial).

- Click the **Select All** button, to copy the above mentioned information and click **Close**.

Upload License

- Select *Upload License* Link.
- In the *Upload License* file screen, click *Browse* / *Choose* file button to locate and upload the license file (**.lmf**).

The *Upload License* allows a single license file upload. It does not provide the ability to upload multiple license files in one upload operation/session.

License Details

The *License Details* section summarizes the total number of licenses and provides the complete information about each of them. It provides the details of the *Feature, Start Date, Expiry Date, Number Of Licenses* and *File Name*.

See the ***License*** screen (*Administration* > *Licensing*) in Online Help for detailed information on *License* topic.

It may take 1-10 minutes to reflect the licenses after the license file is uploaded.

Limitations

The path of the license file saved, must not be too long. The license cannot be applied during such scenarios.

Security

The *FortiWLM* provides infrastructure to manage SSL certificates for various server applications that requires SSL certificate based authorization. The key services are:

- ***WEB Server Application* or *Security Certificate***
- ***VPN Server Application* or *VPN Administration***

Certificate Management

Certificates provide security assurance validated by a *Certificate Authority* (CA). This chapter describes the process to obtain and use certificates. For a Custom Certificate to work properly, you must import not only the Server Certificate, but the entire chain of trust starting with the issuer certificate all the way up to the Root CA. Server certificates are generated based on a specific *Certificate Signing Request* (CSR) and, along with the server certificate, you should get the entire chain of trust.

Generate CSR on the FortiWLM

The Certificate Signing Request or the CSR is a request sent from an applicant to a certificate authority in order to apply for a digital identity certificate.Generate a Certificate Signing Requests (CSR) directly on the *NM* using the web UI by following the below mentioned steps:

1. Select *Administration* > *Security Administration* > *Certificate Management*. The *Certificate Management* screen is displayed.
2. The *Certificate Management* screen displays the following tabs:
   - *"Server Certificates"* ***on page 347***
   - *"Trusted Root CA Certificates"* ***on page 282***

Server Certificates

The server certificates provides a list of generated Certificate Signing Request (CSR) and server signed Certificates.

1. In the *Server Certificates* tab, click *Create CSR*.
2. In the *Create CSR* window, provide the Certificate Alias, Common Name and Email Address
3. Optionally provide the Organizational Unit Name, Organization Name, Locality Name, State or Province Name and Country Code
4. Click Apply. The CSR is generated and appears on the *Server Certificates* tab Click *Close*.
5. Send the CSR to the Certificate issuer for it to be processed. If the CA asks for the operating system type, select Open SSL (if available) or Other.

6. The Certificate entry now displays in the *Server Certificates* page under “Pending CSR.” This entry will be matched to the certificates when they arrive and imported, ensuring that the controller that requested certificates is the only one to use those certificates.

Only the certificates with the *Status type CSR Generated* can be exported to *Export CSR* and can be saved to the hard disk. The other Status types like *In Use*, *Available,* and *Apply Failed*, cannot be exported and saved on to the hard disk.

Importing the Certificate

Remember that certificate request is sent to a CA for authorization. The issued certificate is then stored in an appropriate location. You can either use your own certificates or download factory-issued certificates from Fortinet.

1. Navigate to *Administration* > *Security* > *Certificate Management* > *Server Certificates tab* > *Import*.
2. In the *Import Certificate* wizard, browse for the authorized *Certificate File* by selecting the *Browse* option. Select the C*ertificate Alias* name that is to be imported from the drop-down list. Select *Save*. The authorized certificate is now imported.

Before applying the certificate, ensure if the corresponding CA is located under the trusted root repository by verifying the certificate's validity and the expiry date.

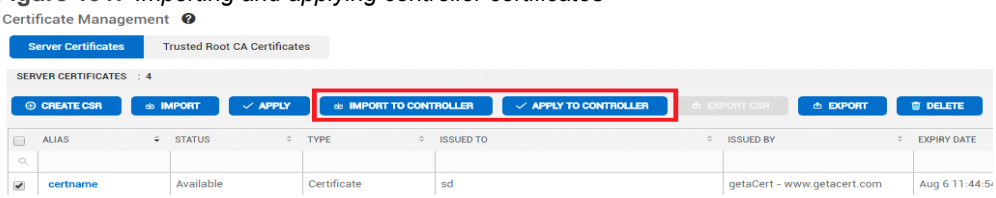
3. Other actions like *View CSR, Export,* and *Delete* can be performed.

Importing Controller Certificates

SSL certificates can be imported and applied to controllers. These certificates can be applied to all controller applications. FortiWLM supports uploading certificates to controller provided that the alias is unique and same certificate alias does not exist on the controller.

Default Certificate or WebEMS_x509 cannot be imported as it is already present on the controller and modifications are restricted; the default certificate can be applied to the controller.

Figure 191: *Importing and applying controller certificates*



Importing External Certificates with Private Key

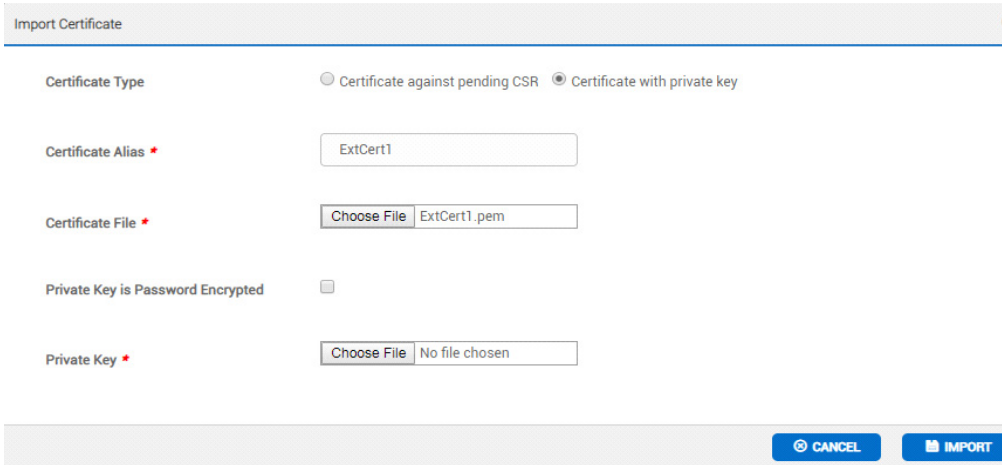
To import an external certificate with private key, select **Certificate with private key**.

1. Create the **Certificate Alias** name that is to be imported from the list.

2. Browse for the authorized **Certificate File** by selecting the **Browse** option.
3. Browse for the **Private Key**. If the key is password protected, select **Private Key is Password Encrypted** and enter the **Private Key Password**.
4. Click **Import**.

The certificate is now imported.

Figure 192: *Certificate with Private Key*



5. Select the certificate and click on **Apply.**
6. Select the VPN or web application and click **Save**. The certificate is applied.

Note:
Corresponding root certificates should be uploaded as trusted root CA certificates prior to uploading the server certificate with private key.

Trusted Root CA Certificates

The *Trusted Root CA Certificates* screen displays a list of trusted third party certificates. Any client or server software that supports the certificates maintains a collection of trusted CA certificates. These CA certificates allows *NM* to validate other certificates. *NM* can validate only certificates issued by one of the CAs in its Trusted Certificates Repository.

Import the Certificate

1. Navigate to *Administration > Security > Certificate Management > Trusted Root CA Certificates tab > Import.*

2. In the *Import Certificate* wizard, browse for the authorized *Certificate File* by selecting the *Browse* option. Select the C*ertificate Alias* name that is to be imported from the drop-down list. Click *Import*. The authorized certificate is now imported.

Before the certificate is applied to an application, a basic verification is performed to ensure,

if the certificate is a valid x.509 standard certificate,

if the expiry date has not crossed, and

if the imported certificate is actually a Root CA certificate.

3. Other actions like *Export CSR* and *Delete CSR* can be performed.

See the ***Certificate Management*** screen (*Administration* > *Security* > *Certificate Management*) in the Online Help for detailed information on *Certificate Management* topic.

VPN Administration

The virtual private network or the VPN based secure communication is enabled between the controller and *FortiWLM*. Only those controllers that are listed in the *FortiWLM*'s *VPN controllers and status list* are allowed to setup a VPN Tunnel with the *FortiWLM* server. Both VPN Controllers and non-VPN Controllers are managed at the same time with each controller being configurable to VPN and is set to the VPN tunnel with *NM*. The tunnel with the VPN server must be established prior to other communications by the *NM*. While using VPN, the controller and *NM* server consists of the tunnel IP address within the *NM* tunnel subnet. This tunnel IP-address is used by all applications and processes within the VPN Node (*Controller*, *FortiWLM*, and *SAM*) to communicate with other nodes. For VPN based communication, the endpoint of the tunnel serves as the *NM* server address.

Configuring the VPN

The system administrator must first configure the VPN connection settings on the services appliance. To configure VPN:

1. Select *Administration* > *Security* > *VPN Administration.*
2. Select the *VPN Server* tab. Enter the desired configuration for the VPN server. Provide the *VPN Service, Encryption, VPN Server Port, IP Pool* and *Net mask* details.

To reflect the changes performed on the *VPN Server* screen, the VPN service must be restarted. The restart is performed automatically.

3. Click *OK* to save the changes. The services appliance is now configured for VPN service and the details are displayed on the *VPN Controllers and Status* screen.

View the VPN Controllers and Status

The VPN Authorized Clients and Status screen displays a list of clients that are added. It displays the IP Address, VPN Tunnel IP Address, VPN Authentication Status and VPN Connectivity Status of each

See the VPN Administration screen (*Administration* > *Security* > *VPN Administration*) in the Online Help for detailed information on *VPN Administration* topic.

User Administration

The *User Administration* in the *Administration* allows you to configure the users and user groups and provide the access permissions.

Users

Users can be created, grouped and assigned group privileges from the web UI of *FortiWLM*. With user groups, users are not assigned permissions directly, but only acquire them by belonging to a user group. If you do not set up controller groups, all controllers remain assigned to the controller group named *Default.* The *Default Controller group* cannot be modified by the *Super user* group. By default, *Admin* belongs to the *Super user group* and *Guest* belongs to the *Default group*. The groups *Default* and *Super user* cannot be deleted nor can their access capabilities be altered. Any member of the *Super user group* can create more user groups and add people to them. Any changes made to group privileges affect all members of the group. Configurations created by a group member can be viewed, edited, or deleted by other members of that group.

A user with administration capability and with no inventory capability can see, create/modify user groups. We do not recommend this user configuration; in most cases, you want to add the Inventory capability to *Admin* users.

User Groups

The *FortiWLM* access assigned to a user group determines what users in that user group can do.

- **Monitor Capability**: Access to the *Monitor* tab and its sub-tabs only - no access to any other tab. This is the default assignment for a group.
- **Configuration Capability**: Access to the Configuration tab and its sub-tabs only - no access to any other tab. To configure controllers, a user must also have Inventory Capability.
- **Inventory Capability**: Access to the Inventory tab and its sub-tabs only - no access to any other tab
- **Report and Notification Capability**: Access to the Report and Notify tabs and their sub-tabs only - no access to any other tab

- **Visualization Capability**: Access to the Visualization tab and its sub-tabs only - no access to any other tab
- **Administration Capability**: Access to the Administration tab and its sub-tabs only - no access to any other tab

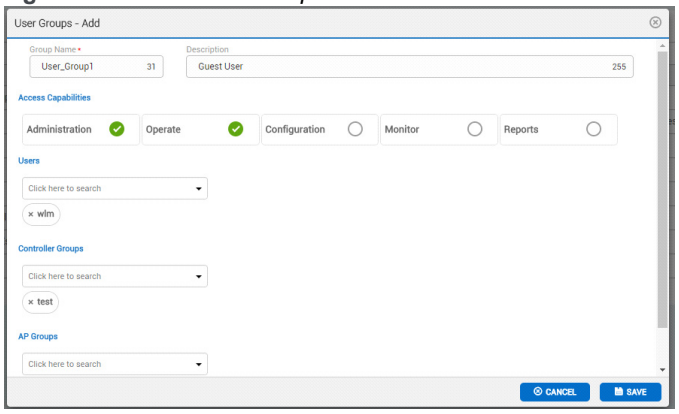
Pre-existing User Groups	Administration Tab	Inventory Tab	Configuration Tab	Monitor Tab	Reports and Notification	Visualization Tab
Superuser	X	X	X	X	X	X
Default (monitor Only)				X		

Adding a User Group

To create another user group (and optionally add users immediately), follow these steps:

1. Navigate to *Administration* > *User Administration* > *Users* > *Add.*
2. In the *Add User Group* screen, provide a name for the user group.

Figure 193: *Add User Group*



3. Optionally provide a group description.
4. Select the configuration for the user group (*Access Capability, Users, and Controller Groups*) as described below.

5. If you don't see the new group listed, click Refresh.

Access Capability	Determine the group access capability by checking tabs the users will be able to click and use: *Administration, Inventory, Configuration, Monitor, Report and Visualization*. After they are all checked, click **>>** to move them to the right. A user with administration capability but no inventory capability can view, create/modify user groups. We do not recommend this user configuration; in most cases, you want to add Inventory capability to Admin users.
Users	Add users to the group by checking names and then clicking **>>** to move them to the right. (Users were created previously by clicking *Administration* > *User Administration* > *Users*.)
Controller Groups	Add permission for users to access controller groups by checking controller group names and then clicking **>>** to move them to the right. The Default group is always present. To add more controller groups, see *"Controller Group Inventory"* ***on page 276***.
AP Groups	Add permission for users to access AP groups by checking the AP Group names and then clicking **>>** to move them to the right. The Default group is always present. To add more AP groups, see *"AP Group Inventory"* ***on page 279***.

6. Click *Save*.

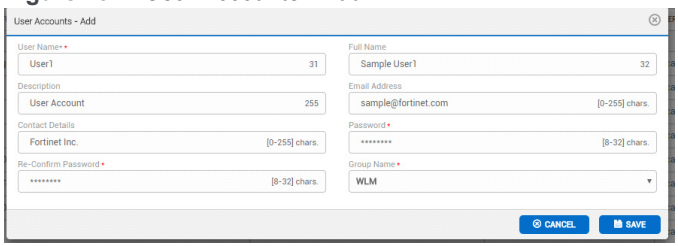
The *User Groups* can be modified or deleted by selecting the user, followed by selecting the respective options.

Adding New Users

To add new users, follow these steps:

1. Navigate to *Administration* > *User Administration* > *Users* > *Add*.
2. In the User Accounts - Add screen, provide a *User Name* and *Password*. It is mandatory to reconfirm the password.

Figure 194: *User Accounts - Add*



3. Select a *Group Name*. The Group Name drop-down box includes all the names of all user groups. *Default* is listed along with any additional groups that you created. A user can only belong to one group.
4. Optionally provide *Full Name, Description, Email Address,* and *Contact Details*.
5. Click *Save*.

The *Users* can be modified or deleted by selecting the user, followed by selecting the respective options.

View a User's Account

To see a user's account, click *Administration* > *User Administration* > *Users* > *View Details*. The following details for the selected user is displayed:

- User Name
- Full Name
- Description
- Email Address
- Contact Details
- Password (********)
- Group Name
- Last Updated

See the *Users* and *User Groups* screens (*Administration* > *User Administration* > *User Groups and Users*) in Online Help for detailed information on *User Groups and Users* topic.

System Settings

Server Details

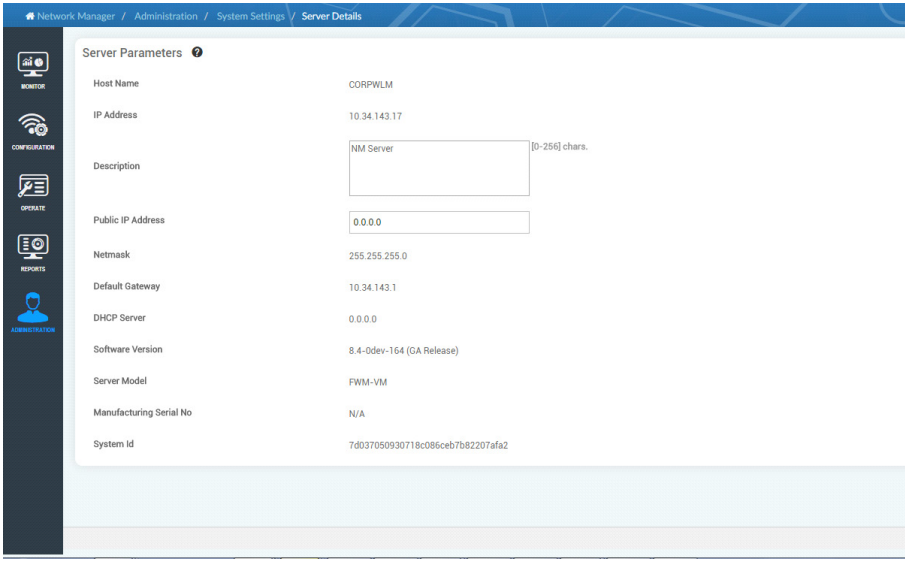
The server parameters screen allows you to view the server parameters of the *NM Services Appliance* (SA200, SA250, SA2000).

1. Navigate to *Administration* > *System Settings* > *Server Details*.

2. In the *Server Parameters* screen you can view the following details.

Field	Description
Description	Displays the user assigned description for the services appliance. For example, it might include appliance location, such as Building_1, Floor2. This field can be modified.
Public IP Address	Displays the IP address. This field is configurable when the FortiWLM server comprises of public IP address.
Host Name	Displays the services appliance host name assigned by DNS. Typically, administrators maintain the same host name even if the IP Address is changed.
Uptime	Displays the elapsed time since the last reboot.
IPv4 Address	Displays the IPv4 address of the appliance that is used to connect FortiWLM GUI.
IPv4 Netmask	Displays the subnet mask for the IPv4 address.
IPv4 Default Gateway	Displays the IPv4 gateway for the appliance.
IPv6 Global Address	The global scope IPv6 address of the appliance used to connect FortiWLM GUI.
IPv6 Link Local Address	The link-local IPv6 address.
Default IPv6 Gateway	IPv6 gateway for the appliance.
DHCP Server	Displays the if the appliance comprises of a static IP address. If it does not comprise of a static IP address, then the DHCP server assigns one.
Software Version	Displays the software version of the NM server.
Server Model	Displays the NM server model number (SA200, SA250 or SA2000)
Manufacturing Serial #	Displays the serial number of the NM server.
System ID	Displays the system ID of the NM server.

Figure 195: *Server Parameters*



Diagnostics

You can collect the *FortiWLM* diagnostics comprising of NM related logs and other files from *Administration* > *System Settings* > *Diagnostics*, download them to a local folder and send to *Fortinet Support* to aid in troubleshooting.

1. Select *Generate Diagnostics* option on the header of the FortiWLM dashboard.
2. You will be redirected to *Administration* > *System Settings* > *Diagnostics*.
3. The data collection starts and the browser window displays the collection status and progress. After the collection is complete, a message for the successful completion of the diagnostics generation is displayed.
4. Select *OK*.
5. The downloaded file is displayed as "*(Latest)*" highlighted with green color.
6. In the Diagnostics screen, you can view the old and latest diagnostics with the below information and perform the following actions:

Field	Description
Date/Time	Displays the *date and time* of the diagnostics captured in mm/dd/yyyy and hh:mm:ss format.
File Name	Displays the diagnostics file name.
Size	Displays the size of the diagnostics file name in KB.

Field	Description
Download	Allows you to download the diagnostics for troubleshooting. To download the diagnostics, follow the below mentioned steps: **1.** Select download icon. **2.** At the *File Download* dialog prompt "*Do you want to open or save this file?*", choose one of the below mentioned options: • **Open with**: • Select *Open* with option to view the diagnostics. • The preferred format to view the diagnostics is *.tar.gz*. • Select *OK*. The *WinZip* application opens. • In *WinZip*, highlight the file listed in the zip archive and click *View*. The *View* dialog displays. • **Save File**: • Select *Save File* option to save the diagnostics. The preferred format to download the diagnostics is *.tar.gz*. • In the *Save As* dialog that opens, navigate to the location you wish to save the file and click *Save*.
Delete	Allows you to delete the selected diagnostics. Select the older diagnostics by clicking the checkbox and click on *Delete* option to delete them from the Diagnostics screen.

Controller Diagnostics

The Controller diagnostics collects the AP and controller crash logs and general diagnostics from FortiWLC. Click on the Generate Diagnostics option to collect diagnostic information about specific controllers.

Note: Download Controller Diagnostics/Snapshot/Crash/Feature Diagnostics file support is available from FortiWLC 8.5.1 and above.

High Availability

High availability provides concurrent and persistent server access using a cluster two instances (primary and backup) of Network Manager. After setting up HA, the Network Manager Server is accessed via a virtual IP. When the connection to the primary server is lost, the backup server continues to provide all services. After the primary server recovers, the control is transferred to the primary server. New data collected by the backup server (during primary outage) is copied and synced between both primary and backup servers.

Note: The license is synchronized between the primary and backup servers. Hence, one license is adequate to manage devices on both the FortiWLM servers.

Configuring High Availability

Configuring HA requires you to add settings to both the servers (primary and backup). To begin setting up HA, access the WebUI of one of the server instance that should be configured as the primary server.

Setting up Primary Server

Go to *Administration* > *System Settings* > *High Availability* > *Cluster Configuration* and update the following:

- Server Mode: Since this server is to be configured as the primary server, select **Primary Server**.
- Secondary Server: Enter the backup server IP address.
- Enter the Shared Secret key.

Click the **Save** button to enable HA functionality.

New tabs **HA Authentication**, **IP Address High Availability** and **Status** are enabled after you save the settings.

HA Authentication (Primary Server)

This tab provides options to export the SSH authentication file which is later imported in the backup server and import the exported SSH authentication file from the backup server.

Click on **EXPORT AUTHENTICATION** to export the SSH authentication file to the local machine, to be later imported into the backup server.

Click on **IMPORT AUTHENTICATION** to import the SSH authentication file which is exported from the backup server.

IP Address High Availability (Primary Server)

This tab provides options to configure the virtual IP address for HA access.

1. Enable VRRP.
2. Set the **Server Mod**e as **Primary**.
3. Enter the Virtual IP Address. This address must be from the same subnet and DHCP pool use to provide the IP address of both instances of the FortiWLM servers. It is recommended that you use a static IP as the virtual IP.
4. Ethernet Interface is automatically populated based on the model of FortiWLM Servers.
5. Enter a **Shared Secret ke**y. This key is used by the server to maintain keep alive between the two servers.

Setting up the Backup Server

In the WebUI of the backup server, update the following:

1. Server Mode: Since this server is to be configured as the backup server, select Backup Server.
2. Enter the IP address and Hostname of the Primary Server.
3. Enter the Shared Secret key.
4. Click the Save button.

New tabs, **HA Authentication** and **IP Address High Availability** are enabled only after you save the settings.

HA Authentication (Backup Server)

This tab provides options to export the SSH authentication file which is later imported in the primary server and import the exported SSH authentication file from the Primary server.

Click on **EXPORT AUTHENTICATION** to export the SSH authentication file to the local machine to be later imported to the primary server.

Click on **IMPORT AUTHENTICATION** to import the SSH authentication file which is exported from the primary server.

IP Address High Availability (Backup Server)

This tab provides options to configure the virtual IP address for HA access.

1. Enable VRRP.
2. Set the **Server Mode** as **Primary**.
3. Enter the Virtual IP Address. This address must be from the same subnet and DHCP pool use to provide the IP address of both instances of the Network Manager servers. It is recommended that you use a static IP as the virtual IP.
4. Ethernet Interface is automatically populated based on the model of Network Manager Servers.
5. Enter a **Shared Secret key**. This key is used by the server to maintain keep alive between the two servers.

Status

Replication Status shows the available servers in the cluster. The cluster table contains status of the servers whether they are presently up or not and also shows the configured status of the server.

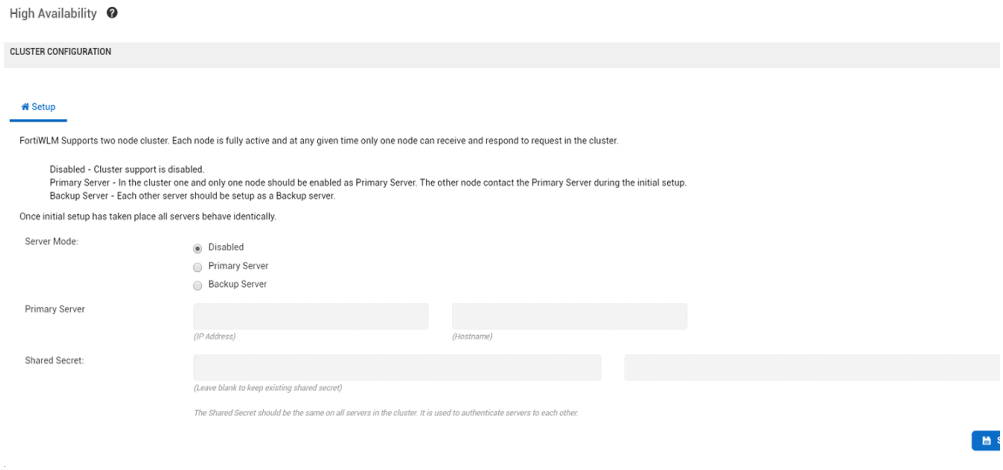
If one server is down it shows the status as "Not working". The configured server could be either Backup Server or Primary Server. User can identify the server status by logging into the

server and checking the server status and for the logged in server it shows as "this server". Also users can check the configured IP addresses of the both Primary and Backup node.

Disabling the HA Cluster

You can disable the HA Cluster and make the primary and backup servers run independently. Perform the following steps on the primary and backup servers.

1. Go to *Administration> System Settings > High Availability > Cluster Configuration*.
2. In the **Setup** tab, set the **Server Mode** to **Disabled**.
3. Click the **Save** button to disable the HA cluster.



Note:

- Reboot the backup node after disabling the HA cluster.
- By default, services on the backup node do not restart after the cluster is disabled. This is because the Controllers start the discovery process on both the primary and backup Forti-WLMs. To restart and use the backup node independently, contact the Forticare Support.
- Once services are restarted on the backup node, delete the existing Controllers and start managing with the new set of Controllers.

Authentication

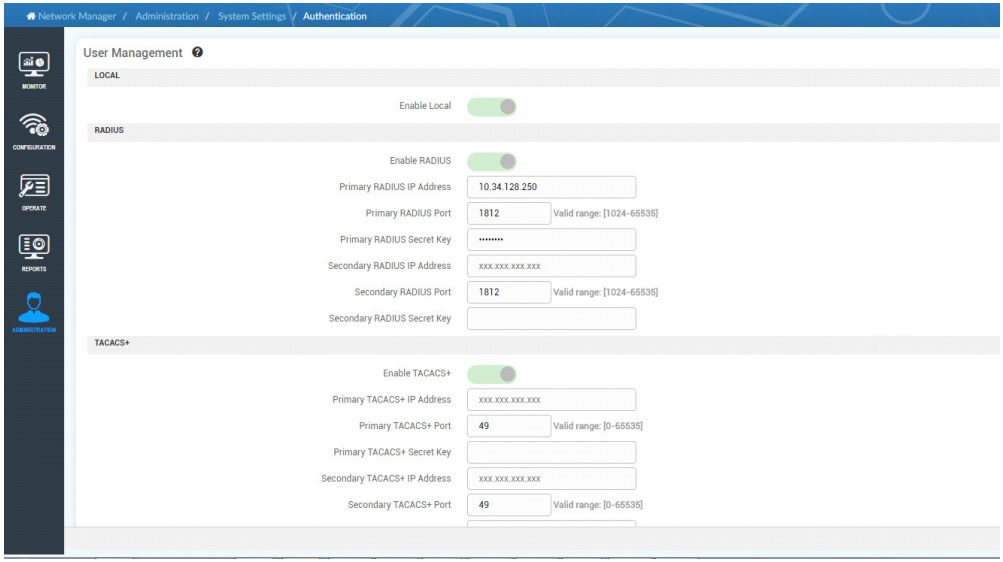
You can add users who can authenticate via TACACS+, RADIUS, or local administrator to access FortiWLM servers. Multiple authentication modes (Local, Radius and TACACS+) can be enabled at a time and authentication to the FortiWLM server can be done using any of the enabled authentication modes. The default user *admin* authentication is possible even when

the **Local** authentication mode is disabled. The order of authentication when all three modes are enabled is Local, Radius and then TACACS+.

Note: No CLI access is provided for non-admin, RADIUS and TACACS+ users.

By default, **Local** authentication mode is enabled.

1. In the FortiWLM WebUI, Go to *Administration* > *Authentication* page.
2. Select the authentication type and enter the related details about the selected authentication server



RADIUS User Authentication

RADIUS user authentication is based on the ***Filter-Id*** attribute value set in the *Connection Request Policies* or *Network Policies* in the RADIUS server.

- The ***Filter-Id*** attribute value set between **1-14** in the RADIUS server allows **monitor only** access to the FortiWLM. This is the lowest authentication level and you can only access the **Monitor** tab in the GUI to view dashboards and related statistics. No configuration changes are allowed.
- The ***Filter-Id*** attribute value set to **15** in the RADIUS server allows **administrative** access to the FortiWLM. You can access FortiWLM as a super user and make configuration changes including adding controllers and applying for license.

This configuration is supported with the Windows Network Policy Server.

Note: When ***Filter-Id*** is set in both *Connection Request Policies* and *Network Policies,* you will have monitor access only.

TACACS+ User Authentication

TACACS+ users authentication is based on the privilege level access in FortiWLM.

- The ***priv-lvl*** attribute value set between **1-14** in the TACACS+ server allows **monitor only** access to the FortiWLM. This is the lowest authentication level and you can only access the **Monitor** tab in the GUI to view dashboards and related statistics. No configuration changes are allowed.
- The ***priv-lvl*** attribute value set to **15** in the TACACS+ server allows **administrative** access to the FortiWLM. You can access FortiWLM as a super user and make configuration changes including adding controllers and applying for license.

Only Cisco ACS server/Cisco ISE is supported for TACACS+ authentication.

Mail Servers

When an error occurs, *FortiWLM* can notify you by email. To indicate the error that triggers notification, set up a *Notification Filter*. To indicate who should be notified and how they are notified, set up a *Notification Profile*. To turn notification *on* and *off,* activate or deactivate the filter.

To notify via email, set up an *SMTP Server* description. You can schedule email notification to occur regularly or you can send email only when a certain event occurs.

Set Up Email Notification

Complete the below tasks to set up email notification:

- Create a User on Email, See *"Create a User on Email"* ***on page 362***
- Configure a Mail Server for Notification, See *"Configure a Mail Server for Notification"* ***on page 362***
- Add a Notification Profile, See *"SNMP"* ***on page 363***
- Add a *FortiWLM* Notification Filter.

Create a User on Email

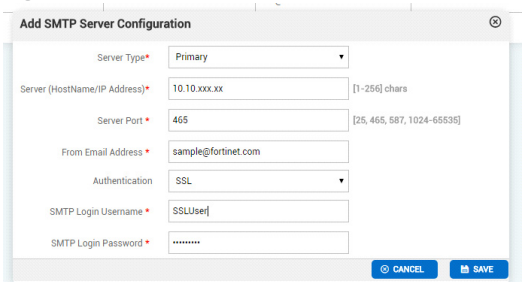
On your email system, create a user like *alert@fortinet.com*. You will use this email user to configure a mail server for notification, add a notification profile, and add a *NM* notification filter.

Configure a Mail Server for Notification

FortiWLM needs mail server information to send automated emails. These servers are used for email notification. To configure the mail server, follow these steps:

1. Navigate to *Administration* > *System Settings* > *Mail Servers* > *Add.*

Figure 196: *SMTP Server Configuration - Add*



2. In the S*MTP Server Configuration - Add* screen, provide the following details.
3. Select primary or secondary for *Server Type*. The *FortiWLM* uses the available primary server.
4. Enter the host name (for example smtp145) or IP Address (IPv4/IPv6) of the SMTP Server (for example, 10.1.4.5). Each field has a maximum of 256 characters.
5. Indicate which port the *SMTP Server* uses. The default server port is 25. If the SMTP server uses another port, modify this setting (1 - 65535).
6. Enter the *From Email Address* (up to 256 chars). The *From Email Address* is the email address you set up to *Create a User on Email*.
7. If you need authentication to access email, change *No* (default) to *Yes*. If Authentication is set to *Yes*, enter an *SMTP Login Username* (up to 64 chars). Enter the corresponding password (up to 64 chars) in the *SMTP Login Password*.
8. You have the option to use a secure connection to send mail. Set it to *Yes* if the *SMTP Server* is enabled with *Secure Connection*. The default option is *No*.
9. Select *Save*. The mail server configuration is added and displayed on the *MTP Server Configuration* screen.
10. To update *SMTP Server Configuration* information, click *Refresh*.

SNMP

Forti WLM supports all versions (SNMPv1, SNMPv2c, and SNMPv3) of SNMP Protocol.

Forti WLM doesn't support write operation through SNMP. You need to provision any required configuration through the web UI.

SNMP displays management data in the form of variables on the managed systems, which describe the system configuration. It uses an extensible design, where the available information is defined by *Management Information Bases* (MIBs). The MIBs describe the structure of the management data of a device subsystem; they comprise a hierarchical name space containing *object identifiers* (OID). Each OID identifies a variable that can be read via SNMP.

MIB Tables

The MIB tables SNMP implementation can be downloaded from NM. The MIB Tables are also available on the Fortinet web site. A summary of the Forti WLM MIB Enterprise tables are:

- mnmControllerInventoryEntry
- mnmControllerStateEntry
- mnmAPEntry
- mnmStationEntry
- mnmApIf80211Entry
- mnmApIf80211statsEntry

Download the MIB Tables for Management Applications

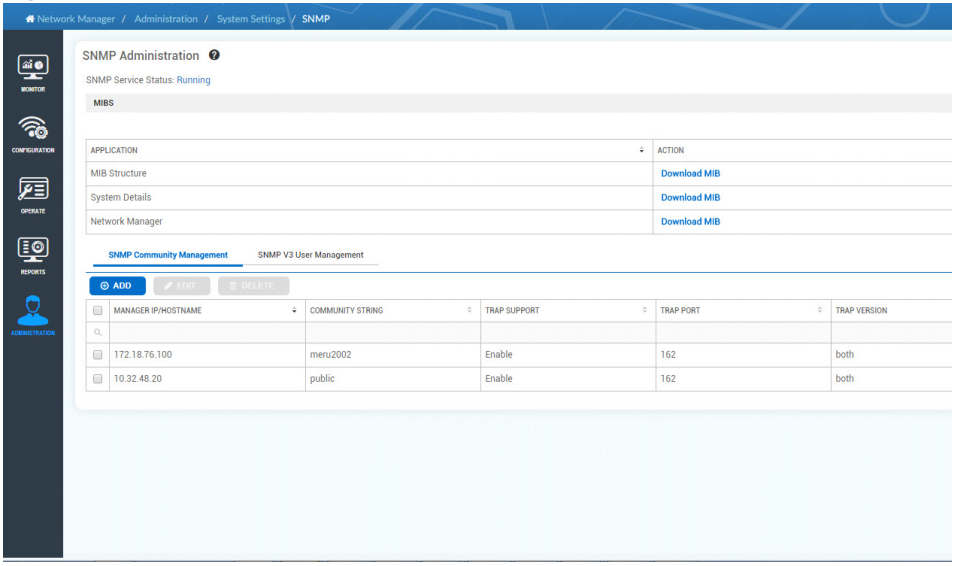
If you are using a third-party SNMP-based *FortiWLM* program, you will need to integrate the Fortinet *NM* proprietary MIB tables that allow the manager program to manage controllers and APs. The MIB tables are available in a compressed (zipped) file that can be copied from the services appliance.

1. Open a Web Browser (IE or Firefox), enter the system IP address (example: https://172.29.0.133) and then enter a user name and password (factory default user name/password is admin/admin).
2. Navigate to *Administration* > *System Settings* > *SNMP* > *Download MIBs*.
3. When the download is complete, you will see the file listed in the *Downloads* list.
4. Save the file mibs(x).tar.gz.

Configure SNMP Service on Forti WLM With the Web UI

1. Open a Web Browser (IE or Firefox), enter the system IP address (example: https://172.29.0.133) and then enter a *User Name* and *Password* (factory default user name/password is admin/admin).
2. Navigate to *Administration* > *System Settings* > *SNMP*.

Figure 197: *SNMP Administration*



3. The *SNMP Administration* screen allows you to perform the following actions.

Stop and Restart an SNMP Service

The following two actions can be performed:

- **Stop SNMP**: This allows you to *Stop* the SNMP and its related applications running on the services appliance.
- **Restart SNMP**: This allows you to *Restart* SNMP and its related applications running on the services appliance.

Status of SNMP Service

- **Stopped**: Here, the SNMP and its related applications are Stopped. The SNMP functionality like *SNMP Configuration*, *Trap Forwarding* and *SNMP Get Requests* are disabled.
- **Running**: Here, the SNMP and its related applications are Up and Running. The SNMP functionality like *SNMP Configuration*, *Trap Forwarding* and *SNMP Get Requests* are enabled.

SNMP Registered Applications on Services Appliance

The below include the list of installed applications registered with the SNMP Manager on the services appliance and are listed for SNMP requests:

1. FortiWLM
2. Service Assurance Manager
3. WIPS

Download MIBS

Download All MIBS to install all applications and **Download MIBS** to install individual applications is installed on the services appliance.

Configure SNMP Parameters

The **SNMP Parameters enables** you to register the external SNMP Managers with the *FortiWLM*. The SNMP v1, v2c and v3 versions are supported to receive requests. The v1, v2c and both are supported for trap forwarding. The *SNMP Administration* screen provides the following tabs to configure the SNMP parameters:

- *"SNMP Community Management"* ***on page 366***
- *"SNMP V3 User Management"* ***on page 366***

SNMP Community Management

The SNMP v1 and v2c requests are diverted to the *SNMP Community Management* tab.

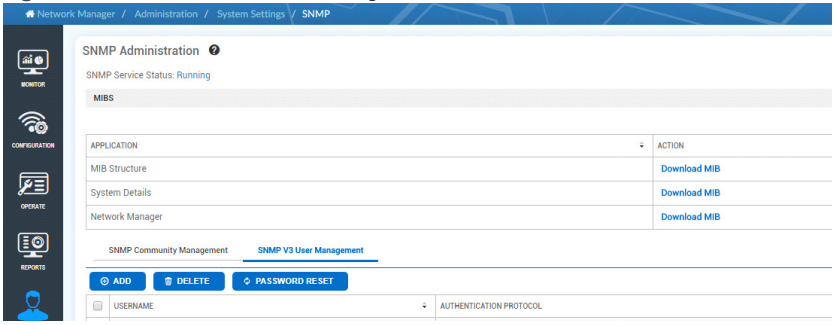
Select *Add* on the *SNMP Community Management* tab. Provide the *Manager IP / Hostname, Community String, Trap Support, Trap Port* and *Trap Version*. Traps for the respective *Manager IP / Hostname* can be filtered by selecting the *Trap Filter* option. The SNMPv1 and v2c traps can be modified or deleted by selecting the respective options.

SNMP V3 User Management

The *SNMP v3* user configurations are diverted to the *SNMP v3 User Management*.

Select *Add* on the *SNMP v3 User Management* tab. Provide the *Username, Authentication Protocol, Authentication String, Privacy Protocol, and Privacy String*. The password of an individual *SNMP v3* can be modified by selecting the *Password Reset* option. The SNMP v3 can be deleted by selecting the respective option.

Figure 198: *SNMP V3 User Management*



See the ***SNMP Administration*** screen (*Administration* > *System Settings* > *SNMP*) in Online Help for detailed information on *SNMP Administration* topic.

Backup Administration

The *FortiWLM* server provides an option to backup and restore the database. The backup database is stored on the server in a pre-defined location. The administrator can restore the database from the backup files. The data backup requires 5GB of free disk space which includes the following information:

- Maps
- Reports
- Licenses
- Controller configuration backup files
- Upgrade logs
- ***Database Information***: The database information includes the **`nmsdb`** database and **`eventdb`** database.

The backups have two different naming conventions that is, one for a complete backup and the other is for the configuration-only backup. The backups are stored in tar file format.

Automated Backup

The data backups can be scheduled daily or weekly. The following are the default values:

- The daily backups are scheduled by default at 1.00 a.m.
- The weekly backups are scheduled by default at 1.00 a.m. on Sunday.

See *"Map Management"* ***on page 334*** for further details.

Backup History

The *FortiWLM* backup history can be viewed by following the below mentioned steps:

1. Click *Administration* > *System Settings* > *Backup History*.
2. The *Backup History* screen is displayed providing the log of the backup and restore activity.

The two possible states for a backup are *Passed* or *Failed*.

If a backup or restore fails, an alarm is raised displaying an error message which is logged into the file **`/data/apps/nms/logs/backup_restore.log.`** An alarm is raised only if the backup fails.

To accomplish this from the CLI, use the command **`sh backup`**; this command lists all backup entries in the backup **`directory /data/backup/nms`**.

If a backup failed after reaching the maximum hard disk size, the backup entry is listed in the backup history table as **`failed`**. Also, a failure message is stored in the **`log backup_re-`**

store.log. To view the **backup_restore.log**, use the CLI command **show backup-restore-history**. This lists the last 25 entries in the log.

Restoring a Backup

You can restore a backup only from the command line interface (CLI). The following are lists of commands to restore a backup:

- **sh backup** lists all backup entries (including failures) in the backup **directory /data/backup/nms**.
- **show backup-restore-history** displays the last 25 backup entries and all failure messages in the **backup_restore.log**.
- **restore <filename>** restores the complete backup.
- **backup [config-only]** performs a backup configuration data.
- **backup [all]** performs a backup complete server data.

See the *"FortiWLM - Command Line Interface"* ***on page 529*** command for details.

Restoring a Backup From External Location

The backups are stored in the tar file.

To restore a backup from an external location, use the **copy** command to *copy* the file back to the appliance, and then use the **restore** command to *restore* the backup. You can also use the CLI command **show backup-restore history** to see all saved backups.

Two backups from the command **backup all** are saved by default. The results of **backup config-only** are not automatically deleted. All of those tar files are saved until you delete them.

An admin can recover a backup from the CLI with the command **restore**. You have two restore options, either *restore the entire backup* or *restore only the configuration information*.

For example, to restore the entire backup *Backup-2014-03-05*, including statistics, from the **backup directory /data/backup/nms,** use this command:

```
default# restore Backup-2014-03-05-01-01-01.tar.gz
```

Restoring only the configuration information restores information like *maps, controller details, and AP details*. Other than statistics, everything is restored.

For example, to restore the configuration only from the file Backup-2014-03-05, use this command:

```
default# restore Backup-2014-03-05-01-01-01.tar.gz config-only
```

Restoring a particular table in the database is not supported.

Restoring the backup data depends upon the data present in the server.

Deleting a Backup

You can delete a backup only from the command line interface (CLI). The following are list of commands to delete a backup:

- **`sh backup`** lists all backup entries (including failures) in the backup **`directory /data/backup/nms`**.
- **`show backup-restore-history`** displays the last 25 backup entries and all failure messages in the **`backup_restore.log`**.
- **`delete backup`** deletes backups.

See the *"FortiWLM - Command Line Interface"* ***on page 529*** command for details.

For example, the command **`delete Backup-2014-03-05-01-01-01.tar.gz`** deletes the backup named **`Backup-2014-03-05-01-01-01.tar.gz`** from the backup **`directory /data/backup/nms`**

Preserve Backup on Remote Server

To preserve backup on remote server you must transfer the data backup to a remote host. Refer to the *"Transfer Backups To Remote Host"* ***on page 377*** for further information.

Cleaning up of unwanted data

The server automatically deletes the historical statistics of backup. Configure the *"Number of Backups To Preserve"* ***on page 376*** and the number of *"Months to keep statistics data"* ***on page 378*** to reduce the disk usage.

A minimum of 5GB free disk space is required to backup the data.

If you want to preserve backups before they are deleted, copy them from the appliance to another location with the CLI copy command, for example:

```
#copy /data/backup/nms/Backup-2014-03-05-01-01-01.tar.gz ftp://anony-
mous@<ip address>/
```

Ensure to copy the latest backup file off the box periodically.

Use the CLI commands **backup all** or **backup config-only** to perform a CLI backup of the appliance when you are logged in as admin; When you execute these CLI commands, the web UI history is also updated.

Flash Backup and Restore with Snapshot

Note:
Snapshot is supported **ONLY** on 32-bit FortiWLM and is **NOT** supported on 64-bit FortiWLM.

The services appliance comprises of a partitioned flash. Two copies of the flash image are maintained so that you can restore the flash if the original becomes corrupted. The flash recovery feature verifies existence of at least one snapshot of the disk on every Saturday and automatically creates a snapshot of the boot partition on the disk, if there is no partition. This ensures that there is at least one snapshot of the disk, though you may not have created it yourself.

The snapshot CLI commands let you copy, view, and delete the flash configuration on the hard disk in the services appliance. For command details see See the *"FortiWLM - Command Line Interface"* ***on page 529*** command for *snapshot create, snapshot delete, snapshot restore,* and *show snapshot* command details.

Create a Flash Backup on Disk with Snapshot

To create a snapshot of the flash configuration on the hard disk of the services appliance, use the command **snapshot create**:

```
default# snapshot create

You booted from the primary partition

This command will create an exact copy of the mirror partition which will
be synchronized with the primary partition before the snapshot is cre-
ated. During the snapshot, services will continue to run, but you will
not be able to run other commands on this console and system performance
will be impacted. We recommend that you use this command during off-peak
hours.

Do you want to proceed? [y/n] y

Syncing disks... done
```

```
Copying Data: ########################

Operation completed successfully
```

To view the snapshot, use the command **show snapshot**:

Snapshot files are archived under - **/data/backup/snapshot/**

Use the **copy scp** option of the CLI command to move this file off the machine.

```
default # show snapshot

snapshot.2.1-29.23:44-10-12-2014

default#
```

You can delete the snapshot.

```
default# snapshot delete snapshot.2.1-29.23:44-10-12-2014

snapshot.2.1-29.23:44-10-12-2014 deleted
```

Limitations for Flash Backup

If you cancel a snapshot backup midway, the incomplete backup is not listed with an error the way a complete backup with an error is listed. Delete an interrupted incomplete backup immediately so that no one tries to restore it.

Restore a Snapshot

Use a snapshot to restore a (possibly corrupted) flash partition.

The command `snapshot restore` reconfigures a services appliance to use the snapshot version of flash. The restore command copies a selected snapshot image back to the backup partition. Synchronization does not start until after rebooting in order to avoid tainting the newly restored partition. Therefore, a second reboot is required. When the next reboot takes place, the system should be rebooted from the restored partition and the original partition will then be updated to match the newly restored partition. The system can then be run from either partition, since they are again identical.

A snapshot will always be restored to the backup partition. If you booted to the primary partition (hda2), then the image will be restored to the mirror partition (hda3). Alternatively, if you booted to the mirror, the image will overwrite the primary. The mirror/primary are equivalent

from the system standpoint. They are only named this way because GRUB will automatically boot to the primary partition without manual intervention.

After restoring the snapshot, reboot the system to boot from the primary partition.

Snapshot Restore Example

```
default# snapshot restore snapshot.16:00-04-05-2014

You booted from the primary partition.

This command will copy the snapshot image snapshot.16:00-04-05-2014 to
the mirror partition.

During snapshot, services will continue to run, but you will not be able
to run other commands on this console and system performance will be
reduced.

It is recommended to run this command during off-peak hours.

Do you want to proceed? [y/n] y

Copying Data:  ######

Operation completed successfully.
```

Reboot the system now and select the mirror partition following the directions *"Reboot a Services Appliance and Select a Partition"* ***on page 373***. The services appliance will be restored to the snapshot version of flash (both primary and secondary).

Corrupted Flash Example

Use the snapshot to recover when a corrupted flash boots with a message like this:

```
Booting 'BOOT FROM PRIMARY IMAGE'

root (hd0,1)

Filesystem type unknown, partition type 0x83

kernel=/boot/vmlinuz root=/dev/hdc2 console=tty0 console=ttyS0,115200
crashkern

el=64M@16M rhgb quiet

Error 17: Cannot mount selected partition
```

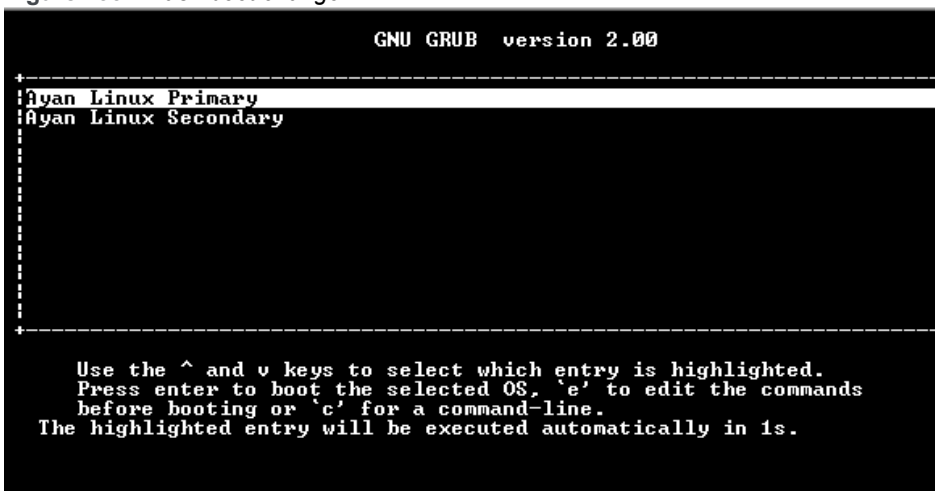
```
Press any key to continue...
```

Reboot a Services Appliance and Select a Partition

The services appliance boots by default from primary flash, but can be configured to boot from mirror flash. To change the boot flash partition, follow these steps:

1. Reboot the services appliance. During reboot, you see the question in *Figure 199 on page 373*.
2. Immediately press Enter to stop the boot process.
3. Select one of the options in *"Flash boot change" **on page 373*** and press Enter.

Figure 199: *Flash boot change*



4. Booting continues with one of the following messages - the pertinent text for SA200 is highlighted in blue below.

```
Booting 'BOOT FROM PRIMARY IMAGE'

Root (hd0.1)

Filesystem type is extfs, partition type 0x83

kernal=/boot/vmlinuz root=/dev/hdc2 console=tty0 console=ttySO, 115200
crashkernel=64M016M

[Linux-bzImage, setup=0x1400, size=0x25ddc0]


------------OR---------------

Booting 'BOOT FROM MIRROR IMAGE'
```

```
Root (hd0.2)

Filesystem type is extfs, partition type 0x83

kernal=/boot/vmlinuz root=/dev/hdc2 console=tty0 console=ttySO, 115200
crashkernel=64M016M

[Linux-bzImage, setup=0x1400, size=0x25ddc0]

Copying Data: ########################

Operation completed successfully
```

With SA200, if you see hdc2 as the backup partition, then you are running from the mirror partition (hdc3). With SA2000, it is the opposite - if you see hdc3 as the backup partitions, then you are running from the mirror partition.

