

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

FortiWLM MEA - Release-Notes

Version 8.6.1

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

April 20, 2021

FortiWLM MEA 8.6.1 Release-Notes

02-861-615221-20210420

TABLE OF CONTENTS

Change log	4
Product Overview	5
Related Documentation	7
What's New	8
Spectrum Analyzer	8
VLAN Probe	8
FortiGate Controllers - Scale Deployment	9
Others	9
Supported FortiOS	11
Enabling FortiWLM MEA	12
Operational Guidelines	13
SNMP Configurations	14
Upgrading FortiWLM MEA	15
Known Issues	17
FortiGate Known Issues	17

Change log

Date	Change description
2021-04-20	FortiWLM MEA 8.6.1 release version.

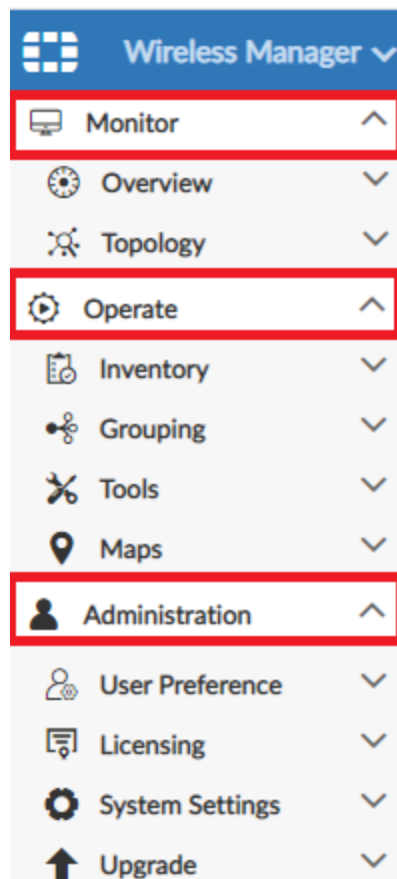
Product Overview

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 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 8.6.1 Administration Guide

What's New

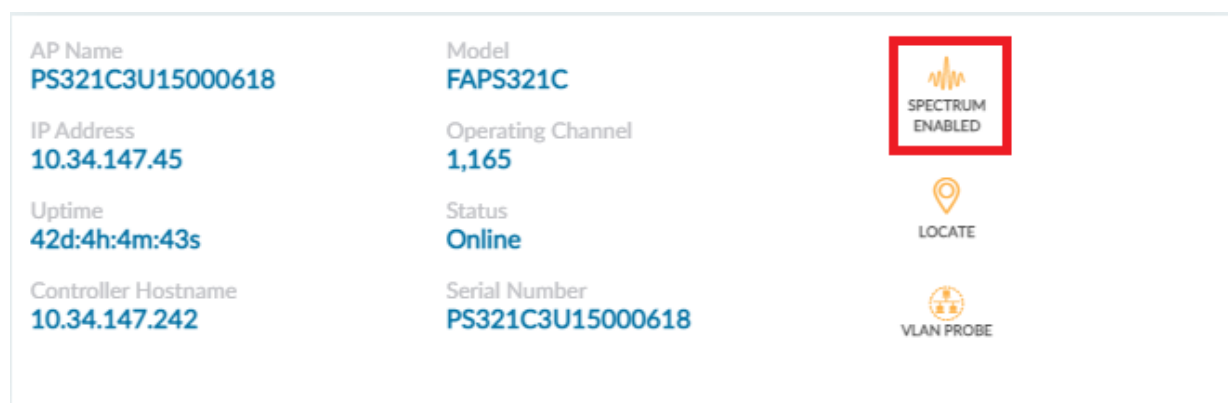
In this release of FortiWLM MEA, the following new features and functionalities are delivered.

- [Spectrum Analyzer on page 8](#)
- [VLAN Probe on page 8](#)
- [FortiGate Controllers - Scale Deployment on page 9](#)
- [Others on page 9](#)

Spectrum Analyzer

The Spectrum Analyzer Dashboard screen presents the interference information gathered from various radios. It provides a graphical representation of the interference devices activity in the 2.4Ghz and 5Ghz spectrum.

