FORTINET

Release Notes

FortiSwitchOS 7.2.6

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

February 9, 2024
FortiSwitchOS 7.2.6 Release Notes
11-726-959791-20240209

TABLE OF CONTENTS

Change log

Date	Change Description
December 18, 2023	Initial release for FortiSwitchOS 7.2.6
December 20, 2023	Added bug 934041.
December 28, 2023	Added bug 984228.
February 9, 2024	Added bug 987504.

Introduction

This document provides the following information for FortiSwitchOS 7.2.6 build 0471.

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.2.6 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 6xx	FS-624F, FS-624F-FPOE, FS-648F, FS-648F-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048E, FS-T1024E
FortiSwitch 2xxx	FS-2048F
FortiSwitch 3xxx	FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D, FSR-424F-POE

What's new in FortiSwitchOS 7.2.6

Release 7.2.6 provides the following new features:

- The FS-1048 model now supports autonegotiation for the 40G direct-attach cable (FN-CABLE-QSFP+).
- You can now generate an elliptic curve (ECDSA) certificate using a certificate signing request (CSR). You can choose an SECP256R1, SECP384R1, or SECP521R1 elliptic curve.
- The Message-Authenticator attribute is now used for authentication in MAC authentication bypass (MAB) Access-Request messages.
- You can now split ports 25 and 26 of the FS-T1024E and FS-1024E models into four subports of 10G (as well as 25G).
- The FS-624F, FS-624F-FPOE, FS-648F, and FS-648F-FPOE models now support FG-TRAN-LX, FG-TRAN-GC, FG-TRAN-SX, FS-TRAN-GC, FR-TRAN-ZX, FR-TRAN-SX, FN-TRAN-GC, FN-TRAN-SX, FN-TRAN-LX, and FN-TRAN-DSL.

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 7.2.6 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 7.2.6 support

The following table lists FortiSwitchOS 7.2.6 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 7.2.6. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
760843	802.1x MAC Authentication Bypass (MAB) switch sessions are not reauthenticated on port4 of a FS-108E.
845706	The output of the `diagnose switch-controller switch-info 802.1X` command differs.
889987	When the port descriptions are too long, a “500 Internal Server Error” is reported.
914774	Enabling energy-efficient Ethernet (EEE) on the FS-448E-POE disrupts traffic.
918017	Using RSPAN on managed FSR-112D switches under FortiOS 7.0.11 causes network interruptions.
919505	MAB authentication fails on FS-148F-FPOE running FortiSwitchOS 7.2.4 for laptops and phones.
919943	When the setting for strong cryptology is changed, the new setting does not take effect until the switch is restarted.
922098	When a device is connected to an FS-148F-FPOE managed by FortiCloud, the network becomes unstable.
922571	The user cannot import the PKCS12 certificate.
924247	Sticky MAC addresses and the MAC learning limit are not working on the FS-1xx models.
927820	The FortiOS event log does not include the source IP address when a security scanning tool is used.
930931	DHCPv6 packets were seen in the internal port of the FS-124F-FPOE models.
934041	The DHCP-snooping performance needs to be improved on the FS-1xxE and FS-1xxF models.
935537	After setting the FS-108F-PoE port to perpetual PoE, the setting did not take effect without restarting the switch.
935918	The VOIP phone and PC connectivity needs to be stable.
940956	Adding or removing an SNMP community on a tier-1 MCLAG switch causes the switch to become unresponsive for 10 seconds on all VLANs when a large number of network interfaces are configured.
941692	After DHCP snooping is enabled on FS-1xx models, devices cannot receive DHCP addresses.
942118	After configuring MACsec on the FS-524D model, the switch becomes unresponsive and stops forwarding traffic.
942140	The MAC address moves between FortiAP units when the FortiAP units are connected to two different FortiSwitch units.
945471	Configuring a low VRRP ID number on one of a pair of FS-T1024E switches causes the switch to lose connection with the backup switch.
950325	The FS-424E model runs out of memory and stops working until the switch is restarted.

Bug ID	Description
954437	When RADIUS accounting is turned on, the daemon for 802.1x port-based authentication occasionally crashes and causes the VLAN assignment to leak.
958507	When using FS-2xx or FS-4xx models, OSPF multicast hello packets from the FortiGate device do not reach third-party switches.
961041	802.1X authentication does not work when the Windows client is used with the FortiGate local database and FIPS.
961512	The *System* > *FortiLAN Cloud* page displays “Invalid License,” even though the FortiSwitch unit is using the Cloud Advanced Management License.
963009	When DHCP discovery and the `set dhcp-snoop-client-req drop-untrusted` command are used, the broadcast traffic received on a trusted ISL trunk port is wrongly broadcasted to an untrusted port.
963375	The FortiGate device cannot discover the FS-1xxE and FS-1xxF models.
965182	MAB events are rejected when using 802.1X authentication, FortiLink, LLDP voice VLAN, MAB, and a phone.
965640	There are random fan alarms for the FS-4xx models.
967568	There is a broadcast/multicast storm while an MCLAG peer is booting up.
967931	A managed FSW-448E-FPOE went offline because of a memory leak.
978579	After the client is disconnected from the port, there are continuous log messages for “authorization status=success.”

Known issues

The following known issues have been identified with FortiSwitchOS 7.2.6. 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.
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.
925173	You cannot import a PKCS12-formatted file if it does not have a password. **Workaround:** Extract the certificate and key from the `.p12` file and then use the GUI to import the certificate and key.
940586, 958210	For the FS-148F, FS-148F-POE, and FS-148F-FPOE models, there might be packet loss after the packet sampler or packet capture is enabled.

Bug ID	Description
974147	The `auto-module` speed does not work on the FSR-424F-POE model for FN-TRAN-SFP2-LX. **Workaround:** Set the speed to `1000auto` or `1000full` to bring up the link.
984228	After upgrading to FortiSwitchOS 7.4.2, 7.4.1, 7.2.6, 7.2.5, or 7.0.7 , the management interface cannot be reached by ping or HTTPS. **Workaround:** Use the `config system interface` command to find the MAC address of the management port and then add 2 to the first byte of the MAC address. For example, if the MAC address is `ac:71:2e:...`, then change the MAC address to `ae:71:2e:...`.
987504	High CPU usage occurs on the FS-1xx series when the IGMP querier is enabled and IGMP snooping is disabled. **Workaround:** Disable the IGMP querier when IGMP snooping is not being used.

www.fortinet.com