FortiSwitch Release Notes

Version 6.2.0

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

11-620-536891-20190922

TABLE OF CONTENTS

Change log

Date	Change Description
April 15, 2019	Initial release for FortiSwitchOS 6.2.0
April 16, 2019	Added bug 539604 to the “Resolved issues” section.
May 1, 2019	Updated the feature matrix.
May 17, 2019	Added bug 539823 to the “Known issues” section.
June 26, 2019	Removed the 1xxE platform from the “Support of RADIUS CoA and disconnect messages” row in the feature matrix.
July 22, 2019	Added bug 572052 to the “Known issues” section.
September 9, 2019	Updated the feature matrix.
September 22, 2019	Updated the feature matrix.

Introduction

This document provides the following information for FortiSwitch 6.2.0 build: 0168.

See the Fortinet Document Library for FortiSwitch documentation.

Supported models

FortiSwitch 6.2.0 supports the following models:

FortiSwitch 1xx	FSW-108E, FSW-108E-POE, FSW-108E-FPOE, FSW-124E, FSW-124E-POE, FSW-124E-FPOE
FortiSwitch 2xx	FSW-224D-FPOE, FSW-224E, FSW-224E-POE, FSW-248D, FSW-248E-POE, FSW-248E-FPOE
FortiSwitch 4xx	FSW-424D, FSW-424D-FPOE, FSW-424D-POE, FSW-448D, FSW-448D-FPOE, FSW-448D-POE
FortiSwitch 5xx	FSW-524D-FPOE, FSW-524D, FSW-548D, FSW-548D-FPOE
FortiSwitch 1xxx	FSW-1024D, FSW-1048D, FSW-1048E
FortiSwitch 3xxx	FSW-3032D, FSW-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What’s new in FortiSwitchOS 6.2.0

Release 6.2.0 provides the following new features:

- VLAN stacking (QinQ)
- Remote SPAN (RSPAN) and encapsulated RSPAN (ERSPAN)
- When STP is disabled, you can enable the forwarding of STP packets using the CLI and GUI.
- IPv6 support has been expanded. You can use IPv6 addresses with DHCP, automatic address configuration, static routes, router advertisement, neighbor cache table, Telnet client, and SSH.
- Power priority (high, critical, or low) for power over Ethernet (PoE) ports

- Multiple ingress groups for access control lists (ACLs), allowing multiple matches
- Enabling and disabling ACLs using a schedule
- Clearing unused classifiers on ASIC hardware for ACL policies
- Storm control can be configured per port using the CLI and GUI.
- IP source guard
- Allowed server list for DHCP snooping
- IGMP proxy using the CLI and GUI
- Wildcards can be configured in more than one system admin profile.
- Enabling and disabling static routes in the GUI and CLI
- Private data encryption using an AES 128-bit key
- LLDP-MED support for enhanced 911 emergency calls
- Power over Ethernet (PoE) negotiation in LLDP-MED
- NetFlow and IPFIX flow tracking and export
- MAC address learning can be configured per VLAN.
- When you have multiple FortiSwitch units and need to locate a specific switch, you can use a command to flash all port LEDs on and off for a specified number of minutes. After you locate the FortiSwitch unit, you can use disable to stop the LEDs from flashing.
- Three additional RADIUS AVP attributes are now supported:
  - acct-fast-framedip-detect
  - framed-mtu-size
  - service-type
- There are two new commands to display the option-82 settings:
  - `diagnose option82-mapping relay <valid_system_interface>`
  - `diagnose option82-mapping snooping <VLAN_ID> <valid_switch_interface>`
- A new command allows you to add the switch's host name in the circuit ID field when DHCP option 82 is enabled.
- The 1xxE models now support IGMP snooping, MAC address learning limit violation log, and dynamic ARP inspection.
- The FSR-112D-POE model now supports access VLANs.
- The 1048E model now supports split ports.
- The following GUI changes were made:
  - You can now configure untagged VLANs and BPDU guard in the GUI.
  - LLDP-MED network policies displayed in the GUI
  - The Add IP Precedence/DSCP Map page and the Edit IP Precedence/DSCP Map page now display the configured mappings.
  - The *Switch* > *Monitor* > *Trunks* page allows you to view a summary of all trunks, including MCLAG trunks.
  - You can now delete unsaved sticky MAC addresses for a specific interface or on all interfaces in the GUI.
  - There is a new Subject Alternative Name field in the Add Local Certificate page.
  - In the Add Instance page, the maximum value for the ID field differes on various platforms.
  - The dashboard displays when the FortiSwitch is managed by FortiSwitch Cloud.
  - When loop guard is triggered, "Triggered" is displayed in the Status column on the *Switch* > *Monitor* > *Loop Guard* page.
  - There is a new Enable checkbox on the *Switch* > *sFlow* page.
  - The Enable sFlow checkbox has been renamed to Enable (under Packet Sampler) on the Edit Physical Port

