# FortiLink Release Notes (FortiOS 8.0.0)

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

April 21, 2026
FortiSwitchOS 8.0.0 FortiLink Release Notes (FortiOS 8.0.0)
11-800-1258047-20260421

# TABLE OF CONTENTS

# Change log

| Date | Change Description |
| --- | --- |
| April 21, 2026 | Initial document release for FortiOS 8.0.0 |

# What's new in FortiOS 8.0.0

The following list contains new managed FortiSwitchOS features added in FortiOS 8.0.0:

- The number of supported FortiSwitch devices has increased for some FortiGate models. This change enhances scalability for larger deployments.

| FortiGate model | Number of supported FortiSwitch units |
|---|---|
| FG-50G, FG-50GP, FG-51G, FG-51GP, FG-50G-5G, FG-51G-5G, FG-50G-DSL, FG-50G-SFP | 16 (from 8) |
| FG-200G, FG-201G | 96 (from 64) |
| FG-2600F, FG-2601F | 300 (from 196) |

- On the *Switch > Interfaces* page of the FortiSwitchOS GUI, 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.
- You can now specify trusted IPv4 and IPv6 hosts for admin accounts in FortiOS for managed FortiSwitch units. This feature enhances network security by restricting access for admins to specific IP addresses.
- The `set speed auto-module` command has been changed to `set speed detect-by-module` (under `config switch-controller managed-switch`):

