



FortiWLM MEA - Release-Notes

Version 8.5.2

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

October 23, 2020

FortiWLM MEA 8.5.2 Release-Notes

02-852-615221-20201023

TABLE OF CONTENTS

Change log	4
Product Overview	5
Related Documentation	7
What's New	8
Supported FortiOS	9
Enabling FortiWLM MEA	10
Operational Guidelines	11
SNMP Configurations	12
Upgrading FortiWLM MEA	13
Known Issues	15
FortiGate Known Issues	16

Change log

Date	Change description
2020-10-23	FortiWLM MEA 8.5.2 release version.

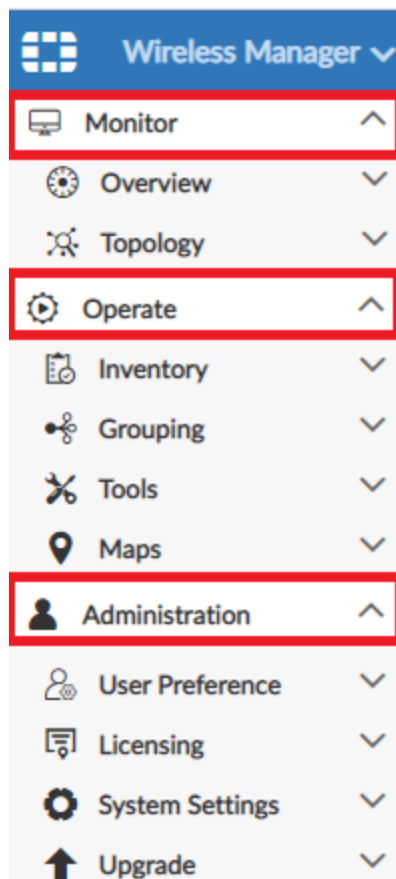
Product Overview

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 8.5.2 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).



Tab	Description
Monitor	<ul style="list-style-type: none"> • Overview – Dashboards that provide a summary view of all network statistics. These dashboards provide at-a-glance system information related to APs, AP groups, stations, station groups, application monitoring, fault management, and heat maps. The Network Health dashboard monitors the devices in your wireless network and provides a health summary of the devices. • Topology – Illustrated physical and logical placement of devices such as APs, controllers, and stations in your network.
Operate	<ul style="list-style-type: none"> • Inventory – Discover and manage controllers and access points. • Grouping – Controllers, APs, and stations are grouped for management purpose. • Tools – Provides station activity log with station events within the selected time interval, syslog with log details of operations performed on the FortiWLM MEA, and diagnostics with logs and other files. • Maps – Create maps to track your APs visually.
Administration	<ul style="list-style-type: none"> • User Preference – Create notification profiles to trigger email notifications for specific recipients when a managed controller goes down. A notification filter is provided to indicate the type of error that triggers notification. • Licensing – Import license key files, request for a license and then upload it. • System Settings – Manage specific system settings such as configuring server parameters, configuring SMTP mail servers for email notification, administering SNMP, and configuring the archival policy for station activity logs. • Upgrade – Upgrade the FortiWLM MEA server to a new released version or install a patch

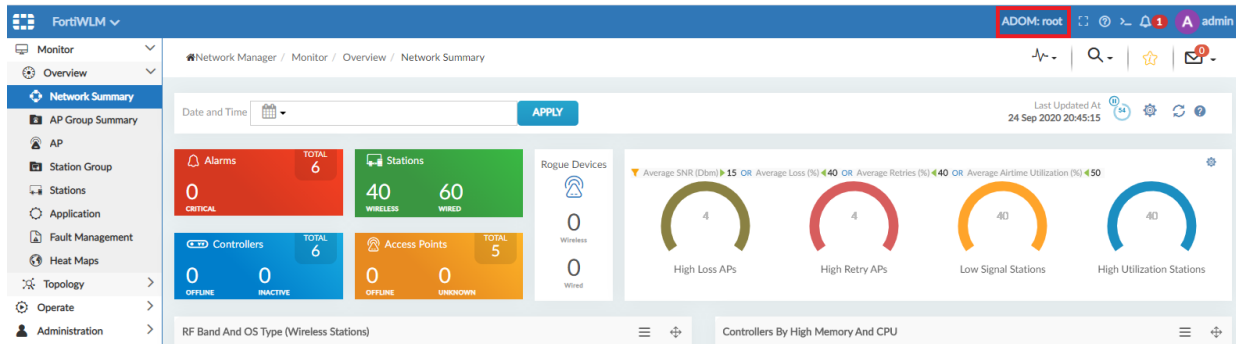
Related Documentation

This release of FortiWLM MEA delivers a comprehensive set of following documentation:

