FortiSwitch - Release Notes

VERSION 3.5.1

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

November 21, 2016

FortiSwitch 3.5.1 Release Notes

11-351-394208-20161121

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
Supported models 5
What's new in 3.5.1 5
Special Notices **6**
Supported Features 6
FortiSwitch 100 6
FortiSwitch 200 8
FortiSwitch 400 9
FortiSwitch 500 11
FortiSwitch 1000 12
FortiSwitch 3000 14
Default STP edge-port state changed to enabled 15
Connecting multiple FSW-R-112D-POE switches 15
Configuring IGMP-Snooping under "vlan enable" + "port based disable" 15
Upgrade Information **16**
Cooperative Security Fabric Upgrade 16
Product Integration and Support **17**
FortiSwitch 3.5.1 support 17
Resolved Issues **19**
Known Issues **20**

Change Log

Date	Change Description
2016-11-16	Initial release.
2016-11-21	Added Resolved Issues > Common Vulnerabilities and Exposures > CVE Reference numbers.
2017-02-28	Added: "As a port is "disabled" by default, you must enable IGMP-S on both the VLAN and the port."

Introduction

This document provides the following information for FortiSwitch 3.5.1 build 0262:

- 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 3.5.1 supports the following models:

FortiSwitch	FSW-108D-POE, FSW-124D, FSW-124D-POE, FSW-224D-POE, FSW-224D-FPOE, FSW-248D, 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
FortiSwitch Rugged	FSW-R-112D-POE, FSW-R-124D

What's new in 3.5.1

FortiSwitch 3.5.1 includes the following features and enhancements:

- Multi-stage load balancing on D series support
- 802.1x capability (MAB, Fallback) enhancement
- 802.1P priority queuing trunk and WRED
- 802.1x enhancement GUI support

Special Notices

Supported Features

Features support by model.

FortiSwitch 100

Feature	FSW-108D-POE	FSW-R-112D-POE	FSW-124D	FSW-124D-POE	FSW-R-124D
48 port lag support					
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			✓	✓	✓

Feature	FSW-108D-POE	FSW-R-112D-POE	FSW-124D	FSW-124D-POE	FSW-R-124D
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 support			✓	✓	✓
802.1x MAC base security mode	✓	✓	✓	✓	✓
ACL		✓	✓	✓	✓
Auto module max speed detection & notification					
CPLD Software Upgrade Support for OS					
DHCP relay feature		✓	✓	✓	✓
DHCP Snooping		✓	✓	✓	✓
HTTPS REST APIs	✓	✓	✓	✓	✓
HW based ECMP					
IGMP Snooping		✓	✓	✓	✓
IP conflict detection & notification	✓	✓	✓	✓	✓
LAG min-max-bundle	✓	✓	✓	✓	✓
LLDP transmit	✓	✓	✓	✓	✓
LLDP-MED		✓	✓	✓	✓

Feature	FSW-224D-POE	FSW-224D-FPOE	FSW-248D	FSW-248D-POE	FSW-248D-FPOE
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 400

Feature	FSW-424D	FSW-424D-POE	FSW-424D-FPOE	FSW-448D	FSW-448D-POE	FSW-448D-FPOE
48 port lag support						
802.1x MAC base security mode	✓	✓	✓	✓	✓	✓
ACL	✓	✓	✓	✓	✓	✓

Feature	FSW-424D	FSW-424D-POE	FSW-424D-FPOE	FSW-448D	FSW-448D-POE	FSW-448D-FPOE
Auto module max speed detection & notification	✓	✓	✓	✓	✓	✓
CPLD Software Upgrade Support for OS						
DHCP relay feature	✓	✓	✓	✓	✓	✓
DHCP Snooping	✓	✓	✓	✓	✓	✓
HTTP REST API	✓	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓	✓

Feature	FSW-424D	FSW-424D-POE	FSW-424D-FPOE	FSW-448D	FSW-448D-POE	FSW-448D-FPOE
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 500

Feature	FSW-524D	FSW-524D-FPOE	FSW-548D	FSW-548D-FPOE
48 port lag support			✓	✓
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-524D	FSW-524D-FPOE	FSW-548D	FSW-548D-FPOE
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		✓

Feature	FSW-1024D	FSW-1048D
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	✓	✓
Storm Control	✓	✓
Virtual Wire	✓	✓
vlan tag by ACL	✓	✓

Feature	FSW-1024D	FSW-1048D
vlan tag by MAC/IP/802.1x	✓	✓

FortiSwitch 3000

Feature	FSW-3032D
48 port lag support	
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	

Feature	FSW-3032D
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.

Configuring IGMP-Snooping under "vlan enable" + "port based disable"

IGMP-Snooping configured under "vlan enable" + "port based disable," does not work well; only "vlan level enable" + "port level enable" can make snooping work. So, because the port is "disabled" by default, you must enable IGMP-Snooping on both the VLAN AND the port.

Upgrade Information

FortiSwitch 3.5.1 supports upgrading from FortiSwitch 3.2.0 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 3.5.1 support

The following table lists 3.5.1 product integration and support information.

Web browser	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 49 • Google Chrome version 54 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 3.5.1. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
382245	DHCP client does not receive an IP when `ip-mac` is globally enabled.
381809	Client drops DCHP offer packet when both DHCP relay and Snooping are enabled.
367235	Oversubscribe destination port causes STP packets to be dropped.
390586	802.1x should not over write static MAC entry.
388771	FortiLink is unable establish a connection with FortiSwitch after upgrading from 192 to 248.
393164	ISL packets are not going out at the configured interval after connection is established.
392001	Enable IGMP snooping on FortiLink internal ports.
368818	Change default certificates from SHA-1 to SHA-256.
389754	Switch send `coldStart` trap to SNMP server after rebooting from the GUI.

Common Vulnerabilities and Exposures

Bug ID	Description
389207	FortiSwitch 3.5.1 is no longer vulnerable to the following CVE References: • 2016-2177 • 2016-2179 • 2016-2181 • 2016-2182 • 2016-6302 • 2016-6303 • 2016-6304 • 2016-6305 • 2015-6306 • 2016-6307 • 2016-6308 Please visit https://fortiguard.com/psirt for more information.

Known Issues

The following known issues have been identified with 3.5.1. For inquires about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
377609	POE port may not reconnect when you remove and insert the link.
393845	When creating a static mac, it is not listed in the mac address table.
393856	`lldpmedd` does not time out fast enough on FSW-R-124D.
393622	`get switch dhcp-snooping status` does not correctly report snoop-enabled-vlans.
383506	EAP tunnel is terminated in the Authenticator (FSW) instead of at Auth-Server (FAC).
395320	IGMP-snooping configured with `vlan enable` and `port based disable` may not work as expected.

Copyright© 2016 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.