

Release Notes

FortiWLM MEA 8.6.5



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

January 18, 2023

FortiWLM MEA 8.6.5 Release Notes

02-865-615221-20230118

TABLE OF CONTENTS

Change log	4
About FortiWLM MEA 8.6.5	5
Product Overview	6
Supported FortiOS and FortiAP	7
Enabling FortiWLM MEA	8
Operational Guidelines	9
SNMP Configurations	10
Upgrading FortiWLM MEA	11
Fixed Issues	13

Change log

Date	Change description
2023-01-18	FortiWLM MEA 8.6.5 release version.

About FortiWLM MEA 8.6.5

This release of FortiWLM MEA resolves open product issues. For more information, see [Fixed Issues](#)

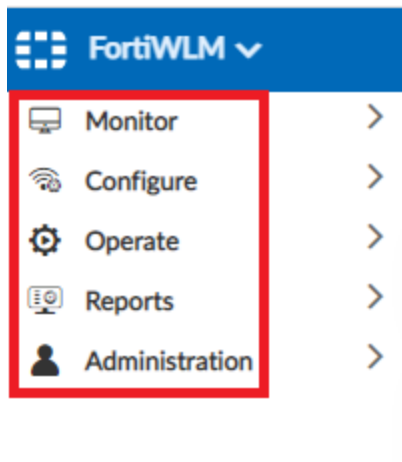
Product Overview

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).



Supported FortiOS and FortiAP

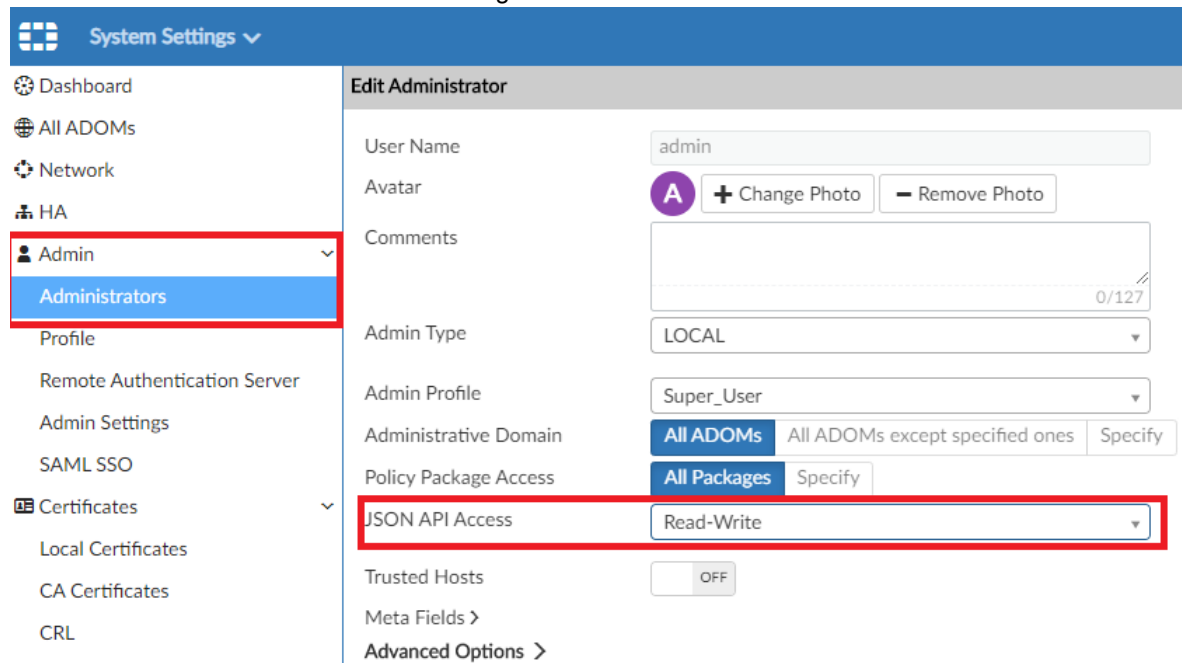
The following versions of FortiOS FortiAPs are supported with this release of FortiWLM MEA.

