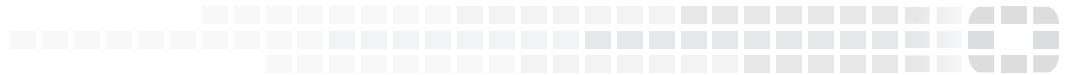




FORTINET®
High Performance Network Security



FortiWAN - Release Notes

VERSION 4.5.6

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



March 7, 2019

FortiWAN 4.5.6 Release Notes Revision 1

38-456-541178-20190307

TABLE OF CONTENTS

Introduction	4
What's new	5
Hardware Support	6
Upgrading	7
Downgrading	9
Resolved issues	10
Known issues	11

Introduction

This document provides a list of new/changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiWAN 4.5.6, build 0338, for model 200B, 1000B, 3000B, VM-02 and VM-04.

FortiWAN is a Link Load Balancing, Multi-Homing and Tunnel Routing system that distributes outbound or inbound internet traffic across multiple WAN links of differing technologies as well as building multi-link VPNs between sites.

For additional documentation, please visit:

<http://help.fortinet.com/fwan/4-5-6/index.htm>

What's new

FortiWAN 4.5.6 is for bug fixes only, please refer to "Resolved issues".

Hardware Support

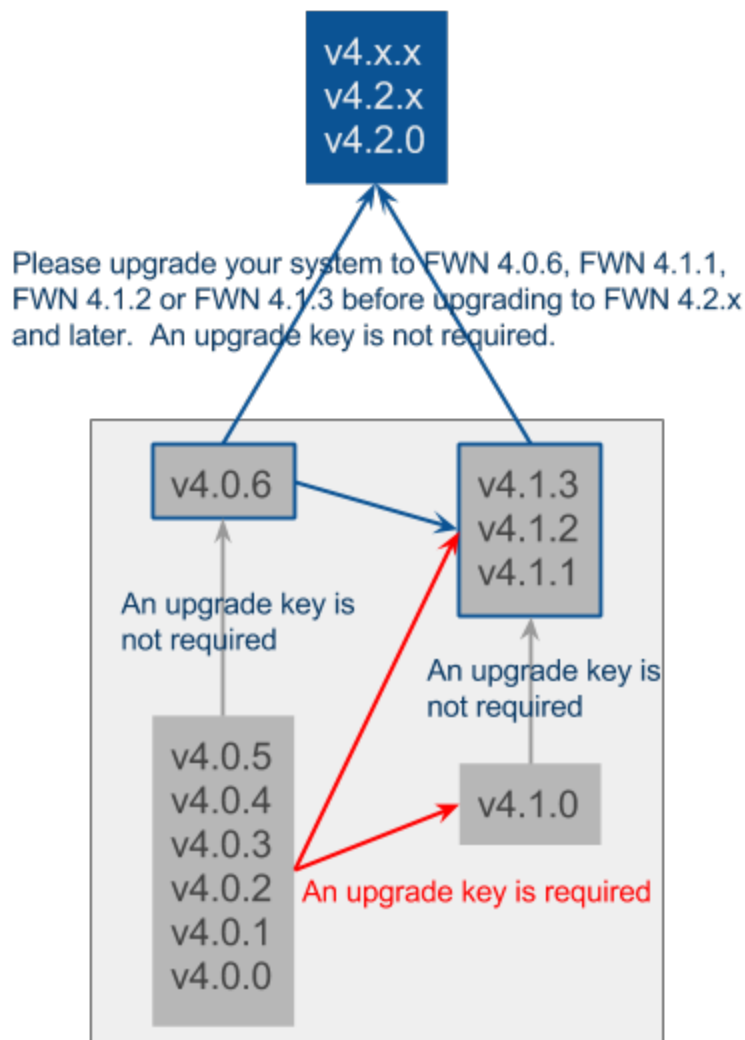
FortiWAN 4.5.6 for FortiWAN supports FortiWAN 200B, FortiWAN 1000B, FortiWAN 3000B, FortiWAN-VM-02 and FortiWAN-VM-04.

AscenLink series models are not supported.