Scheduling Automatic Backups

The data backup is stored in a text format on the NM server. To schedule automatic backups of the controller configuration database, follow these steps:

1. Log into FortiWLM user interface.
2. Choose *Administration* > *System Settings* > *Maintenance* to display the *Maintenance* screen. You can modify the controller configuration backup details by navigating to the *Controller Configuration Backup* section of the *Maintenance* screen.
3. The scheduled configuration backup frequency or the *Backup Schedule* is fixed to *Weekly* and cannot be modified.
4. However, you can configure the day of the week for scheduling the weekly configuration backup activity. Modify the default *Backup Day* (Sunday) by selecting a day in a week for the controller configuration backup to be performed. Select any one of the following options:
   - Sunday
   - Monday
   - Tuesday
   - Wednesday
   - Thursday
   - Friday
   - Saturday

5. The time scheduled is the server's local time with the default time as 1.00 am. Modify the default *Backup Hour* by selecting a desired time of the day for the backup to be performed from the drop-down list.

In the scheduled backup failure scenario, the backup activity for failed controllers is re-initiated every hour until the backup is successful.

6. Click *Save* to save your settings. The data backup is stored in a text format on the nm server.

Capacity Threshold

The *FortiWLM* supports many controllers and access points which operate on a Fortinet services appliance hardware device or in a virtualized environment based on VMware. Access Points contain radio devices that communicate with the Forti WLC and form the wireless LAN (WLAN). The controllers and access points connect to the site's wired LAN through wired switches. The network utilization is derived from per radio statistics. The *Capacity Threshold for Radio* are *Station Count Range, Throughput (Mbps) Range* and *Airtime Utilization(%) Range* values can be modified for each AP model located on the *FortiWLM*. Follow the below mentioned steps to view and modify the Capacity Threshold for Radio:

1. Navigate to *Administration* > *System Settings* > *Capacity Threshold*.
2. The *Capacity Threshold for Radio* screen provides the *Station Count Range, Throughput (Mbps) Range* and *Channel Utilization(%) Range* values for all AP Models.

Figure 200: *Capacity Threshold for Radio*

Capacity Threshold For Radio

		STATION COUNT RANGE				(Mbps)THROUGHPUT RANGE				CHANNEL UTILIZATION(%) RANGE		
	AP MODEL	IDLE	NORMAL	CAPACITY	OVERLOAD	IDLE	NORMAL	CAPACITY	OVERLOAD	IDLE	NORMAL	CAPACITY
	AP1010	Less than 1	1 to 20	21 to 25	More than 25	Less than 10	10 to 70	71 to 80	More than 80	Less than 20	20 to 60	61 to 75
	AP1010e	Less than 1	1 to 20	21 to 25	More than 25	Less than 10	10 to 70	71 to 80	More than 80	Less than 20	20 to 60	61 to 75
	AP1014i	Less than 1	1 to 20	21 to 25	More than 25	Less than 10	10 to 70	71 to 80	More than 80	Less than 20	20 to 60	61 to 75
	AP1020	Less than 1	1 to 20	21 to 25	More than 25	Less than 10	10 to 70	71 to 80	More than 80	Less than 20	20 to 60	61 to 75
	AP1020e	Less than 1	1 to 20	21 to 25	More than 25	Less than 10	10 to 70	71 to 80	More than 80	Less than 20	20 to 60	61 to 75
	AP110	Less than 1	1 to 6	7 to 10	More than 10	Less than 10	10 to 39	40 to 40	More than 40	Less than 20	20 to 60	61 to 75
	AP122	Less than 1	1 to 40	41 to 50	More than 50	Less than 10	10 to 400	401 to 450	More than 450	Less than 20	20 to 60	61 to 75
	AP301	Less than 1	1 to 30	31 to 40	More than 40	Less than 2	2 to 15	16 to 20	More than 20	Less than 20	20 to 60	61 to 75
	AP302	Less than 1	1 to 30	31 to 40	More than 40	Less than 2	2 to 15	16 to 20	More than 20	Less than 20	20 to 60	61 to 75
	AP310	Less than 1	1 to 30	31 to 40	More than 40	Less than 10	10 to 80	81 to 120	More than 120	Less than 20	20 to 60	61 to 75

3. Select an *AP Model* by clicking the check box and select the *Edit* option.
4. In the *Edit Capacity Threshold* pop-up for the selected AP Model number, modify the *Station Count Range, Throughput (Mbps) Range* and *Channel Utilization(%) Range values*.
5. Select *Save*.
6. The modified value for the selected AP model is displayed on the *Capacity Threshold for Radio* screen.

Maintenance

1. Navigate to *Administration* > *System Settings* > *Maintenance*.
2. The *Maintenance* screen provides the following *Server Maintenance Parameters* to be configured.

Field	Description
	Server backup
Backup Schedule	The *Backup Schedule* option allows you to select a period for the backup to be performed. Select an option from the Backup Schedule list. The options are as follows: • No Schedule • Daily (default) • Weekly
Backup Day	The *Backup Day* option allows you to select a day in a week for the server backup to be performed. Select any one of the following options: • Sunday • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday The default backup day is Sunday.
Backup Hour	The *Backup Hour* allows you to select a time of the day for the backup to be performed. The Time is from 1.00 A.M. to 12.00 P.M. The default backup hour is 1.00 A.M.
Number of Backups To Preserve	The *Number of Backups To Preserve* option allows you to enter the number of backups that can be preserved. The range varies from 1-3. The default value is 2. Enter the *Number Of Backups To Preserve*.

Field	Description

Transfer Backups To Remote Host	The *Transfer Backups To Remote Host* option allows you to transfer the data backup to a remote host. Select an option from the *Transfer Backups To Remote Host* list. The options are as follows:
	• **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 a remote host and the above mentioned parameters related to the remote backup transfer.

Overwrite Server Backups On Remote Host	The *Overwrite Server Backups On Remote Host* option allows you to overwrite the server backup on the remote host. Select an option from the *Overwrite Server Backups On Remote Host* list. The options are as follows: • Yes • No
File Transfer Protocol	The *File Transfer Protocol* is the protocol that is used for copying the server backup to remote host. Select an option from the *File Transfer Protocol* list. The options are as follows: • FTP • 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*.

Controller Configuration Backup

Field	Description
Backup Schedule	The *Backup Schedule* option allows you to enter the backup schedule. The Backup Schedule is either *Daily* or *Weekly*. Enter the *Backup Schedule*.
Backup Day	The *Backup Day* option allows you to select a day in a week for the backup to be performed. Select any one of the following options: • Sunday • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday The default backup day is Sunday.
Backup Hour	The *Backup Hour* allows you to select a time of the day for the backup to be performed. The Time is from 1.00 A.M. to 12.00 P.M. The default backup hour is 1.00 A.M.
Statistics	
Months to keep statistics data	The *Months to keep statistics data* option allows you to 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 Enter the *Months to keep statistics data*. The duration to preserve the statistics is between 1 - 6 months. The default value is 3 months.

Field	Description
Long term: 8 hourly data aggregation period begins at (AM)	The *Long term: 8 hourly data aggregation period begins at (AM)* option allows you to enter the start period for the data aggregation. Enter the time for the data aggregation to begin.
Statistics Polling Interval	The Statistics Polling Interval is the period in minutes at which Network Manager receives the statistics from controller. The polling interval can be 1 or 10 minutes. **Note**: When the Statistics Polling Interval is changed from 10 minutes to 1 minute, 1 minute samples are available from the time the polling interval setting is changed. Previous sample data (before the setting change to 1 minute) is also displayed as that of 1 minute. Therefore, it is recommended to not consider such data as it may be misrepresentative. **Notes:** • This feature is enabled only if all FortiWLC controllers discovered in WLM are of version 8.4.4 or higher (except 8.5.0). • This feature is not supported on FortiGate controllers.
Discovery	
Delete unused images on controller to install agent	The Delete unused images on controller to install agent option allows you to delete the unused images on the controller. Select an option from the Delete unused images on controller to install agent list. The options are as follows: • Yes • No
Report Preference	
Number Of Records Per HTML Page For Reporting	The *Number Of Records Per HTML Page For Reporting* option allows you to enter the number of records that can be displayed in the HTML Report page. For Example: In the *Number Of Records Per HTML Page For Reporting* field, if the number entered is 40, then only 40 records are displayed in an HTML page report. The next 40 records are printed on the next page. Enter the *Number Of Records Per HTML Page For Reporting*.

Field	Description
	User Interface preference section
Attribute to be used for display controller name	The *Attribute to be used for display controller* name option allows you to select the attributes to be used to display the controller name. The options are as follows: • **Hostname**: The name/IP Address provided while adding a Controller (default). • **Node Name**: The name that is configured on the Controller.
Allow Simple Password for Local User	By default, FortiWLM requires users to follow strict password rules as part of PCI compliance. However, you can now allow users to create simple passwords by disabling this condition.
Session Timeout in Minutes	As part of PCI compliance, unattended FortiWLM login session will timeout in 5 minutes. Select ***NEVER***, to prevent a session being timed out.
	OUI Update
Last update time	Displays the date and time of the OUI details updated the last time.
Automatically update every week	This option when enabled, will allow the system to automatically update the OUI details every week.
Upload OUI File	This option allows you to upload the OUI file manually to update the system OUI details.

Station Activity Log Archival Policy

The *FortiWLM* handles multiple system activity like *Event Log, Alarm History, Station Activity Logs, User activity Log (Sys Log), NM backups, SD backups saved on the NM server, Statistics data, Inventory and configuration data,* and *E(z)RF system data*. All the above mentioned system activities are stored in the database files which occupy enormous space. The Storage in the *Administration* allows you to archive all the above mentioned data based on polices.

The *NM* is designed in such a manner that each system activity mentioned above is managed in a clever way occupying space. Although, *NM* performs periodical backup and deletes the data from the database, different other configurations are performed, where the operations are executed on the activity data storage. Following are some of the activities:

- Query and view data from the *NM* web UI
- Modify data
- Export data into file from the *NM* web UI
- Backup activities including one time backup and scheduled backup

- Purge activities including one time purge and scheduled purge
- Forward activity records to the external system, user side SNMP manager or email or others.
- Monitor the storage: disk space / number of records / date and time of records

The above mentioned operations are archived in the database. The current design of *NM* database comprises of **`nmsdb`** and **`eventdb`** database partitions. The disk monitoring and station activity log archival is performed on the *eventdb* partition of the *NM* database.

The above mentioned operations on *NM* are archived through the *NM* web UI.

1. Select *Administration* > *System Settings* > *Station Activity Log Archival Policy*. The *Station Activity Log Archival Policy* screen is displayed. The station events here are archived based on the following policies:

- **Events Archival Policy:** The events are archived in a compressed format and then deleted from the NMS.
- **Events Retirement Policy**: The events are archived based on the retirement age or maximum disk space.

2. The *Station Activity Log Archival Policy* screen consists of the following three sections:

- **Disk Usage**: The *Disk Usage* is a pie chart that displays the total Available space and the Used space utilization by the events. The disk usage of 30 GB is provided for the SA200/SA250 and the disk usage of 60 GB is provided for SA2000.
- **Station Activity Log History**: The *Station Activity Log History* graph displays the disk space utilization by the events as bar chart. The "X-Axis" depicts the Day in mm-dd-yy format and "Y-Axis" depicts the Disk Usage in GB.
- **Storage Configuration**: The *Storage Configuration* is based on the Station Activity Log Retirement Policy which enforces the events archival or deletion based on the disk space usage. A maximum of 30 days station log activity events are displayed on the graph. The Storage configuration provides the following options:
  - **Amount of storage to free in retirement**: The *Amount of storage to free in retirement* displays the amount of storage to be deleted during retirement. This is the default selection, where 20% of the events get archived or deleted when the disk usage reaches 100% of 30 GB in SA200/SA250 and 100% of 60 GB in SA2000.
  - **Enable auto system retirement**: The *Enable auto system retirement* option enables the automatic retirement when SA200/SA250 reaches 100% of 30 GB and SA2000 reaches 100% of 60 GB.
  - **Log Retire Options**:
    - **Purge**: This option allows you to delete the records following a configurable predefined setting. The Station activity log purge is based on the percentage of disk usage.
    - **Archive to remote server & Purge from NMS Server**: This option exports the Events in CSV format and transfers the events to a remote server using ftp/scp pro-

tocol and then gets deleted from the NMS. Once all the event tables from oldest events first are selected and exported, the directory will be compressed in tar.gz format. The compressed file is named in backup_events_dd-mm-yy-mm-hh-ss.tar.gz format. The file is then transferred to remote server using the *ftp* and *scp*. Provide the remote server hostname or IP address (IPv4/IPv6), user name, password, and the remote directory path. The compressed file located on the local hard drive gets deleted after the transfer.

Rogue Classification

The rogue access points detected by the controller are categorized into *malicious* and *friendly* based on specific rules that you configure. You can configure multiple rules (maximum of 50) per Rogue Classification profile. These rules are assigned different priorities by ordering them. When a rogue access point is detected its attributes (ESSID, RSSI) are matched against the configured rules and its classification type is defined by the matching rule with highest priority.

Navigate to *Administration* > *System Settings* > *Rogue Classification*.

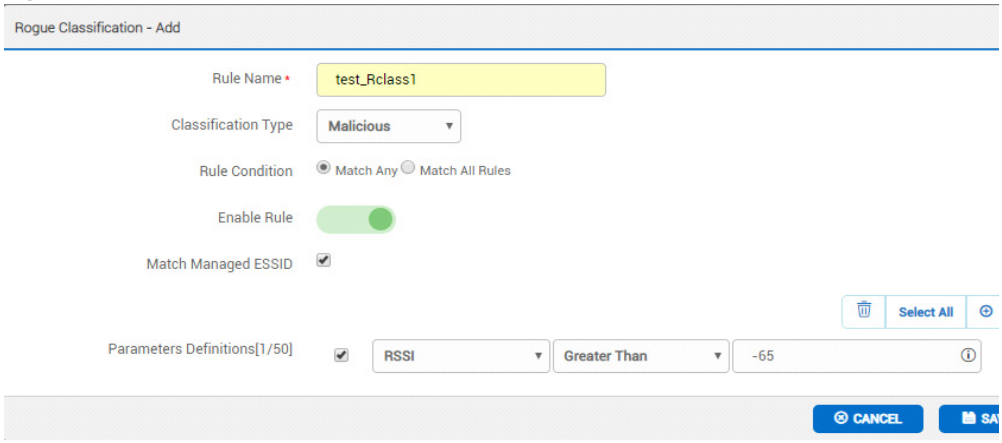
The following actions can be performed on the Rogue Classification screen.

Name of Action	Description
Add	**Add** allows to add a **Rogue Classification Profile**.
Delete	**Delete** allows deleting a **Rogue Classification Profile**. Select the **Delete** option, the **Rogue Classification Profile** gets deleted.
Reorder	Reorder allows configuring the priority of the **Rogue Classification Profile** created. Click **Reorder** and drag the rules listed to set the priority top down.
Edit	**Edit** allows editing an **Rogue Classification Profile**. Select the edit icon, the **Rogue Classification Profile** opens for modification. The **Rule Name cannot be modified.**

Adding Rogue Classification Profile

1. In the **Rogue Classification** screen, select **Add**. The **ADD - Rogue Classification** screen is displayed.
2. Provide the details for the following parameters. You can create multiple Rogue Classification profiles.

Figure 201: *Adding a rogue AP classification profile*



Configure the following fields to create a rogue AP classification profile.

Field	Description
Rule Name	Unique name for this Rogue Classification profile.
Classification Type	The classification of the rogue access point, whether malicious or friendly, based on matching the configured rule.
Rule Condition	Select any of these conditions to apply. • **Match Any** -- If the rogue access point matches a single rule of the many configured rules, then the classification is successful and the access point is marked malicious or friendly accordingly. • **Match All** -- If the rogue access point matches all the configured rules only then the classification is successful and the access point is marked malicious or friendly accordingly.
Enable Rule	To enable or disable the Rogue Classification profile.
Match Managed ESSID	This option compares the ESSID of the discovered rogue access point with the ESSID present in the controller. If a match is found then the access point is considered to be matching the rule.

Field	Description
Parameter Definitions	The following definitions are supported to create a rule. • **ESSID** -- A rule configured based on the ESSID of the detected rogue access point. The supported filters are, **Contains**, **Equals**, **Not Equals**, **Starts With**. • **RSSI** -- A rule configured based on the RSSI value of the detected rogue access point. The supported filters are, **Greater Than** and **Less Than**.

Click **Save**. The Rogue Classification Profile is created.

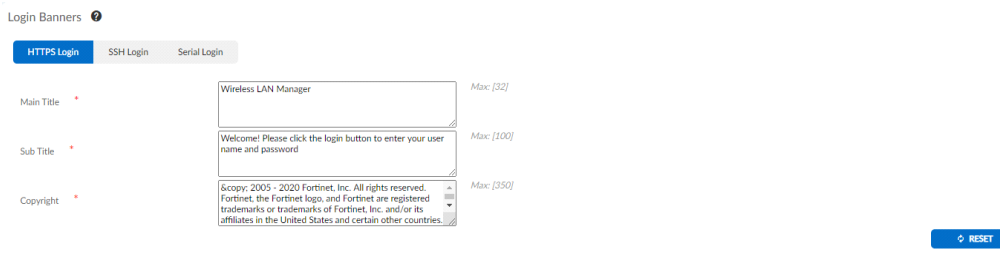
The rogue AP classification is displayed in the **Fault Management** (*Monitor* > *Overview* > *Fault Management*) dashboard.

Login Banners

The login banner defines the text that is displayed when you login into FortiWLM. The login banner applies only to the FortiWLM on which you configure it. You can define login banners for the following access types.

- **HTTPS Login**: Enter the **Main Title** (maximum character limit is 32) of the login page and the accompanying details, that is, the **Sub Title** (maximum character limit is 100), and the **Copyright** (maximum character limit is 350) information.
- **SSH Login**: Enter the **SSH Login Title** of the login screen.
- **Serial Login**: Enter the **Serial Login Title** of the serial console.

Navigate to **Administration > System Settings > Login Banners**.



WLM Upgrade

Use this page to upgrade your network manager server. Before you upgrade, copy the build file (*.fwlm*) to a location accessible via the Network Manager WebUI.

Note: Direct upgrade using the *.fwlm* format is supported release 8.4.2 onwards.

To upgrade do the following:

1. Click **Add** to view file selector pop-up window.
2. In the pop-window, click **Choose File** and browse to the location that has the tar file.
3. Select the tar to upload this to the sever. Once uploaded the build file is listed and provides the following details:
   - Image Name: This usually shows the version of the Network Manager server.
   - Size: The size of the build file in MB
   - Upload Time: The time when the file was uploaded to the server.
4. To install the uploaded file, select the build file option and click the INSTALL button (in the footer of the page).

To install a new patch on a released version. For patch installation, only *.fwlm* format is supported.

1. Click Add to view file selector pop-up window.
2. In the pop-window, click Choose File and browse to the location that has the patch *.fwlm* file.
3. Select the patch file to upload; once uploaded the patch file is listed with the following details:
   - Image Name: The name of the patch file uploaded (displays the version and patch details).
   - Size: The size of the patch file in MB.
   - Upload Time: The time when the patch file was uploaded to the server.
   - Currently Installed: Whether the patch file is installed or not.
   - Action: The logs for patch installation/failure and so on. You can download these.

After the patch file is uploaded, you can perform the following actions:

- To install the uploaded patch file, select the file and click Install.
- To uninstall the patch file, select the file and click uninstall.
- To delete the patch file, select the file and click Delete.
- To view the patch details such as the bug resolutions delivered in the patch, the patch file md5sum, and the available file permissions, click Details.
- To view the patch history such as date of installation and build number, click History.

Notes:

- Patch framework is not supported in an HA setup.
- Non-admin/RADIUS/TACACS+ users cannot configure patch framework through the CLI.

Troubleshooting Notification

The most common notification errors are:

- Including an incorrect email address in an email list
- Selecting incorrect filters in the notification filter

If there is any misconfiguration in the email list, the error "*Failed to send email notification using Primary SMTP server Configuration. Reason: Invalid input data*" is displayed on the *Alarms Dashboard* (*Monitor* > *Overview* > *Fault Management* > *Alarms*).

If the SMTP server supports authentication, configure the email list to identify (and drop) only the incorrect email addresses (see *"Set Up Email Notification"* ***on page 362*** to add authentication details to the email configuration). This way, the SMTP server does not try to resolve email ID domain names when the *Alarm Manager* sends a mail to the SMTP server. Only the misspelled email address receives an error and all correct addresses receive the notification. If authentication is not supported and even one email address is incorrect, no users on the mailing list will receive the message. The only way to correct the problem is to remove or correct the email address.

Notification filters can be configured incorrectly if you don't keep in mind that checking filters is an AND/OR operation. For example, when adding a filter, if you checked all of the options for Alarms and Alarms severity, you receive only clear alarms, which is probably not what you intended. In this case, If you wish to receive Rogue AP alarms only, uncheck the options in 'Alarm severity'.

Administrators in different user groups can configure separate notification profiles for the same controller. Since applying a notification alarm is a global operation, you can configure your notifications correctly and still have notification errors if another administrator managing the same controller mis-configures *their* group's notification list on the controller. If there is any misconfiguration in any one of the notification lists for a controller, it affects all notifications for that controller.

Reporting in Network Manager

FortiWLM provides standard report types that assist you to generate, schedule and view reports. You can create and customize report types and save them as templates for future generation. Reports allow you to perform network analysis, user configuration, device optimization, and network monitoring on multiple levels. These reports provide an interface for multiple configurations, allowing you to act upon information in the reports. It also helps you to proactively identify network issues such as loss, Signal-to-Noise Ratio (SNR), station overcrowding, alarms and so on, occurred in the system.

- *"Create Reports"* ***on page 389***
- *"View Reports"* ***on page 397***
- *"Scheduled Reports"* ***on page 417***
- *"PCI Reports"* ***on page 417***

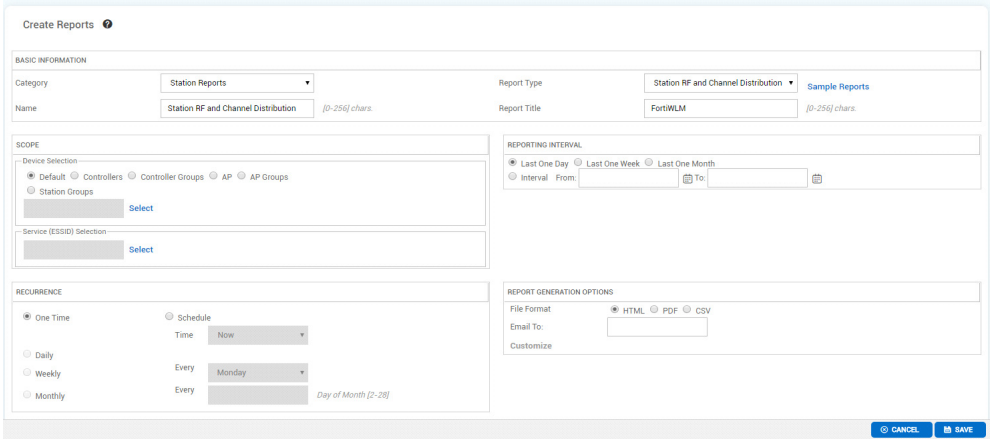
Create Reports

FortiWLM allows you to define new reports and generate one-time reports. 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.

Perform these steps to create and run custom reports:

1. Click *Reports* > *Create Reports*. The *Create Reports* screen with the following sections is displayed: See *Figure 202 on* ***page 390***.
   - Basic Information - See *"Basic Information"* ***on page 390***
   - Scope - See *"Scheduled Reports"* ***on page 417***
   - Reporting Interval - See *"Reporting Interval"* ***on page 395***
   - Recurrence - See *"Recurrence"* ***on page 396***
   - *Report Generation Options - See "Report Generation Options"* ***on page 396***

Figure 202: *Create Reports*



Basic Information

The *Basic Information* section of the *Create Reports* screen allows you to choose a *Category of report*, *Report Type*, provide a *Name* and *Report Title*.

The supported category of reports and its report types are as follows:

Category	Report Type	Description
Station Reports See *"Scope"* ***on page 393***	Station RF and Channel Distribution See *"Station RF and Channel Distribution"* ***on page 398***	Provides the station RF and channel distribution based on the OUI (Organizationally Unique Identifier). A graphical summary of the stations distributed by RF type, stations distributed across 2.4GHz and 5GHz bands and station density on each channel over time is displayed.
	Station Session Details See *"Station Session Details"* ***on page 399***	Provides the average station session trend details. A graphical summary of the station session trend details of throughput, loss, airtime utilization and noise for a connected station is displayed.
	Top Stations See *"Top Stations"* ***on page 400***	Lists the top interfering 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.
	Unique Stations See *"Unique Stations"* ***on page 401***	Provides the unique station details based on all stations connected to a network within the reporting interval. A graphical summary of the stations distributed by RF type, stations distributed across 2.4GHz and 5GHz bands, stations distributed by OUI, stations distributed by device type, and stations distributed by OS type is displayed.

Category	Report Type	Description
AP Reports	Rogue Details See *"Rogue Details"* ***on page 403***	Summarizes individual rogue information. A graphical summary of the rogue mobility trend is displayed.
	Rogue Summary See *"Rogue Summary"* ***on page 404***	Summarizes the rogue device information on the trend of the number of rogues reported on a per controller basis, per hour. The rogue APs and rogue station count is displayed. A graphical summary of the trend on rogue AP, trend on rogue station, and trend on controllers is displayed.
	Top Radio See *"Top Radio"* ***on page 406***	Provides the Top N radios based on station count, throughput, and high airtime utilization.
Inventory Reports	Access Points Inventory See *"Access Points Inventory"* ***on page 407***	Lists and tracks all the access points, with its model and software versions on the network.
	Controller Inventory See *"Controller Inventory"* ***on page 408***	Lists and tracks all the controllers, with its model and software versions on the network.
	Device Availability See *"Device Availability"* ***on page 409***	Lists all the controllers and access points with its availability, uptime and down time of each of them.
Network Health Reports	Alarm Report See *"Alarm"* ***on page 409***	Lists the total number of critical, major and minor alarms raised on the network. A graphical summary of the alarms distribution by category and top 10 controllers and access points with high alarms is displayed.
	Network Utilization and Capacity See *"Network Utilization and Capacity"* ***on page 411***	Displays the classification of APs capacity and consumption based on the data throughput and station count for 2.4 GHz and 5GHz channels. The aggregate usage of all selected APs for 2.4 GHz and 5GHz channels are computed as a percentage of total capacity.

Category	Report Type	Description
Service Reports	Service Usage Summary See *"Service Usage Summary"* **on page 414**	Provides the service usage summary based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed.
	Service Usage Trend See *"Service Usage Trend"* **on page 415**	Provides the service usage trends based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed.

Scope

This section allows you to define the scope of a report by performing the device selection followed by the *Service (SSID) Selection*.

Device Selection

The device selection provides the following options:

Field	Description
Default	By choosing default, report is generated for all the controllers mapped to the nms-server.
Controllers	• Choose the *Controllers* option and click on the *Select* link. • The *Controller* pop-up provides you a list of all controllers located within the network. • Select one or multiple *Controllers* and click on *OK*. • The selected controllers are displayed in the *Controllers* text box.
Controller Groups	• Choose the *Controller Groups* option and click on the *Select* link. • The *Controller* Group pop-up provides you a list of all controller groups located within the network. • Select one or multiple *Controller Group* and click on *OK*. • The selected controller groups are displayed in the *Controller Groups* text box.
AP	• Choose the *AP* option and click on the *Select* link. • The *AP* pop-up provides you a list of all APs located within the network. • Select one or multiple *APs* and click on *OK*. • The selected APs are displayed in the *AP* text box.
AP Groups	• Choose the *AP Groups* option and click on the *Select* link. • The *AP Groups* pop-up provides you a list of all AP groups located within the network. • Select one or multiple *AP Groups* and click on *OK*. • The selected AP groups are displayed in the *AP Group* text box.

Field	Description

Station Groups	• Choose the *Station Groups* option and click on the *Select* link.
	• The *Station Groups* pop-up provides you a list of all station groups located within the network.
	• Select one or multiple *Station Groups* and click on *OK*.
	• The selected station groups are displayed in the *Station Group* text box. This option allows you to select station group profiles for which the report must be generated. On generating a station report, the data is displayed only those stations which meet the below criterion:
	  • Stations must comprise the same 3 byte MAC prefix as the members in the group profile.
	  • Stations whose MAC Address completely matches with the member in the group profile.

Service (SSID) Selection

- Click on the *Select* link to select a *Service SSID*.
- The *SSID* pop-up provides you a list of SSIDs.
- Select the SSIDs and click on *OK*.
- The selected SSID is displayed on the *Service (SSID) t*ext box.

Reporting Interval

These fields depict the time period to be covered by the selected report. These fields are supported for most report types. When these fields do not appear, the report considers the current status. Select the *Schedule* option of the *Recurrence* section, the following options in the *Reporting Interval* section is enabled:

- **Last one day**: Select the *Last one day* option. The last one day's report is generated.
- **Last one week**: Select the *Last one week* option. The last one week's report is generated.
- **Last one month**: Select the *Last one month* option. The last one month's report is generated.
- **Interval**: Select the Interval option. The report for the given interval period is generated.
  - *From* time: The format followed is the mm/dd/yyyy and hh:mm:ss format. The time can be entered manually or by selecting the *Calendar* button.

- *To* time. The format followed is the mm/dd/yyyy and hh:mm:ss format. The time can be entered manually or by selecting the *Calendar* button.

The *Inventory Report* category inclusive of the *Access Point Inventory* and *Controller Inventory* report types consider the present time.

Recurrence

This section allows you to select the time of recurrence. The options are:

- *One Time*: Instant report is generated for the selected reporting interval.
- *Schedule*: This option allows you to define a specific time for report creation. These schedule fields establish the time that a report runs, independent of the *Scope* and *Reporting Interval.*
  - *Daily*: This option allows you to generate daily reports.
  - *Weekly*: This option allows you to generate weekly reports, select *Weekly* option followed by selecting the day of the report generation from the *Every* drop-down list:
    - Monday
    - Tuesday
    - Wednesday
    - Thursday
    - Friday
    - Saturday
    - Sunday
  - *Monthly*: This option allows you to generate monthly reports, select *Monthly* option and enter the *Day of month*; 1-31 is the valid range.

Report Generation Options

To generate a report, select the fields as mentioned in the above from the *Basic Information*, *Recurrence*, *Reporting Level* and *Scope* sections.

Select the following options in the *Report Generation Options*:

- *File Format*: Choose one of the following *Report Generation* file format.
  - *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*.

- *Email To*: Provide an *Email ID* to email a soft copy of the report in the selected file format. Enter email addresses separated by commas when using multiple email addresses.
- *Customize*: The *Customize Report* option allows you to generate customized reports by selecting the desired attributes to be displayed on the report.
  - Select the *Customize* link. The *Customize Report* pop-up displays the following options:
  - *Display Summary Graphs*: The *Display Summary Graphs* 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.
  - *Available Attributes*: This column displays a list of available attributes that can be selected for report generation.
  - *Attributes to be displayed in report*: This column displays a list of selected attributes to be displayed in report.

Select the attributes from the *Available Attributes* column and move to the *Attributes to be displayed* in report column.

Select *Save* to customize the report.

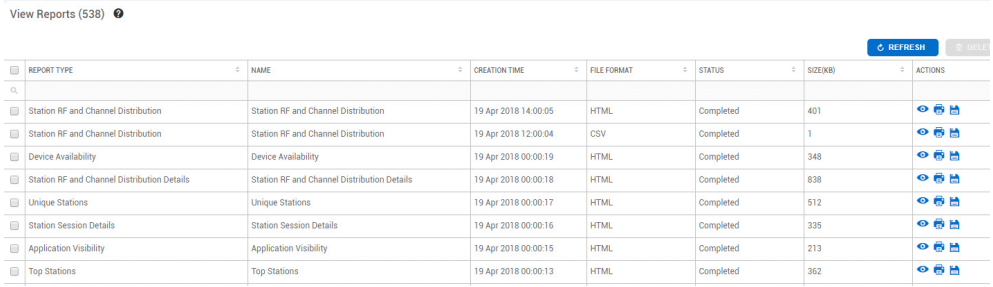
- Click *Save*, to save the report in either of the file formats.
- To view the completed report, click *Reports* > *View Reports*.

View Reports

The *View Reports* screen displays a list of pre-defined reports in *FortiWLM* which are defined in the *Create Reports* screen. It displays the most recent daily version of any report with a single click. Reports in **CSV**, **HTML** or **PDF** format outputs are stored that can be viewed, saved locally, and printed. The *Admin* user can view and edit all report definitions. The users with *monitor* capability can only view the reports and definitions if they have access to all devices in the reports.

1. Click *Reports* > *View Reports*.

Figure 203: *View Reports*



2. The *View Reports* screen provides a list of reports that have been defined in the *Create Reports* screen. See *"Create Reports"* ***on page 389***.
3. The *Report Type, Name, Creation Time, File Format, Status, Size,* and *Action* details for each report type can be viewed.

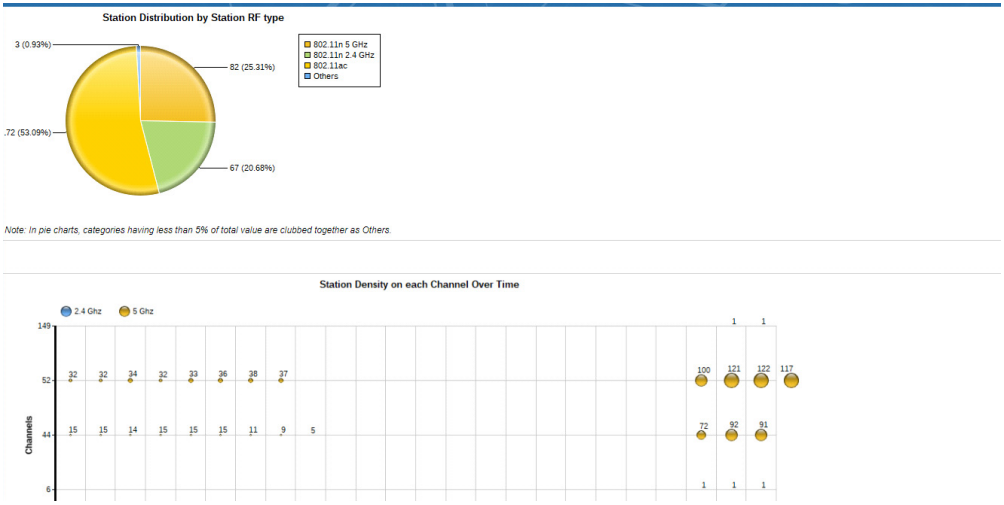
Station Reports

Station RF and Channel Distribution

The *Station RF and Channel Distribution* report type generates reports based on the cumulative statistical data over the reporting interval. It provides the station RF and channel distribution based on OUI. The number of stations per channel over the reporting period with the graphical pie-chart summaries is displayed. Perform these steps to view the most recent version of the *Station RF and Channel Distribution Report*.

1. Navigate to the *Reports* > *View Reports* screen.
2. Select the *Station RF and Channel Distribution* report type to display the report. The primary sections of this report are as follows:
   - Graphs
     - **Station Distribution by RF Type**: Displays the station distribution based on the RF type. For example.,802.11n 2.4 GHz, 802.11a, 802.11n 5 GHz, and Unknown. The categories having less than 5% of total value are clubbed together as *Others*.
     - **Station Density on each Channel Over Time**: Displays the station density on each of the "channels over time" plotted against the selected time range.
   - **Station RF and Channel Distribution Details**: Displays each station's *OUI, Date/Time (GMT), Station Mac, RF Type, AP Name, AP Radio, SSID* and *Channel*. .

Figure 204: *Station RF and Channel Distribution report*



Station Session Details

The *Station Session Details* report type provides the average station session trend (*Throughput, Loss, and Airtime Utilization*) for a connected station. Perform these steps to view the most recent version of the *Station Session Details* report.

1. Navigate to the *Reports* > *View Reports* screen.
2. Select the *Station Session Details* report type to display the report. The primary sections of this report are as follows:

- Graphs
  - **Trend On Airtime Utilization**: Displays the *Airtime Utilization* trend for the selected station.
  - **Trend On Loss**: Displays the *Loss* trend for the selected station.
  - **Trend On Throughput**: Displays the *Throughput* trend for the selected station.
- **Station Session Details**: This section provides each station's *Date/Time, IPV4 Address, IPV6 Address, Controller, AP ID, SSID, User, Throughput (Kbps), Loss%, Airtime Utilization%,* and *AP Name*.

Figure 205: *Station Session Details report*

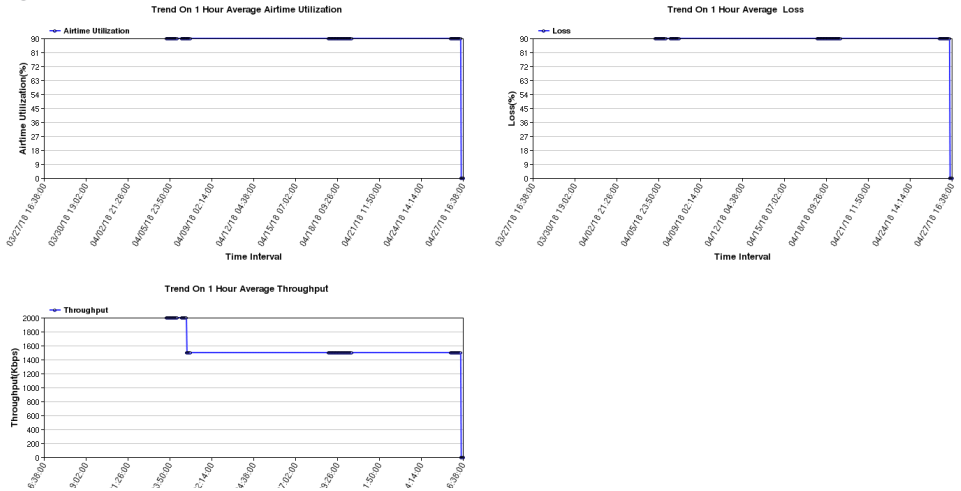
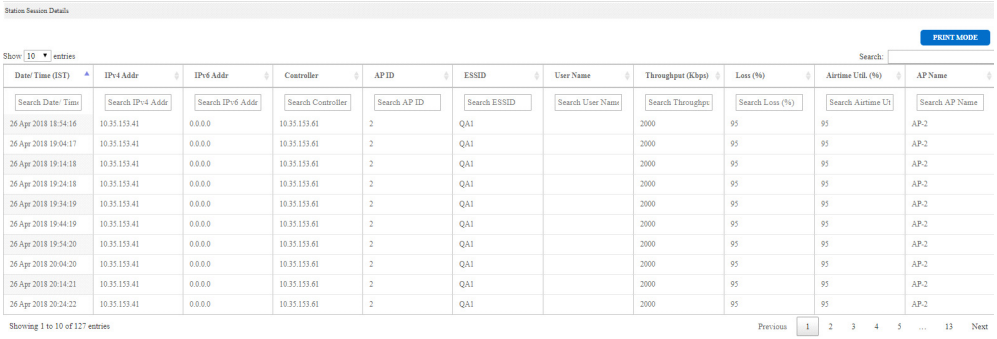


Figure 206: *Station Session details Tabs*

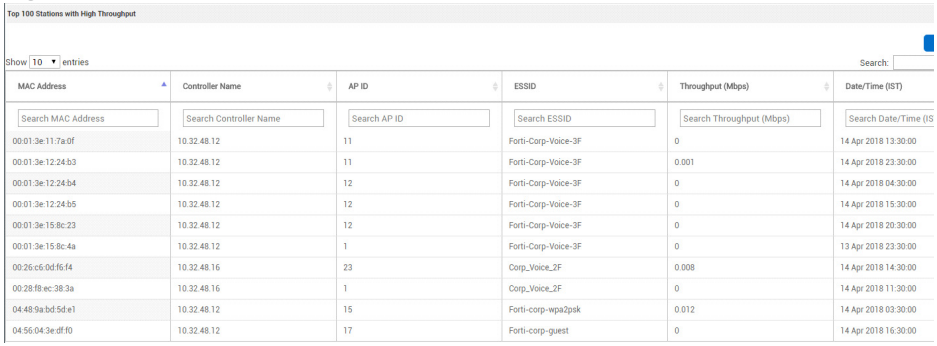


Top Stations

The *Top Stations* report type generates reports for the top interfering stations based on the *Throughput* and *Airtime Utilization*. The default number of stations displayed is 100. This report type generates the top N stations based on the number of bytes transferred and received and total Rx/Tx. Perform these steps to view the most recent version of the *Top Stations* report.

1. Navigate to the *Reports* > *View Reports* screen.
2. Select *Top Stations* report type to display the report.
3. The information includes each station's *Station MAC, Controller, AP Id, SSID, Throughput (Kbps), Airtime Utilization(%),* and *Date/Time (GMT)*.

Figure 207: *Top Stations report*

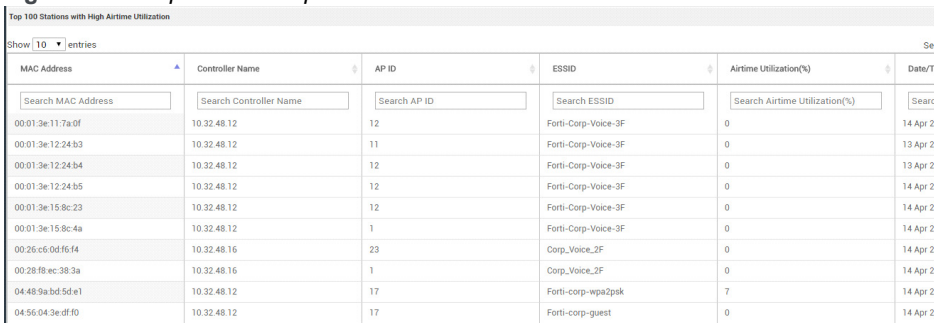


Top 100 Stations with High Throughput

Show 10 entries Search:

MAC Address	Controller Name	AP ID	ESSID	Throughput (Mbps)	Date/Time (IST)
Search MAC Address	Search Controller Name	Search AP ID	Search ESSID	Search Throughput (Mbps)	Search Date/Time (IS
00:01:3e:11:7a:0f	10.32.48.12	11	Forti-Corp-Voice-3F	0	14 Apr 2018 13:30:00
00:01:3e:12:24:b3	10.32.48.12	11	Forti-Corp-Voice-3F	0.001	14 Apr 2018 23:30:00
00:01:3e:12:24:b4	10.32.48.12	12	Forti-Corp-Voice-3F	0	14 Apr 2018 04:30:00
00:01:3e:12:24:b5	10.32.48.12	12	Forti-Corp-Voice-3F	0	14 Apr 2018 15:30:00
00:01:3e:15:8c:23	10.32.48.12	12	Forti-Corp-Voice-3F	0	14 Apr 2018 20:30:00
00:01:3e:15:8c:4a	10.32.48.12	1	Forti-Corp-Voice-3F	0	13 Apr 2018 23:30:00
00:26:c6:0d:f6:f4	10.32.48.16	23	Corp_Voice_2F	0.008	14 Apr 2018 14:30:00
00:28:f8:ec:38:3a	10.32.48.16	1	Corp_Voice_2F	0	14 Apr 2018 11:30:00
04:48:9a:bd:5d:e1	10.32.48.12	15	Forti-corp-wpa2psk	0.012	14 Apr 2018 03:30:00
04:56:04:3e:df:f0	10.32.48.12	17	Forti-corp-guest	0	14 Apr 2018 16:30:00

Figure 208: *Top Stations report*



Top 100 Stations with High Airtime Utilization

Show 10 entries Se

MAC Address	Controller Name	AP ID	ESSID	Airtime Utilization(%)	Date/T
Search MAC Address	Search Controller Name	Search AP ID	Search ESSID	Search Airtime Utilization(%)	Searc
00:01:3e:11:7a:0f	10.32.48.12	12	Forti-Corp-Voice-3F	0	14 Apr 2
00:01:3e:12:24:b3	10.32.48.12	11	Forti-Corp-Voice-3F	0	13 Apr 2
00:01:3e:12:24:b4	10.32.48.12	12	Forti-Corp-Voice-3F	0	13 Apr 2
00:01:3e:12:24:b5	10.32.48.12	12	Forti-Corp-Voice-3F	0	14 Apr 2
00:01:3e:15:8c:23	10.32.48.12	12	Forti-Corp-Voice-3F	0	14 Apr 2
00:01:3e:15:8c:4a	10.32.48.12	1	Forti-Corp-Voice-3F	0	14 Apr 2
00:26:c6:0d:f6:f4	10.32.48.16	23	Corp_Voice_2F	0	14 Apr 2
00:28:f8:ec:38:3a	10.32.48.16	1	Corp_Voice_2F	0	14 Apr 2
04:48:9a:bd:5d:e1	10.32.48.12	17	Forti-corp-wpa2psk	7	14 Apr 2
04:56:04:3e:df:f0	10.32.48.12	17	Forti-corp-guest	0	14 Apr 2

Unique Stations

The *Unique Stations* report type generates reports based on all stations connected to a network within the reporting interval. A *Unique Station* report is available to all groups and stations connected to network in the selected time range. The unique station details with the graphical pie-chart summaries are displayed. Perform these steps to view the most recent version of the *Unique Stations* report.

1. Navigate to the *Reports* > *View Reports* screen.
2. Select the *Top Stations* report type to display the report. The primary sections of this report are as follows:

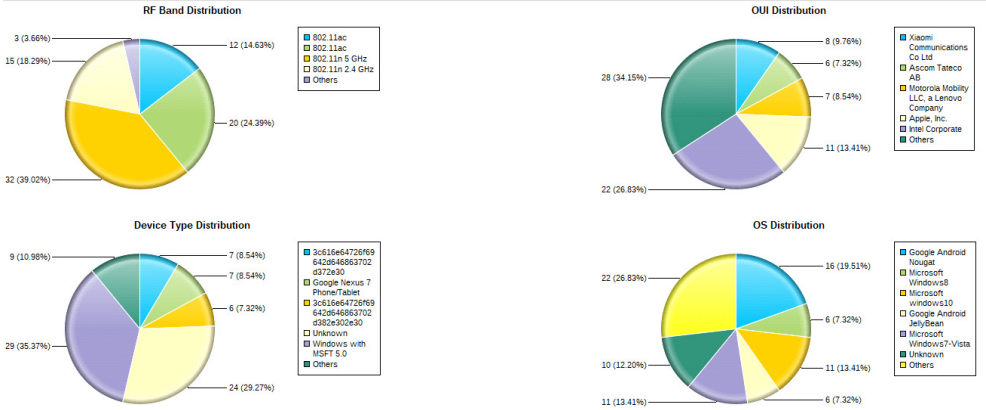
- **Summary**: Displays the total number of *Unique Stations*.
- **Graphs**:
  - **RF Band Distribution**: Displays the station distribution based on the RF Type. For example.,802.11n 2.4 GHz, 802.11a, 802.11n 5 GHz, and Unknown. The categories having less than 5% of total value are clubbed together as *Others*.
  - **OUI Distribution**: Displays the station distribution based on the OUI.
  - **Device Type Distribution**: Displays the station distribution based on the *Device Type*.

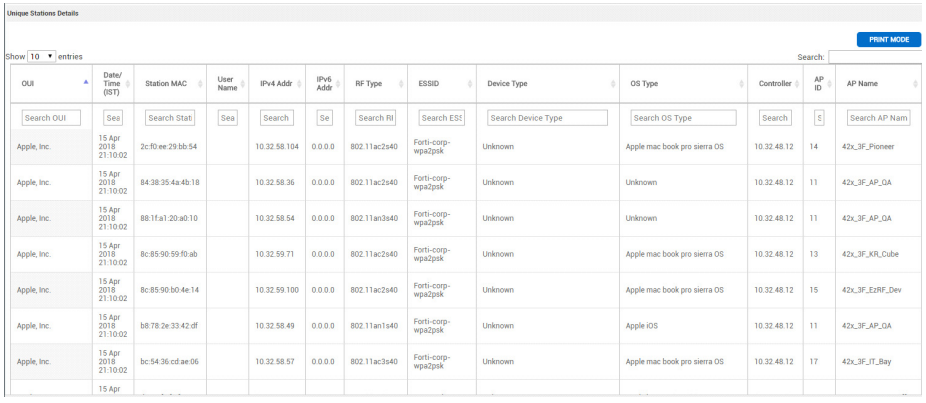
- **OS Distribution**: Displays the station distribution based on the *OS Type*.

The *Device Type Distribution* and *OS Distribution pie-graphs* displays as *unknown*, if controllers below 6.0 version is mapped to the nms-server. The controllers below version 6.0 do not support the *device finger printing* feature

- **Unique Station Details**: Displays the station's *OUI, Date/Time (CST), Station MAC, User, IPv4 Address, IPv6 Address, RF Type, SSID, Device Type, OS Type,* and *Floor*.

Figure 209: *Unique Stations report*





AP Reports

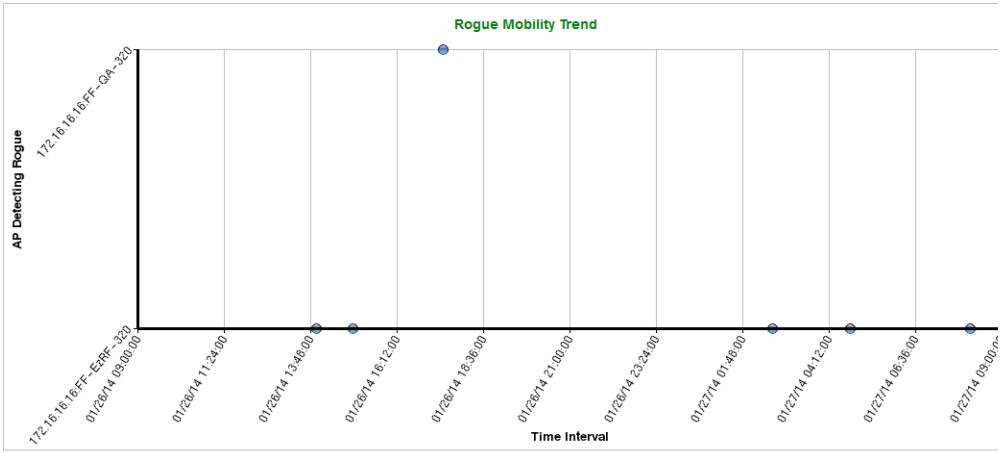
Rogue Details

The *Rogue Details* report type generates individual rogue report. It displays the rogue mobility trend. The trend is plotted against time and APs detecting the rogue. A maximum of hourly data sample is displayed. Perform these steps to view the most recent version of the *Unique Stations* report.

