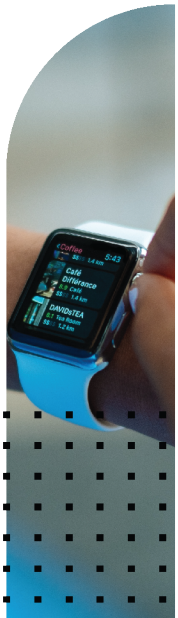
FortiSwitch Devices Managed by FortiOS Release Notes

FortiSwitch 7.0.0



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

April 26, 2021
FortiSwitch 7.0.0 FortiSwitch Devices Managed by FortiOS Release Notes
11-700-691898-20210426

TABLE OF CONTENTS

Change log

Date	Change Description
March 30, 2021	Initial document release for FortiOS 7.0.0
April 2, 2021	Updated the “What’s new in FortiOS 7.0.0” section.
April 7, 2021	Updated the “What’s new in FortiOS 7.0.0” and “Special notices” sections. Added bug 520954 to the “Known issues” section.
April 9, 2021	Updated the “What’s new in FortiOS 7.0.0” section.
April 26, 2021	Added link for the FortiSwitchOS feature matrix.

Introduction

This document provides the following information for FortiSwitchOS 7.0.0 devices managed by FortiOS 7.0.0 build 0066.

See the Fortinet Document Library for FortiSwitch documentation.

NOTE: 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, 91E, FortiGate-VM01	8
FortiGate 60F, 6xE, 80F, 8xE, 90E	16
FortiGate 100D, FortiGate-VM02	24
FortiGate 100E, 100EF, 100F, 101E, 140E, 140E-POE	32
FortiGate 200E, 201E	64
FortiGate 300D to 500D	48
FortiGate 300E to 500E	72
FortiGate 600D to 900D and FortiGate-VM04	64
FortiGate 600E to 900E	96
FortiGate 1000D to 15xxD	128
FortiGate 1100E to 25xxE	196
FortiGate-3*xxx* and up and FortiGate-VM08 and up	300

Supported models

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

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

What's new in FortiOS 7.0.0

The following list contains new managed FortiSwitch features added in FortiOS 7.0.0.

GUI changes

- Three new tests have been added to the FortiSwitch recommendations in the *Security Fabric* > *Security Rating* page to help optimize your network:
  - Check if the quarantine bounce port option is enabled.
  - Check if the PoE status of the switch controller auto-config default policy is enabled.
  - Check if PoE pre-standard detection for all user ports is enabled.
- You can now use the GUI to view and configure FortiSwitch ports that are shared between VDOMs. To share FortiSwitch ports between VDOMs, you must use the CLI. Go to *WiFi & Switch Controller* > *FortiSwitch Ports* to view the shared FortiSwitch ports and edit them.
- A new cloud icon indicates when the FortiSwitch unit is being managed over layer 3.
- The new FortiSwitch NAC VLANs widget shows a pie chart of the assigned FortiSwitch NAC VLANs. When expanded to the full screen, the widget shows a full list of devices grouped by VLAN, NAC policy, or last seen.
- There have been GUI updates to the *FortiSwitch Ports*, *FortiLink Interface*, and *FortiSwitch NAC Policies* pages to simplify the configuration of NAC policies.
  Previously, dynamic port policies had to be configured in the *FortiSwitch Ports*, *FortiLink Interface*, and *FortiSwitch NAC Policies* pages. Now, configuring dynamic port polices is under the *Dynamic Port Policies* tab on the *FortiSwitch Port Policies* page.
- The *FortiSwitch NAC Policies* page is now the *NAC Policies* page.
- The access mode of each FortiSwitch port is listed in the *Mode* column in the FortiSwitch Ports page. Right-click in the *Mode* column to select the access mode of the port:
  - *Static*—The port does not use a dynamic port policy or FortiSwitch NAC policy.
  - *Assign Port Policy*—The port uses a dynamic port policy.
  - *NAC*—The port uses a FortiSwitch NAC policy.

CLI changes

- New FortiOS commands allow you to enable the automatic provisioning of FortiSwitch firmware after authorization. On FortiGate models with a disk, up to four images of the same FortiSwitch model can be uploaded. On FortiGate models without a disk, one FortiSwitchOS image can be uploaded.
- When a FortiSwitch upgrade cannot be completed (because of connectivity issues, for example), you can cancel the upgrade with a new FortiOS command:

```
execute switch-controller switch-software cancel {all | sn <FortiSwitch_serial_ number>
     | switch-group <switch_group_ID>}
```

- Supported managed-switch ports can be configured with a forward error correction (FEC) state of Clause 74 FC-FEC for 25-Gbps ports and Clause 91 RS-FEC for 100-Gbps ports.
- A new FortiOS command allows you to control the cipher used by the switch-controller CAPWAP:

  ```
  config switch-controller system
     set tunnel-mode {compatible | strict}
  end
  ```

