FortiSwitch Release Notes

Version 6.0.0

FortiSwitch Release Notes

September 22, 2019

11-600-469151-20190922

TABLE OF CONTENTS

Change log

Date	Change Description
May 29, 2018	Initial release for FortiSwitchOS 6.0.0
June 7, 2018	Added bug 493778 to the “Known issues” section.
June 14, 2018	Corrected the BGP, IS-IS, and PIM support in the feature matrix.
September 18, 2018	Added bug 510943 to the “Known issues” section.
July 22, 2019	Added bug 572052 to the “Known issues” section.
September 22, 2019	Updated the feature matrix (TDR and split port rows).

Introduction

This document provides the following information for FortiSwitch 6.0.0 build: 0027.

- Supported models on page 5
- Special notices on page 7
- Upgrade information on page 14
- Product integration and support on page 15
- Resolved issues on page 17
- Known issues on page 18

See the Fortinet Document Library for FortiSwitch documentation.

Supported models

FortiSwitch 6.0.0 supports the following models:

FortiSwitch	FSW-108E, FSW-108E-POE, FSW-108E-FPOE, FSW-124E, FSW-124E-POE, FSW-124E-FPOE, FSW-224D-FPOE, FSW-224E, FSW-224E-POE, FSW-248D, FSW-248E-POE, FSW-248E-FPOE, 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 6.0.0

Release 6.0.0 provides the following new features:

- New graphical user interface
- Expanded support for persistent (sticky) MAC addresses to FSW-108E, FSW-124E, FSW-108E-POE, FSW-108E-FPOE, FSW-124E-POE, FSW-124E-FPOE, and FSR-112D-POE
- Expanded support for DHCP snooping to FSW-108E, FSW-124E, FSW-108E-POE, FSW-108E-FPOE, FSW-124E-POE, FSW-124E-FPOE, and FSR-112D-POE
- Expanded support for MAC/IP/protocol-based VLAN assignment to FSW-108E, FSW-124E, FSW-108E-POE, FSW-108E-FPOE, FSW-124E-POE, and FSW-124E-FPOE
- RIP routing distances can be added, edited, and deleted in the GUI (*Router > Config > RIP > Distances*).
- FortiSwitch bandwidth and losses displayed on the dashboard (*System > Dashboard*)
- Certificate selection available in the new SSL Configuration page (*System > Config >SSL*)
- Priority-based flow control
- ARP timeout value can be set
- Monitor mode available to test 802.1x authentication

- DHCP blocking
- Border Gateway Protocol (BGP), Protocol Independent Multicast (PIM), and Intermediate System to Intermediate System Protocol (IS-IS) routing
- auth-fail-vlan is supported in 802.1x MAC-based authentication
- Support of the subject alternative name (SAN) when generating a certificate signing request (CSR)
- The minimum and maximum rate can be specified by percentage for each CoS queue.
- The `diagnose switch mac-address list` command now includes the total number of MAC address entries.
- New `diagnose switch trunk summary` command that displays a summary of the link aggregation information
- New `set mac-violation-timer <integer>` command for setting how many minutes entries in the learning-limit violation log are kept
- Fault relay support (FSR-112D-POE)
- GUI certificate selection for the 802.1x certificate, 802.1x certificate authority (CA), and GUI HTTPS certificate
- Access control list (ACL) policies for ingress, egress, and lookup stages
- New REST API endpoints

Special notices

Supported features for FortiSwitchOS 6.0

The following table lists the FortiSwitch features in Release 6.0 that are supported on each series of FortiSwitch models. All features are available in Release 6.0.0, unless otherwise stated.

