

Release Notes

FortiWLM MEA 8.6.4



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



July 19, 2022

FortiWLM MEA 8.6.4 Release Notes

02-864-615221-20220719

TABLE OF CONTENTS

Change log	4
About FortiWLM MEA 8.6.4	5
Product Overview	6
What's New	7
Supported FortiOS and FortiAP	9
Enabling FortiWLM MEA	10
Operational Guidelines	11
SNMP Configurations	12
Upgrading FortiWLM MEA	13
Fixed Issues	15
Known Issues	16

Change log

Date	Change description
2022-07-19	FortiWLM MEA 8.6.4 release version.

About FortiWLM MEA 8.6.4

FortiWLM MEA release 8.6.4 delivers additional features for FortiGate management. See section [What's New on page 7](#)

Note: This release of FortiWLM MEA requires FortiManager version 7.2.1.

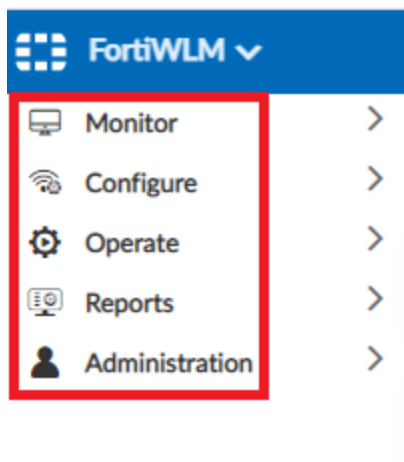
Product Overview

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).



What's New

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

- [Enhanced Scale Deployment](#)
- [VDOM support](#)
- [REST API FortiGate Timeout Configuration](#)
- [Automatic Import of FortiGate Controllers \(from FortiManager ADOM Device Management\)](#)
- [ADOM support for Map Management](#)

Enhanced Scale Deployment

This release of FortiWLM MEA delivers enhanced support for scale deployment of devices. The following scale deployment limits are supported when the polling interval is set to **1 minute** or **10 minutes**.

Devices	Maximum Limit
FortiGate controllers	1600
Access Points	3200
Stations	64000

The hardware requirements for the aforementioned scale deployments are **32 CPU/128 GB RAM/2 TB storage**.

VDOM support

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. To view the VDOM information, navigate to the following GUI pages.

- **Monitor > Overview > Network Summary (Stations)**
- **Operate > Inventory > Access Points**

REST API FortiGate Timeout Configuration

FortiGate REST API time out is now configurable. Navigate to **Operate > Inventory > Devices**. The **High Latency FortiGates** panel in the **Monitor > Overview > Network Summary** dashboard displays the REST API query delays at different times, to aid in the configuration of the REST API timeout.

Automatic Import of FortiGate Controllers (from FortiManager ADOM Device Management)

You can automatically import FortiGates managed by all or specific FortiManager ADOMs. Navigate to **Operate > Inventory > Devices**.

ADOM support for Map Management

Map Management support based on individual ADOM scope.

