FortiSwitch Release Notes

Version 6.2.3

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

April 27, 2020

11-623-589880-20200427

TABLE OF CONTENTS

Change log

Date	Change Description
December 23, 2019	Initial release for FortiSwitchOS 6.2.3
April 27, 2020	Added bug 629721.

Introduction

This document provides the following information for FortiSwitch 6.2.3 build: 0202.

See the Fortinet Document Library for FortiSwitch documentation.

Supported models

FortiSwitch 6.2.3 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424D, FS-424D-FPOE, FS-424D-POE, FS-424E, FS-424E-POE, FS-424E-FPOE,FS-424E-Fiber, FS-M426E-FPOE, FS-448D, FS-448D-FPOE, FS-448D-POE
FortiSwitch 5xx	FS-524D-FPOE, FS-524D, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1048D, FS-1048E
FortiSwitch 3xxx	FS-3032D, FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What’s new in FortiSwitchOS 6.2.3

Release 6.2.3 provides the following new features:

- The `get switch modules` commands now support split ports.
- The following two REST API endpoints now support binary files in addition to base64-encoded strings:
  - execute/restore/image
  - execute/stage/image

- IPv6 static routing (using the `config router static6` commands) is now supported by the following models: FSR-112D-POE, FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE.
- The *Switch* > *Virtual Wires* page now displays an *Edit* button for configured virtual wires.
- You now can specify a 10-Gbps copper interface (with the `set speed 10000cr` command) when splitting ports on the 5xxD, 3032D, and 1048E models.

Special notices

Supported features for FortiSwitchOS 6.2.3

The following table lists the FortiSwitch features in Release 6.2.3 that are supported on each series of FortiSwitch models. All features are available in Release 6.2.3, unless otherwise stated.

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	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	✓	✓	✓	✓	✓	✓	✓	✓	✓
FortiSwitch Cloud configuration	✓	✓	✓	✓	✓	✓	✓	✓	✓
Security and Visibility									
802.1x port mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
User-based (802.1x) VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
802.1x enhancements, including MAB	✓	✓	✓	✓	✓	✓	✓	✓	✓
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	—	—	✓	—	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
IP source guard	—	—	✓	—	✓	✓	—	—	—
Dynamic ARP inspection	✓	—	✓	✓	✓	✓	✓	✓	✓
ARP timeout value	—	✓	✓	✓	✓	✓	✓	✓	✓
Access VLANs	—	✓	✓	✓	✓	✓	✓	✓	✓
VLAN tag by ACL	—	—	✓	—	✓	✓	✓	✓	✓
RMON group 1	—	✓	✓	✓	✓	✓	✓	✓	✓
Reliable syslog (RFC 6587)	—	✓	✓	✓	✓	✓	✓	✓	✓
Packet capture	—	—	✓	—	✓	✓	✓	✓	✓
Layer 2									
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	8	8	8	8	24/48	24/48	24 64
LAG min-max-bundle	—	✓	✓	✓	✓	✓	✓	✓	✓
IPv6 RA guard	—	—	—	—	✓	✓	✓	✓	✓
IGMP snooping	✓	✓	✓	✓	✓	✓	✓	✓	✓
IGMP proxy	✓	✓	✓	✓	✓	✓	✓	✓	✓
IGMP querier	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP transmit	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP-MED	—	✓	✓	✓	✓	✓	✓	✓	✓
LLDP-MED: ELIN support	—	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
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	—	✓	✓	✓	✓	✓	✓	✓	✓
Sticky MAC	✓	✓	✓	✓	✓	✓	✓	✓	✓
Total MAC entries	—	✓	✓	✓	✓	✓	✓	✓	✓
MSTP instances	—	0-15	0-15	0-15	0-15	0-15	0-32	0-32	0-32
STP root guard	—	✓	✓	✓	✓	✓	✓	✓	✓
STP BPDU guard	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rapid PVST interoperation	—	✓	✓	✓	✓	✓	✓	✓	✓
'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	✓	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
MAC/IP/protocol-based VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓
Virtual wire	✓	—	✓	—	✓	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓	✓	✓	✓	✓	✓
Percentage rate control	✓	—	✓	—	✓	✓	✓	✓	✓
VLAN stacking (QinQ)	—	—	✓	—	✓	✓	✓	✓	✓
VLAN mapping	—	—	✓	—	✓	✓	✓	✓	✓
SPAN	✓	✓	✓	✓	✓	✓	✓	✓	✓
RSPAN and ERSPAN	—	RSPAN	✓	—	✓	✓	✓	✓	✓
Layer 3									
Static routing (v4|v6)	✓	—	✓	—	✓	✓	✓	✓	✓
Hardware routing offload (v4|v6)	✓	—	✓	—	✓	✓	✓	✓	✓
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	—	—	—	—	—	—	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Static BFD	—	—	✓	✓	✓	✓	✓	✓	✓
uRPF	—	—	—	—	—	—	✓	✓	✓
DHCP relay feature	✓	—	✓	✓	✓	✓	✓	✓	✓
DHCP server	—	—	—	—	✓	4xx only	✓	✓	✓
High Availability									
MCLAG (multichassis link aggregation)	Partial	—	—	—	✓	✓	✓	✓	✓
STP supported in MCLAGs	—	—	—	—	✓	✓	✓	✓	✓
IGMP snooping support in MCLAG	✓	—	—	—	✓	✓	✓	✓	✓
Quality of Service									
802.1p support, including priority queuing trunk and WRED	✓	—	✓	—	✓	✓	✓	✓	✓
QoS queue counters	—	—	✓	—	✓	✓	✓	✓	✓
QoS marking	—	—	✓	—	✓	✓	✓	✓	✓
Summary of configured queue mappings	✓	—	✓	✓	✓	✓	✓	✓	✓
Egress priority tagging	—	—	✓	—	✓	✓	✓	✓	✓
Miscellaneous									
PoE-pre-standard detection (See Note 1.)	—	✓	✓	FS-1xxE POE	✓	✓	✓	—	—