Interface page.
    - On the Port Security page, the EAP Pass-Through Mode is enabled by default.
- The following REST API changes were made:
    - E911 location information has been added to the response of the monitor/switch/lldp-state endpoint.
    - The MAC address has been added to the response of the monitor/switch/port endpoint.
    - The server IP address has been added to the response of the monitor/switch/dhcp-snooping-client-db endpoint.
    - There are three new API endpoints:
        - execute/backend/standalone-config
        - monitor/switch/log
        - monitor/system/upgrade-status
- The following changes were made to existing CLI commands:
    - For the `diagnose stp instance list <STP_ID> <port_number>` command, the maximum value for <STP_ID> differs on various platforms.
    - For the `set cpu-cos-queue <integer>` command, the value range differs on various platforms.
    - The default DHCP distance (under `config system interface`) is now 5. It was previously 0.
    - Three commands under `config switch interface` have been renamed. The `set sflow-sampler` command is now `set packet-sampler`. The `set sample-rate` command is now `set packet-sample-rate`. The `set polling-interval` command is now `set sflow-counter-interval`.
    - The `set eap-passthru` command is now enabled by default.
    - The output of the `diagnose switch pdu-counters list` command now includes results for each interface.

Special notices

Supported features for FortiSwitchOS 6.2.0

The following table lists the FortiSwitch features in Release 6.2.0 that are supported on each series of FortiSwitch models. All features are available in Release 6.2.0, unless otherwise stated.

