FortiWLM MEA - Release-Notes

Version 8.6.3

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

March 24, 2022
FortiWLM MEA 8.6.3 Release-Notes
02-863-615221-20220324

TABLE OF CONTENTS

Change log

Date	Change description
2022-02-03	FortiWLM MEA 8.6.3 release version.
2022-03-24	Updated the scale deployment limits - Product Overview on page 6

About FortiWLM MEA 8.6.3

FortiWLM MEA release 8.6.3 delivers additional features for FortiGate management and resolves common vulnerabilities. See sections What's New on page 8 and Common Vulnerabilities and Exposures on page 21.

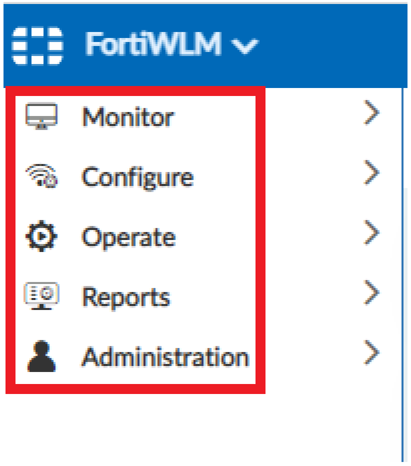
Product Overview

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

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

Note: To ensure a secured Wi-Fi network, Fortinet hardware (controllers and access points) are designed to run only the proprietary firmware developed by Fortinet. Only approved Fortinet access points are configurable with Fortinet controllers and vice versa. Third party access points and software cannot be configured on Fortinet hardware.

FortiWLM MEA supports specific options of the **Monitor**, **Operate**, and **Administration** tabs for FortiGate controllers. You can add and manage FortiGate controllers (with the available options).



The following scale deployment limits are supported for FortiWLM MEA.

Devices	Maximum Limit
10 minutes	
FortiGate controllers	600
Access Points	2000
Stations	25000
1 minute	

Devices	Maximum Limit
FortiGate controllers	600
Access Points	1200
Stations	12000

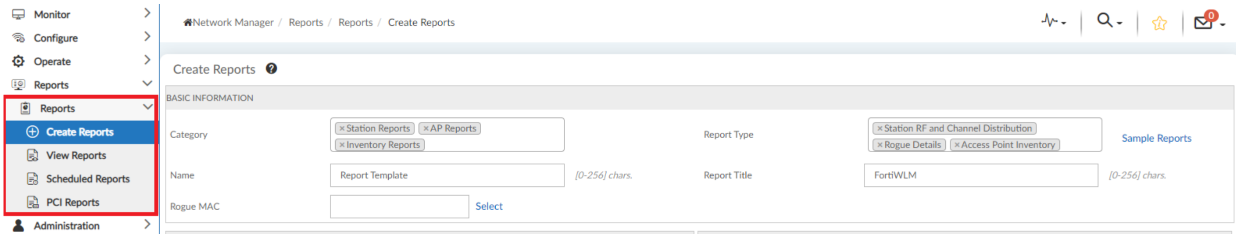
What's New

This release supports additional features for managing FortiGate controllers through FortiWLM MEA.

- Reporting on page 8
- Detailed Dashboards on page 8
- AP Dashboard on page 9
- Trend Dashboards on page 10
- Interfering SSIDs on page 10
- Locationing on page 11
- 1 Minute Polling on page 12

Reporting

The FortiWLM provides standard report types for network analysis, user configuration, device optimization, and network monitoring on multiple levels. These standard report types assist you to generate, schedule, and view a report. You can create and customize report types and save them as templates. You can select and combine multiple report categories and the subsequent report types to generate a single report.



Create Reports

BASIC INFORMATION

Category: ×Station Reports ×AP Reports ×Inventory Reports

Report Type: ×Station RF and Channel Distribution ×Rogue Details ×Access Point Inventory

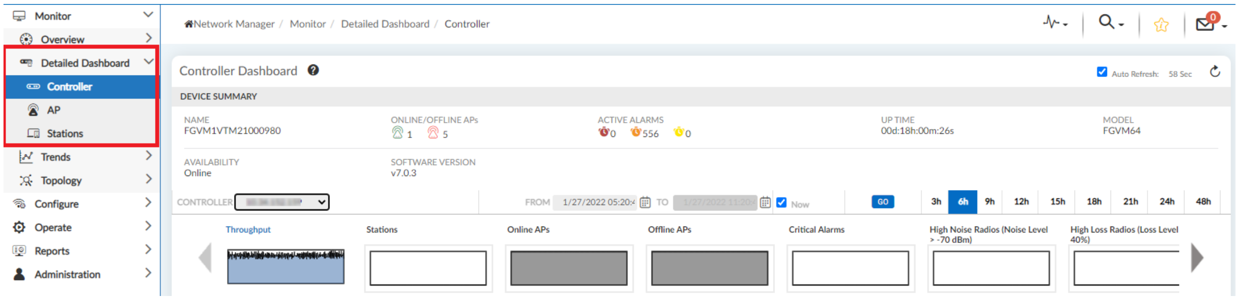
Name: Report Template [0-256] chars.

