FortiSwitch Devices Managed by FortiOS Release Notes

Version 6.4.0

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 2, 2021

11-640-591526-20210902

TABLE OF CONTENTS

Change log

Date	Change Description
March 31, 2020	Initial document release for FortiOS 6.4.0
April 1, 2020	Added bug 623550.
April 20, 2020	Added bug 628121.
September 1, 2021	Updated the “Support of FortiLink features” section.
September 2, 2021	Updated the “Support of FortiLink features” section.

Introduction

This document provides the following information for FortiSwitch 6.4.0 devices managed by FortiOS 6.4.0 build 1579.

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 91E, FortiGate-VM01	8
FortiGate 6xE, 8xE, 90E	16
FortiGate 100D, FortiGate-VM02	24
FortiGate 100E, 100EF, 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 6.4.0

The following list contains new managed FortiSwitch features added in FortiOS 6.4.0:

- An integrated FortiGate network access control (NAC) function is provided to the FortiAP and FortiSwitch networks by using a shared set of NAC policies. The NAC policy can be applied based on data from the user device list. There is also a wizard to help with configuring FortiSwitch NAC settings and defining a FortiSwitch NAC VLAN.
- To more accurately detect Internet of Things (IoT) devices, a new FortiGuard service is available to provide a large database of device IoT identification. Devices detected on the local FortiGate unit and through the FortiAP and FortiSwitch networks can be queried with the FortiGuard IoT device database to provide enhanced identification.
- A FortiLink topology with an HA cluster of four FortiGate units is now supported.
- FortiLink mode can now run over a point-to-point layer-2 network.
- LLDP neighbor devices are now dynamically detected.
- IPv4 source guard can now be configured in FortiOS for managed FortiSwitch units that support IP source guard.
- The number of FortiSwitch units supported by certain FortiGate models has been increased.
- The quarantine feature on the FortiSwitch unit has been extended by allowing a device to be quarantined but remain with the VLAN where it was detected. You can still quarantine devices to a VLAN.
- Administrators can now modify some configuration options of automatically generated VLANs using the `config switch-controller initial-config template` command. These changes are applied at the time of VLAN creation.
- On the Managed FortiSwitch page, you can now view the managed FortiSwitch units in a list, in groups of switches, or in a topology diagram.
- IGMP snooping is now always enabled on managed switch interfaces and cannot be disabled.
- When an inter-switch link (ISL) is formed automatically in FortiLink mode, the `igmps-flood-reports` and `igmps-flood-traffic` options are now disabled by default.
- Storm control is now disabled by default in FortiLink mode.

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
Switch POE Control	D-series, E-series
Link Aggregation Configuration	D-series, E-series
Spanning Tree Protocol (STP)	D-series, E-series
LLDP/MED	D-series, E-series
IGMP Snooping	Not supported on 112D-POE
802.1x Authentication (Port-based, MAC-based, MAB)	D-series, E-series
Syslog Collection	D-series, E-series
DHCP Snooping	Not supported on 1xxE-Series
Device Detection	D-series, E-series
Support FortiLink FortiGate in HA Cluster	D-series, E-series
LAG support for FortiLink Connection	D-series, E-series
Active-Active Split MLAG from FortiGate to FortiSwitch units for Advanced Redundancy	Not supported on FS-1xx Series
sFlow	Not supported on 1xxE-Series
Dynamic ARP Inspection (DAI)	D-series, E-series
Port Mirroring	D-series, E-series
RADIUS Accounting Support	Not supported on 1xxE-Series
Centralized Configuration	D-series, E-series

FortiLink Features	FortiSwitch Models
Access VLAN	D-series, E-series
STP BDPU Guard, Root Guard, Edge Port	D-series, E-series
Loop Guard	D-series, E-serie
Switch admin Password	D-series, E-series
Storm Control	D-series, E-series
802.1x-Authenticated Dynamic VLAN Assignment	D-series, E-series
Host Quarantine on Switch Port	D-series, E-series
QoS	Not supported on 1xxE-Series or 112D-POE
Centralized Firmware Management	D-series, E-series
Automatic network detection and configuration	D-series, E-series
Dynamic VLAN assignment by group name	D-series, E-series
Sticky MAC addresses	D-series, E-series
NetFlow and IPFIX flow tracking and export	D-series, E-series
FortiSwitch split ports	524D, 524D-FPOE, 548D, 548D-FPOE, 1048E, 3032D
Encapsulated remote switched port analyzer (ERSPAN)	2xx and higher
MSTP instances **NOTE:** In FortiLink mode, the FortiGate unit supports 1-14 instances for all platforms.	D-series, E-series
QoS statistics	D-series, E-series
Configuring SNMP through FortiLink	D-series, E-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, and FS-2xxE

Upgrade information

FortiSwitch 6.4.0 supports upgrading from FortiSwitch 3.5.0 and later.

To upgrade, refer to the FortiOS upgrade path at https://support.fortinet.com/Download/FirmwareImages.aspx.

Cooperative Security Fabric upgrade

FortiOS 5.4.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1
- FortiClient EMS 1.0.1
- FortiAP 5.4.1
- FortiSwitch 3.4.2

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Framework - Upgrade Guide*
- *FortiOS 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*
  This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

Product integration and support

FortiSwitch 6.4.0 support

The following table lists 6.4.0 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 6.4.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
517663	When a managed FortiSwitch unit is running the latest GA image and is offline, *Upgrade Available* is still shown on the *WiFi & Switch Controller* > *Managed FortiSwitch* page.
557280	The Physical Topology page and Users & Devices page need tot show FortiSwitch port information.
581370	The `execute switch-controller trigger-config-sync` command is not updating the RADIUS settings from the managed FortiSwitch unit when the RADIUS server has been changed.
586299	When adding a new device to an HA cluster, switch controller QoS settings should not cause HA synchronization to fail.
592111	After managed FortiSwitch units were upgraded to 6.2.2, they cannot be managed from the FortiGate unit.
595671	The output of the `config system gre-tunnel`command is missing the `set key-outbound` and `set key-inbound` parameters.
601547	The user group configured on a FortiGate unit is not pushed to the managed FortiSwitch unit, and the user group configuration is deleted.
607707	Configuration changes from the FortiGate unit are not pushed to the managed FortiSwitch unit.
608231	The LLDP policy did not download completely to the managed FortiSwitch 108E models.
613323	After a FortiGate HA failover, the managed FortiSwitch trunk configuration is not being pushed.

Known issues

The following known issues have been identified with 6.4.0. 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.
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.
607753	CAPWAP is not updated to be a Fabric connection after upgrading from 6.4.0 Beta1 build 1519 to build 1538.
620303	The `mgmt-vlanid` setting can only be changed when FortiLink is disabled. You must use the CLI to change this setting.
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`.
622812	VLANs on a FortiLink interface configured to use a hardware switch interface may fail to come up after upgrading or rebooting.
623550	Before FortiOS 6.4.0, the default VLAN name was `vsw.<fortilink interface name>`. Starting in FortiOS 6.4.0, the default VLAN name is `default`. After upgrading FortiOS from 6.2.3 to 6.4.0, FortiOS still uses `vsw.fortilink` as the default VLAN , resulting in a “Potential conflict of vlanid(1) with initial-config.template(default) and interface(vsw.fortilink) ... please verify” warning. **Workaround:** 1. Disable FortiLink. 2. Remove all switches. 3. Delete all VLAN interfaces (such as `vsw.*`, `qtn.*`, and `snf.*`).
628121	There are FortiLink config sync errors when running FortiOS 6.4.0 and FortiSwitch 6.2.x. Users can ignore these errors.