1. Navigate to the *Reports* > *View Reports* screen.
2. Choose the *AP Reports* category. Select the *Rogue Details* report type to display the report. The primary sections of this report are as follows:

- **Summary**: Displays the details of the selected rogue.
- **Graph**: Displays the *Rogue Mobility Trend* graph. The trend is plotted against AP which detects rogues with high strength and its time as samples.
- **Rogue Details**: Displays the details of the APs detecting rogue along with *Date/Time, Controller, AP Detecting Rogue, AP Location, SSID, Channel* and *RSSI(dBm)*.

Figure 210: *Rogue Details report*



Rogue Details

Date/Time (IST)	Controller	AP Detecting Rogue	AP Location	Channel	RSSI (dBm)
26 Jan 2014 13:58:04	172.16.16.16	FF-EzRF-320		7	-35
26 Jan 2014 14:58:04	172.16.16.16	FF-EzRF-320		36	-46
26 Jan 2014 17:28:03	172.16.16.16	FF-QA-320		108	-54
27 Jan 2014 02:38:01	172.16.16.16	FF-EzRF-320		100	-36
27 Jan 2014 04:47:57	172.16.16.16	FF-EzRF-320		100	-39
27 Jan 2014 08:07:59	172.16.16.16	FF-EzRF-320		36	-50

Rogue Summary

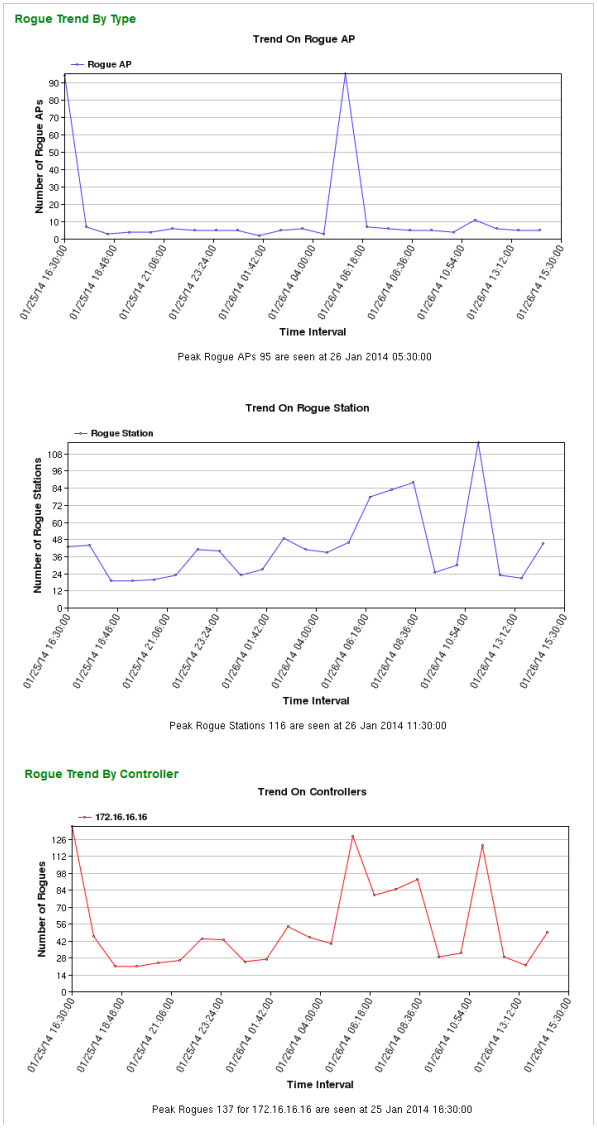
The *Rogue Summary* report type generates reports based on the number of rogues reported on a per controller basis, per hour. Perform these steps to view the most recent version of the *Rogue Summary* report.

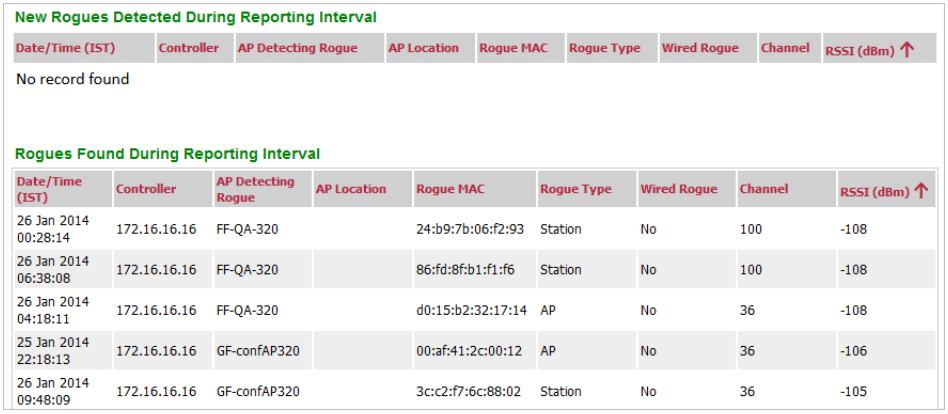
1. Navigate to the *Reports* > *View Reports* screen.
2. Select the *Rogue Summary* report type to display the report. The primary sections of this report are as follows:

- **Summary**: Displays the details of the total number of rogues.
- **Graph**:
  - **Rogue Trend By Type**: The *Rogue Trend By Type* graph is categorized as follows:
    - **Trend On Rogue AP**: Displays the trend type based on the number of *Rogue APs*.
    - **Trend on Rogue Station**: Displays the trend type based on the number of *Rogue Stations*.
- **Rogue Trend By Controllers**: This graph displays the top 10 controllers with the highest number of *Rogues*.

- **New Rogues Detected During Reporting Interval**: Displays the details of new rogues detected during reporting interval with the *Date/Time, Controller, AP Detecting Rogue, AP Location, Rogue MAC, Rogue Type, Wired Rogue, Channel,* and *RSSI (dBm)*.

Figure 211: *Rogue Summary report*





New Rogues Detected During Reporting Interval

Date/Time (IST)	Controller	AP Detecting Rogue	AP Location	Rogue MAC	Rogue Type	Wired Rogue	Channel	RSSI (dBm)
No record found								

Rogues Found During Reporting Interval

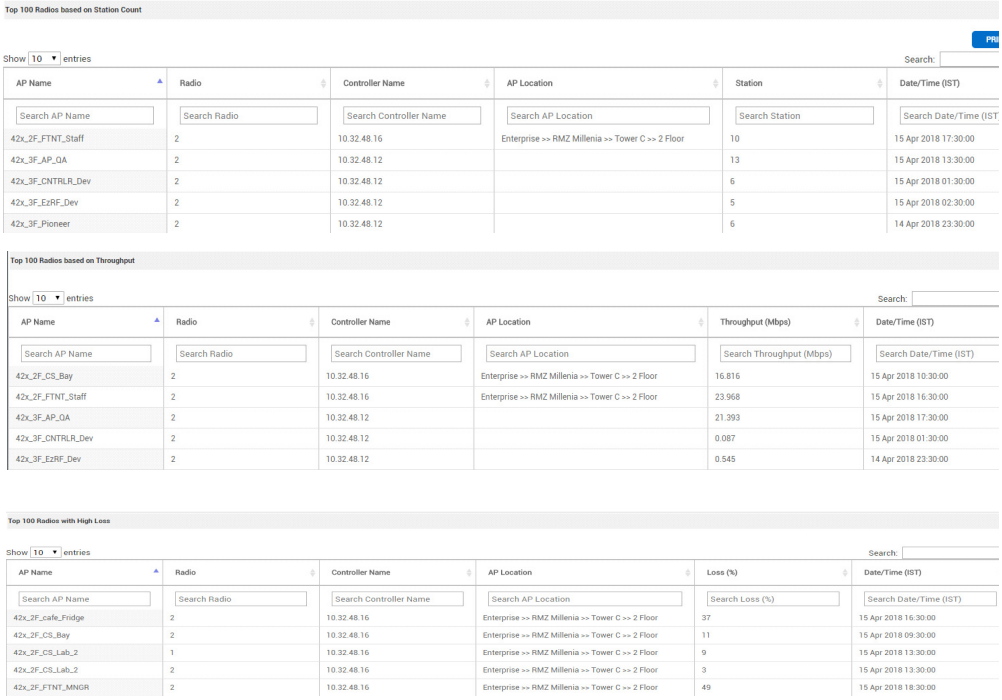
Date/Time (IST)	Controller	AP Detecting Rogue	AP Location	Rogue MAC	Rogue Type	Wired Rogue	Channel	RSSI (dBm)
26 Jan 2014 00:28:14	172.16.16.16	FF-QA-320		24:b9:7b:06:f2:93	Station	No	100	-108
26 Jan 2014 06:38:08	172.16.16.16	FF-QA-320		86:fd:8f:b1:f1:f6	Station	No	100	-108
26 Jan 2014 04:18:11	172.16.16.16	FF-QA-320		d0:15:b2:32:17:14	AP	No	36	-108
25 Jan 2014 22:18:13	172.16.16.16	GF-confAP320		00:af:41:2c:00:12	AP	No	36	-106
26 Jan 2014 09:48:09	172.16.16.16	GF-confAP320		3c:c2:f7:6c:88:02	Station	No	36	-105

Top Radio

The *Top Radio* report type generates reports displaying all the top N radios based on *Station Count, Throughput,* and *High Loss*. The default number of stations displayed is 100. Perform these steps to view the most recent version of the *Top Radio* report.

1. Navigate to the *Reports* > *View Reports* screen.
2. Select *Top Radio* report type to display the report.
3. The details of the *AP Name, Radio, Controller Name, AP Location, Station, Throughput (Mbps), Loss (%)* and *Date/Time (GMT)* is displayed

Figure 212: *Top Radios report*



Top 100 Radios based on Station Count

Show 10 entries Search:

AP Name	Radio	Controller Name	AP Location	Station	Date/Time (IST)
42x_2F_FTNT_Staff	2	10.32.48.16	Enterprise >> RMZ Millenia >> Tower C >> 2 Floor	10	15 Apr 2018 17:30:00
42x_3F_AP_QA	2	10.32.48.12		13	15 Apr 2018 13:30:00
42x_3F_CNTRLR_Dev	2	10.32.48.12		6	15 Apr 2018 01:30:00
42x_3F_EzRF_Dev	2	10.32.48.12		5	15 Apr 2018 02:30:00
42x_3F_Pioneer	2	10.32.48.12		6	14 Apr 2018 23:30:00

Top 100 Radios based on Throughput

Show 10 entries Search:

AP Name	Radio	Controller Name	AP Location	Throughput (Mbps)	Date/Time (IST)
42x_2F_CS_Bay	2	10.32.48.16	Enterprise >> RMZ Millenia >> Tower C >> 2 Floor	16.816	15 Apr 2018 10:30:00
42x_2F_FTNT_Staff	2	10.32.48.16	Enterprise >> RMZ Millenia >> Tower C >> 2 Floor	23.968	15 Apr 2018 16:30:00
42x_3F_AP_QA	2	10.32.48.12		21.393	15 Apr 2018 17:30:00
42x_3F_CNTRLR_Dev	2	10.32.48.12		0.087	15 Apr 2018 01:30:00
42x_3F_EzRF_Dev	2	10.32.48.12		0.545	14 Apr 2018 23:30:00

Top 100 Radios with High Loss

Show 10 entries Search:

AP Name	Radio	Controller Name	AP Location	Loss (%)	Date/Time (IST)
42x_2F_cafe_Fridge	2	10.32.48.16	Enterprise >> RMZ Millenia >> Tower C >> 2 Floor	37	15 Apr 2018 16:30:00
42x_2F_CS_Bay	2	10.32.48.16	Enterprise >> RMZ Millenia >> Tower C >> 2 Floor	11	15 Apr 2018 09:30:00
42x_2F_CS_Lab_2	1	10.32.48.16	Enterprise >> RMZ Millenia >> Tower C >> 2 Floor	9	15 Apr 2018 13:30:00
42x_2F_CS_Lab_2	2	10.32.48.16	Enterprise >> RMZ Millenia >> Tower C >> 2 Floor	3	15 Apr 2018 13:30:00
42x_2F_FTNT_MNGR	2	10.32.48.16	Enterprise >> RMZ Millenia >> Tower C >> 2 Floor	49	15 Apr 2018 18:30:00

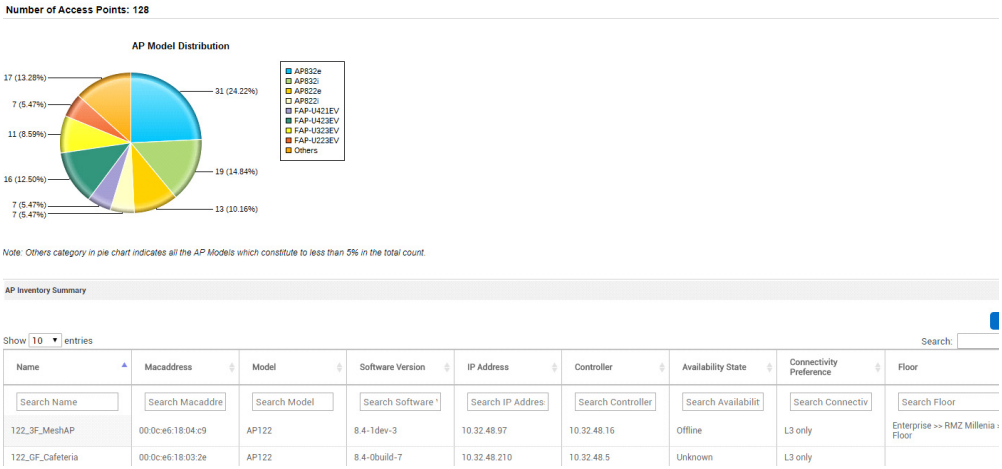
Inventory Reports

Access Points Inventory

The *Access Points Inventory* report type generates the *AP Inventory Summary* which allows you to track all the access points, with its model and software versions on the network. Perform these steps to view the most recent version of the *Access Points Report*.

1. Navigate to the *Reports* > *View Reports* screen.
2. Select *Access Points Inventory* report type to display the report. The primary sections of this report are as follows:
   - **Summary**: Displays the total number of access points.
   - **Graph**: Displays the *AP Model Distribution* graph which depicts the distribution of access points.
   - **AP Inventory Summary**: Displays the details of access point inventory such as *Name, MAC address, Model, Software Version, IP Address, Controller, Availability State, Connectivity Preference* and *Floor*.

Figure 213: *Access Points Inventory report*

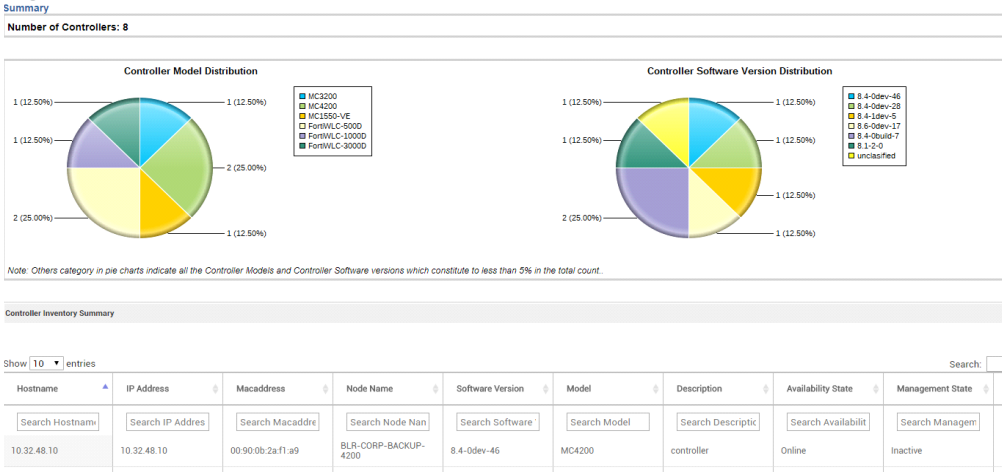


Controller Inventory

The *Controller Inventory* report type generates the *Controller Inventory Summary* which allows you track all the controllers, with its model and software versions on the network. Perform these steps to view the most recent version of the *Controller Inventory* report.

1. Navigate to the *Reports* > *View Reports* screen.
2. Select *Controller Inventory* report type to display the report. The primary sections of this report are as follows:
   - **Summary**: Displays the total number of controllers.
   - **Graph**:
   - **Controller Model Distribution**: Displays the controllers based on the controller model distribution.
   - **Controller Software Version Distribution**: Displays the controllers based on the controller software version distribution.
   - **Controller Inventory Summary**: Displays the details of controller inventory such as *Hostname, IP Address, MAC address, Node Name, Software Version, Model, Description, Availability State, Management State* and *Location*.

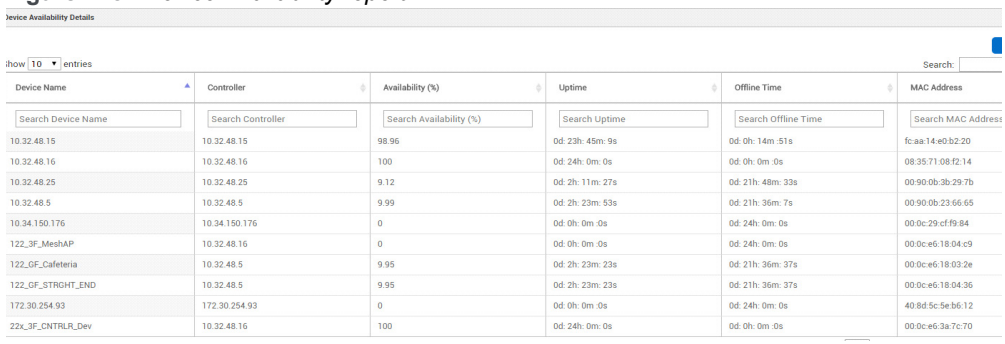
Figure 214: *Controller Inventory* report



Device Availability

The *Device Availability* report type provides you a list of controllers and access points with its availability. It displays the *Device Name, Controller, Availability(%), Uptime, and Offline Time of the AP* and *Controller*.

Figure 215: *Device Availability report*



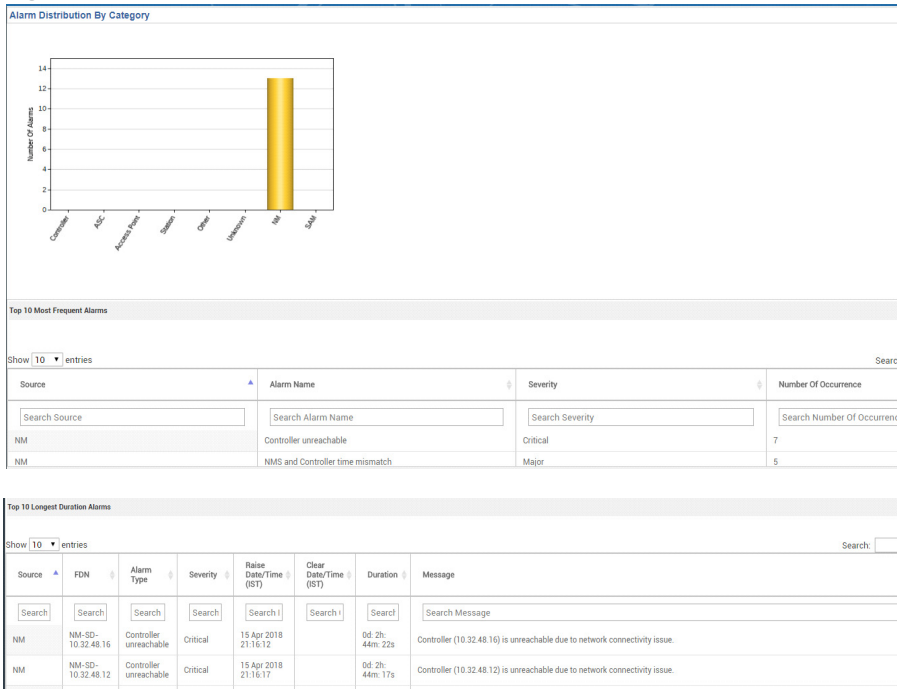
Network Health Reports

Alarm

The *Alarm* report type generates reports based on the total number of critical, major and minor alarms raised on the network. A graphical summary of the alarms distribution by category and top 10 controllers and access points with high alarms is displayed. Perform these steps to view the most recent version of the *Alarm Report*.

1. Navigate to the *Reports* > *View Reports* screen.
2. Choose the *Network Health Reports* category. Select the *Alarm* report type to display the report. The primary sections of this report are as follows:
   - **Summary**: Displays the total number of alarms raised. This includes the critical alarms, major alarms and minor alarms.
   - **Graph**:
     - **Alarm Distribution By Category**: Displays the alarm distribution based on category.
     - **Top 10 Controller with High Alarms**: Displays the alarm distribution based on the controller with high alarms.
     - **Top 10 Access Points with High Alarms**: Displays the alarm distribution based on the access points with high alarms.
   - **Alarm Report tables**: The following types of Alarm Reports are generated:
     - **Top 10 Most Frequent Alarms**: Displays the statistical output of the top 10 most frequent alarms raised with details such as *Category, Alarm Type, Severity,* and *Number of Occurrence*.
     - **Top 10 Longest Duration Alarms**: Displays the statistical output of the top 10 longest duration alarms raised with the details such as *Source, Device ID, Category, Alarm Type, Severity, Raise Date/Time (GMT), Clear Date/Time (GMT), Duration,* and *Message*.
     - **List of Standing Alarms**: Displays the statistical output of top 10 standing alarms raised with the details such as *Date/Time (GMT), Source, Device Name, Category, Alarm Type, Severity,* and *Message.*
     - **Top 10 Devices With High Alarms**: Displays a statistical output of the devices with high alarms raised. It displays the *alarms Device* and *Number of Occurrence*.

Figure 216: *Alarm report*

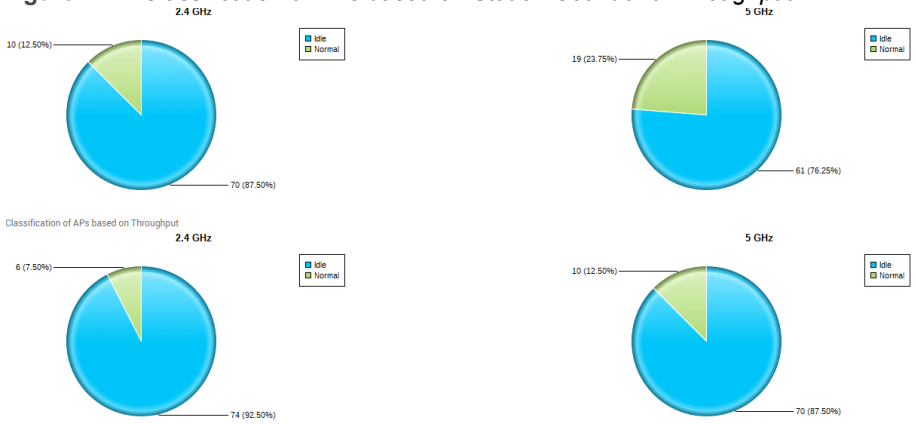


Network Utilization and Capacity

The *Network Utilization and Capacity* report type generates reports based on the overall load of the system. A graphical summary of the classification of APs capacity and consumption based on the data throughput and station count for 2.4 GHz and 5GHz channels is displayed. The aggregate usage of all selected APs for 2.4 GHz and 5GHz channels are computed as a percentage of total capacity. Perform these steps to view the most recent version of the *Alarm Report*.

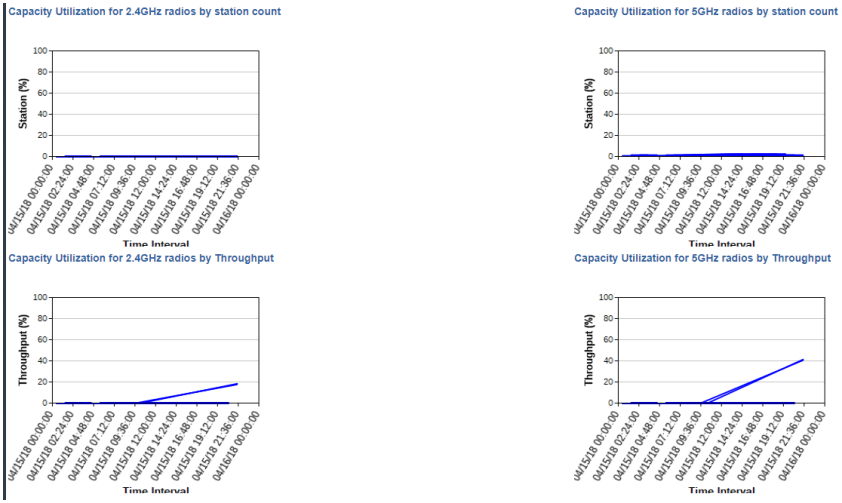
1. Navigate to the *Reports* > *View Reports* screen.
2. Select the *Network Utilization and Capacity* report type to display the report. The primary sections of this report are as follows:

Figure 217: *Classification of APs based on Station Count and Throughput*



- **Graph**:
  - **Capacity Utilization for 2.4GHz radios by station count**: Displays the capacity utilization for 2.4GHz radios by number of stations.
  - **Capacity Utilization for 5GHz radios by station count**: Displays the capacity utilization for 5GHz radios by the number of stations.
  - **Capacity Utilization for 2.4GHz radios by Throughput**: Displays the capacity utilization for 2.4GHz radios by throughput.
  - **Capacity Utilization for 5GHz radios by Throughput**: Displays the capacity utilization for 5GHz radios by throughput.

Figure 218: *Capacity Utilization Trends*



- Network Utilization and Capacity Report tables
  - **List of overloaded APs based on station count**: Displays a statistical output of the list of overloaded APs based on station count as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Settings > Capacity Threshold*). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time,* and *Station Count.*
  - List of capacity APs based on station count: Displays a statistical output of the list of capacity APs based on station count as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Settings > Capacity Threshold*). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time,* and *Station Count.*
  - List of normal APs based on station count: Displays a statistical output of the list of normal APs based on station count as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Settings > Capacity Threshold*). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time,* and *Station Count.*
  - List of idle APs based on station count: Displays a statistical output of the list of idle APs based on station count as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Settings > Capacity Threshold*). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time,* and *Station Count.*
  - List of capacity APs based on Throughput: Displays a statistical output of the list of capacity APs based on throughput as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Settings >*

Capacity Threshold). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time,* and *Station Count.*

- List of normal APs based on Throughput: Displays a statistical output of the list of normal APs based on throughput as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Settings > Capacity Threshold*). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time,* and *Station Count.*
- List of idle APs based on Throughput: Displays a statistical output of the list of idle APs based on throughput as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Settings > Capacity Threshold*). It displays the station's *Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type, Date/Time,* and *Station Count.*
- **List of overloaded APs based on Throughput**: Displays a statistical output of the list of overloaded APs based on throughput as per the threshold value configured for the particular AP model in the *Capacity Threshold* screen (*Administration >System Settings > Capacity Threshold*). It displays the throughput's *Date/Time, Controller, AP Name, AP MAC, AP Location, AP Model, Radio Type,* and *Throughput (Mbps)*.

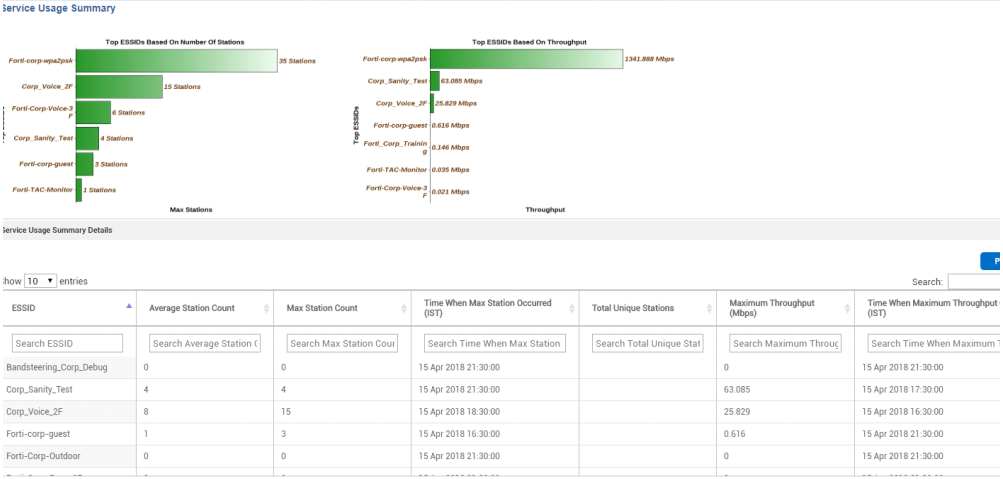
Service Reports

Service Usage Summary

The *Service Usage Summary* report type provides the service usage summary based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed.

1. Navigate to the *Reports* > *View Reports* screen.
2. Choose the *Service Reports* category. Select the *Service Usage Summary* report type to display the report. The primary sections of this report are as follows:
   - **Graph**:
     - **Top SSIDs Based on Number Stations**: Displays the top SSIDs based on number of stations.
     - **Top SSIDs Based on Throughput**: Displays the top SSIDs based on the throughput.
   - **Service Usage Summary**: Displays the *ESSID, Average Station Count, Max Station Count, Time When Max Station Occurred, Total Unique Stations, Maximum Throughput (Kbps)*, and *Time When Maximum Throughput Occurred (GMT).*

Figure 219: *Service Usage Summary report*

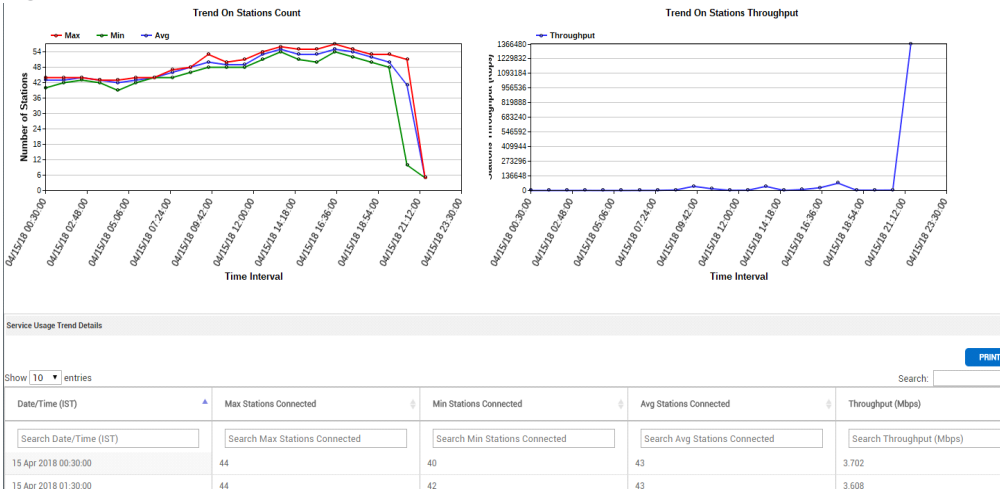


Service Usage Trend

The *Service Usage Trend* report type allows you to generate the service usage trends based on the ESSIDs. A graphical summary of the top SSIDs based on throughput and number of stations is displayed.

1. Navigate to the *Reports* > *View Reports* screen.
2. Select the *Service Usage Trend* report type to display the report. The primary sections of this report are as follows:
    - **Graphs**:
        - **Service Usage Trend**: Displays the trend of *Max, Minimum and Average* stations connected and stations throughput on hourly basis during reporting interval. The graph comprises of three lines, one for *Max* and second one for *Min* and third one for *Average* station count.
        - **Trend on Stations Throughput**:
    - **Service Usage Trend Details**: Displays the *Date/Time (GMT), Max Stations Connected, Min Stations Connected, Avg Stations Connected,* and *Throughput (Kbps)*.

Figure 220: *Service Usage Trend report*



Application Visibility

The *Application Visibility* report type generates the top 10 applications and the top 10 users in your network which allows you to monitor application usage. Perform these steps to view the most recent version of the *Access Points Report*.

1. Navigate to the *Reports* > *View Reports* screen.

2. Select *Application Visibility* report type to display the report. The primary sections of this report are as follows:

Figure 221: *Top 10 applications and Users*

- **Top 10 Application**: The top 10 applications in your network with the following:
  - Number of clients using the application.
  - Number of ESSIDs connected to clients using the application.
  - Total traffic utilization in MB.
- **Top 10 Users:** The top 10 application users in your network with the following:
  - The MAC address of the user.
  - The applications used by the specific user.

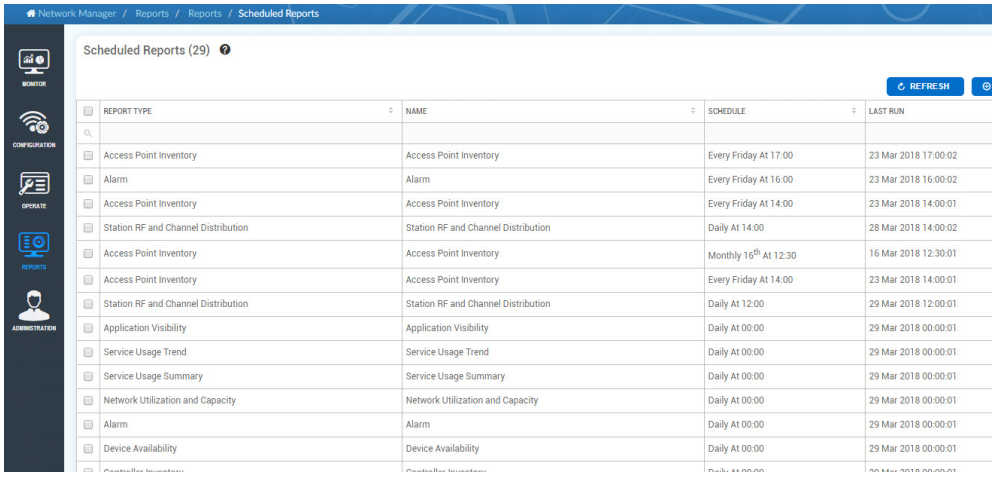
- The ESSIDs connected to clients using the application.
- Total traffic utilization in MB.

Scheduled Reports

The *Scheduled Reports* screen displays a list of *current running* reports and *future reports*. For recurring reports, the next run time is displayed. The generated reports are sorted by generation time.

1. Click *Reports* > *Scheduled Reports*.

Figure 222: *Schedule Reports*



2. It provides the *Report Type, Name, Schedule, Last Run* and *Next Run* details.
3. The report can be scheduled for run by providing the next run details. Select Add option, the *Create Reports screen* is displayed. See *"Create Reports"* ***on page 389***.

PCI Reports

FortiWLM can be validated against specific PCI requirement compliances.

- To run a compliance test, set Run PCI test to **Yes**.
- Now select the tests to validate FortiWLM and click the **RUN TES**T button (located at the bottom of the page).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. The validation results are shown in GREEN ticks if they are passed and in RED CROSS circle if the compliance is not validated or failed.

Click the **DOWNLOAD PDF REPORT** button to get a copy of the valdation results in PDF format.

4 Service Assurance Manager

Service Assurance Manager (SAM) is a predictive diagnostic software with trouble-prevention capability. It diagnosis the health of the wireless network and reports the issue before the users are impacted. The *FortiWLM* infrastructure is used to perform end-to-end system tests, either on-demand or automatically at pre-configured intervals. End-to-end performance tests are run by activating a Virtual Client (VAP) on Fortinet Access Points. Network baseline tests are created and tests are run in the background while *SAM* is still servicing wireless clients. Once baseline network performance is established, any tests that deviate from the baseline can trigger automatic notification. Multiple tests can be configured with *SAM*. Proactive tests are as follows:

- Connectivity tests to measure packet loss and latency
- Voice tests to measure voice quality
- Throughput tests to measure performance

The tests can be configured to run on a variety of wireless profiles like clear, WPA2PSK, and WPA2-AES for every *ESS Profile* available in the *WLAN*. *SAM* summarizes the results obtained and automatically mails to pre-configured destinations.

Notes:

- SAM icons are disabled for APs connected to VPN/NAT/PAT controllers.
- SAM fails when a multiple PSK user exists in FortiWLC. Therefore, use SAM when multiple PSK users are not configured.
- SAM is not supported over WPA3.
- L2 error observed for SAM baseline tests with WPA2 PSK TKIP, WPA2 Enterprise TKIP, WEP64, WEP128, SMS4. Therefore, use other Security modes for running SAM tests.

This table lists the **security modes** supported for the Service Assurance Manager (SAM) on FortiWLM.

AP Model	Security Mode Supported
All supported models	Open
	WPA2 Enterprise AES
	WPA2 PSK AES
	Mixed PSK TKIP
	Mixed Enterprise TKIP

Monitoring SAM

Dashboard

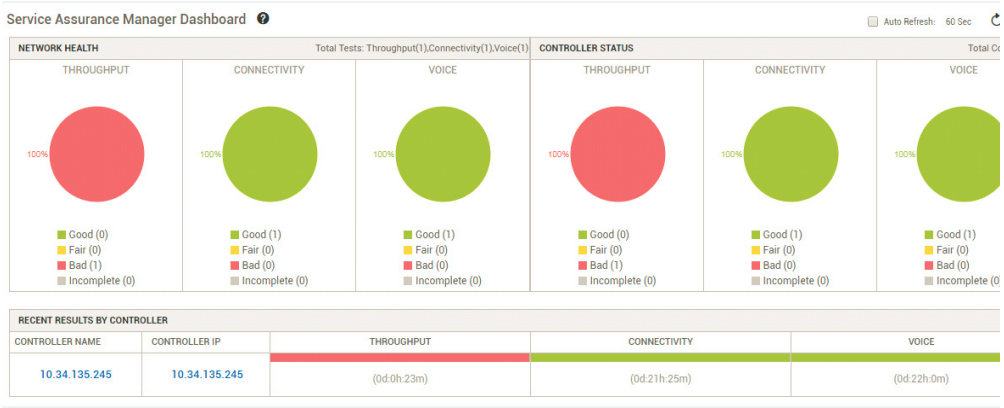
The *SAM Dashboard* provides a rich and interactive view of pertinent wireless data on a single screen. The various charts and statistics described in this chapter helps you determine the overall health of the network.

You are provided with two different dashboards; the *Global Dashboard* providing a general information about the network itself and the *Controller Dashboard* displaying the data on a per-controller basis.

Global Dashboard

The *Global Dashboard* provides information pertinent to the overall health of the wireless deployment. From here, you can observe whether there are any general problems in the network (such as low throughput) as well as more specific matters (such as poor voice quality on wireless calls).

Figure 223: *Global Dashboard View*



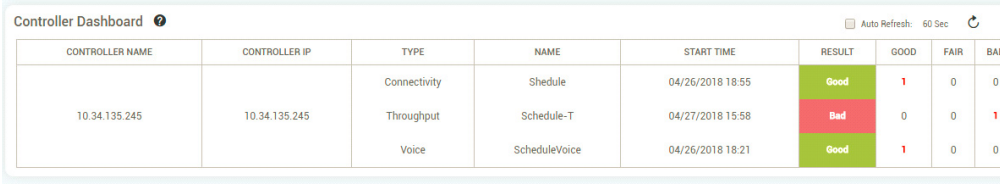
The pie charts shown are color-coded to ensure that you can easily determine whether or not a network issue requires attention.

The lower section of the screen displays the same information divided by controller, allowing you to identify any controllers that are generating bad results. Selecting any of the linked controllers shown in the recent results by controller section will direct you to that controller's test information.

Controller Dashboard

The *Controller Dashboard* displays individual statistics for each wireless controller during deployment.

Figure 224: *Controller Dashboard View*



The dashboard allows you to view the overall throughput health. Select any of the column table heading to sort the data in the table:

1. Navigate to *Monitor* > *Dashboard* > *Controller Dashboard*. The *Controller Dashboard* screen provides a list of all controllers that are tested for *Connectivity, Throughput and Voice* by *SAM* with the following details:

Field	Description
Controller Name	Displays the controller name. The controller name displayed is the controller mapped to the *FortiWLM* inventory; the baseline runs on the indicated controller. This is one of the values that links a baseline to subsequent tests.
Controller IP	Displays the controller IP. The controller IP address displayed is the controller mapped to the *FortiWLM* inventory; the baseline runs on the indicated controller. This is one of the values that links a baseline to subsequent tests.
Type	Displays the test type. The types are as follows: • Connectivity • Throughput • Voice
Name	Displays the test name that is provided to each test.
Start Time	Displays the time at which each test started.
Result	Displays the result of the test. The results appear in different color. The result types are as follows: • Good • Fair • Bad • Stopped • Offline • No Neighbors • APs Offline • Controller Offline Select a colored result to view the elaborate test details for the selected controller which is displayed in a new window.
Good	Displays the count for *Good* results. Click on the count that is hyperlinked. The *Test Details* screen is displayed.
Fair	Displays the count for *Fair* results. Click on the count that is hyperlinked. The *Test Details* screen is displayed.
Bad	Displays the count for *Bad* results. Click on the count that is hyperlinked. The *Test Details* screen is displayed.

Field	Description
N/A	Displays the results that are not applicable.

Click any *Controller IP* address to view the controller's details that were used to create the charts.

Trends

The *Trends* page provides the graphical representation of the *Completed* and *Failed* recurring tests. The following are the types of Trends Dashboard.

- Results Trends - Refer to *"Results Trends"* ***on page 423***
- Failure Trends - Refer to *"Failure Trends"* ***on page 428***

Results Trends

Navigate to *Monitor* > *Trends* > *Result Trends*. The *Results Trend* page provides the graphical representation of the completed recurring tests.

To view the results trend for the completed tests perform the selections in the following three sections:

- *"Header Section"* ***on page 423***
- *"Trend Graphs Section"* ***on page 425***
- *"Matrix Section"* ***on page 428***

Header Section

The header section consists of the following fields as displayed in the below table:

Field	Description
Controller Name	Provides the complete list of *Controller Names* for which the test was run. You can either select the *Controller Name* or the *Controller IP*. By the selection of either of the options, the other is selected automatically.
Controller IP	Provides the complete list of *Controller IPs* for which the test was run. You can either select the *Controller IP* or the *Controller Name*. By the selection of either of the options, the other is selected automatically.

Field	Description

Test Type	Displays the *Test Type* as follows:
	• **Connectivity**: *Connectivity* describes if the station is connected to the AP. Connectivity can be verified by sending ping traffic (ICMP) run from one point to another. The test result for *Connectivity* is displayed in% (percentage) for packet loss and ms (Millisecond) for latency or average round trip times (rtt).
	• **Throughput**:
	Throughput is the amount of data moved successfully from one place to another in a given time period. The throughput test type can further be divided as follows:
	  • **Throughput TCP**: The test result for *Throughput TCP* is displayed in *Mbps*.
	  • **Throughput UDP**: The test result for *Throughput UDP* is displayed in *Mbps,% (percentage)* for *Packet Loss* and *ms (Millisecond)* for *Latency*.
	• **Voice**: *Voice* is simulated using multiple thread of ping traffic.
	The selection of the *Test Type* as *Voice determines* the rest of the options on the page. The test result for *Voice* is displayed in% (percentage) for packet loss and ms (Millisecond) for latency or average round trip times (rtt).
	Note: The connectivity, voice and throughput UDP test type allows you to choose a type of Matrix from the Matrix section. The types are *Latency* and *Packet loss*.
	Select one of the above mentioned *Test Type* from the drop-down list.

Test Name	Displays the *Test Name*. Select a test name from the drop-down list.
Start Time	Select the *Start Time*. The format followed is the *mm/dd/yyyy* and *hh:mm:ss format*. The time can be entered manually or by selecting the calendar icon. The calendar is displayed, where the date and time can be modified manually.
End Time	The *End Time* is automatically selected for the current date. To modify the end time and date, uncheck the *Now* option and enter the date manually. Else select the calendar icon. The calendar is displayed, where the date and time can be modified manually.

1. Select all the parameters from the above mentioned fields.
2. Select the *Show Trend* button. The trend graph gets plotted in the *Trend Graphs* Section.

3. The charts can be modified according to the selected row or column or single cell or for all the table cells.

Trend Graphs Section

The *Trend Graphs Section* displays the trend of *Good, Fair, Bad* and *Incomplete* test results of the selected test type and controller within the specified date range.

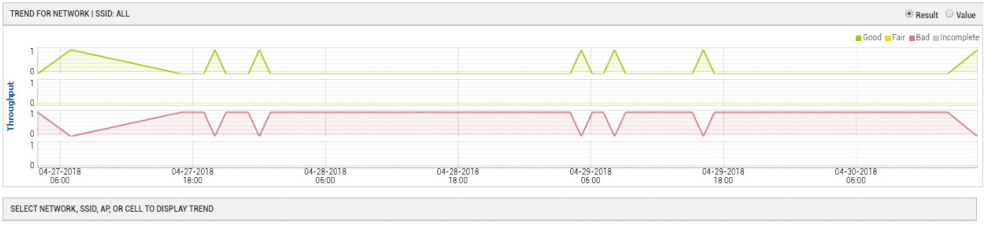
The following two types of Trend graph results are displayed.

- Results Graph - Refer to *"Result graph"* **on page 425**
- Value Graph - Refer to *"Value graph"* **on page 426**

Result graph

The *Result* graph displays the matrix of the test instances. The cell values in the matrix, is the average value for the selected test instance. It displays the incomplete test counts, respectively. The result chart is plotted either by selecting a row or column or single cell or for all table cells. The data for each plotted line in the graph is viewed by hovering the mouse pointer over individual section.

Figure 225: *Results Graph*



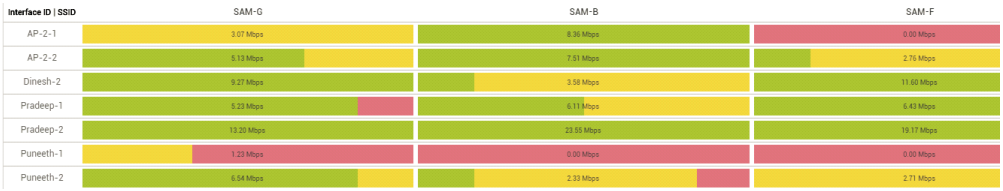
The *Date/Time, Good, Fair, Bad,* and *Incomplete* numbers are displayed with four different colors as follows:

Result Type	Description	Color
Good	If the number of tests with fair and bad results is zero, then a test is good.	
Fair	If no test has a bad result and at least one test has a fair result, then a test is fair.	

Result Type	Description	Color
Bad	If there is at least one test with a bad result, then a test is bad.	
Incomplete	If the test stops in between, then the test is incomplete.	

For Example:

The below example provides the completed results of *Throughput TCP. The* test consists of 3 ESSIDs selected against the radios of applications which need to run the throughput test.



From the above mentioned three samples the throughput completed results, the number of Good, Fair, Bad and Incomplete are calculated.

Good	Fair	Bad	Incomplete
15	10	7	0
5	3	0	0
5	3	0	0

Value graph

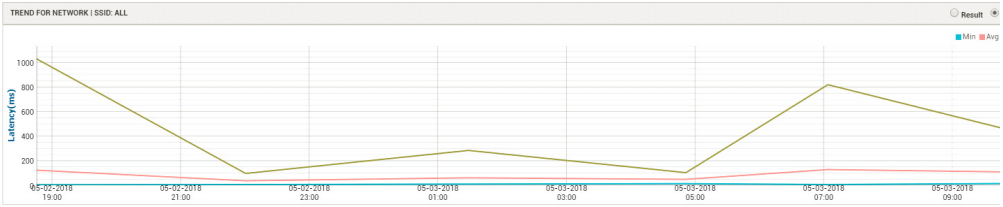
The *Value* graph displays three lines for *Minimum, Average* and *Maximum* values for complete test results. The value chart is plotted either by selecting a row or column or single cell or for all table cells. The individual data for each plotted line in the graph can be viewed by hovering the mouse pointer over the section.

Two buttons are available in the *Value Graph* section. They are as follows:

- Latency
- Packet Loss

The respective graphs are displayed as per the selection of the respective option as mentioned above.

Figure 226: *Results Trend - Value Graph*

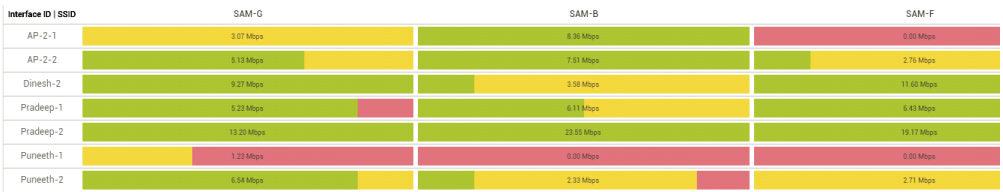


The *Date/Time, Minimum, Average* and *Maximum* numbers are displayed with three different colors as follows:

Result Type	Description	Color
Minimum	The *Minimum* value is calculated by comparing all the values in the each of the test examples and the least value is considered as the minimum value.	
Average	The *Average* value is the sum of all the values in each of the test examples, divided the total by the number of values.	
Maximum	The *Maximum* value is calculated by comparing all the values in each of the test examples and the highest value is considered as the maximum value.	

For Example:

Consider the three sample *Throughput TCP* completed results (Test1, Test 2 and Test 3) with their test details. Each test consists of 2 Rows and 2 columns of data, since we have 2 ESS Profiles and 2 AP-Radios:



From the above mentioned three completed throughput results with their test details, the number of *Minimum, Average* and *Maximum* values can be calculated as follows:

- **Minimum**:
  The *Minimum* value is calculated by comparing all the values in the each of the test examples and the least value is considered as the minimum value.

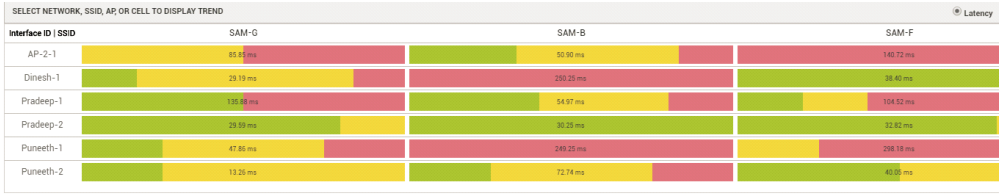
- **Maximum**:
  The *Maximum* value is calculated by comparing all the values in each of the test examples and the highest value is considered as the maximum value.
- **Average**:
  The *Average* value is the sum of all the values in each of the test examples, divided by the total number of values.

Minimum	Average	Maximum
0.00 Mbps	6.56 Mbps	23.55 Mbps

Matrix Section

The *Matrix* of the test instances consists of bar charts for table cells, average test instance value across the results.

