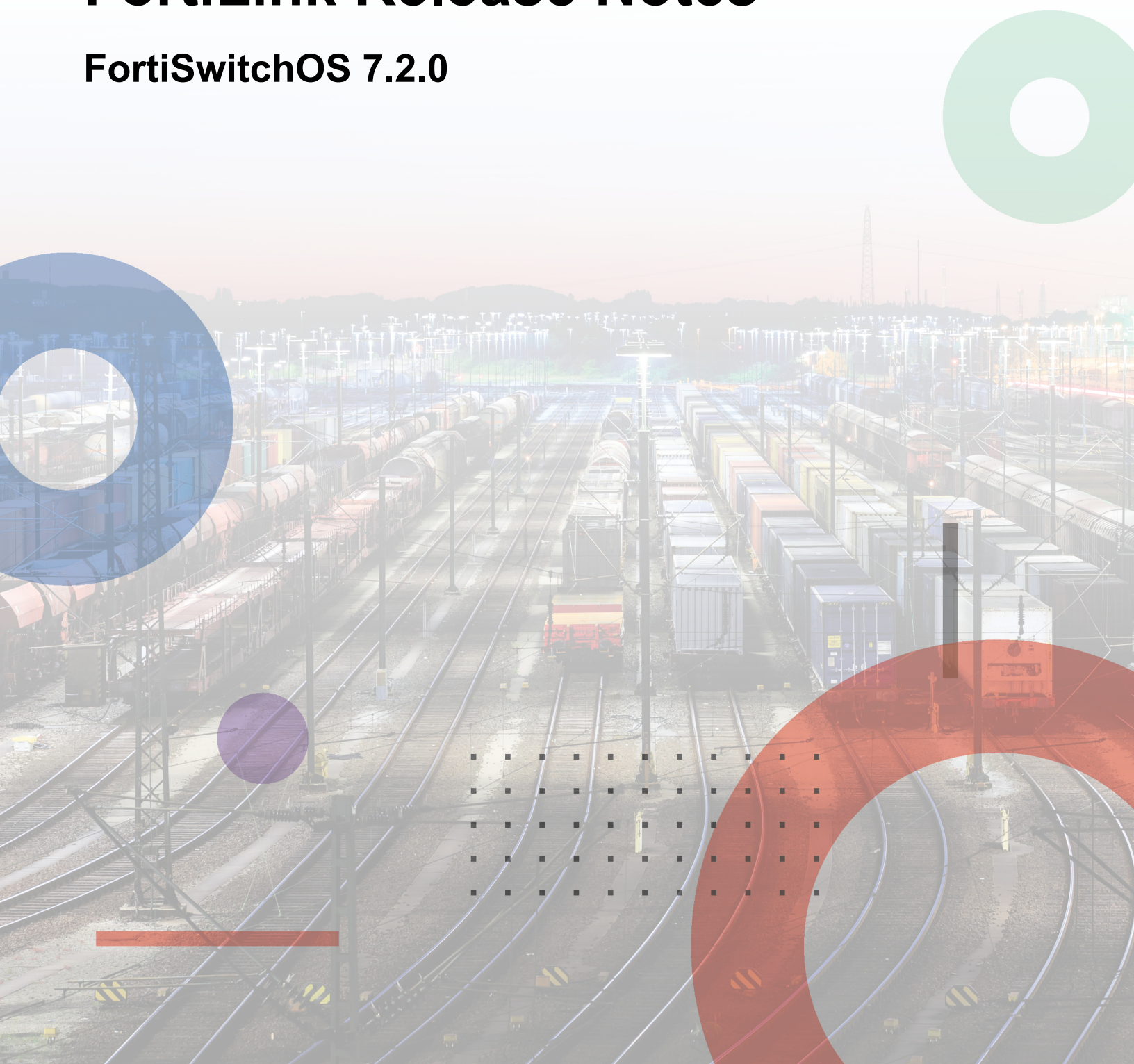
FortiLink Release Notes

FortiSwitchOS 7.2.0



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

September 30, 2022
FortiSwitchOS 7.2.0 FortiLink Release Notes
11-720-774520-20220930

TABLE OF CONTENTS

Change log

Date	Change Description
March 31, 2022	Initial document release for FortiOS 7.2.0
April 12, 2022	Updated the “NAC policies not maintained or converted when upgrading to 7.0.0” section (which is now “NAC policies not maintained or converted when upgrading from 6.4 to 7.2”).
April 25, 2022	Added bug 802786 as a known issue.
April 28, 2022	Added bug 781600 as a known issue.
June 17, 2022	Changed the title.
July 19, 2022	Added the following to the “What’s new in FortiOS 7.2.0” section: “Setting the `switch-mgmt-mode` is no longer needed, so the `set switch-mgmt-mode` command has been removed from `config system global`.”
September 30, 2022	Added another new feature to the “What’s new in FortiOS 7.2.0” section.