Navigate to *Monitor > Overview > AP* and click the **Spectrum Enabled** icon in the AP details tile.



Note: Spectrum Analyzer is supported on all AP models.

- FAP-U models support Spectrum Analyzer only if the radio is configured in **Dedicated Monitor** mode.
- FAP models support Spectrum Analyzer in AP mode and **Dedicated Monitor** mode; in the AP mode, the radio scans only operating channels.
- FAP-U43xF supports Spectrum Analyzer only on radio 3 configured in the **Dedicated Monitor** mode.

VLAN Probe

VLAN probe feature enables FortiAPs to probe connected VLANs and subnets. It sends DHCP probes from the FortiAP's Ethernet interface to specific VLANs on the wired interface and returns information on their availability and subnet details. This helps diagnose and troubleshoot WiFi deployment issues.

Navigate to *Monitor > Overview > AP* and click the **VLAN Probe** icon in the AP details tile.

VLAN Probe

Probe Retries

10

1 to 10

Timeout

1

1 to 60

VLAN Range:

140

to

155

1 - 4094

STOP

START

Search

VLAN ID	Available	SUBNET	AP INTERFACE	Date/Time
145	Available	10.34.145.1/24	eth0	2021-03-31 16:35:32
149	Available	10.34.149.1/24	eth0	2021-03-31 16:35:33
150	Available	10.34.150.1/24	eth0	2021-03-31 16:35:34
151	Available	10.34.151.1/24	eth0	2021-03-31 16:35:38
155	Not Available			

FortiGate Controllers - Scale Deployment

With this release you can monitor and manage FortiGate controllers concurrently associated with APs and stations in a large scale setup as per the following limits.

Supported Limits	FortiWLM MEA
Maximum Number of FortiGate controllers	600
Maximum Number of APs	2000
Maximum Number of Stations	25000
Licenses included (number of APs)	3 (without license)

Others

Offline access points are now displayed in the *Operate > Inventory > Access Point* page.

FortiWLM

ADOM: root admin

Monitor

Operate

Inventory

Devices

Access Points

Grouping

Tools

Maps

Administration

Network Manager / Operate / Inventory / Access Points

REFRESH DELETE FILTER

VIEW LATEST LOG

	AP NAME	SERIALNUMBER	IP ADDRESS	MAC ADDRESS	AP MODEL	RUNTIME IMAGE VERSION	AVAILABILITY STATUS	UPTIME	FORTIWLC / FORTIGATE NAME	ACTIONS
<input type="checkbox"/>										
<input type="checkbox"/>	PS321C3U15000618	PS321C3U15000618	10.34.147.45	90:6c:ac:34:B3:Aa	FAP5321C	PS321C-V6.0-Build0075	Online	33d:02h:43m:42s	10.34.147.242	
<input type="checkbox"/>	PS421E3X16001251	PS421E3X16001251	0.0.0.0	00:00:00:00:00:00	FAP5421E		Offline	00d:00h:00m:00s	10.34.147.242	
<input type="checkbox"/>	PU422ETF18000626	PU422ETF18000626	0.0.0.0	00:00:00:00:00:00	FAPU422EV		Offline	00d:00h:00m:00s	10.34.147.242	
<input type="checkbox"/>	PU321E4R17000089	PU321E4R17000089	0.0.0.0	00:00:00:00:00:00	FAPU321EV		Offline	00d:00h:00m:00s	10.34.147.242	
<input type="checkbox"/>	FP221CTF18021067	FP221CTF18021067	10.34.147.48	70:4c:a5:F9:72:8a	FAP221C	FP221C-V5.6-Build0493	Online	21d:21h:48m:05s	10.34.147.242	

