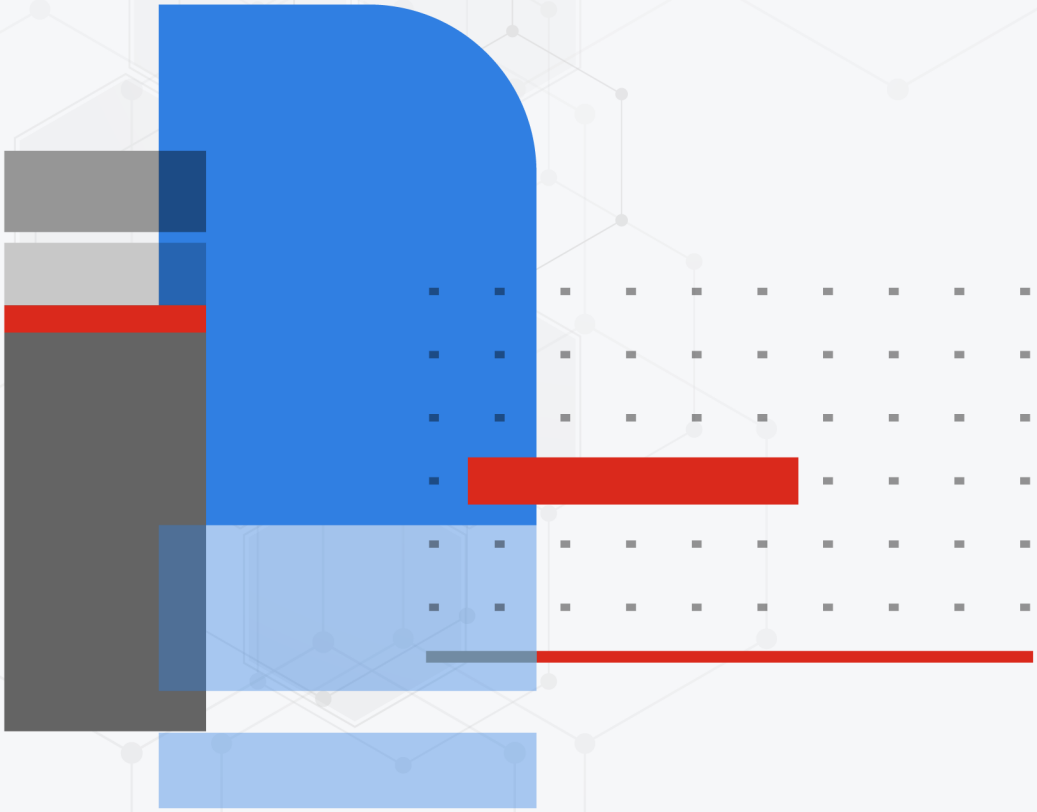
FortiLink Release Notes (FortiOS 7.4.4)

FortiSwitchOS 7.4.3



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/training-certification

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

October 23, 2024
FortiSwitchOS 7.4.3 FortiLink Release Notes (FortiOS 7.4.4)
11-744-980431-20241023

TABLE OF CONTENTS

Change log

Date	Change Description
May 15, 2024	Initial document release for FortiOS 7.4.4
June 6, 2024	Updated What's new in FortiOS 7.4.4 on page 5.
September 26, 2024	Added a note in Upgrade information on page 8.
October 23, 2024	Added bug 1044150.

What's new in FortiOS 7.4.4

The following list contains new managed FortiSwitch features added in FortiOS 7.4.4:

- Two more port speed options are available for managed switches: `40000auto` (autonegotiation of the 40G-CR4 interface of FS-1048E) and `2500full` (25 Gbps full-duplex.). You can select these speeds under the `config switch-controller managed-switch` command.
- The LACP fallback mode is now supported on managed switches. LACP fallback mode allows a selected port to stay up so that a device not running LACP can still connect to the network.
- You can now monitor ARP packets for a specific VLAN on a DHCP-snooping trusted port of a managed FortiSwitch unit and save the VLAN ID, MAC addresses, and IP addresses in the DHCP-snooping database.
- You can now specify a tagged VLAN for users to be assigned to when the authentication server is unavailable. Previously, you could only specify an untagged VLAN. This feature is available with 802.1x MAC-based authentication. It is compatible with both Extensible Authentication Protocol (EAP) and MAC authentication bypass (MAB).
- You can now use RADIUS attributes to configure dynamic access control lists (DACLs) on the 802.1x ports of managed switches. DACLs are configured on a switch or saved on a RADIUS server. You can use DACLs to control traffic per user session or per port for switch ports directly connected to user clients. DACLs apply to hardware only when 802.1x authentication is successful.
- The following switch-controller events can now be used as triggers for zero-touch provisioning:
  - Log ID 32618—A switch port was exported to or returned from a virtual switch.
  - Log ID 32619—A switch was added to or removed from a virtual port pool.
  - Log ID 32620—A switch was added to a switch group.
  - Log ID 32621—A switch was removed from a switch group.
  - Log ID 32622—A switch was connected using FortiLink mode over a layer-2 or layer-3 network.
  - Log ID 32623—The location of a switch changed.
  - Log ID 32624—A new switch peer was detected (either a peer to a single switch or an MCLAG).
- The FS-6xxF models now support the same LAN-segment functionality as the 200 Series and 500 Series.
- FortiSwitch NAC policies have been enhanced:
  - NAC policies now support FortiVoice and FortiFones. The NAC policy will match a dynamic MAC address group of all FortiFones registered with a FortiVoice unit.
  - You can now control how long matched devices are kept for NAC policies. In previous releases, matched devices were deleted when a connection-ID table entry was deleted, the port link status went down, the device was inactive, or the switch was offline.
- You can now control how long matched devices are kept for dynamic port policies (DPPs). In previous releases, matched devices were deleted when the connection-ID table entry was deleted, the port link status went down, the device was inactive, or the switch was offline. In addition, devices matched by DPPs are now matched according to the priority, instead of using First Come, First Serve (FCFS) matching.

