Release Notes

FortiSwitchOS 7.6.6

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

FORTINET®

February 23, 2026
FortiSwitchOS 7.6.6 Release Notes
11-766-1237125-20260223

TABLE OF CONTENTS

Change log

Date	Change Description
December 17, 2025	Initial release for FortiSwitchOS 7.6.6
February 10, 2026	Added bug 1253048.
February 23, 2026	Added bug 1257800.

What’s new in FortiSwitchOS 7.6.6

Release 7.6.6 provides the following new features:

- You can now enable DHCP snooping, ARP inspection, and access-VLAN on the same switch VLAN.
- The FS-624F, FS-624F-FPOE, FS-648F, FS-648F-FPOE, FSR_108F, FSR-112F-POE, and FSR-216F-POE models now support the `get switch acl usage` command.
  - For the FS-624F, FS-624F-FPOE, FS-648F, FS-648F-FPOE, FSR-112F-POE, and FSR-216F-POE models, the command displays how many ingress and egress access control list (ACL) rules are used and available.
  - For the FSR-108F model, the command displays the ingress ACL rules used and available.

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 7.6.6 build 1137:

- Supported models on page 6
- Special notices on page 7
- Upgrade information on page 10
- Product integration and support on page 11
- Resolved issues on page 12
- Known issues on page 13

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.6.6 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 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-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-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.

Upgrade information

FortiSwitchOS 7.6.6 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 7.6.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 7.6.6 support

The following table lists FortiSwitchOS 7.6.6 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 7.6.6. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1139793	FortiSwitchOS needs to use a more recent version of OpenSSH.
1171253	When `admin-restrict-local` is disabled, local and remote authentication do not work.
1176543	After DHCP snooping is enabled on the FS-1024E model, there is high CPU usage by dhcprd, leading to the client being disconnected.
1178539	When a 25G port of the FS-2048F model is connected to Mellanox ESXi, the port keeps flapping.
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.
1189852	When 802.1X authentication, DHCP snooping, and dynamic ARP inspection (DAI) are enabled, DHCP and ARP snooping are not performed. This issue has been fixed on the FS-110G-FPOE, FS-124G-FPOE, FS-124G, FS-148F-FPOE, FS-148F-POE, and FS-148F models. **NOTE:** The issue has not been fixed for the FS-148E-POE model.
1196931	The SFP+ ports of the FS-2048F and FS-3032G models do not work with 1G copper SFP modules.
1206457	After upgrading to FortiSwitchOS 7.4.8 on the FS-1xxF Series, the ports summary does not display.
1207784, 1207815	High memory usage occurs on FS-6xxF models, which causes a network impact with clients connected on these FortiSwitch units.
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 the LLDP profiles are changed in the GUI, MED network policy is disabled.
1213254	The FSR-108F, FSR-112F-POE, and FSR-216F-POE models do not support the DHCP server.
1219674	The ABR router did not update the OSPF area 1 routes from the area 1 NSSA router
1220649	Clients connected to FortiSwitch units are facing being disconnected.
1221171	After upgrading FortiSwitchOS to 7.6.4, multicast traffic is dropped.

Known issues

The following known issues have been identified with FortiSwitchOS 7.6.6. 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.
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-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.

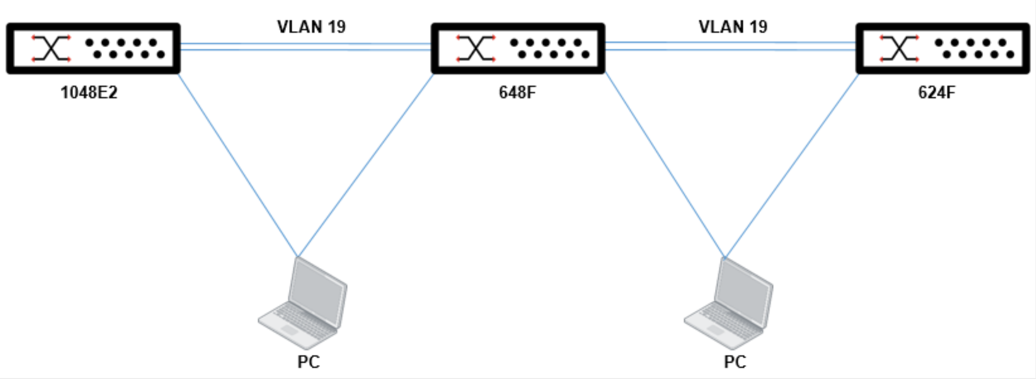
Bug ID	Description
777647	- When MACsec is enabled on a tagged port, the `set exclude-protocol` command does not work on packets with VLAN tags (ARP, IPv4, or IPv6). - If you use the `set exclude-protocol` command with dot1q and packets with VLAN tags (ARP, IPv4, or IPv6), the packets are not MACsec 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.
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.
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.
1184230	The FS-2048F model does not support the `1000auto` speed.
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. **NOTE:** This issue has been fixed on the FS-110G-FPOE, FS-124G-FPOE, FS-124G, FS-148F-FPOE, FS-148F-POE, and FS-148F models.

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td>1222914</td><td>
<b>For the FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124G, FS-124G-FPOE, and FS-110G models:</b>
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.
<b>Workaround:</b> Configure a static multicast group with an unused multicast address and add all ports and trunks as members to let the 224.0.0.x multicast packets flood.
For example:
<pre>
config switch vlan
   edit 300
      set description "vlan300"
      set igmp-snooping enable
      config igmp-snooping-static-group
         edit "group-workaround-test"
            set mcast-addr 239.254.254.254
            set members "port1" "port2" "port3" "port4" "port5" ..
                  "trunk1"
         next
      end
   next
end
</pre>
</td></tr>
<tr><td>1232392</td><td>After configuring RSPAN, the FortiSwitch unit in FortiLink mode crashes. This issues affects the FSR-108F, FSR-112F-POE, and FSR-216F-POE models.</td></tr>
</table>

<table>
<tr><th>Bug ID</th><th>Description</th></tr>
<tr><td>1232415</td><td>

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:



<pre>
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
</pre>

</td></tr>
<tr><td>1253048</td><td>

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.

Workaround: Use FortiSwitchOS 7.6.4 or 7.4.7.

</td></tr>
<tr><td>1257800</td><td>

After restarting an access switch, the managed switch goes offline from the FortiGate device.

Workaround: Breing the port link up/down by shut/no shut the physical port or execute bounce port.

</td></tr>
</table>

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.