Figure 227: *Results Trend - Matrix Section*



Consider the above completed throughput test results. From the above mentioned test results, the *Minimum, Average and Maximum* values can be calculated.

The test results for *Connectivity, Voice* and *Throughput UDP Test Types* are displayed in% (percentage) for *Packet Loss* and ms (Millisecond) for *Latency* or average round trip times (rtt). The test result for *Throughput UDP* is displayed in Mbps,% (percentage) for *Packet Loss* and ms (Milli Second) for *Latency*.

Failure Trends

1. Navigate to *Monitor* > *Trends*> *Failure Trends*. The *Failure Trends* screen provides the graphical representation of the failed recurring tests.
2. This page is divided into the following three sections:
   - *"Header Section"* ***on page 429***
   - *"Failure Trends Graphs Section"* ***on page 430***
   - *"Matrix Section"* ***on page 432***

Header Section

The header section consists of the following fields as displayed in the below table:

Field	Description
Controller Name	Displays the complete list of *Controller Names*, for which the test was run. You can either select the *Controller Name* or the *Controller IP*. By the selection of either of the options, the other is selected automatically.
Controller IP	Displays the complete list of *Controller IPs* for which the test was run. You can either select the *Controller IP* or the *Controller Name*. By the selection of either of the options, the other is selected automatically.

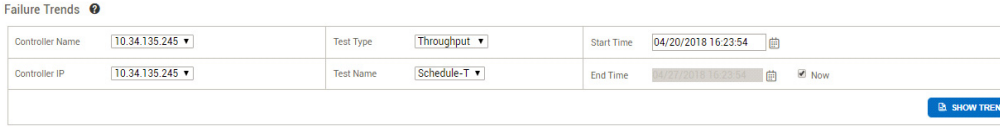
Test Type	Displays the Test Type as follows:
	• **Connectivity**: *Connectivity* describes if the station is connected to the AP. Connectivity can be verified by sending ping traffic (ICMP) run from one point to another. The test result for *Connectivity* is displayed in% (percentage) for packet loss and ms (Millisecond) for latency or average round trip times (rtt).
	• **Throughput**:
	Throughput is the amount of data moved successfully from one place to another in a given time period. The throughput test type can further be divided as follows:
	  • **Throughput TCP**: The test result for *Throughput TCP* is displayed in *Mbps*.
	  • **Throughput UDP**: The test result for *Throughput UDP* is displayed in *Mbps,% (percentage)* for *Packet Loss* and *ms (Millisecond)* for *Latency*.
	• **Voice**: *Voice* is simulated using multiple thread of ping traffic.
	The selection of the *Test Type* as *Voice determines* the rest of the options on the page. The test result for *Voice* is displayed in% (percentage) for packet loss and ms (Millisecond) for latency or average round trip times (rtt).
	Note: The *Connectivity, Voice, and Throughput UDP* test type allows you to choose a type of *Matrix* from the *Matrix* section. The types are Latency and Packet loss.
	Select one of the above mentioned Test Type from the drop-down list.

Field	Description
Test Name	Displays the *Test Name*. Select the test name from the drop-down list.
Start Time	Select the *Start Time*. The format followed is the *mm/dd/yyyy* and *hh:mm:ss format*. The time can be entered manually or by selecting the calendar icon. The calendar is displayed, where the date and time can be modified manually.
End Time	The *End Time* is automatically selected for the current date. To modify the end time and date, uncheck the *Now* option and enter the date manually. Else select the calendar icon. The calendar is displayed, where the date and time can be modified manually.

1. Select all the parameters from the above mentioned fields.
2. Select the *Show Trend* button. The *FCA (Failure Causal Analysis*) graph results are displayed.

The charts can be modified according to the selected row or column or single cell or for all the table cells.

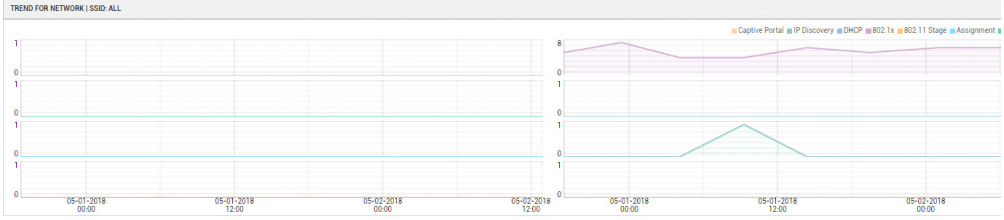
Figure 228: *Failure Trends - Header Section*



Failure Trends Graphs Section

The *Failure Trend Graph* section displays the details of the *Eight* varieties of failure cases. The individual data for each of the stages is plotted in an individual graph. The details can be viewed by hovering the mouse pointer over each graph. The values for each of the stage is displayed with different colors.

Figure 229: *Failure Causal Analysis graph*



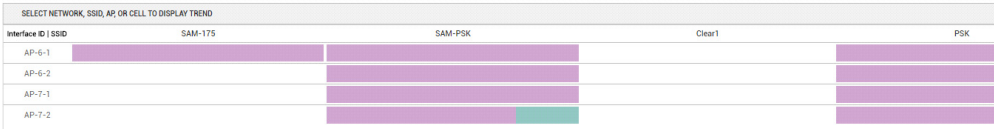
The *FCA (Failure Causal Analysis)* provides details for the failure cases. The following are the eight failed stages:

Result Type	Description	Color
Initiation	Here, *SAM* gathers the data that requires to start a test and initiates the test. If *SAM* fails to gather the data or failed to start a test, *SAM* says the test has failed in this stage.	
MAC Filtering	The station goes through this stage when MAC filtering is enabled. A MAC filtering is either ACL-based or Radius-based. If the authentication of MAC filtering succeeds, the station proceeds to the next stage assignment. If MAC filtering is disabled, this stage is skipped.	
Assignment	Here, the station is assigned to an AP (BSSID). If the station fails to get an assignment from the AP, *SAM* says assignment has failed or not reached.	
802.11 Stage	Here, the station will be authenticated and associated to an AP (BSSID).	
802.1xAuth	This is for *Radius-based User authentication* and for Key exchange. The station goes through this stage only for radius based profiles. If the radius authentication fails or key exchanges are timed out, *SAM* says 802.1x failed. This also includes EAP failures which include wpa-psk and wpa2psk along with Radius failures.	
DHCP	Here, the station tries to get an IP address using DHCP mechanism. If the station receives the IP address, this stage is successful, else *SAM* treats this stage as failed.	
IP Discovery	Once the station receives an IP address using static or DHCP mechanism, this will be updated to the controller. After the controller receives this update the stage is passed. If captive portal is not enabled for connected profiles, the station is successfully connected to the network. If the controller does not get update this stage is failed.	
Captive Portal	The station goes through this stage only if the captive portal is enabled for connected profile. The station does a captive portal Authentication. Once the captive portal authentication is successful, the stage is passed and the client clears all the stages successfully and is connected to the network.	

Matrix Section

The *Matrix Section* of the test instances consists of bar graph depicting the failure count graphically. The values of each of the eight failed stages can be viewed by hovering the mouse pointer over the section.

Figure 230: *Matrix section*



Monitor Tests

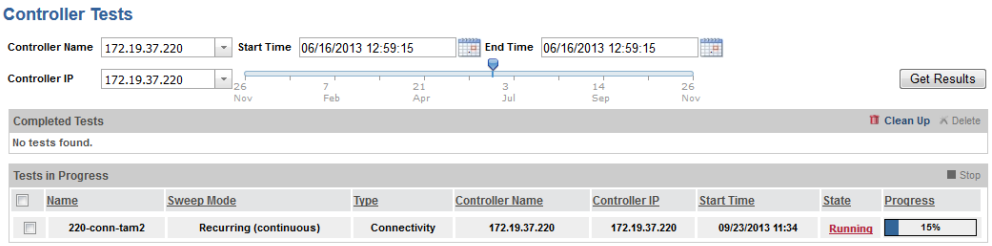
The *Tests* in the *Monitor* menu allows you to monitor the *completed, ongoing baseline* and *scheduled tests*.

View Test Results for a Controller

To view The test result for a controller during the given time period, follow these steps:

1. Navigate to *Monitor* > *Tests* > *Controller Tests*.

Figure 231: *Controller Tests*



2. Select a *controller name* or *IP address* from the drop-down list.
3. The controller list, displays all the controllers for which the test was run in the past and for which the tests that are in progress.
4. Select the *Start Time* and *End Time*. The format followed is the *mm/dd/yyyy* and *hh:mm:ss* format. The time can be entered manually or by selecting the *calendar* icon. The calendar is displayed, where the date and time can manually be modified.
5. The *Start Time* and *End Time* can also be modified by adjusting the slider. The slider can be dragged along a fixed-length line representing a linear range dates.

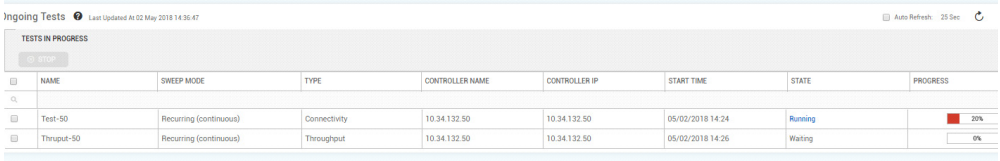
The *Start Time* to *End Time* duration cannot exceed more than one week.

6. Select *Get Results*. The completed test results for the selected controller is displayed. The controller results for the tests that are in progress is also displayed.
7. Select on the result of a test (*Good, Bad, Fair, Failed in the Result* column). Click *Close*.

View a Test in Progress

1. Navigate to *Monitor* > *Tests* > *Ongoing Tests*.

Figure 232: *Ongoing Tests*



2. The *Ongoing Tests* screen lists all the *scheduled* and *baseline* tests that are still in progress. A test is selected by checking the boxes. A test, in a run or wait state can be stopped by clicking *Stop*. If the test in a run state is stopped, the state is modified from *run* to *stop*.
3. The *Tests in Progress* table in the *Ongoing Tests* screen display the *Name, Sweep Mode, Type, Controller Name, Controller IP, Start Time, State and Progress* of the *ongoing scheduled* and *baseline* tests.

See the ***Ongoing Tests*** screen (*Monitor* > *Tests* > *Ongoing Tests*) in Online Help for detailed information on *Ongoing Tests* topic.

View all the Completed Tests

You can view The test result for a selected controller during a given time period, or you can view most recent scheduled *Throughput/ Connectivity/ Voice* test results from *FortiWLM* during a given time period. To view most recent test results from *FortiWLM* during a given time period, follow these steps:

1. Navigate to *Monitor* > *Tests* > *Completed Tests*
2. Select the test result **Good**, **Bad**, **Fair**, **Failed** in the Result column.
   The detailed test results are displayed.

Definitions of Test Results

The result of a successful test can be *good, bad,* or *fair.* The amount of change is configured with the good-threshold and bad-threshold parameters you provided when you created the test (see *"Add a Scheduled Test"* **on page 407**).

Result	What it means
Good	If the number of tests with fair and bad results is zero, then a test is good.
Bad	If there is at least one test with a bad result, then a test is bad. Click the number in this column to see the results of the bad tests.
Fair	If no test has a bad result and at least one test has a fair result, then a test is fair.
Controller Offline	The Controller is offline.
Stopped	The test was stopped.
No Baseline	No baseline (connectivity or throughput) was available for comparison on this controller. This can happen, for example, if you add new access points after the running the last baseline for this controller.

Click *Result* in the *Actions* column to see a list of tests performed over each radio and SSID. To see results for each test, click the cell of the table in the *Actions* popup.

Configuring SAM

Baseline Testing

A baseline, like the name implies, is a standard for future comparison. Baselines are established in *SAM* by running a virtual client to all APs on a controller and measuring the results. This baseline is used for future *Scheduled Test* comparisons at regular intervals.

Design a Baseline

When you design a baseline, the number of controllers sharing an ethernet port connection and bandwidth is taken into consideration. Performing concurrent tests on multiple controllers sharing bandwidth affects testing thresholds set in the baseline. The controller's thresholds are programmed based on the number of controllers. For an accurate comparison, the bandwidth must be the same for subsequent comparisons against the baseline. Another way to alter baseline thresholds is to remove APs and/or SSIDs from the test.

The design of a baseline does not affect throughput, latency or packet loss. The *throughput, latency, and packet loss* during a baseline connectivity test depends on the environment (num-

ber of packets in the air) when a virtual client is operating. However, the number of APs present while configuring a baseline does not affect the results.

Bridged traffic is not displayed in the throughput, as it does not pass through the controller.

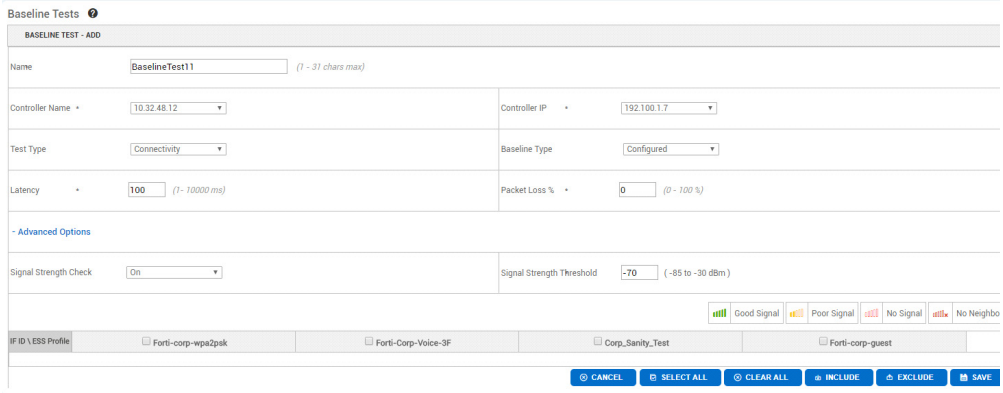
Add a Baseline

We have two options to execute the baseline tests.

- **Configured Test**: This option allows you to create a baseline test by providing theoretical values.
- **Measured Test**: This option allows you to create a baseline test by providing the actual baseline values. It is important to run a measured baseline when the wireless network is operating either normally or under optimal conditions, as it is used to evaluate subsequent tests. To create either type of baseline, follow these steps:

1. Navigate to *Configure* > *Tests* > *Baseline Tests* > *Add Baseline*.

Figure 233: *Baseline Test - Add*



2. In the *Baseline Test - Add* screen, provide the following required information:

Field	Descriptions
Name	Provide a name of the *Baseline Test* primarily for usage. The name consists of up to 31 characters, including numbers, letters, capital letters, and special characters. Special characters cannot be used

Field	Descriptions
Controller Name	Select the *Controller Name* or the Host name from the drop-down list. The controller name displayed, is the controller mapped to the *FortiWLM* inventory; the baseline runs on the indicated controller.
Controller IP	Select the *Controller IP* address from the drop-down list. The controller IP address displayed is the controller mapped to the *FortiWLM* inventory; the baseline runs on the indicated controller.

Test Type	Select the *Test Type* from the drop-down list. The options are as follows:
	• **Connectivity**:
	Connectivity describes if the station is connected to the AP. Connectivity can be verified by sending ping traffic (ICMP) run from one point to another.
	The selection of the *Test Type* as *Connectivity* determines the rest of the options on the page. Refer to *"Test Type - Connectivity"* ***on page 437***.
	• **Throughput**:
	Throughput is the amount of data moved successfully from one place to another in a given time period. The selection of the *Test Type* as *Throughput* determines the rest of the options on the page. The throughput test type can further be divided as follows:
	  • Throughput TCP (Transmission Control Protocol) Refer to *"Throughput - TCP"* ***on page 438***
	  • Throughput UDP (User Datagram Protocol) Refer to *"Throughput - UDP"* ***on page 438***
	• **Voice**:
	Voice is simulated using multiple thread of ping traffic.
	The selection of the *Test Type* as *Voice determines* the rest of the options on the page. Refer to *"Test Type - Voice"* ***on page 440***.
	The scheduled tests that run on the selected controller must match the test type in order to measure against the baseline.

Field	Descriptions
Test Type - Connectivity	
By selecting the *Test Type* as *Connectivity*, the following fields appear:	

Baseline Type	Select the *Baseline Type* from the drop-down list. The options are as follows:
	• **Configured**: The configured option does not permit you to run a baseline test, but it allows you to configure a baseline test based on theoretical values. This option enables the following fields:
	  • **Latency (Connectivity test only)**: Latency is an expression of how much time is taken for a packet of data to get from one designated point to another. A low latency network connection generally experiences small delay times, while a high latency connection generally suffers from long delays.
	  Provide a latency value for a baseline connectivity test (1-1000ms). The default value is 100.
	  • **Packet Loss % (Connectivity test only)**: Packet loss is the failure of one or more transmitted packets to arrive at their destination.
	  Enter the packet loss % value. The default is 0.
	• **Measured**: The measured option allows you to run the baseline test. If there are no tests running on the selected controller, the baseline starts immediately. If there are some tests running on the selected controller, the baseline will wait for the completion of the current running test, although there is a scheduled test waiting to get started. Only other baselines of the same test type (*Connectivity, Throughput or Voice*) will take precedence over this test. This option enables the following fields:
	  • **Notification**: This option enables you to receive notifications of the completed test results through email. Select the notification from the drop-down list.
	  • **Notification Profile**: Select the notification profile from the drop-down list. The notification profiles are configured in the Network Manager. (*Administration > User Preference > Notification Profiles*).
	  • **Notification Message**: Type a notification message (max 64 chars).
	The *"Advanced Options"* ***on page 441*** are displayed when the *Baseline Type*, *Measured* is selected.

Field	Descriptions
Throughput - TCP	

Baseline Type	Select the *Baseline Type* from the drop-down list. The options are as follows:
	• **Configured**: The configured option does not permit you to run a baseline test, but it allows you to configure a baseline test based on theoretical values. This option enables the following fields:
	  • **Throughput**: Enter the *Throughput* value (1-150 Mbps).
	  • **Stream**: Select the *Stream* from the drop-down list. The options is Up (default), Down.
	• **Measured:** The Measured option allows you to run the baseline test. If there are no tests running on the selected controller, the baseline starts immediately. If there are some tests running on the selected controller, the baseline will wait for the completion of the current running test, although there is a scheduled test waiting to get started. Only other baselines of the same test type (*Connectivity, Throughput or Voice*) will take precedence over this test. This option enables the following fields:
	  • **Notification**: This option enables you to receive notifications of the completed test results through email. Select the notification from the drop-down list.
	  • **Notification Profile**: Select the notification profile from the drop-down list. The notification profiles are configured in the *Network Manager* application. (*Administration > User Preference > Notification Profiles*).
	  • **Notification Message**: Type a notification message (max 64 chars).
	  • **Stream**: Select the stream from the drop-down list. The options are as follows:
	  • **Up**: Upstream traffic refers to data that is sent from a computer or network. (default)
	  • **Down**: Downstream traffic refers data that is received by a computer or network.
	The *"Advanced Options"* ***on page 441*** are displayed when the Baseline Type, Measured is selected.

Throughput - UDP	

Field	Descriptions

Baseline Type	Select the Baseline Type from the drop-down list. The options are as follows:
	• **Configured**: The configured option does not permit you to run a baseline test, but it allows you to configure a baseline test based on theoretical values. This option enables the following fields:
	  • **Throughput**: Enter the *Throughput* value (1-150 Mbps).
	  • **Stream**: Select the stream from the drop-down list. The options are as follows:
	  • **Up**: *Upstream* traffic refers to data that is sent from a computer or network. (default)
	  • **Down**: *Downstream* traffic refers data that is received by a computer or network.
	• **Measured**: The *Measured* option allows you to run the baseline. If there are no tests running on the selected controller, the baseline starts immediately. If there are some tests running on the selected controller, the baseline will wait for the completion of the current running test, although there is a scheduled test waiting to get started. Only other baselines of the same test type (*Connectivity, Throughput or Voice*) will take precedence over this test. This option enables the following fields:
	  • **Notification**: This option enables you to receive notifications of the completed test results through email. Select the notification from the drop-down list.
	  • **Notification Profile**: Select the notification profile from the drop-down list. The notification profiles are configured in the *Network Manager* application. (*Administration* > *User Preference* > *Notification Profiles*).
	  • **Notification Message**: Type a notification message (max 64 chars).
	  • **Stream**: Select the stream from the drop-down list. The options are as follows:
	  • **Up**: *Upstream* traffic refers to data that is sent from a computer or network. (default)
	  • **Down**: *Downstream* traffic refers data that is received by a computer or network.
	The *"Advanced Options"* ***on page 441*** are displayed when the Baseline Type, Measured is selected.

Field	Descriptions
Test Type - Voice	

Baseline Type	Select the *Baseline Type* from the drop-down list. The options are as follows:
	• **Configured**: The configured option does not permit you to run a baseline test, but it allows you to configure a baseline test based on theoretical values. This option enables the following fields:
	  • **Latency (Connectivity test only)**: Latency is an expression of how much time is taken for a packet of data to get from one designated point to another. A low latency network connection generally experiences small delay times, while a high latency connection generally suffers from long delays.
	  Provide a latency value for a baseline connectivity test (1-1000ms). The default value is 100.
	  • **Packet Loss % (Connectivity test only)**: Packet loss is the failure of one or more transmitted packets to arrive at their destination.
	  Enter the packet loss % value. The default is 0.
	  • **Number of Calls**: Enter a value for the number of calls (1-15).
	• **Measured**: The Measured option allows you to run the baseline. If there are no tests running on the selected controller, the baseline starts immediately. If there are some tests running on the selected controller, the baseline will wait for the completion of the current running test, although there is a scheduled test waiting to get started. Only other baselines of the same test type (*Connectivity, Throughput or Voice*) will take precedence over this test. This option enables the following fields:

Field	Descriptions
	• **Notification**: This option enables you to receive notifications of the completed test results through email. Select the notification from the drop-down list. • **Notification Profile**: Select the notification profile from the drop-down list. The notification profiles are configured in the *Network Manager* application. (*Administration* > *User Preference* > *Notification Profiles*). • **Notification Message**: Type a notification message (max 64 chars). • **Number of Calls**: Enter a value for the *Number of Calls* (1-15). The *"Advanced Options"* ***on page 441*** are displayed when the Baseline Type, Measured is selected.
Advanced Options	
Retries	Type the number of *Retries*. This field allows you to configure the number of retries when SAM tests fail for an *ESS Profile*. The minimum value is 0 (zero) and the maximum value is 2 (two).
Timeout	Type the *Timeout* value. If the test takes longer than this (10 - 30 seconds), fail it.
Redo Failed Tests	Check the *Redo Failed Tests* option, the tests get repeated for failed tests.
Tunnel Type	Select the *Tunnel Type* from the drop-down list. The options are as follows: • **Ether IP:** This is the default tunnel. Here the data packets are sent through the ether IP tunnel, between the *FortiWLM* and AP. • **Ether UDP:** Here the data packets are sent through the Ether UDP tunnel, between the *FortiWLM* and AP.
Signal Strength Check	Select the *Signal Strength Check* from the drop-down list. The options are as follows: • **On**: The surroundings are examined for the presence or absence of the neighbor APs. If the neighbor AP is present, then the signal strength threshold is examined. The signal strength threshold must be within (-85 to -30 dBm). The default value is -70dBM. • **Off**: The surroundings are not examined for the presence or absence of the neighbor APs.

Field	Descriptions
Signal Strength Threshold	The *Signal Strength Threshold* is applicable only when the *Signal Strength Check* option is *On*. The *Signal Strength Threshold* must be within (-85 to -30 dBm). The default value is -70dBM.
Ping test before Throughput	Select the *Ping test before Throughput* from the drop-down list. The options are as follows: • **On**: The ping is run before running the throughput test. • **Off**: The ping is not run before the throughput test. This option is *On* by default. The throughput tests can still be run when the ICMP is blocked by turning the ping Off.
Buffer Length	Enter the *Buffer Length* value (1KB-1MB). *Buffer Length* is the amount of data to be sent. The default value is 128 KB.
Window Size	Enter a value for the *Window Size*. (8KB-128KB). The *Window Size* is the TCP window size. The default value is 85.3 KB.
Packet Size	Enter the *Packet Size value* (1 -1280 Bytes). The *Packet Size* is the size of UDP data packet to be sent. The default Value 1024 Bytes. Range is (1-1280 Bytes).
Buffer Size	Enter a value for the *Buffer Size*. (8KB-128KB). The buffer size is the socket send buffer size (SO_SNDBUF). The default value is 85.3KB.
Bandwidth	Enter the *Bandwidth* value (1Kbps-50 Mbps). The bandwidth is the amount of UDP data to be pumped in bits/sec. The default value is 5Mbps.
Logging Detail	Select the *Logging Detail* from the drop-down list. The options are as follows: • **Log only critical messages**: This option logs only the critical messages. • **Log all messages**: This option logs all the messages.

3. Select at least one cell for the baseline test and select the *Include* option.

If you receive the error “Please include at least one cell for baseline test” that means that no cell has been selected. Go back and select them.

If there are no rows or columns listed, then the selected controller has no APs with IP address.

4. Click *Save* to save the baseline as configured baseline (indicated in the *Baseline Type* column) at the top of the list.
5. Click *Save & Run* to save and run the baseline as measured baseline. The *Save & Run* option is displayed only for the *Measured Baseline Type*.

If you have selected the *Measured Baseline Type*, a virtual client with its own IP address runs on each interface, each profile, measuring the current values for the selected controller. The completed test results of the measured baseline test results are displayed on the baseline tests screen. You can schedule a throughput test, once a baseline test is established.

If you stop any test, you must restart the test from the beginning.

Scheduling Tests

The tests are the central activity of the *SAM* application that is dealt the most. A baseline test is performed occasionally, but the scheduled tests and their results are monitored constantly. The test results can be notified through email.

Scheduled tests are measured against a baseline test for *Connectivity, Throughput,* and *Voice* using the configurations provided while creating the test to link the three. Only *APs* and *SSIDs* within the baseline test is measured in subsequent tests. The tests that are run without a corresponding baseline displays the status as *No Baseline*.

Tests are measured against the below mentioned values for Voice.

- **Good**: Packet Loss = 0%, RTT <= 100ms
- **Fair**: Packet Loss < 2%, RTT <= 120ms
- **Bad**: Packet Loss > 2% or RTT > 120ms

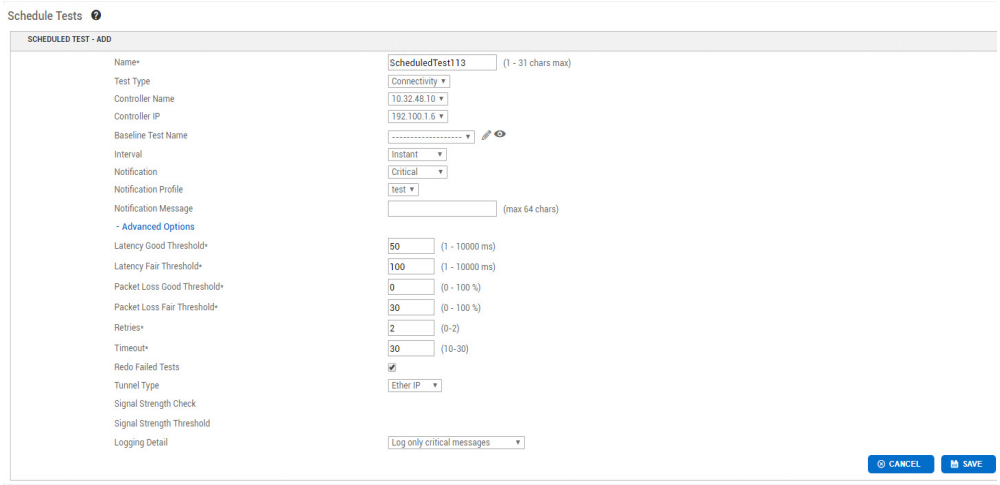
Add a Scheduled Test

You can configure many number of scheduled tests against a baseline test. You can either create a test, disable or enable it to activate immediately. Tests are scheduled on a regular interval and the test results are verified by viewing the results or by scheduling an email notification.

To add a *Scheduled Test,* follow these steps:

1. Navigate to *Configure* > *Tests* > *Scheduled Tests* > *Add Test*.
2. In the *Scheduled Test - Add* screen, provide the following details for the *Scheduled Test - Add.*

Figure 234: *Schedule Test - Add*



Field	Description
Name	Provide a name of the scheduled test primarily for usage. The name consists of up to 31 characters, including numbers, letters, capital letters, and special characters.

Field	Description

Test Type	Select the *Test Type* from the drop-down list. The options are as follows:
	• **Connectivity**:
	Connectivity describes if the station is connected to the AP. Connectivity can be verified by sending ping traffic (ICMP) run from one point to another.
	The selection of the *Test Type* as *Connectivity* determines the rest of the options on the page. Refer to *"Test Type - Connectivity"* ***on page 448***.
	• **Throughput**:
	Throughput is the amount of data moved successfully from one place to another in a given time period. The selection of the *Test Type* as *Throughput* determines the rest of the options on the page. The throughput test type can further be divided as follows:
	  • Throughput TCP (Transmission Control Protocol). Refer to *"Throughput - TCP"* ***on page 450***
	  • Throughput UDP (User Datagram Protocol). Refer to *"Throughput - UDP"* ***on page 452***
	• **Voice**:
	Voice is simulated using multiple thread of ping traffic.
	The selection of the *Test Type* as *Voice determines* the rest of the options on the page. Refer to *"Test Type - Voice"* ***on page 454***.
	The scheduled tests that run on the selected controller must match the test type in order to measure against the baseline.

Controller Name	Select the *Controller Name* or the *Host name* from the drop-down list. The controller name displayed is the controller mapped to the *FortiWLM* inventory; the test runs on the indicated controller.
Controller IP	Select the *Controller IP* address from the drop-down list. The controller IP address displayed is the controller mapped to the *FortiWLM* inventory; the test runs on the indicated controller.
Baseline Test Name	Select a *Baseline Test Name* from the drop-down list. This value links a baseline to this test. The test will be run only for the *IF ID/ESS Profile* listed in the baseline. You can modify the *IF ID/ESS Profile* named in the baseline by selecting *Edit icon* next to the drop-down list. **Note:** Only the baseline tests with *Completed* status is displayed.

Field	Description

Interval	Select an *Interval* type from the drop-down list. The following are the options:
	• **Instant**: This option enables to run the scheduled test once, immediately after it is saved. The tests with the *Instant* interval type gets displayed on the *Ongoing Tests* screen (*Monitor* > *Tests* > *Ongoing*). It does not get displayed on the *Schedule Tests* screen.
	• **Once**: This option enables to run the scheduled test immediately after it is saved. The following fields are displayed upon selection.
	  • **Status**: Select *Enabled or Disabled* from the drop-down list. The *Enabled* option (default) activates a test. The *Disabled* option does not run the test.
	  • **Start Time**: Select the *Start Time* from the *Calendar* in *mm/dd/yyyy* and *hh:mm:ss* format.
	• **Continuous**: This option enables to execute the scheduled test continuously till you disable the test. The following fields are displayed upon selection.
	  • **Status**: Select *Enabled or Disabled* from the drop-down list. The *Enabled* option (default) activates a test. The *Disabled* option does not run the test.
	• **Hourly**: This option enables to execute the scheduled test every hour at the time given *Start Time*. The following fields are displayed upon selection.
	  • **Status**: Select *Enabled or Disabled* from the drop-down list. The *Enabled* option (default) activates a test. The *Disabled* option does not run the test.
	  • **Start Time**: Select the *Start Time* from the *Calendar* in *mm/dd/yyyy* and *hh:mm:ss* format.
	• **Daily**: This option enables to execute the scheduled test every day at the given *Start Time*. The following fields are displayed upon selection.
	  • **Status**: Select *Enabled or Disabled* from the drop-down list. The *Enabled* option (default) activates a test. The *Disabled* option does not run the test.
	  • **Start Time**: Select the *Start Time* from the *Calendar* in *mm/dd/yyyy* and *hh:mm:ss* format.

Field	Description

	• **Weekly**: This option enables to execute the scheduled test every week as per the scheduled day and time of the week indicated in the *Start Time* field. The following fields are displayed upon selection.
	  • **Status**: Select *Enabled or Disabled* from the drop-down list. The *Enabled* option (default) activates a test. The *Disabled* option does not run the test.
	  • **Start Time**: Select the *Start Time* from the *Calendar* in *mm/dd/yyyy* and *hh:mm:ss* format.

Notification	Select the *Notification* from the drop-down list. This (*SAM* defined tests only) determines if anyone is to be emailed when one or more threshold violations are noticed in a test. The following are the types: • **None**: Never notify anyone. • **Critical**: Email only when the *Bad Threshold* value in a *Scheduled Test* is met or exceeded at least once. • **Major**: Email only when the *Good Threshold* value in a *Scheduled Test* falls below the setting at least once. • **Information**: Email irrespective of the results threshold.
Notification Profile	Select the *Notification Profile* from the drop-down list. The notification profiles are configured in the *Network Manager* application. (*Administration > User Preference > Notification Profiles*). Indicate a profile name here; all email addresses in the profile will be sent the *Notification Message Subject* as indicated.
Notification Message	Type a notification message (max 64 chars).
Advanced Options	Optional. Click the *Advanced Options*. The following information is displayed for the respective Test Type.

Field	Description
Test Type - Connectivity	
By selecting the *Test Type* as *Connectivity*, the following fields appear in the *Advanced Options*:	
Latency Good Threshold	Type a value for the *Latency Good Threshold*. The latency value is between 1 ms and 10000 ms. Latency recorded at or below this setting is considered to be good.
Latency Fair Threshold	Type a value for the *Latency Fair Threshold*. The latency value is between 1 ms and 10000 ms. Latency recorded at or below this setting is considered fair until latency crosses the threshold for good (set above). The latency above this number is marked as bad.
Packet Loss Good Threshold	Type a value for *Packet Loss Good Threshold*. This is a percentage below which a packet loss result is considered good. This number is the default threshold for all tests. If the baseline for a particular test displays a poorer number, that becomes the actual threshold for that test.
Packet Loss Bad Threshold	Type a value for *Packet Loss Bad Threshold*. This is a percentage above which a packet loss result is considered bad. This number is the default threshold for all tests. If the baseline for a particular test displays a poorer number, that becomes the actual threshold for that test. A number between the good and bad threshold is considered fair.
Retries	Type the number of *Retries*. This field allows you to configure the number of retries when SAM tests fail for an *ESS Profile*. The minimum value is 0 (zero) and the maximum value is 2 (two).
Timeout	Type the *Timeout* value. If the test takes longer than this (10 - 30 seconds), fail it.
Redo Failed Tests	Check the *Redo Failed Tests* option the tests get repeated for failed tests. If the value for *Timeout* (above) is exceeded, retry the test again until the value of *Retries* (above) is met.
Tunnel Type	Select the *Tunnel Type* from the drop-down list. The options are as follows: • **Ether IP**: This option is the default tunnel. Here the data packets are sent through the Ether IP tunnel, between the *FortiWLM* and AP. • **Ether UDP**: Here the data packets are sent through the Ether UDP tunnel, between the *FortiWLM* and AP.

Field	Description
Signal Strength Check	Displays the *Signal Strength Check*. The options are as follows: • **On**: The surroundings are examined for the presence or absence of the neighbor APs. If the neighbor AP is present, then the *Signal Strength Threshold* is examined. The S*ignal Strength Threshold* must be within (-85 to -30 dBM). The default value is -70dBM. • **Off**: The surroundings are not examined for the presence or absence of the neighbor APs.
Signal Strength Threshold	Displays the *Signal Strength Threshold*. This is displayed only when the *Signal Strength Check* option is *On*. The *Signal Strength Threshold* must be within (-85 to -30 dBM). The default value is -70dBM.
Logging Detail	Select the *Logging Detail* from the drop-down list. The options are as follows: • **Log only critical messages**: This option logs only the critical messages. • **Log all messages**: This option logs all the messages.

Field	Description
Throughput - TCP	
By selecting the *Test Type* as *Throughput-TCP*, the following fields appear in the *Advanced Options*:	
Throughput Good Threshold	Type a value for the *Throughput Good Threshold*. When the range (0 - 100%) is met or exceeded during a test, throughput is good and no counters are incremented. When throughput value falls below the range, but not below the value of the T*hroughput Fair Threshold* (see below) the throughput is considered to be fair and the counter for fair throughput is incremented for this test. For Example: Set the good throughput threshold at 20% and fair throughput threshold at 10%. In that case, any throughput from 10% to 20% is considered fair and anything above 20% is considered good. A bad throughput is anything below 10%.
Throughput Fair Threshold	Type a value for the *Throughput Fair Threshold*. When throughput is below the range, throughput is considered as bad and the counter for bad throughput is incremented for the test.
Retries	Type the number of *Retries*. This field allows you to configure the number of retries when SAM tests fail for an *ESS Profile*. The minimum value is 0 (zero) and the maximum value is 2 (two).
Timeout	Type the *Timeout* value. If the test takes longer than this (10 - 30 seconds), fail it.
Redo Failed Tests	Check the *Redo Failed Tests* option. If the value for *Timeout* (above) is exceeded, retry the test again until the value of *Retries* (above) is met.
Tunnel Type	Select the *Tunnel Type* from the drop-down list. The options are as follows: • **Ether IP**: This is the default tunnel. Here the data packets are sent through the Ether IP tunnel, between the *FortiWLM* and AP. • **Ether UDP**: Here the data packets are sent through the Ether UDP tunnel, between the *FortiWLM* and AP.
Signal Strength Check	Displays the *Signal Strength Check*. The options are as follows: • **On**: The surroundings are examined for the presence or absence of the neighbor APs. If the neighbor AP is present, then the Signal Strength Threshold is examined. The Signal Strength Threshold must be within (-85 to -30 dBM). The default value is -70dBM. • **Off**: The surroundings are not examined for the presence or absence of the neighbor APs.

Field	Description
Signal Strength Threshold	Displays the *Signal Strength Threshold*. This is displayed only when the *Signal Strength Check* option is *On*. The *Signal Strength Threshold* must be within (-85 to -30 dBm). The default value is -70dBM.
Ping test before Throughput	Select the *Ping test before Throughput* from the drop-down list. The options are as follows: • **On**: The ping is run before running the throughput test. The throughput tests are conducted based on the success of the ping. • **Off**: The ping is not run before the throughput test. This option is *On* by default. The throughput tests can still be run when the ICMP is blocked by turning the ping Off.
Logging Detail	Select the Logging Detail from the drop-down list. The options are as follows: • **Log only critical messages**: This option logs only the critical messages. • **Log all messages**: This option logs all the messages.

Field	Description
Throughput - UDP	
By selecting the *Test Type* as *Throughput - UDP*, the following fields appear in the *Advanced Options*:	
Throughput Good Threshold	Type a value for the *Throughput Good Threshold*. When the range (0 - 100%) is met or exceeded during a test, throughput is good and no counters are incremented. When throughput value falls below the range, but not below the value of the *Throughput Fair Threshold* (see below), the throughput is considered to be fair and the counter for fair throughput is incremented for this test. For Example: Set the good throughput threshold at 20% and fair throughput threshold at 10%. In that case, any throughput from 10% to 20% is considered fair and anything 20% or more is good. Bad throughput is anything below 10%.
Throughput Fair Threshold	Type a value for the *Throughput Fair Threshold*. When throughput is below the range, throughput is considered as bad and the counter for bad throughput is incremented for the test.
Retries	Type the number of *Retries*. This field allows you to configure the number of retries when SAM tests fail for an *ESS Profile*. The minimum value is 0 (zero) and the maximum value is 2 (two).
Timeout	Type the *Timeout* value. If the test takes longer than this (10 - 30 seconds), fail it.
Redo Failed Tests	Check the *Redo Failed Tests* option. If the value for *Timeout* (above) is exceeded, retry the test again until the value of Retries (above) is met.
Tunnel Type	Select the *Tunnel Type* from the drop-down list. The options are as follows: • **Ether IP**: This is the default tunnel. Here the data packets are sent through the Ether IP tunnel, between the *FortiWLM* box and AP. • **Ether UDP**: Here the data packets are sent through the Ether UDP tunnel, between the *FortiWLM* box and AP.
Signal Strength Check	Displays the *Signal Strength Check*. The options are as follows: • **On**: The surroundings are examined for the presence or absence of the neighbor APs. If the neighbor AP is present, then the Signal Strength Threshold is examined. The Signal Strength Threshold must be within (-85 to -30 dBm). The default value is -70dBM. • **Off**: The surroundings are not examined for the presence or absence of the neighbor APs.

Field	Description
Signal Strength Threshold	Displays the Signal Strength Threshold. This is displayed only when the Signal Strength Check option is **On**. The Signal Strength Threshold must be within (-85 to -30 dBm). The default value is -70dBM.
Ping test before Throughput	Select the *Ping test before Throughput* from the drop-down list. The options are as follows: • **On**: The ping is run before running the throughput test. The throughput tests are conducted based on the success of the ping. • **Off**: The ping is not run before the throughput test. This option is *On* by default. The throughput tests can still be run when the ICMP is blocked by turning the ping Off.
Logging Detail	Select the *Logging Detail* from the drop-down list. The options are as follows: • **Log only critical messages**: This option logs only the critical messages. • **Log all messages**: This option logs all the messages.

Field	Description
Test Type - Voice	
By selecting the *Test Type* as *Voice*, the following fields appear in the *Advanced Options*:	
Number of Calls	Type a value for the *Number of Calls* (1-100). **Note:** The *Number of Calls* option is disabled or non editable, as its values are taken from the selected baseline (only for viewing).
Retries	Type the number of *Retries*. If the test fails, try again this number of times (0 - 2).
Timeout	Type the *Timeout* value. If the test takes longer than this (10 - 30 seconds), fail it.
Redo Failed Tests	Check the *Redo Failed Tests* option. If the value for *Timeout* (above) is exceeded, retry the test again until the value of *Retries* (above) is met.
Tunnel Type	Select the *Tunnel Type* from the drop-down list. The options are as follows: • **Ether IP**: This is the default tunnel. Here the data packets are sent through the *Ether IP* tunnel, between the *FortiWLM* and AP. • **Ether UDP**: Here the data packets are sent through the Ether UDP tunnel, between the *FortiWLM* and AP.
Signal Strength Check	Displays the *Signal Strength Check*. The options are as follows: • **On**: The surroundings are examined for the presence or absence of the neighbor APs. If the neighbor AP is present, then the *Signal Strength Threshold* is examined. The *Signal Strength Threshold* must be within (-85 to -30 dBm). The default value is -70dBM. • **Off**: The surroundings are not examined for the presence or absence of the neighbor APs.
Signal Strength Threshold	Displays the *Signal Strength Threshold*. This is displayed only when the *Signal Strength Check* option is *On*. The *Signal Strength Threshold* must be within (-85 to -30 dBm). The default value is -70dBM.
Logging Detail	Select the *Logging Detail* from the drop-down list. The options are as follows: • **Log only critical messages**: This option logs only the critical messages. • **Log all messages**: This option logs all the messages.

3. Click **Save**. The test added is displayed on the *Completed Tests* of the *Monitor Dashboard*.

The test will run as indicated; multiple tests can run simultaneously for different controller IPs. SA2000 can run up to 14 overlapping tests and SA200 can run up to seven. If you look at the directions for a test, you'll see that the Interval can be set to Instant.

Modify a Test Criteria

To edit the criterion for a *Scheduled Test*, follow the below steps:

1. Navigate to *Configure* > *Tests* > *Scheduled Tests* > select a test > *Edit*.
2. In the *Scheduled Test - Edit* screen, perform the changes as required.
3. Select *Save*. The updated test is displayed on the *Scheduled Test* screen.

Enable a Test

To enable a scheduled test, follow these steps:

1. Navigate to *Configure* > *Tests* > *Scheduled Tests.*
2. Select one or more tests by clicking the radio button to activate the test.

Infrastructure

The security permissions (*User Name* and *Password*) for the RADIUS based WPA, WPA2, 802.1x, Mixed *ESS Profiles* and *Captive Portal* must be configured in *SAM*. The below procedure provides a brief description to configure security permissions for *SAM client* and *Captive Portal*.

SAM Clients

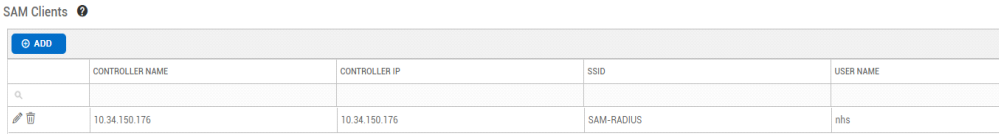
The security permissions (*User Name* and *Password*) for the RADIUS based WPA, WPA2, 802.1x, Mixed *ESS Profiles* must be configured.

Add Security Permission for SAM Clients

To add security permission for a *SAM* client, follow these steps:

1. Navigate to *Configure* > *Infrastructure* > *SAM Clients* > *Add option.*

Figure 235: *SAM Clients*



2. In the *Add SAM Client* pop-up, provide the following details:

Field	Description
Controller Name	Select the controller name that is associated to the *RADIUS Key* record.
Controller IP	Select the controller IP address that is associated to the *RADIUS Key* record.
SSID	Type the SSID that is associated to the WPA, WPA2, 802.1x, Mixed *ESS Profiles*.
User Name	Type a user name used by the SAM client on the selected SSID, for example Fortinet guest. The special character @ symbol is allowed for configuring the user name.
Password	Type the *Password* associated with the user identity.

3. Click *Save*. The client security is now configured.

Edit Security Permission for SAM Clients

To edit the security permission for a *SAM* client, follow the below steps:

1. Navigate to *Configure* > *Infrastructure* > *SAM Clients*.
2. Select a client security followed by selecting the *Edit* option.
3. In the *Edit SAM Client* pop-up, provide the following details:

Field	Description
Controller Name	Displays the controller name that is associated to the *RADIUS Key* record.
Controller IP	Displays the controller IP address that is associated to the *RADIUS Key* record.
SSID	Modify the SSID that is associated to the WPA, WPA2, 802.1x, Mixed *ESS Profiles*.
User Name	Modify the user name used by the SAM client on the selected SSID.
Password	Modify the *Password* associated with the user identity.

4. Click *Save*. The updated client security is now displayed on the *SAM Clients* screen.

Delete Security Permission for SAM Clients

To delete security permission for a *SAM* client, follow these steps:

1. Navigate to *Configure* > *Infrastructure* > *SAM Clients.*
2. Select a client security followed by selecting the *delete* icon. A conformation message is displayed to continue the deletion.
3. Select *OK* to proceed and *Cancel* to cancel the deletion.

Captive Portals

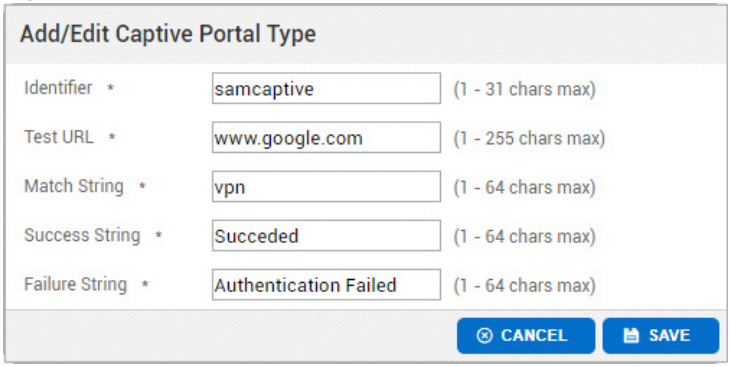
If you want to provide limited wireless access to a group of users, use *Captive Portal*. *Captive Portal* is a feature designed to isolate temporary users on a network. For example, guests in a company or students using a library. If *Captive Portal* is enabled, the *HTTP* protocol over *Secure Socket Layer* (SSL, also known as HTTPS) provides an encrypted login interchange with the RADIUS server until the user is authenticated and authorized. During this interchange, all traffic with the client station except *DHCP, ARP, and DNS* packets is dropped until access is granted. If access is not granted, the user is unable to leave the *Captive Portal* login page. If access is granted, the user is released from the *Captive Portal* page and is allowed to enter the *WLAN*.

The security for *SAM* virtual client must be configured, as it connects to the *Wireless LAN* and runs the connectivity and performance tests subsequently. This implies that the SSID identified consists of an enterprise-mode security profile involving RADIUS. The security for *SAM* virtual client is performed by configuring the *Captive Portal Users and Types* in the *SAM* web UI.

Add Captive Portal Types

1. Navigate to *Configure* > *Infrastructure* > *Captive Portals* > *Captive Portal Types* > *Add option.*

Figure 236: *Add/Edit Captive Portal Type*



2. In the *Add/Edit Captive Portal Type* pop-up, provide the following information:

Field	Description
Identifier	Provide the name for a given *Captive Portal.* Later, when you configure the *Captive Portal* users, use this same identifier. This links the I*dentification String, Success String & Failure String* to the users.
Test URL	Provide the web site that the client tries to access, For example: google.com
Match String	Provide a identification string from the *Captive Portal's* login form. For the *Fortinet Captive Portal*, the default value is (lowercase only) vpn.
Success String	Provide the string from the *Captive Portal's login* form success ID confirmation that appears on the page immediately following a successful login. For the *Fortinet Captive Portal*, the default value is Succeeded.
Failure String	Provide the confirmation that appears on the page immediately following an incorrect login. For the default *Fortinet Captive Portal*, the value is *Authentication Failed*.

3. Select *Save*. The new *Captive Portal* is included and is displayed on the *Captive Portals* screen.

Edit Captive Portal Types

To edit the security permission for a *SAM* client, follow the below steps:

1. Navigate to *Configure* > *Infrastructure* > *Captive Portals* > *Captive Portal Types.*
2. Select a captive portal type followed by selecting the *Edit* option.

3. In the *Add/Edit Captive Portal Type* pop-up, provide the following details:

Field	Description
Identifier	Displays the name for a given *Captive Portal.*
Test URL	Modify the web site that the client tries to access, For example: google.com
Match String	Modify the identification string from the *Captive Portal's* login form. For the *Fortinet Captive Portal*, the default value is (lowercase only) vpn.
Success String	Modify the string from the *Captive Portal's login* form success ID confirmation that appears on the page immediately following a successful login. For the *Fortinet Captive Portal*, the default value is Succeeded.
Failure String	Modify the confirmation that appears on the page immediately following an incorrect login. For the default *Fortinet Captive Portal*, the value is *Authentication Failed*.

