FortiSwitch Release Notes

Version 6.4.0

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

July 22, 2020

11-640-591529-20200722

TABLE OF CONTENTS

Change log

Date	Change Description
April 2, 2020	Initial release for FortiSwitchOS 6.4.0
April 3, 2020	Updated the following sections: • “What’s new in FortiSwitchOS 6.4.0” • “Supported features for FortiSwitchOS 6.4.0”
April 9, 2020	Added bug 625325.
April 20, 2020	Added CVE-2019-9506.
April 27, 2020	Added bug 629721.
June 23, 2020	Updated the “Supported features for FortiSwitchOS 6.4.0” section (“Monitor system temperature” row).
July 22, 2020	Updated the “Supported features for FortiSwitchOS 6.4.0” section.

Introduction

This document provides the following information for FortiSwitch 6.4.0 build: 0410.

See the Fortinet Document Library for FortiSwitch documentation.

Supported models

FortiSwitch 6.4.0 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, FS-448E, FS-448E-POE, FS-448E-FPOE
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 6.4.0

Release 6.4.0 provides the following new features.

GUI changes

- You can now enable or disable energy-efficient Ethernet (EEE) on the Edit Physical Port page. A new EEE column in The Physical Switch Ports page shows which ports have EEE enabled.
- You can now add the allowed DHCP server list on the Add VLAN page and Edit VLAN page.

- You can now create RSPAN and ERSPAN (auto and manual) port mirrors in the GUI.
- You can now delete multiple router access lists at the same time on the Access Lists page.
- When configuring OSPF routing, you can now redistribute BGP and ISIS routes.
- When configuring RIP routing, you can now redistribute BGP and ISIS routes.
- You can now see the IGMP-snooping learned multicast groups by going to *Switch* > *Monitor* > *IGMP Snooping*.
- You can now check if BPDU guard has been triggered and on which ports by going to *Switch* > *Monitor* > *BPDU Guard*.
- You can now configure IGMP static groups by going to *Switch* > *VLAN*.
- IGMP snooping is always enabled on switch interfaces and cannot be disabled.
- You can now specify the polling interval for sFlow.
- You can now create an ACL ingress policy, ACL egress policy, ACL prelookup policy, and a policer by going to the *Switch* > *ACL* menu.
- You can now configure IP source guard static entries by going to *Switch* > *IP Source Guard*.
- LLDP-MED support for enhanced 911 emergency calls
- The default number of minutes before contacting NTP server to synchronize the time (Sync Interval) has changed from 1 minute to 10 minutes, and the polling interval is now slower when the system time is synchronized.

CLI changes

- The time-domain reflectometer (TDR)/cable diagnostics feature is now supported on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
- Quality of service (QoS) is now supported on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
- Access control lists (ACLs) are now supported on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
- Static bidirectional forwarding detection (BFD) is now supported on the FSR-112D model.
- You can now use ingress pause metering to limit the input bandwidth of an ingress port.
- You can now use LLDP to advertise the energy-efficient Ethernet (EEE) configuration.
- Loop guard can now detect physical loops.
- You can now specify how an aggregator groups ports when the trunk is in LACP mode.
- You can now specify the number of microseconds that circuits are turned off to save power for EEE and the number of microseconds during which no data is transmitted while the circuits that were turned off are being restarted.
- You can now use the `diagnose switch acl schedule {egress | ingress | prelookup}` command to list ACL policies with a schedule.
- You can now use the `diagnose switch acl hw-entry-index <id>` command to find the hardware mapping for the specified ACL policy identifier or the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
- The default number of minutes before contacting NTP server to synchronize the time (syncinterval) has changed from 1 minute to 10 minutes, and the polling interval is now slower when the system time is synchronized.
- You can now use SHA1 authentication for the NTP server.
- You can now use the `set flap-timeout` command to set the number of minutes before the flag guard is reset.
- IPv6 support has been expanded. You can now connect to a RADIUS server with IPv6. You can use IPv6 addresses with the link monitor, OSPF routing, VRRP, DHCP snooping, and NTP servers.
- When you redistribute routes from OSPF, you can now configure a summary of external routes to reduce the amount of router resources needed.

- The new `diagnose ip router fwd` commands display information about layer-3 forwarding.
- The new `diagnose ip router ospf6` commands display information about IPv6 OSPF.
- The new `diagnose ip router static` commands display information about static routing.
- The new `diagnose debug ospf6` commands enable or disable the debugging level for OSPF routing for IPv6 traffic.
- The new `diagnose debug static` commands enable or disable the debugging level for static routes.
- The new `diagnose debug unit_test` command enables or disables the debugging of unit tests.
- The `execute router restart` command was removed.
- The `get router info fwd` command was removed.
- The following commands were renamed:

