

A decorative pattern of concentric hexagons in a light blue color, scattered across the top dark blue header area.

FortiWLM MEA - Release-Notes

Version 8.5.4

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

May 02, 2022

FortiWLM MEA 8.5.4 Release-Notes

02-854-615221-20220502

TABLE OF CONTENTS

- Change log 4**
- About FortiWLM MEA 8.5.4 5**
- Product Overview 6**
- Supported FortiOS 8**
- Enabling FortiWLM MEA 9**
- Operational Guidelines 10**
 - SNMP Configurations 11
- Upgrading FortiWLM MEA 12**
- Common Vulnerabilities and Exposures 14**

Change log

Date	Change description
2022-05-02	FortiWLM MEA 8.5.4 release version.

About FortiWLM MEA 8.5.4

FortiWLM MEA release 8.5.4 delivers resolved common vulnerabilities; see section [Common Vulnerabilities and Exposures on page 14](#).

Note: This release is supported for upgrade only on FortiManager 6.4.8

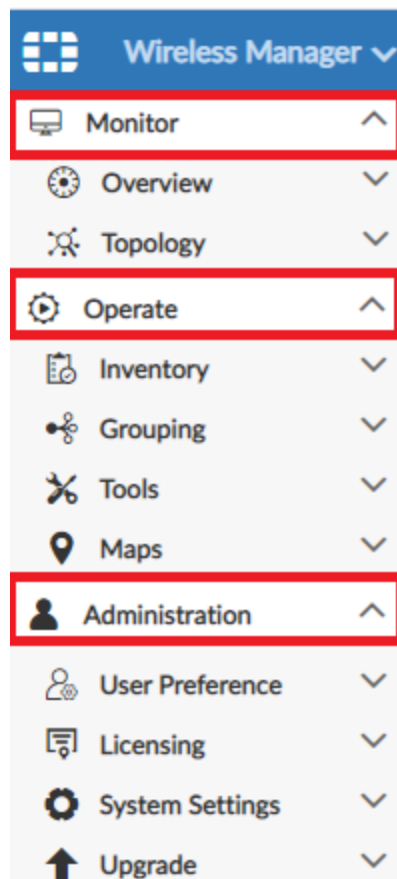
Product Overview

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).



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

Supported FortiOS

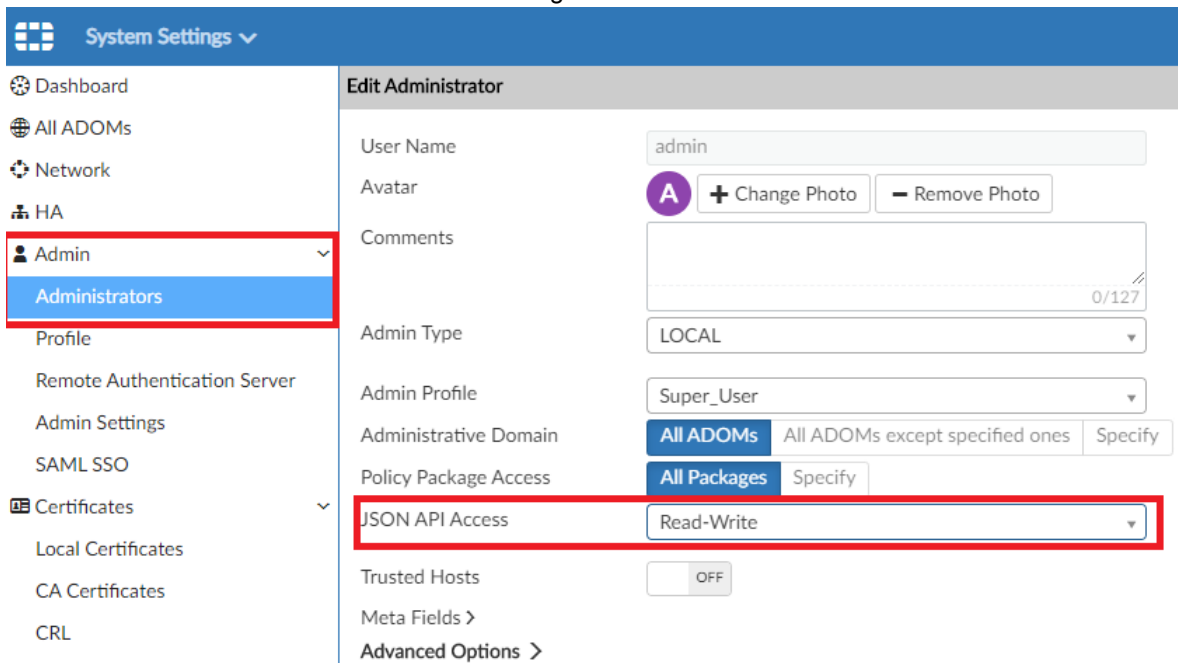
The following versions of FortiOS are supported with this release of FortiWLM MEA.

