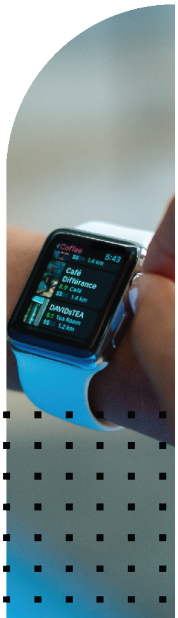
Release Notes

FortiSwitchOS 7.0.3



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 7.0.3 Release Notes
11-703-745512-20231211

TABLE OF CONTENTS

Change log

Date	Change Description
November 29, 2021	Initial release for FortiSwitchOS 7.0.3
December 6, 2021	Added FS-424E, FS-424E-POE, and FS-424E-FPOE to the list of FortiSwitch platforms that now support dynamic ACLs in FortiSwitchOS 7.0.3.
February 7, 2022	Added bug 724813.
February 22, 2022	Added bug 776675.
February 24, 2022	Added bug 784585.
June 7, 2022	Removed bug 718440.
December 11, 2023	Removed bug 673433.

Introduction

This document provides the following information for FortiSwitchOS 7.0.3 build 0058.

See the Fortinet Document Library for FortiSwitchOS documentation.

Supported models

FortiSwitchOS 7.0.3 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-1048D, FS-1048E
FortiSwitch 3xxx	FS-3032D, FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in FortiSwitchOS 7.0.3

Release 7.0.3 provides the following new features:

- NAC LAN segments are now supported on the FS-124F, FS-124F-POE, and FS-124F-FPOE models in FortiLink mode. FortiOS 7.0.1 or higher is required.
- To support the IEEE 802 LLDP MIB, the following OIDs have been added:

Name	OID
lldpLocalSystemData lldpLocChassisIdSubtype lldpLocChassisId lldpLocSysName lldpLocSysDesc lldpLocSysCapSupported lldpLocSysCapEnabled	.1.0.8802.1.1.2.1.3
lldpLocPortTable lldpLocPortNum lldpLocPortIdSubtype lldpLocPortId lldpLocPortDesc	.1.0.8802.1.1.2.1.3.7
lldpLocManAddrTable lldpLocManAddrSubtype lldpLocManAddr lldpLocManAddrLen lldpLocManAddrIfSubtype lldpLocManAddrIfId lldpLocManAddrOID	.1.0.8802.1.1.2.1.3.8

- The `execute 802-1x clear mac <MAC_address>` command allows you to clear the authorized session associated with a specific MAC address.
- TLS 1.0 is no longer supported. To configure which TLS version to use for web administration, use the `set https-ssl-versions {tlsv1-1 | tlsv1-2 | tlsv1-3}` command under `config system web`. In previous releases, the command was `set admin-https-ssl-versions {tlsv1-0 | tlsv1-1 | tlsv1-2 | tlsv1-3}` under `config system global`. **NOTE:** TLS 1.3 is not supported in FIPS mode.
- Dynamic access control lists (DACLs) are now supported on the following platforms:
  - FSR-124D
  - FS-224D-FPOE
  - FS-248D
  - FS-424D
  - FS-424D-POE
  - FS-424D-FPOE
  - FS-424E
  - FS-424E-POE

  - FS-424E-FPOE
  - FS-448D
  - FS-448D-POE
  - FS-448D-FPOE
  - FS-224E
  - FS-224E-POE
  - FS-248E-POE
  - FS-248E-FPOE
  - FS-524D
  - FS-524D-FPOE
  - FS-548D
  - FS-548D-FPOE
  - FS-1024D
  - FS-1048D
  - FS-3032D
- When the maximum number of 802.1x-authorized clients for a port, which is 20, is exceeded, a warning log (including the MAC address) is reported. For example:
  ```
  "6: 1969-12-31 16:02:09 log_id=0104010017 type=event subtype=switch pri=warning vd=root
       MAC=f0:4d:a2:be:a3:31 , not authorized, exceed port9 maximum of 20 MAC sessions."
  ```
- When the maximum number of 802.1x-authorized clients for the system, which is 10 x the model number of ports, is exceeded, a warning log (including the MAC address) is reported. For example, on an FS-224E model:
  ```
  "1: 2021-11-02 20:25:49 log_id=0104010010 type=event subtype=switch pri=warning vd=root
       MAC=f0:4d:a2:be:a3:31 , not authorized, exceed system maximum of 240 MAC sessions."
  ```
- The following are the new REST API endpoints:
  - The `monitor/switch/dhcp-snooping-limit-db-details` endpoint displays details about the DHCP-snooping lease-count database.
  - The `monitor/switch/cable-diag` endpoint displays the results of a time-domain reflectometer (TDR) diagnostic test on the cables connected to a specific port.
- The following are the REST API schema changes:
  - The `cmdb/system/fsw-cloud` endpoint has been renamed and is now the `cmdb/system/flan-cloud` endpoint.
  - The response from the `monitor/switch/capabilities` endpoint has been updated to reflect the current switch capabilities.