Report Title: FortiWLM [0-256] chars.

Rogue MAC:

Detailed Dashboards

The detailed dashboards provide at-a-glance system information for controllers, APs, and stations.



Controller Dashboard

☑ Auto Refresh: 58 Sec

DEVICE SUMMARY

NAME: FGVM1VTM21000980

ONLINE/OFFLINE APs: 1 5

ACTIVE ALARMS: 0 556 0

UP TIME: 00d:18h:00m:26s

MODEL: FGVM64

AVAILABILITY: Online

SOFTWARE VERSION: v7.0.3

CONTROLLER: [redacted]

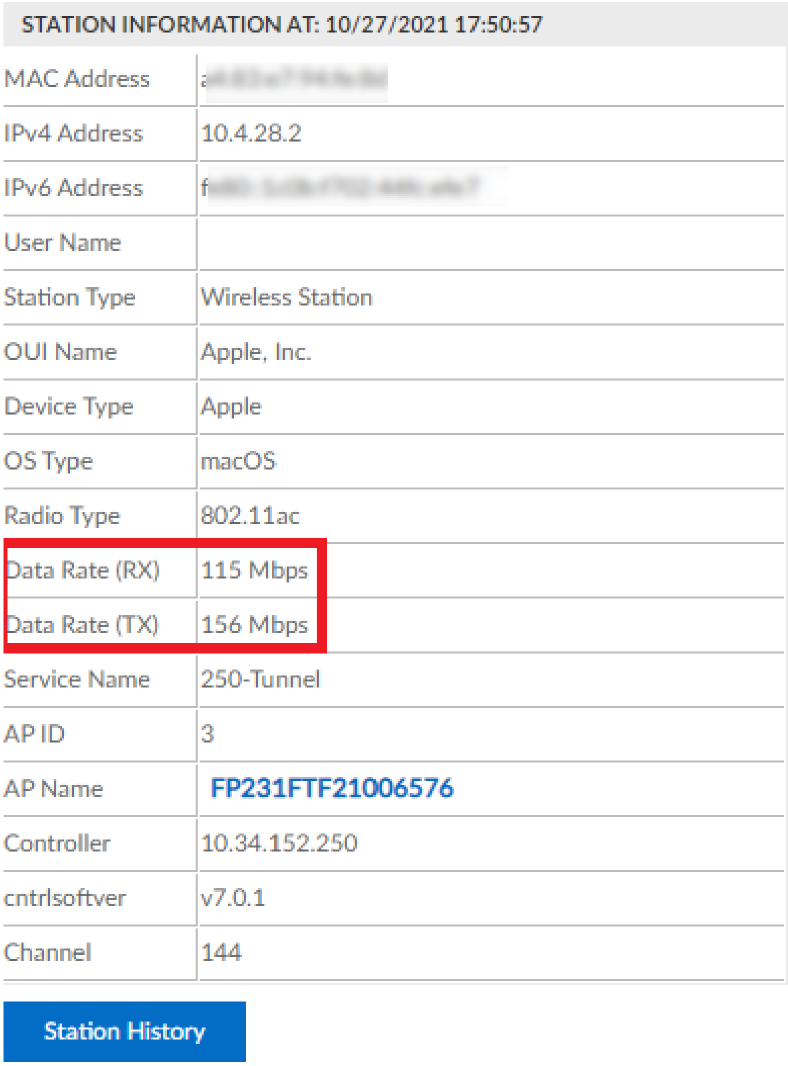
FROM 1/27/2022 05:20: TO 1/27/2022 11:20: ☑ Now

- **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, 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.
- **APs** - The AP dashboard screen displays an in-depth information about the AP activity. It provides the graphical representation of the wireless statistics such as *Throughput, Stations, Noise Level, Loss*%, and

Channel Utilization% for each of the radio on AP and wired statistics for LAN1 and LAN2 interfaces such as inbound/outbound octets and input/output errors.

- **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 data rate in the **Stations** detailed dashboard is now split into **Data Rate** (Rx) and **Data Rate** (Tx) displayed in the station summary.



