



FortiSwitch Devices Managed by FortiOS Release Notes

Version 6.4.5

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FORTINET PRIVACY POLICY

<https://www.fortinet.com/corporate/about-us/privacy.html>

FEEDBACK

Email: techdocs@fortinet.com



FortiSwitch Devices Managed by FortiOS Release Notes

September 1, 2021

11-645-674482-20210901

TABLE OF CONTENTS

| | |
|--|-----------|
| Change log | 4 |
| Introduction | 5 |
| Supported models..... | 5 |
| What's new in FortiOS 6.4.5..... | 6 |
| Special notices | 9 |
| Support of FortiLink features..... | 9 |
| Upgrade information | 12 |
| Product integration and support | 13 |
| FortiSwitchOS 6.4.6 support..... | 13 |
| Resolved issues | 14 |
| Known issues | 15 |

Change log

| Date | Change Description |
|-------------------|---|
| February 18, 2021 | Initial document release for FortiOS 6.4.5 |
| February 26, 2021 | Added another feature to the “What’s new in FortiOS 6.4.5” section. |
| September 1, 2021 | Updated the “Support of FortiLink features” section. |

Introduction

This document provides the following information for FortiSwitch 6.4.6 devices managed by FortiOS 6.4.5 build 1828.

- [Special notices on page 9](#)
- [Upgrade information on page 12](#)
- [Product integration and support on page 13](#)
- [Resolved issues on page 14](#)
- [Known issues on page 15](#)

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-3xxx 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.

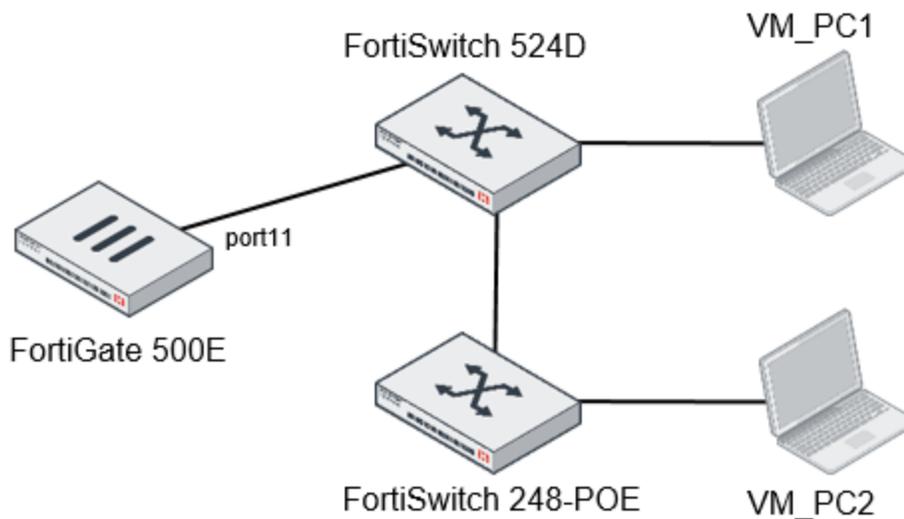
What's new in FortiOS 6.4.5

The following list contains new managed FortiSwitch features added in FortiOS 6.4.5:

- You can now use wildcards in a MAC address in a NAC policy.

When configuring a NAC policy, you can use the wildcard * character when manually specifying a MAC address to match the device.

```
config user nac-policy
  edit <policy>
    set mac "xx:xx:xx:**:**:"
  next
end
```



In this example, VM_PC1 and VM_PC2 both have MAC addresses that start with 00:0c:29. A NAC policy is created on the FortiGate 500E to match both PCs. After the PCs are connected to the FortiSwitch units, they are detected by the NAC policy and assigned to Lab_VLAN.

To configure a MAC address with wildcards in a NAC policy:

- Configure a MAC policy to be applied on the managed FortiSwitch units through the NAC device:

```
config switch-controller mac-policy
  edit "LAB_Linux"
    set fortilink "port11"
```

```

        set vlan "Lab_VLAN"
    next
end

```

2. Configure the NAC policy matching pattern to identify matching NAC devices:

```

config user nac-policy
  edit "VM-Policy"
    set mac "00:0c:29:**:**:**"
    set switch-fortilink "port11"
    set switch-mac-policy "LAB_Linux"
  next
end

```

3. Check that the NAC devices are added:

```

# show switch-controller nac-device
config switch-controller nac-device
  edit 2
    set description "auto detected @ 2020-11-30 14:13:45"
    set mac 00:0c:29:d4:4f:3c
    set last-known-switch "S248EPTF18001384"
    set last-known-port "port6"
    set matched-nac-policy "VM-Policy"
    set mac-policy "LAB_Linux"
  next
  edit 3
    set description "auto detected @ 2020-11-30 14:16:07"
    set mac 00:0c:29:a8:0a:1c
    set last-known-switch "S524DN4K16000116"
    set last-known-port "port7"
    set matched-nac-policy "VM-Policy"
    set mac-policy "LAB_Linux"
  next
end

```

- PoE pre-standard detection is now disabled by default.