Upgrading

FortiWAN 200B, FortiWAN 1000B and FortiWAN 3000B may have FWN 4.0.x installed respectively. In that case upgrade to FWN 4.5.6 as follows:

In early versions of FortiWAN firmware, it was necessary to obtain a Firmware Upgrade License Key to upgrade major releases of firmware (4.0.x - 4.1.x - 4.2.x). In late 2015, Fortinet decided to align the FortiWAN firmware upgrade policy with other Fortinet products, Firmware Upgrade Keys would no longer be required. In order to implement that, changes needed to be made in some maintenance releases of FortiWAN firmware. Please use the diagram below to select the current firmware you have and the desired latest firmware. You might need to first upgrade to a higher maintenance release (e.g. 4.0.1 - 4.0.6) of your current firmware (this never requires a key) before you can upgrade to the latest major release.



In the past FortiWAN (and AscenLink) required sequential major firmware upgrades (e.g. 4.0.x-4.1.x-4.2.x). With the above changes to “keyless” upgrades you will be able to upgrade directly to any release after the current one, “jumping” unneeded releases (e.g. 4.0.6-4.2.x).

After that, start the upgrade procedure as follow:

- Always back up your system configurations and store in a safe place before upgrading.
- Note that if you are upgrading from version 4.2.2 and earlier, please ensure that:
 - There are no duplicate label names among your original aggregated LAN or DMZ ports (go to *System > Network Setting > VLAN and Port Mapping* on Web UI). If there are duplicates, system will fail to boots up after upgrading to this release.
 - There is no any underscore character contained in label names of the original aggregated LAN or DMZ ports.
- Log on to FortiWAN 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, unplug the power 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.

Note that upgrade from AscenLink is not supported.

Fortinet default account/password

Fortinet default account/password (admin/null) is supported for FortiWAN's web-based manager and CLI for new shipped FortiWAN appliances with V4.1.0 and later firmware. However upgrading from earlier versions to V4.1.0 or later does not add the Fortinet default account/password to local authentication database of your current system. To login to the Web UI or CLI with Fortinet default account/password, you are still required to manually add it to your FortiWAN.

Downgrading

In that case downgrade to previous releases of firmware (4.0.x, 4.1.x or 4.2.0 - 4.2.4), you can downgrade directly to any release before the current one without any key being required. The downgrade procedure is similar to the upgrade one as follow:

- Always back up your system configurations and store in a safe place before downgrading.
- Note that if you are downgrading to version 4.2.2 or earlier, you must delete all aggregated port settings (go to *System > Network Setting > VLAN and Port Mapping* on Web UI) before downgrading, or system will fail to boots up after downgrading.
- Log on to FortiWAN as Administrator and go to [System > Administrator] page.
- Click Downgrade to start the downgrade procedure
 - Click Browse to select the old firmware image that you want to downgrade to.
 - Select Upload.
- Be patient while firmware is being downgraded. During the downgrade, do not turn off the system, unplug the power or repeatedly click the Submit button.
- The message "Downgrade succeeded" will appear after the downgrade is completed. Please reboot the system afterward for the firmware to take effect.

Note that downgrade from AscenLink is not supported.

Resolved issues

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

Table 1: Resolved issues

Bug ID	Description
535724	It was failed to email logs (Log Control) if log push is configured five days after boot up.
533859	FWN-VM v4.5.x did not support SCSI controller.
529594	Diag.data had the var/log/* files lost.
526874	WLHD did not restart PPPoE client when it detected the link was DOWN but PPP session was OK still.
517812	FortiWAN - Default only self resource reference (CSP) to avoid XSS attacks
537150	It happened on FortiWAN 3000B that bmstatd got crashed and GUI dashboard reported nothing.

Common Vulnerabilities and Exposures

FortiWAN 4.5.6 is no longer vulnerable to the CVE-References in the below table.