Previous command	New command
`diagnose ip router launch-info show`	`diagnose ip router process show`
`diagnose ip router {bfd | bgp | isis | ospf | pim | rip | zebra} debug`	`diagnose debug {bfd | bgp | isis | ospf | pim | rip | zebra}`
`get router info v6-routing-table`	`get router info6 routing-table`
(under `config router isis`) `config isis-interface`	(under `config router isis`) `config interface`
(under `config router isis`) `config isis-net`	(under `config router isis`) `config net`
(under `config router ospf`) `config ospf-interface`	(under `config router ospf`) `config interface`

- IGMP snooping is always enabled on switch interfaces and cannot be disabled.
- When an inter-switch link (ISL) is formed automatically, the `igmps-flood-reports` and `igmps-flood-traffic` options are now disabled by default.
- You can now specify how many seconds are allowed for the 802.1x reauthentication before it times out.
- The RADIUS Service-Type attribute now supports sending multiple values.
- The output of the `diagnose debug report` command now includes quality of service (QoS) queue statistics and access control list (ACL) usage.
- Physical port loopbacks are now supported.
- DHCP option-82 data can now be generated in ASCII format.
- When QinQ mode is enabled, you can now set the priority value if packets follow the priority of the service tag (S-tag).
- You can now use bidirectional forwarding detection (BFD) when configuring static routes for IPv6 traffic.
- You can now enable or disable the capability to automatically form an inter-switch link (ISL) between switches.
- FC-FEC (cl74) is enabled as the default setting for ports that have been split to 4x25G.
- Explicit congestion notification (ECN) is now supported.
- The Precision Time Protocol (PTP) transparent-clock mode is now supported.
- When splitting ports on the FS-3032E model, you can disable some 100G ports to allow up to sixty 25G, 10G, or 1G ports.

REST API changes

- The output for the `GET monitor/system/flash-list` endpoint now includes `next-boot` and `active` fields. When the `active` field is set to `yes`, that partition will be used after the switch is restarted.
- You can now use the `POST execute/download/sniffer-profile` endpoint to download a packet capture file in JSON or binary format.
- The `GET monitor/switch/modules-status` endpoint now supports multiple lanes and split ports.

Other changes

- The following tables in the specified SNMP management information base (MIB) files are now supported:
  - entityMIB (.1.3.6.1.2.1.47)
    - entPhysicalTable (.1.3.6.1.2.1.47.1.1.1)
  - entitySensorMIB (.1.3.6.1.2.1.99)
    - entPhySensorTable (.1.3.6.1.2.1.99.1.1)
  - powerEthernetMIB (.1.3.6.1.2.1.105)
    - pethPsePortTable (.1.3.6.1.2.1.105.1.1)
    - pethMainPseTable (.1.3.6.1.2.1.105.1.3.1)

Special notices

Supported features for FortiSwitchOS 6.4.0

The following table lists the FortiSwitch features in Release 6.4.0 that are supported on each series of FortiSwitch models. All features are available in Release 6.4.0, 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	✓	✓	✓	✓	✓	✓	✓	✓	✓
Auto topology	—	✓	✓	✓	✓	✓	✓	✓	✓
Security and Visibility									
802.1x port mode	✓	✓	✓	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓	✓	✓	✓	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
User-based (802.1x) VLAN assignment	✓	✓	✓	✓	✓	✓	✓	✓	✓
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	✓	✓	✓	✓	✓	✓	✓	✓	✓
DHCPv6 snooping	—	—	—	—	✓	✓	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Allowed DHCP server list	✓	✓	✓	✓	✓	✓	✓	✓	✓
IP source guard	✓	—	✓	—	✓	✓	—	—	—
Dynamic ARP inspection	✓	—	✓	✓	✓	✓	✓	✓	✓
ARP timeout value	—	✓	✓	✓	✓	✓	✓	✓	✓
Access VLANs	—	✓	✓	✓	✓	✓	✓	✓	✓
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
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	—	—	—	—	—	—	✓	✓	✓
Ingress pause metering	—	—	—	—	✓	✓	✓	✓	3032D
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 (v4|v6) (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
RIP (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
VRRP (v4|v6) (See Note 3.)	✓	—	—	—	✓	✓	✓	✓	✓
BGP (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
IS-IS (See Note 3.)	—	—	—	—	—	—	✓	✓	✓
PIM (See Note 3.)	—	—	—	—	—	—	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Hardware-based ECMP	—	—	—	—	—	—	✓	✓	✓
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	—	—	✓	—	✓	✓	✓	✓	✓
ECN	—	—	—	—	✓	—	✓	✓	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
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 (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)	—	✓	✓	FS-124E-POE FS-124E-FPOE FS-148E FS-148E-POE	✓	✓	✓	✓	✓
Cut-through switching	—	—	—	—	—	—	—	✓	✓
Add CLI to show the details of port statistics	—	✓	✓	✓	✓	✓	✓	✓	✓
Configuration of the QSFP low-power mode	—	—	—	—	—	—	✓	1048D 1048E	✓

