Release Notes

FortiSwitchOS 7.2.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 12, 2023
FortiSwitchOS 7.2.4 Release Notes
11-724-877650-20231212

TABLE OF CONTENTS

Change log

Date	Change Description
March 17, 2023	Initial release for FortiSwitchOS 7.2.4
April 12, 2023	Moved bug 891323 from “Resolved issues” to “Known issues.”
July 20, 2023	Added another new feature (additional weaker ciphers algorithms are now removed).
December 12, 2023	Removed bug 673433.

Introduction

This document provides the following information for FortiSwitchOS 7.2.4 build 0444.

- Supported models on page 5
- Special notices on page 8
- Upgrade information on page 10
- Product integration and support on page 11
- Resolved issues on page 12
- Known issues on page 13

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.2.4 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048E, FS-T1024E
FortiSwitch 3xxx	FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What’s new in FortiSwitchOS 7.2.4

Release 7.2.4 provides the following new features:

- You no longer need to configure TTL for all FortiSwitch platforms that support the layer-3 multichassis link aggregation group (MCLAG) feature.
- When a local certificate is generated through the Simple Certificate Enrollment Protocol (SCEP), the SCEP URL and password will be saved.
- OS image signature verification is now available in specific BIOS versions for the following platforms:

FortiSwitch model	Required BIOS version
FS-108E	04000010 or later
FS-108E-POE	04000017 or later
FS-108E-FPOE	04000017 or later
FS-124E	04000010 or later
FS-124E-POE	04000017 or later
FS-124E-FPOE	04000017 or later
FS-148E	04000010 or later
FS-148E-POE	04000015 or later
FS-224E	04000015 or later
FS-224E-POE	04000018 or later
FS-248E-POE	04000018 or later
FS-248E-FPOE	04000018 or later

- To increase the security of strong cryptography, additional weaker ciphers algorithms are now removed. When you enable strong cryptography (`set strong-crypto enable` under `config system global`), the following ciphers and algorithms are currently supported:
  - Ciphers (encryption algorithms):
    - chacha20-poly1305@openssh.com
    - aes128-ctr
    - aes192-ctr
    - aes256-ctr
    - aes128-gcm@openssh.com
    - aes256-gcm@openssh.com
  - Key-exchange algorithms:
    - curve25519-sha256@libssh.org
    - diffie-hellman-group-exchange-sha256
  - Host-key algorithm:
    - ssh-ed25519

- Message authentication code algorithms:
  - umac-128-etm@openssh.com
  - hmac-sha2-256-etm@openssh.com
  - hmac-sha2-512-etm@openssh.com

Refer to the FortiSwitch feature matrix for details about the features supported by each FortiSwitch model.

Special notices

Zero-touch management

When a new FortiSwitch unit is started, by default, it will connect to the available manager, which can be a FortiGate device, FortiLAN Cloud, or FortiSwitch Manager. All ports are enabled for auto discovery. The “internal” interface is the DHCP client in all FortiSwitch models. If you do not want your FortiSwitch unit to be managed, you must disable the features that you do not want active.

By default, auto-network is enabled in FortiSwitchOS 7.2.0 and later

After an `execute factoryreset` command is executed on a FortiSwitch unit in standalone mode, the auto-network configuration is enabled by default. If you are not using auto-network, you must manually disable it:

```
config switch auto-network
   set status disable
end
```

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.

⚠ If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following CLI command to convert the admin password from SHA256 to SHA1 encryption:

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

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

FortiSwitchOS 7.2.4 supports upgrading from FortiSwitchOS 3.5.0 and later.

For the FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, and FS-M426-FPOE models, there is a two-step upgrade process if you are upgrading from FortiSwitchOS 6.0.x or 6.2.x to 7.2.x:

1. Upgrade from FortiSwitchOS 6.0.x or 6.2.x to FortiSwitchOS 6.4.12 or later.
2. Upgrade from FortiSwitchOS 6.4.12 or later to 7.2.x.

If you do not follow the two-step upgrade process, the FortiSwitch unit will not start after the upgrade, and you will need to use the serial console to conclude the upgrade (BIOS and OS).