Supported FortiOS and FortiAP

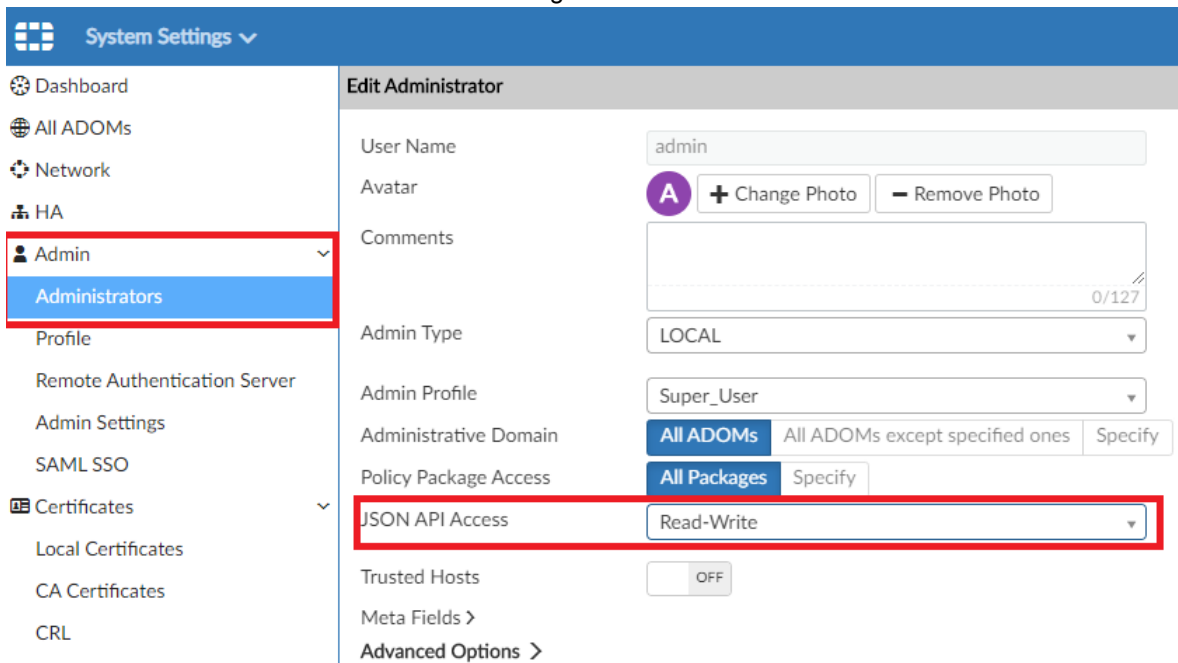
The following versions of FortiOS FortiAPs are supported with this release of FortiWLM MEA.

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
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

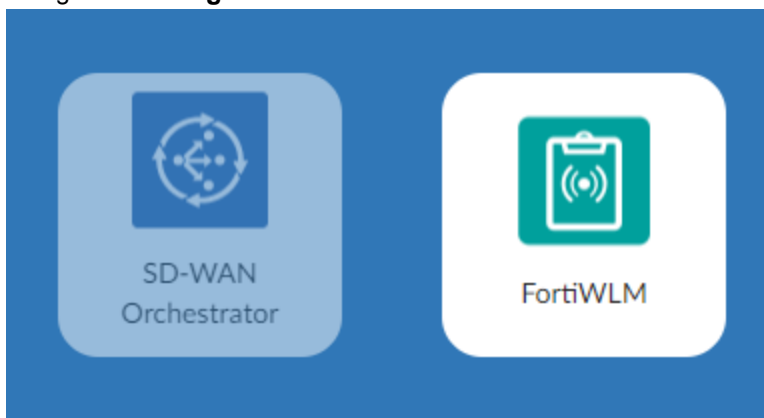
Follow this procedure to enable FortiWLM MEA.

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, and 'Administrators' is selected. The main area shows the 'Edit Administrator' page 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'.

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
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**.

