Release Notes

FortiSwitchOS 7.4.7

July 23, 2025
FortiSwitchOS 7.4.7 Release Notes
11-747-1149691-20250723

TABLE OF CONTENTS

Change log

Date	Change Description
June 17, 2025	Initial release for FortiSwitchOS 7.4.7
July 15, 2025	Added bug 1181295.
July 23, 2025	Added bug 1184230.

What’s new in FortiSwitchOS 7.4.7

Release 7.4.7 provides the following new features:

- When the airflow differs on variants of the same switch model of supported platforms, the airflow direction is displayed on both the *Dashboard* and in the *About This Switch* dialog.
- You can now use the CLI to set the maximum amount of power on power over Ethernet (PoE) ports to 30 W, 60 W, or the maximum amount of power for that port.
- RADIUS change of authorization (CoA) is now supported in dynamic access control lists (DACLs).
- When you are using MAC Authentication Bypass (MAB) with 802.1X authentication, you can now limit the number of sessions allowed on a port. Limiting the number of devices or PCs per port helps increase the security of the network.

Introduction

This document provides the following information for FortiSwitchOS 7.4.7 build 0914:

- Supported models on page 6
- Special notices on page 7
- Upgrade information on page 11
- Product integration and support on page 12
- Resolved issues on page 13
- Known issues on page 15

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.4.7 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-110G-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-124G, FS-124G-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, FS-T1024F-FPOE
FortiSwitch 2xxx	FS-2048F
FortiSwitch 3xxx	FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D, FSR-216F-POE, FSR-424F-POE

Special notices

SSH host keys must be regnerated and user certificates must be imported again when downgrading from FortiSwitchOS 7.4.6 and later

When FortiSwitchOS 7.4.6 or later is downgraded, users need to regenerate the SSH host keys and import the user certificates again.

Upgrading MCLAG peer group switches from FortiSwitchOS 7.4.2 and earlier to FortiSwitchOS 7.4.3 and later

FortiSwitchOS 7.4.3 has changes in the MCLAG ICL communication that are incompatible with previous versions; therefore, the upgrade of the MCLAG peer group will have a longer impact than usual. Below are the recommended procedures.

From the FortiGate Switch Controller:

1. Disable network monitoring on the FortiGate device:
   ```
   config switch-controller network-monitor-settings
      set network-monitoring disable
   end
   ```
2. Stage the FortiSwitch firmware image on the FortiSwitch units using the "`execute switch-controller switch-software stage`" command on the FortiGate device.
3. Restart the MCLAG peer group switches at the same time.

From the FortiSwitch CLI:

The following recommended procedure will minimize downtime when upgrading MCLAG (the expected impact is within 20 seconds) from FortiSwitchOS 7.4.2 and earlier to FortiSwitchOS 7.4.3 and later.

1. If MCLAG split-brain protection is enabled, disable it in both switches in the MCLAG peer group.
2. In the FortiSwitchOS CLI, use the `diagnose switch mclag icl` command to find out which switch has the lower MAC address. .
   ```
   3032E-1 # diagnose switch mclag icl
   _FlInK1_ICL0_
          icl-ports             1-2
          egress-block-ports    3-5,31.1,32.1,17.3,17.4,31.2,32.2,32.3,32.4
          interface-mac         84:39:8f:13:96:4d   <-- local switch MAC address
          local-serial-number   FS3E32T422000275
          peer-mac              84:39:8f:13:99:59   <-- peer switch MAC address
   ```

```
peer-serial-number    FS3E32T422000281
Local uptime          0 days 23h:55m: 0s
Peer uptime           0 days 23h:55m: 0s
MCLAG-STP-mac         84:39:8f:13:96:4c
keepalive interval    1
keepalive timeout     60
dormant candidate     Peer
split-brain           Disabled
```

3. Stage the image in both switches using the `execute stage image` CLI command)
4. Restart the switch with the lower MAC address.

   In the preceding example, the local switch has the lower MAC address, so the local switch should be restarted first
5. Wait for the switch to restart and check that all links come up (the LACP trunks could be in a down state).
6. Restart the other switch.
7. After MCLAG comes up, enable split-brain protection if it was enabled before the upgrade.

Reduce configuration revisions before downgrading from 7.4.2 and later versions

For the FS-4xx, FS-5xx, FS-6xx, FS-1024E, FS-1048E, FS-3032E, FS-T1024E, and FS-2048F models only: If you are downgrading from FortiSwitchOS 7.4.2 and later, you cannot have more than 20 saved configuration revisions.