STATION INFORMATION AT: 10/27/2021 17:50:57

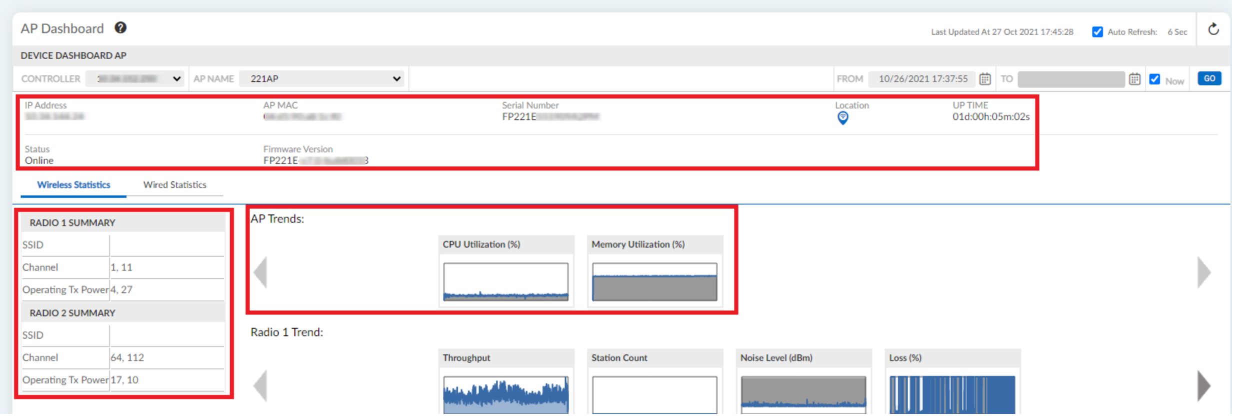
MAC Address	[redacted]
IPv4 Address	10.4.28.2
IPv6 Address	[redacted]
User Name	
Station Type	Wireless Station
OUI Name	Apple, Inc.
Device Type	Apple
OS Type	macOS
Radio Type	802.11ac
Data Rate (RX)	115 Mbps
Data Rate (TX)	156 Mbps
Service Name	250-Tunnel
AP ID	3
AP Name	FP231FTF21006576
Controller	10.34.152.250
cntrlsoftver	v7.0.1
Channel	144

AP Dashboard

The AP dashoard enhancement in this release delivers the following new fields. Navigate to **Monitor > Detailed Dashboard > AP**.

- **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.



AP Dashboard

Last Updated At 27 Oct 2021 17:45:28 ☑ Auto Refresh: 6 Sec

DEVICE DASHBOARD AP

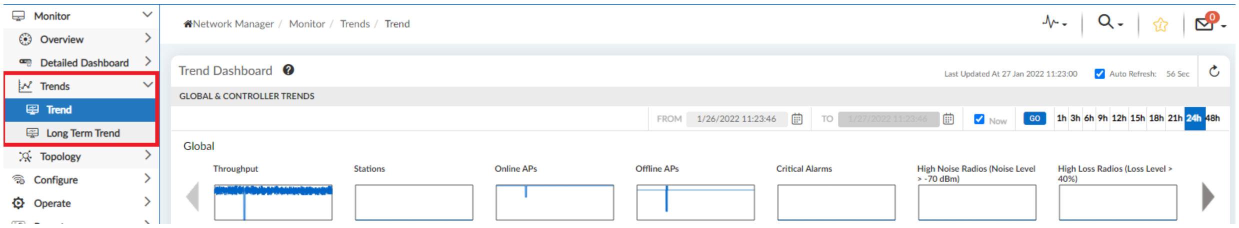
CONTROLLER [redacted] AP NAME 221AP FROM 10/26/2021 17:37:55 TO ☑ Now GO

IP Address [redacted]
AP MAC [redacted]
Serial Number FP221E[redacted]
Location
UP TIME 01d:00h:05m:02s
Status Online
Firmware Version FP221E[redacted]3

RADIO 1 SUMMARY	
SSID	
Channel	1, 11
Operating Tx Power	4, 27
RADIO 2 SUMMARY	
SSID	
Channel	64, 112
Operating Tx Power	17, 10

Trend Dashboards

The trend dashboards provide the aggregate global trend performance and controller error rates over a period of time. FortiWLM collects statistics from a controller and stores it in the database.



Trend Dashboard

Last Updated At 27 Jan 2022 11:23:00 ☑ Auto Refresh: 56 Sec

GLOBAL & CONTROLLER TRENDS

FROM 1/26/2022 11:23:46 TO 1/27/2022 11:23:46 ☑ Now GO 1h 3h 6h 9h 12h 15h 18h 21h 24h 48h

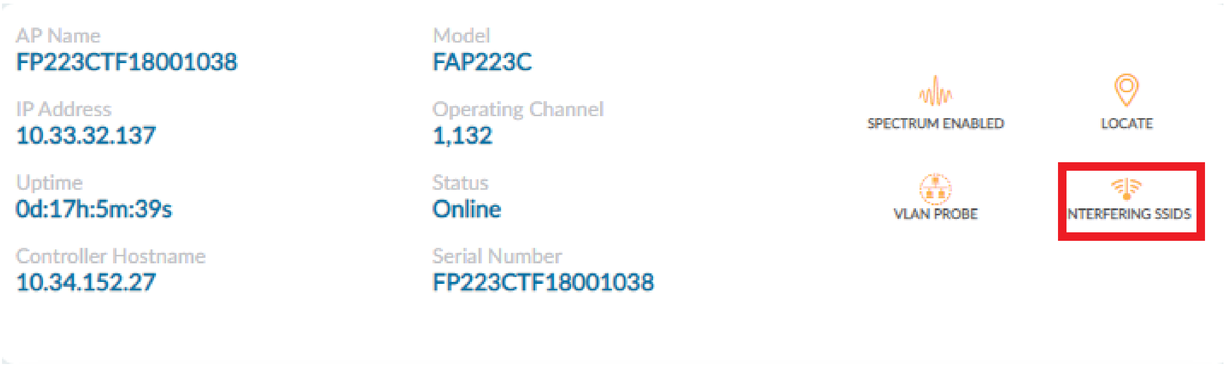
Global
Throughput
Stations
Online APs
Offline APs
Critical Alarms
High Noise Radios (Noise Level > -70 dBm)
High Loss Radios (Loss Level > 40%)