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
PoE modes support: first come, first served or priority based (PoE models)	—	✓	✓	FS-1xxE POE	✓	✓	✓	—	—
Control of temperature alerts	—	✓	✓	—	✓	✓	✓	✓	✓
Split port (See Note 6.)	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)	—	✓	✓	—	✓	✓	✓	✓	✓
Cut-through switching	—	—	—	—	—	—	—	✓	✓
Add CLI to show the details of port statistics	—	✓	✓	✓	✓	✓	✓	✓	✓
Configuration of the QSFP low-power mode	—	—	—	—	—	—	✓	1048D 1048E	✓
Energy-efficient Ethernet	—	✓	✓	✓	✓	✓	✓	—	—
PHY Forward Error Correction (see Note 5)	—	—	—	—	—	—	—	1048E	3032E

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 MAC learning limit and per-trunk MAC learning limit are not supported on the 448D/448D-POE/448D-FPOE/248E-POE/248E-FPOE/248D series.
5. Supported only in 100G mode (clause 91).
6. On the 3032E, you can split one port at the full base speed, split one port into four sub-ports of 25 Gbps each (100G QSFP only), or split one port into four sub-ports of 10 Gbps each (40G or 100G QSFP).

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 6.2.3 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 6.2.3 support

The following table lists 6.2.3 product integration and support information.

Web browser	• 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 6.2.3. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
571826	The IGMP-snooping daemon crashes when it receives a VLAN tag with the priority bits set.
580967	Protocol Independent Multicast (PIM) routing does not work on the FSW-3032E switch.
583436	There are SFP recover messages for 3032D ports.
587071	On the 1048D, 1024D, and 3032D models, using the GUI or REST API to make any change to the OSPF interface (such as changing the BFD mode) might cause the loss of the MD5 keys.
589099	The physical port's link stays down when a USB 2.0 to Fast Ethernet Adapter is connected to a FortiSwitch 108E port with the speed set to auto and the Energy-efficient Ethernet enabled.
589129, 591704	Using MAB authentication might cause high CPU usage.
589310	The web CLI crashes when the switch admin profile is authenticated with a RADIUS server.
591542	Spanning Tree Protocol (STP) is not stable when using Siemens Relay Siprotec 5.
592559	Ping fails after the speed configuration of an FS-1048E port is changed and the switch is rebooted.
594255	In some FortiLink loop topologies in FortiGate HA mode, periodic high CPU usage cause the HA status to flap.
596126	The FortiGate firewall user monitor shows the wrong IP address for RADIUS accounting updates from a FortiSwitch unit.
597129	There is an intermittent loss of SSH and HTTPS access to the standalone FortiSwitch unit; the voice quality is intermittently degraded.

Known issues

The following known issues have been identified with 6.2.3. 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.
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.
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.

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.
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.
629721	HTTP and HTTPS connections from the same client or from the same browser do not work. **Workaround:** Use HTTP and HTTPS connections from different clients (with a different IP address) or different browsers (for example, Firefox for HTTP and Chrome for HTTPS) or clear the cookies between using HTTP and HTTPS.