



FortiSwitch - Release Notes

3.5.3

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 17, 2018

FortiSwitch 3.5.3 Release Notes

11-353-410990-20180617

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported models	5
What's new in 3.5.3	5
Special Notices	6
Supported Features	6
FortiSwitch 100	6
FortiSwitch 200	8
FortiSwitch 400	9
FortiSwitch 500	11
FortiSwitch 1000	13
FortiSwitch 3000	14
Default STP edge-port state changed to enabled	15
Connecting multiple FSW-R-112D-POE switches	15
Upgrade Information	16
Cooperative Security Fabric Upgrade	16
Product Integration and Support	17
FortiSwitch 3.5.3 support	17
Resolved Issues	19
Known Issues	20

Change Log

Date	Change Description
2017-04-04	Initial release.
2017-04-07	Revision 1: • Added Known Issue #415380. • Updated the document ID to 11-353-410990-20170404.
2017-06-30	Added a fixed issue (405123).
2018-06-17	Updated the description of bug 405123.

Introduction

This document provides the following information for FortiSwitch 3.5.3 build: 0265

- [Supported models](#)
- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

See the [Fortinet Document Library](#) for FortiSwitch documentation.

Supported models

FortiSwitch 3.5.3 supports the following models:

FortiSwitch	FSR-112D-POE, FSR_124D, FSW-108D-POE, FSW-124D, FSW-124D-POE, FSW-224D-FPOE, FSW-224D-POE, FSW-248D-FPOE, FSW-248D-POE, FSW_248D, FSW-424D, FSW-424D-FPOE, FSW-424D-POE, FSW-448D, FSW-448D-FPOE, FSW-448D-POE, FSW-524D-FPOE, FSW-524D, FSW-548D, FSW-548D-FPOE, FSW-1024D, FSW-1048D, FSW-3032D
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in 3.5.3

FortiSwitch 3.5.3 includes the following features and enhancements:

- 802.1x improvements (FortiSwitch Port Security Policy Framework)

Special Notices

Supported Features

Features support by model.

FortiSwitch 100

Feature	FSW-108D-POE	FSR-112D-POE	FSW-124D	FSW-124D-POE	FSR-124D
48 port lag support					
801.1x port mode	✓	✓	✓	✓	✓
802.1x MAC base security mode			✓	✓	✓
ACL			✓	✓	✓
Auto module max speed detection & notification					
CPLD Software Upgrade Support for OS					
DHCP relay feature			✓	✓	✓
DHCP Snooping			✓	✓	✓
HTTP REST APIs	✓	✓	✓	✓	✓
HW based ECMP					

Feature	FSW-108D- POE	FSR-112D- POE	FSW-124D	FSW-124D- POE	FSR-124D
IGMP Snooping			✓	✓	✓
IP conflict detection & notification	✓	✓	✓	✓	✓
LAG min-max-bundle	✓	✓	✓	✓	✓
LLDP transmit	✓	✓	✓	✓	✓
LLDP-MED	✓	✓	✓	✓	✓
Loop-guard	✓	✓	✓	✓	✓
MAC-IP Binding					
POE-pre-standard detection	✓	✓		✓	
QOS: 802.1p support			✓	✓	✓
SFLOW	✓	✓	✓	✓	✓
Software Routing Only	✓	✓			
Static BFD			✓	✓	✓
Static L3/HW based routing			✓	✓	✓
Storm Control	✓	✓	✓	✓	✓
Virtual Wire			✓	✓	✓
vlan tag by ACL			✓	✓	✓
vlan tag by MAC/IP/802.1x	✓	✓	✓	✓	✓

FortiSwitch 200

Feature	FSW-224D- POE	FSW-224D- FPOE	FSW-248D	FSW-248D- POE	FSW-248D- FPOE
48 port lag sup- port			✓	✓	✓
802.1x port mode	✓	✓	✓	✓	✓
802.1x MAC base security mode		✓	✓	✓	✓
ACL		✓	✓	✓	✓
Auto module max speed detection & notification					
CPLD Software Upgrade Sup- port for OS					
DHCP relay fea- ture		✓	✓	✓	✓
DHCP Snoop- ing		✓	✓	✓	✓
HTTPS REST APIs	✓	✓	✓	✓	✓
HW based ECMP					
IGMP Snoop- ing		✓	✓	✓	✓
IP conflict detection & notification	✓	✓	✓	✓	✓
LAG min-max- bundle	✓	✓	✓	✓	✓
LLDP transmit	✓	✓	✓	✓	✓