Starting with this version, the factory default setting for power over Ethernet (PoE) pre-standard detection is `disable` for both managed and standalone FortiSwitch units.

Depending on the FortiSwitch model, you can manually change the `poe-pre-standard-detection` setting on the global level or on the port level.



PoE pre-standard detection is a global setting for the following FortiSwitch models: FSR-112D-POE, FS-548DFPOE, FS-524D-FPOE, FS-108D-POE, FS-224D-POE, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, and FS-124EFPOE. For the other FortiSwitch PoE models, PoE pre-standard detection is set on each port.

On the global level, set `poe-pre-standard-detection` with the following commands:

```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    set poe-pre-standard-detection {enable | disable}
  next
end
```

On the port level, set `poe-pre-standard-detection` with the following commands:

```
config switch-controller managed-switch
  edit <FortiSwitch_serial_number>
    config ports
      edit <port_name>
        set poe-pre-standard-detection {enable | disable}
      next
    end
  next
end
```

When you upgrade FortiOS, the setting of `poe-pre-standard-detection` stays the same. When you downgrade from FortiOS 6.4 to FortiOS 6.2, the setting of `poe-pre-standard-detection` stays the same.

- You can now use the `set fortalink-p2p-native-vlan <VLAN>` command (under `config switch global`) to specify the native VLAN on the inter-switch link (ISL) when `fortilink-p2p` is enabled. By default, the native VLAN is 4094.
- The `set fortlink-p2p {enable | disable}` command under `config switch physical port` has been changed to `set fortalink-p2p {enable | disable}`.

Special notices

Support of FortiLink features

The following table lists the FortiSwitch models supported by FortiLink features.

| FortiLink Features | FortiSwitch Models |
|---|---|
| Centralized VLAN Configuration | D-series, E-series, F-series |
| Switch POE Control | D-series, E-series, F-series |
| Link Aggregation Configuration | D-series, E-series, F-series |
| Spanning Tree Protocol (STP) | D-series, E-series, F-series |
| LLDP/MED | D-series, E-series, F-series |
| IGMP Snooping | D-series, E-series, F-series |
| 802.1x Authentication (Port-based, MAC-based, MAB) | D-series, E-series, F-series |
| Syslog Collection | D-series, E-series, F-series |
| DHCP Snooping | D-series, E-series, F-series |
| Device Detection | D-series, E-series, F-series |
| Support FortiLink FortiGate in HA Cluster | D-series, E-series, F-series |
| LAG support for FortiLink Connection | D-series, E-series, F-series |
| Active-Active MCLAG from FortiGate to FortiSwitch units for Advanced Redundancy | Not supported on FS-1xx Series |
| sFlow | Not supported on FS-1xxE Series or FS-1xxF Series |
| Dynamic ARP Inspection (DAI) | D-series, E-series, F-series |
| Port Mirroring | D-series, E-series, F-series |
| RADIUS Accounting | D-series, E-series, F-series |
| Centralized Configuration | D-series, E-series, F-series |

| FortiLink Features | FortiSwitch Models |
|---|---|
| Block Intra-VLAN Traffic | D-series, E-series, F-series |
| STP BDPU Guard, Root Guard, Edge Port | D-series, E-series, F-series |
| Loop Guard | D-series, E-series, F-series |
| Switch admin Password | D-series, E-series, F-series |
| Storm Control | D-series, E-series, F-series |
| 802.1x-Authenticated Dynamic VLAN Assignment | D-series, E-series, F-series |
| Host Quarantine on Switch Port | D-series, E-series, F-series |
| QoS | Not supported on FSR-112D-POE |
| Centralized Firmware Management | D-series, E-series, F-series |
| Automatic network detection and configuration | D-series, E-series, F-series |
| Dynamic VLAN assignment by group name | D-series, E-series, F-series |
| Sticky MAC addresses | D-series, E-series, F-series |
| NetFlow and IPFIX flow tracking and export | D-series, E-series, F-series |
| FortiSwitch split ports | FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE, FS-1048E, FS-3032D, and FS-3032E |
| Encapsulated remote switched port analyzer (ERSPAN) | FS-2xx and higher |
| MSTP instances | D-series, E-series, F-series |
| NOTE: In FortiLink mode, the FortiGate unit supports 1-14 instances for all platforms. | |
| QoS statistics | D-series, E-series, F-series |
| Configuring SNMP through FortiLink | D-series, E-series, F-series |
| IPv4 source guard | FSR-124D, FS-224D-FPOE, FS-248D, FS-424D-POE, FS-424D-FPOE, FS-448D-POE, FS-448D-FPOE, FS-424D, FS-448D, FS-2xxE, and FS-4xxE |
| Integrated FortiGate network access control (NAC) function | D-series, E-series, F-series |
| FortiGuard IoT identification | D-series, E-series, F-series |

