FortiWAN - Release Notes

Version 4.5.9

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 COOKBOOK
https://cookbook.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: techdocs@fortinet.com

February 25, 2022
FortiWAN 4.5.9 Release Notes
00-400-000000-20220225

TABLE OF CONTENTS

Change Log

Date	Change Description
February 25, 2022	Initial release.

Introduction

This document provides a list of new/changed features, upgrade instructions and caveats and resolved issues for FortiWAN 4.5.9, build 0345, 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 https://docs.fortinet.com/product/fortiwan/4.5.

What's New

FortiWAN 4.5.9 addresses bug fixes and there are no new features. Please refer to Resolved Issues on page 11.

Hardware Support

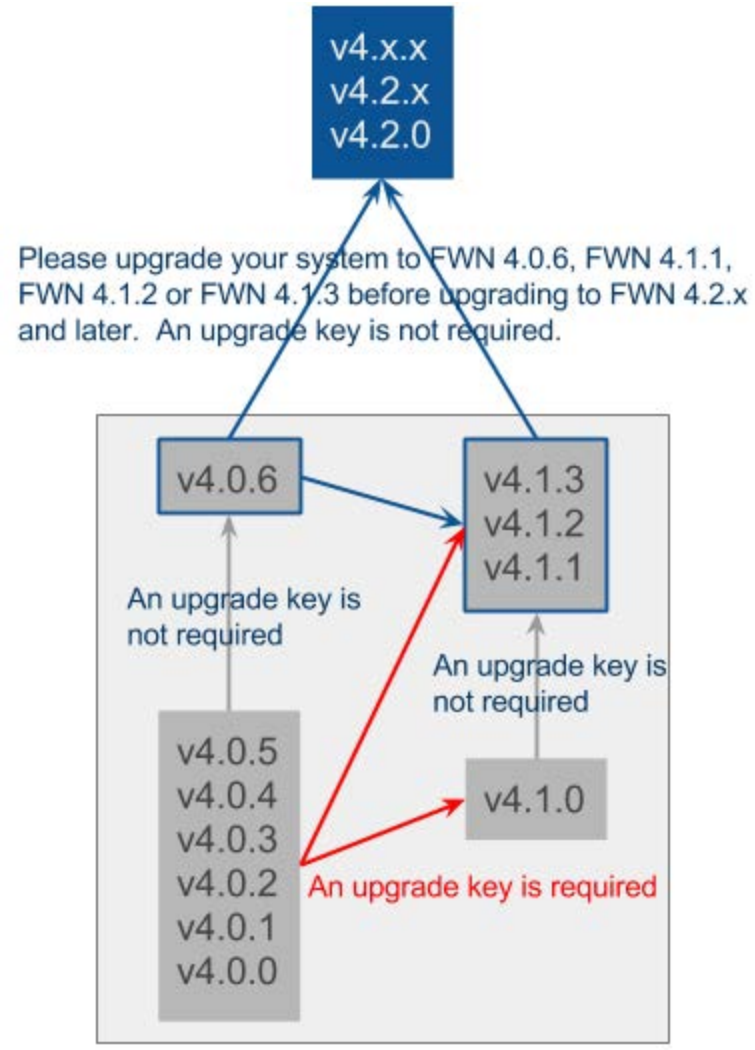
FortiWAN 4.5.9 for FortiWAN supports FortiWAN 200B, FortiWAN 1000B, FortiWAN 3000B, FortiWAN-VM-02 and FortiWAN-VM-04.

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 FWAN 4.5.9 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 follows:

- Always back up your system configurations and store in a safe place before upgrading.
- **Note**: 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, the system will fail to boot up after upgrading to this release.
  - There are no underscored characters contained in the label names of the original aggregated LAN or DMZ ports.
- Log in 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 the 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: Upgrading 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**: 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, otherwise, the system will fail to boot up after downgrading.
- Log in 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 the 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: Downgrading from AscenLink is not supported.

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.

Bug ID	Description
0735383	Report pages become unavailable after upgrading to FortiWAN 4.5.9.

Common Vulnerabilities and Exposures

FortiWAN 4.5.9 is no longer vulnerable to the CVE-References in the below table.

For more information, visit https://www.fortiguard.com/psirt.

Bug ID	Description
0769987	CVE-2021-41184, CVE-2021-41183, CVE-2021-41182
0758509	CVE-2021-25219
0757445	CVE-2021-21703
0744294	CWE-788: Access of Memory Location After End of Buffer
0722570	CWE-79: Improper Neutralization of Input During Web Page Generation ("Cross-site Scripting")
0720032/ 0720031/ 0720030/ 0720029/ 0719701/ 0718189/ 0717225/ 0715967	CWE-121: Stack-based Buffer Overflow
0719675/ 0718490/ 0718187/ 0714980	CWE-78: Improper Neutralization of Special Elements used in an OS Command ("OS Command Injection")
0718186	CWE-327: Use of a Broken or Risky Cryptographic Algorithm
0716614/ 0714977	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ("SQL Injection")
0715949	CWE-760: Use of a One-Way Hash with a Predictable Salt