FortiSwitch Release Notes

Version 3.6.6

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 3.6.6 Release Notes

11-366-481579-20191108

TABLE OF CONTENTS

Change log

Date	Change Description
May 15, 2018	Initial release
May 21, 2018	Revised the description of bug 489769.
September 18, 2018	Added bug 510943 to the “Known Issues” section.
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 3.6.6 build: 0416.

See the Fortinet Document Library for FortiSwitch documentation.

Supported models

FortiSwitch 3.6.6 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-3032D
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What’s new in 3.6.6

FortiSwitch 3.6.6 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	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	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	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	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	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	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 3.6.6 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 3.6.6 support

The following table lists 3.6.6 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 3.6.6. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
423940	In some cases, the MAC address and VLAN ID are shown (diagnostic command) twice on the same interface after splitting ports.
448106	The `diagnose stp instance list` command needs to include mapped VLAN IDs, cost column, and flag column.
448125	An error occurs when the RADIUS primary server fails.
465271	Polling MAC addresses causes the Multiple Spanning Tree Protocol (MSTP) to become unstable.
467602	The assigned snmp-index value is missing for split ports.
467944	After an upgrade, the second-tier switches in an MCLAG are in a down state, and the first-tier core switches are in a discarding state.
469519	After creating a system interface in the GUI, the VLAN of the new system interface is not automatically added to the internal interface.
472686	After the STP root guard is removed, the port of the STP instance 1 stays in the “DESIGNATED DISCARDING” state.
473314	After updating the STP settings, the max-age and forward-time values were not updated on the root FortiSwitch unit.
474829	After the STP root path was changed on 1xxE switches, MAC addresses are not cleared.
474997	A FortiSwitch unit sends 802.1x authentication requests to all RADIUS servers with a different NAS ID than the one defined in *Switch* > *Interface* > *Security Groups*.
475062	Duplicate STP BPDUs cause the STP daemon to use too much of the CPU.
475090	The `unset qos-policy` command does not work on split ports.
475806	The default fan speed is too low on FS-124D-POE and FS-248D-POE.
475946	Entering the `exec shutdown` command causes a “No such file or directory” error.
476724	Unnecessary and obsolete CLI commands need to be removed.

Bug ID	Description
476742	The encryption scheme for some passwords was updated.
477300	If the temperature of the FortiSwitch unit fluctuates constantly, there are many alert messages logged for high temperatures.
477318	After the trunk configuration is changed and an `end` or `next` command is entered, the switch stops functioning.
478138	SNMP stops functioning.
479354	The MIB file does not define fsTrapHBFail and fsTrapHBReceived.
479529	After a broadcast storm, the GUI shows that all ports are powered but some ports are not on line.
479791	The RADIUS accounting START message is missing the Class attribute.
479799	The RADIUS accounting START message is missing the Fortinet-Group-Name attribute.
479851	When the `exec switch-controller stage-tiered-swtp-image all <image-name>` command is used in FortiLink mode, the FortiLink sessions bounce, and the image upgrade fails.
480240	Going to *System* > *Config* > *Revisions* and selecting the *Diff* button does not work.
480264	Synchronizing MAC addresses in a MCLAG can cause the general FortiSwitch control daemon to stop functioning.
481661	Ports 53 and 54 of the 1048E model are disabled.
482442, 482443	Use-after-free flaws were corrected.
482672	When the STP is disabled on a port, the STP state still changes in the event log when the port status changes.
483504	Some managed FortiSwitch units randomly leave and rejoin FortiLink mode.
483679	After disabling and then enabling routes, the switch stops learning MAC addresses.
483780	When DHCP snooping is enabled in an HA-mode topology with dual-homed FortiSwitch access, the DHCP discover broadcast packets loop.
484565	When a managed FortiSwitch is configured as a RADIUS accounting server through FortiOS, the default accounting port is not used.
485388	When using 802.1x and MAB authentication, the native VLAN changes from 1 to 98.

Bug ID	Description
487539	After sending a RADIUS coa-request-bounce-port message to the FortiSwitch unit, it becomes nonresponsive.
488000	When new switches are connected in a ring to switches in a two-tier MCLAG, the FortiLink connections flap.
489111	Enabling IGMP snooping causes the control packets to loop in a two-tier MCLAG topology in FortiLink mode.
489913	If you shut down the active link to the FortiGate unit on one of the FortiSwitch units in an MCLAG topology, the STP priority value changes.

Known issues

The following known issues have been identified with 3.6.6. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
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.
438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
380239	IGMP-snooped multicast groups are not immediately flushed out of the snooping table when the querier port is shut down.
460999	When you enable Energy Efficiency Ethernet (EEE) on an Apple Thunderbolt to Gigabit Ethernet Adapter, the FortiSwitch port might flap continuously. **Workaround:** If you are using MacBook with the Apple Thunderbolt to Gigabit Ethernet Adapter, disable EEE on the Apple Thunderbolt to Gigabit Ethernet Adapter when connecting to the FortiSwitch unit.

489769	In a two-tier MCALG topology, some second tier FortiSwitch MCLAG peer groups have high levels of STPD processing. When this happens, Fortinet recommends *both* of the the following actions:
	
	(a) Disabling STP on the first tier MCLAG trunks with the following commands:
	
	`config switch global`
	`  set mclag-stp-aware disable`
	`end`
	
	STP will still be operational on each peer.
	
	(b) Do NOT use access-ring connections on the first tier MCLAG peer group.

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.