| FortiLink Features | FortiSwitch Models |
|---|--|
| Point-to-point layer-2 network supported | D-series, E-series, F-series |
| Dynamic detection of LLDP neighbor devices | D-series, E-series, F-series |
| Explicit congestion notification (ECN) | FS-1024D, FS-1048D, FS-1048E, FS-3032D, FS-3032E, FS-4xxE, and FS-5xxD |
| Aggregation mode selection for trunk members | D-series, E-series, F-series |
| Multiple attribute values sent in a RADIUS Access-Request | D-series, E-series, F-series |
| PTP transparent-clock mode | FS-1048E, FS-224D, FS-224E, FS-3032D, FS-3032E, FS-424D, FS-4xxE, and FS-5xxD |
| Rapid PVST interoperation | D-series, E-series, F-series |
| Support of matching EMS tags in NAC policies | D-series, E-series, F-series |
| Flash port LEDs | D-series, E-series, F-series |
| Cable diagnostics | Not supported on FSR-112D-POE, FS-1024D, FS-1048D, FS-1048E, FS-3032D, or FS-3032E |
| Automated detection and recommendations | D-series, E-series, F-series |
| Flow control | D-series, E-series, F-series |
| Ingress pause metering | 200 series, 400D and 400E series, 500 series, FS-1024D, FS-1048D, FS-1048E, and FS-3032D |

Upgrade information

FortiSwitchOS 6.4.6 supports upgrading from FortiSwitchOS 3.5.0 and later.

To determine a compatible FortiOS version, check the FortiLink Compatibility matrix (<https://docs.fortinet.com/document/fortiswitch/6.4.5/fortilink-compatibility>).

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. See <https://docs.fortinet.com/document/fortigate/6.4.4/fortios-release-notes>.

Product integration and support

FortiSwitchOS 6.4.6 support

The following table lists FortiSwitchOS 6.4.6 product integration and support information.

| | |
|------------------------------------|--|
| Web browser | <ul style="list-style-type: none">• Mozilla Firefox version 52• Google Chrome version 56 <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 FortiOS 6.4.5. For inquiries about a particular bug, please contact [Customer Service & Support](#).

| Bug ID | Description |
|--------|--|
| 686031 | In FortiOS 6.4.4 with FortiSwitchOS 6.4.5, LLDP traffic causes the memory used by the flcfg daemon to keep increasing. |

Known issues

The following known issues have been identified with FortiOS 6.4.5. For inquiries about a particular bug or to report a bug, please contact [Fortinet Customer Service & Support](#).

| Bug ID | Description |
|----------------|---|
| 298348, 298994 | Enabling the <code>hw-switch-ether-filter</code> command on the FG-92D model (the default setting) causes FortiSwitch devices to not be discovered. |
| 527695 | <p>Starting in FortiOS 6.4.0, VLAN optimization is enabled by default (<code>set vlan-optimization enable</code> under <code>config switch-controller global</code>). 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.</p> <p>On a network with <code>set allowed-vlans-all enable</code> configured (under <code>config switch-controller vlan-policy</code>), the setting reverts to the default, which is disabled, when upgrading to FortiOS 6.4.0. If you want to maintain the <code>allowed-vlans-all</code> behavior, you can restore it after the upgrade.</p> |
| 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 <i>FortiSwitch Ports</i> page is slow with a large topology. |
| 621785 | <code>user.nac-policy[].switch-scope</code> might contain a data reference to <code>switch-controller.managed-switch</code> . When this reference is set by an admin, the admin needs to remove this reference before deleting the <code>managed-switch</code> . |



FORTINET®



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.