Feature	GUI supported	112D-POE	FSR-124D	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Management and Configuration								
CPLD software upgrade support for OS	—	—	—	—	—	—	1024D 1048D	—
Firmware image rotation (dual-firmware image support)	—	✓	✓	148E 148E-POE	✓	✓	✓	✓
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	✓	✓	✓	✓	✓	✓	✓	✓
802.1x enhancements, including MAB	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
MAB reauthentication disabled	—	✓	✓	✓	✓	✓	✓	✓
open-auth mode	✓	✓	✓	✓	✓	✓	✓	✓
Support of the RADIUS accounting server	Partial	✓	✓	✓	✓	✓	✓	✓
Support of RADIUS CoA and disconnect messages	—	✓	✓	—	✓	✓	✓	✓
EAP Pass-Through	✓	✓	✓	✓	✓	✓	✓	✓
Network device detection	—	—	✓	—	✓	✓	✓	✓
IP-MAC-Binding	✓	—	—	—	—	✓	✓	✓
sFlow	✓	✓	✓	—	✓	✓	✓	✓
Flow export	—	—	✓	—	✓	✓	✓	✓
ACL	—	—	✓	—	✓	✓	✓	✓
Multistage ACL	—	—	—	—	—	✓	✓	✓
Multiple ingress ACLs	—	—	✓	—	✓	✓	✓	✓
Schedule for ACLs	—	—	✓	—	✓	✓	✓	✓
DHCP snooping	✓	✓	✓	✓	✓	✓	✓	✓
Allowed DHCP server list	—	✓	✓	✓	✓	✓	✓	✓
DHCP blocking	—	—	✓	—	✓	✓	✓	✓
IP source guard	—	—	✓	—	✓	—	—	—
Dynamic ARP inspection	✓	—	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
ARP timeout value	—	✓	✓	✓	✓	✓	✓	✓
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	8	24/48	24/48	24 64
LAG min-max-bundle	—	✓	✓	✓	✓	✓	✓	✓
IGMP snooping	✓	—	✓	✓	✓	✓	✓	✓
IGMP proxy	✓	—	✓	✓	✓	✓	✓	✓
IGMP querier	—	—	✓	✓	✓	✓	✓	✓
LLDP transmit	—	✓	✓	✓	✓	✓	✓	✓
LLDP-MED	—	✓	✓	✓	✓	✓	✓	✓
LLDP-MED: ELIN support	—	✓	✓	✓	✓	✓	✓	✓
LLPD-MED: PoE negotiation	—	✓	✓	✓	✓	✓	—	—
Per-port max for learned MACs	—	—	✓	✓	✓	✓	—	—
MAC learning limit (See Note 4.)	—	—	✓	✓	✓	✓	—	—
Learning limit violation log (See Note 4.)	—	—	✓	✓	✓	✓	—	—
set mac-violation-timer	—	✓	✓	—	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Sticky MAC	✓	✓	✓	✓	✓	✓	✓	✓
Total MAC entries	—	✓	✓	✓	✓	✓	✓	✓
MSTP instances	—	0-15	0-15	0-15	0-15	0-32	0-32	0-32
STP root guard	—	✓	✓	✓	✓	✓	✓	✓
STP BPDU guard	✓	✓	✓	✓	✓	✓	✓	✓
'forced-untagged' or 'force-tagged' setting on switch interfaces	—	✓	✓	✓	✓	✓	✓	✓
Private VLANs	✓	—	✓	—	✓	✓	✓	✓
Multi-stage load balancing	—	—	—	—	—	—	✓	✓
Priority-based flow control	—	—	—	—	—	✓	✓	✓
Storm control	✓	✓	✓	✓	✓	✓	✓	✓
Per-port storm control	✓	✓	✓	✓	✓	✓	✓	✓
MAC/IP/protocol-based VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓
Virtual wire	✓	—	✓	—	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓	✓	✓	✓	✓
Percentage rate control	✓	—	✓	—	✓	✓	✓	✓
VLAN stacking (QinQ)	—	—	✓	—	✓	✓	✓	✓
VLAN mapping	—	—	✓	—	✓	✓	✓	✓
SPAN	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
RSPAN and ERSPAN	—	—	✓	—	✓	✓	✓	✓
Layer 3								
Static L3/hardware-based routing	✓	—	✓	—	✓	✓	✓	✓
Software routing only	✓	✓	—	✓	—	—	—	—
OSPF (See Note 3.)	✓	—	—	—	✓	✓	✓	✓
RIP (See Note 3.)	✓	—	—	—	✓	✓	✓	✓
VRRP (See Note 3.)	✓	—	—	—	✓	✓	✓	✓
BGP (See Note 3.)	—	—	—	—	—	✓	✓	✓
IS-IS (See Note 3.)	—	—	—	—	—	✓	✓	✓
PIM (See Note 3.)	—	—	—	—	—	✓	✓	✓
Hardware-based ECMP	—	—	—	—	—	✓	✓	✓
Static BFD	—	—	—	—	—	—	✓	✓
DHCP relay feature	✓	—	✓	✓	✓	✓	✓	✓
High Availability								
MCLAG (multichassis link aggregation)	Partial	—	—	—	✓	✓	✓	✓
STP supported in MCLAGs	—	—	—	—	✓	✓	✓	✓
IGMP snooping support in MCLAG	✓	—	—	—	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Quality of Service								
802.1p support, including priority queuing trunk and WRED	✓	—	✓	—	✓	✓	✓	✓
QoS queue counters	—	—	✓	—	✓	✓	✓	✓
QoS marking	—	—	✓	—	✓	✓	✓	✓
Summary of configured queue mappings	✓	—	✓	✓	✓	✓	✓	✓
Miscellaneous								
PoE-pre-standard detection (See Note 1.)	—	✓	✓	FS-1xxE POE	✓	✓	—	—
PoE modes support: first come, first served or priority based (PoE models)	—	✓	✓	FS-1xxE POE	✓	✓	—	—
Control of temperature alerts	—	✓	✓	—	✓	✓	✓	✓
Split port	Partial	—	—	—	—	✓	1048E	✓
TDR (time-domain reflectometer)/cable diagnostics support	✓	—	✓	—	✓	✓	—	—
Auto module max speed detection and notification	✓	—	—	—	—	✓	✓	—
Monitor system temperature (threshold configuration and SNMP trap support)	—	✓	✓	—	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Cut-through switching	—	—	—	—	—	—	✓	✓
Add CLI to show the details of port statistics	—	✓	✓	✓	✓	✓	✓	✓
Configuration of the QSFP low-power mode	—	—	—	—	—	✓	1048D	✓
Energy-efficient Ethernet	—	✓	✓	✓	✓	✓	—	—