- Online Help integrated into the FortiWLM MEA application
- FortiWLM MEA 8.5.2 Administration Guide

What's New

This release of FortiWLM MEA provides support for managing FortiGate controllers through Administrative domains (ADOMs). The ADOMs enable administrators to manage only those controllers that they are specifically assigned, based on the ADOMs which they access. You can manage FortiWLM MEA using the root ADOM or create a new ADOM. The FortiWLM MEA can now operate in the ADOM and non-ADOM modes.



In the ADOM mode, you can add FortiGate controllers managed by the particular ADOM of the FortiManager. In the non-ADOM mode, you can add any FortiGate controller managed by FortiManager. To add a FortiGate controller, navigate to **Inventory > Devices**.

For more information on creating and managing ADOMs, and adding FortiGate controllers, see the *FortiWLM MEA 8.5.2 Administration Guide*.

Supported FortiOS

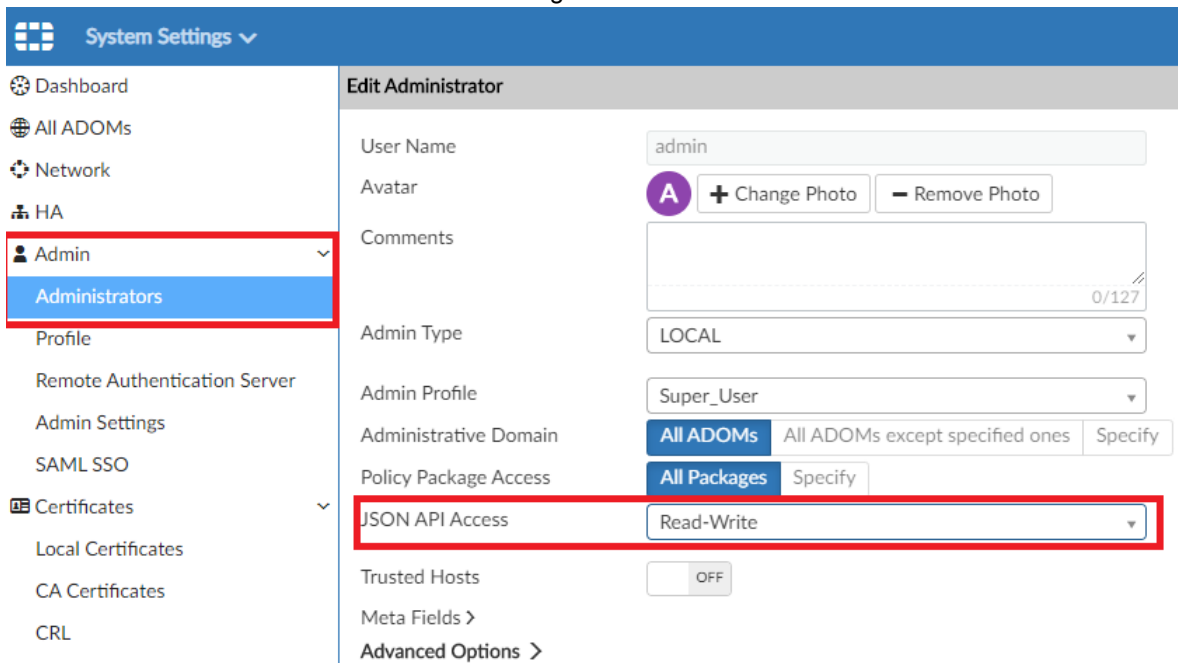
The following versions of FortiOS are supported with this release of FortiWLM MEA.