Supported FortiOS

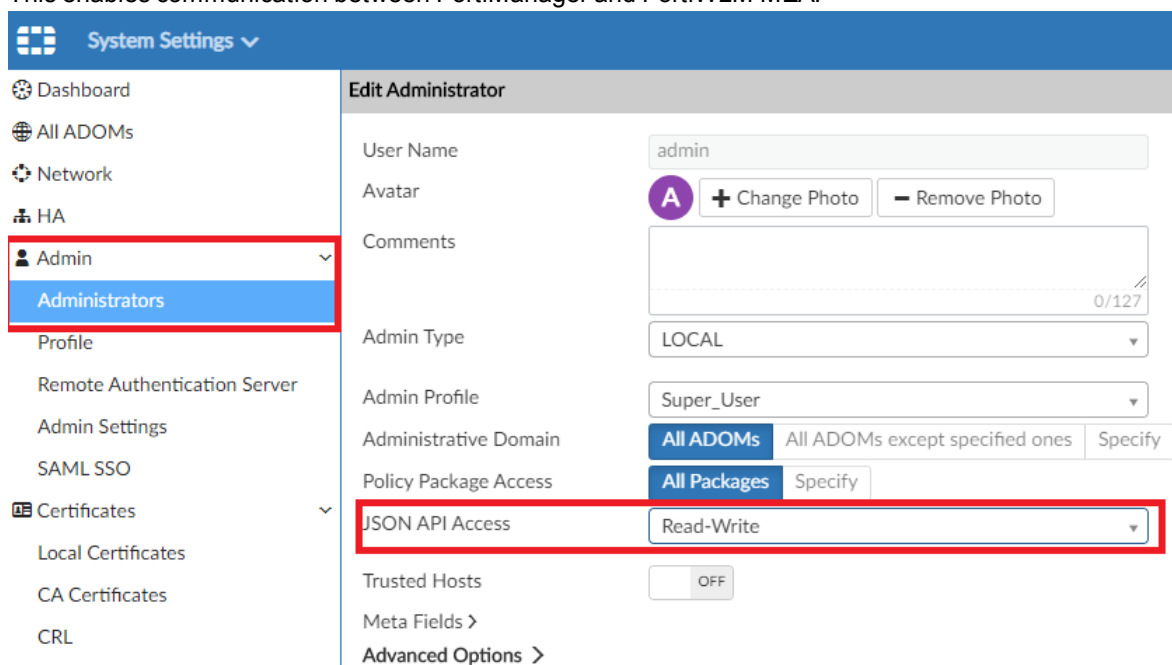
The following versions of FortiOS are supported with this release of FortiWLM MEA.

- 6.0.6 (limited monitoring)
- 6.2.0
- 6.2.1
- 6.2.2
- 6.2.3
- 6.4.0
- 6.4.1
- 6.4.2
- 6.4.3
- 6.4.4
- 6.4.5
- 7.0.0

Enabling FortiWLM MEA

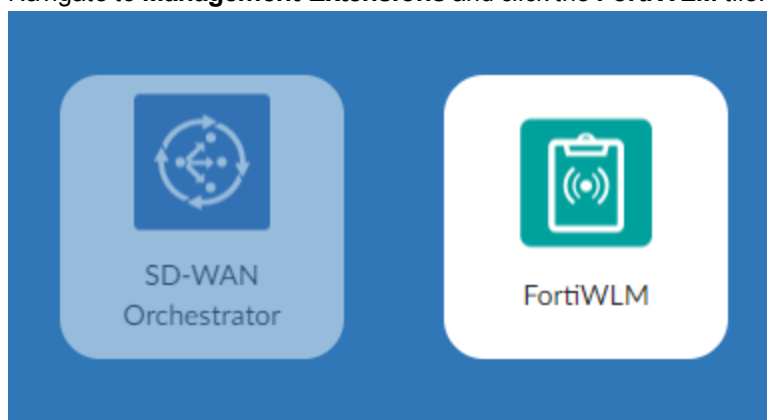
Follow this procedure to enable FortiWLM MEA.

