FORTINET

Release Notes

FortiSwitchOS 8.0.0

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

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

May 18, 2026
FortiSwitchOS 8.0.0 Release Notes
11-800-1258131-20260518

TABLE OF CONTENTS

Change log

Date	Change Description
May 13, 2026	Initial release for FortiSwitchOS 8.0.0
May 18, 2026	Updated What's new in FortiSwitchOS 8.0.0 on page 5.

What's new in FortiSwitchOS 8.0.0

Release 8.0.0 provides the following new features:

- GUI elements (such as radio buttons, checkboxes, and fields) now are highlighted in light blue to show that they have been changed. Some changed GUI elements, such as radio buttons and checkboxes, also have a circular arrow, which can be clicked to revert the changes.
- Two types of OpenSSH security keys, sk-ecdsa-sha2-nistp256 and sk-ssh-ed25519, are now supported for multifactor authentication (MFA). These security keys support FIDO2 hardware tokens.
- The layer-2 interface for Routed VLAN interfaces (RVIs) is now shown on the *Switch > Interfaces* page with a checkmark in the *L2 Interface* column. When you edit an RVI in the GUI, only the options that can be changed are displayed. In addition, you can now enable or disable the ARP monitor for RVIs in the GUI.
- DNS support has been enhanced:
  - You can now use the domain name system (DNS) over Transport Layer Security (TLS). DNS over TLS (DoT) is a security protocol for encrypting and encapsulating DNS queries and responses over the TLS protocol. DoT increases user privacy and security by preventing eavesdropping and manipulation of DNS data using man-in-the-middle attacks. DNS over TLS uses port 853. All FortiSwitch models support DNS over TLS.
  - When a Certificate Authority (CA) certificate is specified for the DNS server, FortiSwitchOS now validates the certificate before establishing the connection between the FortiSwitch unit and the DNS server.
  - The `set dns-cache-limit` command (under `config system dns`) now specifies the maximum size of the DNS cache memory from 1 to 1,023 KB with a default of 512 KB. Previously, the command specified the maximum number of entries in the DNS cache.
- The length of the `set location` field (under the `config system snmp sysinfo` command) in the CLI has changed from 35 to 255 characters.
- Configuration files backed up from the FortiSwitch unit are now signed by the FortiSwitch unit. When you restore the configuration file, the FortiSwitch unit verifies that the configuration file was generated on the same FortiSwitch unit and that the configuration file has not been changed since it was generated. You can select in the CLI whether the FortiSwitch unit rejects an unverified file or accepts it and logs a warning.
- For the FS-424E-Fiber, FS-448E, FS-448E-POE, and FS-448E-FPOE models, you can now specify that FortiSwitchOS automatically selects the best source for the system clock. If multiple values are valid, the priority is Precision Time Protocol (PTP), then a Network Time Protocol (NTP) server, and finally a manual setting.
- To increase network security, the security level for OpenSSL is now set to 2 by default. Before FortiSwitchOS 8.0.0, the security level for OpenSSL was set to 0 by default.

  You can now configure the OpenSSL security level in the CLI for various FortiSwitch applications. By default, all applications are set to 2. You can change the OpenSSL security level from 0 to 5, with 0 being the least secure and 5 being the most secure.
- FortiSwitchOS now supports the Federal Risk and Authorization Management Program (FedRAMP) for the FSR-424FPOE, FS-4xxE, FS-6xxF, FS-1024E, FS-1048E, FS-T1024E, FS-T1024F-FPOE, FS-2048F, FS-3032E models.
- After the password of an admin is changed, all sessions being used by that admin are automatically closed. Previously, the admin could continue using active sessions after the admin's password was changed.
- You can now specify the public keys of up to three SSH clients in the GUI. These clients are authenticated without being asked for the administrator password.

- You can now use File Transfer Protocol (FTP) and SSH FTP (SFTP) to import local certificates and certificate authority (CA) certificates in the CLI.
- You can now use the CLI to turn off all LEDs on the front panel of certain FortiSwitch units. This feature is supported by the following models: FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-110G-FPOE, FS-124G, and FS-124G-FPOE.
- The `set speed auto-module` command has been changed to `set speed detect-by-module` (under `config switch physical-port`).
- The FSR-424F-POE model now supports split ports. Ports 29 and 30 can be split into 4x10G.
- The FS-3032G model now supports split ports. Ports 1 to 31 can be split into 4x25G when configured for 100G or split into 4x10G when configured for 40G.