Feature	FSW-224D- POE	FSW-224D- FPOE	FSW-248D	FSW-248D- POE	FSW-248D- FPOE
LLDP-MED	✓	✓	✓		✓
Loop-guard	✓	✓	✓	✓	✓
MAC-IP Bind- ing					
POE-pre-stand- ard detection	✓	✓		✓	✓
QOS: 802.1p support		✓	✓	✓	✓
SFLOW	✓	✓	✓	✓	✓
Software Rout- ing Only	✓				
Static BFD		✓	✓	✓	✓
Static L3/HW based routing		✓	✓	✓	✓
Storm Control	✓	✓	✓	✓	✓
Virtual Wire		✓	✓	✓	✓
vlan tag by ACL		✓	✓	✓	✓
vlan tag by MAC/IP/802.1x	✓	✓	✓	✓	✓

FortiSwitch 400

Feature	FSW-424D	FSW-424D- POE	FSW-424D- FPOE	FSW-448D	FSW-448D- POE	FSW-448D- FPOE
48 port lag sup- port						
802.1x port mode	✓	✓	✓	✓	✓	✓

Feature	FSW-424D	FSW-424D- POE	FSW-424D- FPOE	FSW-448D	FSW-448D- POE	FSW-448D- FPOE
802.1x MAC base security mode	✓	✓	✓	✓	✓	✓
ACL	✓	✓	✓	✓	✓	✓
Auto module max speed detection & notification	✓	✓	✓	✓	✓	✓
CPLD Software Upgrade Sup- port for OS						
DHCP relay fea- ture	✓	✓	✓	✓	✓	✓
DHCP Snoop- ing	✓	✓	✓	✓	✓	✓
HTTP REST API	✓	✓	✓	✓	✓	✓
HW based ECMP						
IGMP Snoop- ing	✓	✓	✓	✓	✓	✓
IP conflict detection & notification	✓	✓	✓	✓	✓	✓
LAG min-max- bundle	✓	✓	✓	✓	✓	✓
LLDP transmit	✓	✓	✓	✓	✓	✓
LLDP-MED	✓	✓	✓	✓	✓	✓
Loop-guard	✓	✓	✓	✓	✓	✓
MAC-IP Bind- ing						

Feature	FSW-424D	FSW-424D- POE	FSW-424D- FPOE	FSW-448D	FSW-448D- POE	FSW-448D- FPOE
POE-pre-stand- ard detection		✓	✓		✓	✓
QOS: 802.1p support	✓	✓	✓	✓	✓	✓
SFLOW	✓	✓	✓	✓	✓	✓
Software Rout- ing Only						
Static BFD	✓	✓	✓	✓	✓	✓
Static L3/HW based routing	✓	✓	✓	✓	✓	✓
Storm Control	✓	✓	✓	✓	✓	✓
Virtual Wire	✓	✓	✓	✓	✓	✓
vlan tag by ACL	✓	✓	✓	✓	✓	✓
vlan tag by MAC/IP/802.1x	✓	✓	✓	✓	✓	✓

FortiSwitch 500

Feature	FSW-524D	FSW-524D-FPOE	FSW-548D	FSW-548D-FPOE
48 port lag support			✓	✓
802.1x port mode	✓	✓	✓	✓
802.1x MAC base security mode	✓	✓	✓	✓
ACL	✓	✓	✓	✓
Auto module max speed detection & notification	✓	✓	✓	✓
CPLD Software Upgrade Support for OS				

Feature	FSW-524D	FSW-524D-FPOE	FSW-548D	FSW-548D-FPOE
DHCP relay feature	✓	✓	✓	✓
DHCP Snooping	✓	✓	✓	✓
HTTP REST APIs	✓	✓	✓	✓
HW based ECMP	✓	✓	✓	✓
IGMP Snooping	✓	✓	✓	✓
IP conflict detection & notification	✓	✓	✓	✓
LAG min-max-bundle	✓	✓	✓	✓
LLDP transmit	✓	✓	✓	✓
LLDP-MED	✓	✓	✓	✓
Loop-guard	✓	✓	✓	✓
MAC-IP Binding	✓	✓	✓	✓
POE-pre-standard detection		✓		✓
QOS: 802.1p support	✓	✓	✓	✓
SFLOW	✓	✓	✓	✓
Software Routing Only				
Static BFD	✓	✓	✓	✓
Static L3/HW based routing	✓	✓	✓	✓
Storm Control	✓	✓	✓	✓
Virtual Wire	✓	✓	✓	✓
vlan tag by ACL	✓	✓	✓	✓
vlan tag by MAC/IP/802.1x	✓	✓	✓	✓