- **Trend** - The global trends and trends per controller are graphically represented in the trend dashboard. The global trends (all controllers) are displayed in the graphs on the top portion of the window such as *Throughput* , *Stations, Online APs, Offline APs, Critical Alarms, High-Noise Radios, High-Loss Radios, High-Loss Stations, Low-RSSI Stations*, and *Rogue APs* and trends per controller on the lower portion of the window.
- **Long Term Trend** - The long term trend dashboard displays the per-controller view or the aggregate-controller view (default view). It provides graphical representation of the *Throughput* , *Controllers, APs, Stations, Rx/Tx (MB)*, and *Alarms*. 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.

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. Navigate to **Monitor > Overview > AP** and click **Intefering SSIDs**.

To view the interfering SSID details, ensure that the AP radio is configured in the access point mode in FortiGate (Managed FortiAP Profile).



AP Name
FP223CTF18001038

IP Address
10.33.32.137

Uptime
0d:17h:5m:39s

Controller Hostname
10.34.152.27

Model
FAP223C

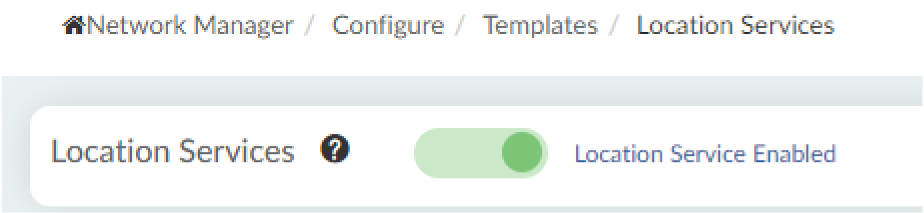
Operating Channel
1,132

Status
Online

Serial Number
FP223CTF18001038

Locationing

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



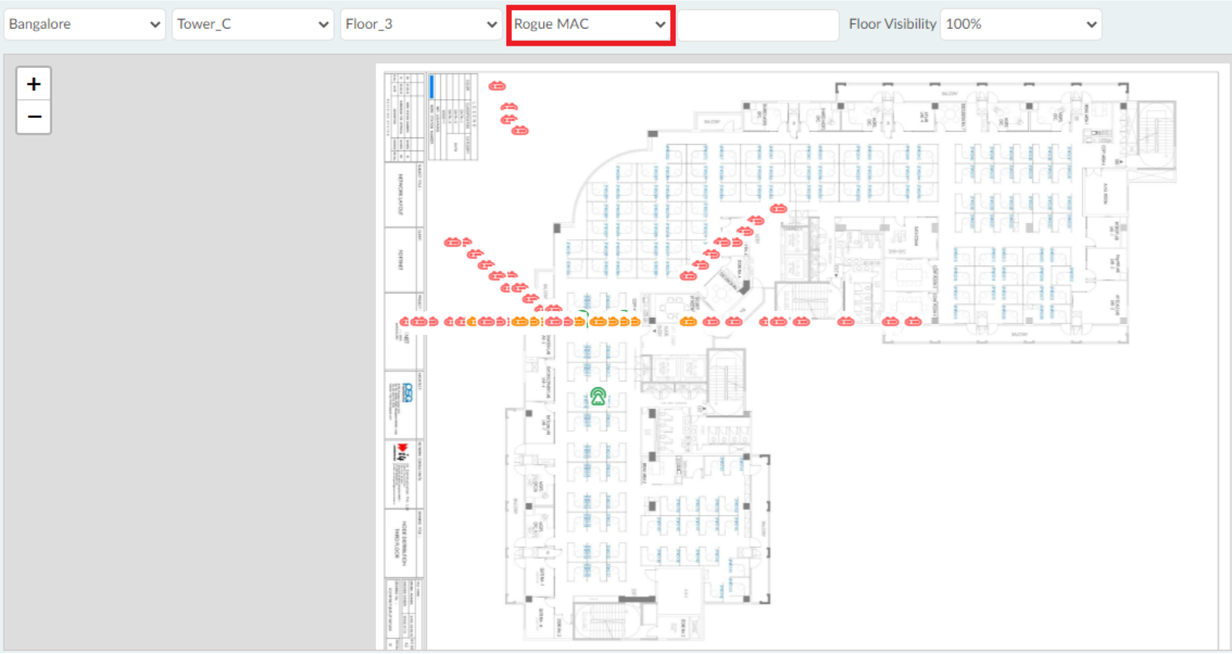
Network Manager / Configure / Templates / Location Services