Software/Hardware	Versions
FortiOS	<ul style="list-style-type: none">• 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• 7.0.5• 7.2.0• 7.2.1• 7.2.2
FortiAP	<ul style="list-style-type: none">• FortiAP version 6.4.x and 7.2.0• FortiAP-U versions 6.2.4

Enabling FortiWLM MEA

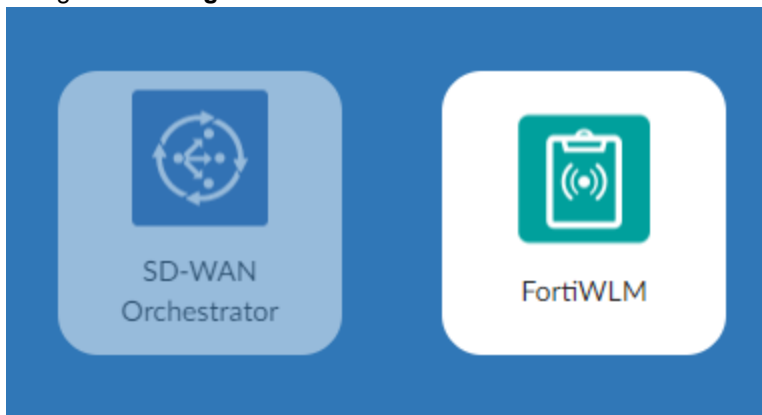
Follow this procedure to enable FortiWLM MEA.

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. On the left, the 'System Settings' menu is open, with 'Admin' and 'Administrators' highlighted. The main panel shows the 'Edit Administrator' configuration for the 'Admin' user. The 'JSON API Access' dropdown is set to 'Read-Write' and is highlighted with a red box. Other 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' > Advanced Options >.

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	7.0.0/7.0.1/7.0.2/7.0.3/7.0.5/7.2.0/7.2.1/7.2.2
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**.

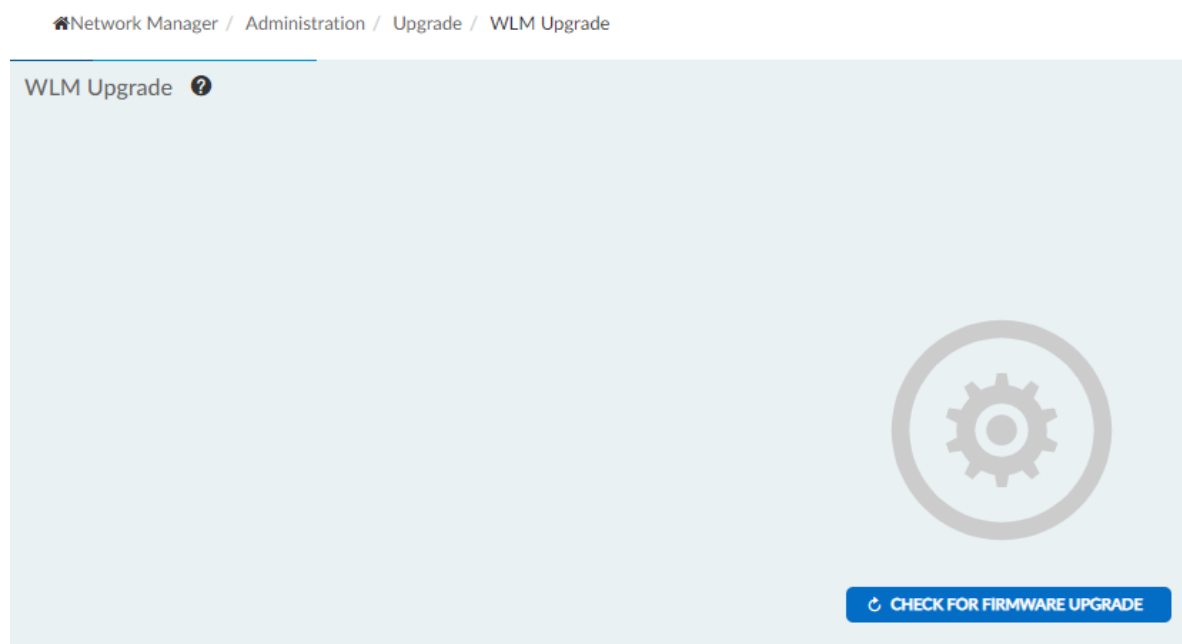
Upgrading FortiWLM MEA

The following upgrade paths are supported for this release of FortiWLM MEA.