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set speed detect-by-module
         next
      end
   next
end
```

- 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.
- For the FS-6xxF, FSR-216F-POE, FSR-108F, and FSR-112F-POE models, you now configure the port-selection criteria at the global switch-controller level. For all other FortiSwitch models, the port-selection criteria is configured at the trunk level.
- By default, inter-switch links (ISLs) that are automatically formed are assigned a Spanning Tree Protocol (STP) port cost of 1. You can now change that behavior with a new CLI command, `set auto-stp-priority`. By default, this command is enabled, and ISL ports are assigned an STP cost of 1. When this command is disabled, the ISL ports are assigned the STP cost based on the link speed of trunk members. This command is available for all switch models.
- You can now define static groups for particular multicast addresses in a VLAN that has IGMP snooping enabled. You can specify multiple ports in the static group, separated by a space. The trunk interface can also be included in a static group.

- A new toggle button, *Advanced Switching Features*, allows you to enable the following advanced switching features:
  - On the *WiFi & Switch Controller > FortiSwitch Port Policies* page:
    - *LLDP* tab
    - *QoS* tab
    - *VLAN policies* tab
    - *PTP* tab
  - On the *WiFi & Switch Controller > Managed FortiSwitches* page:
    - *MC-LAG Peer* column
    - *Config Sync Status* column
  - On the *Diagnostics and Tools* pane:
    - *Config Sync Status* field (under the switch serial number)
  - On the *WiFi & Switch Controller > FortiSwitch Ports* page:
    - *PTP* column (values are shown only when the FortiSwitch unit supports PTP)
    - *PTP Interface Policy* column (values are shown only when the FortiSwitch unit supports PTP)
- You can now use the LLDP 802.3 TLV to advertise and control the energy-efficient Ethernet (EEE) configuration on managed FortiSwitch units, allowing EEE capabilities to be broadcast across the network.
- The FS-624F, FS-624F-FPOE, FS-648F, and FS-648F-FPOE models now support FortiLink Secure Fabric encryption. Previously, they only supported FortiLink Secure Fabric authentication.
- Several enhancements have been made to the FortiSwitch network access control (NAC) and dynamic port policy (DPP). These changes improve port security and provide flexibility in NAC deployments.
  - You can now use the CLI to specify how many hours that the NAC policies and DPPs keep matched devices. Previously, you could only specify the number of days to keep matched devices. The maximum amount of time is still 120 days (3,072 hours). Set the `match-period` to 0 to always keep the matched devices.
  - When NAC is enabled on a managed switch port, you can now configure the Power over Ethernet (PoE) settings.
  - You can now specify a QoS policy that is applied if the device that matches the NAC policy is the only device on the port.
- You can now limit the number of 802.1X-authenticated sessions allowed on a port. Limiting the number of devices or PCs per port helps increase the security of the network. The default number of sessions allowed per port is 20, and you can configure 2-20 sessions per port.
- You can now move an 802.1X-authenticated client device between ports that are not directly connected to the FortiSwitch unit without having to delete the 802.1X session or make any other configuration changes. The switch controller reauthenticates the client device that has been disconnected from one port and then connected to a different port, even if the client device is behind a hub or IP phone. For example, you can move an 802.1X client PC that connects through an IP phone to port1 of the FortiSwitch unit to a port of a third-party switch that connects to port2 of the FortiSwitch unit. MAC move improves flexibility and reliability in dynamic network environments.
- The FortiOS GUI now supports using both FortiSwitch NAC and 802.1X authentication on the same switch port. Previously, this feature was supported only in the FortiOS CLI.
- You can now configure in the CLI how long MAC authentication bypass (MAB) sessions are kept. This feature is supported on all FortiSwitch models.
- You can now configure a private data encryption key for all managed switches on the FortiGate device. This centralized configuration simplifies network administration and reduces the chance of errors. Using private data encryption prevents exposing credentials in plain text when the FortiGate configuration is backed up.
- The FortiGate GUI has been improved to make switch management easier.

- You can now control when custom commands for a specific managed FortiSwitch unit are pushed from the FortiGate device to the managed FortiSwitch unit. Before FortiOS 8.0.0, custom commands for managed FortiSwitch units were pushed only when the full configuration was updated. You can now specify that custom commands for a specific managed FortiSwitch unit are pushed after any configuration change on the manged FortiSwitch unit. The custom commands are pushed last after the other configuration changes are pushed.
- When you set the `tunnel-mode` to `compatible` (under the `config switch-controller global` command in the FortiSwitchOS CLI), the OpenSSL security level is overridden and changes to 0 on the switch that the command is executed on. If you set the `tunnel-mode` to `strict`, the OpenSSL security level is defined by the level set for each FortiSwitch application.

# Introduction

This document provides the following information for FortiSwitch 8.0.0 devices managed by FortiOS 8.0.0 build 0167:



See the Fortinet Document Library for FortiSwitchOS documentation.

Refer to the FortiLink Compatibility table to find which FortiSwitchOS versions support which FortiOS versions.

FortiLink is not supported in transparent mode.

The maximum number of supported FortiSwitch units depends on the FortiGate model:

| FortiGate Model Range | Number of FortiSwitch Units Supported |
