FortiSwitch Release Notes

Version 3.6.8

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 8, 2019

FortiSwitch 3.6.8 Release Notes

11-368-501311-20191108

TABLE OF CONTENTS

Change log

Date	Change Description
September 4, 2018	Initial release of FortiSwitchOS 3.6.8
September 10, 2018	Moved bug 497248 from Resolved Issues to Known Issues. Removed bug 501876.
September 18, 2018	Added bug 510943 to the “Known Issues” section.
October 18, 2018	Added 1048E to the “Supported models” and “Supported features for FortiSwitchOS 3.6” sections.
February 5, 2019	Added bug 535736 to the “Known Issues” section.
November 8, 2019	Added bug 593993 to the “Known Issues” section.

Introduction

This document provides the following information for FortiSwitch 3.6.8 build: 0424.

See the Fortinet Document Library for FortiSwitch documentation.

Supported models

FortiSwitch 3.6.8 supports the following models:

FortiSwitch	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-1048E, FSW-3032D
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What’s new in 3.6.8

FortiSwitch 3.6.8 is a patch release only. No new features or enhancements have been implemented in this release.

Special notices

Supported features for FortiSwitchOS 3.6

The following table lists the FortiSwitch features in Release 3.6 that are supported on each series of FortiSwitch models. All features are available in Release 3.6.0, unless otherwise stated.

