FortiSwitch Release Notes

Version 3.6.11

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

February 4, 2020

FortiSwitch 3.6.11 Release Notes

11-3611-589876-20200204

TABLE OF CONTENTS

Change log

Date	Change Description
November 8, 2019	Initial document release for FortiSwitchOS 3.6.11
February 4, 2020	Updated the “Common vulnerabilities and exposures” section.

Introduction

This document provides the following information for FortiSwitch 3.6.11 build: 0432.

See the Fortinet Document Library for FortiSwitch documentation.

Supported models

FortiSwitch 3.6.11 supports the following models:

FortiSwitch	FS-108D-POE FS-124D FS-124D-POE FS-224D-POE FS-248D-FPOE FS-248D-POE

What's new in 3.6.11

FortiSwitch 3.6.11 is a patch release only. No new features or enhancements have been implemented in this release.

Special notices

Supported features for FortiSwitchOS 3.6.11

The following table lists the FortiSwitch features in Release 3.6.11 that are supported on each series of FortiSwitch models. All features are available in Release 3.6.11, unless otherwise stated.

Feature	GUI supported	108D-POE 224D-POE	124D 124D-POE 200 Series
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	8
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	✓	—	✓
Software routing only	✓	✓	—
CPLD software upgrade support for OS	—	—	—

Feature	GUI supported	108D-POE 224D-POE	124D 124D-POE 200 Series
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	—	—	✓
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)	—	—	—

Feature	GUI supported	108D-POE 224D-POE	124D 124D-POE 200 Series
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)	—	—	✓
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)	—	—	✓
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)	—	—	✓

Feature	GUI supported	108D-POE 224D-POE	124D 124D-POE 200 Series
DHCP snooping: entry limit per port (release 3.6.2)	—	—	✓
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)	—	—	✓
Configuration of the QSFP low-power mode (release 3.6.4)	—	—	—
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 forwarding 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.

Upgrade information

FortiSwitch 3.6.11 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 3.6.11 support

The following table lists 3.6.11 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)	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

Resolved issues

The following issues have been fixed in 3.6.11. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
570837	There's a memory leak when checking the speed of trunk members.
577403	Some applications stop responding randomly.
581484	Micro-segmentation does not work correctly when the “access VLAN” feature is enabled.
585824	There's a memory leak when LLDP applies port changes.
586363	When an access control list (ACL) is deleted, the port range used for the ACL needs to be freed.
586650	The CLI stops responding after deleting a virtual wire.
586762	After upgrading managed FortiSwitch units, the output of the `execute switch-controller get-sync-status all` command includes HTTPS commands.
588561	The REST API can lose nondefault values.
591141	A DHCP host cannot get the DHCP IP address.

Common vulnerabilities and exposures

FortiSwitchOS 3.6.11 is no longer vulnerable to the following CVEs:

- CVE-2019-11477
- CVE-2019-11478
- CVE-2019-11479
- CVE-2019-17657
- CVE-2007-6750

Visit https://fortiguard.com/psirt for more information.

Known issues

The following known issues have been identified with 3.6.11. 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. **Workaround:** Upgrade to FortiSwitchOS 6.2.0.
391607	Switch does not send gratuitous ARP for IP conflict when the system boots up and adds a new switch virtual interface (SVI). **Workaround:** Upgrade to FortiSwitchOS 6.2.0.
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. **Workaround:** Upgrade to FortiSwitchOS 6.2.0.
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. **Workaround:** Upgrade to FortiSwitchOS 6.2.0.
438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
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 **Workarounds:** Change to HTTPS mode using the following commands: config switch-controller global set https-image-push enable end Alternatively, you can upgrade to FortiOS 6.0.5 or 6.2.0.
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.