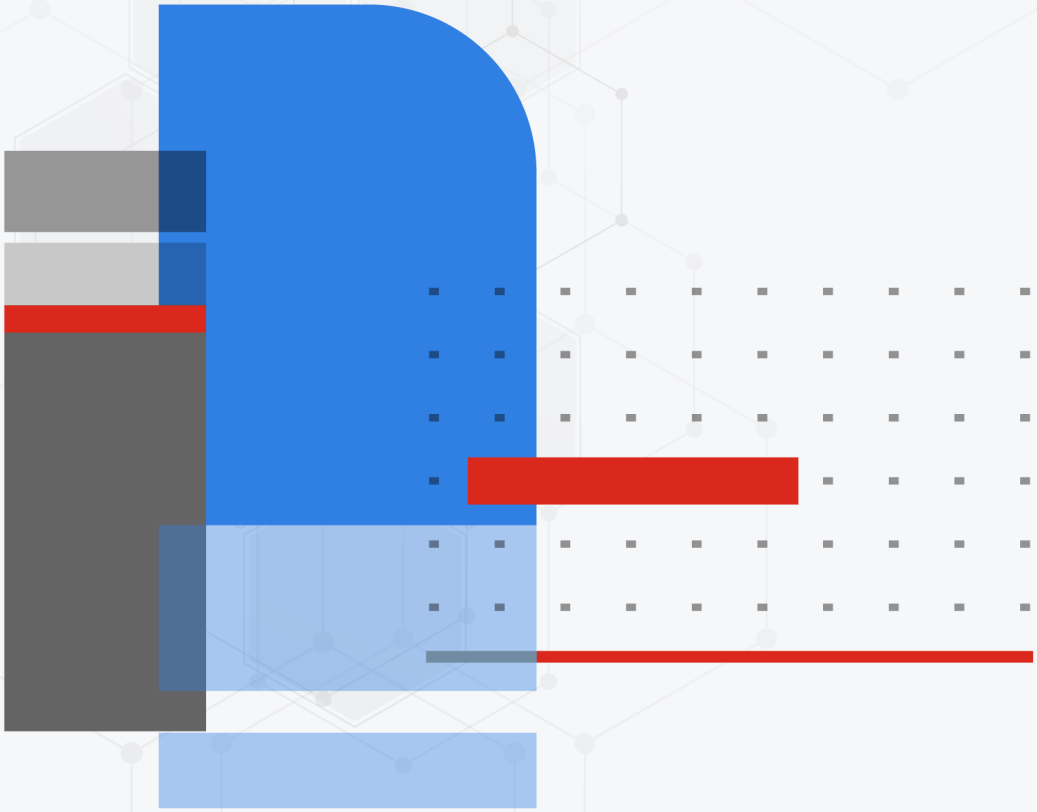
Release Notes

FortiSwitchOS 7.4.2



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 7, 2023
FortiSwitchOS 7.4.2 Release Notes
11-742-959771-20231207

TABLE OF CONTENTS

Change log

Date	Change Description
December 7, 2023	Initial release for FortiSwitchOS 7.4.2

Introduction

This document provides the following information for FortiSwitchOS 7.4.2 build 0801.

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.4.2 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 7.4.2

Release 7.4.2 provides the following new features:

- You can now bind 240 MAC addresses to VLANs for the FS-624F and FS-624F-FPOE models. You can now bind 480 MAC addresses to VLANs for the FS-648F and FS-648F-FPOE models.
- The FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FSR-424F-POE, FS-M426E-FPOE, FS-448E, FS-448E-FPOE, and FS-448E-POE models now support equal cost multi-path (ECMP) routing.
- The FS-2048F model now supports Virtual Extensible LAN (VXLAN) interfaces.
- 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 link monitor configuration in the GUI and CLI has changed:
  - You must now set the server IP address when you create a link monitor. This option supports remote peer monitoring.
  - Ping is now the default protocol when using IPv4 addresses, instead of Address Resolution Protocol (ARP).
  - The gateway IP address (IPv4 and IPv6) is no longer mandatory.
- You can now assign a priority to each VLAN. If there is more than one VLAN with the same name (specified in the `set description` command), FortiSwitchOS selects the VLAN with the lowest `assignment-priority` value (which is the highest priority) of the VLANs with names (specified in the `set description` command) that match the value of the RADIUS Tunnel-Private-Group-Id or Egress-VLAN-Name attribute. The `assignment-priority` value can be 1-255. By default, the `assignment-priority` is 128. The lowest `assignment-priority` value gets the highest priority.
- The time zone is now reported in the FortiSwitchOS local log and syslog entries.
- You can use the new *Router* > *Config* > *Key Chains* page to create, edit, or delete key chains in the GUI. Key chains are used for MD5 authentication for Routing Information Protocol (RIP) or Intermediate System to Intermediate System Protocol (IS-IS) routing.
- The FS-624F, FS-624F-FPOE, FS-648F, and FS-648F-FPOE models now support multichassis link aggregation groups (MCLAGs).