  In addition, the FS-3032G model now supports Clause 108 RS-FEC.
- You can now edit multiple network interfaces and physical ports in the GUI at the same time. If the items have different values, the differences are highlighted in purple. You must select or enter the value to be used for the purple elements.
- You can now perform IEEE 802.1X authentication with the EAP pass-through mode disabled.
- The FSR-216F-POE, FSR-112F-POE, and FSR-108F models now support forced priority tagging.
- The FSR-108F, FSR-112F-POE, FSR-216F-POE, FS-624F, FS-624F-FPOE, FS-648F, and FS-648F-FPOE models now support the MAC move feature. When 802.1x authentication is being used, you can move an 802.1X client between ports that are not directly connected to the FortiSwitch unit.
- The FSR-108F, FSR-112F-POE, and FSR-216F-POE models now support Media Access Control security (MACsec), both in the static (PSK) mode and the dynamic-CAK mode, as well as the MACsec traffic statistics. These models support only the GCM-AES-128 cipher suite.
- The FS-1024E, FS-T1024E, FS-T1024F-FPOE, and FS-2048F models now support IP source guard.
- You can now use IPv6 routing with multichassis link aggregation groups (MCLAGs) with Virtual Router Redundancy Protocol (VRRP), open shortest path first (OSPF), and Border Gateway Protocol (BGP). This feature is available for the FSR-424F-POE, 200 Series, FS-4xxE, FS-1024E, FS-1048E, FS-1048G, FS-T1024E, FS-T1024F-FPOE, FS-2048F, FS-3032E, and FS-3032G models.
- FortiSwitchOS now supports the Data Center Bridging Exchange (DCBX) protocol, Enhanced Transmission Selection (ETS), and Priority-based Flow Control (PFC) for the FS-T1024E, FS-T1024F-FPOE, FS-2048F, FS-3032E, and FS-3032G models.

  Four new DCBX TLVs can be added to LLDP profiles for ETS configuration, ETS recommendation, PFC configuration, and Application Priority.

  ETS allows you to assign class of service (CoS) queues to priority groups for priority-based flow control. There are 16 priority groups. You can assign a guaranteed percentage of link bandwidth to each priority group. For example, the new `ets-qos-default` QoS policy creates priority groups for lossy traffic, lossless traffic, and high-priority traffic.

  DCBX application priority allows you to communicate the priority for various protocols. For example, the new `default-dcbx` LLDP profile creates six application priority entries for Fibre Channel over Ethernet (FCoE) traffic using EtherType 0x8906, FCoE traffic using EtherType 0x8914, RDMA over Converged Ethernet (RoCE) version 1 traffic, RoCE version 2 traffic, Internet Small Computer Systems Interface (iSCSI) traffic using TCP port 860, and iSCSI traffic using TCP port 3260.
- On the *Switch > Interfaces* page, the  icon now indicates that `auto-network` is enabled on the switch. When the icon is blue, it indicates an active inter-switch link (ISL) trunk. Previously, the icon indicated that FortiLink discovery was enabled.
- The FS-448E-FPOE and FS-448E-POE models now support two Media Redundancy Protocol (MRP) rings.

