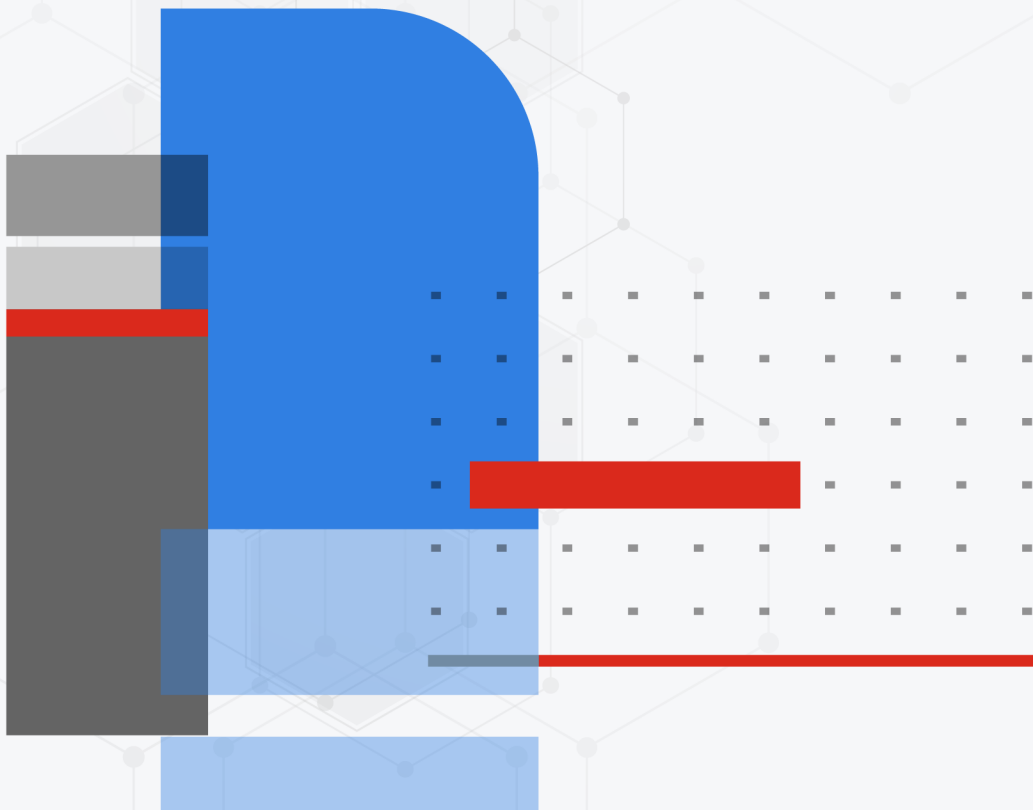




FortiLink Release Notes (FortiOS 7.4.6)

FortiSwitchOS 7.4.5



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



December 12, 2024

FortiSwitchOS 7.4.5 FortiLink Release Notes (FortiOS 7.4.6)

11-746-1104740-20241212

TABLE OF CONTENTS

Change log	4
What's new in FortiOS 7.4.6	5
Introduction	6
Special notices	8
Support of FortiLink features	8
Upgrade information	9
Product integration and support	10
FortiSwitchOS 7.4.5 support	10
Resolved issues	11
Known issues	12

Change log

Date	Change Description
December 12, 2024	Initial document release for FortiOS 7.4.6

What's new in FortiOS 7.4.6

The following list contains new managed FortiSwitch features added in FortiOS 7.4.6:

- The password security for managed switches has been improved. Empty passwords for the FortiSwitch admin account are no longer allowed. If a switch has no admin password set when it is authorized, the FortiGate device will generate an admin password for the FortiSwitch unit. FortiSwitch units that already have an admin password configured will remain unaffected.

To log in to the FortiSwitch CLI or GUI, you can configure the switch profile (under the `config switch-controller switch-profile` command) with an admin password on the FortiGate device, which is the Fortinet-recommended FortiLink setup.

A new command has been introduced to retain the password of the managed switch during deauthorization or to reset the managed switch to factory default settings during deauthorization. This command helps to clear the previously FortiGate-set random password on the managed switch when it is deauthorized.

Introduction

This document provides the following information for FortiSwitch 7.4.5 devices managed by FortiOS 7.4.6 build 2726:

- [Special notices on page 8](#)
- [Upgrade information on page 9](#)
- [Product integration and support on page 10](#)
- [Resolved issues on page 11](#)
- [Known issues on page 12](#)

See the [Fortinet Document Library](#) for FortiSwitchOS documentation.

Refer to the [FortiLink Compatibility table](#) to find which FortiSwitchOS versions support which FortiOS versions.



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, FG-81FP, FG-90G, FG-91G	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 7.4.5 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 7.4.5 support

The following table lists FortiSwitchOS 7.4.5 product integration and support information.

Web browser	<ul style="list-style-type: none">• Microsoft Edge 112• Mozilla Firefox version 113• Google Chrome version 113 <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 7.4.6. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
1077496	The flpold and flcfdg processes cause high CPU usage.

Known issues

The following known issues have been identified with FortiOS 7.4.6. 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.
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	<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.
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> .
789914	<ul style="list-style-type: none"> 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 (<code>set lan-internal-vlan</code>) 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.

Bug ID	Description
910962	<p>After setting values for <code>src-mac</code>, <code>dst-mac</code>, and <code>vlan</code> for the ACL classifier, you cannot use the <code>unset</code> command to remove these settings.</p> <p>WORKAROUND:</p> <ol style="list-style-type: none">1. Remove <code>set acl-group <ACL_group_name></code> from under the <code>config switch-controller managed-switch</code> command.2. Delete the ACL group.3. Delete the ACL.4. Reconfigure the ACL.
940248	<p>When both network device detection (<code>config switch network-monitor settings</code>) and the switch controller routing offload are enabled, the FS-1048E switch generates duplicate packets.</p>
1044150	<p>When the <code>tunnel-mode</code> is set to <code>strict</code> or <code>moderate</code> (under the <code>config switch-controller system</code> command), the FortiOS configuration might not be pushed to managed FortiSwitch units.</p>



www.fortinet.com

Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.