4. Click *Save*. The updated captive portal type is now displayed on the *Captive Portals* screen.

Delete Captive Portal Types

To delete the captive portal types, follow these steps:

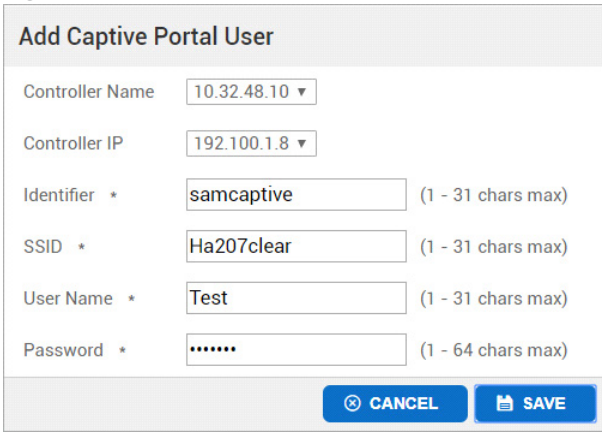
1. Navigate to *Configure > Infrastructure > Captive Portals > Captive Portal Types.*
2. Select a captive portal type followed by selecting the *delete* icon. A *conformation* message is displayed to continue the deletion.
3. Select *OK* to proceed and *Cancel* to cancel the deletion.

The identifier that is still in association with user or users cannot be deleted. The corresponding users must be deleted first.

Add Captive Portal Users

1. Navigate to *Configure > Infrastructure > Captive Portals > Captive Portal Users > Add option.*

Figure 237: *Add Captive Portal User*



2. In the *Add Captive Portal User* pop-up, provide the following information:

Field	Description
Controller Name	Select the Controller Name from the drop-down list.
Controller IP	Select the Controller IP from the drop-down list.
Identifier	Provide a Captive portal type to which this SSID is linked; use the same identifier that you used to configure the Captive Portal type (see above).
SSID	Provide a identification string from the *Captive Portal's* login form. For the *Fortinet Captive Portal*, the default value is (lowercase only) vpn.
User Name	Provide the string from the *Captive Portal's login* form success ID confirmation that appears on the page immediately following a successful login. For the *Fortinet Captive Portal*, the default value is Succeeded.
Password	Provide the confirmation that appears on the page immediately following an incorrect login. For the default *Fortinet Captive Portal*, the value is *Authentication Failed*.

3. Select *Save*. The new *Captive Portal User* is included.

Edit Captive Portal Users

To edit the security permission for a *SAM* client, follow the below steps:

1. Navigate to *Configure* > *Infrastructure* > *Captive Portals* > *Captive Portal Users.*
2. Select a captive portal users followed by selecting the *Edit* option.

3. In the *Edit Captive Portal User* pop-up, provide the following details:

Field	Description
Controller Name	Displays the *Controller Name*.
Controller IP	Displays the *Controller IP* address
Identifier	Modify the name for a given *Captive Portal.*
SSID	Modify the identification string from the *Captive Portal's* login form. For the *Fortinet Captive Portal*, the default value is (lowercase only) vpn.
User Name	Modify the string from the *Captive Portal's login* form success ID confirmation that appears on the page immediately following a successful login. For the *Fortinet Captive Portal*, the default value is Succeeded.
Password	Modify the confirmation that appears on the page immediately following an incorrect login. For the default *Fortinet Captive Portal*, the value is *Authentication Failed*.

4. Click *Save*. The updated captive portal user is now displayed on the *Captive Portals* screen.

Delete Captive Portal Users

To delete the captive portal types, follow these steps:

1. Navigate to *Configure* > *Infrastructure* > *Captive Portals* > *Captive Portal Users.*
2. Select a captive portal user followed by selecting the *delete* icon. A *conformation* message is displayed to continue the deletion.
3. Select *OK* to proceed and *Cancel* to cancel the deletion.

Get MACs

MAC filtering controls a user station's access to the WLAN by permitting or denying access based on specific MAC addresses. A MAC address is unique to each IEEE 802-compliant networking device. In 802.11 wireless networks, network access can be controlled by permitting or denying a specific station MAC address, assigned to its wireless NIC card, from attempting to access the WLAN.

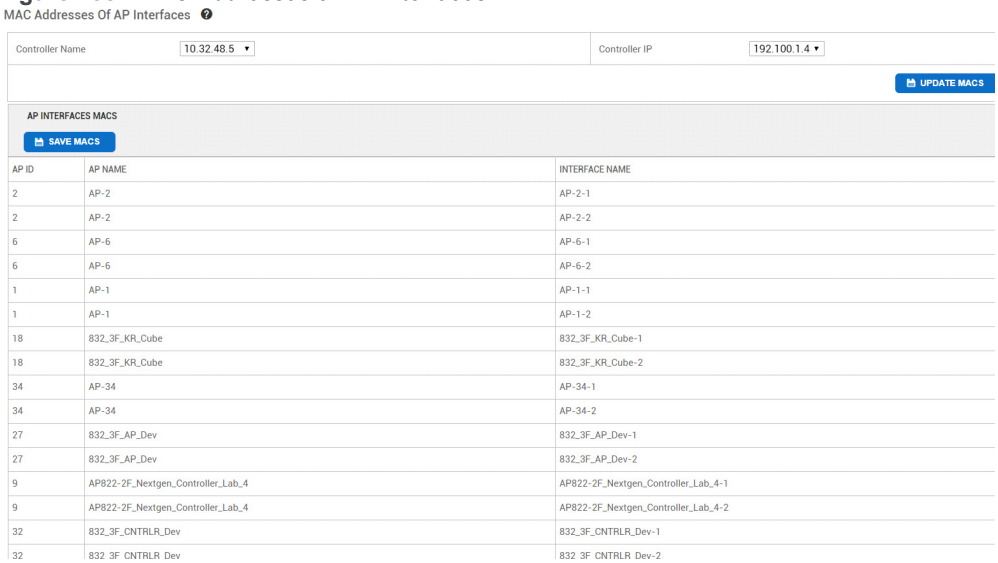
The *Get MACs* feature allows you to procure the virtual clients MAC addresses for the selected controller.

To find a controller's AP MAC addresses, follow these steps:

1. Navigate to *Configure* > *Infrastructure* > *Get MACs*.
2. In the MAC Addresses of AP Interfaces screen, select a *Controller Name/ Controller IP* address from the drop-down list and click one of the following buttons.

- **Show MACs**: A list of virtual *Client MAC* addresses for the selected controller is displayed.
  When you click the *Show MACs* for the first time, the server gathers all the client MAC addresses from each AP connected to the controller and stores the data. The time taken to display the MACs, depends on the number of APs connected to the controller. The next time you select that controller and click *Show MACs*, the list from the stored file appears quickly.
- **Update MACs**: This option refreshes the AP MAC list and provide the updated MAC list. Click *Update MACs* to procure the updated MAC list.
- **Save MACs**: The updated AP MAC addresses can be downloaded by selecting the *Save MACs* option. The MAC addresses list can also be uploaded to the selected controller to grant access or deny access for MAC filtering.

Figure 238: *MAC Addresses of AP Interfaces*



AP ID	AP NAME	INTERFACE NAME
2	AP-2	AP-2-1
2	AP-2	AP-2-2
6	AP-6	AP-6-1
6	AP-6	AP-6-2
1	AP-1	AP-1-1
1	AP-1	AP-1-2
18	832_3F_KR_Cube	832_3F_KR_Cube-1
18	832_3F_KR_Cube	832_3F_KR_Cube-2
34	AP-34	AP-34-1
34	AP-34	AP-34-2
27	832_3F_AP_Dev	832_3F_AP_Dev-1
27	832_3F_AP_Dev	832_3F_AP_Dev-2
9	AP822-2F_Nextgen_Controller_Lab_4	AP822-2F_Nextgen_Controller_Lab_4-1
9	AP822-2F_Nextgen_Controller_Lab_4	AP822-2F_Nextgen_Controller_Lab_4-2
32	832_3F_CNTRLR_Dev	832_3F_CNTRLR_Dev-1
32	832 3F CNTRLR Dev	832 3F CNTRLR Dev-2

Administering SAM

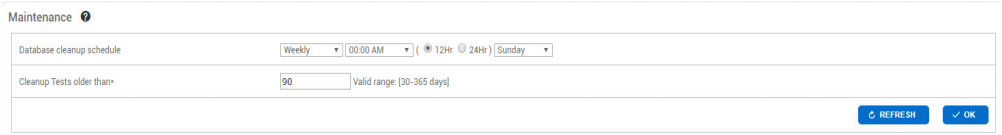
Maintenance

In *SAM* all the *Baseline* and *Scheduled* sweeps are configured to run continuously (once, instant, hourly, daily, and weekly sweeps). The results of the sweeps are stored in the database and may occupy enormous space. To prevent accumulation of older data, you can schedule a regular cleanup activity from the *Maintenance* page in *SAM*.

To access the *Maintenance* screen:

1. Navigate to *Administration* > *Maintenance*.

Figure 239: *Maintenance*



2. On the *Maintenance* screen, select the following fields:

- *Database cleanup schedule*: Select the database cleanup schedule from the drop-down list. Following are the options:
  - *No Schedule*: This is the default field. Here the database cleanup schedule is not configured.
  - *Daily*: The daily option allows you to select the time and time format (12 Hr or 24 Hr).
  - *Weekly*: The weekly option allows you to select,
    - the time from the drop-down list,
    - the time format (12 Hr or 24 Hr) and
    - the day of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday or Saturday) from the drop-down list.
- *Cleanup Tests older than*: This option allows you to enter the number of days. The data older than the number of days entered will be deleted.
- *For Example*: Enter the value as 30 in the *Cleanup Tests older* than the field. The data older than 30 days is deleted from the scheduled time. The valid range provided is [30-365 days].

3. Select *OK* to accept all the changes performed on the *Maintenance* screen.
4. Select *Refresh* to view the changes performed.

License Manager

The *Licensing* for the *Service Assurance Manager* is performed in the *FortiWLM.* The procedure for procuring and uploading the license is similar in all 3 products (*NM*, *SAM,* and *SM*). The licenses procured are displayed in the *License Usage Summary* section of *FortiWLM*.

License Usage Summary

The *License Usage Summary* section provides a graphical representation of the License usage for *EZRF-NM-VISUALIZE, EzRF-NM-BASE, and SAM*. The following varieties of graphs with different colors are represented:

- **License Consumed** - The number of licenses used. This is represented in yellow color.
- **Available licenses** - The number of licenses available which remains unused. This is represented in green color.
- **Unlicensed** - The number of licenses which are Unlicensed. This is represented in red color.

See *"FortiWLM Licensing"* ***on page 351***.

Although, the license for *SAM* is procured and uploaded in the *FortiWLM* application, the applying of the license is performed in *SAM*.

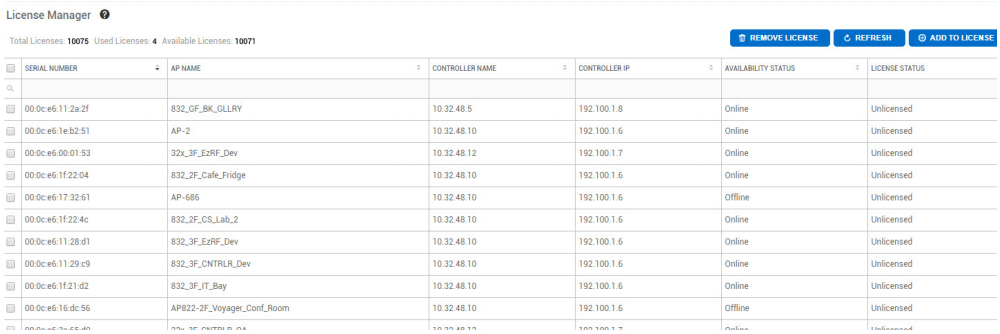
The *License Management* for *SAM* 2.0 installed on *FortiWLM* 3.0, is handled by *FortiWLM* 3.0. Uploading or validating the license is handled by the *FortiWLM*.

The *License Management* link will no more be available for *SAM* 2.0 when installed on the *FortiWLM* 3.0 and above.

Apply License

1. Navigate to *Administration* > *License Manager*.

Figure 240: *License Manager*



2. The *License Manager* screen displays the following details:
   - **Total Licenses**: Displays the total number of licenses allocated. This includes the sum of both *Used* and *Available* licenses.
   - **Used Licenses**: Displays the number of used licenses.
   - **Available Licenses**: Displays the number of available licenses.

3. It also displays a table of unlicensed APs, as listed below:

Field	Description
Serial Number	Displays the *MAC address* of the AP.
AP Name	Displays the *AP Name*.
Controller Name	Displays the *IP address* or the name of the controller.
Controller IP	Displays the *IP address* of the controller.
License	Displays the *License Status* of the controller. The following are the types: • Licensed • Unlicensed

4. The unlicensed APs can be licensed by following the below mentioned steps:
   - Select the unlicensed APs from the table by clicking the check box.
   - Select *Add to License* option. A confirmation message is displayed notifying that APs once added to the license can't be removed.
   - Select *OK* to proceed. The MAC addresses of the selected APs are added to the database.
   - Select *Refresh* option to view the changes performed.

Remove License

The *Remove License* option allows you to remove *offline APs* and *unknown APs* (APs that are not present in Inventory table) by following the below mentioned steps:

1. Select the unlicensed APs from the table by clicking the check boxes.
2. Select *Remove License* option.
3. A confirmation message is displayed notifying the removal of APs.
4. Select *OK* to proceed. The selected APs are deleted from the database.
5. Select *Refresh* option to view the changes performed.

Reporting SAM

In *Reports* page, one-time reports can be generated by following these steps:

1. Navigate to *Reports & Notify* > *Reports* > *Instant Reports*.
2. Select a *Report Type* from the drop-down list. The following are the types of report displayed in the list.
   - Tests Report
   - Trends Report

3. Select the *Controller Name* or the *Hostname* from the drop-down list. By selecting the *Controller Name*, the *Controller IP* is auto selected and vice versa.
4. Select the *Start Time*. The format followed is the *mm/dd/yyyy* and *hh:mm:ss* format. The time can be entered manually or by clicking the calendar icon.
   The calendar is displayed, where the date and time can manually be modified.
5. The *End Time* is automatically selected for the current date. To modify the *End Time* and *Date*, uncheck the *Now* option and enter manually. Else click the calendar icon. The calendar is displayed, where the date and time can manually be modified.
6. Click *Show Results* button.
7. A list of completed test, that falls in the selected time durations appears on the same screen with the fields as displayed in the below table:

The below mentioned fields are displayed only for the Report Type - Tests report.

For the Report Type - Trends Report, the Controller Name and the Controller IP are displayed.

Field	Description
Name	Displays the name of the report.
Type	Displays a test type.
Controller Name	Displays the name of the controller.
Start Time	Displays the start time of the test.
Controller IP	Displays the IP address of the controller.
Start Time	Displays the start time.
End Time	Displays the end time of the test.
Result	Displays the type of result. If *Good, Fair, Bad, Controller Offline, No Neighbors, Stopped or Config Retrieval Failed*.
Good	Displays the number of *Good* test type of result. If the number of tests with fair and bad results is zero, then a test is *Good*.
Fair	Displays the number of *Fair* test type of result. If no test has a bad result and at least one test has a fair result, then a test is fair.
Bad	Displays the number of Bad test type of result. If there is at least one test with a bad result, then a test is bad.
Controller Offline	Displays the number of controller offline type of result. If the server is unable to reach the controller while starting a test, the controller offline message is displayed in the results section.

Field	Description
No Neighbors	Displays the number of no neighbors type of result. If there are *No APs* or if all the APs in the controller looks offline or not reachable, then the no neighbors message is displayed in the results section.
Stopped	Displays the number of *Stopped* types of result. If you stop a running test, the output is displayed as *Stopped*. Clicking on this will display the test details of the percentage completed.
Config retrieval failed	Displays the number of config retrieval failed type of result. If, for some reason the test starts and we are unable to retrieve any configuration, the config retrieval failed is displayed in the results section.

8. To generate a report, select a test and click on the *Generate Report* button.
9. Multiple tests can be selected and reports can be generated. The Report is generated and can be saved in the following formats.

Name of the Format	Icon	Explanation
Save HTML Report		Click the *HTML* icon to export and save the report to *HTML* format.
Save Pdf Report		Click the *Pdf* icon to export and save the report to *Pdf* format.
Save Excel Report		Click the *Excel* icon to export and save the report to *Excel* format.

10. The report can also be emailed by clicking the  Icon and notification profile.
11. Click the  Icon to print the report.

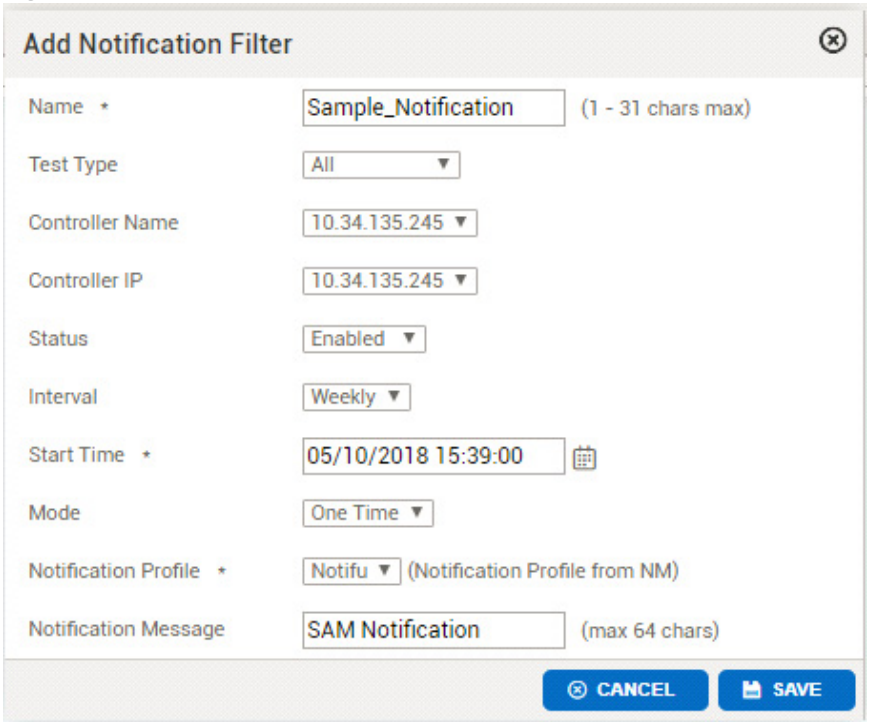
Notification

Add a Notification Filter in SAM

A notification filter defines the conditions that trigger an email. When you create a notification filter you also name a notification profile. When the notification filter is triggered, it sends a message to the list of recipients in the notification profile. Configure a notification filter in SAM by following these steps:

1. Navigate to *Reports & Notify* > *Notify* > *Notification* > *Add*.

Figure 241: *Add Notification Filter*



2. In *Add Notification Filter* screen, provide the following information as mentioned in the below table:

Field	Explanation
Name	Provide the test name. The test name can be from 1 - 31 characters long, including letters, numbers, and special characters.
Test Type	Select the test type from the drop-down list. This field is either *All, Throughput, Connectivity or Voice.*
Controller Name	Select controller name from the drop-down list. The list includes all the controller names mapped to the *FortiWLM* inventory.
Controller IP	Select controller IP from the drop-down list. The list includes all the controller names mapped to the *FortiWLM* inventory.
Status	*Enabled* is the default option. Select *Disable* to deactivate this filter; then it will not monitor the controller.

Field	Explanation
Interval	Select the time Interval. The interval options is *Daily* and *Weekly*.
Start Time	Select the *Start Time*. The format followed is the *mm/dd/yyyy* and *hh:mm:ss* format. The time can be entered manually or by clicking the calendar icon. The calendar is displayed, where the date and time can manually be modified.
Mode	Select the notification mode from the drop-down list. The notification mode determines how many times the message is sent to the email recipients listed in the profile. The options are as follows: • **One Time**: This option enables you to send the email once when the trigger incident occurs and then delete the entry from the notification list. • **Recurring**: This option enables you to keep sending emails at the configured date and time every week, until the profile is disabled.
Notification Profile	Select the notification profile from the drop-down list. Notification profiles display a list of emails configured in the *FortiWLM* application. Indicate a profile here; all email addresses in the profile will be sent the *Notification Message* indicated below.
Notification Message	Provide a subject or notification message up to 64 characters long.

3. Click *Save*.
4. The *Notification Filter* is added and displayed on the *Notification Filters* screen.

Edit Notification Filters

Edit a Notification Filter by following these steps:

1. Navigate to *Reports & Notify* > *Notify* > *Notification*.
2. Select a notification filter and click the *Edit* icon that corresponds to the filter.
3. Modify the fields.
4. Click *Save*.

Delete Notification Filters

Delete a Notification Filter by following these steps:

1. Navigate to *Reports & Notify* > *Notify* > *Notification*.

2. Select a notification filter and click the *Delete* icon that corresponds to the filter. A confirmation message for deletion is displayed.
3. Click *OK*.
4. Click *Refresh*. The filter is removed from the drop-down list.

5 Wireless Intrusions Prevention System (WIPS)

Fortinet's WIPS provides complete wireless threat detection and mitigation into the wireless network infrastructure. It detects wireless intrusions using predefined and custom signatures on an integrated platform with other WLAN management applications.

While creating the *AP Packet Capture* profile, the following are mandatory parameter values to be configured for WIPS.

- **Destination**: L3 mode
- **UDP Port**: 9178
- **IP Address**: Specify the controller or FortiWLM IP address, wherever WIPS is enabled.

Note: Fortinet recommends to configure the AP in **ScanRogues** Mode (*Configure > Wireless > Radio*).

Signatures

Signatures detect attacks on the wireless infrastructure by analyzing the wireless packets flowing in the network. There are 20 predefined signatures in WIPS; you can use these 20 signatures as written or you can reconfigure them. You can also create custom signatures, which are called rules. This chapter contains instructions for configuring rules.

Predefined Signatures

To see the WIPS predefined signatures, follow these steps:

Click *Configure* > *Predefined Signatures*.

Enable or disable signatures by clicking the respective check boxes. Here is a short description of each signature

- Adhoc Network: Adhoc networks are peer-to-peer networks between wireless computers that cause a security hole by providing an unintended bridge into the corporate network thereby compromising the critical corporate data.
- Antistumbler: The netstumbler is a wireless scanning utility that allows the detection and configuration of wireless LANs by sending out periodic probe requests and could open up

the network to other attacks. It raises an alert if the number of probe requests sent by a station crosses the configured count within the expiration timeout.

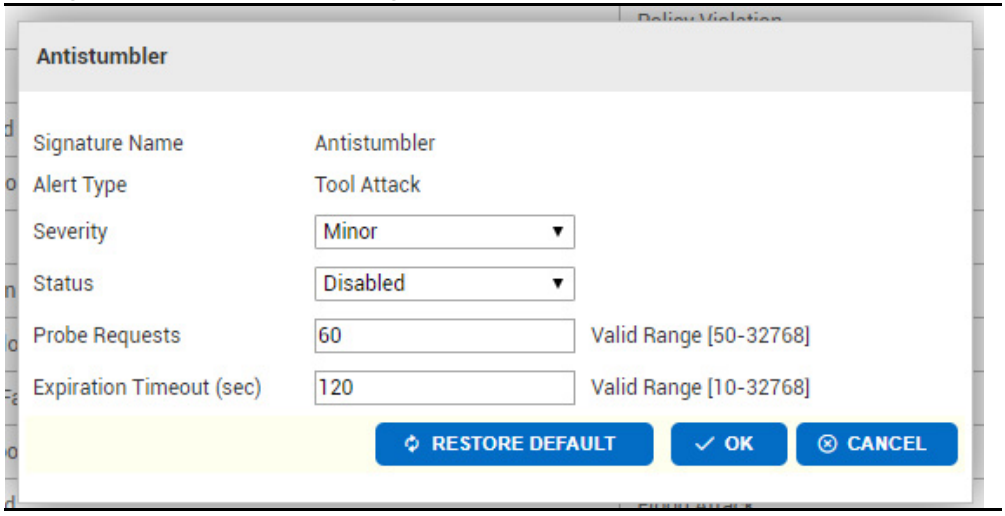
- Association Flood: A flood of Association requests from malicious stations to APs use up the internal resources of APs thus causing a Denial of Service attack on APs.
- Authentication Flood: A flood of Authentication requests from malicious stations to APs use up the internal resources of APs thus causing a Denial of Service attack on APs.
- Channel Hogger: A single station hogs the channel for too long a time and doesn't allow other stations to use the channel.
- De-authentication Flood: A flood of De-authentication requests from malicious stations to APs use up the internal resources of APs thus causing a Denial of Service attack on APs.
- Disassociation Flood: A flood of Disassociation requests from malicious stations to APs use up internal resources of APs, causing a Denial of Service attack on APs.
- EAP Handshake Failure: Attempts by hackers to crack EAP authentication passwords by doing a dictionary or brute force attack
- EAPoL Logoff Flood: A flood of EAPoL Logoff requests from malicious stations to APs use up the internal resources of APs, causing a Denial of Service attack on APs.
- EAPoL Start Flood: A flood of EAPoL Start requests from malicious stations to APs use up the internal resources of APs, causing a Denial of Service attack on APs.
- Fake AP: Fake AP tool can generate beacons with varying MAC address, SSID, channel number and transmission power for every packet, thus causing stations confusion because there are many spoofed APs in the network.
- Fragmentation and Re-Assembly: Malicious stations deliberately send fragments so that APs resources and processing capacity can be exhausted in reassembly. This constitutes a Denial of Service attack on APs. The following are the parameters which are considered for this signature.
- Large Duration ID: A station can specify large duration values in the frames it transmits and use up the medium continuously for transmission thereby denying access to other stations.
- MAC Spoof: A wireless station or AP may spoof the MAC address of a valid station or a valid AP thus causing man-in-the-middle attacks and compromising the wireless network.
- Null Probe Response: Denial of Service attack carried out by sending many probe packets with NULL SSIDs.
- Overutilized AP: AP sends too many authentication responses that fill up its internal tables thereby resulting in a Denial of Service attack.
- PRGA: WEP networks are vulnerable to arbitrary packet injection attacks using Pseudo Random Generation Algorithm (PRGA) determination techniques. An attacker that observes the WEP challenge/ response exchange can XOR the contents of the challenge and the response together to generate 128-bytes of PRGA thus compromising the wireless network.
- Rogue AP: A malicious AP masquerading as a valid AP causes stations to associate with itself thereby compromising the wireless network.

- Too Big SSID: Denial of Service attack carried out by sending many probe packets with very large SSID.
- Unregulated Channel: Wireless devices configured to use channels that are not regulated for use in a particular geographic domain cause interference to other radio systems.

Reconfiguring Predefined Signatures

You can edit some parameters of the default signatures by following these steps:

1. Click *Configure* > *Predefined Signatures*.
2. Either select the check box corresponding to a signature and click **Edit** or click the settings icon near the corresponding check box.



As shown above, the signature table shows these parameters of all the signatures:

- Signature: The name of the signature. (not editable)
- Alert Type: The alert type into which the signature is categorized. (not editable)
- Severity: The severity of the signature, Critical, Major or Minor (editable)
- Status: Either Enabled or Disabled (editable). When a signature is disabled, no alerts are raised if an attack matches that particular signature.

Change any of the editable parameters listed in the following signatures:

Signature	What can be changed
Adhoc Network	Severity, Status
Antistumbler	Severity, Status Probe Requests: Maximum number of probe requests a station can send Expiration Timeout: Time period used to keep count of probe requests from a particular station
Association Flood/Authentication Flood/De-authentication Flood/ Disassociation Flood/ EAPoL Logoff Flood/EAPoL Start Flood	Severity, Status Threshold**:** Maximum number of requests a station can send Expiration Timeout: Time period used to keep count of respective requests from a particular station
Channel Hogger	Severity, Status Maximum Duration: The maximum duration for which a station can use a channel within the expiration timeout. Expiration Timeout: Expiration timeout for the maximum duration.
EAP Handshake Failure	Severity, Status **Threshold Count:** Number of handshake failures allowed by administrator Threshold Period: Threshold period for handshake failures' count
Fake AP	Severity, Status
Fragmentation and Re-Assembly	Severity, Status Minimum Fragment Size: Minimum size with which a station can send a data packet Small Fragment Threshold: Maximum number of packets a station can send with size less than Minimum Fragment Size within the expiration timeout More Fragment Threshold: Number of data packets a station can send with the More Fragment bit set to 1 Expiration Timeout: Time ut period for the above parameters

Signature	What can be changed
Large Duration ID	Severity, Status Maximum Duration: Maximum value of the duration ID field with which a station can send a packet
MAC Spoof	Severity, Status Threshold: Number of abnormal sequence number gaps during time delta period used to keep count of abnormal sequence number gap Tolerate Gap: Sequence number gap allowed between two consecutive frames issued from same MAC address Expiration Timeout: Time period used to keep count of abnormal sequence number gaps. The range for this field is [2, 4294967295]. The time is in seconds.
Null Probe Response	Severity, Status
Overutilized AP	Severity, Status Threshold: Maximum number of authentication responses an AP can send within the expiration timeout Expiration Timeout: Timeout period for the threshold
PRGA	Severity, Status Threshold: Number of packets with the same IV that a station can send Expiration Timeout: Time period within which a crossed threshold raises an alert
Rogue AP	Severity, Status Expiration Timeout: A malicious AP sending at least two beacons within the expiration timeout results in a Rogue AP alert.
Long SSID	Severity, Status Max SSID Length: If the length of the SSID crosses the configured Max SSID length parameter, an alert is raised.
Unregulated Channel	Severity, Status Allowed Channels: List of allowed channels in which a valid station is allowed to send a packet

3. Click **OK**.

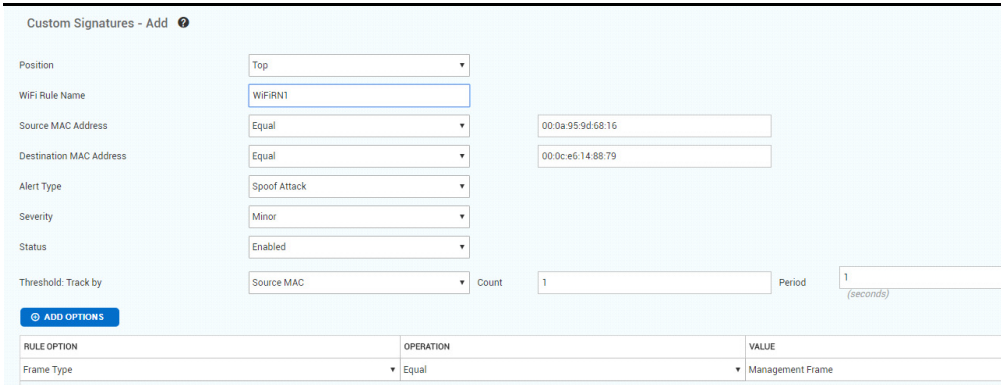
Custom Signatures

A Rule is a dynamic signature to detect wireless attacks by analyzing the packets. You can add any number of rules to WIPS. The packets will be matched against each rule (same as signatures) and if there is a match, then an alert is raised for that rule and the remaining rules are skipped.

Add a Custom Signature

To add a custom signature, follow these steps:

1. Click *Configure* > *Custom Signatures*.



2. Click **Add**.
3. From the Position drop-down list, select the position where the rule needs to be added in the priority list:
   - Top
   - Bottom
   - Above the Selected Rule (when Add rule is clicked with a rule selected.)
   - Below the Selected Rule (when Add rule is clicked with a rule selected.)
4. In the WiFi Rule Name text box, type the name that will be displayed when an alert for this rule is raised.
5. In the Source MAC address, enter a valid MAC address. Wireless packets from this MAC address will be checked by this rule. You can also enter any for the rule to check wireless packets from any MAC address.
6. In the Destination MAC address, enter a valid MAC address. Wireless packets to this MAC address will be checked by this rule. You can also enter any for the rule to check wireless packets to any MAC address.
7. In the Alert Type drop-down list, select any of the following options:

- Spoof Attack
- Misconfig Packet Attack
- Dictionary Attack
- Flood Attack
- Tool Attack
- Rogue Attack
- Man in Middle Attack
- Policy Violation

8. In the Severity drop-down list, select Minor / Major / Critical.
9. From the Status drop-down list, select:
   - Disabled: to disable the rule
   - Enabled: to enable the rule
10. The Threshold option has the following additional parameters that must be configured.
    - Track by: Select one of the two options
    - Source MAC: The packets are tracked by the source MAC address.
    - Destination MAC: The packets are tracked by the destination MAC address.
    - Count: The maximum number of times the event is allowed within a specified time interval before raising alert for this event.
    - Period: The time duration is the time interval used to count the number of occurrences of a particular event. The time is in seconds.
11. Optionally, click **Add Options**. Select Frame Type from the drop-down list, select Equal or Not Equal for Operation, and select one of these values:
    - Management Frame
    - Control Frame
    - Data Frame
12. Optionally, click **Add Options**. Select Frame Sub-type from the drop-down list, select Equal or Not Equal for Operation, and select one of these values:
    - Association Request
    - Association Response
    - Reassociation Request
    - Reassociation Response
    - Probe Request
    - Probe Response
    - Beacon
    - Announcement Traffic Indication Message(ATIM)

- Disassociation
- Authentication
- Deauthentication
- Power Save(PS)-Poll
- Request To Send(RTS)
- Clear To Send(CTS)
- Acknowledgement(ACK)
- Contention-Free(CF)-End
- CF-End + CF-Ack
- Data
- Data + CF-Ack
- Data + CF-Poll
- Data + CF-Ack + CF-Poll
- Null Function (no data)
- CF-Ack (no data)
- CF-Poll (no data)
- CF-Ack + CF-Poll (no data):
- QoS Data
- QoS Data + CF-Ack
- QoS Data + CF-Poll
- QoS Data + CF-Ack + CF-Poll
- QoS Null
- QoS CF-Poll (no data)
- QoS CF-Ack + CF-Poll (no data)

13. Optionally, click **Add Options**. Select EAPoL Type from the drop-down list, select Equal or Not Equal for Operation, and select one of these values:
    - EAPoL Packet
    - EAPoL Start
    - EAPoL Logoff
    - EAPoL Key
    - EAPoL ASF Alert
14. Optionally, click **Add Options**, select Duration from the drop-down list, select Equal or Not Equal for Operation, and then enter the Duration time for the rule, with minimum and maximum values 0 and 32768 seconds.

15. Optionally, click **Add Options**, select Address4 from the drop-down list, and then enter a valid transmit MAC address. Note that two bytes are used for the frame control field, followed by two bytes for the duration/ID field. Address 1 is the destination address; address 2 is the source address. Address 3 is the BSSID of the network. The Sequence Control field uses two bytes to accommodate fragmentation and packet reassembly. Address 4 is optional, used only in a wireless distribution system (WDS) to indicate the transmitter address.
16. Optionally, click **Add Options**, select BSSID from the drop-down list, select Equal or Not Equal for Operation, and then enter a valid MAC address for a BSSID.
17. Optionally, click **Add Options**, select Fragment Number from the drop-down list, select Equal or Not Equal for Operation, and then enter a valid Fragment Number, 0 or 1.
18. Optionally, click **Add Options**, select Frame Control from the drop-down list, select Equal or Not Equal for Operation, and then enter a valid Fragment Number; minimum and maximum values are 0 and 65535.
19. Optionally, click **Add Options**, select WEP Bit from the drop-down list, and then select On or Off. If On, packets with WEP bit set will match this rule option and if Off, packets with WEP bit not set will match this rule option.
20. Optionally, click **Add Options**, select From AP Bit from the drop-down list, and then select the value On or Off. If On, packets with the From DS bit set will be compared to this rule. If Off, packets with the From DS bit not set will be compared to this rule.
21. Optionally, click **Add Options**, select To AP Bit from the drop-down list, and then select the value On or Off. If On, packets with the To DS bit set will be compared to this rule. If Off, packets with the To DS bit not set will be compared to this rule.
22. Optionally, click **Add Options**, select More Data Bit from the drop-down list, and then select the value On or Off. If On, packets with the More Data bit set will be compared to this rule. If Off, packets with the More Data bit set will not be compared to this rule.
23. Optionally, click **Add Options**, select More Fragments from the drop-down list, and then select the value On or Off. If On, packets with the More Fragments bit set will be compared to this rule. If Off, packets with the More Fragments bit set will not be compared to this rule.
24. Optionally, click **Add Options**, select Order Bit from the drop-down list, and then select the value On or Off. If On, packets with the Order bit set will be compared to this rule. If Off, packets with the Order bit set will not be compared to this rule.
25. Optionally, click **Add Options**, select Power Management Bit from the drop-down list, and then select the value On or Off. If On, packets with the Power Management bit set will be compared to this rule. If Off, packets with the Power Management bit set will not be compared to this rule.
26. Optionally, click **Add Options**, select Retry Bit from the drop-down list, and then select the value On or Off. If On, packets with the Retry bit set will be compared to this rule. If Off, packets with the Retry bit set will not be compared to this rule.
27. Optionally, click **Add Options**, select Sequence Number from the drop-down list, and provide a Sequence Number: The minimum and maximum value is 0 and 4095.

28. Optionally, click **Add Options**, select SSID, and enter an SSID for the value where SSID is a alphanumeric string.
29. Optionally, click **Add Options**, and select Max SSID Length, and then enter the length of the SSID for a value.
30. Optionally, click **Add Options**, select Allowed Channels, select equal or not equal, and then enter the allowed channels for this particular region separated by spaces.
31. Optionally, click **Add Options**, select EAP Code, select equal or not equal, and then enter an EAP code for a value.
32. Optionally, click **Add Options**, and select Protected Flag, and then select the value On or Off.
33. Click OK.

Edit or Delete a Custom Signature

To edit a rule, follow these steps:

1. Click *Configure* > *Custom Signatures.*
2. To edit a rule, click on the checkbox against the rule to select it and click **Edit**.
3. To delete a rule, click on the checkbox against the rule to select it and click on **Delete**.
4. Click **Save** for the configuration changes to take effect.

Viewing WIPS Alerts

There are two ways to look at alerts; you can look at charts of alert trends on the Dashboard or you can look at lists of actual alerts on the Alerts page.

Look at Trend Graphs

Monitor Trend Graphs from the dashboard (WIPS > Monitor > Dashboard). The Alerts Trend Graph shows trend lines for Critical/Major/Minor Alerts for the selected Start/End Time interval.

The Trend Graph Title bar also shows allows you to display all three trends utilizing the same scale by clicking Show Relative Trend; by default, this function is disabled as by the nature of wireless networks, there will typically be far more Minor and Major alerts, rendering the Critical chart less useful when viewed on the same scale.

More Graph Information

Tool tips and Show Details provide more information. Click any point in a graph or its corresponding legend to open a pop-up window that provides additional detail.

Look at Pie Charts

Monitor pie charts from the dashboard (WIPS > Monitor > Dashboard). Several charts are provided, allowing you to view alerts filtered by multiple different criteria. For all charts except

Alerts by Severity, the largest pie segments are displayed at the top of the chart to allow you to identify regions or devices with the most issues.

More Graph Information

Tool tips and Show Details provide more information. Click any point in a graph or its corresponding legend to open a pop-up window that provides additional detail.

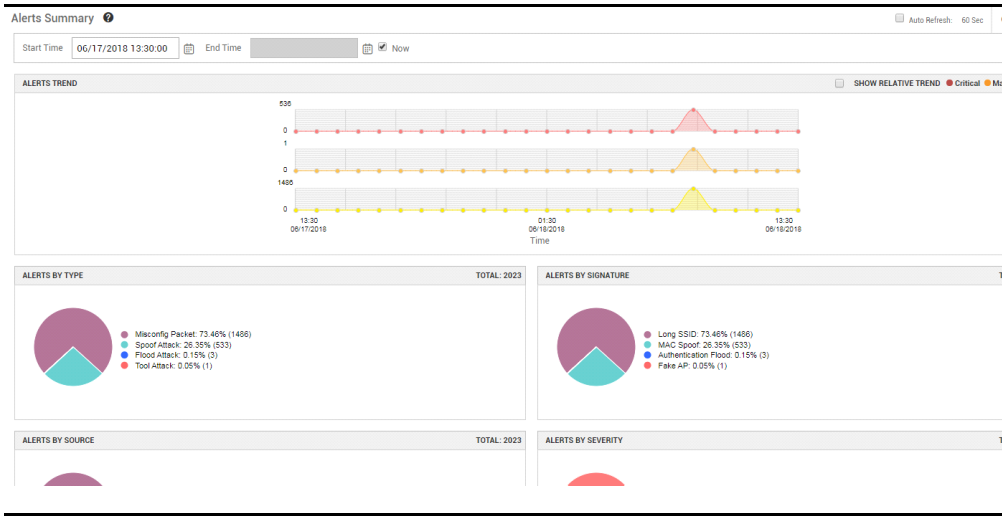
Look at Alerts

Select a Start/End Time interval to search for alerts during that interval. Double click a row to see details about that alert. Double click an alert row to see detail. Mark the alert as read/unread from the detail window. If you are seeing an unreasonably high number of alerts, be sure that packet truncation length is set to zero; partial packets cause false positives.

Alert Charts on the Dashboard

The dashboard provides information about the alerts raised in the WIPS database. The dashboard consists of five graphs - a trend graph and four pie charts that display alerts categorized by alert type, alert source, alert signature, and alert severity.

Display the dashboard by clicking *Monitor* > *Dashboard*.



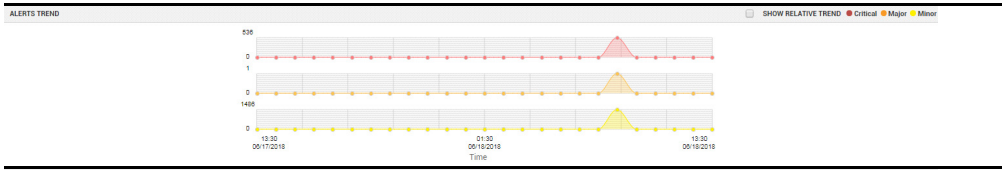
The dashboard can be plotted for a maximum of 30 days. To look at the alerts over a specific period of time, enter the relevant times for Start Time and End Time, and then click Show Trend. To look at the alerts from a specific start time to the current time, click Now instead of providing a time. When you click Show Trend, the Start Time and the End Times are rounded

to the nearest hours in such a way that the interval covers both the specified start and end times. This refreshes all five graphs.

What Do the Charts Mean?

Alerts Trend Graph

The top graph - Alerts Trend - displays the critical, major and minor alerts raised over the specified period of time.



The Alerts Trend graph actually consists of three different graphs that provide a quick glance at each alert severity level: Critical (red), Major (orange), and Minor (yellow). The graphs are divided into intervals of one hour each. The Start and End point of the graph correspond to the Start and End Time you specify. Move the mouse anywhere on the trend graph to see the legend and the alerts raised in that interval.

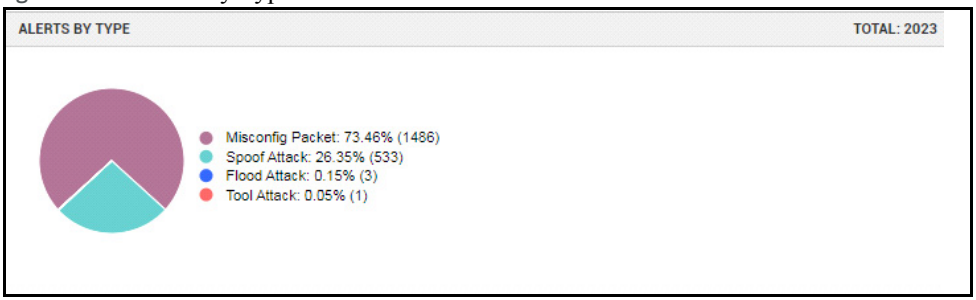
To see more alert details, click anywhere in the interval to display up a popup window with the following details of all alerts in that interval:

Column Name	Description
Date/Time	Date and time the alert was raised
Signature Name	Signature for which the alert was detected
Alert Type	The type of alert detected
Severity	Severity of the alert
AP Name	Name of the AP that sniffed the packet
AP IP	IP address of the AP that sniffed the packet
Channel	Channel on which the packet was sniffed
Source	MAC Address of the sender
Destination	MAC Address of the intended recipient

Alerts by Type Graph

The alert type gives various signature classes for which alerts have been raised in that particular interval.

Figure 242: Alerts by Type



Mouse over any slice from the chart to highlight that segment and its corresponding portion of the legend. The legend alongside the graph indicates the type.

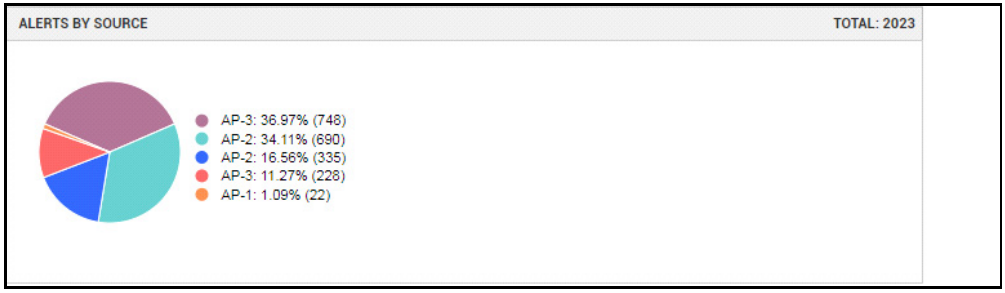
To see more alert details, click anywhere in the chart (or in the legend) to display up a popup window with the following details of all alerts in that interval:

Column Name	Description
Date/Time	Date and time the alert was raised
Signature Name	Signature for which the alert was detected
Alert Type	The type of alert detected
Severity	Severity of the alert
AP Name	Name of the AP that sniffed the packet
AP IP	IP address of the AP that sniffed the packet
Channel	Channel on which the packet was sniffed
Source	MAC Address of the sender
Destination	MAC Address of the intended recipient

Alerts by Source Graph

An alert source is an AP that sniffed packets for an alert.

Figure 243: Alerts by Source



The first nine segments of the Alerts by Source graph indicate the top nine AP sources in decreasing order from most packets found. The last slice is a consolidated list of all remaining sources. The legend alongside the graph indicates the sources.

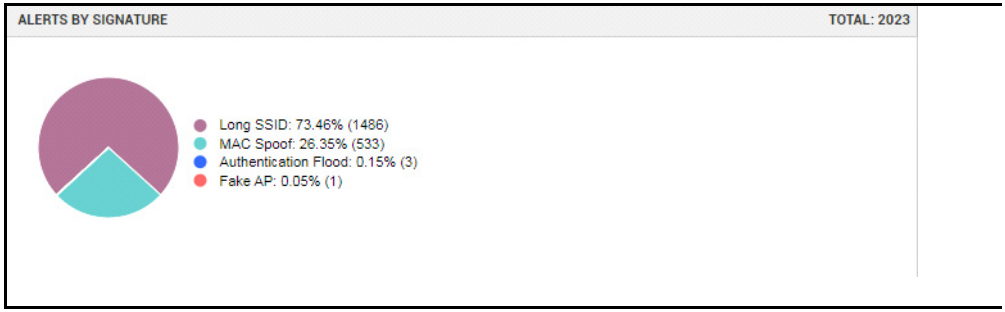
To see more alert details, click anywhere in the chart (or legend) to display up a popup window with the following details of all alerts in that interval:

Column Name	Description
Date/Time	Date and time the alert was raised
Signature Name	Signature for which the alert was detected
Alert Type	The type of alert detected
Severity	Severity of the alert
AP Name	Name of the AP that sniffed the packet
AP IP	IP address of the AP that sniffed the packet
Channel	Channel on which the packet was sniffed
Source	MAC Address of the sender
Destination	MAC Address of the intended recipient

Alerts by Signature Graph

An alert signature is a specific configuration designed to detect an intrusion or attack.

Figure 244: Alerts by Signature



The first nine segments of the Alerts by Signature graph indicate the top nine signature types in decreasing order from most packets found. The last slice is a consolidated list of all remaining signatures. The legend alongside the graph indicates the sources.

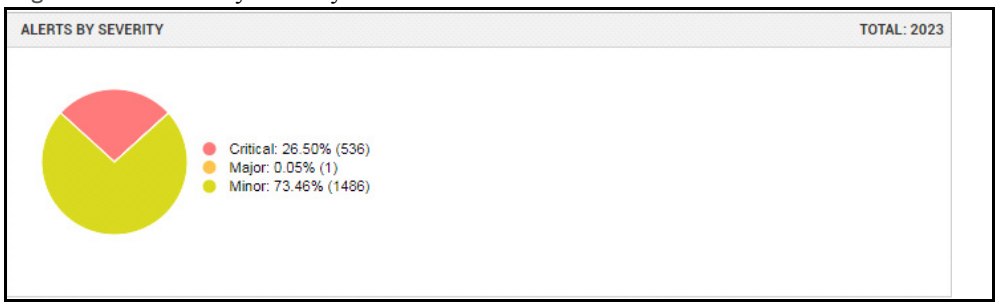
To see more alert details, click anywhere in the chart (or legend) to display up a popup window with the following details of all alerts in that interval:

Column Name	Description
Date/Time	Date and time the alert was raised
Signature Name	Signature for which the alert was detected
Alert Type	The type of alert detected
Severity	Severity of the alert
AP Name	Name of the AP that sniffed the packet
AP IP	IP address of the AP that sniffed the packet
Channel	Channel on which the packet was sniffed
Source	MAC Address of the sender
Destination	MAC Address of the intended recipient

Alerts by Severity Graph

The three severity levels are color-coded for easy reference: Critical (red), Major (orange), and Minor (yellow).

Figure 245: Alerts by Severity



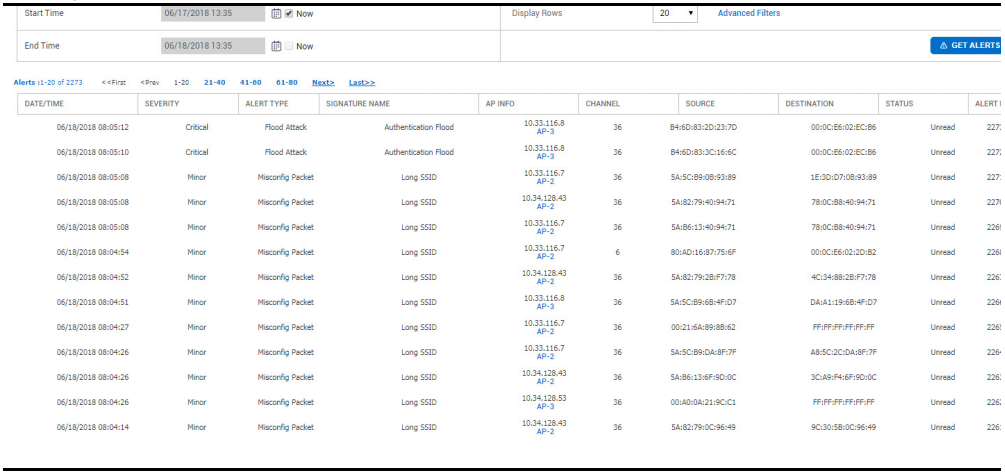
Since critical alerts are considered the most pressing, the red pie slice is always located towards the top of the chart. The legend alongside the graph indicates the number of each type detected.