- 6.0.6 (limited monitoring)
- 6.2.0
- 6.2.2
- 6.2.3
- 6.4.0
- 6.4.1
- 6.4.2
- 6.4.3

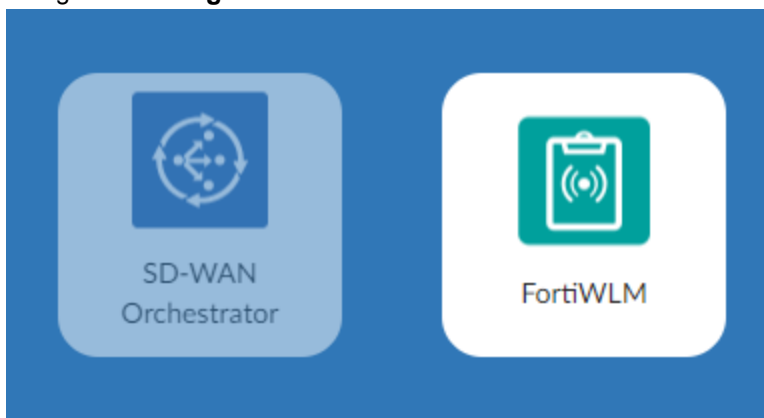
Enabling FortiWLM MEA

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.



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.

- RF Planner supports only FAP-U's (Universal APs).
- Third parties cannot query FortiWLM MEA data using SNMP.
- Application control is supported on FortiOS version 6.2.2 and later.
- Application control is supported only for disk, FortiAnalyzer, and memory based log storages.
- Station activity logs are supported on FortiOS version 6.2.0 and later.
- Station logs can be accessed from the disk, FortiCloud, or FortiAnalyzer. Disk availability is for specific FortiGate models.

Feature	FortiOS Versions		
	6.0.6	6.2.0/6.2.1	6.2.2/6.2.3/ 6.4.0/6.4.1/6.4.2
Dashboard Status			
Application Control	X	X	✓
Station Data	✓	✓	✓
Station activity logs	X	✓	✓
AP Dashboard			
Retry %	X	X	✓
Loss %	X	X	X
Channel Utilization%	✓	✓	✓
SNR (dBm)	X	X	✓
Station Dashboard			
Retry %	X	X	X
Loss %	X	✓	✓
Channel Utilization%	X	X	X
SNR (dBm)	✓	✓	✓

SNMP Configurations

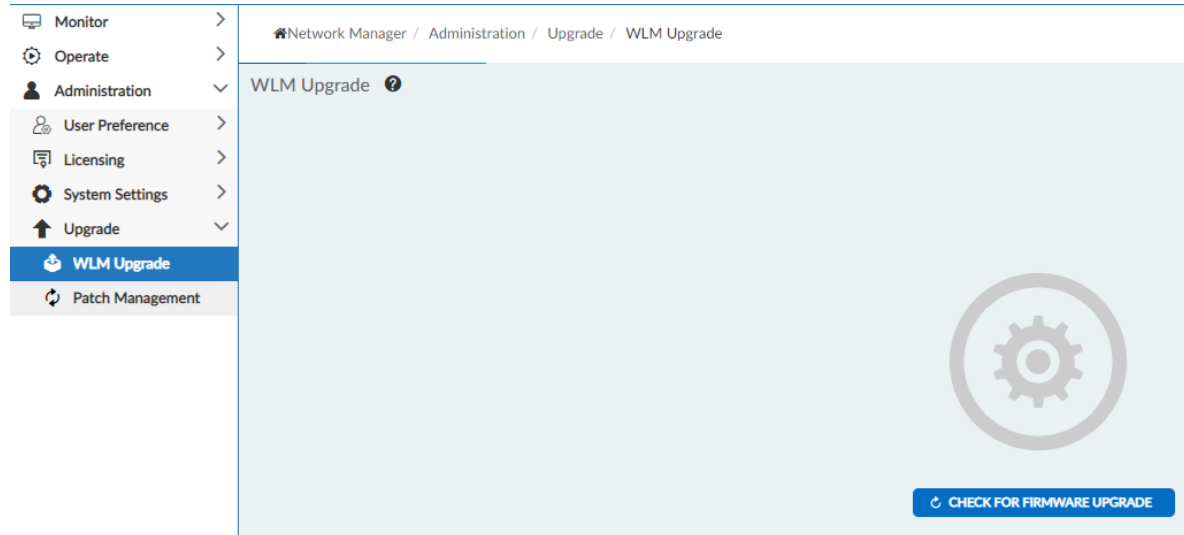
SNMP Traps use port 10162 to receive the AP down Alarm from FortiGate. The following FortiGate configuration is required in the FortiGate GUI.

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**.