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 the 448D series.
5. Access VLANs are not supported on 108D-POE or 224D-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 6.2.0 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 6.2.0 support

The following table lists 6.2.0 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)	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 6.2.0. For inquiries about a particular bug, please contact 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).
416655	When using DHCP, the IPv6 address cannot be configured. Also, the automatic configuration of the global address does not work.
424432	The IGMP reports received on the tier-1 FortiSwitch units in FortiLink mode (with MCLAG enabled) are not synchronized.
450820, 452205	DHCP snooping does not work with access VLANs.
475628	VLANs 0 and 4095 were incorrectly allowed to be used as part of the configuration and are no longer supported. Configurations such as `config switch vlan` and `config switch interface` (`set allowed-vlans`, `set native-vlan`, or `set private-vlan`) that tried to use 0 or 4095 are considered invalid and will be rejected, in full or part, possibly leaving a partial configuration. Fortinet recommends that, if you used 0 or 4095, you need to remove such references by manually backing up, editing for removal, and restoring the configuration after an upgrade.
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.
489064	The output of the `get switch modules summary` command shows LOS in the RX column for SFP ports.
489451	The fsModel SNMP trap should not appear in logs.
494714	After disconnecting one of the ports used to form an MCLAG between two FortiSwitch units, the ICL/ISL is not removed after 10 minutes.
505451	LACP trunks are periodically reset on the FortiSwitch unit.
516101	There is an increase in latency between clients and VM servers every half an hour.
520300	You cannot add port1 when you create a new mirror or edit an existing mirror.

Bug ID	Description
522490	After adding 12 FortiSwitch units to a two-tier MCLAG, the 448DN crashed when the `diagnose stp instance list` command was run.
522605	Tracebacks were seen when a 448DN was connected to 48 switches.
534922, 515211	Upgrading from FortiSwitchOS 6.0.3 can cause the switch to stop responding.
537187	The `set security-mode` command needs to be removed from under `config switch interface`.
539604	The network goes down when tier 2 of an MCLAG topology consists of all 1048E switches.
540302	When IGMP reports with the group destination IP address outside of the multicast range are received, the IGMP reports should be dropped, instead of being registered in the IGMP snooping table as group entries.

Common vulnerabilities and exposures

FortiSwitchOS 6.2.0 is no longer vulnerable to the following CVEs:

- CVE-2018-0739

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

Known issues

The following known issues have been identified with 6.2.0. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
382518, 417024, 417073, 417099, 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. **Workarounds:** —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the `execute interface dhcpclient-renew <interface>` command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values. **Workaround:** 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.
539823	The Cisco expansion module BEKEM cannot be powered up on a FortiSwitch unit. **Workaround:** When you use a Cisco phone, follow these guidelines: —When you configure the LLDP profile with the `config switch lldp profile` command, you need to include the `set 802.3-tlvs power-negotiation` option. —When you configure the LLDP profile with the `config switch lldp profile` command, do not configure the `set med-tlvs power-management` option.
542031	For the 5xx switches, the `diagnose switch physical-ports led-flash` command flashes only the SFP port LEDs, instead of all the port LEDs.

Bug ID	Description
548783	Some models support setting the mirror destination to “internal.” This is intended only for debugging purposes and might prevent critical protocols from operating on ports being used as mirror sources.
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.