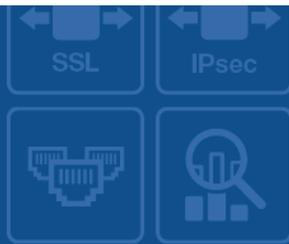


FortiWAN - Release Notes

VERSION 4.2.5



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



September 9, 2016

FortiWAN 4.2.5 Release Notes Revision 2

38-425-384107-20160909

TABLE OF CONTENTS

Introduction	4
What's new	5
Hardware Support	6
Upgrading	7
Downgrading	9
Resolved issues	10
Known issues	12

Introduction

This document provides a list of new/changed features, upgrade instructions and caveats, resolved issues, and known issues for FortiWAN 4.2.5, build 0148, 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/4-2-5/index.htm>

What's new

FortiWAN 4.2.5 is for bug fixes only, please refer to "Resolved issues".

Hardware Support

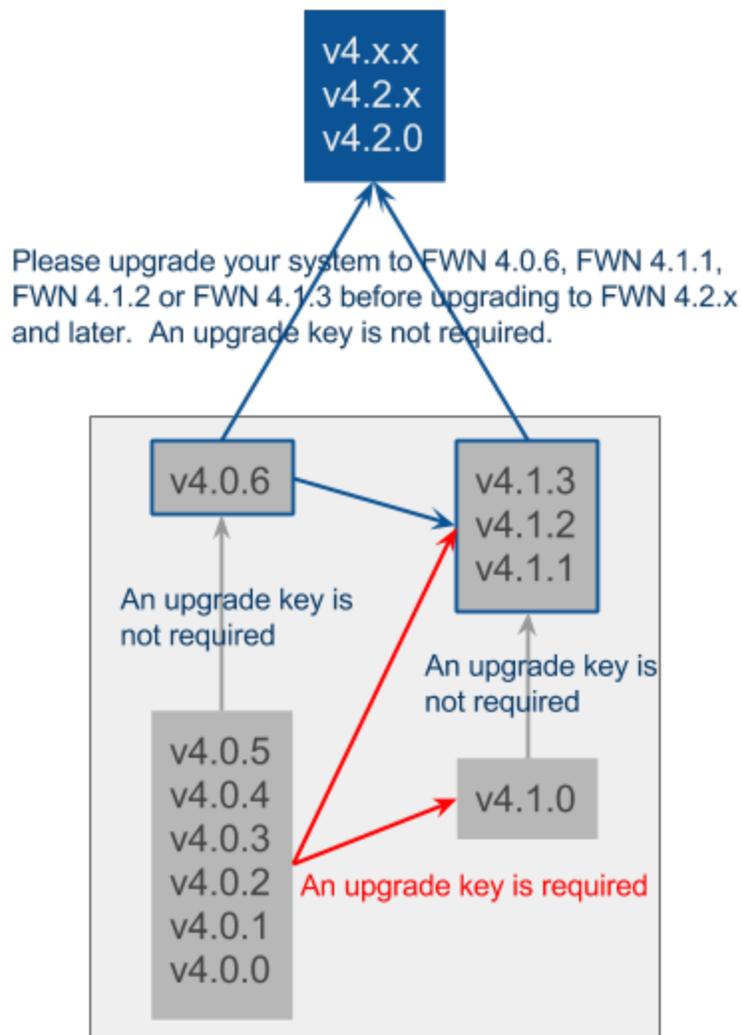
FortiWAN 4.2.5 for FortiWAN supports FortiWAN 200B, FortiWAN 1000B, FortiWAN 3000B, FortiWAN-VM-02 and FortiWAN-VM-04.

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 4.2.5 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.

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
370054	Compared with FortiWAN V4.0.x, data transmission performance of Tunnel Routing running on FortiWAN V4.1.x and V4.2.0 - V4.2.2 was lower. In release V4.2.3, the performance of one-way Tunnel Routing transmission (download or upload at a time) was improved by disabling the GRO module, but bidirectional transmission (download and upload at the same time) was still lower than expected. TCP control packets (TCP packets without carrying data payloads) distributed over tunnels were very likely to be overwhelmed if the tunnels were full of bidirectional traffic, which resulted in out-of-order delivery to packets of the TR connections. By fixing TCP control packets of the connections to a single tunnel (data packets of the connections will still be distributed among tunnels), out-of-order delivery is significantly reduced in this release and the overall performance of bidirectional TR transmission gets improved.
379884	FortiWAN's Web UI refused a SRV record of a Multihoming domain if the contained SRV target was not in the same domain.
381565	It failed to reset MTU of a WAN link from default 1500 to 1492 on Web UI. Other values were acceptable but 1492.
381609	FortiWAN was vulnerable to command injection attacks. A remote attacker could execute system commands to system back-end by injecting statements in GET method request (see CVE-2016-4965).
381610	A non-administrative authenticated attacker could manipulate the "UserName" parameter of GET method requests to have access privilege using FortiWAN's tcpdump tool (see CVE-2016-4966 and CVE-2016-4967).
381613	Low-rights authenticated users could view the system configuration in some firmware versions. This should only be available to administrative rights users (see CVE-2016-4967).
381614	A security vulnerability that might result in disclosure of PHP cookie was found affecting FortiWAN. An attacker could use it to log into FortiWAN Web UI as an administrator (see CVE-2016-4968).
381616	A Cross-Site Scripting (XSS) vulnerability was found affecting FortiWAN. Privileged guest user accounts and restricted user accounts could inject malicious scripts to the application-side or client-side of FortiWAN's Web UI to steal sensitive information. This potentially enables XSS attacks (see CVE-2016-4969).
382162	After system being rebooted, it failed to apply new configuration of DNS Proxy to system backend but Web UI displayed a success message rather than popping up errors. ProxyDNS still operated as the old configuration.