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

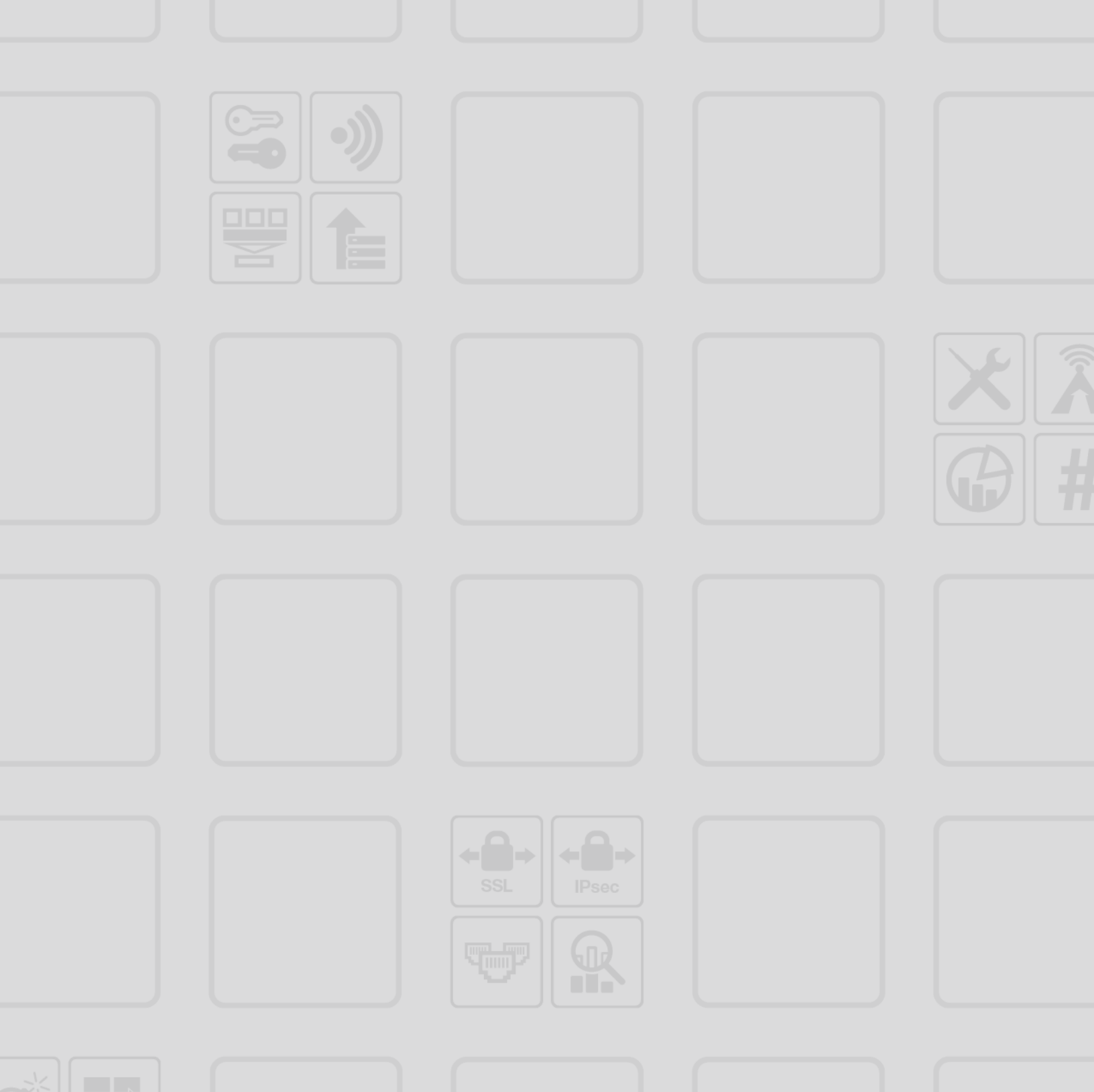
Bug ID	CVE references and other vulnerabilities
521297	• CVE-2018-0732

Known issues

This section lists the known issues of this release, but is not a complete list. For inquiries about a particular bug, please contact [Fortinet Customer Service & Support](#).

Table 2: Known issues

Bug ID	Description
272709	The Status LEDs on the front panel of FortiWAN units do not function currently. They are reserved for future use.
406701	FWN-1000B and 3000B will not recognize an existing RJ45 Copper SFP if it removed and re-inserted in a working system. User is required to: • renegotiate the NIC through the CLI command <code>diagnose hardware ethtool -r [port_name]</code> (specify <code>port_name</code> with <code>port1</code>, <code>port2</code>, <code>port3</code>, etc.), or • reboot the system in order for the SFP to operate. User can install new RJ45 SFP without affecting system. Removing an RJ45 SFP and inserting a fiber SFP in its place will have the same issue.



FORTINET®

High Performance Network Security



Copyright© 2019 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.