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	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	112D-POE	1xxE	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.)	—	✓	FS-1xxE POE	✓	✓	—	—
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	Partial	—	—	—	✓	1048E	✓
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	—	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
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)	—	—	—	—	—	✓	✓
MCLAG (multichassis link aggregation)(release 3.6.0)	Partial	—	—	✓	✓	✓	✓
Dynamic layer-3 protocols (OSPF, RIP, and VRRP) (release 3.6.0) (See Note 3.)	✓	—	—	✓	✓	✓	✓
Dynamic ARP inspection (release 3.6.0)	✓	—	—	✓	✓	✓	✓
Firmware image rotation (dual-firmware image support) (release 3.6.0)	—	✓	—	✓	✓	✓	✓
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 (releases 3.6.0 and 6.0.0)	—	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	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)	—	✓	FS-1xxE POE	✓	✓	—	—
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 and 6.0.0)	—	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	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)	Partial	✓	—	✓	✓	✓	✓
Support of RADIUS CoA and disconnect messages (release 3.6.3)	—	✓	—	✓	✓	✓	✓
EAP Pass-Through (release 3.6.3)	✓	✓	—	✓	✓	✓	✓
DHCP snooping: CLI for DHCP-snooping server database (release 3.6.3 and 6.0.0)	—	✓	✓	✓	✓	✓	✓
Unicast hashing (release 3.6.4)	—	—	—	✓	✓	✓	✓
STP supported in MCLAGs (release 3.6.4)	—	—	—	✓	✓	✓	✓
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	112D-POE	1xxE	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 and 6.0.0)	—	✓	✓	✓	✓	✓	✓
Enabling packet forwarding to CPU (release 3.6.4)	—	—	—	✓	—	—	—
Bandwidth and losses on dashboard (release 6.0.0)	✓	✓	✓	✓	✓	✓	✓
Certificate selection in GUI (release 6.0.0)	✓	✓	✓	✓	✓	✓	✓
Priority-based flow control (release 6.0.0)	—	—	—	—	—	✓	✓
ARP timeout value (release 6.0.0)	—	✓	✓	✓	✓	✓	✓
Monitor mode (release 6.0.0)	—	✓	✓	✓	✓	✓	✓
DHCP blocking (release 6.0.0)	—	—	—	✓	—	—	—
BGP and IS-IS (release 6.0.0)	—	—	—	—	✓	✓	✓
PIM (release 6.0.0)	—	—	—	—	✓	✓	✓
auth-fail-vlan support in MAC-based authentication (release 6.0.0)	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
SAN in CSRs (release 6.0.0)	—	✓	✓	✓	✓	✓	✓
Percentage rate control (release 6.0.0)	✓	✓	—	✓	✓	✓	✓
Total MAC entries (release 6.0.0)	—	✓	✓	✓	✓	✓	✓
diagnose switch trunk summary (release 6.0.0)	—	✓	✓	✓	✓	✓	✓
set mac-violation-timer (release 6.0.0)	—	✓	—	✓	✓	✓	✓
Fault relay support (release 6.0.0)	—	✓	—	—	—	—	—
GUI certificate selection (release 6.0.0)	✓	✓	✓	✓	✓	✓	✓
Multistage ACL (release 6.0.0)	—	—	—	—	✓	✓	✓

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 6.0.0 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 6.0.0 support

The following table lists 6.0.0 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 6.0.0. 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.
481686	When you access the GUI of a FortiSwitch unit through FortiSwitch Cloud and then open the CLI console from the FortiSwitch GUI, you cannot use the embedded CLI console of the managed FortiSwitch unit.
483228	Some ingress ACL rule IDs fail on the 524D, 1024D, 448D-FPOE, and 1048E models. Failing IDs include 245, 501, 757, 1013, 1269, 1525, 1781, 2037, 2549, 3061, 3573, and 4085.
484725	Include the FortiSwitchOS version in the bootstrap message.

Known issues

The following known issues have been identified with 6.0.0. 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 802.1x Dynamic VLAN functionality.
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).
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.
480605	When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server.
481151	When IGMP snooping and PIM are enabled on the same VLAN, multicast traffic might still flood. **Workaround:** Remove the SVI and then add it from a protocol-independent multicast (PIM) network containing a VLAN with IGMP snooping enabled or disabled.
488044	On a Protocol Independent Multicast (PIM) topology using the assert mechanism, when the assert winner lost the route to the source, no multicast route was created, and the multicast traffic stopped.
488359	When the same host joins multicast groups from different sources, all multicast routes are deleted if some of the sources are set to Exclude (Record Type 2).

Bug ID	Description

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 following actions:
	(a) Disable 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.

491980	When configuring RIP routing in *Router > Config > RIP > Interfaces*, setting the Send Version and Receive Version to *Global* or *Both* does not work. Setting the send-version and receive-version to both in the CLI causes an Internal Server Error.
493089	In a network topology that contains layer-2 loops, the network monitor should be disabled.
493778	If an admin account has configurations for the pre-6.0 GUI dashboards, upon upgrading to FortiSwitchOS 6.0.0, that account's password will be reset to blank, and all administrator accounts after that one will be lost, regardless of their configuration. **Workarounds:** • Before upgrading to FortiSwitchOS 6.0.0 from 3.x.x, purge all dashboard and dashboard-tabs entries from all admins (using the `config dashboard` and `config dashboard-tabs` CLI commands). Do not log in to the GUI and upgrade the unit from the CLI. After the upgrade, the GUI can be used. • If you have FortiSwitchOS 6.0.0 running and you are restoring a config file generated on the 3.x.x release, first delete the entire "config dashboard" and "config dashboard-tabs" sections (from "config" through to "end") for all administrators. • If this issue has already occurred, reset the administrator accounts and passwords from the CLI.
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
572052	Backup files from FortiSwitchOS 3.x that have 16-character-long passwords fail when restored on FortiSwitchOS 6.x. In FortiSwitchOS 6.x, file backups fail with passwords longer than 15 characters. **Workaround:** Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.