Introduction

This document provides the following information for FortiSwitchOS 7.2.0 devices managed by FortiOS 7.2.0 build 1157:

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, 91E, FortiGate-VM01	8
FortiGate 6xE, 8xE, 90E	16
FGR-60F, FG-60F, FGR-60F-3G4G, FG-61F, 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 25xxE	196

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

What's new in FortiOS 7.2.0

The following list contains new managed FortiSwitch features added in FortiOS 7.2.0:

- Zero-touch management is now more efficient. When a new FortiSwitch unit is started, by default, it will connect to the available manager, which can be a FortiGate device, FortiLAN Cloud, or FortiSwitch Manager. Only one manager can be used at a time. The FortiSwitch configuration does not need to be backed up before the FortiSwitch unit is managed, and the FortiSwitch unit does not need to be restarted when it becomes managed. All ports are enabled for auto discovery. The "internal" interface is the DHCP client in all FortiSwitch models.

  Setting the `switch-mgmt-mode` is no longer needed, so the `set switch-mgmt-mode` command has been removed from `config system global`.
- You can now use Virtual Extensible LAN (VXLAN) interfaces to create a layer-2 overlay network. After a VXLAN tunnel is set up between a FortiGate device and a FortiSwitch unit, the FortiGate device can use the VXLAN interface to manage the FortiSwitch unit.
- NAC LAN segments are now supported on the following FortiSwitch models in FortiLink mode: FSR-112D-POE, 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, and FS-148E-POE.
- The new `execute switch-controller switch-action 802-1X clear-auth-mac <FortiSwitch_serial_number> <MAC_address>` command allows you to clear the 802.1X-authorized session associated with a specific MAC address. Also, the `execute switch-controller switch-action 802-1X clear-auth <FortiSwitch_serial_number> <port_name>` command has been changed to `execute switch-controller switch-action 802-1X clear-auth-port <FortiSwitch_serial_number> <port_name>`.
- The new *WiFi & Switch Controller* > *FortiSwitch Clients* page lists all devices connected to the FortiSwitch unit for a particular VDOM. Double-clicking a row displays the *Device Info* pane, which lists the NAC policies and dynamic port policies that the device matches. Hovering over the device name displays the detail window, where you can do the following:
  - Create a firewall device address.
  - Create a firewall IP address.
  - Quarantine the host.
- The number of managed FortiSwitch units has increased from 16 to 24 on the following FortiGate models: FGR-60F, FG-60F, FGR-60F-3G4G, FG-61F, FG-80F, FG-80FB, FG-80FP, FG-81F, and FG-81FP.
- You can now configure multiple flow-export collectors using the `config collectors` command. For each collector, you can specify the collector IP address, the collector port number, and the collector layer-4 transport protocol for exporting packets. You can also specify how often a template packet is sent using the new `set template-export-period` command.
- You can now configure NAC LAN segments in the GUI.
- Administrators can now use the FortiSwitch profile to control whether users can log in with the managed FortiSwitchOS console port. By default, users can log in with the managed FortiSwitchOS console port.
- You can now use asterisks as a wildcard character when you pre-authorize FortiSwitch units. Using a FortiSwitch template, you can name the managed switch and configure the ports. When the FortiSwitch unit is turned on and discovered by the FortiGate device, the wildcard serial number is replaced by the actual serial number and the settings in the FortiSwitch template are applied to the discovered FortiSwitch unit.
- Dynamic discovery in FortiLink mode over a layer-3 network detects FortiSwitch split ports and newer FortiSwitch models. Split ports on all supported FortiSwitch models can be managed and displayed correctly on a FortiGate device.
- You can now configure flap guard through the switch controller.