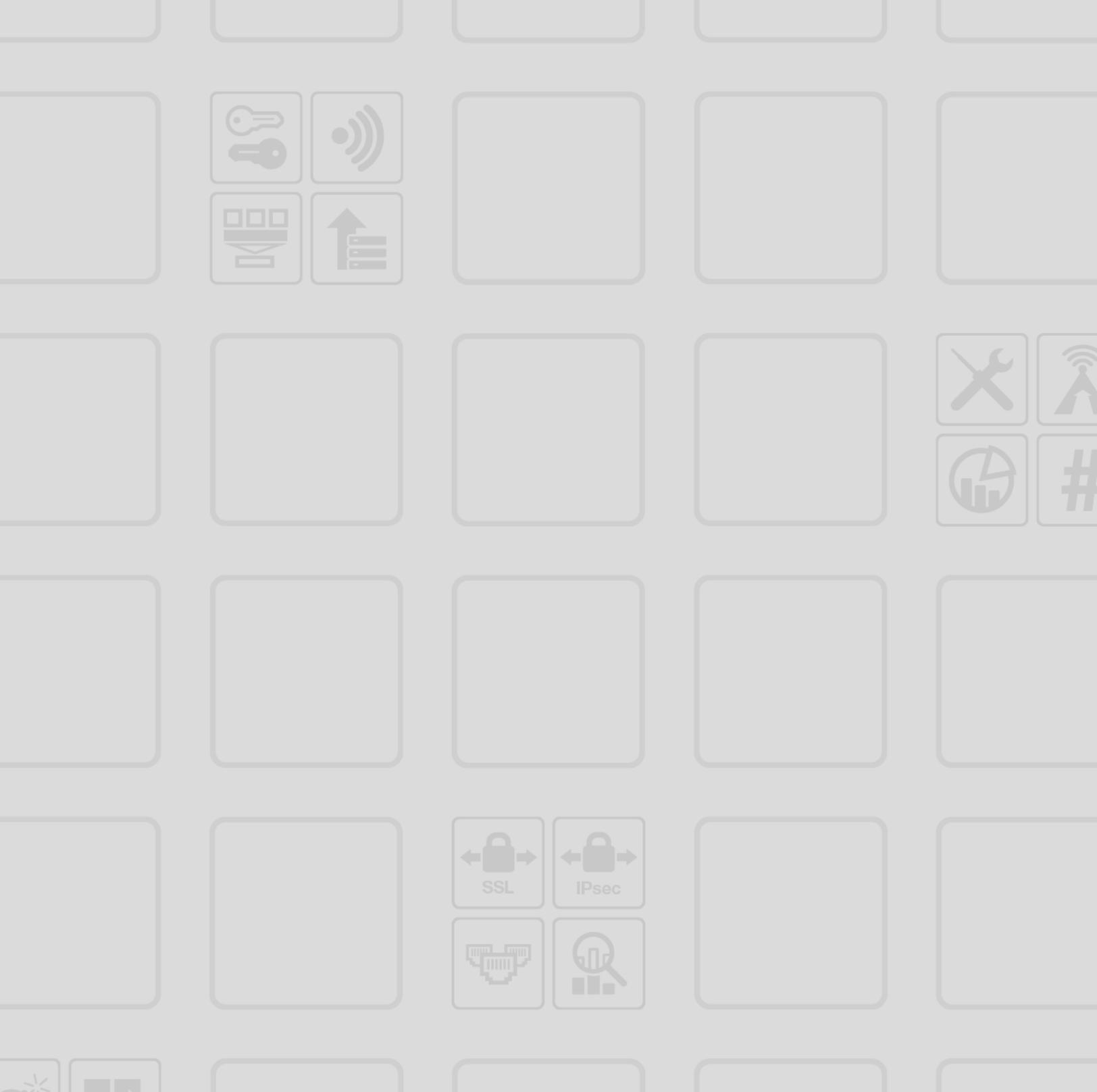
Bug ID	Description
383485	IP grouping went wrong to evaluate an IP address if the IP address belonged to multiple groups and positions of those IP groups listed on Web UI (System > IP Grouping) were changed (by clicking Move Down or Move Up buttons). Services (Firewall, Auto Routing and etc.) filter rules associated with those IP groups might be impacted.
383488	It failed to export a Multihoming configuration to FortiWAN if the configuration contained any non-numerical character in the IP Number field of a PTR record.
383571	FortiWAN kernel was patched to fix security a vulnerability CVE-2016-5696.
384068	The PHP package employed by FortiWAN was upgraded to 5.5.38 to fix security vulnerabilities CVE-2016-6288, CVE-2016-6289, CVE-2016-6290, CVE-2016-6296 and CVE-2016-6297.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires 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.



FORTINET

High Performance Network Security



Copyright© 2016 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.