  By default, `tunnel-mode` is set to `compatible`, which lets the switch-controller CAPWAP use AES128-SHA:DES-CBC3-SHA. If you set `tunnel-mode` to `strict`, the switch-controller CAPWAP uses the cipher set in FortiOS.
- You can now manually create an inter-switch link (ISL) trunk. You can also enable or disable automatic VLAN configuration on the manually created (static) ISL trunk.
- Fortinet now supports Federal Information Processing Standard Publication (FIPS) 140-2 (Level 2) for the following managed FortiSwitch models:
  - FS-424E
  - FS-424E-FPOE
  - FS-M426E-FPOE
  - FS-424E-Fiber
  - FS-448E
  - FS-448E-FPOE
  - FS-1048E
  - FS-3032E
- There are more authentication protocols and privacy (encryption) protocols supported under the `config switch-controller snmp-user` command. The following authentication protocols are available for the `set auth-proto` command:
  - HMAC-MD5-96
  - HMAC-SHA-1
  - HMAC-SHA-224
  - HMAC-SHA-256
  - HMAC-SHA-384
  - HMAC-SHA-512

  The following privacy (encryption) protocols are available for the `set priv-proto` command:
  - CFB128-AES-128 symmetric encryption protocol
  - CFB128-AES-192 symmetric encryption protocol
  - CFB128-AES-192-C symmetric encryption protocol
  - CFB128-AES-256 symmetric encryption protocol
  - CFB128-AES-256-C symmetric encryption protocol
  - CBC-DES symmetric encryption protocol
- There were some FortiOS CLI changes for the FortiSwitch network access control. The `set switch-port-policy` command under `config user nac-policy` was removed. The `config switch-controller nac-settings` command is now the `config switch-controller fortilink-settings` command.

GUI and CLI changes

- You can now specify rules that dynamically determine port policies. After you create the FortiLink policy settings, you define the dynamic port policy rules. When a rule matches the specified device patterns, the switch-controller

actions control the port's properties.

- The FortiGate NAC engine is responsible for assigning the device to the right VLAN based on the NAC policy when a device first connects to a switch port or when a device goes from offline to online. This process has been optimized to shorten the amount of time it takes for a new device to be recognized and assigned to the VLAN. These optimizations include the following:
  - A new event-based approach.
  - A new NAC MAC cache table that populates MAC addresses from the FortiSwitch unit immediately after an event.
  - NAC inactive timers are now applied to the NAC MAC cache table.
  - Added `nac-periodic-interval` to run the NAC engine at intervals in case any events are missed. The range is 5 to 60 seconds, and the default setting is 15 seconds.

  Before these optimizations, the process took approximately 65 seconds from the time the device links to a switch port to matching the device to a NAC policy. After optimization, the process takes a maximum of 16 seconds with a minimum `nac-periodic-interval` of 5 seconds.

Special notices

Support of FortiLink features

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

Downgrading FortiSwitchOS 7.0.0 to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 to 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 to FortiSwitch 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 to versions earlier than 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 FortiSwitch 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”.

If you do not want to convert the format of the FortiSwitch admin password, you can use the FortiOS CLI to override the managed FortiSwitch admin password with the FortiGate admin password.

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

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

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

To override the managed FortiSwitch admin password with the FortiGate admin password:

```
config switch-controller switch profile
```

```
edit <FortiSwitch_profile_name>
   set login-passwd-override enable
   set login-passwd <new_password>
end
```

NAC policies not maintained or converted when upgrading to 7.0.0

Existing NAC policies are not maintained or automatically converted into dynamic port policies after upgrading to FortiOS 7.0.0. They have to be reconfigured.

Upgrade information

FortiSwitchOS 7.0.0 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 7.0.0 support

The following table lists FortiSwitchOS 7.0.0 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)	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 7.0.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
567996	Slow load times for the *Managed FortiSwitch* and *FortiSwitch Ports* pages when there is a large number of FortiSwitch units.
649913	The HA cluster does not synchronize when a user configures an active LACP with MCLAG using a FortiManager unit.
671135	The flcfg process crashes when a user configures FortiSwitch units through FortiLink.
686325	A high rate of LLDP traffic can halt FortiSwitch configuration synchronization.
690904	The user cannot de-authorize a managed FortiSwitch unit or assign a VLAN on a FortiSwitch port on a tenant VDOM.

Known issues

The following known issues have been identified with FortiOS 7.0.0. 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. 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.
602397	The *FortiSwitch Ports* page is slow with a large topology.
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`.

www.fortinet.com

Copyright© 2021 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.