FortiSwitch Devices Managed by FortiOS Release Notes

Version 6.2.2

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

November 8, 2019

11-622-571508-20191108

TABLE OF CONTENTS

Change log

Date	Change Description
October 9, 2019	Initial document release
November 5, 2019	Added bug 592111.
November 6, 2019	Updated the “Support of FortiLink features” table.
November 8, 2019	Added more details to bug 592111.

Introduction

This document provides the following information for FortiSwitch 6.2.2 devices managed by FortiOS 6.2.2 build 1010.

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 80D, 91E, 92D, FortiGate-VM01	8
FortiGate-60E, 60E-POE, 61E, 80E, 80E-POE, 81E, 81E-POE, 90E	16
FortiGate-100D, 140D, 140D-POE, FortiGate-VM02	24
FortiGate 100E, 100EF, 101E, 140E, 140EP, 200E, 201E	32
FortiGate-300 to 5*xx*	48
FortiGate-600 to 900 and FortiGate-VM04	64
FortiGate-1000 and up	128
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 6.2.2

NOTE: Some new features in FortiOS 6.2.2 depend on FortiSwitch 6.2.2; these features will not work until FortiSwitch 6.2.2 is released.

The following list contains new managed FortiSwitch features added in FortiOS 6.2.2.

- FortiSwitch redundancy is now available for FortiGate models that do not support the FortiLink aggregate interface.
- You can now configure IGMP flood reports and traffic on automatically configured interfaces.
- Power over Ethernet (PoE) type-length-value structures (TLVs) are now available for FortiSwitch LLDP profiles.
- A new CLI command allows you to change which VLANs the `set allowed-vlans-all` command affects.
- Remote SPAN (RSPAN) is now supported.
- You can now enable FortiLink VLAN optimization on FortiGate units.
- You can now create a FortiLink aggregate interface without adding physical member ports.
- You can now reset and restore port statistics counters on a managed FortiSwitch unit.
- FortiLink custom TLVs in the LLDP profile are now disabled with the `set auto-isl disable` command.
- When a device using DHCP is quarantined, you can now automatically toggle (bounce) the link of the switch port where the quarantined device was last seen.
- You can now use the aggregate interface as the FortiLink interface on all platforms: FGR-30D, FGR-35D, FGT-30E, FGT-30E-MI, FGT-30E-MN, FGT-50E, FGT-51E, FGT-52E, FGT-60E, FGT-60E-POE, FGT-61E, FGT-80D, FG-80E, FGT-80E-POE, FGT-81E, FGT-81E-POE, FG-90E, FGT-91E, FGT-92D, FWF-30E, FWF-30E-MI, FWF-30E-MN, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, and FWF-61E.

What's new in FortiOS 6.2.1

The following list contains new managed FortiSwitch features added in FortiOS 6.2.1.

- Instead of exporting FortiSwitch logs to a FortiGate unit, you can send FortiSwitch logs to one or two remote Syslog servers.
- You can now configure SNMP on FortiSwitch units.
- You can now use quarantines with 802.1x MAC-based authentication.
- You can now control when inactive MAC addresses are removed from the FortiSwitch hardware even when the mac-aging-interval is disabled.
- You can create Syslog entries when MAC addresses are learned, aged out, or removed.

What's new in FortiOS 6.2.0

The following list contains new managed FortiSwitch features added in FortiOS 6.2.0:

- You can now have FortiGate units in HA mode that are managing FortiSwitch units in an MCLAG with LACP.
- You can now make the following global system configuration changes in FortiLink mode (asterisks indicate the default values):

```
config system global
   set admin-concurrent {enable* | disable}
```

```
    set admin-https-pki-required {enable | disable*}
    set admin-sport <443*>
    set admin-https-ssl-versions {tlsv1-0 | tlsv1-1* | tlsv1-2*}
end
```

WARNING: Before changing these settings, ensure that the configuration is valid for your system for proper operation.

