FortiSwitch Release Notes

Version 6.0.2

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

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

FortiSwitch Release Notes

September 22, 2019

11-602-505798-20190922

TABLE OF CONTENTS

Change log

Date	Change Description
November 2, 2018	Initial release for FortiSwitchOS 6.0.2
December 3, 2018	Added bug 520954 to the “Known issues” section. Changed STP to MSTP in the “Supported features for FortiSwitchOS 6.0” section.
February 5, 2019	Added bug 535736 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 6.0.2 build: 0046.

- 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 16
- Known issues on page 18

See the Fortinet Document Library for FortiSwitch documentation.

Supported models

FortiSwitch 6.0.2 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 FortiSwitchOS 6.0.2

Release 6.0.2 provides the following new features:

- A new column on the Physical Ports Interfaces page (*Switch* > *Interface* > *Physical*) shows the traffic for each interface over the last day.
- A new column on the Physical System Interfaces page (*System* > *Network* > *Interface* > *Physical*) shows when secondary IP addresses, DHCP relay, and VRRP are enabled.
- Persistent (sticky) MAC addresses are now displayed on the *Switch* > *MAC Entries* page.
- The output of the `diagnose stp instance list` command now includes topology change notifications (TCNs) for the number of events triggered, the number of events received, and how much time has elapsed since the TCN occurred.
- You can now enable or disable “Frame VLAN Apply” and “Open Authentication” in the GUI (on the *Switch* > *Interface* > *Physical* page).
- The *Switch* > *Port* > *Physical* page and the *Switch* > *Port* > *POE* page have been combined.
- You can use the new *Switch* > *POE* page to configure PoE settings for the entire switch instead of configuring each port.

- FortiSwitchOS now supports dynamic VLAN assignment by group name.
- You can now use the CLI and GUI to select the two new port speeds (*10Gbps Copper Interface* and *10Gbps SFI Interface*) for SFP+ ports on supported FortiSwitch units.
- Three additional RADIUS attributes are now supported to track the source port in the 802.1x authentication request:
    - NAS-Port-ID—Name of the interface, such as “port3"
    - NAS-Port—Port number, such as “3”. A split port (for example, Port30.1) would have the NAS-Port attribute of “30”.
    - NAS-Port-Type—Only the “Ethernet” port type is supported.
- The flap-guard feature has been enhanced:
    - You can now configure the flap-guard triggered state so that the setting is retained when the switch is rebooted.
    - You can now set flap guard on each port instead of setting flap guard on the entire switch.
    - The range for the flap rate has expanded to 1-30.
    - For the CLI, the commands under `config switch flapguard settings` are now under `config switch physical-port`; the `diagnose flapguard instance status` command is now the `diagnose flapguard status` command.
    - More information is provided in the output of the `diagnose flapguard status` command.
- The Operation area on the Dashboard now displays a temperature chart for FortiSwitch models that have temperature sensors.
- Energy-efficient Ethernet is now available on FSR-112D-POE.