Location Services: Location Service Enabled

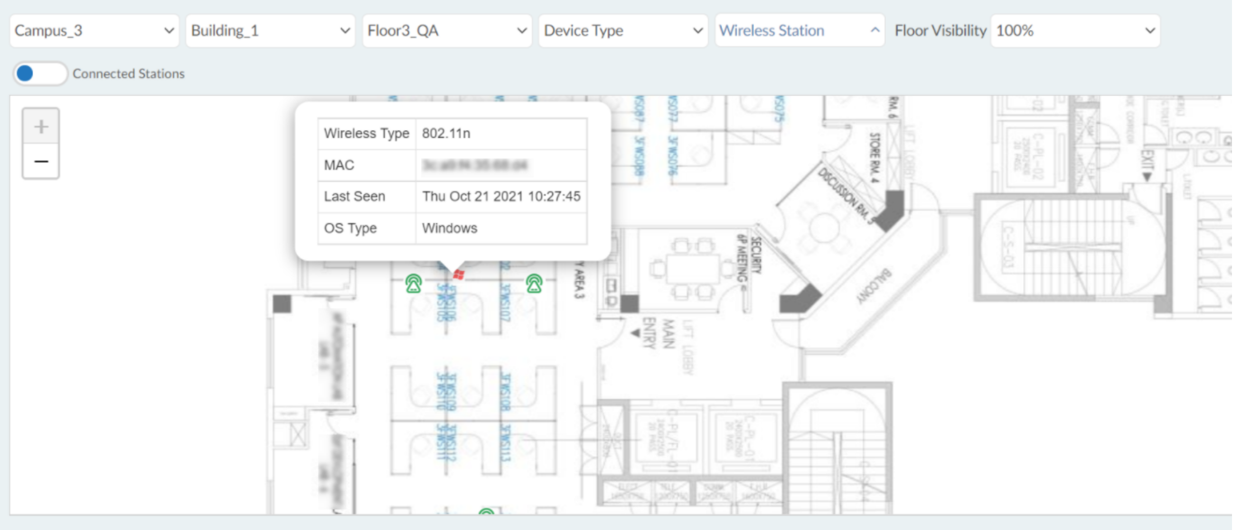
- Configure the WIDS profile for the AP radio.
- Configure the following parameters in **Location Based Services > FortiPresence**.
  - Project Name: **FWLM**
  - Password: The secret key displayed in **Administration > System Settings > Maintenance**.
  - FortiPresence server IP: FortiWLM IP address.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

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

The locationing feature now plots the current location of all rogue APs on the floor map imported into the FortiWLM. Navigate to **Monitor > Overview > Location Services**.



Bangalore | Tower_C | Floor_3 | Rogue MAC | Floor Visibility 100%



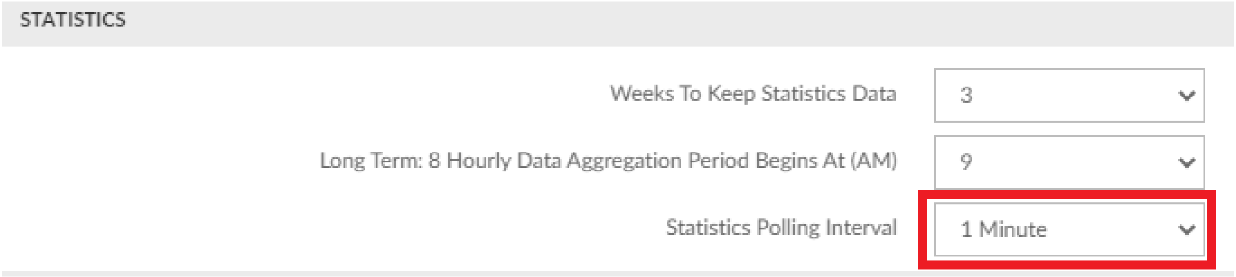
Campus_3 | Building_1 | Floor3_QA | Device Type | Wireless Station | Floor Visibility 100%

Connected Stations

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

1 Minute Polling

You can now configure the Statistics Polling Interval at 1 minute. Navigate to **Administration > System Settings > Maintenance**.



STATISTICS

Weeks To Keep Statistics Data: 3

Long Term: 8 Hourly Data Aggregation Period Begins At (AM): 9

Statistics Polling Interval: 1 Minute

Notes:

- After modifying the polling interval (1 minute to 10 minutes or vice versa), it is recommended NOT to refer to the old data.
- When you upgrade FortiWLM MEA to this release, the default statistics polling interval is 10 minutes and in new installations of this release the default is 1 minute.