FortiSwitch 1000

Feature	FSW-1024D	FSW-1048D
48 port lag support		✓
802.1x port mode	✓	✓
802.1x MAC base security mode	✓	✓
ACL	✓	✓
Auto module max speed detection & notification	✓	✓
CPLD Software Upgrade Support for OS	✓	✓
DHCP relay feature	✓	✓
DHCP Snooping	✓	✓
HTTP REST APIs	✓	✓
HW based ECMP	✓	✓
IGMP Snooping	✓	✓
IP conflict detection & notification	✓	✓
LAG min-max-bundle	✓	✓
LLDP transmit	✓	✓
LLDP-MED	✓	✓
Loop-guard	✓	✓
MAC-IP Binding	✓	✓
POE-pre-standard detection		
QOS: 802.1p support	✓	✓
SFLOW	✓	✓
Software Routing Only		
Static BFD	✓	✓
Static L3/HW based routing	✓	✓

Feature	FSW-1024D	FSW-1048D
Storm Control	✓	✓
Virtual Wire	✓	✓
vlan tag by ACL	✓	✓
vlan tag by MAC/IP/802.1x	✓	✓

FortiSwitch 3000

Feature	FSW-3032D
48 port lag support	
802.1x port mode	✓
802.1x MAC base security mode	✓
ACL	✓
Auto module max speed detection & notification	
CPLD Software Upgrade Support for OS	
DHCP relay feature	✓
DHCP Snooping	✓
HTTP REST APIs	✓
HW based ECMP	✓
IGMP Snooping	✓
IP conflict detection & notification	✓
LAG min-max-bundle	✓
LLDP transmit	✓
LLDP-MED	✓
Loop-guard	✓
MAC-IP Binding	✓

Feature	FSW-3032D
POE-pre-standard detection	
QOS: 802.1p support	✓
SFLOW	✓
Software Routing Only	
Static BFD	✓
Static L3/HW based routing	✓
Storm Control	✓
Virtual Wire	✓
vlan tag by ACL	✓
vlan tag by MAC/IP/802.1x	✓

Default STP edge-port state changed to enabled

The default STP edge-port state on all switch interfaces is changed to **enabled**.

This change allows a port to transition directly the forwarding state, and skips the listening and learning stages. When a port is an edge port, it doesn't generate topology changes on link status changes, which results in a more stable network. These are key advantages of RSTP faster convergence and less topology changes. A STP enabled ports still transmits BPDU. When a STP enabled port receives a BPDU, it immediately loses edge port status and becomes a normal spanning tree port. A ports edge-status state can still be disabled if desired by using the following CLI commands:

```
S124DN3W14000095 # config switch interface
S124DN3W14000095 (interface) # edit port9
S124DN3W14000095 (port9) # set edge-port
disabled Disable interface as edge port.
enabled Enable interface as edge port.
```

Connecting multiple FSW-R-112D-POE switches

The FSW-R-112D-POE switch does not support interconnectivity to other FSW-R-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade Information

FortiSwitch 3.5.3 supports upgrading from FortiSwitch 3.5.0 and later.

Cooperative Security Fabric Upgrade

FortiOS 5.4.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1
- FortiClient EMS 1.0.1
- FortiAP 5.4.1
- FortiSwitch 3.4.2

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Framework - Upgrade Guide*
- *FortiOS 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*

This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

Product Integration and Support

FortiSwitch 3.5.3 support

The following table lists 3.5.3 product integration and support information.