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
Management and Configuration							
CPLD software upgrade support for OS	—	—	—	—	—	1024D 1048D	—
Firmware image rotation (dual-firmware image support) (release 3.6.0)	—	✓	—	✓	✓	✓	✓
HTTP REST APIs for configuration and monitoring	—	✓	✓	✓	✓	✓	✓
Support for switch SNMP OID	✓	✓	✓	✓	✓	✓	✓
IP conflict detection and notification	✓	✓	✓	✓	✓	✓	✓
Security and Visibility							
802.1x port mode	✓	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓	✓	✓	✓	✓
User-based (802.1x) VLAN assignment	✓	✓	—	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
802.1x enhancements, including MAB (release 3.5.1)	✓	✓	✓	✓	✓	✓	✓
MAB reauthentication disabled (release 3.6.4)	—	✓	—	✓	✓	✓	✓
open-auth mode (release 6.0.0)	✓	✓	✓	✓	✓	✓	✓
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)	✓	✓	—	✓	✓	✓	✓
Network device detection (release 3.6.2)	—	—	—	✓	✓	✓	✓
IP-MAC-Binding	✓	—	—	—	✓	✓	✓
sFlow	✓	✓	—	✓	✓	✓	✓
ACL	—	—	—	✓	✓	✓	✓
Multistage ACL (release 6.0.0)	—	—	—	—	✓	✓	✓
DHCP snooping	✓	✓	✓	✓	✓	✓	✓
DHCP blocking (release 6.0.0)	—	—	—	✓	—	—	—
Dynamic ARP inspection (release 3.6.0)	✓	—	—	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
ARP timeout value (release 6.0.0)	—	✓	✓	✓	✓	✓	✓
Access VLANs (See Note 5.)	—	—	—	✓	✓	✓	✓
VLAN tag by ACL	—	—	—	✓	✓	✓	✓
Layer 2							
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)
LAG min-max-bundle	—	✓	✓	✓	✓	✓	✓
IGMP snooping	✓	—	—	✓	✓	✓	✓
IGMP querier (release 3.6.4)	—	—	—	✓	✓	✓	✓
LLDP transmit	—	✓	—	✓	✓	✓	✓
LLDP-MED	—	✓	✓	✓	✓	✓	✓
Per-port max for learned MACs	—	—	✓	✓	✓	—	—
MAC learning limit (release 3.6.0) (See Note 4.)	—	—	✓	✓	✓	—	—
Learning limit violation log (release 3.6.4) (See Note 4.)	—	—	—	✓	✓	—	—
set mac-violation-timer (release 6.0.0)	—	✓	—	✓	✓	✓	✓
Sticky MAC (releases 3.6.0 and 6.0.0)	✓	✓	✓	✓	✓	✓	✓
Total MAC entries (release 6.0.0)	—	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
MSTP	—	✓	✓	✓	✓	✓	✓
STP root guard (release 3.6.2)	—	✓	✓	✓	✓	✓	✓
STP BPDU guard (release 3.6.2)	—	✓	✓	✓	✓	✓	✓
'forced-untagged' or 'force-tagged' setting on switch interfaces (release 3.6.0)	—	✓	—	✓	✓	✓	✓
Private VLANs	✓	—	—	✓	✓	✓	✓
Multi-stage load balancing (release 3.5.1)	—	—	—	—	—	✓	✓
Priority-based flow control (release 6.0.0)	—	—	—	—	—	✓	✓
Storm control	✓	✓	✓	✓	✓	✓	✓
MAC/IP/protocol-based VLAN assignment	✓	✓	✓	✓	✓	✓	✓
Virtual wire	✓	—	—	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓	✓	✓	✓
Percentage rate control (release 6.0.0)	✓	—	—	✓	✓	✓	✓
Layer 3							
Static L3/hardware-based routing	✓	—	—	✓	✓	✓	✓
Software routing only	✓	✓	✓	—	—	—	—
OSPF (release 3.6.0) (See Note 3.)	✓	—	—	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
RIP (release 3.6.0) (See Note 3.)	✓	—	—	✓	✓	✓	✓
VRRP (release 3.6.0) (See Note 3.)	✓	—	—	✓	✓	✓	✓
BGP (release 6.0.0)	—	—	—	—	✓	✓	✓
IS-IS (release 6.0.0)	—	—	—	—	✓	✓	✓
PIM (release 6.0.0)	—	—	—	—	✓	✓	✓
Hardware-based ECMP	—	—	—	—	✓	✓	✓
Static BFD	—	—	—	—	—	✓	✓
DHCP relay feature	✓	—	✓	✓	✓	✓	✓
High Availability							
MCLAG (multichassis link aggregation) (release 3.6.0)	Partial	—	—	✓	✓	✓	✓
STP supported in MCLAGs (release 3.6.4)	—	—	—	✓	✓	✓	✓
Quality of Service							
802.1p support, including priority queuing trunk and WRED (release 3.5.1)	✓	—	—	✓	✓	✓	✓
QoS queue counters (releases 3.6.2 and 3.6.3)	—	—	—	✓	✓	✓	✓
QoS marking (release 3.6.4)	—	—	—	✓	✓	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Summary of configured queue mappings (release 6.0.1)	✓	—	✓	✓	✓	✓	✓
Miscellaneous							
PoE-pre-standard detection (See Note 1.)	—	✓	FS-1xxE POE	✓	✓	—	—
PoE modes support: first come, first served or priority based (PoE models) (release 3.6.0)	—	✓	FS-1xxE POE	✓	✓	—	—
Control of temperature alerts (release 3.6.4)	—	✓	—	✓	✓	✓	✓
Split port	Partial	—	—	—	✓	1048E	✓
TDR (time-domain reflectometer)/cable diagnostics support (release 3.6.0)	✓	—	—	✓	✓	—	—
Auto module max speed detection and notification	✓	—	—	—	✓	✓	—
Monitor system temperature (threshold configuration and SNMP trap support) (release 3.6.0)	—	✓	—	✓	✓	✓	✓
Cut-through switching (release 3.6.4)	—	—	—	—	—	✓	✓