- Layer-3 Precision Time Protocol (PTP) is now supported for the FSR-424F-POE, FS-424E-Fiber, FS-448E, FS-448E-POE, FS-448E-FPOE models.
- Layer-2 network address translation (NAT) is now supported for the FSR-108F, FSR-112F-POE, and FSR-216F-POE models.
- You can now allow a Border Gateway Protocol (BGP) speaker to belong to multiple autonomous systems. This feature provides flexibility when networks are being reconfigured, as well as an additional layer of security when a company wants to protect their internal AS numbers. This feature is available for the FSR-424F-POE, FS-4xxE, FS-6xxF, FS-1024E, FS-1048E, FS-1048G, FS-T1024E, FS-T1024F-FPOE, FS-2048F, FS-3032E, and FS-3032G models.
- You can now specify the open shortest path first (OSPF) reference bandwidth for routed VLAN interfaces (RVIs). When the reference bandwidth divided by the interface bandwidth is less than 1, the OSPF cost is set to 1. Lower interface bandwidths with the same reference bandwidth result in higher OSPF costs. By default, the OSPF reference bandwidth is set to 100 megabits per second. The range of values is 1-4,294,967. The OSPF reference bandwidth supports both IPv4 and IPv6. This feature is available on the FSR-424F-POE, 200 Series, FS-4xxE, FS-6xxF, FS-1024E, FS-1048E, FS-1048G, FS-T1024E, FS-T1024F-FPOE, FS-2048F, FS-3032E, and FS-3032G models.
- You can now specify the network type of OSPF interfaces. By default, Ethernet links in OSPF form a broadcast network. Now, you can specify a point-to-point network or a point-to-multipoint network. For a point-to-point network or a point-to-multipoint network, no designated router or backup designated router election occurs, which simplifies OSPF and improves the OSPF performance. This feature is supported in IPv4 and IPv6. This feature is available on the FSR-424F-POE, 200 Series, FS-4xxE, FS-6xxF, FS-1024E, FS-1048E, FS-1048G, FS-T1024E, FS-T1024F-FPOE, FS-2048F, FS-3032E, and FS-3032G models.
- Syslog messages are now listed on the *Log > Entries* page for the following:
  - When you download a local certificate, remote certificate, certificate authority, or certificate revocation list from the GUI
  - When there are GUI runtime errors

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

Introduction

This document provides the following information for FortiSwitchOS 8.0.0 build 0047:

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 8.0.0 supports the following models:

FortiSwitch 1xx	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 6xx	FS-624F, FS-624F-FPOE, FS-648F, FS-648F-FPOE
FortiSwitch 1xxx	FS-1024E, FS-1048E, FS-T1024E, FS-T1024F-FPOE, FS-1048G
FortiSwitch 2xxx	FS-2048F
FortiSwitch 3xxx	FS-3032E, FS-3032G
FortiSwitch Rugged	FSR-108F, FSR-112F-POE, 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 7.6.2 and later

When FortiSwitchOS 7.6.2 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.x and earlier to FortiSwitchOS 7.6.0 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.x and earlier to FortiSwitchOS 7.6.0 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-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.

Upgrade information

FortiSwitchOS 8.0.0 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 7.6.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 7.6.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 8.0.0 support

The following table lists FortiSwitchOS 8.0.0 product integration and support information.

Web browser	• Microsoft Edge 135 • Mozilla Firefox version 138 • Google Chrome version 136 Other web browsers might 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.