To see more alert details, click anywhere in the chart (or legend) to display up a popup window with the following details of all alerts in that interval:

Column Name	Description
Date/Time	Date and time the alert was raised
Signature Name	Signature for which the alert was detected
Alert Type	The type of alert detected
Severity	Severity of the alert
AP Name	Name of the AP that sniffed the packet
AP IP	IP address of the AP that sniffed the packet
Channel	Channel on which the packet was sniffed
Source	MAC Address of the sender
Destination	MAC Address of the intended recipient

Alerts Page

To see a list of alerts, click *Monitor* > *Alerts*. The list of alerts can be updated at any time by clicking the *Get Alerts* button.



Configure More Chart Filters

To set more filters on which WIPS alerts are displayed, follow these steps:

1. Click *Monitor* > *Alerts* > *Advanced Filters* > *Add Filter*.
2. Select any Filter ID from the drop down menu.
3. Enter the Filter Value by either choosing from the drop down menu if it is available or by entering the value.
4. Click *Done*.
5. Click *Get Alerts*.

Remove Chart Filters

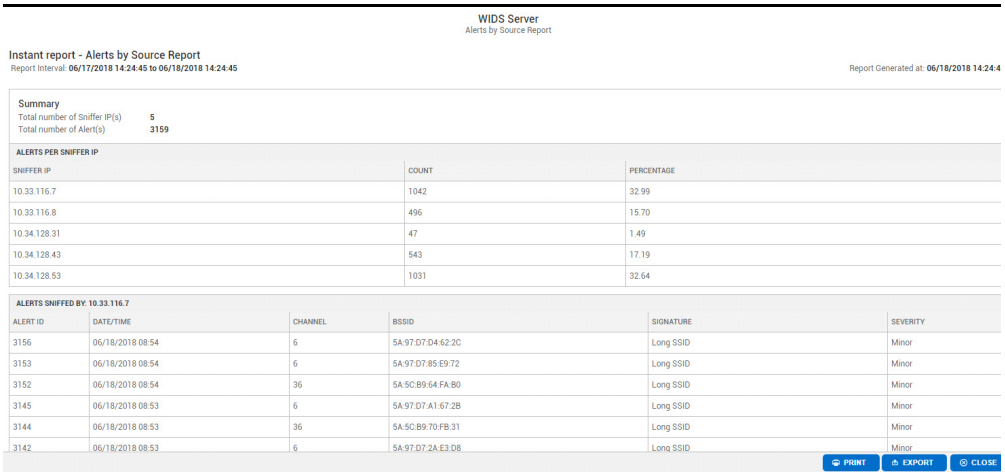
To remove a WIPS chart filter, follow these steps:

1. Click *Monitor* > *Alerts* > *Advanced Filters*.
2. Select the filter you want to remove.
3. Click *Remove Filter*.
4. Click *Done*.
5. Click *Get Alerts*.

Reports

You can schedule a WIPS report to be generated at regular intervals. Once a report is generated, it is available under *Monitor* > *Reports* > *Available Reports*. WIPS supports two report types:

- Alerts Reports
- Alerts by Source Reports



WIDS Server
Alerts by Source Report

Instant report - Alerts by Source Report
Report Interval: 06/17/2018 14:24:45 to 06/18/2018 14:24:45
Report Generated at: 06/18/2018 14:24:4

Summary
Total number of Sniffer IP(s) 5
Total number of Alert(s) 3159

ALERTS PER SNIFFER IP

SNIFFER IP	COUNT	PERCENTAGE
10.33.116.7	1042	32.99
10.33.116.8	496	15.70
10.34.128.31	47	1.49
10.34.128.43	543	17.19
10.34.128.53	1031	32.64

ALERTS SNIFFED BY: 10.33.116.7

ALERT ID	DATE/TIME	CHANNEL	BSSID	SIGNATURE	SEVERITY
3156	06/18/2018 08:54	6	5A:97:D7:D4:62:2C	Long SSID	Minor
3153	06/18/2018 08:54	6	5A:97:D7:85:E9:72	Long SSID	Minor
3152	06/18/2018 08:54	36	5A:5C:B9:64:FA:B0	Long SSID	Minor
3145	06/18/2018 08:53	6	5A:97:D7:A1:67:2B	Long SSID	Minor
3144	06/18/2018 08:53	36	5A:5C:B9:70:FB:31	Long SSID	Minor
3142	06/18/2018 08:53	6	5A:97:D7:2A:E3:D8	Long SSID	Minor

PRINT EXPORT CLOSE

Look at Reports

To see a list of reports, starting from Network Manager, click *Monitor* > *Reports*.

Generate Reports

To generate instant reports, starting from Network Manager, follow these steps:

1. Click *Monitor* > *Reports* > *Instant Reports*.
2. Select a Report Type.
3. Select a time interval.
4. Click **Generate Report**.

Export and View Reports

To export and review reports, starting from Network Manager, follow these steps:

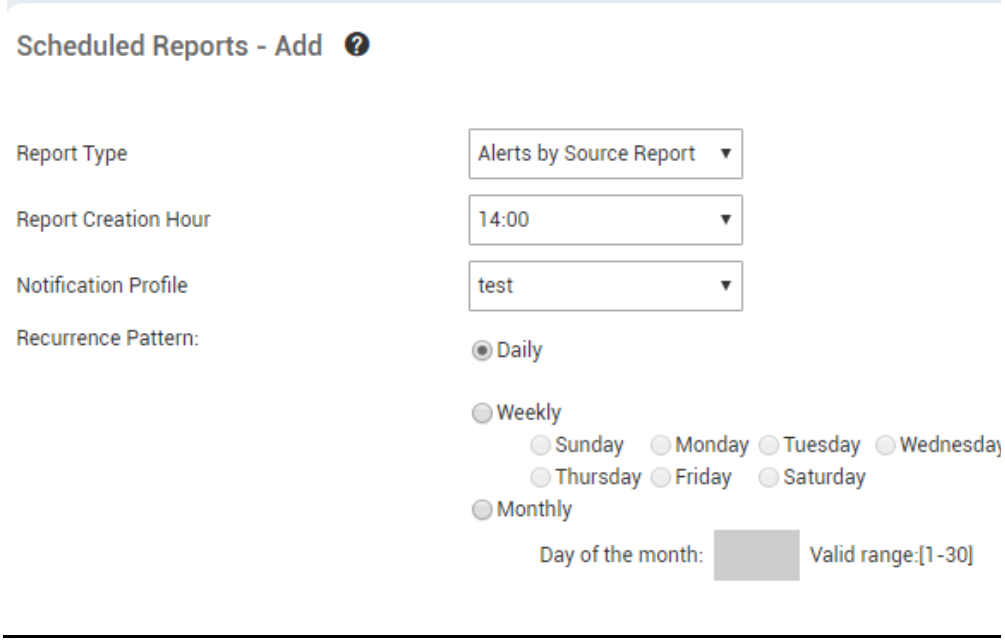
1. Click *Monitor* > *Reports* > *Available Reports*.
2. To view a report, select a report and click **View Report**.

3. To export a report to the local computer, select a report and click **Export**.
4. The exported report has .html and .csv files zipped as *.tgz file. Use a tar unzip utility such as RAR to unzip the report files.

Schedule a WIPS Report

To schedule a WIPS report, follow these steps:

1. Click *Configure* > *Reports* > *Scheduled Reports*.



2. Click **Add**.
3. Select a Report Type, either Alerts Report or Alerts by Source Report.
4. Select the Report Creation Hour from the drop-down list.
5. Select the Notification profile (list of addresses) created in Network Manager.

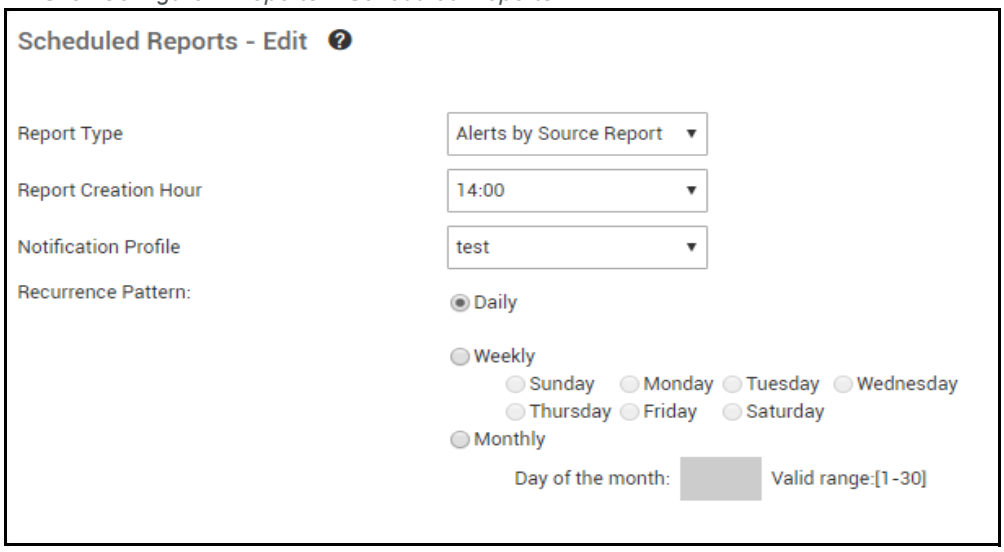
Choose one of the Recurrence Patterns. For daily reports, click Daily. For a weekly report, click Weekly and select the day of report generation. For monthly report, click Monthly and enter the day of the month (1 to 31 is the valid range).

Click **OK**.

Edit a Scheduled Report

To edit the scheduling of an WIPS report, follow these steps:

1. Click *Configure* > *Reports* > *Scheduled Reports*.



2. Select a report and click **Edit**.
3. Make changes (see details under “Schedule a WIPS Report”).
4. Click **OK**.

Delete a Scheduled Report

To delete a WIPS report, follow these steps:

1. Click Configure > *Reports* > *Scheduled Reports*.
2. Select a report and click **Delete**.
3. Click **OK**.

Export a Report

To export a completed WIPS report to a .tar file, follow these steps:

1. Click *Monitor* > *Report* > *Available Reports*.
2. Select a report and click **Export**.
3. Click **Save**.
4. Provide a name.
5. Click **Save**.
6. Click **Open**.

The downloaded tar file can be extracted using the WinRar or Winzip application in Windows. In Linux the tar files can be extracted using the "tar"command. For example:

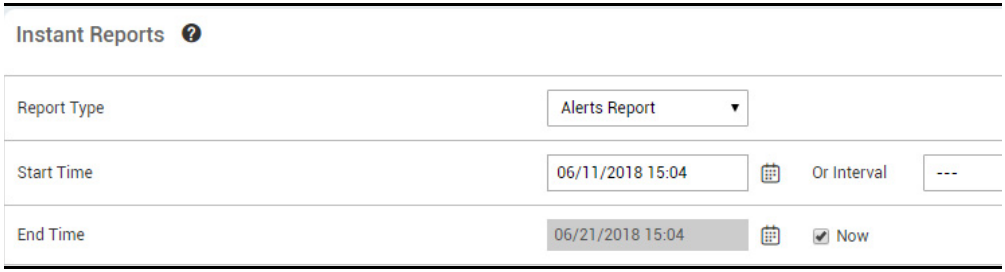
tar -zxvf filename.tgz

Scheduled reports compress both HTML and CSV versions in the file; however, Instant reports include only the HTML version.

Create an Instant Report

You do not have to schedule reports; you can create one instantly. To create an instant WIPS report, follow these steps:

Click *Monitor* > *Reports* > *Instant Report*.



Delete Old Reports

To delete a copy of a completed WIPS report (scheduled or instant), follow these steps:

1. Click *Monitor* > *Reports* > *Available Reports*.
2. Select a report and click **Delete**.
3. Click **OK**.

Maintenance

Configuring Trusted APs

(Optional) There will probably be APs in your area that will always be present because your networks share the same airspace. You don't want to be constantly alerted that your neighbors have APs; these alerts are called false positives. To prevent this, create a list of trusted APs.

Trusted APs can be configured using either the Add option or by importing a CSV file. The Add option lets you add one entry at a time. The Import option allows you to add multiple entries at once.

This page displays the list of trusted APs in the network. You can Add, Delete, Edit, Save and Import trusted APs.

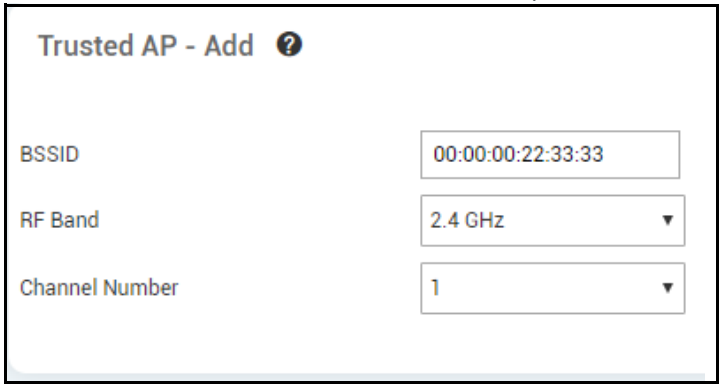
Add a Trusted AP

To add a Trusted AP, follow these steps:

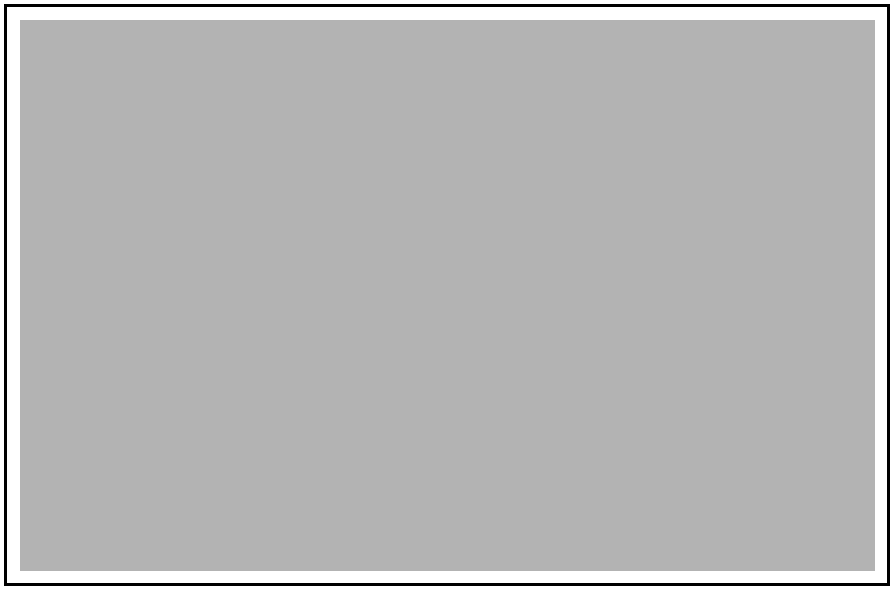
1. Click *Configure* > *Trusted APs*. A list of trusted APs appears.
2. Click **Add**.
3. Provide a valid BSSID, RF Band and Channel Number on which the AP is operating.
4. Click **OK**.

Import a Trusted AP

To add one or more Trusted APs, follow these steps:



1. Click *Configure* > *Trusted APs*. A list of trusted APs appears.
2. Select an AP and click **Import**.
3. Click **Browse** and provide one or more valid CSV filenames; these files must contain the Trusted AP details in the following syntax: ***<MAC address> <rf band><channel>***, for example, 11:12:AB:32:55:C3,5 GHz,34. Here is a sample list:



4. Click **OK** to load the Trusted AP entries.

Edit a Trusted AP

To edit a Trusted AP, follow these steps:

1. Click *Configure* > *Trusted APs*. A list of trusted APs appears.
2. Select an AP and click **Edit** and change the value in the required field.
3. Click **OK**.
4. Click **Save**.

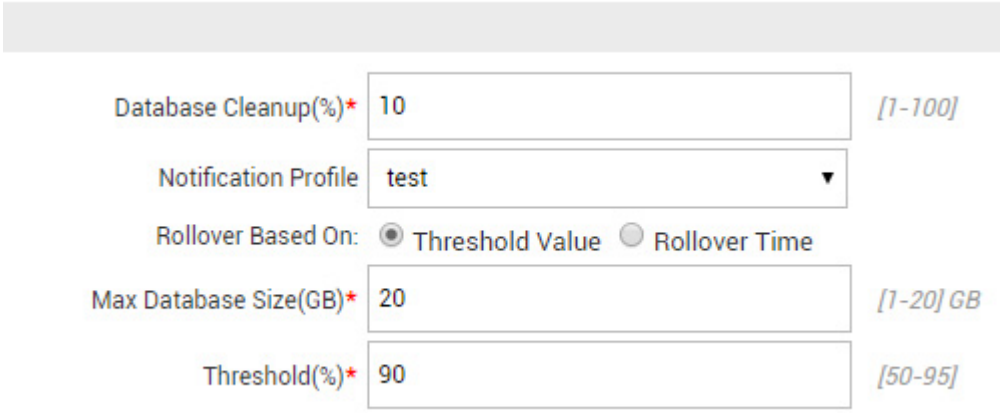
Delete a Trusted AP

To delete a Trusted AP, follow these steps:

1. Click C*onfigure* > *Trusted APs.* A list of trusted APs appears.
2. Select an AP and click **Delete**.
3. Click **OK**.

Configuring Database Maintenance

Set the configuration parameters for initiating DB Rollover by following these steps:



1. Click *Configure* > *System Administration* > *Maintenance*.
2. Provide a Database Cleanup (%)of memory to be cleaned up if the size of the database crosses the Threshold.
3. Select the Notification Profile to be used when the cleanup process is triggered.
4. Specify which mechanism should be used for identifying when the cleanup process should be initiated: based on a database size threshold (Threshold Value) or a specific time (Rollover Time).
5. If using a size threshold, provide a Maximum Database Size in GB (1-1024) and threshold percentage. When the database reaches the percentage specified of the maximum size, cleanup will occur.
6. If specifying a time interval, specify the time at which the rollover should take place and its repeat frequency (either a one-time only occurrence or repeated daily, weekly, or monthly runs).
7. Click **Save**.

Configuring Syslog

Configure logging of messages on a remote machine by following these steps:

1. Click *Configure* > *System Administration* > *Maintenance*.

2. Select Enable or Disable from the Syslog status drop-down box.
3. Provide the Hostname/IP Address of the remote machine where logs are to be stored.
4. Click **Save**.

If the configured Syslog server hostname/IP address is wrong or not reachable, syslog messages will not be logged anywhere.

Configuring Auto Refresh

Configure the Auto Refresh time for the Dashboard page by following these steps:

1. Click *Configure* > *System Administration* > *Maintenance*.
2. Provide the number of seconds (60-300) between refreshes on the Dashboard page.
3. Click **Save**.

Command Line Interface (CLI)

WIPS includes CLI commands for alerts, signatures, starting/stopping, and backup/recovery.

Listing Alerts from the CLI

```
wips show-alerts severity <level>
```

This command lists the most recent 10 alerts of a given severity level. The options for severity are: Critical, Major, Minor, All (to list alerts of all the severities). Here is an example of each:

- `wips show-alerts severity critical`
- `wips show-alerts severity major`
- `wips show-alerts severity minor`
- `wips show-alerts severity all`

```
wips show-alerts severity <level> category <signature name>
```

This command lists the most recent 10 alerts of a given severity level in a given category. The options for severity are: Critical, Major, Minor, All (to list alerts of all the severities). Category can be any signature name or all for all the signature types. This example uses the signature option all.

- `wips show-alerts severity critical category all`
- `wips show-alerts severity major category all`

- `wips show-alerts severity minor category all`
- `wips show-alerts severity all category all`

```
wips show-alerts severity <level> category <signature name> stime
<start time>
```

This command lists the most recent 10 alerts of a given severity level in a given category at a given start time. The options for severity are: Critical, Major, Minor, All (to list alerts of all the severities). Category can be any signature name or all for all the signature types. Start time must be in the format MM/DD/YYYY HH:MM:SS.

This example will display the most recent 10 critical alerts from the signature named ‘auth’ that took place between January 21, 2010 and now.

- `wips show-alerts severity Critical category auth stime  '01/21/2010 18:22:02'`

```
wips show-alerts severity <level> category <signature name> stime
<start time> etime <end time>
```

This command lists the most recent 10 alerts of a given severity level in a given category between a given start time and end time. The options for severity are: Critical, Major, Minor, All (to list alerts of all the severities). Category can be any signature name or all for all the signature types. Start time and end time must be in the format MM/DD/YYYY HH:MM:SS.

This example will display the most recent 10 critical alerts from the signature named ‘auth’ that took place between January 21, 2010 and March 21, 2010.

- `wips show-alerts severity all category all stime  '01/21/2010 18:22:02' etime '03/21/2010 08:22:22'`

```
wips show-alerts severity <level> category <signature name> stime
<start time> etime <end time> order <asc|desc>
```

This command lists the most recent 10 alerts of a given severity level in a given category between a given start time and end time. The options for severity are: Critical, Major, Minor, All (to list alerts of all the severities). Category can be any signature name or all for all the signature types. Start time and end time must be in the format MM/DD/YYYY HH:MM:SS.

This example will display the most recent 10 critical alerts from the signature named ‘auth’ that took place between January 21, 2010 and March 21, 2010 in ascending order (most recent alert last).

- `wips show-alerts severity Critical category auth stime '01/21/2010 18:22:02' etime '03/21/2010 08:22:22' order asc`

```
wips show-alerts severity <level> category <signature name> stime
<start time> etime <end time> order <asc|desc> count <number>
```

This command lists the indicated number of most recent alerts of a given severity level in a given category between a given start time and end time. The options for severity are: Critical, Major, Minor, All (to list alerts of all the severities). Category can be any signature name or all for all the signature types. Start time and end time must be in the format MM/DD/YYYY HH:MM:SS.

This example will display the most recent 20 critical alerts from the signature named ‘auth’ that took place between January 21, 2010 and March 21, 2010 in ascending order (most recent alert last).

- `wips show-alerts severity Critical category auth stime '01/21/2010 18:22:02' etime '03/21/2010 08:22:22' order asc count 20`

Listing Signatures from the CLI

```
wips show-signatures
```

This command lists all signatures along with their configured parameters. An example of this is:

```
wips show-custom-signatures
```

This command lists all custom signatures (rules) along with their configured parameters. An example of this is:

```
wips show-custom-signatures
```

Controlling WIPS From the CLI

Start/Restart/Stop WIPS

To start/restart/stop the WIPS application, use the following CLI commands:

- `wips application start`
- `wips application restart`
- `wips application stop`

Back Up and Restore WIPS Database and Configuration

To backup the database and the configuration folder of the WIPS application, use the command:

```
wips db-backup
```

To store the backed up file onto a remote machine provide the remote server's IP/ Hostname along with the path on the remote machine and user name as follows:

```
wips db-backup remoteserver 10.1.1.1 username root path /root/
```

To restore only the configuration folder from a backed up file, use the command:

```
wips db-restore restore config file Backup-wips_04-13-2010_23-35-
05.tar.gz
```

To restore both the configuration folder and the database, use the command:

```
wips db-restore restore all file Backup-wips_04-13-2010_23-35-
05.tar.gz
```

To restore configuration and the database from a remote machine, use the command:

```
wips db-restore restore all file Backup- wips_04-13-2010_23-35-
05.tar.gz remoteserver 10.1.1.1 username root path /root/
```

To list all files in the backed up configuration folder and database, use the following CLI command:

```
wips list-backup
```

6 FortiWLM - Virtual Edition

FortiWLM supports the Virtual Edition of the Application Suite. The following virtual software platforms are supported:

- VMware ESXi 6.0, 6.5, and 7.0
- KVM
- Hyper-V (Windows 2016 only).

Deploying FortiWLM with VMWare ESXi

This document describes the procedure to deploy virtual FortiWLM, **FWM-VM** as FWLM-VM-100D and FWLM-VM-1000D on VMWare ESXi.

Supported Hardware Configuration

This table lists the supported configuration for FWLM-VM-100D and FWLM-VM-1000D.

Configuration	FWLM-VM-100D	FWLM-VM-1000 D
Processor and Cores	Any Processor @ 2GHz or Higher. 4 Cores - 4 Threads	Any Processor @ 3.20GHz or Higher. 4 Cores - 8 Threads
Memory (DRAM)	4GB	16GB
Storage	1TB	2TB
Minimum Disk I/O	100MBps	100MBps
Network	1-4 1G RJ-45	1-4 1G RJ-45
Scale Numbers	AP: 1000 Stations: 5000 Spectrum Sensors: 100	AP: 15000 Stations: 75000 Spectrum Sensors: 750

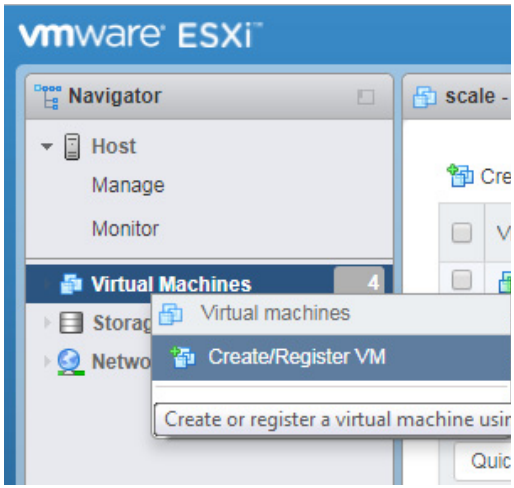
Downloading the Virtual Machine Package File

You can download the virtual controller packages from the Fortinet Customer Support web-site. To access the support website you need a Fortinet Customer Support account.

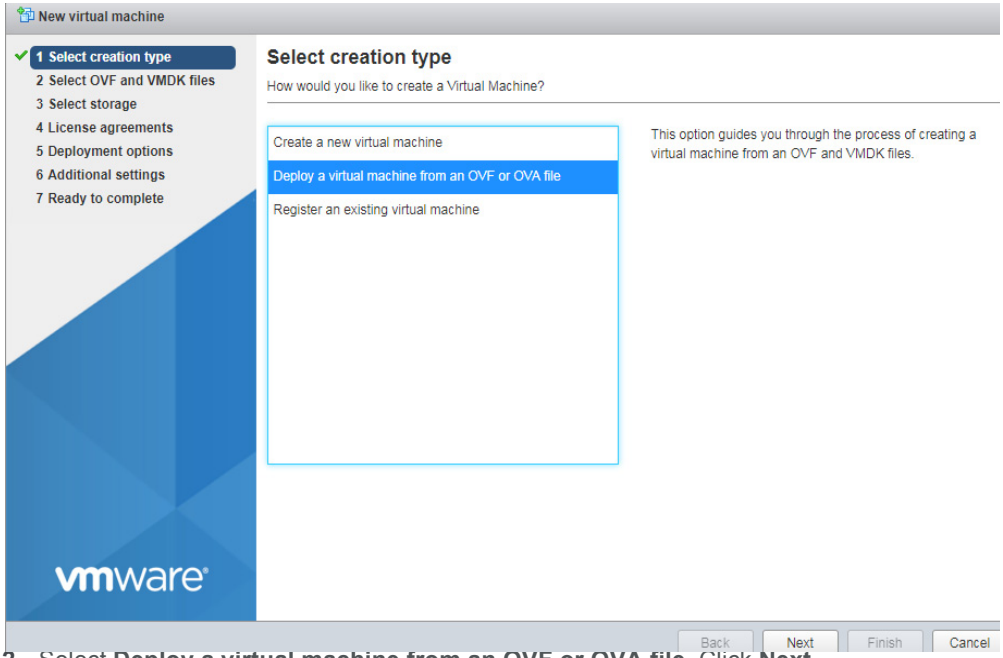
The file name is, *forti-wlm-x.x-xbuild-y-x86_64.ova*, where *x.x-x* is the release version number, for example, 8.4.0.

Creating the Virtual Machine

1. Open the VMWare ESXi console and navigate to **Virtual Machines < Create/Register VM**.

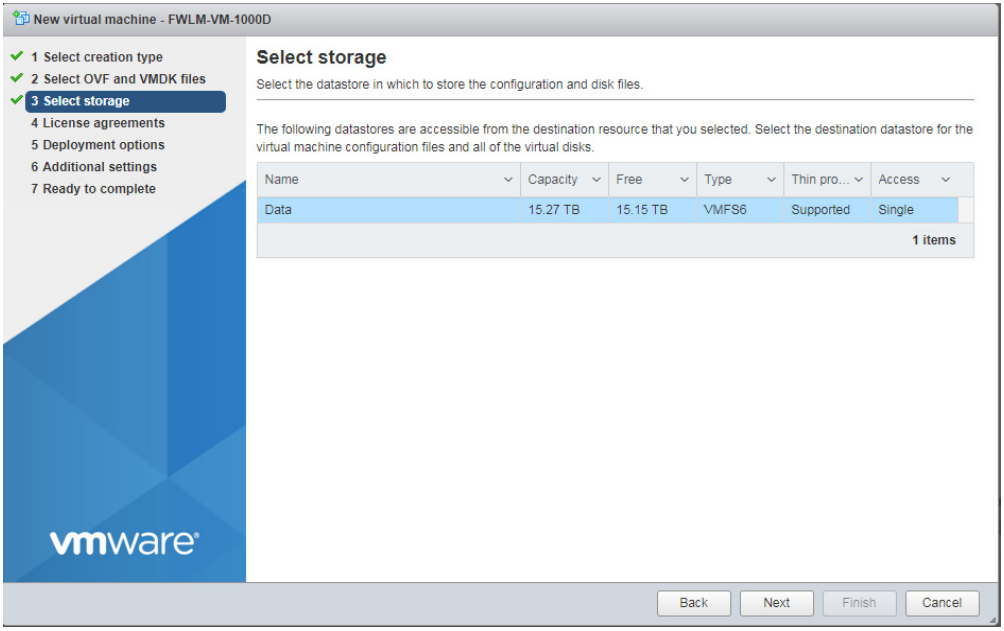


The **New Virtual Machine** wizard is displayed.

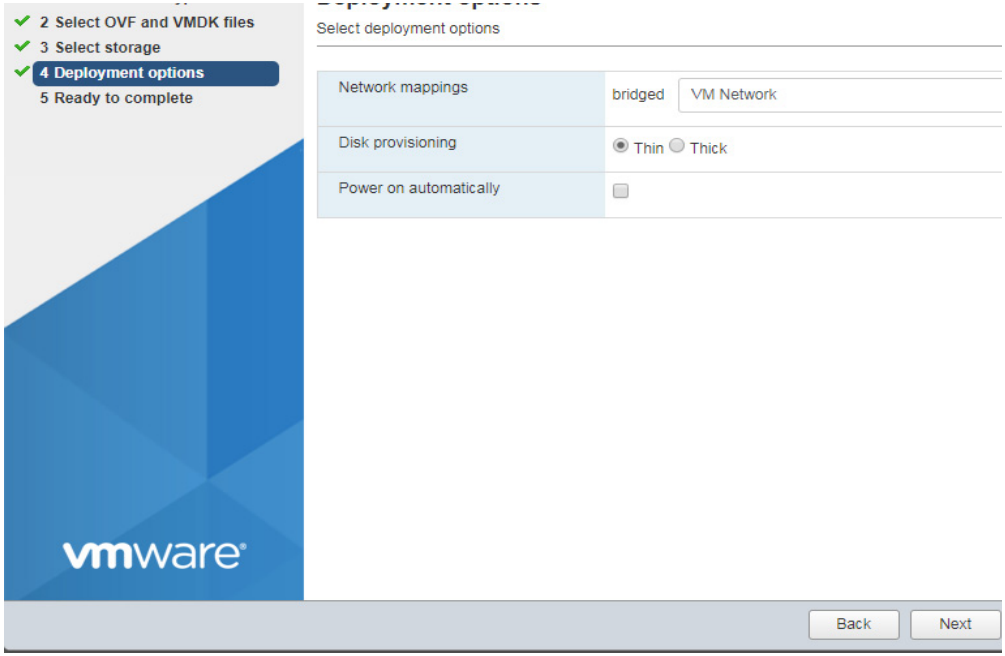


2. Select **Deploy a virtual machine from an OVF or OVA file**. Click **Next**.
3. Enter a unique name for the virtual machine and click on the space, as indicated, to select or drag and drop the downloaded OVA file. Click **Next**.

4. Select the datastore to store configuration and disk files. Click **Next**.



The deployment options are displayed. Click **Next**.



5. Select the **Network mappings** as **bridged VM Network**, **Disk provisioning** should be **Thin**. Disable **Power on automatically**. Click **Next**.
6. Review the configured settings and click **Finish**.

The virtual machine is created.

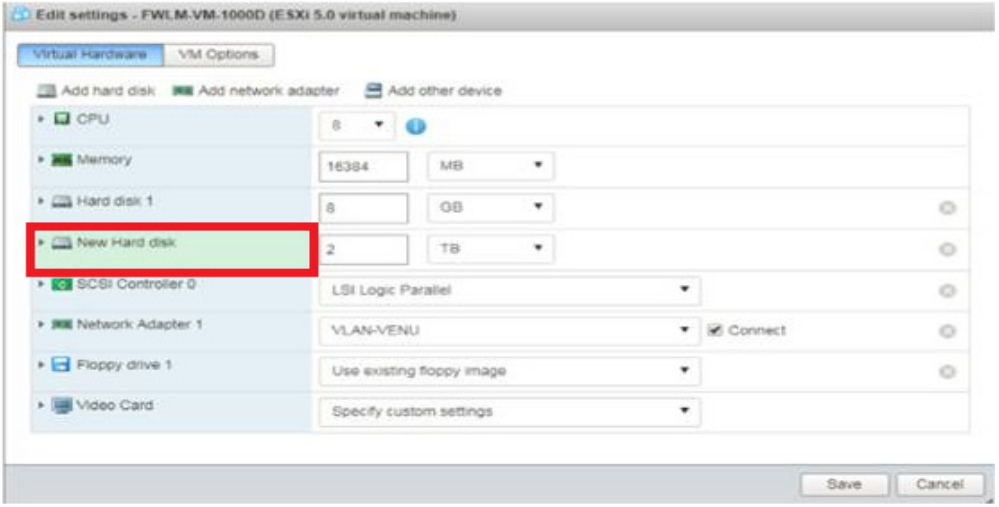
Configuring the Virtual Machine

After creating a virtual machine, configure it to work as a FWLM-VM-100D or FWLM-VM-1000D.

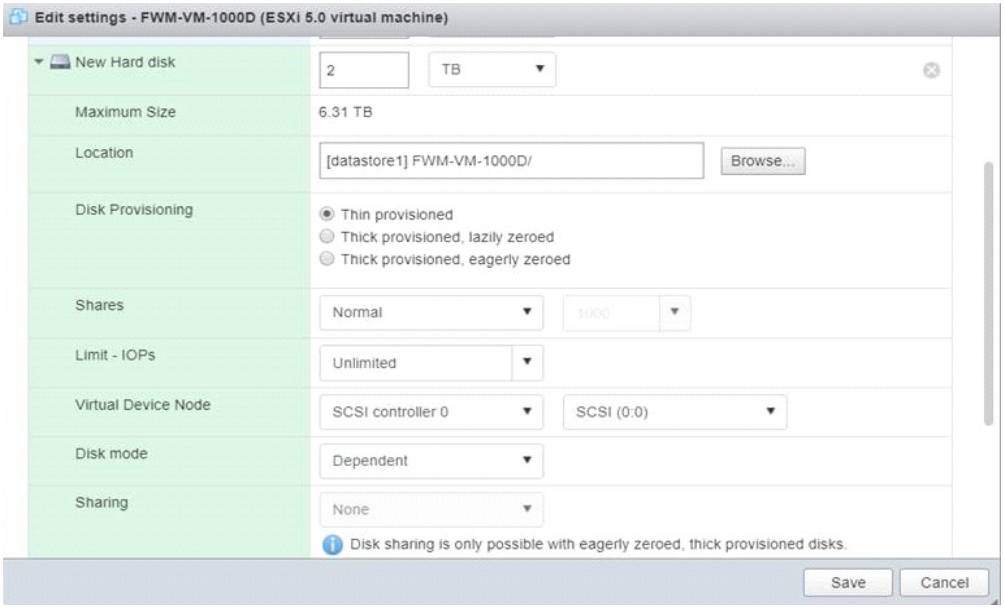
1. Select the listed virtual machine and right-click. Select **Edit settings**.
2. Modify the **CPU** and the **Memory**.
3. Click **Add hard disk** to add a new hard disk.

Note: The hard disk should be of type **SCSI**.

4. Click **Save**.



The new hard disk added is depicted in the image below. The **Disk Provisioning** should be **Thin Provisioned**.



Starting the Virtual Machine

After configuring the newly created virtual machine, select the listed virtual machine and right-click. Select **Power < Power on**.

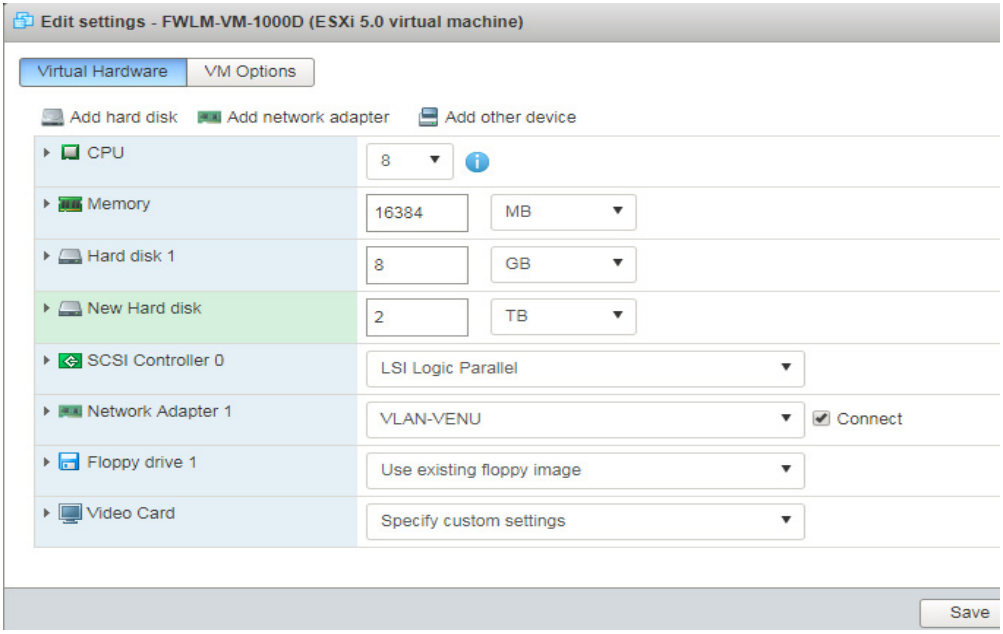
The Virtual Machine starts.

Expanding the Virtual Hard Disk

You can increase the storage space of a virtual machine by expanding its virtual hard disk. Follow these steps to expand the virtual hard disk.

Note:
Decreasing the size of the virtual hard disk is not supported.

1. Run the **resizedisk** command from the IOS CLI to enable resizing the disk.
2. Select the virtual machine on the ESXi console and right click.
3. Select **Power < Power off** to power off the Guest VM.
4. Right click the virtual machine and select **Edit Settings.**
5. Under **Virtual Hardware,** modify the hard disk size**.**



KVM Virtualization

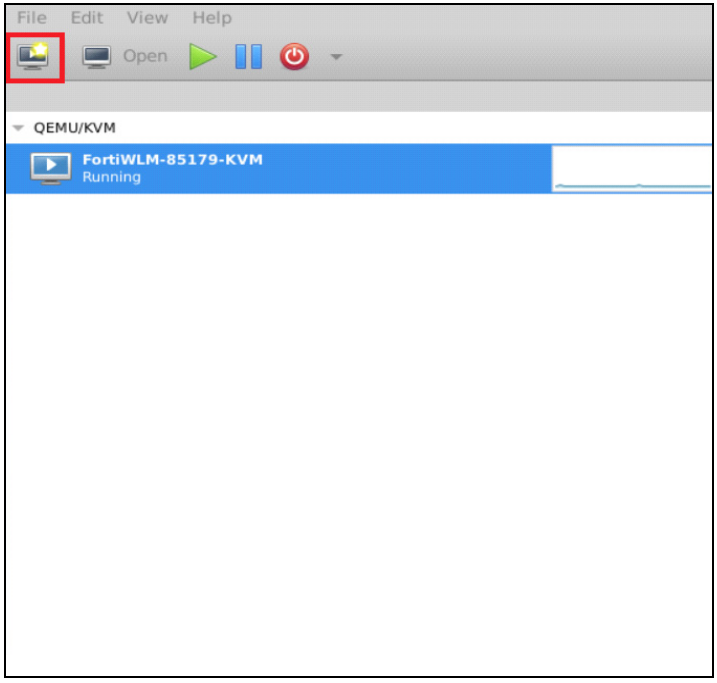
Network Manager virtual image can be installed in a KVM Hypervisor. The following are the steps to set up a virtual server and install Network Manager.

Notes:

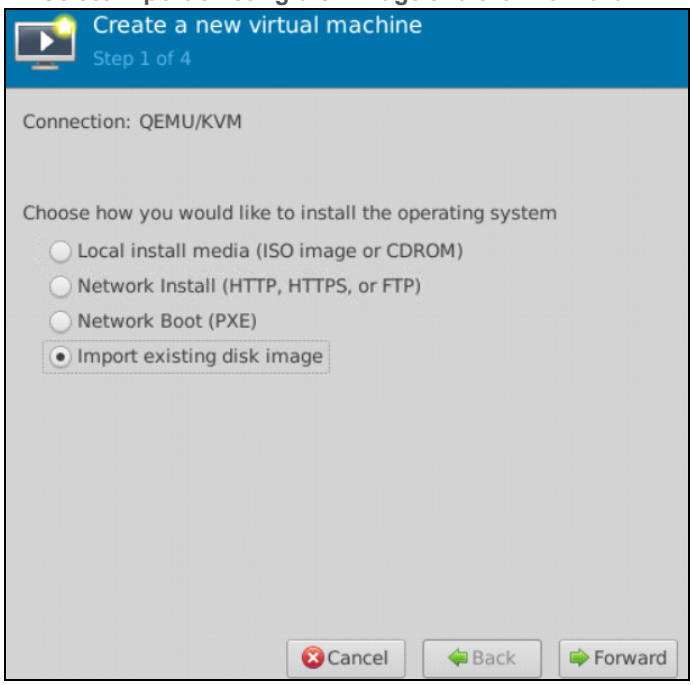
- FortiWLM can be installed on KVM Hypervisor upon **CentOS** or **Ubuntu**.
- The installation steps in virtual manager may vary based on the GUI.
- This procedure installs FortiWLM on KVM Hypervisor upon Ubuntu version **20.04** with QEMU emulator version **4.2.0 (Debian 1:4.2-3ubuntu6.2)**.

Download the release image file, for example, ***forti-wlm-8.5-xbuild-xx-x86_64.img.KVM.zip***

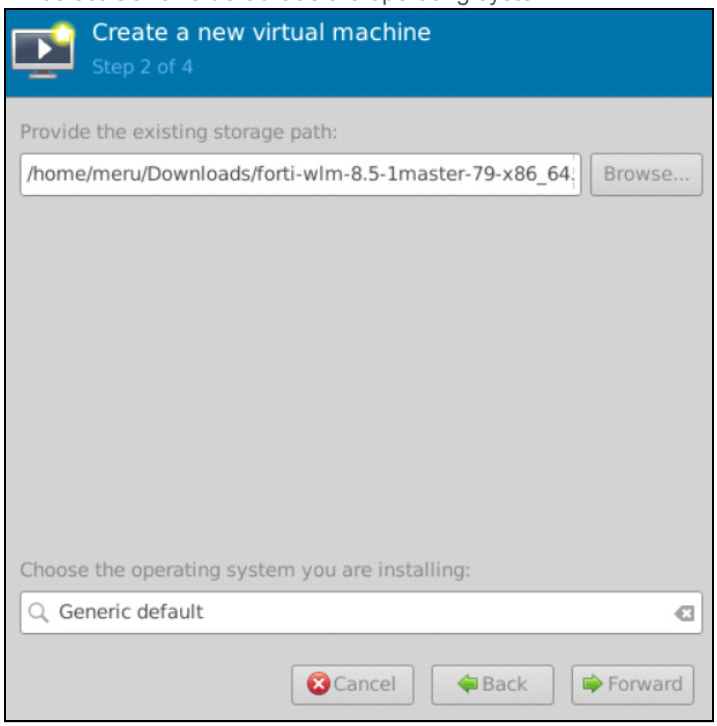
1. Click on **Monitor** *Icon* in Virtual Machine Manager GUI to create a new FortiWLM Virtual Machine..



2. Select **Import existing disk image** and click **Forward**.

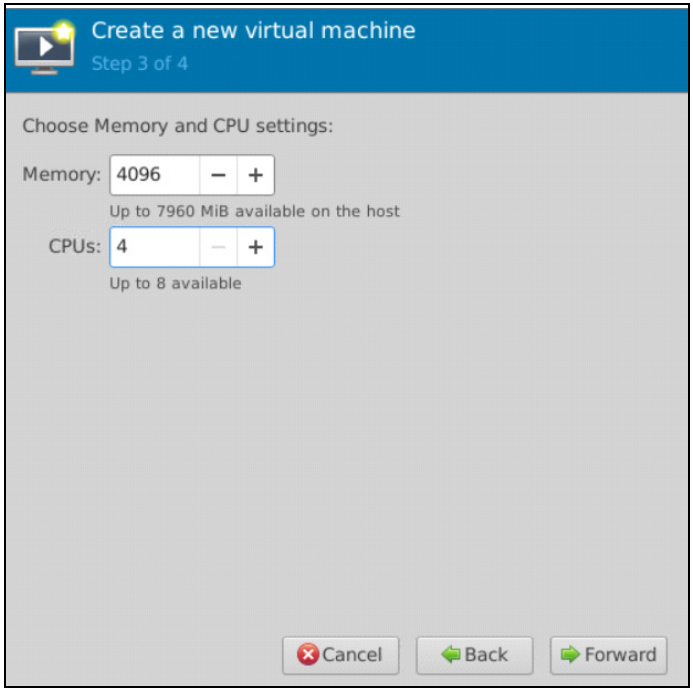


3. Browse to the FortiWLM image file (***forti-wlm-8.5-1build-xx-x86_64.img***) locally and select **Generic default** as the operating system.

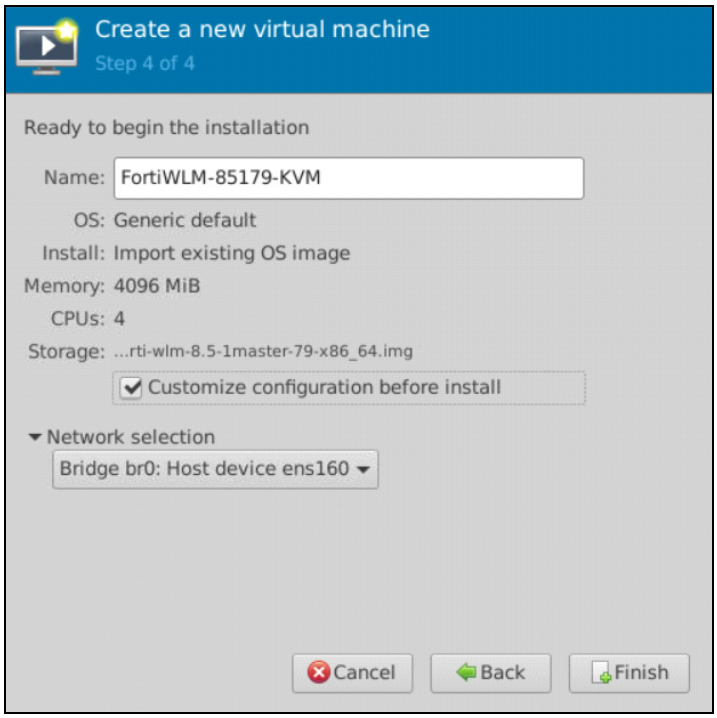


Click **Forward**.

4. Specify the RAM and CPUs for FortiWLM VM and Click **Forward.**
   Note: It is recommended to use RAM at least 4 GB and 4 CPU.

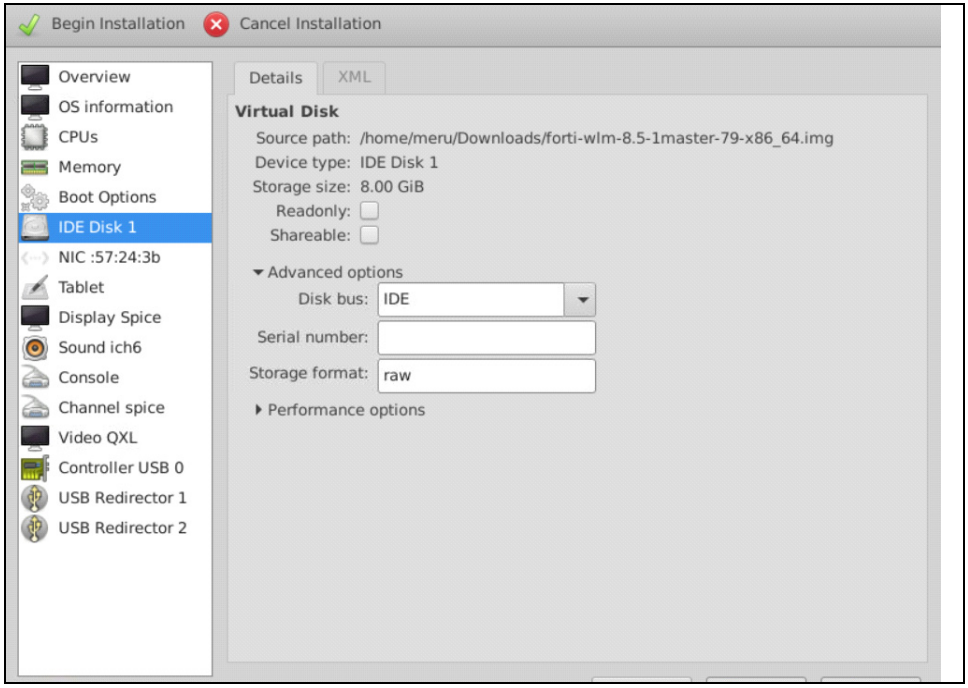


5. Enter the name of the FortiWLM VM and select **Customize configuration before Install**.



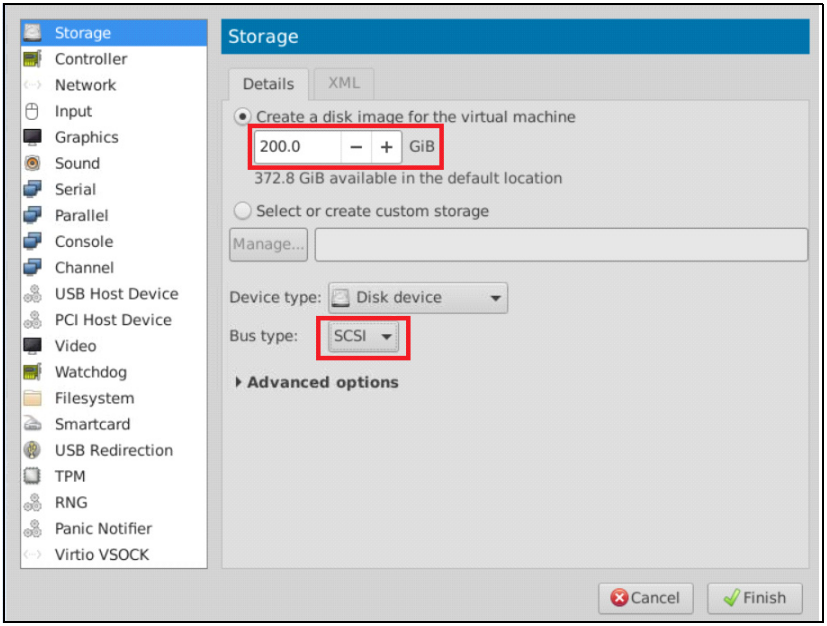
Note: Check the network for VM connectivity. In this example attached the same network bridge br0. Click **Finish**.