Web browser	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
--------------------	---

**FortiOS
(FortiLink Support)**

- 5.4.1 and later
FortiSwitch must be upgraded first before upgrading FortiOS. Please read the *Upgrade Information > Cooperative Security Fabric Upgrade* section in this document.
- 5.4.0
FortiSwitch models: FSW-108D-POE, FSW-124D, FSW-124D-POE, FSW-224D-POE, FSW-224D-FPOE, FSW-248D-POE, FSW-248D-FPOE, FSW-424D, FSW-424D-POE, FSW-424D-FPOE, FSW-448D, FSW-448D-POE, FSW-448D-FPOE, FSW-524D, FSW-524D-FPOE, FSW-548D, FSW-548D-FPOE, FSW-1024D, FSW-1048D, FSW-3032D, FSR-112D-POE

FortiGate models: FG-60D, FG-60D-POE, FG-90D, FG-90-POE, FG-100D, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200D, FG-240D, FG-280D, FG-280D-POE, FG-600C, FG-800C, FG-1000C, FG-1500D, FG-1200D, FG-3700D, FG-3700DX

FortiWiFi models: FWF-60D, FWF-60D-POE, FWF-90D, FWF-90D-POE
- 5.2.3 and later
FortiSwitch models: FSW-108D-POE, FSW-124D, FSW-124D-POE, FSW-224D-POE, FSW-224D-FPOE, FSR-112D-POE

FortiGate models: FG-60D, FG-90D, FG-100D, FG-140D, FG-200D, FG-240D, FG-280D, FG-600C, FG-800C, FG-1000C, FG-60D-POE, FG-90D-POE, FG-140D-POE, FG-140D-POE-T1, FG-280D-POE

FortiWiFi models: FWF-60D, FWF-60D-POE, FWF-90D, FWF-90D-POE
- 5.2.2
FortiSwitch models: FSW-224D-POE

FortiGate models: FG-90D, FG-90D-POE, FG-100D, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200D, FG-240D, FG-280D, FG-280D-POE, FG-600C, FG-800C, FG-1000C

FortiWiFi models: FWF-90D, FWF-90D-POE

Resolved Issues

The following issues have been fixed in 3.5.3. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
403226	Cleanup internal certificates (Replace with new SHA256 signed cert from entrust)
405123	Upgrade OpenSSL lib for misc security issues.
403985	SPI-NOR based platform image upgrade process too slow and consume too much memory.
393518	qsfp: mismatching port-id between driver and user-space on platform 548D.
405504	Support 64 characters username in all authentication modules.
409612	Allow ports with igmp-snooping enabled into virtual wires, but reject VLANs with IGMP snooping enabled.
405717	The interface goes int default when increasing power usage onto the interface.
413228	L3 pkts not coming to kernel when sflow is enabled on the switch interface.
311065	TFTP performance in OS download.
383506	FSW Standalone: EAP tunnel is terminated at Authenticator(FSW) instead of at Auth-Server (FAC).
405123	FortiSwitch 3.5.3 is no longer vulnerable to the following CVE-References: • 2017-3731 • 2017-3732 • 2016-7055

Known Issues

The following known issues have been identified with 3.5.3. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
377609	PoE port does not reboot when you remove and insert the link.
393845	Newly-created static MACs are missing from the MAC address table.
393856	LLDP-MED does not time out quickly-enough on FSR124D.
393622	get switch dhcp-snooping status does not report correctly snoop-enabled-vlans.
393186	FSW does NOT allow timezones 00, 76, 82 and 86.
408113	The local user failed authentication when eap-passthru is enabled by default. Workaround: The user can change eap-passthru to disabled.
414802	IGMP-Snooping: Traffic flooding to newly assigned VLAN source port. Workaround: Create the VLAN and enable IGMP-S/DHCP-S before configuring the port.
414570	802.1 does not clean up completely when adding 802.1x interface to the trunk port. Workaround: Clear the 802.1x configuration before migrating to the trunk.
410200	802.1x: VLAN programming received from a RADIUS server can be overwritten by CLI configuration. Workaround: Do NOT manually change the VLAN assignment on a port that is in an authentication state.

Bug ID	Description
414060	When 802.1x is enabled with DHCP Snooping, DHCP Discover could leak to the server. Note: DHCP could leakage to the server/cserver could occur when .1x MAC-based mode is enabled. You could lose connectivity because of that. We recommend using port-based if DHCP blocking and .1x is critical to your business. Note: The 802.1x MAC-based mode is supported on the following models: • FS-108D-POE • FS-224D-POE • FSR-112D-POE
415380	When DHCP-Snooping is enabled, DHCP traffic could be inadvertently blocked preventing clients from receiving DHCP-assigned addresses when at least one ingress or ingress port is a trunk (Link Aggregate Group). Workaround: Disable DHCP-Snooping on the VLAN.



Copyright© 2018 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.