Feature	GUI supported	112D-POE	FSR-124D	1xxE	4xxE	200 Series 400 Series	500 Series	1024D 1048D 1048E	3032D 3032E
Energy-efficient Ethernet	✓	✓	✓	✓	✓	✓	✓	—	—
PHY Forward Error Correction (see Note 5)	—	—	—	—	—	—	—	1048E	3032E
PTP transparent clock	—	—	—	—	✓	✓	✓	1048E	✓

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 FSR-112D-POE switches

The FSR-112D-POE switch does not support interconnectivity to other FSR-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitch 6.4.0 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 6.4.0 support

The following table lists 6.4.0 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 6.4.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
527565	You cannot quarantine a host when MAB is enabled on a FortiSwitch port.
529230	There is traffic loss when the MCLAG-ICL (tier 2) is down.
541370	The 802.1x MAC-based authentication for managed FortiSwitch units fails with the Cisco IP Phone model CP7821.
542650	When a phone is rebooted, traffic could not be passed until authentication was cleared.
543789	The LLDP-MED daemon shows high memory usage in the core switch.
554298	When ssh-key-sha1 is disabled in the FortiGate GUI, the user cannot connect to the FortiSwitch unit.
559783	IGMP stopped functioning after IGMP snooping was enabled on the FS-108E model.
562870	When network monitoring is enabled, 5xx switches stop forwarding traffic to the FortiGate.
564912	When DHCP snooping is enabled, the PXE client does not start.
567984	During bootup, the port LLDP profile changes from “default” to “default-auto-isl” before connecting to the FortiGate unit.
571242	FortiSwitch units go offline randomly or stop forwarding traffic at random times.
571826	The IGMP-snooping daemon stops functioning when IGMP v3 is used to add or leave a group.
576264	The `diagnose switch-controller dump trunk-state` command is not displaying output on the FortiGate unit.
576578	After upgrading to FortiSwitchOS 6.2.1, two out of four ports are not delivering power.
581484	When “access VLAN” is enabled, microsegmentation is not working correctly.
583436	Managed FS-3032D units are displaying SFP recover messages.
585372	Ports 39-48 are not being displayed on the FS-248E-FPOE GUI.

Bug ID	Description
589310	When the switch admin profile is authenticated with a RADIUS server, the CLI stops functioning.
597129	The iptables operation uses too much of the CPU, resulting in access loss and degradation of voice quality.
605451	In FortiOS, the max_poe_budget is always 0 when the managed FortiSwitch unit is online.
605698	MSTP is taking too long to transition from Alternative/Discarding to Designated/Forwarding.
605781	When a custom user profile is used to authenticate with TACACS, the user cannot use HTTP to access the switch's internal interface.
617415	There are frequent failures of 802.1x authentication.

Common vulnerabilities and exposures

FortiSwitchOS 6.4.0 is no longer vulnerable to the following CVEs:

- CVE-2019-11358
- CVE-2019-11477
- CVE-2019-11478
- CVE-2019-11479
- CVE-2019-17657
- CVE-2019-9506

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

Known issues

The following known issues have been identified with 6.4.0. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
382518, 417024, 417073, 417099, 438441	DHCP snooping and dynamic ARP inspection (DAI) do not work with private VLANs (PVLANs).
414972	IGMP snooping might not work correctly when used with 802.1x Dynamic VLAN functionality.
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.
563811	The DHCP server fails to send DHCPOFFER when the server uses the internal interface with snooping enabled and client accesses through relay.

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.
578050	Setting the `max-reauth-attempt` value in 802.1x MAC-based authentication does not work.
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.
606044	The value for cable length is wrong when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
609375	The FortiSwitchOS supports four priority levels (critical, high, medium, and low); however, The SNMP PowerEthernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
610149	The results are inaccurate for open and short cables when running cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
615591	For power supply unit (PSU) sensors on supported hardware, the value of EntitySensorStatus will be 1 (ok) if the sensor has detected that the PSU is inserted/connected. If the PSU is not inserted (or the sensor operational status is unavailable on that platform), the value is 2 (unavailable).
617755	The internal interface cannot obtain IPv6 addresses with dhcpv6-snooping enabled on the native VLAN.

Bug ID	Description
625325	Upgrading to FortiSwitchOS 6.4.0 causes fan failures for the following FortiSwitch models: • FS-224D-FPOE • FS-224E-POE • FS-224E-FPOE • FS-248D • FS-248D-POE • FS-248D-FPOE • FS-248E-POE • FS-248E-FPOE • FS-424D • FS-424D-POE • FS-424D-FPOE • FS-424E • FS-424E-POE • FS-424E-FPOE • FS-424E-FIBER • FS-448E • FS-448E-POE • FS-448E-FPOE • FS-M426E-FPOE • FS-448D • FS-448D-POE • FS-448D-FPOE For the FS-1048E model, upgrading to FortiSwitchOS 6.4.0 causes the fan to always run at full speed. **WORKAROUND:** Upgrade to FortiSwitchOS 6.4.1
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.