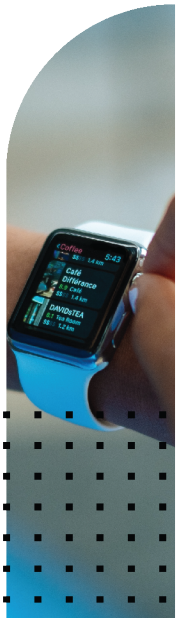
# FortiSwitch Devices Managed by FortiOS Release Notes

## FortiSwitch 7.0.1



**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

July 15, 2021
FortiSwitch 7.0.1 FortiSwitch Devices Managed by FortiOS Release Notes
11-701-711493-20210715

# TABLE OF CONTENTS

# Change log

| Date | Change Description |
| --- | --- |
| July 15, 2021 | Initial document release for FortiOS 7.0.1 |

# Introduction

This document provides the following information for FortiSwitchOS 7.0.1 devices managed by FortiOS 7.0.1 build 0157.

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



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 |

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

# What's new in FortiOS 7.0.1

The following list contains new managed FortiSwitch features added in FortiOS 7.0.1.

- You can now use LAN segments when configuring FortiSwitch NAC settings to prevent hosts from having to renew IP addresses when moving to another VLAN.
- Use the new `diagnose switch-controller switch-info port-properties [<FortiSwitch_serial_number>] [<port_name>]` command to check the port properties of managed FortiSwitch units.
- You can now configure in FortiOS which DHCP servers that DHCP snooping includes in the server access list. These servers on the list are allowed to respond to DHCP requests.
- You can now change the order in which FortiSwitch units are displayed in the Topology view.
- You can now configure a dynamic firewall address for devices and use it in a NAC policy. When a device matches the NAC policy, the MAC address for that device is automatically assigned to the dynamic firewall address, which can be used in firewall policies to control traffic from/to these devices.
- Three SNMP OIDs have been added to the FortiOS enterprise MIB 2 tables in FortiOS 7.0.1. They report the FortiSwitch port status and FortiSwitch CPU and memory statistics.

# Special notices

## Support of FortiLink features

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

## 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 and later 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”.

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 FortiSwitchOS 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 7.0.1 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 7.0.1 support

The following table lists FortiSwitchOS 7.0.1 product integration and support information.

| | |
|---|---|
| **Web browser** | • Mozilla Firefox version 52<br>• Google Chrome version 56<br>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 7.0.1. For inquiries about a particular bug, please contact Customer Service & Support.

| Bug ID | Description |
|---|---|
| 602397 | The *FortiSwitch Ports* page is slow with a large topology. |
| 647817 | Configuration changes made on the FortiGate device are not taking effect on the managed FortiSwitch unit. |
| 676306 | The HTTP and HTTPS daemon has signal 6 and 11 crashes at `cmf_query_create_child` because of a segfault in the `/api/v2/monitor/switch-controller/managed-switch/transceivers` endpoint. |
| 682430 | After failing to create FortiLink, an empty entry was created in NTP under the interface configuration. |
| 689392 | The switch port's *Errors* counters for managed FortiSwitch units show a zero when the port actually has errors. |
| 699533 | In FortiOS 7.0.0, the default authentication protocol for a switch-controller SNMP user is SHA256; this default is incompatible with FortiSwitch units running 6.4.1 and earlier versions. Before FortiOS 7.0.0, the default authentication protocol was SHA1. |
| 702942 | The FortiLink trunk is not formed on a FortiSwitch unit connected to a FortiGate device. When managed switches are learned on the software switch and hardware switch, they were deleted from the CLI, and the FortiLink daemon did not clear the states for those switches, so new switches were not learned. |
| 717506 | The user was unable to add descriptions for shared FortiSwitch ports. |

# Known issues

The following known issues have been identified with FortiOS 7.0.1. 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.<br><br>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. |
| 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`. |
| 723501 | When STP is enabled on the hardware switch interface, FortiLink lost connection to the FortiSwitch unit. |

www.fortinet.com