Introduction

This document provides the following information for FortiSwitch 7.4.3 devices managed by FortiOS 7.4.4 build 2662:

See the Fortinet Document Library for FortiSwitchOS documentation.

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

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, FortiGate-VM01	8
FortiGate 6xE, 8xE, 90E, 91E	16
FGR-60F, FG-60F, FGR-60F-3G4G, FG-61F, FGR-70F, FGR-70F-3G4G, FG-80F, FG-80FB, FG-80FP, FG-81F, and FG-81FP	24
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 26xxF	196
FortiGate-3xxx 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.

Special notices

Support of FortiLink features

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

Upgrade information

Check the FortiSwitchOS Release Notes before upgrading the FortiSwitch firmware from the FortiGate Switch Controller.

FortiSwitchOS 7.4.3 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 7.4.3 support

The following table lists FortiSwitchOS 7.4.3 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 FortiOS 7.4.4. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
899414	The *connected via* field on the *Diagnostics and Tools* slide and the *WiFi & Switch Controller* > *FortiSwitch Clients* page incorrectly show the status of the LACP interface as “down.” .This is cosmetic and does not affect the operation of the LACP interface. The correct status of the LACP interface can be checked on the *FortiSwitch Ports* page or by using the command line.
911232	The security rating shows an incorrect warning for unregistered FortiSwitch units on the *WiFi & Switch Controller* > *Managed FortiSwitches* page.
925554	The FG-60F GUI incorrectly shows the VLAN interfaces of hardware switches and software switches as down.
965482, 968134	The FortiGate 200F models have a lower performance when managing FS-6xxF switches in head-of-the-line (HOL) mode.
977740	When there are switch interfaces, the VDOM should not change to transparent mode.
982651	By default, the re-authentication timeout for 802.1X authentication is 1 hour; this value cannot be changed from the FortiGate device.
984404	After upgrading the FortiGate to FortiOS 7.4.2, the managed FortiSwitch unit is shown as “not registered” in the GUI.
988335	If the network has more than 20 MAC addresses in a network access control (NAC) environment, the Control and Provisioning of Wireless Access Points (CAPWAP) protocol might go down.
1000663	The configurations of managed-switch ports are being removed after the switch is restarted. This issue only affects user-created trunks.

Known issues

The following known issues have been identified with FortiOS 7.4.4. 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. 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`.
789914	• When LAN segments are enabled on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models, the internal VLAN (`set lan-internal-vlan`) is assigned automatically by default. If the same VLAN is configured on the FortiGate device, the configuration fails when it is pushed to the FortiSwitch unit without any warning message. **WORKAROUND:** Use a custom command. • All sub-VLANs must belong to the same MSTP instance if the FortiLink configuration includes the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models.
813216	After CAPWAP offload is enabled or disabled, FortiLink goes down.
814674	When upgrading a FortiAP or FortiSwitch unit that is connected to a downstream FortiGate device, a “Failed to retrieve upgrade progress” message appears.

Bug ID	Description
910962	After setting values for `src-mac`, `dst-mac`, and `vlan` for the ACL classifier, you cannot use the `unset` command to remove these settings. **WORKAROUND:** 1. Remove `set acl-group <ACL_group_name>` from under the `config switch-controller managed-switch` command. 2. Delete the ACL group. 3. Delete the ACL. 4. Reconfigure the ACL.
940248	When both network device detection (`config switch network-monitor settings`) and the switch controller routing offload are enabled, the FS-1048E switch generates duplicate packets.
1044150	When the `tunnel-mode` is set to `strict` or `moderate` (under the `config switch-controller system` command), the FortiOS configuration might not be pushed to managed FortiSwitch units.

www.fortinet.com