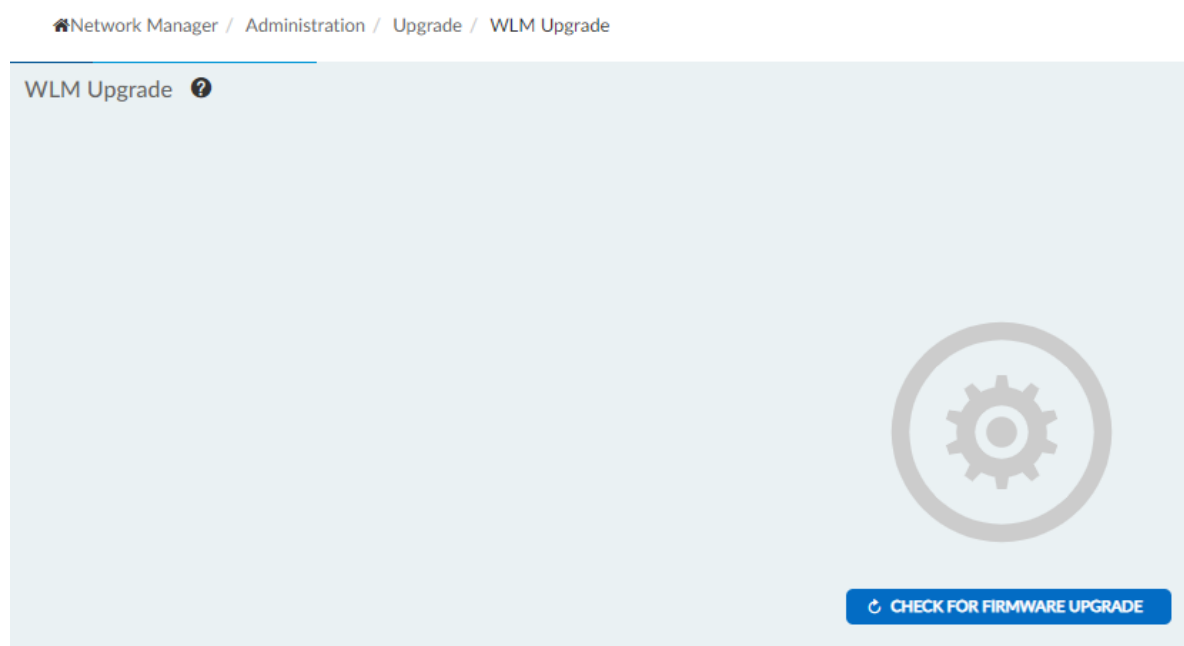
Upgrading FortiWLM MEA

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

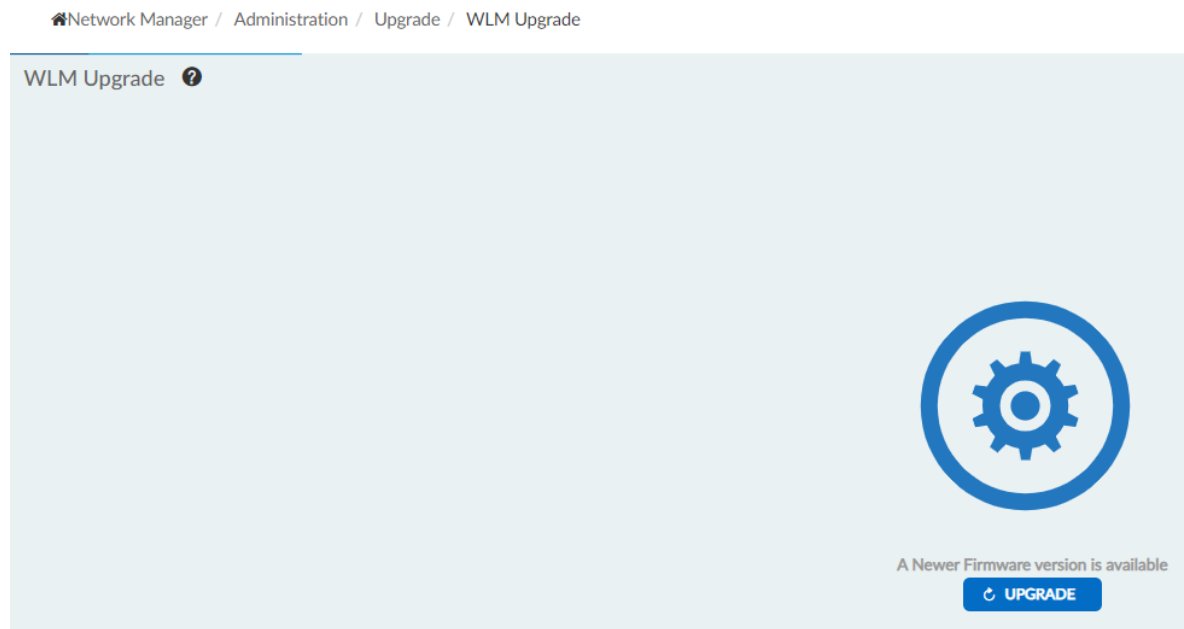
From...	To...
8.6.2 (FortiManager 7.0.2)	8.6.4 (FortiManager 7.2.1)
8.6.3 (FortiManager 7.0.3)	

