



FortiLink Release Notes (FortiOS 7.6.3)

FortiSwitchOS 7.6.2



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



July 31, 2025

FortiSwitchOS 7.6.2 FortiLink Release Notes (FortiOS 7.6.3)

11-763-1108980-20250731

TABLE OF CONTENTS

Change log	4
What's new in FortiOS 7.6.3	5
Introduction	6
Special notices	7
Support of FortiLink features	7
Upgrade information	8
Product integration and support	9
FortiSwitchOS 7.6.2 support	9
Resolved issues	10
Known issues	11

Change log

Date	Change Description
April 16, 2025	Initial document release for FortiOS 7.6.3
April 23, 2025	Added bug 1137075.
July 15, 2025	Added bug 1174647.
July 16, 2025	Revised the description of bug 1174647.
July 31, 2025	Added bug 1142958.

What's new in FortiOS 7.6.3

The following list contains new managed FortiSwitchOS features added in FortiOS 7.6.3:

- You can now use CLI commands to check the system status and the fan status.
- When you create a device NAC policy in the FortiOS GUI, FortiOS now suggests values when you select the hardware vendor, device family, type, operating system, or host to match. For example, if you want the NAC policy to match a device family, FortiOS suggests *FortiSwitch*, *FortiGate*, *FortiAP*, *FortiFone*, *FortiCam*, *FortiRecorder*, *FortiManager*, *FortiAnalyzer*, *Mac*, *iPhone*, *Galaxy*, *Virtual Machine*, and *Printer*. These suggestions make it easier and quicker to create a device NAC policy.
- You can now use the CLI to prevent the switch controller from automatically creating VLANs.
- You can now use FortiLink to manage FortiSwitch units using IPv6 addresses. Previously, only IPv4 addresses were supported.
- You can now specify the source IP address in a FortiSwitch unit for the following:
 - Layer-3 FortiLink with CAPWAP tunnel mode (in-band management and out-of-band management) (IPv4 and IPv6)
 - Layer-3 FortiLink with HTTPS tunnel mode (in-band management and out-of-band management) (IPv4)
 - FortiCloud management (IPv4)

This feature requires FortiSwitchOS 7.4.7, 7.6.2, or later but supports all versions of FortiOS.

Introduction

This document provides the following information for FortiSwitch 7.6.2 devices managed by FortiOS 7.6.3 build 3510:

- [Special notices on page 7](#)
- [Upgrade information on page 8](#)
- [Product integration and support on page 9](#)
- [Resolved issues on page 10](#)
- [Known issues on page 11](#)

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
FGR-60F, FG-60F, FGR-60F-3G4G, FG-61F, FG-70F, FG-71F, FG-80F, FG-80FB, FG-80FP, FG-81F, FG-81FP, FG-90G, FG-91G, FortiGate-VM02	24
FortiGate 100F, 101F	32
FG-120G, FG-121G	48
FortiGate 200E, 201E, 200F, 201F, 800D, 900D, FortiGate-VM04	64
FortiGate 300E to 500E	72
FortiGate 600E to 900E, 400F, 401F, 601F	96
FortiGate 1000D, 600F	128
FortiGate 900G, 901G, 1000F, 1001F, 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 7.6.2 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 7.6.2 support

The following table lists FortiSwitchOS 7.6.2 product integration and support information.

Web browser	<ul style="list-style-type: none">• Microsoft Edge 112• Mozilla Firefox version 113• Google Chrome version 113 Other web browsers might 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 7.6.3. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Bug ID	Description
1015992	The <i>Lockdown ISL</i> setting cannot be disabled in FortiLink mode.
1016034	After HA failover, the <i>Lockdown ISL</i> setting is enabled automatically.
1043815	Upgrading the firmware for a large number (more than 100) of FortiSwitch units at the same time might cause performance issues with the GUI and some devices might not upgrade.
1108965	After deleting the <code>dhcp-snooping-static-client</code> entry and then shutting down or bringing up a port, there is a configuration synchronization error when making any configuration changes.
1130242	The FortiGate device is pushing a partial SNMP community configuration to the managed FortiSwitch unit, instead of the full configuration.
1113465	On a random basis, VLANs fail to be assigned on FortiSwitch ports when devices matching a dynamic port policy (DPP) come online; this is caused by a race condition during the FortiSwitch initialization.
1138333	The FortiLink configuration daemon needs to use memory more efficiently.
1142958	Any FortiSwitch unit in FortiLink HTTPS mode with “static-isl” enabled in the ISL trunks is displayed as directly connected to the FortiGate device, even when it is not directly connected.

Known issues

The following known issues have been identified with FortiOS 7.6.3. 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	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. 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.
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.
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	<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>
961142	<p>An interface in FortiLink flaps when using an MLAG with DAC on the OPSFPP-T-05-PEB transceiver.</p>
1113304	<p>After the FortiGate device is upgraded from FortiOS 7.6.0 to 7.6.1 or higher when the LLDP configuration is set to <code>vdom</code> or disabled under the FortiLink interface, the FortiSwitch units are offline.</p> <p>WORKAROUND:</p> <p>Enable the <code>lldp-reception</code> and <code>lldp-transmission</code> LLDP configurations under the FortiLink interface or rebuild the FortiLink interface.</p> <p>For example:</p> <pre>config system global set lldp-reception enable set lldp-transmission enable end</pre>
1137075	<p>In the <i>WiFi & Switch Controller > Managed FortiSwitches</i> page, the Topology view shows the link between FortiSwitch units with a dotted line instead of a solid line.</p> <p>Workaround: To see if FortiLink is up or down, use the <code>execute switch-controller get-conn-status</code> command or use the List view in the <i>WiFi & Switch Controller > Managed FortiSwitches</i> page.</p>
1138430	<p>The <code>switch-id</code> for managed switches cannot be longer than 16 characters.</p>
1174647	<p>This issue affects a FortiGate device running any version of FortiOS and managing one or more FortiSwitch units that are running FortiSwitchOS 7.4.7 (or later) or 7.6.2 (or later). When the total number of trunk members exceeds five on any managed switch, the Topology view displays incorrectly on the FortiGate device; however the data traffic is not affected.</p> <p>Workarounds:</p> <ul style="list-style-type: none"> • Downgrade FortiSwitchOS to 7.6.1 or 7.4.6. • Reduce the total number of trunk member ports to five or fewer on the affected switch. • Change the FortiLink management mode to HTTPS on the affected switch. <p>If you are changing the FortiLink management mode to HTTPS:</p> <ol style="list-style-type: none"> a. If the switch is a core switch and <code>fortilink-neighbor-detect</code> is set to <code>lldp</code>, change the <code>fortilink-neighbor-detect</code> mode to <code>fortilink</code>. Before doing so, verify that the FortiLink trunk on the switch does not have the <code>set static-isl enable</code> setting. b. After changing the <code>fortilink-neighbor-detect</code> mode to <code>fortilink</code> on the FortiGate device, ensure that the name of the FortiLink trunk on the switch does not include the <code>-0</code>

Bug ID	Description
	<p>suffix.</p> <p>c. Enable <code>set isl-static enable</code> in that FortiLink trunk.</p>



www.fortinet.com

Copyright© yyyy 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.