Feature	GUI supported	112D-POE	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D
Add CLI to show the details of port statistics (release 3.6.0)	—	✓	✓	✓	✓	✓	✓
Configuration of the QSFP low-power mode (release 3.6.4)	—	—	—	—	✓	1048D	✓
Energy-efficient Ethernet (release 6.0.1)	—	✓	✓	✓	✓	—	—

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 (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 6.0.2 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 6.0.2 support

The following table lists 6.0.2 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 6.0.2. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
481151	When IGMP snooping and PIM are enabled on the same VLAN, multicast traffic might still flood.
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).
489769	In a two-tier MCLAG topology, some second tier FortiSwitch MCLAG peer groups have high levels of STPD processing.
497248	After enabling `mclag-stp-aware`, there are "STP state DISCARDING" errors, and some switches go down.
502742	The output of the `get switch modules summary` command does not identify 10G SFP+ modules correctly.
506762	The FortiSwitch unit cannot be accessed through the GUI or SSH after an IP camera is connected to it.
507257, 511286, 514884, 515100, 515388, 518410	Managed switches randomly go down until the switch-controller CAPWAP control daemon is restarted on the switch.
507488	STP caused network disruption after distribution switches were added to a one-tier MCLAG topology.
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.
509113	A user cannot log in to the GUI with remote admin credentials using a TACACS server.
509115	When a RADIUS administrator account is set up to accept wildcards, the FortiSwitch unit forwards the wildcard name to the RADIUS server instead of the user name.
509427	Logging in to the GUI does not work with the user is configured on an LDAP server.
510229	A user cannot ping between D-series switches and E-series switches when they have different native VLAN configurations on the internal interface and uplink interface.

Bug ID	Description
510885	Error messages refer to initXXXXXXXXXXX instead of the appropriate daemon.
511172	The default interval for DNS resolution for the FortiSwitch Cloud needs to change from 15 to 45 seconds.
511654	“(Class A, B, C)” needs to be removed from the sFlow Collector page (*Switch > sFlow*).
511802	“Sequence Number” needs to be changed to “ID” for the *Router > Config > Static* page, Add Static Route page, and Edit Static Route page
511909	Some of the values in the output of the `diagnose switch physical-ports cable-diag` command are wrong.
511995	After a port is disabled and then enabled, the BPDU guard state machine is not updated.
513389	When the VM is moved to a new switch, the MAC address table entry for the VM is not updated automatically.
513937	When a laptop is connected to a switch, there is a delay in the ARP response for the gateway IP address.
514783	The `config switch-controller custom-command` command does not work in multi-tier managed FortiSwitch topologies.
517534	An “IP Conflict” message is displayed for a VRRP configuration.
518683	The `execute switch-controller custom-command` command does not work with an admin account configuration.

Common vulnerabilities and exposures

FortiSwitchOS 6.0.2 is no longer vulnerable to the following CVEs:

- CVE-2017-6214
- CVE-2018-15473
- CVE-2015-9251

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

Known issues

The following known issues have been identified with 6.0.2. 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).
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.
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.
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.
520954	When a “FortiLink mode over a layer-3 network” topology has been configured, the FortiGate GUI does not always display the complete network.
521441	The “internal” system interface does not perform hardware offloading of routes and is only software forwarding. Users can use VLAN switched virtual interfaces for full hardware offloading.

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
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.