FortiSwitch Devices Managed by FortiOS Release Notes

Version 6.2.0

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

May 7, 2019

11-620-541330-20190507

TABLE OF CONTENTS

Change log

Date	Change Description
March 28, 2019	Initial release
April 5, 2019	Updated the “What’s new in FortiOS 6.2.0” section. Removed bug 357360 and added bugs 545395, 545629, and 547163.
April 16, 2019	Updated the “Support of FortiLink features” table.
April 24, 2019	Added bug 553284.
May 7, 2019	Updated the “Support of FortiLink features” table.

Introduction

This document provides the following information for FortiSwitch 6.2.0 devices managed by FortiOS 6.2.0 build 0866.

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

The following table shows the FortiSwitch models that support FortiLink mode.

FortiGate and FortiWifi Models 3x, 5x, 6x, 7x, 8x, 9x, 1xx, 2xx, 3xx, 4xx, 5xx, 6xx, 8xx, 9xx, 1xxx, 2xxx, 3xxx	FortiSwitch Models D and E Series
FortiOS 5.6 GA and later	For FortiSwitch D-series models, FortiSwitchOS 3.6.4 GA or later is required for all managed switches. For FortiSwitch E-series models, FortiSwitchOS 6.0.0 GA or later is required for all managed switches.

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

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	Not supported on 1xxE-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

Upgrade information

FortiSwitch 6.2.0 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 6.2.0 support

The following table lists 6.2.0 product integration and support information.

Web browser	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.
FortiOS (FortiLink Support)	FortiLink is supported on all FortiSwitch models when running FortiOS 5.4.0 and later and FortiSwitchOS 3.2.1 and later.

Resolved issues

The following issues have been fixed in 6.2.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
403313	LACP active cannot be enabled on an MCLAG in FortiLink mode.
424432	The IGMP reports received on the tier-1 FortiSwitch units in FortiLink mode (with MCLAG enabled) are not synchronized.
489064	The output of the `get switch modules summary` command shows LOS in the RX column for SFP ports.
494714	After disconnecting one of the ports used to form an MCLAG between two FortiSwitch units, the ICL/ISL is not removed after 10 minutes.
503110	A FortiSwitch 1048E restarts continuously when managed by a FortiGate unit.
511671	When a 448D switch in FortiLink mode stopped responding, the crash log showed “signal 11 (Segmentation fault) received.”
525257	You cannot configure the TLS version and related SSL parameters in FortiLink mode.
529688	After a FortiSwitch unit is restarted, the FortiGate unit sends traffic out of the wrong port.
530605	When the FortiSwitch unit is discovered on a FortiLink interface, there should be default fcam and fvoi VLANs available.
535736	If a FortiSwitch firmware image is an even multiple of 1024 bytes, it will not upgrade properly using the default FortiLink upgrade mechanism.
541871	Some users are unable to use SSH with a public key to connect to a managed FortiSwitch unit.

Known issues

The following known issues have been identified with 6.2.0. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description

545395	Bulk-image staging might fail for some FortiSwitch units.
	
	CAPWAP is the default mode for image staging. In large deployments, scaling-related issues might be encountered when using CAPWAP for bulk staging. Some FortiSwitch units might fail to stage the image properly due to the extra load on the setup during the process.
	
	Fortinet recommends using HTTP mode instead of the bulk-staging transaction when the CAPWAP mode presents issues. With the FOS 6.0.x and 6.2.0 releases, use the following commands to change to HTTP mode:
	
	`config switch global`
	`  set https-image-push enable`
	`next`

545629	Under http-push mode, the staging upgrade for 1048E and 3032E never ends . FOS version: 6.2.0 only Impacted switches: 1048E and 3032E If the http-image push mode is used for a stage upgrade, the firmware installation could complete successfully on the 1048E or 3032E switch. However, the status in the FortiGate unit (from the `exec switch-controller get-upgrade-status` command) shows the upgrade has not finished. **Workaround:** The issue can be resolved by killing the child process of flcfgd on FortiGate. 1. On the FortiGate unit, execute "fnsysctl ps" and list all /bin/flcfgd processes with PID's 2. Keep the parent process of flcfgd, that is, the one with the smallest PID. The rest of flcfgd processes are child processes. 3. Execute the "fnsysctl kill -9 <child process id of flcfgd>" command. 4. (Optional) Access the switch and verify the next-boot image version by running the `diagnose sys flash list` command.

Bug ID	Description
547163	The FortiGate unit cannot push the configuration to a managed FortiSwitch unit. FOS versions: 6.0.x and 6.2.0 The FortiGate unit cannot push the configuration or fails in pushing the new image to the managed FortiSwitch unit. Execute the `execute switch-controller get-sync-status all`"command. If you see "pending" under config and upgrade, use the following procedure to resolve the issue. 1. On the FortiGate unit, execute "fnsysctl ps" and find the "/bin/flcfgd" processes. If only one process is found, then it is not the problem. 2. Kill the child process of flcfgd, that is, the larger number of the flcfgd process ID with the "fnsysctl kill -9 <child process ID of flcfgd>" command. 3. (Optional) Re-push the image to the previous pending switch if the new image installation is needed. 4. (Optional) Access the switch and verify the next-boot image version with the `diagnose sys flash list` command.
553284	For the 1048E model, the 6x40G phy-mode configuration does not work in FortiLink mode.