|---|---|
| FortiGate 40F, FG-50G, FortiGate-VM01 | 8 |
| FG-50G, FG-50GP, FG-51G, FG-51GP, FG-50G-5G, FG-51G-5G, FG-50G-DSL, FG-50G-SFP | 16 |
| FGR-50G-5G, FGR-60F, FG-60F, FGR-60F-3G4G, FG-61F, FG-70F, FG-70G, FGR-70G, FG-71F, FG-80F, FG-80FB, FG-80FP, FG-81F, FG-81FP, FG-90G, FG-91G, FortiGate-VM02 | 24 |
| FortiGate 100F, 101F | 32 |
| FG-120G, FG-121G | 48 |
| FortiGate 200E,201E, 200F, 201F, 800D, 900D, FortiGate-VM04 | 64 |
| FortiGate 300E to 500E | 72 |
| FortiGate 200G, 201G, 600E to 900E, 400F, 401F, 601F | 96 |
| FortiGate 1000D, 600F | 128 |
| FortiGate 900G, 901G, 1000F, 1001F, 1100E to 2500E | 196 |
| FG-2600F, FG-2601F, FortiGate-3xxx and up and FortiGate-VM08 and up | 300 |

New models (NPI releases) might not support FortiLink. Contact Customer Service & Support to check support for FortiLink.

# Special notices

## Support of FortiLink features

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

# Upgrade information

Check the FortiSwitchOS Release Notes before upgrading the FortiSwitch firmware from the FortiGate Switch Controller.

FortiSwitchOS 8.0.0 supports upgrading from FortiSwitchOS 3.5.0 and later.

To determine a compatible FortiOS version, check the FortiLink Compatibility matrix.

Within the Security Fabric, the FortiSwitch upgrade is done after the FortiGate upgrade. Refer to the latest *FortiOS Release Notes* for the complete Security Fabric upgrade order.

# 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<br>• Mozilla Firefox version 138<br>• Google Chrome version 136<br>Other browser versions have not been tested but might fully function. 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 FortiOS 8.0.0. For inquiries about a particular bug, please contact Customer Service & Support.

| Bug ID | Description |
|---|---|
| 947247 | Wired clients are not displayed in the physical topology when connected to a FortiSwitch unit. |
| 961142 | An interface in FortiLink is flapping with an MCLAG FortiSwitch unit using DAC on an OPSFPP-T-05-PAB transceiver. |
| 1075365 | Upgrading or restarting managed FortiSwitch units fails when FortiLink is in HTTPS mode. |
| 1105000 | After an aggregate FortiLink went down, the user needed to manually bring the interface down and then manually bring the interface up.<br>**Workaround:** Change the `fortilink-neighbor-detect` setting from `fortilink` to `lldp`. |
| 1114032 | The GUI becomes slow or unresponsive when transceiver-related API requests fail. |
| 1134306 | A VLAN configuration mismatch occurs when a user configures LAN extension and VLANs locally on FortiExtender. |
| 1135460 | The health status becomes unknown after the user renames a switch in the switch controller on some FortiGate models. |
| 1137075 | In the *WiFi & Switch Controller > Managed FortiSwitches* page, the *Topology* view shows the link between FortiSwitch units with a dotted line instead of a solid line.<br>**Workaround:** To see if the FortiLink is up or down, use the `execute switch-controller get-conn-status` command or use the *List* view in the *WiFi & Switch Controller > Managed FortiSwitches* page. |
| 1137213 | The extension device registration fails through the FortiOS GUI when the FortiCare agreement acknowledgment flag is reset after updates. |
| 1138263 | The FortiSwitch port configurations fail to update, and GUI display issues occur when the user-info process overloads system resources with excessive connections. |
| 1138430 | The maximum length allowed for managed FortiSwitch names has been increased from 16 to 35 characters, enabling customers to use more detailed and descriptive names for better network device management and organization. |
| 1141909 | The 10G port on the FortiGate-120G is not coming up when connected to a FortiSwitch S148F port using a 10G DAC cable.<br>**Workaround:** Use a 1M DAC cable or optical cable. |
| 1144076 | High CPU usage occurs in cmdbsvr when FortiLink is enabled and the FortiLink interfaces are connected to the firewall. |
| 1149256 | A renamed FortiSwitch unit failed to synchronize to a secondary FortiGate device. |
| 1153868 | Synchronization errors occur when a FortiLink switch is renamed with a name containing special characters. |

| Bug ID | Description |
|---|---|
| 1154361 | LLDP PDUs are now sent reliably over the FortiLink interface, even when over 1,000 VLANs have been configured. This enhancement improves network stability and device discovery in large-scale deployments. |
| 1154530 | When renaming the switch name in a FortiGate device with 36 characters, the last character is missing after being pushed to the FortiSwitch unit. |
| 1155546 | Duplicate entries occur in the switch-controller managed-switch list when renaming a managed switch. |
| 1164685 | Local MAC addresses are not added to the user device list when the `mab-entry-as dynamic` mode is enabled on the FortiSwitch unit. |
| 1165703 | Random devices not matching to the NAC policy occurs when multiple MAC addresses are present on the same user-device-store entry. |
| 1168050 | If you add a FortiSwitch unit to the FortiGate device in the GUI and the FortiSwitch unit is already registered to a different FortiCare account, the FortiGate device now displays “Registered to another account” instead of “Registration delayed.” |
| 1170323 | Interfaces cannot be enabled as FortiLink interfaces on FortiGate devices with hardware revision 2. |
| 1174647 | FortiLink connections might not display correctly in the *Topology* view in the FortiGate GUI when using MCLAG aggregation. |
| 1183135 | Filtering by allowed VLANs fails to display expected results when using certain FortiOS versions. |
| 1195908 | Virtual VLAN switch forwarding issues occur when STP is enabled in HA setups with multiple members on the FortiGate-600F. |
| 1198110 | FortiSwitch disconnection is observed when adding managed switches. |
| 1208846 | Authentication issues occur when upgrading FortiGate devices due to RADIUS authentication type mismatch |