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 7.0.3 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. See https://docs.fortinet.com/document/fortiswitch/7.0.0/managed-switch-release-notes.

Product integration and support

FortiSwitchOS 7.0.3 support

The following table lists FortiSwitchOS 7.0.3 product integration and support information.

Web browser	• Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

Resolved issues

The following issues have been fixed in FortiSwitchOS 7.0.3. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
488900	The processing load of background tasks needs to be reduced.
724558	A network outage is caused by the flash module of the FS-1048E failing.
735913	The Spanning Tree Protocol (STP) flaps on an FS-448DN, and roles are changed.
741267	After a user edits the physical interface in the GUI, clicking *OK* causes a “Request timed out. Please try again later.” error.
741354	The DHCP client module crashes with a signal 11 (segmentation fault) in a two-tier MCLAG network topology using managed FortiSwitch units.
743749	After a third-party hub is disconnected and then connected, MAC Authentication Bypass (MAB) sometimes does not work.
746584	The FS-448D stops responding after a random number of days.
748177	When the network monitor is enabled, the MCLAG trunk becomes unstable.
749315	The VLAN ID of a switch virtual interface (SVI) should not be the same as the native VLAN ID of a layer-2 internal interface.
749744	Setting the 10G module’s speed to 1G should not cause error messages.
752085	When the switch receives a recordAgreement, the FS-1024D sends the bridge protocol data unit (BPDU) with the proposal bit on every 2 seconds.
753630	When the 802.1x port-based authentication daemon crashes, MAB does not function until the switch is restarted.
754232	The user is receiving “internal PS changes to good state” and “internal PS changes to bad state” warning messages.

Common vulnerabilities and exposures

FortiSwitchOS 7.0.3 is no longer vulnerable to the following CVEs:

- CVE-2021-3711
- CVE-2021-3712
- CWE-190

Visit https://fortiguard.com/psirt for more information.

Known issues

The following known issues have been identified with FortiSwitchOS 7.0.3. 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	When DHCP snooping is enabled on the FSR-112D-POE, the switched virtual interface (SVI) cannot get the IP address from the DHCP server. **Workarounds:** —Use a static IP address in the SVI when DHCP snooping is enabled on that VLAN. —Temporarily disable dhcp-snooping on vlan, issue the `execute interface dhcpclient-renew <interface>` command to renew the IP address. After the SVI gets the IP address from the DHCP server, you can enable DHCP snooping.
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 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.

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.
724813	The `set enforce-first-as {disable | enable}` command should have been placed under `config neighbor` and does not work in its current location (directly under `config router bgp`). There is no patch available for this issue.
734917	When you configure a PIM multicast flow with a range of group addresses for SVIs and the group address range overlaps with a dynamic IGMPv3 group receiver that has joined groups in a different VLAN, then the dynamic IGMPv3 receiver will still receive multicast traffic unexpectedly even after leaving the joined groups.
776675	• FortiSwitchOS cannot use the NAS-Filter-Rule when it exceeds 65 characters. • If you specify more than one port or port range (for example, `10.105.0.106/24 100,200,300` or `10.105.0.106/24 100-200,300, 700-900`) when defining the source or destination in a dynamic ACL entry, FortiSwitchOS applies the first port or port range and ignores the rest. • If you specify the destination port after the `any` keyword, you must specify `any 0.0.0.0/0 <port_number>`. For example, instead of `permit in TCP any to any 90 cnt`, use `permit in TCP any to any 0.0.0.0/0 90 cnt` instead.
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.

www.fortinet.com