6. Select **Disk bus** as the **IDE** and **Storage format** as **raw** for the IDE Disk 1.



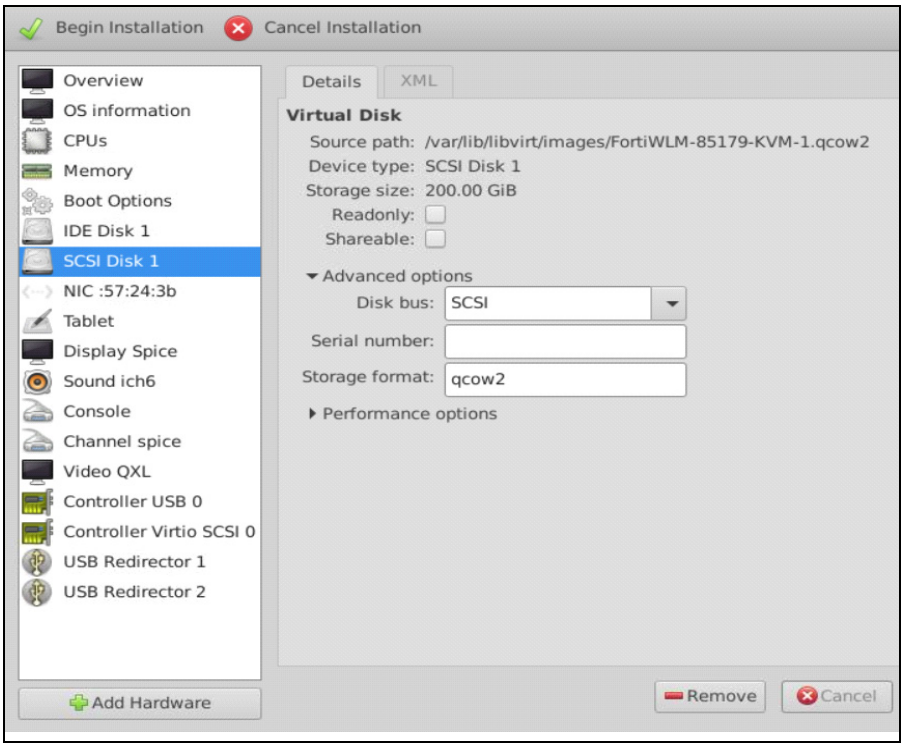
Click **Add Hardware** to add the SCSI hard disk.

7. Select the hard disk size as per the requirement and **Bus type** as **SCSI**.



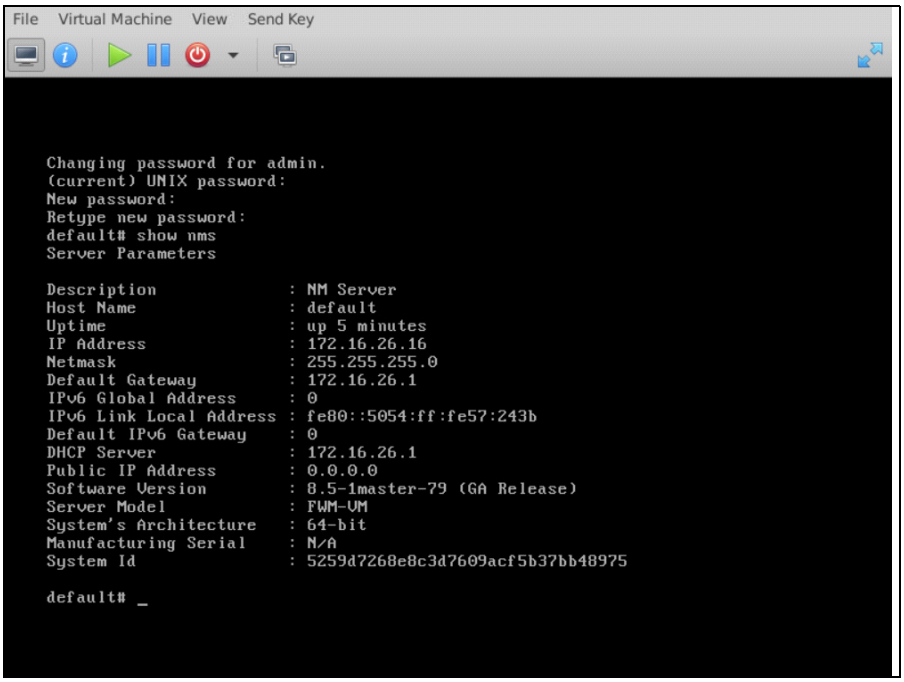
Click **Finish**.

8. Add SCSI Disk 1 and **Storage format** is **qcow2**.



9. Click **Begin Installation** to start the Virtual Machine.

The FortiWLM comes up in some time. Run the **show nms** command to see if the system is ready.

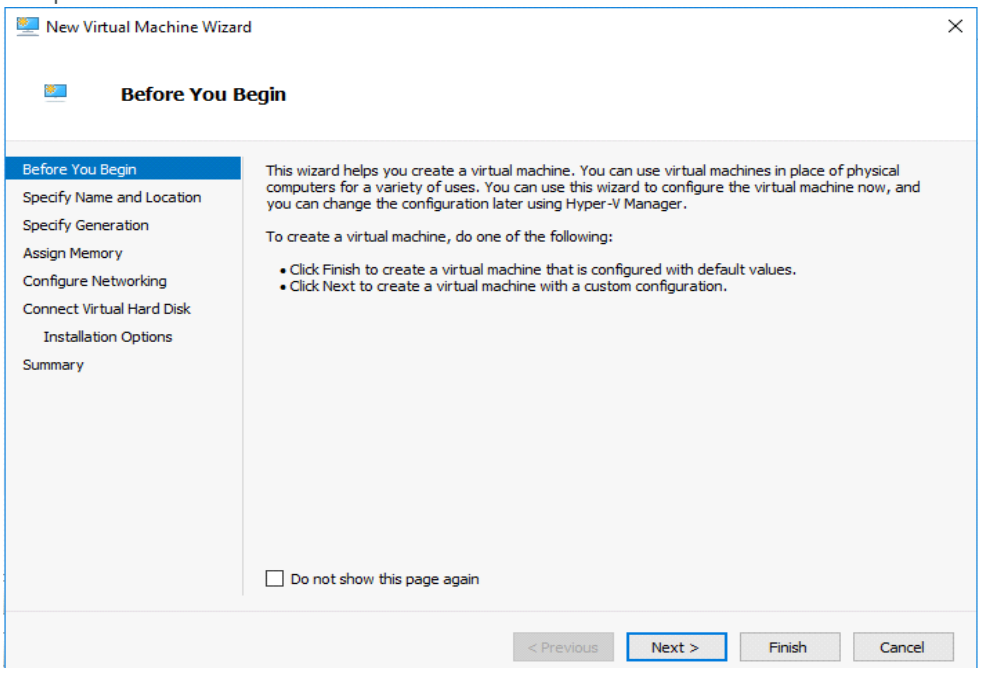


Hyper-V Virtualization

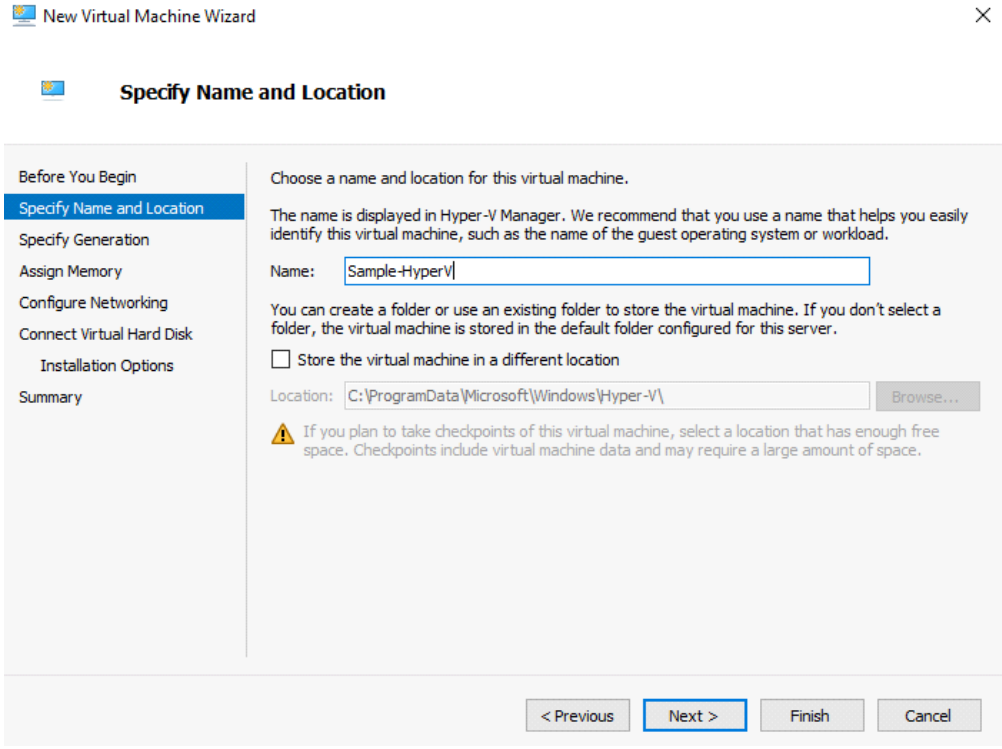
Note: Hyper-V virtualization is supported only in Windows 2016 Servers.

To Install, unzip the downloaded package files (*.vhd.HV.zip*) and perform the following step to deploy 64-bit Hyper-V instance of FortiWLM.

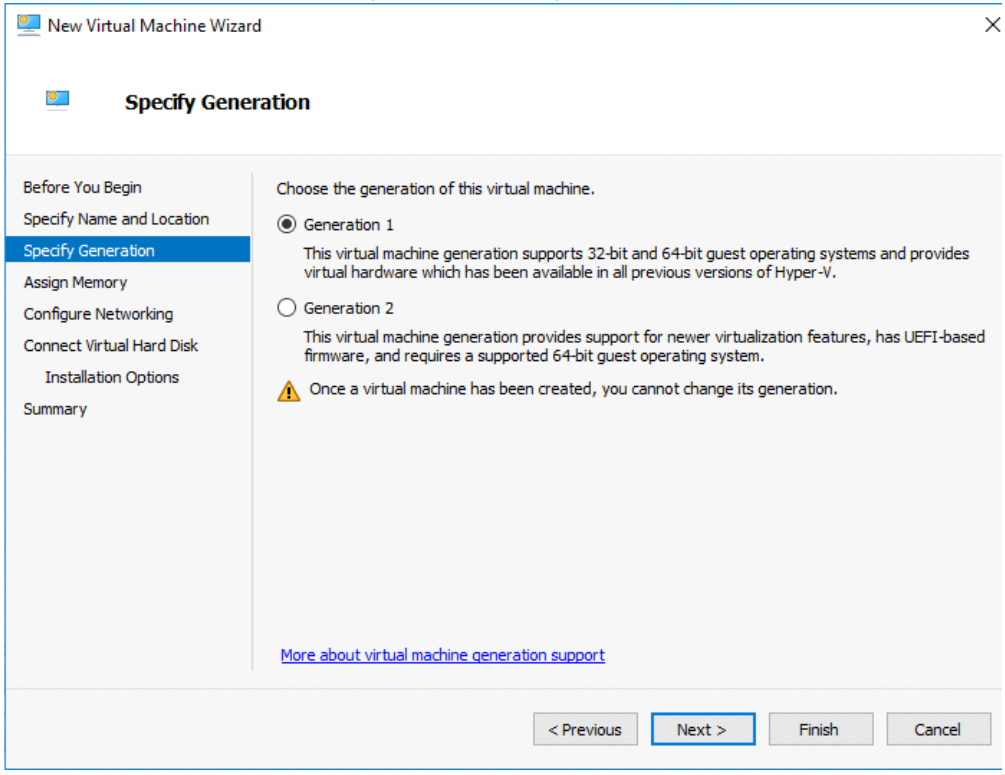
1. Open Hyper-V Manager and right click on Hyper-V Server and select **Create New VM** to open the New Virtual Machine Wizard. Click the **Next** button..



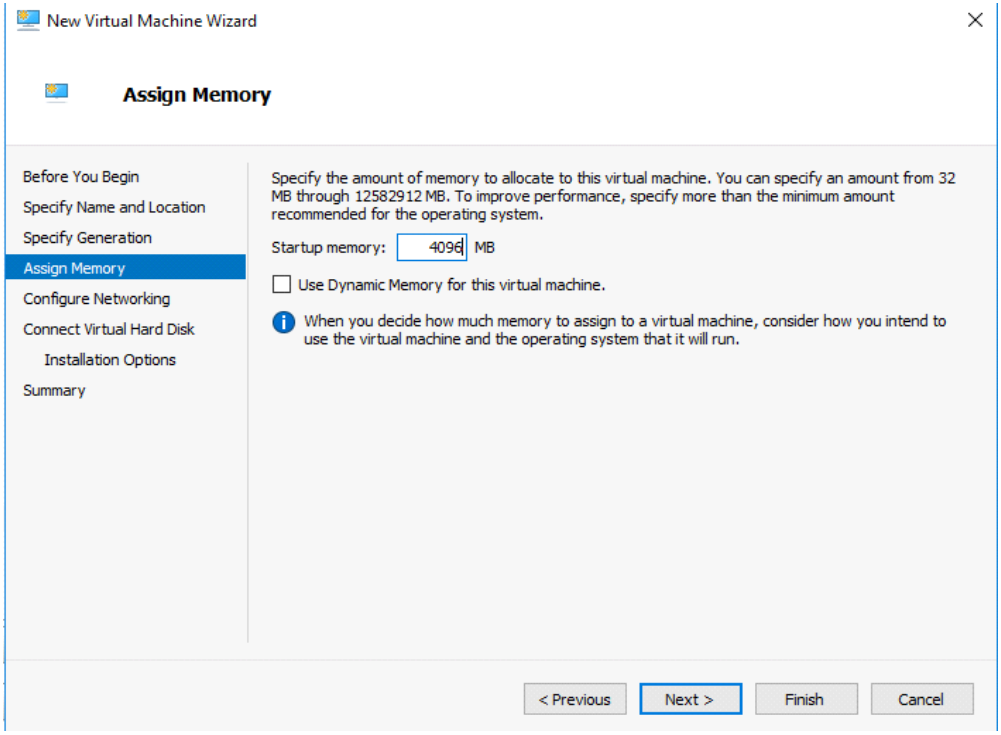
2. Enter the **Name** and select the **Location** by clicking on **Browse** button to store the Virtual Machine.



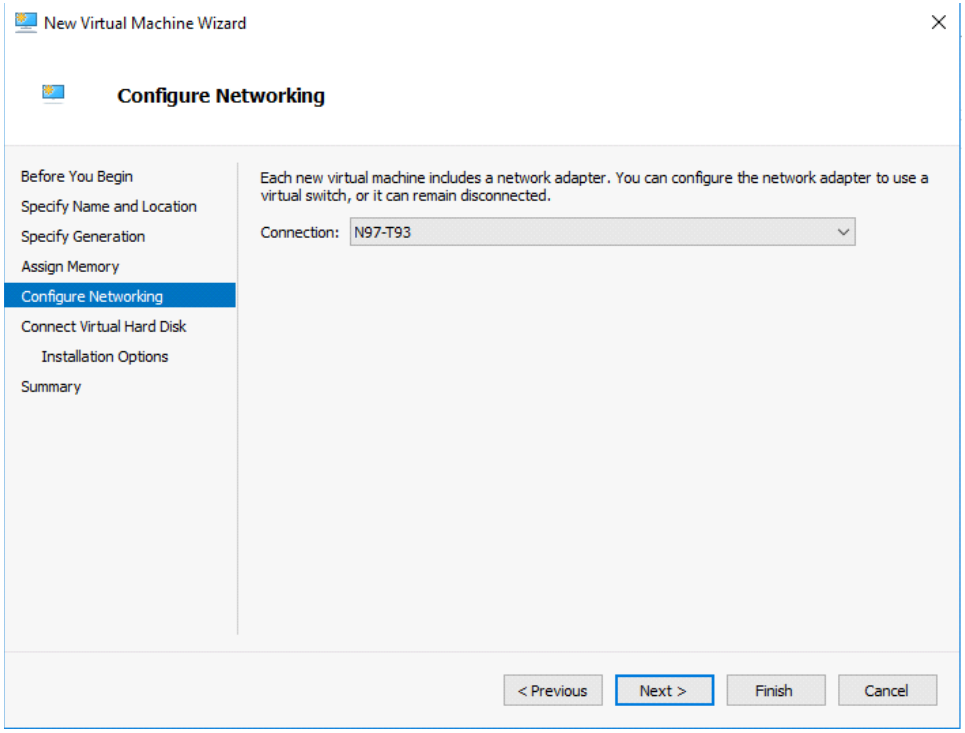
3. Select **Generation1** in **Specify Generation** page and click on **Next.**



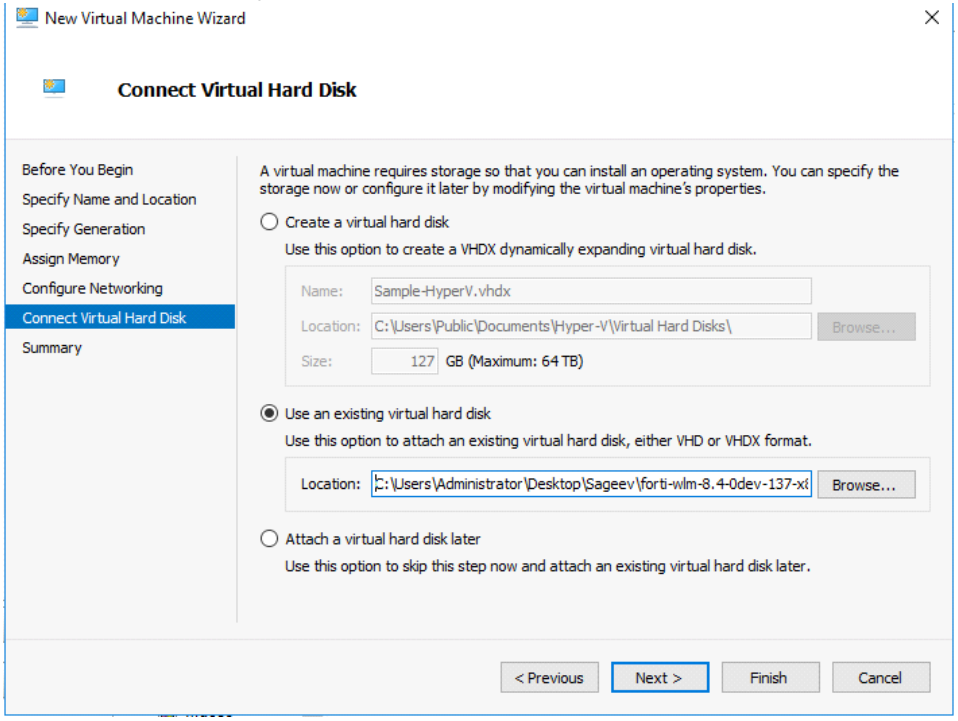
4. Enter the RAM size. Recommended RAM size is **4 GB (4096 MB)** and click on **Next.**



5. Select the network adapter connect and Click **Next.**



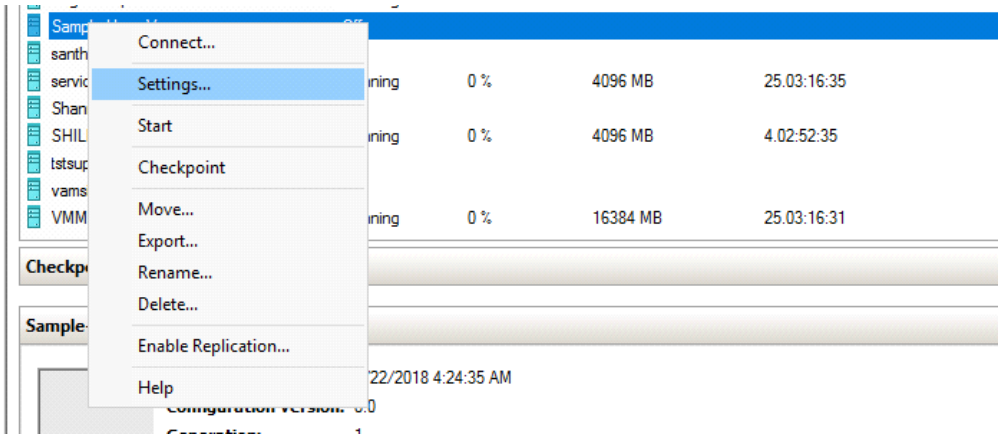
6. Select **Use an existing virtual hard disk** and click **Browse** to select the Hyper-V Disk "*.vhd" (stored locally). And click **Next.**



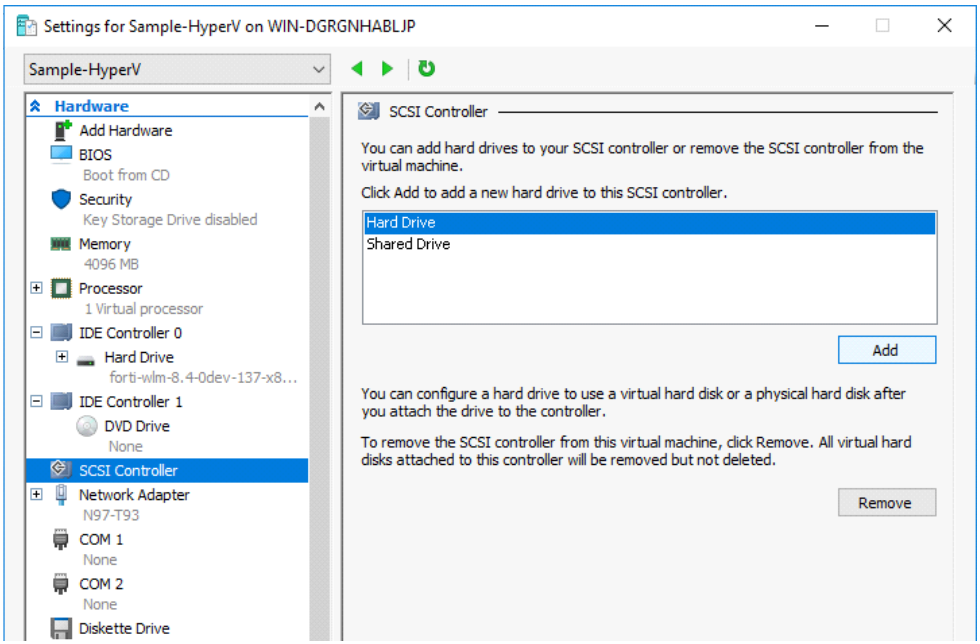
The new Virtual Machine is created.

Creating Virtual Disk

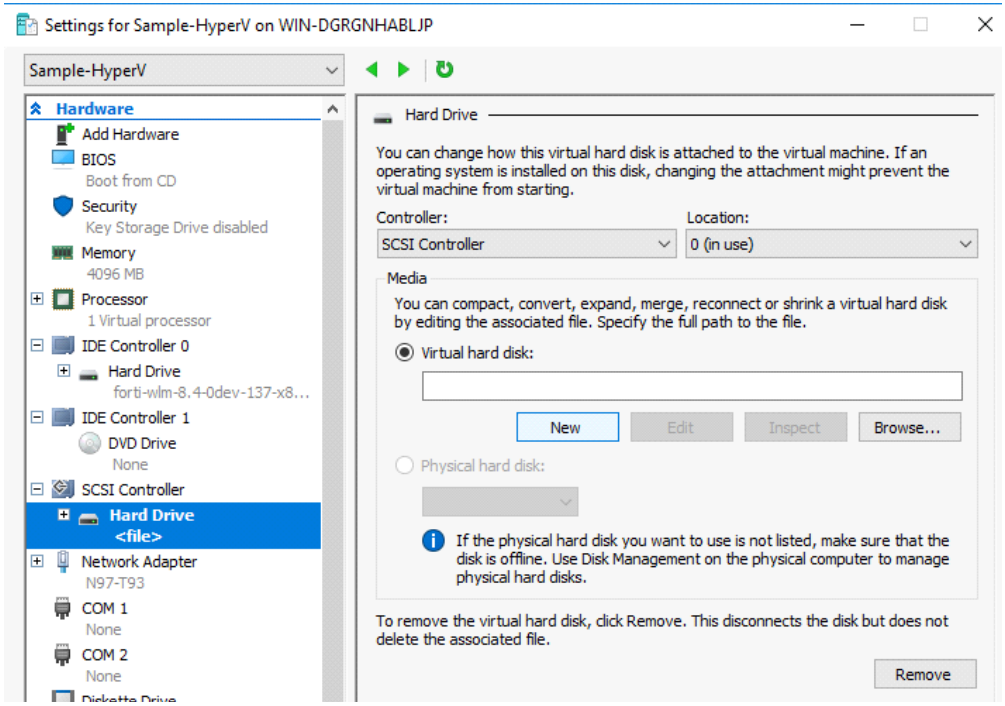
1. Browse to the **Settings** on the VM instance created.



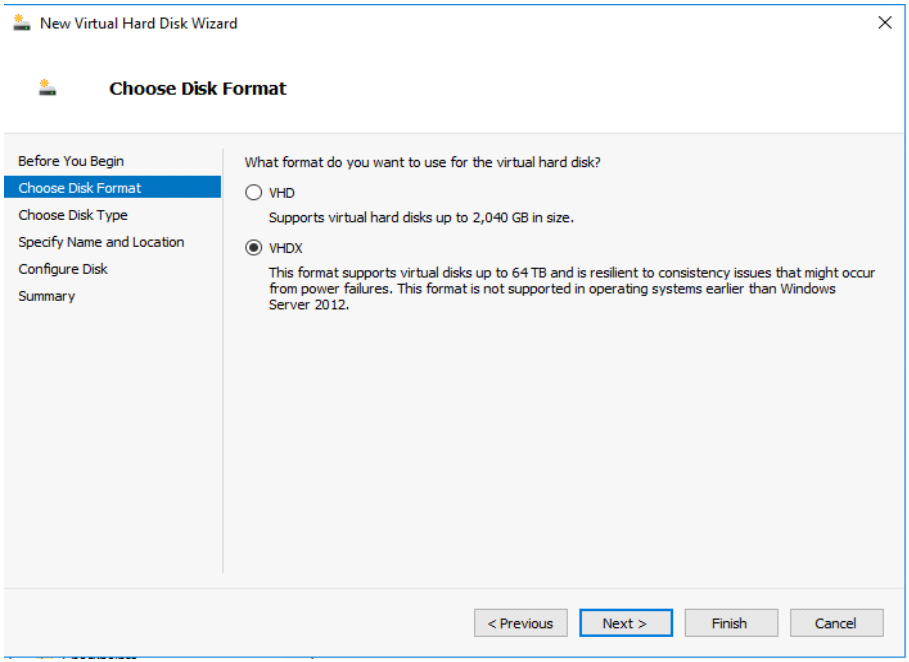
2. Select the **SCSI Controller** device and select **Hard Drive**. Click **Add.**



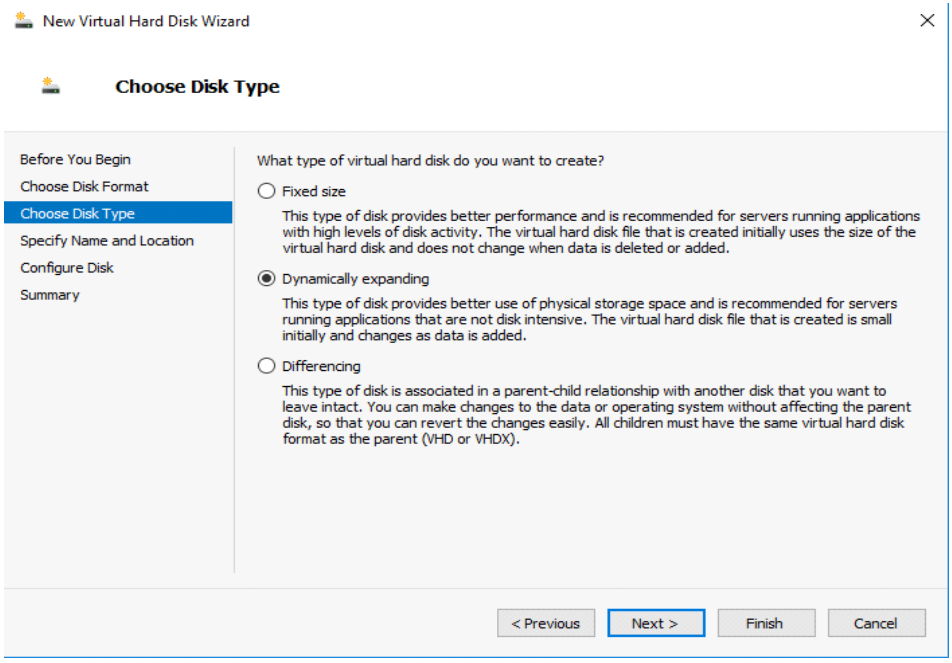
3. Click on **New** to Create a New Virtual Hard disk.


Settings for Sample-HyperV on WIN-DGRGNHABLJP
Sample-HyperV
Hardware
Add Hardware
BIOS
Boot from CD
Security
Key Storage Drive disabled
Memory
4096 MB
Processor
1 Virtual processor
IDE Controller 0
Hard Drive
forti-wlm-8.4-0dev-137-x8...
IDE Controller 1
DVD Drive
None
SCSI Controller
Hard Drive
<file>
Network Adapter
N97-T93
COM 1
None
COM 2
None
Hard Drive
You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.
Controller:
SCSI Controller
Location:
0 (in use)
Media
You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.
Virtual hard disk:
New
Edit
Inspect
Browse...
Physical hard disk:
If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.
To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.
Remove

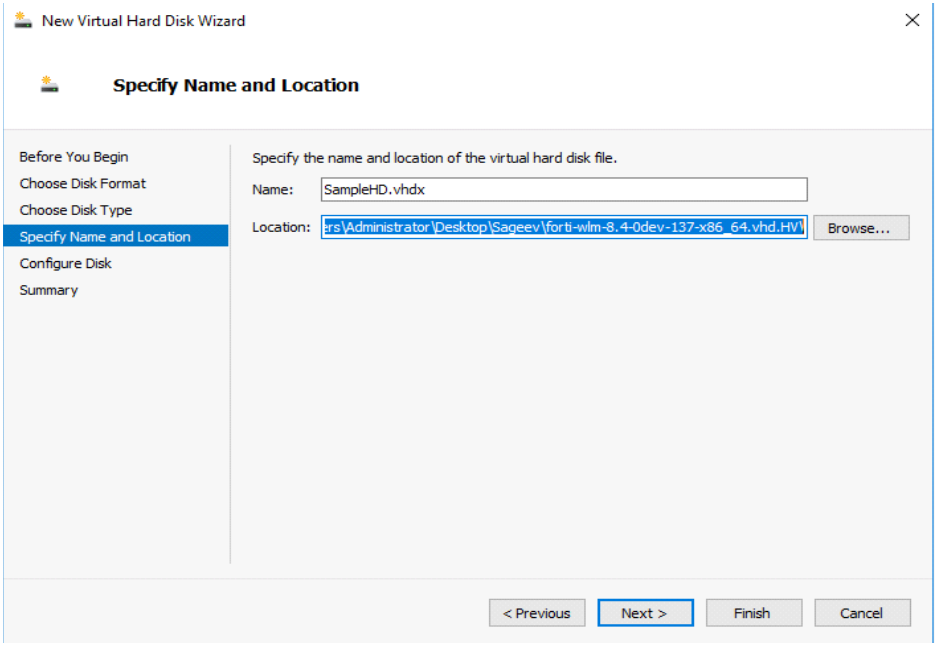
4. Select virtual disk format as **VHDX** and click **Next.**



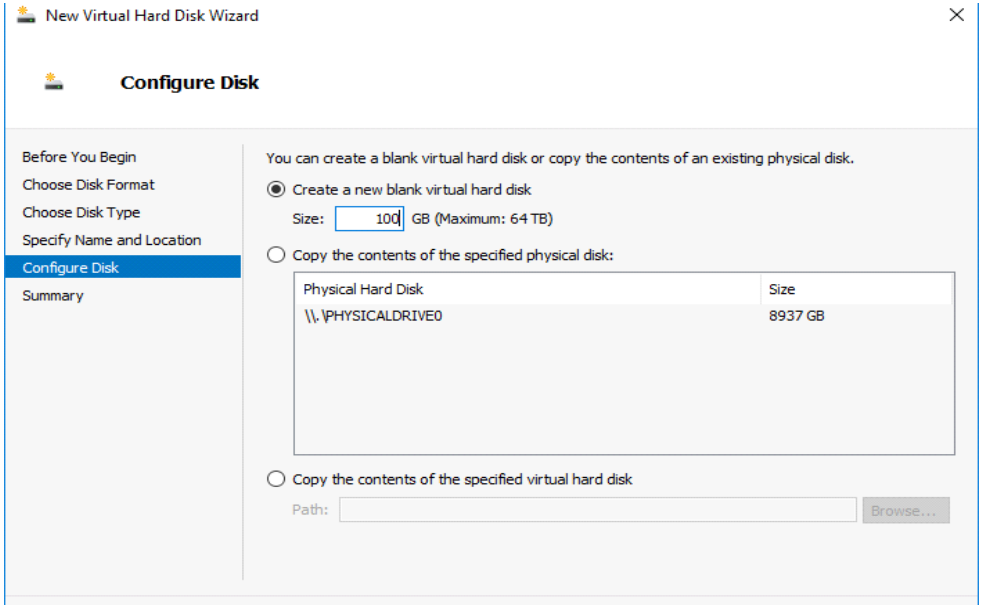
5. Select the disk type as **Dynamically Expanding** and click **Next.**



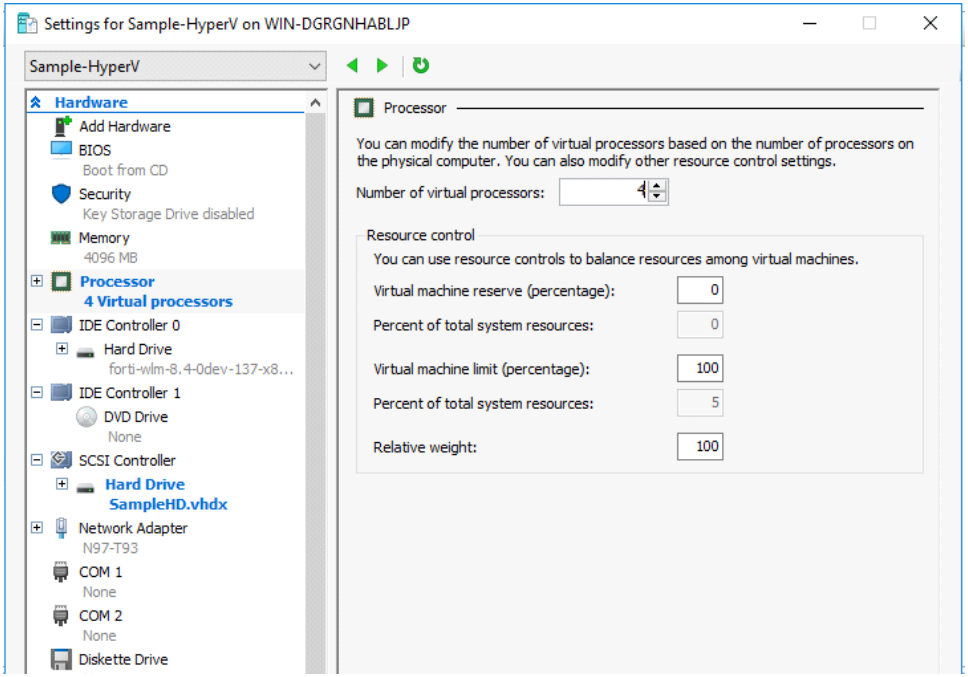
6. Enter the name of the disk and click **Browse** to specify the path to store the virtual disk.Click **Next.**



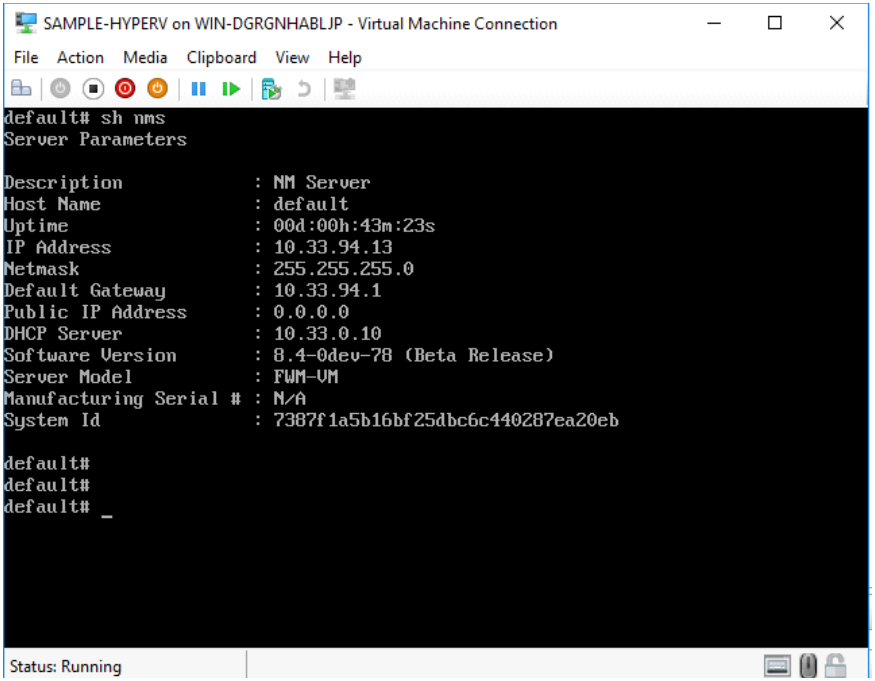
7. Enter the size of the disk. Minimum size is 100GB and click **Next**.



8. Select the **Processor** and enter the **Number of virtual processors** (minimum 4 processors).



9. Start the virtual machine and when the system is ready, run the **show nms** command.



Troubleshooting FortiWLM-Virtual Edition

The following table lists the common problems faced after installing *E(z)RF-Virtual Edition* with potential solutions. If your problem does not appear in the table or the solution provided doesn't remedy the situation, contact *Fortinet Technical Support* for further assistance.

Message	Possible Cause and Solution
Unable to connect to MKS: Virtual machine config file doesn't exist	This message can appear due to one of the following problems: The *vmx* files found missing in the datastore. Only *img*, *vmdf* and *vswp* files were existing. Solution: Restart the management services. Create another instance and restore the backup taken from the previous instance.

7 FortiWLM - Command Line Interface

FortiWLM can be accessed from the CLI using the IP address. You must have the access level Admin to use the CLI.

backup

Copies either both the NMS server statistics and configuration or just the configuration to the directory **/data/backup/nm**.

Syntax

backup all (NM, SAM, and SM)
backup config-only (NM Config only)

Command Mode

Global configuration

Default

Full backups are done daily by default.

Usage

Log in as *Admin* to do a *data/configuration or a configuration backup*. Backups are written to the directory */data/backup/nms* and have the naming convention Backup-yyyy-mm-dd-hr-mn-sec for *backup all* and Backup_configuration -yyyy-mm-dd-hr-mn-sec for **backup config-only**. By default, two complete backups and all configuration-only backups are saved; you can alter the number of complete backups that are saved.

This table indicates what is copied for a full backup versus a configuration backup:

Backing up requires 5GB of free disk space.

If you use this CLI **backup** command, the web UI backup details will also be updated (*Last Updated, Start Time and End Time columns)* in the GUI history.

There are two possible states for a completed backup: *passed* or *failed*. If a backup or restore fails, error messages are logged into the file */data/apps/nms/logs/backup.log* and a major alarm is raised for the backup failure. If a backup failed after reaching the maximum hard disk size, the backup entry is listed in the backup history table as failed. Also, a failure message is stored in the log backup_restore.log. View this log information using the command **show backup-restore-history** which displays the last 25 entries from the backup-restore-history table.

Example

This command performs a complete backup:

```
default# backup all


Backup is started. Backup may take several hours depending on system
   scale...

Started compressing backup...

Successfully backed up the data

default#
```

The command **show backup** lists the backup file (which includes time and date) and the size of the backup. For example. in this example, backups were done on March 21, 22, 23 of 2013:

```
EzRF1138# sh backup

Backup File Name                    Size(bytes)

Backup-2013-03-21-01-01-01.tar.gz    376035

Backup-2013-03-22-01-01-01.tar.gz    407017

Backup-2013-03-23-01-01-01.tar.gz    439965

EzRF1138#
```

This example uses **delete backup to** delete the backup named Backup-2013-03-05-01-01-01.tar.gz from the directory */data/backup/nms*:

```
default# delete backup Backup-2013-03-05-01-01-01.tar.gz
```

This command performs a back up of the configuration only:

```
default# backup config-only

Backup is started. Backup may take several hours depending on system
   scale...

Started compressing backup...

Successfully backed up the configuration

default#
```

Related Command

"restore" on page 552
"show" on page 558

calendar

Sets both the hardware clock of the appliance and the time for the NMS server.

Syntax

```
calendar set <MM/DD/YYYY> <hh:mm:ss>
```

Command Mode

Global configuration

Default

NA

Usage

Simultaneously sets both the hardware clock of the appliance and the time for the NMS server; requires a reboot.

Example

```
EzRFserver1148# calendar set ?

<MM/DD/YYYY>           Enter the date in MM/DD/YYYY to set the date.

EzRFserver1148# calendar set 02/21/2013 ?

<hh:mm:ss>             Enter the time in hh:mm:ss to set the clock.

EzRFserver1148# calendar set 02/21/2013 16:13:00

This command requires a controller reboot. Do you want to proceed [yes/no]

y
```

configure

Sets the admin and/or guest password in the appliance.

Syntax configure terminal

Command Mode Global configuration

Default admin

Usage This command is only used to set the admin and or guest password in the appliance.

Example

```
EzRFserver1148# configure terminal
EzRFserver1148 (config)# ?
end                    Exits global configuration mode.
exit                   Exits global configuration mode.
passwd                 Changes EXEC password.

EzRFserver1148 (config)# passwd admin
<CR>
EzRFserver1148 (config)# passwd admin
Changing password for user admin.
New password:
BAD PASSWORD: it is too short
Retype new password:
passwd: all authentication tokens updated successfully.
EzRFserver1148(config)#
```

copy

Copies files locally or remotely using either FTP or SCP commands.

Syntax

FTP syntax:

```
copy /data/apps/nms/logs/meru.gather.EzRF1138.2013-02-21.16-25-38.tar.gz
   ftp://<user name>@<destinationip>/<destination path>
```

SCP syntax:

```
copy /data/apps/nms/logs/meru.gather.EzRF1138.2013-02-21.16-25-38.tar.gz
   scp://<user name>@<destinationip>/<destination path>
```

FTP syntax to copy a backup file from a remote source to the appliance:

```
copy ftp://<username>@<ipaddress>/Backup-yyyy-mm-dd-hh-mm-ss.tar.gz /
   cdbackup
```

Command Mode

Global configuration

Default

NA

Usage

Copy files to/from the appliance, for example, backup files.

Example

This example gathers diagnostic data on an SA2000 and copies it to another location.

```
EzRF1148# diagnostics

Getting process information ...

Getting system log information ...

Getting kernel information ...

Getting network information ...

Getting software information ...

Getting version information ...

Getting disk information ...

Getting Meru data ...
```

```
Data gathering phase complete


/data/apps/nms/logs/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz created


Use the copy scp option of the CLI command to move this file off the
   machine. For example:

execute copy /data/apps/nms/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz
   scp://<user_name>@<destination_ipaddress><destination_path>


/data/apps/nms/logs/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz


EzRF1148# copy /data/apps/nms/logs/meru.gather.EzRF1148.2013-03-23.16-36-
   48.tar.gz scp://<user_name>@<destination_ipaddress><destination_path>
```

Related Command *"diagnostics" **on page 537***

crashdump

Command used by Fortinet support to view SA200 logs.

date

Displays today's date and time.

Syntax date

Command Mode Global configuration

Default NA

Usage Use this command to check the date and time that the appliance is using.

Example

```
default# date
Fri Feb  6 22:13:31 UTC 2013
```

default

Resets some appliance settings to default values.

Syntax

```
default {history | prompt | terminal}
```

history	Restores the history buffer size to the default value (**10**).
prompt	Restores the prompt string to the default value (**host name**).
terminal	Sets various terminal characteristics to the defaults.

Command Mode Global configuration

Default

Usage Use this command to reset the history buffer, command prompt, and terminal characteristics to default values.

Example This command resets the history buffer size to 10 commands and then shows the last 10 commands executed on the appliance.

```
default# default history

default# sh history

    3  configure

    4  configure

    5  configure terminal

    6  exit

    7  copy
```

```
 8  date
 9  debug server
10  debug controller
11  default history
12  sh history
```

delete

Deletes either a file, a backup, or a flash image.

Syntax

delete {<*filename*> | backup <*filename*>| flash <*image*>**| app-images** <*image*>**}**

filename	Name of the file to delete (requires directory information).
backup filename	Deletes named backup file from the directory /data/backup/nms.
flash image	X.X-NNN.
app-images	Deletes the application images.

Command Mode

Global configuration

Default

Usage

Use this command to delete a backup file or flash image.

Example

This example deletes a diagnostics file:

```
default# delete meru.user-diagnostics.EzRF1138.2013-03-03.10-40-03.tar.gz
```

This example deletes a backup image:

```
default# delete backup Backup-2013-03-04-01-01-02.tar.gz
```

This example deletes a flash image:

```
default# delete flash 2.0-141
```

This example deletes a application image:

```
default# delete app-images meru-nms-iphone-feature-1.0-7
```

diagnostics

Gathers NMS server diagnostics into a compressed file.

Syntax **`diagnostics`**

Command Mode Global configuration

Default NA

Usage Use this command to gather NMS server diagnostics into a compressed file. You can then move the file off of an appliance with either SCP or FTP **`copy`** commands:

```
copy /data/apps/nms/meru.gather.EzRF1138.2013-02-21.16-25-38.tar.gz ftp://
   <user_name>@<destination IP>/<destination path>

copy /data/apps/nms/meru.gather.EzRF1138.2013-02-21.16-25-38.tar.gz scp://
   <user_name>@<destination IP>/<destination path>
```

Example This example gathers diagnostic data on an SA2000 and copies it to another location.

```
EzRF1148# diagnostics

Getting process information ...

Getting system log information ...

Getting kernel information ...

Getting network information ...

Getting software information ...

Getting version information ...

Getting disk information ...

Getting Meru data ...

Data gathering phase complete
```

```
/data/apps/nms/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz created


Use the copy scp option of the CLI command to move this file off the
   machine


execute copy /data/apps/nms/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz
   scp://<user_name>@<destination IP><destination path>


/data/apps/nms/meru.gather.EzRF1148.2013-03-23.16-36-48.tar.gz


EzRF1148# copy /data/apps/nms/meru.gather.EzRF1148.2013-03-23.16-36-
   48.tar.gz scp://<user_name>@<destination IP><destination path>
```

Related Command

"copy" on page 533

dir

Displays directory contents.

Syntax

```
dir backup
dir images
dir platform-images
```

backup	List the contents of the directory containing backup, **/data/backup/nms**
images	List the contents of the directory present in the appliance, **/opt/meru/images**
platform-images	List the contents of the directory containing application images present in the appliance, **/data/platform/images**

Command Mode

Global configuration

Default

Usage

Use this command to display directory contents.

Example

This example displays the backup directory and then displays the images directory:

```
default# dir ?

<CR>

backup                  The directory containing the backup databases.

images                  The directory containing the system images.


default# dir backup

total 195580

-rw-r--r-- 1 root root  99023357 Mar 19 01:02 Backup-2013-03-19-13-31-
   01.tar.gz

-rw-r--r-- 1 root root 101009548 Mar 19 12:32 Backup-2013-03-20-01-01-
   01.tar.gz

-rw-r--r-- 1 root root      1196 Mar 19 12:32 backup_restore.log

drwxr-xr-x 2 root root     24576 Mar 19 12:32 daily_backup


default# dir images

total 136

drwxrwxr-x 5  522  522  4096 Mar 16 09:14 meru-2.0-156

drwxrwxr-x 5  522  522  4096 Mar 19 09:14 meru-2.0-157

-rw-r--r-- 1 root root 23654 Mar 14 11:31 meru.user-
   diagnostics.default.2013-03-14.11-31-09.tar.gz

-rw-r--r-- 1 root root 24062 Mar 16 11:03 meru.user-
   diagnostics.default.2013-03-16.11-03-21.tar.gz

-rw-r--r-- 1 root root 24902 Mar 18 22:58 meru.user-
   diagnostics.default.2013-03-19.11-28-02.tar.gz
```

```
-rw-r--r-- 1 root root 23560 Mar 19 11:36 meru.user-
   diagnostics.default.2013-03-20.00-06-54.tar.gz

-rw-r--r-- 1 root root 23625 Mar 19 13:25 meru.user-
   diagnostics.default.2013-03-20.01-55-51.tar.gz

-rw-r--r-- 1 root root     0 Mar 18 22:57 pre-upgrade-config

-rw-r--r-- 1 root root     0 Mar 20 10:08 script.log

-rw------- 1 root root  1712 Mar 18 22:57 upgrade.log

default#


default# dir platform-images

total 131900

-rwxr--r-- 1 root root 134912139 Dec 29 22:41 meru-4.1.SR1-7-VMC2000.img.gz

drwxr-xr-x 2  522 root      4096 Dec 31 15:40 meru-nms-iphone-feature-1.0-7

drwxr-xr-x 2  522 root      4096 Dec 31 17:05 meru-nms-wips-feature-1.0-35
```

enable

Enables privileged mode when you are in non-privileged mode.