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

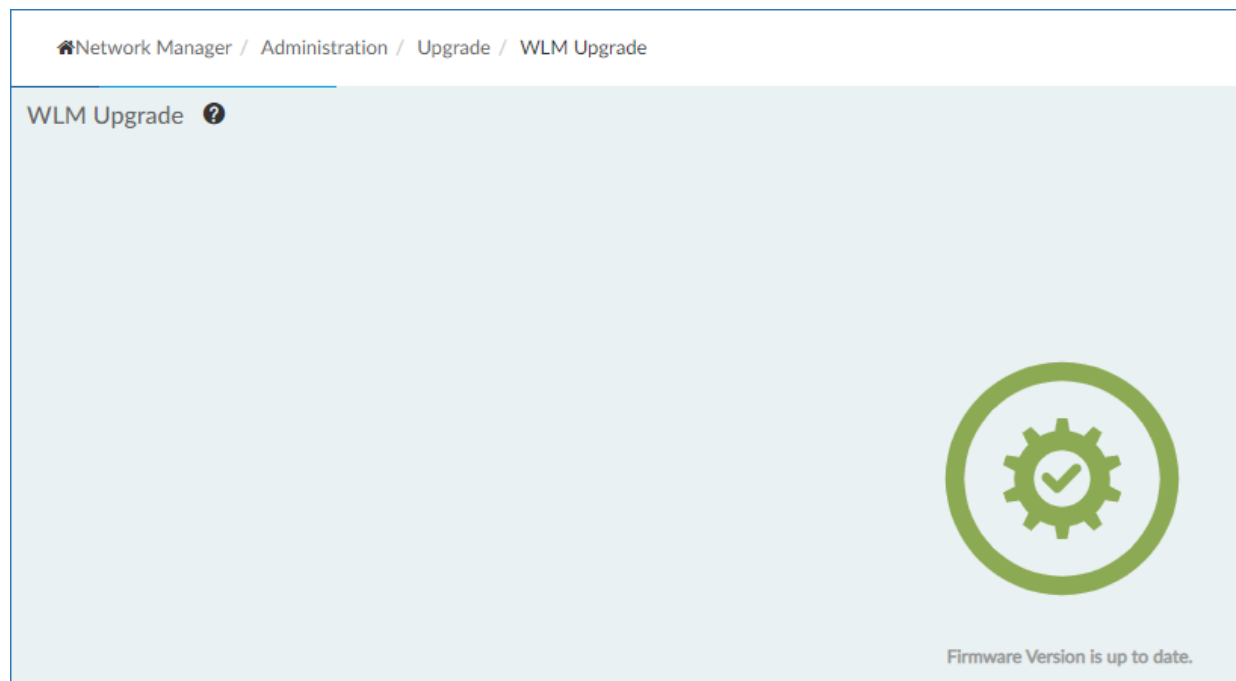
1. Click **Check For Firmware Upgrade**.



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
778472	Request to display an error message while creating campus names with special characters.
782353	Fault Management did not work on FortiWLM.
801028	The reports feature did not work after upgrading to FortiWLM 8.6.3.

Known Issues

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

Bug ID	Description	Impact	Workaround
807255	[scale deployment] Sometimes, <i>nmsfgtmgr</i> crashes are observed.	In a setup with 1000+ FortiGates, the FortiAP and station count may decrease during the period between the crash and recovery.	
821346	FortiWLM MEA data generated after the last automatic back up, is lost post upgrade.	Data or statistics generated from the last backup are lost.	
824261	Not allowed to delete maps [created before upgrade] even if the child nodes do not exist.		First, delete the FortiAPs and the maps from all ADOMs, then recreate the maps.
824945	Reports are duplicated (displayed twice) after upgrade.		Delete the duplicate report manually.



www.fortinet.com

Copyright© 2022 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.