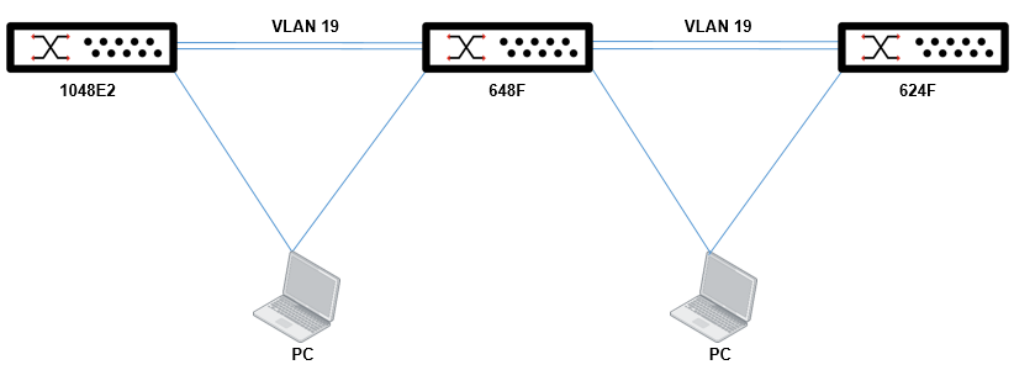
Resolved issues

The following issues have been fixed in FortiSwitchOS 8.0.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
903001	Do not use `mgmt` as the name of a switch virtual interface (SVI). `mgmt` is reserved for the physical management switch port.
1157423	FortiSwitchOS needs to support ifXTable (OID: 1.3.6.1.2.1.31.1.1).
1171253	When `set admin-restrict-local enable` is configured, remote authentication to the local admin does not work.
1176543	Enabling DHCP snooping on the FS-1024E model caused high CPU usage, leading to the client being disconnected.
1178539	The 25G port flaps when connected to ESXi.
1179853	Servers connected to the FSR-108F, FSR-112F, FSR-216F, or FS-6xxF models lost connectivity when using the 802.1X MAC-based MAB mode.
1180087	When IoT scanning is enabling, the switch must be periodically restarted.
1183066	A dual-homed MCLAG network setup using FS-3032E switches running FortiSwitchOS 7.4.6 has intermittent reachability issues.
1183689	After upgrading to FortiSwitchOS 7.4.7, there is a “config sync error” for the MCLAG peer group.
1189044	Access VLANs are not supported when MCLAG is deployed in a dual-site active-passive HA topology.
1189852	For the FS-148E-POE model, when 802.1X authentication, DHCP snooping, and dynamic ARP inspection (DAI) are enabled, DHCP and ARP snooping are not performed.
1192880	When managing an FS-1024E, FortiLink went down suddenly, and the user could not communicate with the switch, and the switch console did not respond.
1193263	DNS does not work with FortiSwitchOS 7.4.7.
1194010	Going to the *Switch > Storm Control* page results in an Internal Server Error.
1195396	Users need to be able to configure the netmask for VVRP.
1195601	MAC addresses in an MCLAG are not being synchronized, causing network interruptions.
1196931	The SFP+ ports of the FS-2048F and FS-3032G do not work with 1G copper SFP.
1201314	When `lan-segment` is enabled in a FortiLink topology, the vlan-range cannot be added in an STP instance.

Bug ID	Description
1204156	The `diagnose switch 802 status` command does not work on the FS-148E when using SSH.
1206457	After upgrading to FortiSwitchOS 7.4.8 on the FS-1xxF Series, the ports summary does not display.
1207784	The FS-6xxF models have high memory, which causes a network impact for clients connected on these FortiSwitch units.
1207815	The network is unstable with a FortiGate device connected to both tier 1 and tier 2.
1208778	Some switch platforms send out packets with the cfi bit set to 1, which might cause the packet to be dropped by the remote side.
1208893, 1219236	A static trunk, _FLinkDhcpDisc_, with port1 as a member, prevents the FS-1xxG model from being managed properly by the FortiGate device.
1210081	When LLDP are when changed using the GUI, the MED network policy is disabled.
1212514	The GUI is incorrectly showing an internal server error for operational switch.
1213843	There is an “Unable to retrieve ingress data, please try again later.” error when the user searches for an ingress ACL in the GUI.
1219236	DHCP snooping does not work when the FS-124G model is the uplink switch connected to the FortiGate HA pair.
1219674	The ABR router did not update the OSPF area 1 routes from the area 1 NSSA router.
1220649	When DHCP snooping is enabled, clients connected to the FortiSwitch unit might be disconnected.
1221171	After FortiSwitchOS is upgraded to 7.6.4, multicast traffic is dropped.
1221312	The FS-124G-FPOE idle noise level is high after it is turned on.
1222914	**For the FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124G, FS-124G-FPOE, and FS-110G models:** 224.0.0.x packets stop flooding when the first multicast port list group is created and this port list group is used to forward 224.0.0.x packets.
1225430	High CPU usage on the FS-148F-FPOE causes the FortiSwitch to disconnect from the FortiGate device.
1225551	The corresponding CA certificate needs to be present in the switch before the local certificate can be accepted.
1227872, 1229597	Sometimes STP instances other than 0 might not get updated MCLAG STP MAC addresses.
1229352	The FS-448E-FPOE model incorrectly logs “FortiLink: internal echo reply timed out.”
1230130	For FS-248E-POE, FS-248E-FPOE, and FS-224E_POE only. The switches crash after upgrading to FortiSwitchOS 7.6.4, 7.6.1, or 7.4.7.

Bug ID	Description
1231938	In FortiLink mode, when the quarantine hosts feature is enabled, all the quarantine hosts flood to all FortiSwitch units, causing 802-1x authentication to fail. This issue affects all switch models.
1232392	After configuring RSPAN, the FortiSwitch unit in FortiLink mode crashes. This issues affects the FSR-108F, FSR-112F-POE, and FSR-216F-POE models.