Syntax

`enable <priv mode password>`

Command Mode

Global configuration

Default

By default, the appliance is already in privileged mode.

Usage

You need to be in privileged mode to enter config mode and use all of the commands. By default, the appliance is already in privileged mode. This command enables privileged mode if you have switched to non-privileged mode. **Enable** works only if you are logged in as admin; guest users cannot switch to privileged mode.

Example

These commands list the options (?) and then switch to privileged mode:

```
EzRF1138> ?
debug                   Turns on debugging.
default                 Reset to default values.
enable                  Enables privileged mode.
exit                    Exit the CLI.
help                    Displays help information.
no                      Disables various parameters.
prompt                  Customizes the CLI prompt.
quit                    Exit the CLI.
show                    Displays various system parameters.
terminal                Displays or sets terminal characteristics.
EzRF1138> enable *********
EzRF1138#
```

exit

Exit the CLI.

Syntax `exit`

Command Mode Global configuration

Default NA

Usage If you exit the CLI, you will have to log in again to execute commands.

Example `default# exit`

help

Displays help information.

Syntax help

Command Mode Global configuration

Default NA

Usage Use the help command to list all available commands with short descriptions.

Example

```
default# help
```

backup	Performs a backup of the nms-server data
calendar	Sets hardware clock and system time but requires a reboot
cd	Sets the current working directory.
certificate	Certificate Management on NM server.
configure	Enter global configuration mode
copy	Copies files locally or remotely
crashdump	Enable or disable crashdump feature, or list crashdumps
date	Displays today's date
default	Reset to default values
delete	Deletes a file from the file system
diagnostics	Gathers FortiWLM diagnostics in a compressed file
dir	Displays directory contents
enable	Enables privileged mode
exit	Exit the CLI
help	Displays help information
no	Disables various parameters
ping	Test network connectivity
poweroff	Power off the system
prompt	Customizes the CLI prompt
pwd	Displays the current working directory
quit	Exit the CLI
raid	RAID management commands
reload	Reboot the nms-server
reload-gui	Restart GUI services
restore	Restores the backed up data
setup	Performs initial setup
show	Displays various system parameters
snapshot	Create or restore a snapshot of the current flash
terminal	Displays or sets terminal characteristics
timezone	Sets the time zone of the system
traceroute	Test network connectivity

no

Disables various parameters such as debug.

Syntax

```
no <parameter>
```

`ntp-server`	Disables time synchronization and removes NTP server settings.
`prompt`	Disables the display of the CLI prompt.
`terminal`	Disable the history buffer for the current session.

Command Mode

Global configuration

Default

Usage

Use the **no** command in combination with the three parameters listed above to turn them off.

patch

Installs/uninstalls a patch on a released version.

Syntax

```
patch install <patch file name>
```

```
patch uninstall <patch file name>
```

Command Mode

Global configuration

Default

NA

Usage

- Specify the name of the downloaded patch (*.fwlm*) to be installed.
- Specify the name of the installed path (*.fwlm*) to be removed/uninstalled.

Example

```
patch install forti-8.5-0reldev-1-patch-TestPatch1_x86_64-generic-
   rpm.tar.fwlm

patch uninstall forti-8.5-0reldev-1-patch-TestPatch1_x86_64-generic-
   rpm.tar.fwlm
```

ping

Tests network connectivity for IPv4.

Syntax

```
ping <argument abbreviation>
```

Argument Abbreviation	Argument	Information
-L	loopback	Suppresses loopback of multicast packets. This flag only applies if the ping destination is a multicast address.
-c	count	Stops after sending count ECHO_REQUEST packets. With deadline option, ping waits for count ECHO_REPLY packets, until the timeout expires.
-i	interval	Waits interval seconds between sending each packet. The default is to wait for one second between each packet normally, or not to wait in flood mode. Only a superuser may set interval to values less than 0.2 seconds.
-w	deadline	Specifies a timeout, in seconds, before ping exits, regardless of how many packets have been sent or received. In this case, ping does not stop after the count packet is sent; it waits either for the deadline to expire, until count probes are answered, or for some error notification from the network.
-p	pattern	You can specify up to 16 pad bytes to fill out a packet you send. This is useful for diagnosing data-dependent problems in a network. For example, **-p ff** causes a sent packet to be filled with ones.
-s	packet size	Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.

-t	ttl	Sets the IP Time to Live.
-I	interface or server.(vlan tag)	Sets the source address to a specified interface address. Argument may be numeric IP address or name of device. When pinging IPv6 link-local address, this option is required.
-M	mtu discovery hint	Selects Path MTU Discovery strategy. The hint may be either **do** (prohibit fragmentation, even local one), **want** (do PMTU discovery, fragment locally when packet size is large), or **don't** (do not set DF flag).
-S	sndbuf	Sets socket sndbuf. If not specified, the default buffers not more than one packet.
-T	time stamp option	Sets special IP timestamp options. Timestamp option may be either **tsonly** (only timestamps), **tsandaddr** (timestamps and addresses) or **tsprespec host1 [host2 [host3 [host4]]]** (timestamp prespecified hops).
-Q	tos	Sets Quality of Service -related bits in ICMP datagrams. The tos can be either a decimal or hex number. Traditionally (RFC1349), these have been interpreted as: 0 for reserved (currently being redefined as congestion control), 1-4 for Type of Service and 5-7 for Precedence. Possible settings for Type of Service are: minimal cost: 0x02, reliability: 0x04, throughput: 0x08, low delay: 0x10. Multiple TOS bits should not be set simultaneously. Possible settings for special Precedence range from priority (0x20) to net control (0xe0). You must be root (CAP_NET_ADMIN capability) to use Critical or higher precedence value. You cannot set bit 0x01 (reserved) unless ECN has been enabled in the kernel. In RFC2474, these fields has been redefined as 8-bit Differentiated Services (DS), consisting of: bits 0-1 of separate data (ECN will be used, here), and bits 2-7 of Differentiated Services Code point (DSCP).

hop1 ...	A hop is an intermediate connection in a string of connections linking two network devices. Each time the packet is forwarded to the next router, a hop occurs.
destination	Destination is either the IP address or the host name.

Command Mode Global configuration

Default NA

Usage Use the **ping** command to test network connectivity.

Example

```
default# ping yahoo.com

PING yahoo.com (206.190.60.37) from 172.18.111.220 : 56(84) bytes of data.

64 bytes from w2.rc.vip.re4.yahoo.com (206.190.60.37): icmp_seq=1 ttl=49
   time=247 ms

64 bytes from w2.rc.vip.re4.yahoo.com (206.190.60.37): icmp_seq=2 ttl=49
   time=248 ms

64 bytes from w2.rc.vip.re4.yahoo.com (206.190.60.37): icmp_seq=3 ttl=49
   time=249 ms

64 bytes from w2.rc.vip.re4.yahoo.com (206.190.60.37): icmp_seq=4 ttl=49
   time=247 ms
```

ping6

Tests network connectivity for IPv6.

Syntax `ping6 <hostname>`

Command Mode Global configuration

Default NA

Usage Use the **ping6** command to test network connectivity.

Example

```
default# ping6 2001:470:ecfb:120::250

PING 2001:470:ecfb:120::250(2001:470:ecfb:120::250) from
   2001:470:ecfb:120:56ae:c82c:a1d8:5b12 bond0: 56 data bytes

64 bytes from 2001:470:ecfb:120::250: icmp_seq=1 ttl=128 time=0.505 ms

64 bytes from 2001:470:ecfb:120::250: icmp_seq=2 ttl=128 time=0.325 ms

64 bytes from 2001:470:ecfb:120::250: icmp_seq=3 ttl=128 time=0.344 ms

64 bytes from 2001:470:ecfb:120::250: icmp_seq=4 ttl=128 time=0.378 ms

64 bytes from 2001:470:ecfb:120::250: icmp_seq=5 ttl=128 time=0.385 ms

64 bytes from 2001:470:ecfb:120::250: icmp_seq=6 ttl=128 time=0.294 ms


--- 2001:470:ecfb:120::250 ping statistics ---

6 packets transmitted, 6 received, 0% packet loss, time 4999ms

rtt min/avg/max/mdev = 0.294/0.371/0.505/0.071 ms
```

poweroff nms-server

Powers off the NMS server gracefully.

Syntax `poweroff nms-server`

Command Mode Global configuration

Default NA

Usage Use the **poweroff nms-server** command to shut down the appliance.

Example

```
EzRF1138# poweroff nms-server

Are you sure you want to poweroff the nms-server [y|n]? y
```

```
Broadcast message from root (pts/0) (Tue Mar 24 15:05:37 2013):

The system is going down for system halt NOW!

EzRF1138#
```

Related Command

"reload" ***on page 551***
"reload-gui" ***on page 552***

prompt

Customizes the CLI prompt.

Syntax

```
prompt <prompt>
```

Command Mode

Global configuration

Default

The default prompt is **default**.

Usage

Use this command to change the CLI command prompt for the current session only.

Example

```
default# prompt ?

<prompt>                Enter the name of the prompt you want to display.

default# prompt MeruDemo

MeruDemo#
```

pwd

Displays the current working directory.

Syntax

```
pwd
```

Command Mode

Global configuration

Default By default, the path is directed to images in the directory system images.

Usage

Example

```
MeruDemo# pwd
images
MeruDemo#
```

quit

Exits the CLI.

Syntax

```
quit
```

Command Mode Global configuration

Default NA

Usage If you execute the command **quit**, you have to reconnect to the appliance CLI to use it again.

Example

```
default# quit
```

raid replace

Use this command on SA2000 only to replace a RAID drive and rebuild the array.

Syntax

```
raid replace {lower | upper}
```

lower	Disengage the lower appliance disk in preparation for removal.
upper	Disengage the upper appliance disk in preparation for removal.

Command Mode Global configuration

Default NA

Usage Use this command when you need to replace a disk in the RAID array of the appliance. Identify a failed hard disk with the command **`show raid`**.

if you execute this command on an appliance, it changes the appliance from running mode to degraded mode.

When a RAID array is under reconstruction, rebooting the server may lead to unpredictable result including loss of data.

Example

```
default# raid replace upper
```

reload

Reboots the E(z)RF server (similar to the safe reboot command)

Syntax **`reload`**

Command Mode Global configuration

Default NA

Usage Use this command to reboot the appliance.

Example

```
EzRF1138# reload nms-server

Are you sure you want to reboot [y|n]? y

Broadcast message from root (pts/0) (Tue Mar 24 15:14:51 2013):

The system is going down for reboot NOW!

EzRF1138#
```

Related Command

"poweroff nms-server" ***on page 548***
"reload-gui" ***on page 552***

reload-gui

Reloads the Web User Interface.

Syntax

```
reload-gui
```

Command Mode

Global configuration

Default

NA

Usage

use this command to recover the appliance from the error **system busy**. This restarts web service.

Example

```
default# reload-gui

default#
```

Related Command

"poweroff nms-server" ***on page 548***
"reload" ***on page 551***

restore

The **restore** command restores backups from the directory /data/backup/nms. Administrators can restore an entire backup or just the configuration with no statistics (config-only).

Syntax

```
#restore Backup<build>-<hostname>-<year>-<mm>-<dd>-<hr>-<min>-<sec>.tar.gz

#restore Backup_configuration-<build>-<hostname>-<year>-<mm>-<dd>-<hr>-
   <min>-<sec>.tar.gz
```

Command Mode

Global Configuration

Default

All backups are stored in the directory **/data/backup/nms**.

Usage

The **restore backup** version of the command restores all data that was backed up (maps, nmsdb, eventdb, reports, controller details, alarms, statistics) when the backup was done with **backup all**. The **restore backup config only** version of the command restores only the configuration when the backup was done with **backup all**. When the backup was done with **backup-config-only**, the configuration is restored.

Restoring a particular table in the database is not supported. To restore a backup from an external location, use the copy command to copy the file to the appliance, then use the restore command. For example, to copy using ftp:

```
EzRF1138# copy ftp ://<username >@<ipaddress>/Backup-2013-03-04-01-01-
   02.tar.gz /data/backup/nms/
```

Examples

To recover the full backup done December 13th from the backup folder **/data/backup/nms**, use this command:

```
default# restore Backup-2.1-70-SA2000-2013-12-13-01-01-01.tar.gz
```

To recover only the configuration from a backup done December 9th, use this command:

```
default# restore Backup_configuration-2.1-70-SA2000-2013-12-09-18-16-
   34.tar.gz
```

Related Command

"backup" on page 529
"copy" on page 533

reload default factory

The **reload default factory** command resets the FortiWLM device to its last installed build. All configurations and settings are erased.

- **Note:**
  Configurations pushed to controllers and APs are retained on those devices after factory reset on FortiWLM.
- Fortinet recommends that you have console access while applying the factory default settings on SA2000; you are prompted to confirm (Y) creating an array to proceed with the reset.

Caution:
Fortinet recommends that you take a backup of any data before doing a factory reset. Factory reset will erase all existing data from your device.

Syntax

```
#reload default factory
```

Command Mode Global Configuration

Default NA

Usage Ensure the following before performing the factory reset:

- Ensure that you have console access to your device.
- Disable HA.

Example

```
default# reload default factory
default#
```

Related Command

"backup" ***on page 529***

"copy" ***on page 533***

setup

Run **`setup`** for initial services appliance setup, or to add controllers to FortiWLM, or to change the IPv4 and IPv6 address assignment configurations.

Syntax **`setup`**

Command Mode Global configuration

Default NA

Usage Run the **`setup`** command to initialize the appliance for first-time use and to change the following settings after setup: appliance name, NTP server, host name, IPv4 address, DHCP, time, DNS, NTP server settings, admin, guest passwords, and the following IPv6 address assignment options:

- Auto configuration (all configuration from router advertisements)
- DHCPv6
- Statically assigned addresses (global and/or link local scope)

Example This example sets up the static IP, NAT server, DNS server, and Time zone in the appliance.

```
FortiWLM# setup
```

```
Begin system configuration...

Host Name configuration for this machine

Current hostname is EzRF1148

Would you like to change the hostname [yes/no/quit]?: n

Currently default password is used for admin

Would you like to change the password [yes/no/quit]?: y

Changing password for user admin.

New password:

BAD PASSWORD: it is too short

Retype new password:

passwd: all authentication tokens updated successfully.

Currently default password is used for guest

Would you like to change the password [yes/no/quit]?: y

Changing password for user guest.

New password:

BAD PASSWORD: it is too short

Retype new password:

passwd: all authentication tokens updated successfully.

IP configuration for this machine.

Would you like to configure networking [yes/no/quit]?: y

Would you like to use Dynamic IP configuration (DHCP) [yes/no/quit]?: n

Please enter the IP configuration for this machine.

Each item should be entered as an IP version 4 style address in dotted-
   decimal notation (for example, 10.20.30.40)

Enter IP address, or q to quit: 172.18.114.8

Is 172.18.114.8 correct [yes/no/quit]?: y
```

```
Enter netmask, or q to quit: 255.255.255.0
Is 255.255.255.0 correct [yes/no/quit]?: y
Enter default gateway (IP), or q to quit: 172.18.114.1
Is 172.18.114.1 correct [yes/no/quit]?: y
Would you like to configure a Domain Name Server [yes/no/quit]?: y
Domain Name Server (DNS) configuration for this machine.
Enter one or more DNS name servers.
For this prompt only use q when finished entering name servers.
Enter Name Server IP Address, or q to quit: 1.1.1.1
Is 1.1.1.1 correct [yes/no/quit]?: y
Enter Name Server IP Address, or q to quit: q
Please enter DNS domain name, or q to quit: fortinet.com
Is fortinet.com correct [yes/no/quit]?: y
The time is now Fri Jun  5 19:03:05 UTC 2013
Would you like to change the time zone for this machine [yes/no/quit]?: y
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
```

```
10) Pacific Ocean

11) none - I want to specify the time zone using the Posix TZ format.

#? 5

Please select a country.

1) Afghanistan           11) East Timor           21) Kazakhstan
   31) Myanmar (Burma)       41) Sri Lanka

2) Armenia               12) Georgia              22) Korea (North)
   32) Nepal                 42) Syria

3) Azerbaijan            13) Hong Kong            23) Korea (South)
   33) Oman                  43) Taiwan

4) Bahrain               14) India                24) Kuwait
   34) Pakistan              44) Tajikistan

5) Bangladesh            15) Indonesia            25) Kyrgyzstan
   35) Palestine             45) Thailand

6) Bhutan                16) Iran                 26) Laos
   36) Philippines           46) Turkmenistan

7) Brunei                17) Iraq                 27) Lebanon
   37) Qatar                 47) United Arab Emirates

8) Cambodia              18) Israel               28) Macau
   38) Russia                48) Uzbekistan

9) China                 19) Japan                29) Malaysia
   39) Saudi Arabia          49) Vietnam

10) Cyprus               20) Jordan               30) Mongolia
   40) Singapore             50) Yemen


#? 14

The following information has been given:

India

The name of the time zone is 'Asia/Calcutta'.

Is the above information OK?

1) Yes
```

```
2) No

#? 1

The following command is the alternative way of selecting the same time
   zone

timezone set Asia/Calcutta

Set system time for this machine.

Synchronize time with a Network Time Protocol (NTP) server [yes/no/quit]?:
   y

Please enter the name or IP address of an NTP server, or q to quit: 1.1.1.1

Is 1.1.1.1 correct [yes/no/quit]?: y

System configuration completed.


Do you want to commit your changes and reboot [yes/no/quit]?: y

Broadcast message from root (pts/0) (Sat Jun  6 00:33:36 2013):

Now rebooting system...

The system is going down for reboot NOW!
```

In order to configure NTP Host Name, the user needs to set the DNS Server.

show

Displays various system parameters.

Syntax

show <*parameter*>

`arp`	Displays ARP table with IP-MAC address mappings
`backup`	Displays backed up directories
`backup-restore-history`	Displays the last 25 entries in the backup-restore-history table.

`calendar`	Displays hardware clock
`crashdump`	Displays SA200 crash file
`debug`	Displays the debug information
`features`	Displays added applications such as Service Assurance Manager
`file system`	Displays information about the file system
`flash`	Displays system image filenames in flash memory
`history`	Displays contents of the history buffer
`hostname`	Displays host name
`ip`	Displays IPv4 addresses assigned to the FortiWLM, default gateway, DNS servers, DHCP server, and domain details.
`ip6`	Displays IPv6 addresses assigned to the FortiWLM, default gateway, DNS servers, and domain details.
`ipv6-neighbor`	Displays the IPv6 neighbor table.
`memory`	Displays memory used by running processes
`nms`	Displays nms configuration
`ntp-server`	Displays NTP server used for time synchronization

`patch`	Displays the patch details. The following are supported:
	`show patch`
	`show patch content <patch filename>`
	`show patch detail <patch filename>`
	`show patch history`
	`show patch verify <patch filename>`
	`show patch installed`

`raid`	Displays RAID status
`snapshot`	Displays the time and date of flash backup created with the command **`snapshot`**
`terminal`	Displays terminal settings
`timezones`	Displays valid time zone names

Command Mode

Global configuration

Default

NA

Usage

Use this command to display the various information listed above.

Example

This example displays memory used by running processes:

```
default# show memory
MemTotal:      8308116 KB
MemFree:       3179376 KB
Buffers:        173892 KB
Cached:        4687724 KB
SwapCached:          0 KB
Active:        4913624 KB
Inactive:       108524 KB
HighTotal:     7469568 KB
HighFree:      2614564 KB
LowTotal:       838548 KB
LowFree:        564812 KB
SwapTotal:           0 KB
SwapFree:            0 KB
Dirty:             864 KB
Writeback:           0 KB
AnonPages:       59384 KB
Mapped:         148508 KB
Slab:            92120 KB
PageTables:       4740 KB
NFS_Unstable:        0 KB
Bounce:              0 KB
CommitLimit:   4154056 KB
```

```
Committed_AS:   583356 KB

VmallocTotal:   118776 KB

VmallocUsed:       956 KB

VmallocChunk:   117540 KB

HugePages_Total:     0

HugePages_Free:      0

HugePages_Rsvd:      0

Hugepagesize:     2048 KB

default#
```

This example lists the last 25 entries in the log backup_restore.log:

```
EzRF1138# show backup-restore-history

2013-03-18 20-31-46        backup    Successfully taken the server backup
   in file "Backup-2013-03-18-20-30-08.tar.gz"

2013-03-18 20-32-03        backup    Successfully taken the server backup
   in file "Backup-2013-03-18-20-31-50.tar.gz"

2013-03-18 20-32-20        delete    Deleted the backup file "Backup-2013-
   03-18-20-30-08.tar.gz"

2013-03-19 01-01-14        backup    Successfully taken the server backup
   in file "Backup-2013-03-19-01-01-01.tar.gz"

2013-03-19 12-35-43       restore    Restored the server data from the
   backup file "Backup-2013-03-18-20-31-50.tar.gz"

2013-03-19 15-54-06       restore    Restored the server data from the
   backup file "Backup-2013-03-19-01-01-01.tar.gz"

2013-03-20 01-01-01        backup    Backup failed. Available disk space is
   low!. 7(GB) available from 247(GB) total.

2013-03-21 01-30-39        backup    Successfully taken the server backup
   in file "Backup-2013-03-21-01-29-28.tar.gz"

2013-03-21 01-30-39        delete    Deleted the backup file "Backup-2013-
   03-18-20-31-50.tar.gz" on backup limit exceeded
```

```
2013-03-21 01-34-21        backup    Successfully taken the server backup
   in file "Backup-2013-03-21-01-34-09.tar.gz"

2013-03-20 20-09-19        backup    Successfully taken the server backup
   in file "Backup-2013-03-20-20-09-04.tar.gz"
```

snapshot

Copies or restores a snapshot of the flash to/from the services appliance disk.

Syntax

snapshot {create | restore | delete}

`create`	Creates a snapshot of the existing [primary or mirror] partition
`restore`	Restores the snapshot into the other partition
`delete`	Deletes the snapshot of the other partition

To **view** all the snapshot execute **`show snapshot`**

```
EzRFScale# show snapshot

snapshot.2.1-116.15:17-07-08-2013

snapshot.2.1-106.01:00-04-18-2013
```

To **delete** the snapshot execute **`snapshot delete`**

```
EzRFScale# snapshot delete

snapshot.2.1-106.01:00-04-18-2013

snapshot.2.1-106.01:00-04-18-2013 deleted.
```

Command Mode

Global configuration

Default

NA

Usage

Use this command for flash backup and recovery to/from the services appliance disk. You can recover primary flash from either mirrored flash or from this backup that you created with snapshot. (Note that the snapshot cannot be copied off of the services appliance.) If you

upgrade the services appliance, you cannot use the flash backup snapshot feature. The Snapshot works on SA200, SA250 and SA2000.

Example

This example creates a snapshot:

```
default# snapshot create

--- System Snapshot Utility ---

Snapshot function:          CREATE

Last snapshot was created:  <No valid snapshot exists yet>

Active partition is:        /dev/hda2

Source partition is:        /dev/hda2

Destination partition is:   /dev/hda3


*> The snapshot process disables all system services for up to 20 minutes!
   <*

Are you sure you want to proceed? [y/n]
```

This example restores a snapshot when the primary flash is corrupted:

```
default# snapshot restore snapshot.16:00-04-05-2013

You booted from the primary partition.

This command will copy the snapshot image snapshot.16:00-04-05-2013 to the
   mirror partition.

During snapshot, services will continue to run, but you will not be able to
   run other commands on this console and system performance will be
   reduced.

It is recommended to run this command during off-peak hours.

Do you want to proceed? [y/n] y

Copying Data:  ######

Operation completed successfully.
```

tcpdump

Captures the network packets and prints the content to a readable format. It can read packets from a network interface card or from a saved packet capture file.

Syntax

tcpdump {-i | -r | -w} <*value*>

-i	Specifies the network interface on which the packet capture must be applied. Enter a valid network interface name. For example: eth0, eth1
-r	Specifies the saved capture file which needs to be processed by **tcpdump**. Enter the absolute path of captured **pcap/cap** file names.
-w	Specifies the path name of the file on which the captured packets must be dumped. Enter a file name file appropriate **cap/pcap** extension.

Command Mode

Global configuration

Default

NA

Usage

This command prints the network traffic with respect to the specified interface and dumps them in to capture files.

Example

This command captures the traffic across the interface eth0 and prints them on the terminal.

```
default# tcpdump -i eth0

tcpdump: WARNING: eth0: no IPv4 address assigned

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes

06:50:32.332363 IP default.ssh > win7-vparama.fortinet.com.49286: P
   1629843522:1629843622(100) ack 2480788854 win 138

06:50:32.332553 IP win7-vparama.fortinet.com.49286 > default.ssh: . ack 100
   win 251

06:50:32.332965 IP default.57718 > india-snow.fortinet.com.domain:  15506+
   PTR? 41.10.16.172.in-addr.arpa. (43)
```

```
06:50:32.333972 IP default.ssh > win7-vparama.fortinet.com.49286: P
   100:296(196) ack 1 win 138

06:50:32.334649 IP india-snow.fortinet.com.domain > default.57718:  15506*
   1/0/0 (86)

06:50:32.335001 IP default.44653 > india-snow.fortinet.com.domain:  37771+
   PTR? 7.0.16.172.in-addr.arpa. (41)
   This command sets the size of the terminal history buffer:
```

This command captures the traffic across the interface eth0 and writes into a pcap file /root/capeth0.pcap

```
default# tcpdump -i eth0 -w /root/capeth0.pcap

tcpdump: WARNING: eth0: no IPv4 address assigned

tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96
   bytes
```

This command reads the saved capture file /root/capeth0.pcap and prints it in a readable form in the terminal

```
default# tcpdump -r /root/capeth0.pcap

reading from file /root/capeth0.pcap, link-type EN10MB (Ethernet)

06:52:53.280228 IP default.ssh > win7-vparama.fortinet.com.49286: P
   1629949234:1629949334(100) ack 2480790470 win 138

06:52:53.281791 IP default.ssh > win7-vparama.fortinet.com.49286: P
   100:232(132) ack 1 win 138

06:52:53.281972 IP win7-vparama.fortinet.com.49286 > default.ssh: . ack 100
   win 253

06:52:53.353649 arp reply 172.18.198.210 is-at 00:90:0b:1a:f0:4f (oui
   Unknown)

06:52:53.481885 IP win7-vparama.fortinet.com.49286 > default.ssh: . ack 232
   win 252

06:52:53.780792 arp reply 172.18.198.47 is-at 00:90:0b:28:82:a7 (oui
   Unknown)

06:52:53.813046 arp reply 172.18.198.200 is-at 00:10:f3:28:70:42 (oui
   Unknown)
```

```
06:52:54.679916 ec:9a:74:c2:a3:62 (oui Unknown) > 09:00:09:09:13:a6 (oui
   Unknown), ethertype Unknown (0x88b7), length 66:

       0x0000:  0040 7f51 000f ec9a 74c2 a360 8648 fd4b  .@.Q....t..`.H.K

       0x0010:  a667 5c83 4176 1df8 7b20 8aca 77f4 5519  .g\.Av..{...w.U.

       0x0020:  0800 0900 0302 0000 0000 0000 0000 0000  ................

       0x0030:  a85b b197                                .[..
```

terminal

Displays or sets terminal characteristics history, length, and width.

Syntax

terminal {history | length | width) <*value*>

history	Displays or sets the size of the terminal history buffer. Enter a value from 0 to 1000.
length	Sets the number of rows for the termina**l**. Enter a value from 0 to 256.
width	Sets the number of columns for the terminal. Enter a value from 1to 1024.

Command Mode

Global configuration

Default

NA

Usage

This command changes terminal history, row length or row width if a value is provided and displays the current settings if no value is provided.

Example

This command displays the terminal history.

```
default# terminal history

    1  raid

    2  show memory

    3  snapshot

    4  snapshot create
```

This command sets the size of the terminal history buffer:

```
default# terminal history 25
```

timezone

Sets the time zone of the system.

Syntax

timezone menu
timezone set <*zone*>

menu	Sets the appliance to a time zone by asking a series of questions
set	Sets the appliance to the time zone named (see list below)

Command Mode

Global configuration

Default

America/Los_Angeles

Usage

Sets the time zone of the system to the specified zone: Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Tripoli, Africa/Tunis, Africa/Windhoek, America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, America/Aruba, America/Asuncion, America/Atikokan, America/Bahia, America/Barbados, America/Belem, America/Belize, America/Blanc-Sablon, America/Boa_Vista, America/Bogota, America/Boise, America/Buenos_Aires, America/Cambridge_Bay, America/Campo_Grande, America/Cancun, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Chihuahua, America/Cordoba, America/Costa_Rica, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunepe, America/El_Salvador, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/

Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Hermosillo, America/Indiana/Indianapolis, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Petersburg, America/Indiana/Vevay, America/Indiana/Vincennes, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/Kentucky/Louisville, America/Kentucky/Monticello, America/La_Paz, America/La_Rioja, America/Lima, America/Los_Angeles, America/Maceio, America/Managua, America/Manaus, America/Martinique, America/Mazatlan, America/Mendoza, America/Menominee, America/Merida, America/Mexico_City, America/Miquelon, America/Moncton, America/Monterrey, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/North_Dakota/Center, America/North_Dakota/New_Salem, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port_of_Spain, America/Porto_Velho, America/Puerto_Rico, America/Rainy_River, America/Rankin_Inlet, America/Recife, America/Regina, America/Rio_Branco, America/Rio_Gallegos, America/San_Juan, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund, America/Shiprock, America/St_Johns, America/St_Kitts, America/St_Lucia, America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa, America/Thule, America/Thunder_Bay, America/Tijuana, America/Toronto, America/Tortola, America/Tucuman, America/Ushuaia, America/Vancouver, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife, Antarctica/Casey, Antarctica/Davis, Antarctica/DumontDUrville, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/Rothera, Antarctica/South_Pole, Antarctica/Syowa, Antarctica/Vostok, Arctic/Longyearbyen, Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Ashgabat, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Choibalsan, Asia/Chongqing, Asia/Colombo, Asia/Damascus, Asia/Dhaka, Asia/Dili, Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Harbin, Asia/Hong_Kong, Asia/Hovd, Asia/Irkutsk, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Katmandu, Asia/Krasnoyarsk, Asia/Kuala_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macau, Asia/Magadan, Asia/Makassar, Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novosibirsk, Asia/Omsk, Asia/Oral, Asia/Phnom_Penh, Asia/Pontianak, Asia/Pyongyang, Asia/Qatar, Asia/Qyzylorda, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Sakhalin, Asia/Samarkand, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Thimphu, Asia/Tokyo, Asia/Ulaanbaatar, Asia/Urumqi, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan, Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Faeroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley, Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Currie, Australia/Darwin, Australia/Hobart, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/Perth, Australia/Sydney, Europe/Amsterdam, Europe/Andorra, Europe/Athens, Europe/Belgrade, Europe/Berlin, Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest, Europe/Chisinau, Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Guernsey, Europe/Helsinki, Europe/Isle_of_Man, Europe/Istanbul, Europe/Jersey, Europe/Kaliningrad, Europe/Kiev, Europe/Lisbon, Europe/Ljubljana, Europe/London, Europe/Luxembourg, Europe/Madrid,

Europe/Malta, Europe/Mariehamn, Europe/Minsk, Europe/Monaco, Europe/Moscow, Europe/Oslo, Europe/Paris, Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara, Europe/San_Marino, Europe/Sarajevo, Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Uzhgorod, Europe/Vaduz, Europe/Vatican, Europe/Vienna, Europe/Vilnius, Europe/Volgograd, Europe/Warsaw, Europe/Zagreb, Europe/Zaporozhye, Europe/Zurich, Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte, Indian/Reunion, Pacific/Apia, Pacific/Auckland, Pacific/Chatham, Pacific/Easter, Pacific/Efate, Pacific/Enderbury, Pacific/Fakaofo, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Ponape, Pacific/Port_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis

Example

This example uses menus to set the timezone to Americas > United States > pacific Time. The driveline command is listed at the end of the example.

```
default# Tilimsen menu

Please identify a location so that time zone rules can be set correctly.

Please select a continent or ocean.

 1) Africa

 2) Americas

 3) Antarctica

 4) Arctic Ocean

 5) Asia

 6) Atlantic Ocean

 7) Australia

 8) Europe

 9) Indian Ocean

10) Pacific Ocean

11) none - I want to specify the time zone using the Posix TZ format.

#? 2
```

```
Please select a country.

 1) Anguilla              18) Ecuador              35) Paraguay
 2) Antigua & Barbuda     19) El Salvador          36) Peru
 3) Argentina             20) French Guiana        37) Puerto Rico
 4) Aruba                 21) Greenland            38) St Kitts & Nevis
 5) Bahamas               22) Grenada              39) St Lucia
 6) Barbados              23) Guadeloupe           40) St Pierre &
    Miquelon
 7) Belize                24) Guatemala            41) St Vincent
 8) Bolivia               25) Guyana               42) Suriname
 9) Brazil                26) Haiti                43) Trinidad & Tobago
10) Canada                27) Honduras             44) Turks & Caicos Is
11) Cayman Islands        28) Jamaica              45) United States
12) Chile                 29) Martinique           46) Uruguay
13) Colombia              30) Mexico               47) Venezuela
14) Costa Rica            31) Montserrat           48) Virgin Islands (UK)
15) Cuba                  32) Netherlands Antilles 49) Virgin Islands (US)
16) Dominica              33) Nicaragua
17) Dominican Republic    34) Panama
#? 45
Please select one of the following time zone regions.
 1) Eastern Time
 2) Eastern Time - Michigan - most locations
 3) Eastern Time - Kentucky - Louisville area
 4) Eastern Time - Kentucky - Wayne County
 5) Eastern Time - Indiana - most locations
```

```
 6) Eastern Time - Indiana - Crawford County

 7) Eastern Time - Indiana - Starke County

 8) Eastern Time - Indiana - Switzerland County

 9) Central Time

10) Central Time - Indiana - Daviess, Dubois, Knox, Martin, Perry & Pulaski
    Counties

11) Central Time - Indiana - Pike County

12) Central Time - Michigan - Dickinson, Gogebic, Iron & Menominee Counties

13) Central Time - North Dakota - Oliver County

14) Central Time - North Dakota - Morton County (except Mandan area)

15) Mountain Time

16) Mountain Time - south Idaho & east Oregon

17) Mountain Time - Navajo

18) Mountain Standard Time - Arizona

19) Pacific Time

20) Alaska Time

21) Alaska Time - Alaska panhandle

22) Alaska Time - Alaska panhandle neck

23) Alaska Time - west Alaska

24) Aleutian Islands

25) Hawaii

#? 19

The following information has been given:


        United States

        Pacific Time
```

```
The name of the time zone is 'America/Los_Angeles'.

Is the above information OK?


Please enter 1 for Yes, or 2 for No.

#? 1


The following command is the alternative way of selecting the same time
   zone


        timezone set America/Los_Angeles


The time zone is succesfully set

default#
```

traceroute

Tests network connectivity.

Syntax traceroute <*hostname*>

Hostname refers to any controller or network IP address.

Command Mode Global configuration

Default

Usage Check network connectivity with this command.

Example

```
EzRF1138# traceroute 172.18.112.4

traceroute to 172.18.112.4 (172.18.112.4), 30 hops max, 40 byte packets
```

```
1  172.18.113.1 (172.18.113.1)  1.201 ms  2.049 ms  2.035 ms

2  172.18.112.4 (172.18.112.4)  1.030 ms  1.039 ms  1.026 ms
```

traceroute6

This command traces the path of the packets to a specific destination.

Syntax

```
traceroute6 <hostname>
```

Command Mode

Global configuration

Default

NA

Usage

Use this command to obtain the IP address and status for all routers between the FortiWLM and a specified remote destination. Instead of a hostname, you can alternatively specify a domain name instead of an IP address or a hostname.

Example

```
FortiWLM# traceroute6 2001:470:ecfb:120::250

traceroute to 2001:470:ecfb:120::250 (2001:470:ecfb:120::250) from
   2001:470:ecfb:138:20c:29ff:fe11:9233, 30 hops max, 24 byte packets

1  2001:470:ecfb:138::1 (2001:470:ecfb:138::1)  0.416 ms  0.266 ms  0.177
   ms

2  2001:470:ecfb:3e0::1 (2001:470:ecfb:3e0::1)  0.256 ms  0.302 ms  0.235
   ms

3  2001:470:ecfb:3e1::2 (2001:470:ecfb:3e1::2)  0.265 ms  0.303 ms  0.269
   ms

4  2001:470:ecfb:120::250 (2001:470:ecfb:120::250)  0.349 ms  0.396 ms
   0.344 ms
```

nms-server unregister (controller command)

Issue this command from a controller to remove or add the controller from/to E(z)RF.

Syntax

```
nms-server unregister
nms-server register
```

Command Mode

Global configuration

Default

NA

Usage

nms-server unregister unregisters the controller from the server and is only executable from the controller CLI. Once you unregister the controller from the server, the controller goes into an offline inactive state.

Once the controller is no longer managed by FortiWLM (nms server), all profiles are owned by the controller and you can edit or delete any profile from the controller, including E(z)RF created profiles. To register a controller, use the command **register**.

Example

This example unregisters the controller 192.168.143.27 then registers it again. Log on to controller 192.168.143.27 and issue these commands:

```
EzRF10121 # configure terminal

EzRF10121(config)# nms-server unregister 192.168.143.27

SUCCESS: Unregister is complete

EzRF10121(config)#

example for nms-server register

EzRF10121(config)# nms-server register  1 192.168.143.27 34 2.1-3.6.1-A-70

SUCCESS: Register is complete
```

upgrade nms-server

Upgrades the appliance to the version indicated.

Syntax

upgrade nms-server <*version*>

Version will have the format 2.0-159.

Command Mode Global configuration

Default NA

Usage Upgrade the appliance to a new firmware build with this command.

Example

```
EzRF1138# upgrade server 2.0-159

This will overwrite all existing system images. Are you sure [y|n]? y

Current Version is 2.0-151

Upgrading Server

Stopping Meru services...

Stopping WLAN services:  [################################] Upgrading the
   current configuration.  This may take a while.  Please be patient ...

Removing startup database.

Removing running database.

Starting upgrade: ##

Installing base RPMs: ##############################################

Installing meru-common-2.0-1.i386.rpm: ######

Installing meru-kernel-2.0-1.i386.rpm: ##############################

Installing meru-nms-agent-2.0-1.i386.rpm: ###

Installing meru-nms-server-2.0-1.i386.rpm: #######

Installing meru-wnc-2.0-1.i386.rpm: ######

Installing meru-wnc-key-2.0-1.i386.rpm: ###

Installing meru-wnc-nms-2.0-1.i386.rpm: ##########################

Transition nmsdb to current schema...

Starting postgresql...OK

Current nmsdb database version is 2 ...
```

```
Beginning transition to version 3 ...
Performing upgrade to version 3 ...
Database transition complete!
Stopping postgresql...OK
Transition eventdb to current schema...
Starting postgresql...OK
eventdb is already up-to-date with version 3.
Stopping postgresql...OK
Upgrade complete.

Broadcast message from root (pts/1) (Tue Mar 24 12:34:32 2013):
Now rebooting system...
The system is going down for reboot NOW!

EzRF1138#
```

A Appendix - Using FortiWLM

Troubleshooting FortiWLM

The following are troubleshooting tips for *FortiWLM*.

#	Problem description	Troubleshooting Tips
1.	How to recover the appliance from the degraded mode	**Root cause:** Degraded mode indicates that one of the hard disks in the appliance failed. **Troubleshooting**: Identify the failure hard disk by the RAID status alarm. In CLI use RAID replace <upper/lower> depending on which hard disk has failed. -> Power off nms-server. -> Replace the failure hard disk. -> Power on appliance. After reloading the appliance, the RAID process will restart and the RAID state will be **recover mode**.
2.	How can I check the details of the appliance like IP address, S/W version details and uptime?	**Troubleshooting**: You have two options. Log in to the appliance and type the command **`sh nms`** in the appliance, or navigate to *Administration* > *System Settings* > *Server details* in the web UI.

#	Problem description	Troubleshooting Tips
3.	Server details are not displayed in the appliance when this command is issued: **`appliancetesting# sh nms`** You see the message: *Unable to establish communication with configuration server.*	**Root cause:** Some of the services might not be started in the appliance. **Recover procedure:** Reboot the appliance using the command **`reload nms-server`**
4.	When loading a new image onto the SA2000, a controller already added to FortiWLM has an upgrade failure.	**Root cause:** SSH is blocked when a different version of the image is loaded on the FortiWLM SA2000 server. **Troubleshooting:** Delete the known hosts in FortiWLM SA2000 server and the controller in the path: **/root/.ssh/known_hosts** Re-add the controller from the web UI. **Note:** This requires root intervention.
5.	If the administrative state of a controller is inactive, it indicates that discovery is not successful. For example, if you select the controller from inventory and then click **Settings**, the discovery state is **DISCOVERY_STATUS_UPGRADE_FAILURE**.	**Root cause:** Controller may be in the process of being upgraded. **Troubleshooting:** Either delete and add the controller or wait and try discovery again.

#	Problem description	Troubleshooting Tips
6.	The discovery state is **DISCOVERY_STATUS_IN_PROGRESS**.	**Root cause:** Either the discovery process has hung or the link is too slow. **Troubleshooting:** Execute the **reload** `nms-server` command from IOCLI.
7.	The discovery state is **DISCOVERY_STATUS_KEEP-ALIVES_MISSED**	**Root cause:** Either the FortiWLM agent is not running or discovery is not receiving a keep alive message from FortiWLM agent on the controller. **Troubleshooting:** Verify the status of Agent by executing the command **`SHOW NMS-SERVER`** on controller. The result should indicate **connected**.
8.	The Management server message says**UNSUPPORTED_CONTROLLER_ERSION**	**Root cause:** Controller version is not supported by FortiWLM. **Troubleshooting:** Upgrade the FortiWLM to a compatible software version that supports the System Director.

#	Problem description	Troubleshooting Tips
9.	If the discovery state is **"DISCOVERY_STATUS_CONTROLLER_VERSION_NOT_FOUND"**	**Root cause:** Discovery process failed to obtain the controller version. **Troubleshooting:** Verify that you can SSH into the controller and then execute the **`Show Controller`** command to make sure that proper values are returned.
10.	If the Management server message displays "agent copy failed"	**Root Cause:** Image copy failed due to insufficient space on the controller to extract the Image. Troubleshooting: Free up some space on the controller by using **`delete flash:<older SD version>`** command.
11.	If the Management state displays **"controller Not reachable"** for VPN Controller	**Root Cause**: The VPN Controller is upgraded before the **running configuration** is saved. **Troubleshooting**: Enter the *NMS Server IP* and *Port Number* in the controller to reestablish the VPN [1194] tunnel in the *VPN Server Administration* screen.

#	Problem description	Troubleshooting Tips
12.	"*Authentication Failed*"	**Root Cause**: This message is displayed, if you have entered a wrong password on the controller or if the admin password has been changed. **Troubleshooting**: Navigate to *Operate* > *Inventory* > *Devices* >*Select a controller* > *Edit option* On the *Controller Inventory Details* screen, in the *Password* field, update the password and click *Save* option. The controller is rediscovered.
13.	"*Controller Not Reachable*"	**Root Cause**: This message is displayed for the following reasons: • The controller is down. • The controller is up and not reachable from E(z)RF server. (It uses port 22). **Troubleshooting**: Check if port 22 is opened. Once controller is reachable from FortiWLM server, it tries to re-register the controller after 10 minutes. Check the IP Address of the controller. (In case of RMA controller acquires a new IP address).
14.	"*Unsupported Controller Version*"	**Root Cause**: This message is displayed, if an unsupported version of controller is connected to the FortiWLM. **Troubleshooting**: Verify the supported versions of the controller. See the *FortiWLM Release Notes*.

#	Problem description	Troubleshooting Tips
15.	*“Agent Installation Failed”*	**Root Cause**: • Package Security Check Failed. • Integrity Verification Error
16.	“Already added in other server”	**Root Cause**: The controller is added to different nms-server. **Troubleshooting**: Controller-cli>>sh nms-server Verify the Server IP/Controller ID/Server connectivity status on the controller. The server IP and controller ID must match with E(z)RF Inventory table. 1 172.18.198.26 3 4.0-6.0-A-16 connected Delete the controller from other E(z)RF server.
17.	“NMS server could not detect controller version”	**Root Cause**: The controller is not fully operational **Troubleshooting**: Verify Fortinet services on the controller and restart the service.

#	Problem description	Troubleshooting Tips
18.	“Registration Failed”	**Root Cause**: This message is displayed during the following possible scenarios: • Controller time mismatch • Not enough space **Troubleshooting**: • Verify controller space. • Reset the controller time.
19.	“Controller Time mismatch”	**Root Cause**: This message is displayed during the following possible scenarios: • Controller time mismatch. **Troubleshooting**: • Verify the controller time. • Reset the controller time.
20.	“Installing NMS Agent”	**Root Cause**: This message is displayed during the following possible scenarios: • While installing NMS agent on the controller. • If the E(z)RF server upgrade comprises of more controllers (on a scale setup)

#	Problem description	Troubleshooting Tips
21.	*"Heartbeat Missed"*	Root Cause: This message is displayed during the following possible scenarios: • E(z)RF server misses 3 consecutive "Keep-Alive" message and is not reachable from E(z)RF server. • The controller may be down. Troubleshooting: Verify the link between E(z)RF server and controller.
22.	"Authentication Fail"	Root Cause: The controller "admin" password has been modified on the controller **Troubleshooting**: • Navigate to *Operate* > *Inventory* > *Devices* > *Select controller* > *Edit* option. • In the *Controller Inventory Details - Update* screen, update the controller password in the *Password* field. • Select Save option. • It triggers controller rediscovery.

Migrating from Virtual FortiWLM 32-bit to Virtual FortiWLM 64-bit

To use the current features and retain data, when upgrading from pre-8.4, perform this procedure to migrate a virtual FortiWLM 32-bit to a virtual FortiWLM 64-bit.

The migration can be performed to the current 64-bit version from two prior versions ONLY, for example, data from 8.3.3 and 8.3.2 can only be migrated to 8.4. Hence, it is recommended to migrate pre-8.4 virtual FortiWLM 32-bit **to** 8.4/8.4.1/8.4.2 virtual FortiWLM 64-bit and then **to** 8.5.0.

1. Backup the data in 32-bit FortiWLM and copy it using the copy scp/ftp command.
2. Install the 64-bit FortiWLM image; use the *forti-wlm-x.x-xbuild-y-x86_64.ova* file.
3. Shutdown the 32-bit WLM instance.
4. Run the following commands in the 64-bit FortiWLM to copy and restore the backed up 32-bit data:

- ***copy scp://<user name>@<IP server>/<Backup file path> /data/backup/nms/.***
  OR
- ***copy ftp://<user name>@<IP server>/<Backup file path> /data/backup/nms/.***
- ***restore <Backup file name>***

The following are recommended to perform the migration operation:

- Do not change the name of the database backup file.
- During the backup/restore operation, do not close the CLI session; closing the session aborts the backup/restore operation. For more information, see the backup and restore command details in chapter *FortiWLM - Command Line Interface.*

Notes:

- Migration from SA2000-VE to FWM-VM 64-bit requires a new license file to be installed on FWM-VM 64-bit.
- Migration from FWM-VM 32-bit to FWM-VM 64-bit does NOT require any license changes if the system ID is the same on both. However, if the system ID differs then a new license file is required for FWM-VM 64-bit.

For licensing options contact the *Sales Account team*.

Resetting System and System Passwords

The passwords for the system users “admin' and “guest” can be reset to their default values during a system boot. When the *FortiWLM* prompts “accepting reset request” display, type **pass** to reset the passwords.

To reset the settings for the entire system to their default values, type **reset** at the reset system values prompt.

By performing a reset of the settings for the entire system, deletes the existing configuration.

Security Sensors Capability

The *Hardware Sensors (AP433is/PSM3x)* is an RISC based subsystem in a sensor. It is completely dedicated to monitor the airwaves of the time. By having a dedicated subsystem, the sensor is able to classify and report on the type and source of interference almost instantly and without taking CPU resources away from the wireless radio.

Fortinet WILAN is designed to work with one available channel and still provides a better user experience over systems requiring multiple available channels. The other systems may change the channel of Access Points to avoid potential interference. This often leads to a worse degradation of the overall performance of the network, as the underlying systems are not designed to cope with many number of Access Points sharing the same channel.

With Fortinet, the complete network or a part of the network can be moved to a clearer channel. Fortinet's Air Traffic Control partitions the wireless airspace and delivers high quality connections to the wireless users.

Fortinet sensors capability

- Analog cordless phones
- Frequency- Hopping Spread Spectrum (FHSS) digital cordless phones
- Direct-Sequence Spread Spectrum (DSSS) digital cordless phones
- Motorola Canopy Wireless
- Non-Wifi Wireless Bridges
- Wireless video cameras
- Wireless game controllers

Conventional microwave ovens

- Inverter microwave ovens
- Motion Detectors (S-Band radar-based)1-4 second typical classification time
- Wireless baby monitors
- Estimates channel utilization for both 802.11 and non-802.11 traffic

Spectrum Radio

- Embedded classification processor with dedicated memory
- 40MHz analysis bandwidth
- 80MHz sampling frequency
- Concurrent 2.4GHz and 5GHz WLAN frequency band sampling
- -90 dBm to 0dBm detection range
- Frequency bands. 2.4GHz to 2.5GHz and 4.9GHz to 5.875 GHz

IEEE 802.11Radio

- Frequency Band
  2.402 to 2.485 GHz, 5.15 to 5.25 GHz, 5.725 to 5.825 GHz
- Operating Channels
  1 through 11 for 2.4 GHz band
  32 through 160 for 5 GHz band

- Data Rates (Mbps)
  20 MHz: 130, 117, 104, 78, 65, 58.5, 54, 52, 48, 39, 36, 26, 24,19.5, 18, 13, 12, 11, 9, 6.5, 5.5, 2, 1 Mbps
  40 MHz: 300, 270, 243, 216, 162, 135, 121.5, 108, 81.5, 81, 54,48, 40.5, 36, 27.5, 27, 24, 18, 13.5, 12, 11, 9, 6, 5.5, 2, 1 Mbps with automatic rate adaption
- Average Transmit Power
  2.4n (20 HT): 17 dBm, 2.4n (40 HT): 16 dBm
  5.0n (20 HT): 18 dBm, 5.0n (40 HT): 16 dBm
- Receive Sensitivity (for max data rates)
  11a: -77 dBm, 11n (5 GHz): -72 dBm, 11g: -77 dBm,
  11n (2.4 GHz): -74 dBm

For **PSM3x** sensor AP, the **IEEE 802.11Radio** cannot be used for service clients. It can be used for *WIPS*, *SAM* and *Location* tracking and so on.
In **AP433is** sensor AP, the **IEEE 802.11Radio** can be used for service clients.