- 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
- 6.4.4
- 6.4.5
- 6.4.6
- 6.4.7
- 6.4.8

Enabling FortiWLM MEA

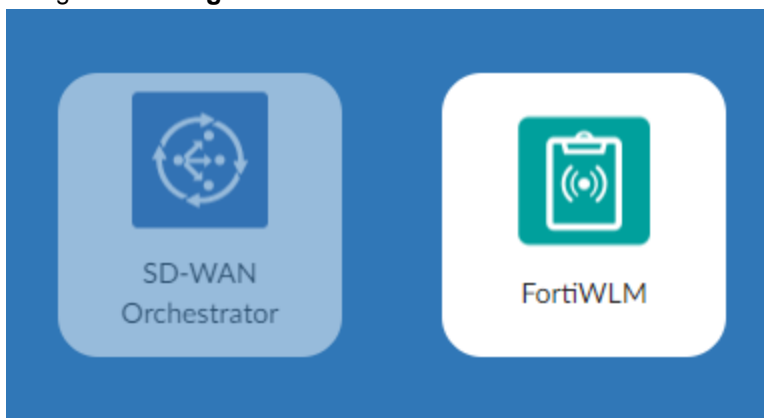
Follow this procedure to enable FortiWLM MEA.

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.



The screenshot displays the FortiManager GUI's 'System Settings' section. On the left, a sidebar menu lists various settings, with 'Administrators' selected and highlighted in blue. The main content area is titled 'Edit Administrator' and shows the configuration for the 'admin' user. The 'JSON API Access' dropdown menu is set to 'Read-Write' and is highlighted with a red rectangular box. Other visible fields include 'User Name' (admin), 'Avatar' (A), 'Comments' (0/127), 'Admin Type' (LOCAL), 'Admin Profile' (Super_User), 'Administrative Domain' (All ADOMs), 'Policy Package Access' (All Packages), 'Trusted Hosts' (OFF), and 'Meta Fields'.

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-Us (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 to 6.4.8
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

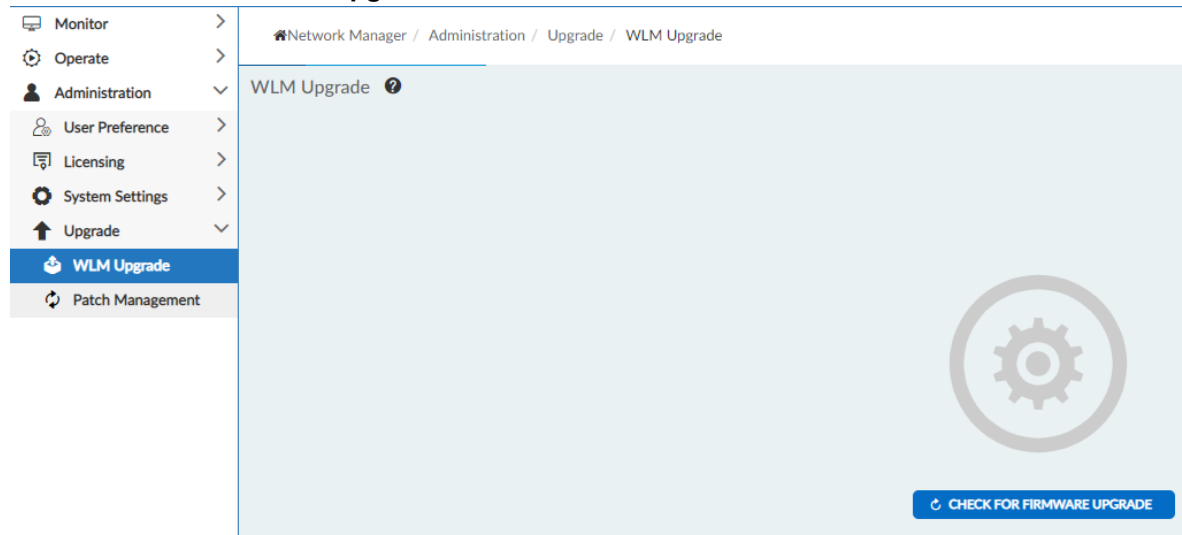
SNMP Traps use port 10162 to receive the AP down Alarm from FortiGate. The following FortiGate configuration is required in the FortiGate GUI.