Supported FortiOS

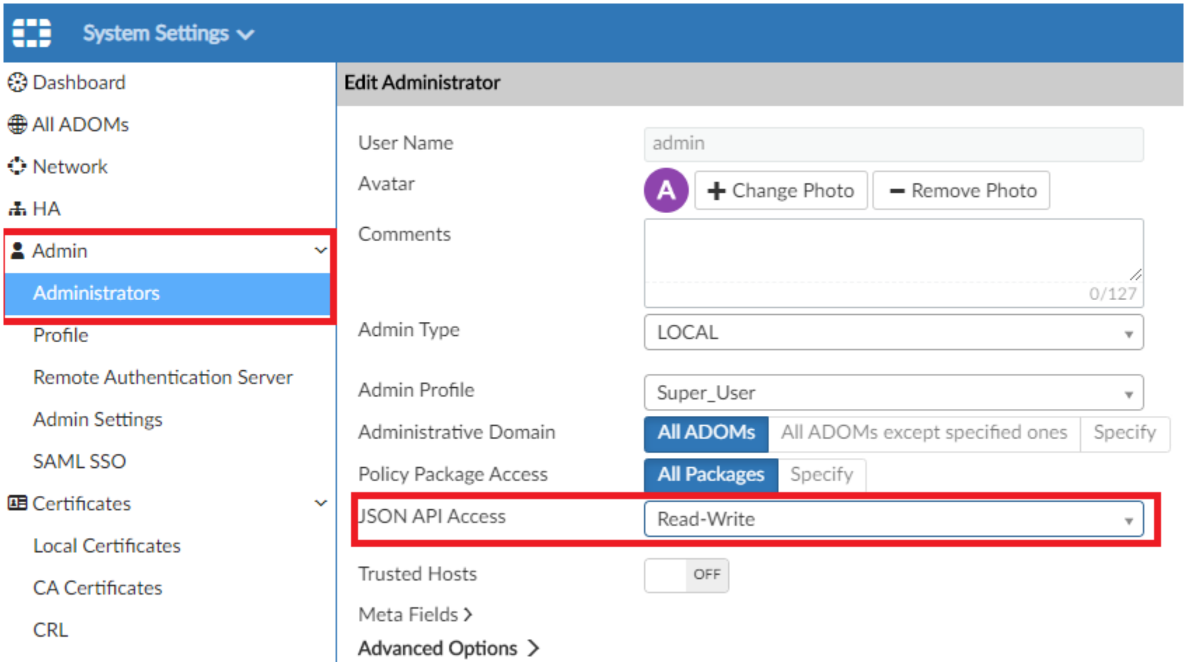
The following versions of FortiOS are supported with this release of FortiWLM MEA.

- 6.2.2
- 6.2.3
- 6.4.0
- 6.4.1
- 6.4.2
- 6.4.3
- 6.4.4
- 6.4.5
- 6.4.6
- 6.4.7
- 7.0.0
- 7.0.1
- 7.0.2
- 7.0.3

Enabling FortiWLM MEA

Follow this procedure to enable FortiWLM MEA.

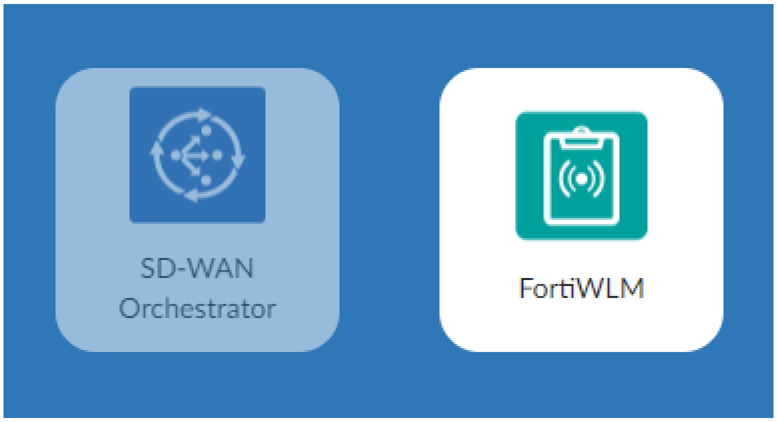
1. Connect to the FortiManager GUI.
2. Navigate to **System Settings > Administrators > Admin** and set **JSON API Access** to **Read-Write**. This enables communication between FortiManager and FortiWLM MEA.



Edit Administrator

User Name: admin
Avatar: A
Comments: 0/127
Admin Type: LOCAL
Admin Profile: Super_User
Administrative Domain: All ADOMs | All ADOMs except specified ones | Specify
Policy Package Access: All Packages | Specify
JSON API Access: Read-Write
Trusted Hosts: OFF

3. Navigate to **Management Extensions** and click the **FortiWLM** tile.



Note: After FortiManager is restored, FortiGate controllers are in the offline state in FortiWLM MEA. Disable the offline state in the FortiManager manually and all FortiGate controllers appear online after approximately 10 minutes.

Operational Guidelines

This section describes information related to the usage of FortiWLM MEA/FortiGate.

- Third parties cannot query FortiWLM MEA data using SNMP.
- Application control is supported on FortiOS version 6.2.2 and later.
- Station activity logs are supported on FortiOS version 6.2.0 and later.