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 shows the FortiManager GUI. On the left is a navigation menu with 'System Settings' expanded, showing 'Admin' and 'Administrators' (highlighted with a red box). The main area is titled 'Edit Administrator' and shows fields for 'User Name' (admin), 'Avatar', 'Comments', 'Admin Type' (LOCAL), 'Admin Profile' (Super_User), 'Administrative Domain' (All ADOMs), 'Policy Package Access' (All Packages), 'JSON API Access' (Read-Write, highlighted with a red box), 'Trusted Hosts' (OFF), 'Meta Fields', and '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				
	6.0.6	6.2.0/6.2.1	6.2.2/6.2.3	6.4.0/6.4.1/6.4.2/6.4.3/6.4.4/6.4.5	7.0.0
Dashboard Status					
Application Control	X	X	✓	✓	✓
Station Data	✓	✓	✓	✓	✓
Station activity logs	X	✓	✓	✓	✓
AP Dashboard					
Retry %	X	X	✓	✓	✓
Loss %	X	X	✓	✓	✓
Channel Utilization%	✓	✓	✓	✓	✓
SNR (dBm)	X	X	✓	✓	✓
Average Throughput	X	X	X	X	✓
Station Dashboard					
Retry %	X	X	✓	✓	✓
Loss %	X	✓	✓	✓	✓
Channel Utilization%	X	X	X	X	X
SNR (dBm)	✓	✓	✓	✓	✓

SNMP Configurations

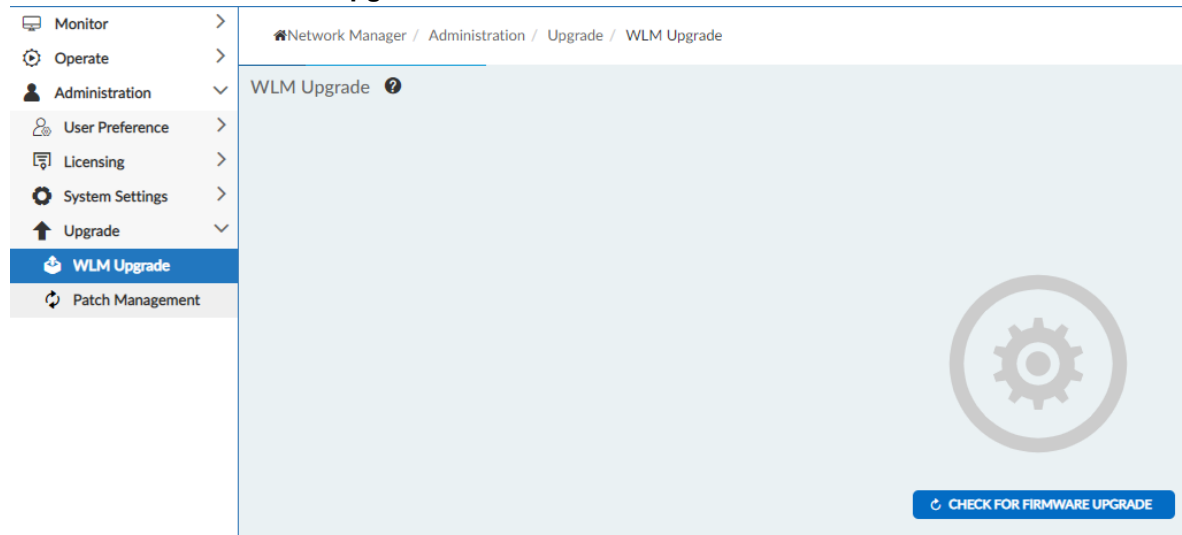
SNMP Traps use port 10162 to receive the AP down Alarm from FortiGate. The following FortiGate configuration is required in the FortiGate GUI.

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**.