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	8	24/48	24/48	24 (3.5.0) 64 (3.5.1)
Auto module max speed detection and notification	✓	—	—	✓	✓	—
IP conflict detection and notification	—	✓	✓	✓	✓	✓
IP-MAC binding	✓	—	—	✓	✓	✓
Static BFD	—	—	—	—	✓	✓
Hardware-based ECMP	—	—	—	✓	✓	✓
Private VLANs	✓	—	✓	✓	✓	✓
LLDP transmit	—	✓	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓	✓	✓
LAG min-max-bundle	—	✓	✓	✓	✓	✓
sFlow	✓	✓	✓	✓	✓	✓
Storm control	✓	✓	✓	✓	✓	✓
ACL	—	—	✓	✓	✓	✓
Static L3/hardware-based routing	✓	—	✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Software routing only	✓	✓	—	—	—	—
CPLD software upgrade support for OS	—	—	—	—	1024D 1048D	—
PoE-pre-standard detection (See Note 1.)	✓	✓	✓	✓	—	—
VLAN tag by ACL	—	—	✓	✓	✓	✓
ACL redirect to mirror destination as trunk/LAG	—	—	✓	✓	✓	✓
MAC/IP/protocol-based VLAN assignment	✓	✓	✓	✓	✓	✓
802.1x port mode	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓	✓	✓	✓
User-based (802.1x) VLAN assignment	✓	✓	✓	✓	✓	✓
Virtual wire	✓	—	✓	✓	✓	✓
HTTP REST APIs for configuration and monitoring	—	✓	✓	✓	✓	✓
Split port	—	—	—	✓	—	✓
IGMP snooping	—	—	✓	✓	✓	✓
Per-port max for learned MACs	—	—	✓	✓	—	—
802.1p support, including priority queuing trunk and WRED (release 3.5.1)	—	—	✓	✓	✓	✓
DHCP snooping	—	—	✓	✓	✓	✓
LLDP-MED	—	✓	✓	✓	✓	✓
DHCP relay feature	—	—	✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Support for switch SNMP OID	—	✓	✓	✓	✓	✓
Access VLANs (See Note 5.)	—	—	✓	✓	✓	✓
802.1x enhancements, including MAB (release 3.5.1)	✓	✓	✓	✓	✓	✓
Multi-stage load balancing (release 3.5.1)	—	—	—	—	✓	✓
MCLAG (multichassis link aggregation)(release 3.6.0)	—	—	✓ (not on 124D/124D-POE)	✓	✓	✓
Dynamic layer-3 protocols (OSPF, RIP, and VRRP) (release 3.6.0) (See Note 3.)	✓	—	✓ (not on 124D/124D-POE)	✓	✓	✓
Dynamic ARP inspection (release 3.6.0)	—	—	✓	✓	✓	✓
Firmware image rotation (dual-firmware image support) (release 3.6.0)	—	✓ (not on 108D-POE)	✓	✓	✓	✓
TDR (time-domain reflectometer)/cable diagnostics support (release 3.6.0)	✓	—	✓	✓	✓	✓
MAC learning limit (release 3.6.0) (See Note 4.)	—	—	✓	✓	—	—
Sticky MAC on switch interfaces (release 3.6.0)	—	—	✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
PoE modes support: first come, first served or priority based (PoE models) (release 3.6.0)	—	✓	✓	✓	—	—
ACL: egress mask action support (release 3.6.0)	—	—	✓	✓	✓	✓
Monitor system temperature (threshold configuration and SNMP trap support) (release 3.6.0)	—	✓	✓	✓	✓	✓
'forced-untagged' or 'force-tagged' setting on switch interfaces (release 3.6.0)	—	✓	✓	✓	✓	✓
Selective packet sampling to CPU (useful diagnostic tool) (release 3.6.0)	—	—	✓	✓	✓	3.6.1
Add CLI to show the details of port statistics (release 3.6.0)	—	✓	✓	✓	✓	✓
Display progress (%) during firmware upgrade (release 3.6.0)	✓	✓	✓	✓	✓	✓
STP root guard (release 3.6.2)	—	✓	✓	✓	✓	✓
STP BPDU guard (release 3.6.2)	—	✓	✓	✓	✓	✓
IGMP snooping: static multicast groups (release 3.6.2)	—	—	✓	✓	✓	✓
DHCP snooping: entry limit per port (release 3.6.2)	—	—	✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Network device detection (release 3.6.2)	—	—	✓	✓	✓	✓
QoS queue counters (releases 3.6.2 and 3.6.3)	—	—	✓	✓	✓	✓
Support of the RADIUS accounting server (release 3.6.3)	—	✓	✓	✓	✓	✓
Support of RADIUS CoA and disconnect messages (release 3.6.3)	—	✓	✓	✓	✓	✓
802.1x authentication: EAP-TLS support (release 3.6.3)	—	✓	✓	✓	✓	✓
DHCP snooping: CLI for DHCP-snooping server database (release 3.6.3)	—	—	✓	✓	✓	✓
Unicast hashing (release 3.6.4)	—	—	✓	✓	✓	✓
STP supported in MCLAGs (release 3.6.4)	—	—	✓ (not on 124D/124D-POE)	✓	✓	✓
QoS marking (release 3.6.4)	—	—	✓	✓	✓	✓
MAB reauthentication disabled (release 3.6.4)	—	✓	✓	✓	✓	✓
Cut-through switching (release 3.6.4)	—	—	—	—	✓	✓
Control of temperature and PoE alerts (release 3.6.4)	—	✓	✓	✓	✓	✓
IGMP querier (release 3.6.4)	—	—	✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Configuration of the QSFP low-power mode (release 3.6.4)	—	—	—	✓	1048D	✓
Learning limit violation log (release 3.6.4) (See Note 4.)	—	—	✓	✓	—	—
Sticky MAC addresses saved to static MAC table (release 3.6.4)	—	—	✓	✓	✓	✓
Enabling packet for-warding to CPU (release 3.6.4)	—	—	✓	—	—	—

Notes

1. PoE features are applicable only to the model numbers with a POE or FPOE suffix.
2. 24-port LAG is applicable to 524D, 524_FPOE, 1024D, and 3032D models. 48-port LAG is applicable to 548D, 548-FPOE, and 1048D models.
3. To use the dynamic layer-3 protocols, you must have an advanced features license.
4. The per-VLAN learning limit and per-trunk learning limit are not supported on dual-chip platforms (248 and 448 series).
5. Access VLANs are not supported on 108D-POE, 224D-POE, or 112D-POE.