To check how many saved configuration revisions you have:

```
execute revision list config
```

To delete a specific configuration revision:

```
execute revision delete config <revision_ID>
```

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 7.4.7 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 7.4.7 support

The following table lists FortiSwitchOS 7.4.7 product integration and support information.

Web browser	• Microsoft Edge 112 • Mozilla Firefox version 113 • Google Chrome version 113 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 7.4.7. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1087244	After upgrading the switch to FortiSwitchOS 7.2.5, the FortiSwitch unit is unresponsive.
1091216	After a random power outage caused the FortiSwitch unit to restart, the switch configuration is lost.
1097393	The FSW-148F-FPOE model is not providing power to a third-party access point.
1098018	When performing 802.1x EAP authentication, authentication will fail if the RADIUS server sends jumbo frames.
1099627	There is a delay in MAC address learning on the ICL trunk interface for the FS-6xxF models.
1101944	The FortiSwitch unit is not providing power to a specific VoIP phone (Grandstream GXP2160 model).
1108484	The PoE splitter does not work with the FS-148F-FPOE model.
1112481	STP topology change notifications and LACP trunk flapping occur during an SNMP walk on the FS-624F-FPOE model.
1114261	The switch logs showed that the SFP module was removed from the switch ports 24, 25, 26, 27, and 28 and inserted back after 2 seconds.
1117174	The automation stitch should run without issues when %%date%% is used on the file name under the automation action configuration.
1119270	The IPv6 devices behind FortiLink cannot be reached.
1119673	In a FortiLink environment, the FortiSwitch VRRP configuration should not be deleted after a reboot.
1119678	The password for the RADIUS server is not being saved on FortiSwitch unit.
1120734	There is a delay in the display when the multicast stream is changed.
1122248	The `remark-dscp` action is not working in the egress ACL for the FS-6xxF models.
1124465	There is a high fan noise coming from the FS-124F-POE model.
1128640	The interswitch link (ISL) is not displayed in a FortiLink over a point-to-point layer-2 network.
1128657	Upgrading FortiSwitchOS from 7.0.6 to 7.4.6 or 7.6.1 causes the ICL trunk to change the native VLAN to 4094 and the allowed VLANs to 1-4094.
1129639	When performing a traceroute to the FortiGate device from the PC in an MCLAG topology, the IP addresses of the standalone switches are missing.
1129689	There is a “500 Internal Server Error” on the FS-6xxF models when the user tries to create an ingress/egress ACL policy using the FortiSwitchOS GUI.
1131249	After restarting FS-4xxE switches, the PoE status and the state of the AP trunk member port on MCLAG set to “disabled disabled.”

Bug ID	Description
1136109	In the FS-624F model, the QoS queue should drop packets that exceed the limit instead of bringing down CAPWAP tunnel.
1140195	After enabling DHCP snooping, there is high memory usage. This only affects the broadcast DHCP reply from the DHCP server; it does not affect unicast packets or the broadcast discover message from the DHCP client.
1140866	An error during a FortiSwitch restarting causes the configuration to be lost.
1142136	MAB authentication happens continuously on a port connected to an IP phone.
1144655	The *Switch* > *Interfaces* page does not load.
1159503	For FortiSwitchOS 7.4.x and higher on the FSW-224E-POE model, ERSPAN randomly stops because the MAC table is not being updated.

Known issues

The following known issues have been identified with FortiSwitchOS 7.4.7. 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.
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 - LLDP-assigned VLANs - NAC - Block intra-VLAN traffic
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.
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.

Bug ID	Description
978361	If restoring the FortiSwitch configuration from the GUI fails, the next firmware upgrade (using the CLI or GUI) or configuration restore will fail. **Workaround:** **1.** Go to *System* > *Config* > *Revisions* and click *Restore*. **2.** Choose the wrong configuration file and then click *Apply*. You will see a “Failed to restore configuration.” error message. **3.** Choose the right configuration file and then click *Apply*. You will see a “Failed to restore configuration.” message. **4.** Choose the right configuration file a second time and then click *Apply*. You will see a “Settings successfully restored. Please wait while the system restarts.” message.
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.
942068, 1006513	After using a dynamic port policy to remove or add a port, the profile was not updated after the user logged out of the EAP session.
1181295	After you add or delete ACL rules, traffic does not hit the ACL rules in the order in which they were added. For example, if ACLrule1, ACLrule2, and ACLrule3 are configured and then ACLrule1 is deleted and ACLrule4 is added, traffic hits ACLrule4 before ACLrule2 and ACLrule3. **Workaround:** If you want to change the order of the ACL rules, delete the current ACL and then configure a new ACL with the ACL rules in the correct order.
1184230	The FS-2048F model does not support the `1000auto` speed.

www.fortinet.com