| 1216623 | High CPU usage occurs when FortiLink IoT triggers packet capture in the switch. |
| 1216633 | The user cannot change the switch name when there is a space is in the name.<br>**Workaround:** Back up the configuration file from the FortiGate device running 7.6.4, manually change the FortiSwitch name in the configuration file, and then restore the configuration back onto the FortiGate device. |
| 1220590 | Intermittent connectivity loss occurs in FortiSwitch units when upgrading FortiOS to 7.6.4. |
| 1229555 | Incorrect VLAN assignment occurs when NAC policies use host name filters with NetBIOS Name Service group names. |
| 1231001 | PoE control issues occur when NAC mode is used on FortiSwitch ports. |
| 1232304 | FortiSwitch units go offline when upgrading the FortiGate device from 7.2.10 to 7.4.x. |
| 1236067 | Devices connected to FortiSwitch units remain online when unplugged and idle for more than 30 seconds. |
| 1238312 | VLANs from other VDOMs are not added to the port when `allowed-vlans-all` is enabled. |

| Bug ID | Description |
|---|---|
| 1239300 | Incorrect port information is displayed when running the `diagnose switch-controller switch-info port-stats` command. |
| 1239751 | FortiSwitch units go offline when upgrading the FortiGate device from 7.2.10 to 7.4.x. |
| 1244391 | The PORTID column is empty (in the output from the `diagnose switch-controller mac-cache show` command) when the FortiGate switch controller is connected to a FortiSwitch stacking configuration. |
| 1249140 | Blank output occurs when running the `diagnose switch-controller switch-info mclag peer-consistency-check` command.<br>**Workaround:** Use the `diagnose switch-controller switch-info mclag peer-consistency-check` command with the trunk name. |
| 1249243 | Ports fail to work when configured with the same settings as other working ports after VLAN reconfiguration in a FortiGate HA A-P cluster.<br>**Workaround:** Do not use '/' in the trunk name. |
| 1254816 | Authentication fails when both hardware and software switches have 802.1X security mode enabled with the `set security-mac-auth-bypass mac-auth-only` command.<br>**Workaround:**<br>1. Turn off port1 and port2 on FG-301E.<br>2. Turn off the software switch,.<br>3. Remove all 802.1X-related settings on ssw1.<br>4. Turn on ssw1 and enable the 802.1X settings.<br>5. Turn on port2 on FG-301E and wait until port2 is authenticated.<br>6. Turn on port1 on FG-301E. |

# Known issues

The following known issues have been identified with FortiOS 8.0.0. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

| Bug ID | Description |
|---|---|
| 298348, 298994 | Enabling the `hw-switch-ether-filter` command on the FG-92D model (the default setting) causes FortiSwitch devices to not be discovered. |
| 520954 | When a "FortiLink mode over a layer-3 network" topology has been configured, the FortiGate GUI does not always display the complete network. |
| 527695 | Starting in FortiOS 6.4.0, VLAN optimization is enabled by default (`set vlan-optimization enable` under `config switch-controller global`). On a network running FortiSwitchOS earlier than 6.0.0, this change results in a synchronization error, but the network still functions normally. If you have FortiSwitchOS 6.0.x, you can upgrade to remove the synchronization error or disable VLAN optimization.<br><br>On a network with `set allowed-vlans-all enable` configured (under `config switch-controller vlan-policy`), the setting reverts to the default, which is disabled, when upgrading to FortiOS 6.4.0. If you want to maintain the allowed-vlans-all behavior, you can restore it after the upgrade. |
| 586801 | NetBIOS stops working when proxy ARP is configured and the access VLAN is enabled because FortiGate units do not support NetBIOS proxy. |
| 621785 | `user.nac-policy[].switch-scope` might contain a data reference to `switch-controller.managed-switch`. When this reference is set by an admin, the admin needs to remove this reference before deleting the `managed-switch`. |
| 789914 | • When LAN segments are enabled on 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-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models, the internal VLAN (`set lan-internal-vlan`) is assigned automatically by default. If the same VLAN is configured on the FortiGate device, the configuration fails when it is pushed to the FortiSwitch unit without any warning message. **WORKAROUND:** Use a custom command.<br>• All sub-VLANs must belong to the same MSTP instance if the FortiLink configuration includes 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-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models. |
| 813216 | After CAPWAP offload is enabled or disabled, FortiLink goes down. |
| 814674 | When upgrading a FortiAP or FortiSwitch unit that is connected to a downstream FortiGate device, a "Failed to retrieve upgrade progress" message appears. |

| Bug ID | Description |
|---|---|
| 910962 | After setting values for `src-mac`, `dst-mac`, and `vlan` for the ACL classifier, you cannot use the `unset` command to remove these settings.<br>**WORKAROUND:**<br>1. Remove `set acl-group <ACL_group_name>` from under the `config switch-controller managed-switch` command.<br>2. Delete the ACL group.<br>3. Delete the ACL.<br>4. Reconfigure the ACL. |
| 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. |
| 1113304 | After the FortiGate device is upgraded from FortiOS 7.6.0 to 7.6.1 or higher when the LLDP configuration is set to vdom or disabled under the FortiLink interface, the FortiSwitch units are offline.<br>**WORKAROUND:**<br>Enable the `lldp-reception` and `lldp-transmission` LLDP configurations under the FortiLink interface or rebuild the FortiLink interface.<br>For example:<br>`config system global`<br>`set lldp-reception enable`<br>`set lldp-transmission enable`<br>`end` |
| 1187046 | The FortiGate device fails to detect the FortiLink-HTTPS tunnel mode when the FortiLink interface is enabled |
| 1275148 | Allowed VLANs are deleted when adding new allowed VLANs on a trunk port. |

www.fortinet.com