FORTINET
High Performance Network Security

FortiWAN Manager - Release Notes

VERSION 4.5.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

June 24, 2019

FortiWAN Manager 4.5.1 Release Notes Revision 1

38-451-566941-20190624

TABLE OF CONTENTS

Introduction

This document provides a list of new/changed features, upgrade instructions and caveats and resolved issues for FortiWAN Manager 4.5.1, build 0179.

FortiWAN Manager is a central management tool to perform monitoring, configuration backup/restore, firmware update and other management operations to multiple remote FortiWAN devices.

For additional documentation, please visit:

http://help.fortinet.com/fwanmgr/4-5-1/index.htm

What's new

The following list summarizes new and enhanced features. For details, see the FortiWAN Manager Handbook.

- **Support for Bandwith Manager** - Supports 8 priority levels in Bandwith Manager for managing the FortiWAN that are later than 4.5.0.

Hardware Support

FortiWAN Manager 4.5.1 is available as a virtual appliance, which requires a virtual machine environment. FortiWAN Manager supports the following hypervisor versions:

- VMware vSphere ESXi 5.0/5.1
- VMware vSphere Hypervisor 5.0/5.1

FortiWAN Manager 4.5.1 also requires the managed FortiWAN device running the firmware version later than FWN 4.2.0. Earlier version is not supported.

Upgrading

Start the upgrade procedure as follow:

- Always back up your system configurations and store in a safe place before upgrading.
- Log on to FortiWAN Manager as Administrator and go to [System > Administrator] page.
- Click Update to start the upgrade procedure
    - Click Browse to select the path where the new firmware image is saved.
    - Select Upload.
- Be patient while firmware is being upgraded. During the upgrade, do not turn off the system or repeatedly click the Submit button.
- The message “Update succeeded” will appear after the upgrade is completed. Please reboot the system afterward for the firmware to take effect.

Resolved issues

This section lists the resolved issues of this release, but is not a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
437952	The NSA IP contained in the ACCESS-REQUEST that FortiWAN Manager sent to a RADIUS server for authentication did not correspond to the specified NSA IP.
390317	CLI shows no error when setting multicast IP to port1
471796	PHP upgraded
484521	Failover setting of an AR policy in Config Editor gets lost if switching the pages to others and back to AR
484945	TCP ports 80/443 may fail RFC5961 test (CVE-2004-0230)
545174	NTP upgraded
553804	OpenSSH upgraded
560931	OpenSSL upgraded
560938	Apache httpd upgraded

Common Vulnerabilities and Exposures

FortiWAN Manager 4.5.1 is no longer vulnerable to the CVE-References in the below table.

Visit https://fortiguard.com/psirt for more information.

Bug ID	Description
484858	CVE-2018-1000001, CVE-2018-6485, CVE-2018-6551
508639	CVE-2018-5391
510768	CVE-2018-15473
513337	CVE-2018-17082
560944	CVE-2019-9023

FORTINET®

High Performance Network Security