

Release Notes

FortiSwitchOS 7.2.10



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



November 11, 2025

FortiSwitchOS 7.2.10 Release Notes

11-7210-1109039-20251111

TABLE OF CONTENTS

Change log	4
Introduction	5
Supported models	5
What's new in FortiSwitchOS 7.2.10	6
Special notices	7
Zero-touch management	7
By default, auto-network is enabled in FortiSwitchOS 7.2.0 and later	7
Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported	7
Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first	7
Connecting multiple FSR-112D-POE switches	8
Upgrade information	9
Product integration and support	10
FortiSwitchOS 7.2.10 support	10
Resolved issues	11
Known issues	12

Change log

Date	Change Description
March 21, 2025	Initial release for FortiSwitchOS 7.2.10
July 23, 2025	Added bug 1184230.
November 11, 2025	Added bug 1104529.

Introduction

This document provides the following information for FortiSwitchOS 7.2.10 build 0539:

- [Supported models on page 5](#)
- [Special notices on page 7](#)
- [Upgrade information on page 9](#)
- [Product integration and support on page 10](#)
- [Resolved issues on page 11](#)
- [Known issues on page 12](#)

See the [Fortinet Document Library](#) for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.2.10 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 7.2.10

Release 7.2.10 provides the following new feature:

- 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.

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 FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.



If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following CLI command to convert the admin password from SHA256 to SHA1 encryption:

```
execute system admin account-convert <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 7.2.10 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 7.2.10 support

The following table lists FortiSwitchOS 7.2.10 product integration and support information.

Web browser	<ul style="list-style-type: none">• Microsoft Edge 114• Mozilla Firefox version 113• Google Chrome version 114 <p>Other web browsers may function correctly, but are not supported by Fortinet.</p>
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 7.2.10. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
1055187	Multicast traffic is not being forwarded.
1085819	When the Virtual Router Redundancy Protocol (VRRP) virtual router IP address is assigned to a secondary IP address, the virtual router IP address uses the network mask of the primary IP address.
1087244	After FortiSwitchOS is upgraded to 7.2.7, the switch is unresponsive.
1101930	The SFP port on the switch goes down, and the switch must be restarted for the SFP port to come up again.
1104529	Devices randomly drop from the network.
1119270	IPv6 devices behind FortiLink are unreachable.
1119678	The RADIUS server password is not saved on the switch when the switch is managed by FortiLink.

Known issues

The following known issues have been identified with FortiSwitchOS 7.2.10. 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	<p>When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server.</p> <p>Workarounds:</p> <ul style="list-style-type: none"> —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the <code>execute interface dhcpclient-renew <interface></code> command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
510943	<p>The time-domain reflectometer (TDR) function (cable diagnostics feature) reports unexpected values.</p> <p>Workaround: When using the cable diagnostics feature on a port (with the <code>diagnose switch physical-ports cable-diag <physical port name></code> CLI command), ensure that the physical link on its neighbor port is down. You can disable the neighbor ports or physically remove the cables.</p>
542031	For the 5xx switches, the <code>diagnose switch physical-ports led-flash</code> 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	<p>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.</p> <p>Workaround: Use passwords with a maximum of 15 characters for FortiSwitchOS 3.x and 6.x.</p>
585550	When packet sampling is enabled on an interface, packets that should be dropped by uRPF will be forwarded.

Bug ID	Description
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.
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 <code>get switch acl counters</code> commands always show the number of bytes as 0.
667079	For the FSR-112D-POE model: <ul style="list-style-type: none"> 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 <code>set flood-unknown-multicast</code> under the <code>config switch global</code> command.
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: <ul style="list-style-type: none"> log-mac-event DHCP snooping LLDP-assigned VLANs NAC Block intra-VLAN traffic
828603	The <code>oids.html</code> file is not accurate.
829807	eBGP does not advertise routes to its peer by default unless the <code>set ebgp-requires-policy disable</code> 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.
925173	You cannot import a PKCS12-formatted file if it does not have a password. Workaround: Extract the certificate and key from the <code>.p12</code> file and then use the GUI to import the certificate and key.
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.

Bug ID	Description
974147	The <code>auto-module</code> speed does not work on the FSR-424F-POE model for FN-TRAN-SFP2-LX. Workaround: Set the speed to <code>1000auto</code> or <code>1000full</code> to bring up the link.
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.
1184230	The FS-2048F model does not support the <code>1000auto</code> speed.



www.fortinet.com

Copyright© yyyy Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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. 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.