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 3.6.8 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 3.6.8 support

The following table lists 3.6.8 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 3.6.8. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
436896	The LED status is not correct when the ports are not powered.
475561, 500513	A connectivity fault prevents the firmware for a managed FortiSwitch unit from being upgraded.
485909	During the firmware upgrade for multiple managed FortiSwitch units, some of the switches flapped, which caused the upgrade to fail.
489064	When connecting two 224D FortiSwitch units together, the SFP ports RX alarm reports a loss of signal, but traffic is not interrupted.
489769	In a two-tier MCLAG topology, some second tier FortiSwitch MCLAG peer groups have high levels of STP daemon processing.
493593	When the CLI console session times out, the FortiSwitch unit does not exit the session.
494830	FortiSwitchOS v3.6.8 is no longer vulnerable to the following CVE-Reference: CVE-2017-6214
495806	The automatic module configuration For the FS-1048D model needs to select the 10000cr speed for DAC cables.
500424	When adding hosts fails, the egress objects become stale.
501949	Disabling FortiSwitch Cloud causes the CLI to exit.
502058	The `execute router restart` command does not delete layer-3 egress objects that are pointed to by multiple routes.
502079	Running multiple SNMP queries at the same time causes a timeout.
502280	After the FSW-124E-POE is upgraded to 3.6.6, 3.6.7, or 6.0, there is a high-pitched noise when the switch starts.
502742	The output of the `get switch modules detail` command misidentifies 10G DAC cables.
503538	Running the `execute factoryresetfull` command did not remove licenses.

Bug ID	Description
504559	When a valid resistor is detected, a false error is logged.
505291	Segmentation faults occasionally cause the system to crash.
505336	When there is 100% line-rate traffic sent to a FortiSwitch unit, there are continuous PoE-related messages displayed on the console.
505888	After enabling image rotation (with the `set image-rotation enable` command) and running the `execute factoryreset` command, the FortiSwitch unit does not update the default configuration file.
505911	IGMP snooping does not work on the FortiSwitch 2xx and 4xx models.
506573	The 448DP and 448DF models are shown as having the same model ID and name.
506604	The FortiSwitch unit forwards VLAN packets instead of blocking them.
507967	After enabling strong-crypto on a FortiSwitch unit in standalone mode, the switch cannot be accessed by SSH.
509043	When the power consumption is more than 25.5 watts, the `get switch poe inline` command returns the wrong value for power consumption.
509141	Relative file paths should not refer to external files.
510885	Error messages refer to initXXXXXXXXXX instead of the appropriate daemon.

Known issues

The following known issues have been identified with 3.6.8. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
380239	IGMP-snooped multicast groups are not immediately flushed out of the snooping table when the querier port is shut down.
391607	Switch does not send gratuitous ARP for IP conflict when the system boots up and adds a new switch virtual interface (SVI).
414972	IGMP snooping might not work correctly when used with the 802.1x dynamic VLAN functionality in the 802.1x MAC-based authentication.
416655	When using DHCP, the IPv6 address cannot be configured. Also, the automatic configuration of the global address does not work.
424432	When MCLAG is enabled In FortiLink mode, IGMP reports are not synchronized if the `igmps-report-flood` and `igmps-traffic-flood` options are disabled the the FortiLink/ISL/MCLAG trunks.
438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
464703, 508490	The PoE_Max LED does not light up when the PoE exceeds its alarm threshold.
497248	After enabling mclag-stp-aware, there are “STP state DISCARDING” errors, and some switches go down.
509787	FortiSwitch Cloud is disabled when upgrading FortiSwitch firmware.
510943	When using the cable diagnostics feature on a port (with the `diagnose switch physical-ports cable-diag <physical port name>` CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.

Bug ID	Description
535736	If a FortiSwitch firmware image is an even multiple of 1024 bytes, it will not upgrade properly using the default FortiLink upgrade mechanism. The following builds are known to be affected: **version 3.x** build 0415/FSW_124D_POE **version 6.x** build 0039/FSW_1048E build 0043/FSW_124E build 0141/FSW_224D_FPOE build 0052/FSW_548D_FPOE **Workaround:** Change to HTTPS mode using the following commands: config switch-controller global set https-image-push enable end
593993	When the switch-controller.global.https-image-upgrade is enabled, the FS-108D-POE/FS-224D-POE might fail to upgrade. **Workaround:** Disable https-image-upgrade.