For FortiSwitch units managed by FortiGate units, refer to the *FortiLink Release Notes* for upgrade information.

Product integration and support

FortiSwitchOS 7.2.4 support

The following table lists FortiSwitchOS 7.2.4 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)	Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.2.4. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
829804	Changed which CLI commands are available, depending on whether the user has the enhanced debugging license.
833450	Do not use multicast IP addresses in the ranges of 224-239.0.0.x and 224-239.128.0.x on the FS-2xxD, FS-2xxE, FS-4xxD, and FS-4xxE models.
848619	When connecting FS-124F-POE to FS-148F-POE with the FTLF8519P3BNLFTN, the SFP module port does not come up on the FS-148F-POE when auto-module is configured.
856123	When the “network-monitor settings” are enabled, there are multiple “CPU_SENSOR (78.0%) cleared warning threshold of (85.0%)” messages in the log.
859563	When the admin password contains a space and is set in the GUI, the user cannot log in using the GUI.
867758	FortiSwitch units using IPv6 do not respond to SNMPv3 requests.
868358	It should optional to specify the Certificate Authority (CA) name when downloading the CA certificate using the Simple Certificate Enrollment Protocol (SCEP).
868886, 869843	The GUI for the FS-224E-POE, FS-248E-POE, FS-448E-POE, FS-248E-FPOE, and FS-426E-FPOE-MG models shows the ports in brown and the message, “This port is unavailable under the current configuration.”
869616	The FortiAnalyzer and FortiSwitch logs have multiple entries about the fan tray being detected or undetected on an FS-1048E switch, although the fan status is good.
872727	After upgrading to FortiSwitchOS 7.0.5, the status of PSU2 is wrongly reported as “Not inserted.”
874684	Some layer-2 managed FortiSwitch units are flagged as being layer-3 switches in the output for the `execute switch-controller get-conn-status` command.
877360	Using one of the `mac-move` commands on FX-1xxE and FS-1xxF models causes protocol packets to be dropped when allowing an 802.1X client to move between ports that are not directly connected to the FortiSwitch unit without having to delete the 802.1X session.
879156	Creating a new LLDP-MED profile in the GUI results in an Internal Server Error.

Known issues

The following known issues have been identified with FortiSwitchOS 7.2.4. 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.
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.
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.

Bug ID	Description
606044/610149	The results are inaccurate 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 Power Ethernet MIB only supports three levels. To support the MIB, a power priority of medium is returned as low for the PoE MIB.
659487	The FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE, FS-148E, and FS-148E-POE models support ACL packet counters but not byte counters. The `get switch acl counters` commands always show the number of bytes as 0.
667079	For the FSR-112D-POE model: • If you have enabled IGMP snooping or MLD snooping, the FortiSwitch unit does not support IPv6 features and cannot pass IPv6 protocol packets transparently. • If you want to use IGMP snooping or MLD snooping with IPv6 features, you need to enable `set flood-unknown-multicast` under the `config switch global` command.
748210	The MAC authentication bypass (MAB) sometimes does not work on the FS-424E when a third-party hub is disconnected and then reconnected.
784585	When a dynamic LACP trunk has formed between switches in an MRP ring, the MRP ring cannot be closed. Deleting the dynamic LACP trunk does not fix this issue. MRP supports only physical ports and static trunks; MRP does not support dynamic LACP trunks. **Workaround:** Disable MRP and then re-enable MRP.
793145	VXLAN does not work with the following: • log-mac-event • DHCP snooping • LLDP-assigned VLANs • NAC • Block intra-VLAN traffic
828603	The `oids.html` file is not accurate.
829807	eBGP does not advertise routes to its peer by default unless the `set ebgp-requires-policy disable` command is explicitly configured or inbound/outbound policies are configured.
867108	Depending on your browser type/version, web UI access might fail when using TLS 1.3 and client certificate authentication. **Workaround:** Use TLS 1.2.
891323	Going to the *Router* > *Config* > *OSPF* > *Areas* page results in an Internal Server Error.

FERTINET®

www.fortinet.com