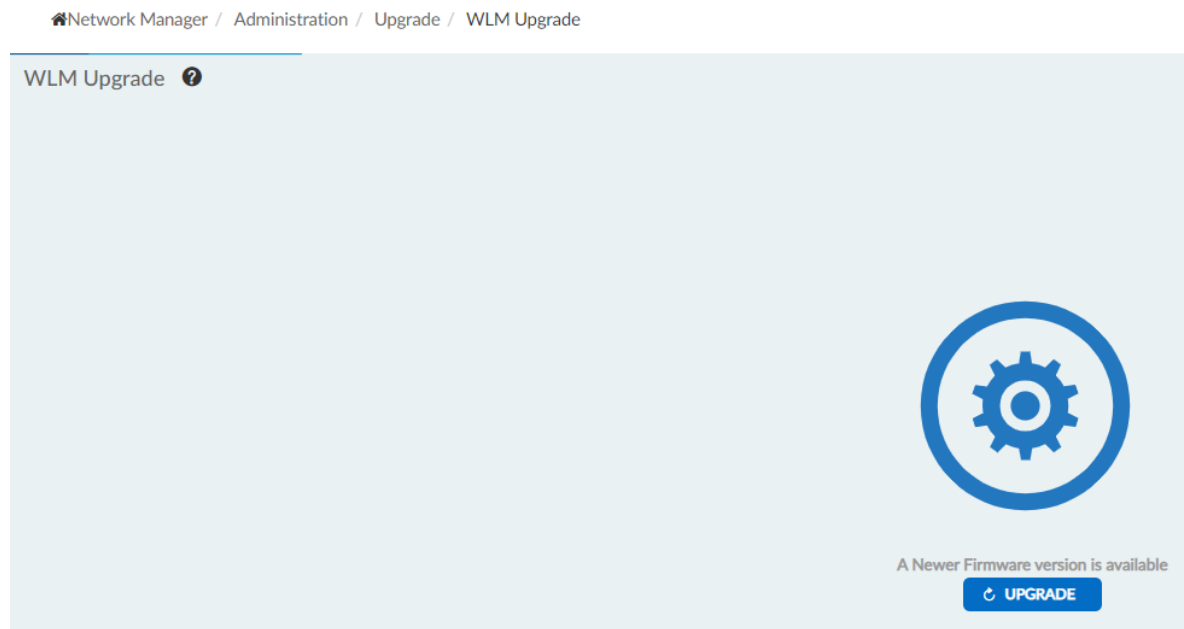
From...	To...
8.6.3 (FortiManager 7.0.3)	8.6.5 (FortiManager 7.2.1)
8.6.4 (FortiManager 7.2.1)	

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

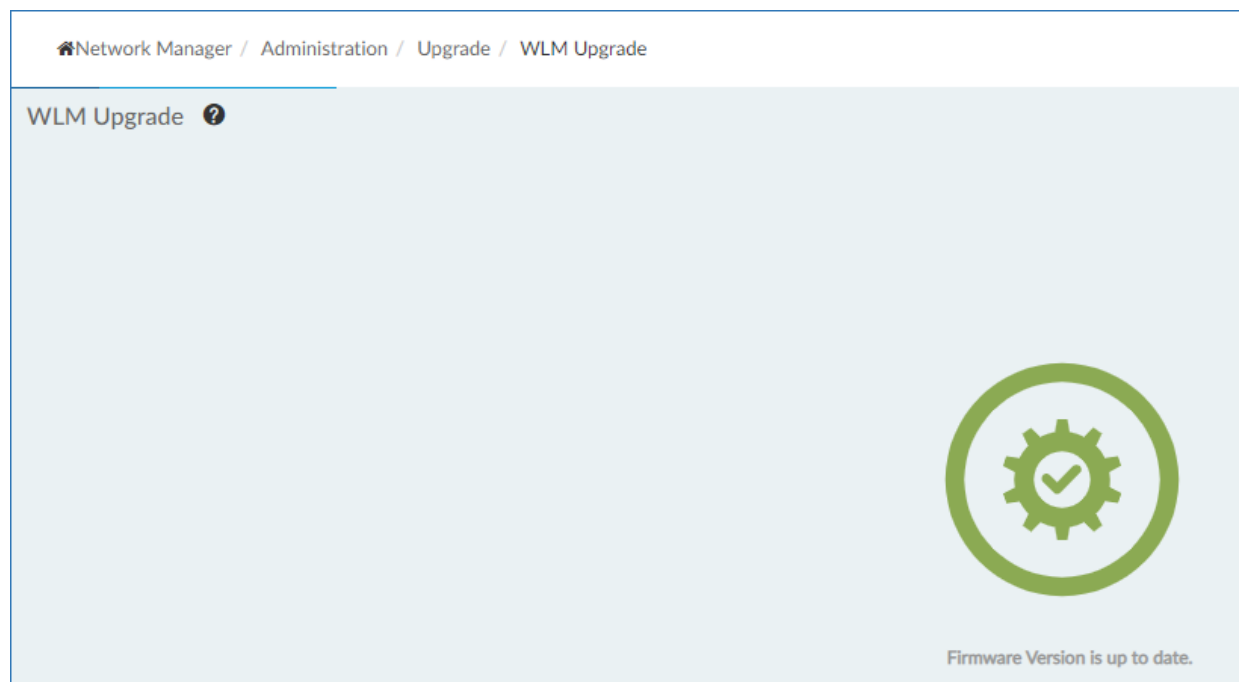
1. Click **Check For Firmware Upgrade**.



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.




Fixed Issues

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

Bug ID	Description
832624	Incorrect data displayed in the Network Summary dashboard.
861950	Unable to delete buildings from the maps.
871231	SSIDs and AP details not displayed in the Channel Summary page.

www.fortinet.com



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.