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 your FortiSwitchOS version requires converting the admin password format first

Before downgrading to a FortiSwitchOS version earlier than 7.0.0, you need to ensure that the administrator password is in SHA1 format. Use the `execute system admin account-convert-sha1` command to convert the administrator password to SHA1 encryption.

Before downgrading to FortiSwitchOS 7.0.0 or later, you need to ensure that the administrator password is in SHA1 or SHA256 format.

- Use the `execute system admin account-convert-sha1` command to convert the administrator password to SHA1 encryption.
- Use the `execute system admin account-convert-sha256` command to convert the password for a system administrator account to SHA256 encryption.

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

To convert the format of the admin password to SHA1 format:

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

   ```
   execute system admin account-convert-sha1 <admin_name>
   ```

2. Downgrade your firmware.

To convert the format of the admin password to SHA256 format:

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

   ```
   execute system admin account-convert-sha256 <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 7.4.2 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 7.4.2 support

The following table lists FortiSwitchOS 7.4.2 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 7.4.2. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
703374	The link does not come up when using SP-CABLE-FS-SFP+3 or SP-CABLE-FS-SFP+5.
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.
927820	The FortiOS event log does not include the source IP address when a security scanning tool is used.
927850	The following are the maximum numbers of saved configuration revisions: • 1xx-2xx: 20 revisions • 4xx-6xx: 40 revisions • 1xxx-3xxx: 80 revisions
934041	The DHCP-snooping performance needs to be improved on the FS-1xxE and FS-1xxF models.
935918	The VOIP phone and PC connectivity needs to be stable.
939257	If you set the `sample-direction` to `tx` or `both`, the output of the `get system flow-export-data flows all` command might be wrong.
950123	The HTTP and HTTPS daemon randomly returns “Forbidden” error pages on the FS-548D-FPOE model.
950325	The FS-424E model runs out of memory and stops working until the switch is restarted.
958254	After being upgraded to the FortiSwitchOS 7.4.1 GA build, the FortiSwitch unit still displays the “Caution: This firmware failed signature verification!” error.
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.
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.
965511	If the internal system interface has the default DHCP gateway enabled and the default route is added to the hardware, IP multicast packets are looped across MCLAG routers.

Bug ID	Description
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.

Known issues

The following known issues have been identified with FortiSwitchOS 7.4.2. 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 the VLAN and then use 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 FS-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.
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.

Bug ID	Description
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.
673433	Some 7-meter direct-attach cables (DACs) cause traffic loss for the FS- 448E model.
748210	The MAC authentication bypass (MAB) sometimes does not work on the FS-424E when a third-party hub is disconnected and then reconnected.
777647	• When MACsec is enabled on a tagged port, the `set exclude-protocol` command does not work on packets with VLAN tags (ARP, IPv4, or IPv6). • If you use the `set exclude-protocol` command with dot1q and packets with VLAN tags (ARP, IPv4, or IPv6), the packets are not MACsec encrypted and are transmitted as plain text. • Only 0x88a8 type packets apply to qinq.
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.

Bug ID	Description
882480	When the `set switch-controller-access-vlan` command is enabled on the FortiGate device, any host in the access VLAN cannot ping its default gate in the FortiGate device.
903001	Do not use `mgmt` as the name of a switch virtual interface (SVI). `mgmt` is reserved for the physical management switch port.
916405	FortiSwitchOS should not allow MACsec and 802.1X authentication to be configured on the same port.
940248	When both network device detection (`config switch network-monitor settings`) and the switch controller routing offload are enabled, the FS-1048E switch generates duplicate packets.
950895	In Release 7.4.1, VXLAN supports only one MSTP instance.
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.
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.

www.fortinet.com