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**.

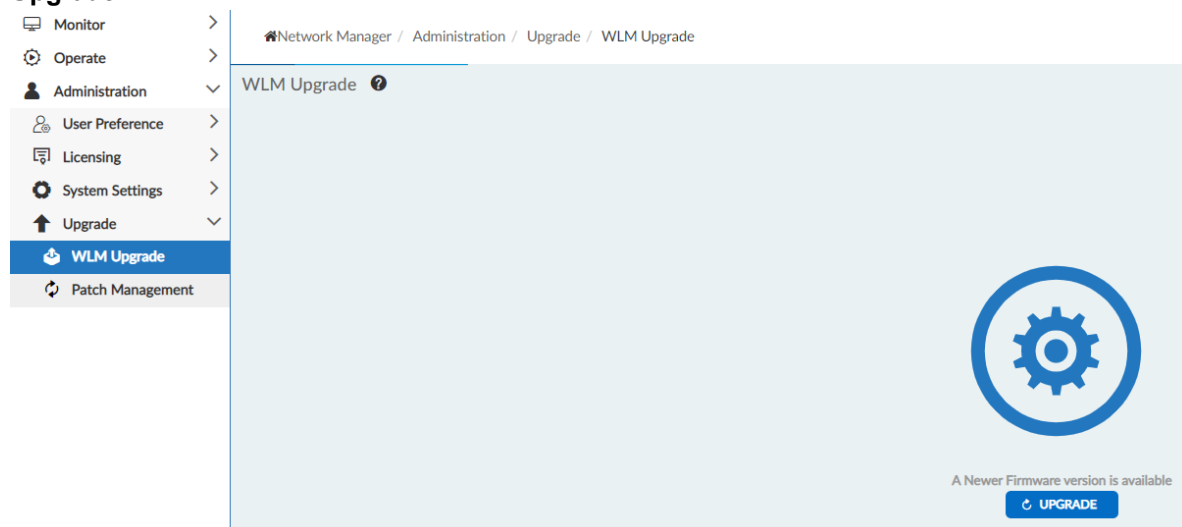
Upgrading FortiWLM MEA

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

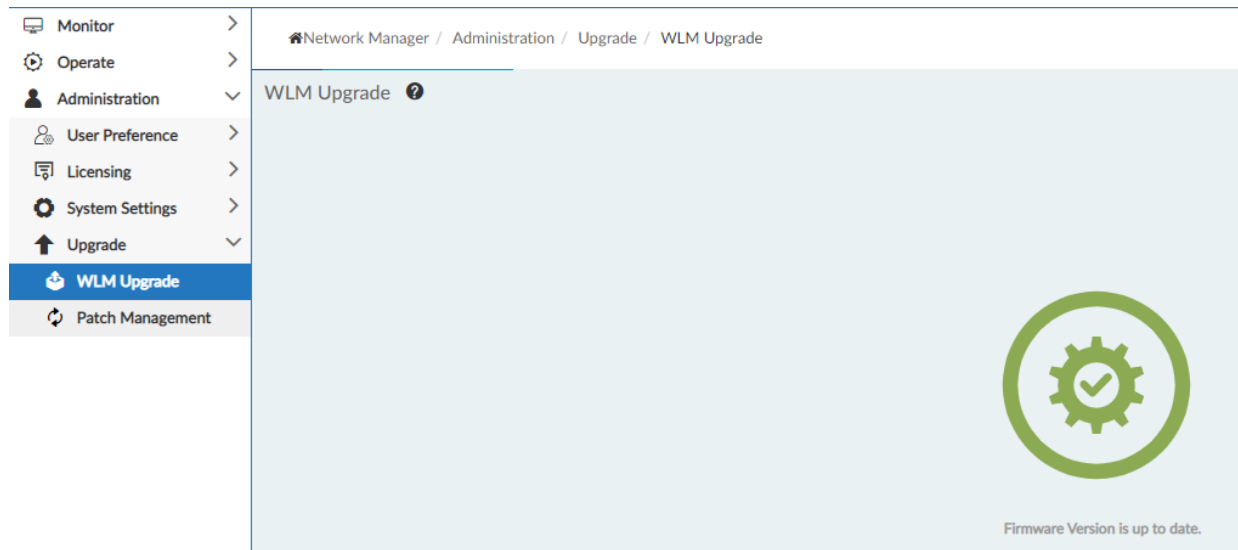
1. Click **Check For Firmware Upgrade**.



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.



Common Vulnerabilities and Exposures

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

Vulnerability	Description
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

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



Copyright© 2022 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.