- There are new commands that let you use automatic network detection and configuration.
- FortiSwitch units in FortiLink mode now support dynamic VLAN assignment by group name.
- FortiLink interfaces are now configured on the new *WiFi & Switch Controller > FortiLink Interface page*.
- You can now combine the configuration of multiple standalone FortiSwitch units into a single FortiGate-compatible configuration.
- You can make dynamically learned MAC addresses persistent (sticky) when the status of a managed FortiSwitch port changes (goes down or up).
- You can sample IP packets on managed FortiSwitch units and then export the data in NetFlow format or Internet Protocol Flow Information Export (IPFIX) format. You can choose to sample on a single ingress or egress port, on all FortiSwitch units, or on all FortiSwitch ingress ports.
- FortiSwitch split ports are now supported.
- You can now use encapsulated remote switched port analyzer (ERSPAN) for port mirroring.
- You can now use a traffic policy to control quarantined devices.
- Multiple Spanning Tree Protocol (MSTP) is now supported.
- The following features are now supported on FortiSwitch ports shared between VDOMs:
  - POE pre-standard detection (on a per-port basis if the FortiSwitch model supports this feature)
  - Learning limit for dynamic MAC addresses on ports, trunks, and VLANs (if the FortiSwitch unit supports this feature)
  - QoS egress CoS queue policy (if the FortiSwitch unit supports this feature)
  - Port security policy
- You can now use the GUI to configure a MCLAG.
- The number of FortiSwitch units supported by certain FortiGate models has been increased.
- You can change the ping setting to use the FortiSwitch serial number instead of the FortiSwitch IP address when checking that the FortiSwitch unit is accessible from the FortiGate unit.
- You can configure different access to the FortiSwitch management interface and the FortiSwitch internal interface.
  NOTE: After you upgrade to FortiOS 6.2, the allowaccess settings for the FortiSwitch mgmt and internal interfaces are overridden by the default local-access security policy.
- By default, two trunks are created in HA mode when there are managed FortiSwitch units. One trunk is created between the active FortiGate unit and FortiSwitch unit; another trunk is created between the backup FortiGate unit and FortiSwitch unit.
- You can use the `diagnose switch-controller switch-info qos-stats <FortiSwitch_serial_number> <port_name>` command to get QoS statistics on the specified port of a managed FortiSwitch unit.

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-series
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, 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

Upgrade information

FortiSwitch 6.2.2 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 6.2.2 support

The following table lists 6.2.2 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 6.2.2. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
554298	When a FortiGate unit has the strong-crypto setting enabled and the ssh-kex-sha1 setting disabled, the managed FortiSwitch unit cannot be accessed.
562870	Enabling the network monitor might cause random stalling to the CPU packet receiving queue.
563939	Setting the reauth-period to 0 in the CLI causes the command to fail.
567984	When a managed FortiSwitch unit is restarted, the LLDP profile configuration for the ports changes from “default” to “default-auto-isl” briefly.
570375	Some packets might loop back momentarily in an MCLAG setup, at the time when the MCLAG trunk was added.

Known issues

The following known issues have been identified with 6.2.2. 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.
578629	When a second ICL is added to an existing ICL for a second-tier MCLAG, the port is added to existing FortiLink trunk instead of the ICL. **Workaround:** Enter the `set fortilink-neighbor-detect lldp` command on the FortiGate FortiLink interface.
586801	NetBIOS stops working when proxy ARP is configured and the access VLAN is enabled because FortiGate units do not support NetBIOS proxy.

592111	FortiSwitchOS 6.2.2 GA might cause a buffer leak in the FortiLink CAPWAP daemon when interoperating with FortiOS release 6.2.1 or lower in FortiLink mode. This buffer leak might lead to the CAPWAP tunnel being disconnected between a FortiSwitch unit and a FortiGate unit. This issue is specific to LLDP neighbor change notifications from a FortiSwitch unit to a FortiGate unit and might not happen frequently.
	
	Workarounds for FortiOS 6.2.0 and later:
	- Upgrade to FortiOS 6.2.2 GA.
	- If you cannot upgrade your FortiGate unit, use FortiSwitchOS 6.2.1 GA or earlier.
	
	Workarounds for FortiOS 6.0.x and earlier:
	Disable the LLDP transmission on the FortiLink interface on the FortiGate unit using the following CLI commands:
	
	`config system interface`
	`edit <FortiLink_interface>`
	`set lldp-transmission disable`
	`next`
	`end`