Features	FortiOS Versions		
	6.2.2/6.2.3	**6.4.0/6.4.1/6.4.2/6.4.3/6.4.4/ 6.4.5/6.4.6/6.4.7**	**7.0.0/7.0.1/7.0.2/7.0.3**
Dashboard Status			
Application Control	✓	✓	✓
Station Data	✓	✓	✓
Station activity logs	✓	✓	✓
AP Dashboard			
Retry %	✓	✓	✓
Loss %	✓	✓	✓
Channel Utilization%	✓	✓	✓
SNR (dBm)	✓	✓	✓
Average Throughput	X	X	✓
Station Dashboard			
Retry %	✓	✓	✓
Loss %	✓	✓	✓
Channel Utilization%	X	X	X
SNR (dBm)	✓	✓	✓

SNMP Configurations

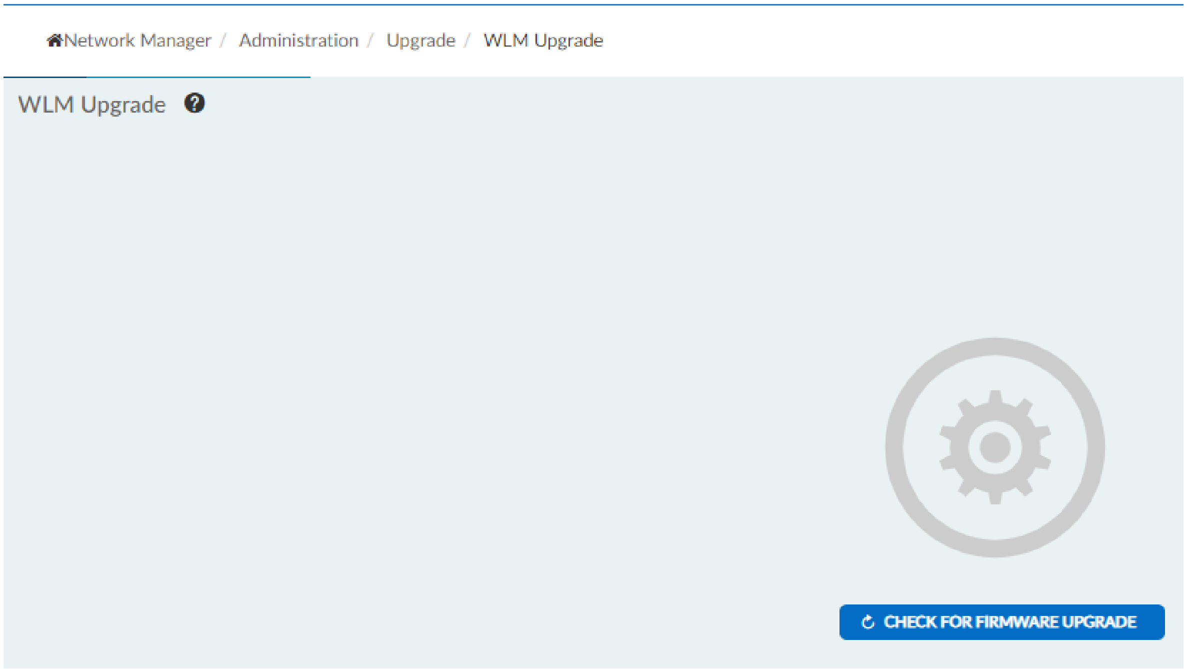
SNMP Traps use port 10162 to receive the AP down Alarm from FortiGate. The following FortiGate configuration is required in the FortiGate GUI.

1. Navigate to **System > SNMP**.
2. Create/edit **SNMP v1/v2c** configuration with Traps configured to use 10162 as the **Local Port** and **Remote Port**.