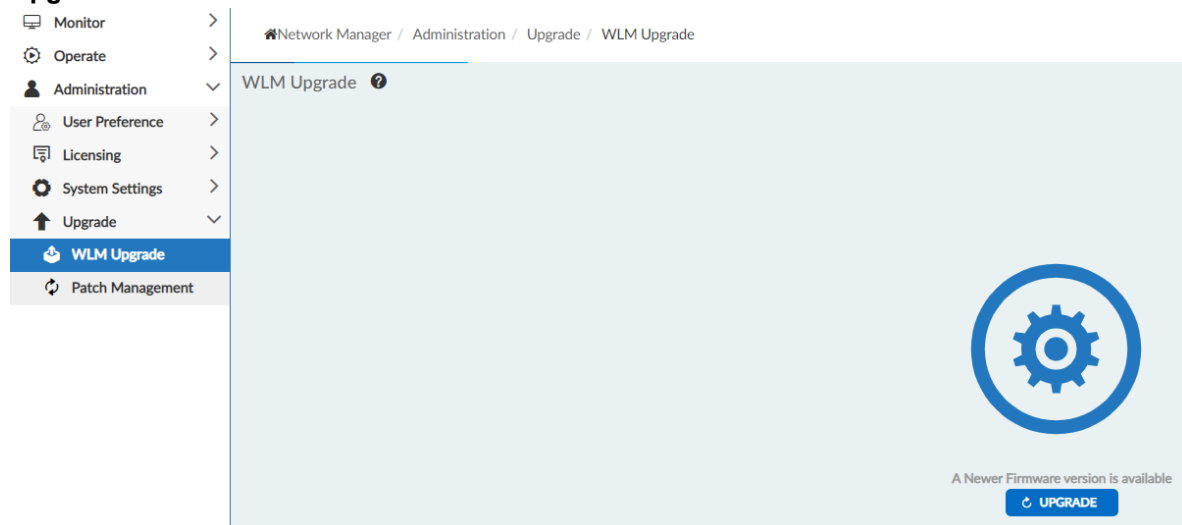
Upgrading FortiWLM MEA

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

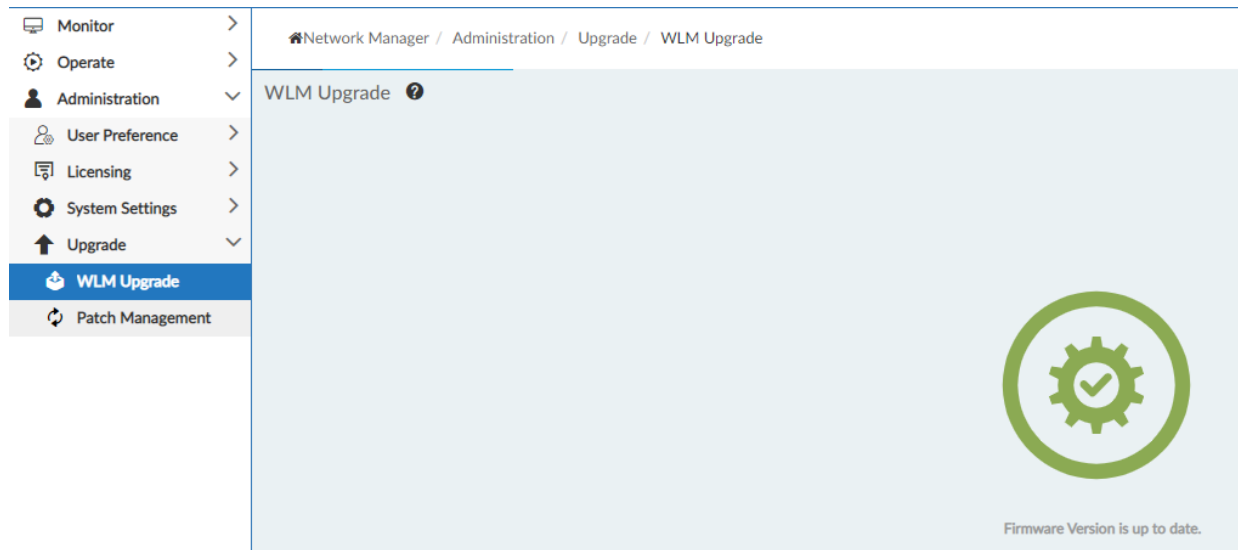
1. Click Check For Firmware Upgrade.



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.



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.		
656127	The Managment Administrative State is the only editable field in the Device inventory.		
703316	FortiGate does not respond when the VLAN Probe timeout value is configured at 60 seconds.		

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© 2021 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.