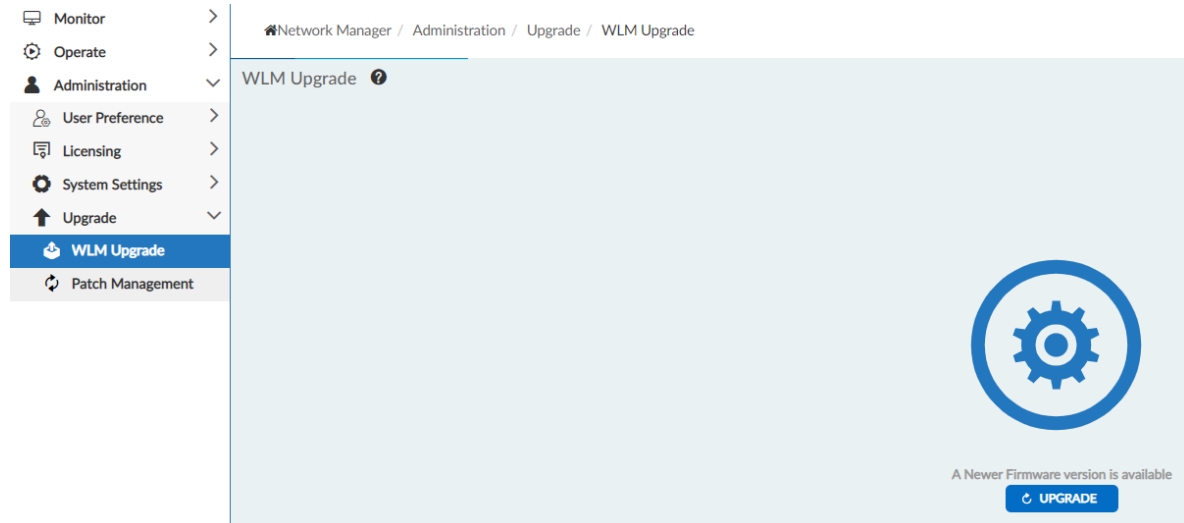
Upgrading FortiWLM MEA

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

1. Click Check For Firmware Upgrade.




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



FortiWLM MEA is upgraded to the new firmware version.

Network Manager / Administration / Upgrade / WLM Upgrade

WLM Upgrade ?



Firmware Version is up to date.

The image shows a screenshot of the FortiWLM MEA administration interface. On the left is a navigation menu with items: Monitor, Operate, Administration, User Preference, Licensing, System Settings, Upgrade, WLM Upgrade (highlighted in blue), and Patch Management. The main content area shows the breadcrumb path 'Network Manager / Administration / Upgrade / WLM Upgrade' and the title 'WLM Upgrade' with a help icon. A large green gear icon with a checkmark inside a circle is centered on the page, with the text 'Firmware Version is up to date.' below it.

Known Issues

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

Bug ID	Description	Impact	Workaround
614988	Search operation does not work for all records in the station activity log.		
627299	Mismatched FortiAnalyzer events in the station activity log of FortiWLM MEA.		
645328	[FAP-421E] The operating channel for both radios is displayed as 0.		
653406/656967	FAP-U43xF/FAP-231E model is displayed as UNKOWN in the AP inventory.		
656124	The Import option in the Device inventory is not supported.		
656127	The Managment Administrative State is the only editable field in the Device inventory.		
656956	Sometimes, the FortiGate state is not synchronized properly with FortiManager and an error message is received for a FortiGate with status UP .		
656964	FortiGate 100E controller model is displayed as Unknown and the node name is not displayed.		
656966	FortiGate 100F and 101F controller models are displayed as FGT_UNKOWN_MODEL in the Device inventory.		
660486	The following FortiManager operations are delayed by approximately 10 minutes in FortiWLM MEA. <ul style="list-style-type: none"> • Deleting FortiGate controller in FortiManager. • Disabling central management in FortiManager managed FortiGate controller. • Moving FortiGate controller across 		

Bug ID	Description	Impact	Workaround
	ADOMs.		
662407	When the ADOM name is modified, managed FortiGate data is deleted.		
656970	Station activity logs with FQDNs as hostnames are not exported.		

FortiGate Known Issues

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

Bug ID	Description	Impact	Workaround
596765	Incorrect AP throughput value is displayed in the AP dashboard.		
606980	TX and RX rates are not displayed for stations.		
607039	TX and RX rates are not displayed for APs.		
607065	Station retries data is not displayed in the AP and station dashboards.		
607938	Only 100 records are fetched at a time for FortiCloud based events.		
610902	Station channel utilization data is not displayed in the AP and station dashboards.		



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.