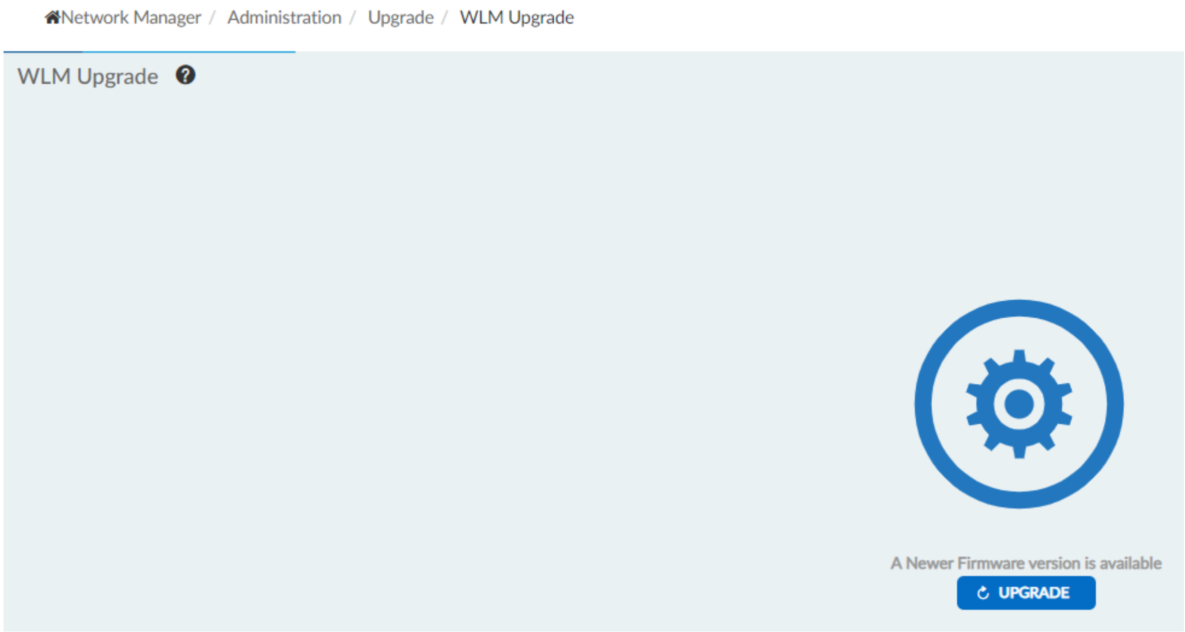
Upgrading FortiWLM MEA

To upgrade your FortiWLM MEA, navigate to **Administration > Upgrade** in the GUI.

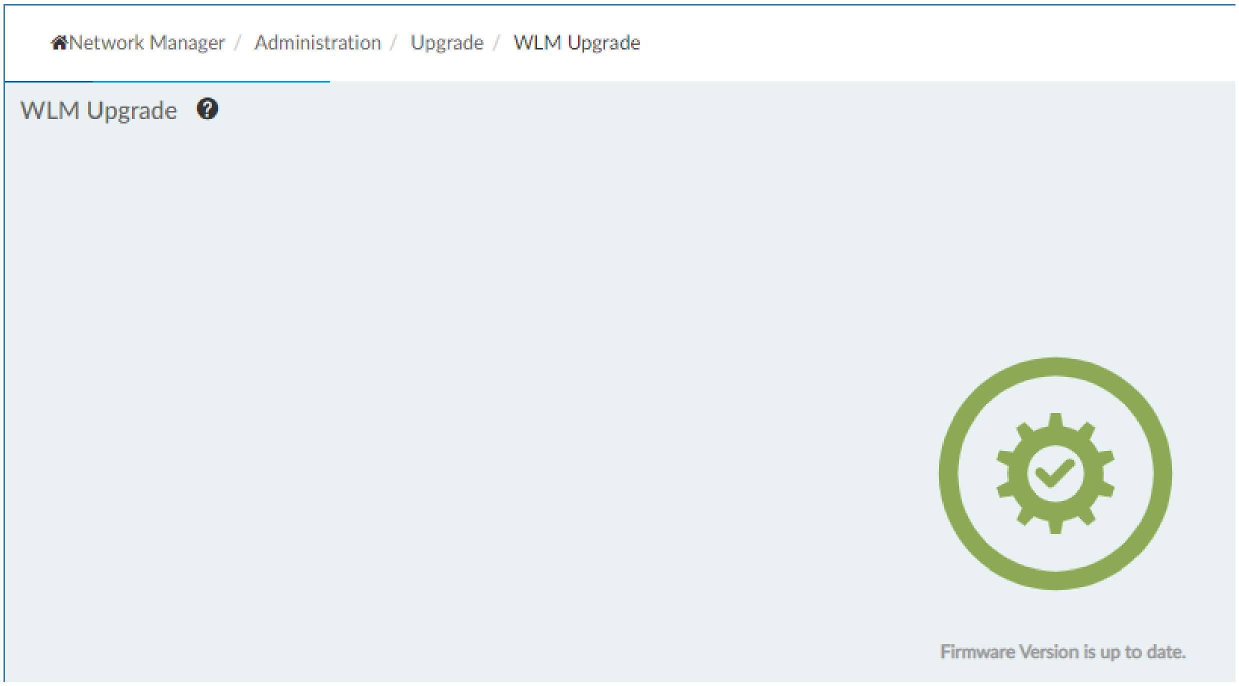
1. Click **Check For Firmware Upgrade**.


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

2. FortiWLM MEA checks for the available new release versions and the upgrade option appears. Click **Upgrade**.


Network Manager / Administration / Upgrade / WLM Upgrade
WLM Upgrade
A Newer Firmware version is available
UPGRADE

FortiWLM MEA is upgraded to the new firmware version.



WLM Upgrade

Firmware Version is up to date.

Known Issues

These are the known issues in this release of FortiWLM MEA.

Bug ID	Description	Impact	Workaround
760419	ARRP replanning does not happen post FortiWLM upgarde and restore.		
762282	[FAP-22xEV/FAP-U42xEV] The *tx_ discard_percentage* is 100 for most of the times.	The data loss value is not accurate.	

Common Vulnerabilities and Exposures

This release of FortiWLM MEA is no longer vulnerable to the following.

Vulnerability	Description
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
731576	jQuery and Bootstrap vulnerabilities.
734094	Command Injection in script handlers.

Visit https://www.fortiguard.com/psirt for more information.