1232415	When IGMP snooping is enabled in a VLAN, ingress 224.0.0.0/24 control-plane traffic from an external port does not flood to other active ports in the same VLAN. This issues affects FS-6xxF models.
	Workaround: Configure a static mrouter port for switch ports connected to external routers. In the following example, IGMP snooping is enabled in VLAN 19, and FS-648F is the IGMP-snooping querier:
	 
	`config switch interface`
	`  edit "pc_1048E2_648F"`
	`  set allowed-vlans 10,12,19-20,44`
	`  set igmp-snooping-flood-reports enable`
	`  set mcast-snooping-flood-traffic enable`
	`  set snmp-index 62`
	`  next`
	`end`
	
	`config switch interface`
	`  edit "pc_648F_624F"`
	`  set allowed-vlans 19,38-39`
	`  set igmp-snooping-flood-reports enable`
	`  set mcast-snooping-flood-traffic enable`
	`  set snmp-index 59`
	`  next`
	`end`

1232960	The device stops responding when VLAN assignment MAC addresses are cleared.
1233466	Restarting the core MCLAG peer switch causes a loop in the network.
1236922	There is unexpected unicast traffic on nondestination ports.
1241195	ARP packets are not being included in the ACL counters.

Bug ID	Description
1241228	When IGMP snooping is enabled on the FS-148F-POE model, 224.0.0.22 traffic fails to be flooded.
1241538	The real-time bandwidth graph is not being displayed in the GUI of standalone FortiSwitch units.
1241838, 1257800	After restarting an access switch, the managed switch goes offline from the FortiGate device. **Workaround:** Bring the port link up/down by shut/no shut the physical port or execute bounce port.
1243545	Creating an MCLAG topology in FortiSwitchOS 7.6.5 causes the FortiSwitch units to disconnect until the FortiLink interface is brought down and then up again.
1245966	The FS-124G-FPOE model has a loud fan.
1247199, 1257680	No RADIUS traffic is seen, and authentication stops working.
1249226	The user is unable to configure a port of the FSR-112D-POE model to the 802.3 AF mode.
1249370	If the FortiGate device does not include a support CA, FortiLink does not come up.
1250281	The network topology with an MCLAG pair at the distribution layer with one uplink from each industrial switch into each member of the MCLAG pair and an MRP ring on the access layer does not work with the FSR-108F, FSR-112F, or FSR-216F models.
1250364	MAC addresses are not being learned on the trunk for the VLAN that has inter-VLAN blocking enabled.
1253048	In FortiSwitchOS 7.4.8, 7.4.9, 7.6.5, and 7.6.6, the `source-ip` value is ignored for TACACS authentication requests.
1258573	After the VLAN IP is changed, the MCLAG topology with standalone FS-3032E units and large number of VRRP instances becomes unstable.
1258888	The downstream switch incorrectly becomes the STP root when `auto-stp-priority` is enabled.
1261414	The switch incorrectly returns a zero count for the RX and TX broadcast counters.
1261423	The switches are not automatically coming up with the management VLAN as the vlan-range on instance 15.
1263254	The switch management port is displayed as up in the dashboard even when the port is not connected.
1267137	STP should remain disabled on FortiLink interfaces towards the FortiGate device when MCLAG peers are brought up.
1268315	The link monitor stops working randomly.
1272895	In an MCLAG topology, sometimes one MCLAG peer switch will have the mapped VLANs and the other MCLAG peer switch does not.
1275274	Enabling DHCP snooping causes high CPU usage on all switches.
1275885	GET API responses have “\n” appended to MAC addresses.

Known issues

The following known issues have been identified with FortiSwitchOS 8.0.0. 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.
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.
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-124E, 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-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.

Bug ID	Description
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.
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.
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.
950895	In Release 7.4.1, VXLAN supports only one MSTP instance.
1016796	For the FSR-216F-POE, FSR-108F, and FSR-112F-POE models only, `log-mac-event` fails when the MAC address was learned on another interface at the same time as when the MAC address was moved.
1065965	The `set multicast-routing` command (under `config router multicast`) was removed because multicast routing is enabled by default.
1184230	The FS-2048F model does not support the `1000auto` speed.
1279825	When the Enhanced Transmission Selection (ETS) is enabled on a port interface, you should not be able to enable priority-based flow control on the same port interface.
1282646	When `set force-egr-prio-tag` is enabled on a port, the VLAN tag on the egress packet from the port is changed to VLAN 0 even though the port's native VLAN is not the same as the packet's. **Workaround:** Make sure that all ports that have `set force-egr-prio-tag` enabled have the same native VLAN setting.

Bug ID	Description
1293262	The `set packet-sampler disabled` command does not disable the packet sampler and does not return an error. **Workaround:** Restart the FortiSwitch unit.

www.fortinet.com