

Release Notes

FortiSwitchOS 7.0.6



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/support-and-training/training.html>

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



December 11, 2023

FortiSwitchOS 7.0.6 Release Notes

11-706-819463-20231211

TABLE OF CONTENTS

Change log	4
Introduction	5
Supported models	5
What's new in FortiSwitchOS 7.0.6	6
Special notices	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	7
Upgrade information	8
Product integration and support	9
FortiSwitchOS 7.0.6 support	9
Resolved issues	10
Known issues	12

Change log

Date	Change Description
January 26, 2023	Initial release for FortiSwitchOS 7.0.6
March 1, 2023	Revised the description of bug 857391.
December 11, 2023	Removed bug 673433.

Introduction

This document provides the following information for FortiSwitchOS 7.0.6 build 0092.

- [Supported models on page 5](#)
- [Special notices on page 7](#)
- [Upgrade information on page 8](#)
- [Product integration and support on page 9](#)
- [Resolved issues on page 10](#)
- [Known issues on page 12](#)

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

Supported models

FortiSwitchOS 7.0.6 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-424D, FS-424D-FPOE, FS-424D-POE, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448D, FS-448D-FPOE, FS-448D-POE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D-FPOE, FS-524D, FS-548D, FS-548D-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048D, FS-1048E, FS-T1024E
FortiSwitch 3xxx	FS-3032D, FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in FortiSwitchOS 7.0.6

Release 7.0.6 provides the following new features:

- Three RADIUS attributes are now supported for RADIUS CoA-Request messages:
 - Tunnel-Type—VLAN (13)
 - Tunnel-Medium-Type—IEEE-802 (6)
 - Tunnel-Private-Group-ID—VLAN ID or VLAN name (13)

NOTE: These attributes are also supported in FortiSwitchOS 6.4.12 and 7.2.2 or later.

- The default value for the `set dhcp-snoop-client-req` command (under `config system global`) is now `drop-untrusted`, instead of `forward-untrusted`.

Refer to the [FortiSwitch feature matrix](#) for details about the features supported by each FortiSwitch model.

Special notices

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 7.0.6 supports upgrading from FortiSwitchOS 3.5.0 and later.

For FortiSwitch units managed by FortiGate units, refer to the [FortiSwitch Devices Managed by FortiOS Release Notes](#) for upgrade information.

Product integration and support

FortiSwitchOS 7.0.6 support

The following table lists FortiSwitchOS 7.0.6 product integration and support information.

Web browser	<ul style="list-style-type: none">• Mozilla Firefox version 52• Google Chrome version 56 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 7.0.6. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
801678	After enabling MAC authentication bypass (MAB) on some FortiSwitch models, the FortiGate device removes the NAC device after an inactivity timeout.
806907	Packet loss occurs when using the SP-CABLE-FS-SFP+5 direct-attach cable with FS-124F switches.
824605	The object identifier (OID) 1.3.6.1.2.1.10.7.2.1.19 does not work on FS-1048E.
831495	The TV multicast receivers do not unsubscribe from the multicast stream.
831546	Logging in to a FortiSwitch unit that is managed by FortiSwitch Manager displays a message that incorrectly refers to FortiLink and FortiGate.
837168	The following switches make a high fan noise: <ul style="list-style-type: none"> • FS-224D-FPOE • FS-224E-POE • FS-248D • FS-424D • FS-424D-POE • FS-424D-FPOE • FS-448D • FS-448D-FPOE
846994	Configuring the <code>set group-name</code> command under <code>config match for config user tacacs+</code> does not work.
848619	After configuring the <code>set speed auto-module</code> command (under <code>config switch physical-port</code>) on some switches (such as the FS-124F or FS-148F), the fiber interface does not come up.
849465	Using FN-TRAN-GC with the FS-108E or FS-108F switch causes link flapping or wrongly shows that the link is up when the cable is not connected.
850859	FortiSwitchOS sends the wrong OID for the SNMPv3 trap for link-down events.
857391	After upgrading FortiSwitchOS, multiple FS-448E switches report that the fan has failed, although the fan status is OK.
858223	The “System reboot is required after disk error” log entry is incorrectly labeled as “notice,” instead of “emergency.”
861492	The mgmt interface MAC address is set to 00:01:02:03:04:05 after a reboot or factory reset.
866231	The <code>set status down</code> command (under <code>config switch physical-port</code>) does not work on the SFP+ ports on the FS-426E-FPOE for certain versions of FortiSwitchOS. If you need to shut down any of the SFP+ ports on the FS-426E-FPOE, do not use FortiSwitchOS 7.0.5, 7.2.0, 7.2.1, or 7.2.2.

Bug ID	Description
867758	FortiSwitch units using IPv6 do not respond to SNMPv3 requests.
869616	The FortiAnalyzer and FortiSwitch logs have multiple entries about the fan tray being detected or undetected on an FS-1048E switch, although the fan status is good.

Known issues

The following known issues have been identified with FortiSwitchOS 7.0.6. 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.
463161	Upgrading the FS-448D from FortiSwitchOS 3.5.6 to 3.6.3 fails with an "Invalid root configuration data." error.
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.
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 functionalities and cannot pass IPv6 protocol packets transparently.• If you want to use IGMP snooping or MLD snooping with IPv6 functionalities, you need to enable <code>set flood-unknown-multicast</code> under the <code>config switch global</code> command.
724813	The <code>set enforce-first-as {disable enable}</code> command should have been placed under <code>config neighbor</code> and does not work in its current location (directly under <code>config router bgp</code>). There is no patch available for this issue.
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.
833450	Do not use multicast IP addresses in the ranges of 224-239.0.0.x and 224-239.128.0.x on the FS-2xxD, FS-2xxE, FS-4xxD, and FS-4xxE models.



www.fortinet.com

Copyright© 2023 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.