- You can enable the MAC Authentication Bypass (MAB) option for devices (such as network printers) that cannot respond to the 802.1X authentication request. With MAB enabled on the port, the system will use the device MAC address as the user name and password for authentication. If a link goes down, you can select whether the impacted devices must reauthenticate. By default, reauthentication is disabled. You can use the FortiOS CLI to enable MAB reauthentication globally or locally:
  - On the global level, use the new `set mab-reauth` command to enable or disable MAB reauthentication.
  - On the local level, you can override the 802.1X settings for a specific managed switch and then use the new `set mab-reauth` command to enable or disable MAB reauthentication.
- You can now add multiple managed FortiSwitch VLANs to a software switch using the GUI or CLI. In previous releases, you could add only one managed FortiSwitch VLAN per FortiGate device to a software switch.
- You can now configure link-aggregation groups (LAGs) as members of a software switch that is being used for FortiLink.
- In previous releases, changing FortiSwitch split ports and then restarting the managed FortiSwitch unit caused the FortiGate device to have to rediscover and re-authorize the FortiSwitch unit. Now, the FortiGate device automatically updates the port list after split ports are changed and the FortiSwitch unit restarts. When split ports are added or removed, the changes are logged.
- The *WiFi & Switch Controller* > *FortiSwitch Ports* page has been improved.
  - In *Trunk* view, the *FortiSwitch Ports* page has been improved in the following ways:
    - The *LLDP Profile*, *Loop Guard* , and *Security Policy* columns were removed.
    - When you right-click a port, the menu now contains a *Mode* submenu.
    - When you right-click a port, the menu now contains the option to clear port counters.
    - The *Enabled Features* column lists LACP when it has been enabled.
  - In *Port* view, the *FortiSwitch Ports* page has been improved in the following ways:
    - New *VLAN*, *Dynamic VLAN*, and *Transceiver Power (Transmitted/Received)* columns are now available.
    - When you double-click a port, a new *Port Statistics* pane is displayed, which shows the transmitted and received traffic, frame errors by type, and transmitted and received frames. You can also select a port and then click the *View Statistics* button in the upper right corner. The *Compare with* dropdown list allows you to select another port to compare with the currently selected port. The statistics are refreshed every 15 seconds.
    - When you right-click a port, the menu now contains the option to clear port counters.
- The *Diagnostics and Tools* pane (from *WiFi & Switch Controller* > *Managed FortiSwitches*) has been improved.
  - The *General* pane now reports the fan status, power supply unit (PSU) status, and port health.
  - Clicking the new *Legend* button in the *General* pane displays the *Health Thresholds* pane, which lists the thresholds for the good, fair, and poor ratings of the general health, port health, and MC-LAG health.
  - A new *Clients* tab lists the FortiClient users of the selected FortiSwitch unit.
- IGMP snooping and MLD snooping are now supported on FortiLink NAC LAN segments when a FortiSwitch unit is controlled by a FortiGate device.

Special notices

Support of FortiLink features

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

Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than 6.2.6 or 6.4.4 is not supported

Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.2.6 and later 6.2 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to FortiSwitchOS 6.4.4 and later 6.4 versions is supported. Downgrading FortiSwitchOS 7.0.0 and later to versions earlier than FortiSwitchOS 6.2.6 or 6.4.4 is not supported.

Downgrading FortiSwitchOS 7.0.0 and later requires converting the admin password first

Because FortiSwitchOS 7.0.0 changed from SHA1 to SHA256 encryption for admin passwords, you need to convert the format of the admin password before downgrading from FortiSwitchOS 7.0.0 and later to an earlier FortiSwitchOS version.

If you do not convert the admin password before downgrading from FortiSwitchOS 7.0.0 and later, the admin password will not work after the switch reboots with the earlier FortiSwitchOS version.

The encrypted admin password in FortiSwitchOS 7.0.0 and higher starts with “SH2”, and the encrypted admin password for earlier FortiSwitchOS versions starts with “AK1”.

If you do not want to convert the format of the FortiSwitch admin password, you can use the FortiOS CLI to override the managed FortiSwitch admin password with the FortiGate admin password.

To convert the format of the admin password in FortiSwitchOS 7.0.0 and later before downgrading to an earlier FortiSwitchOS version:

1. Enter the following FortiSwitchOS CLI command to convert the admin password from SHA256 to SHA1 encryption:

   ```
   execute system admin account-convert <admin_name>
   ```

2. Downgrade your firmware.

To override the managed FortiSwitch admin password with the FortiGate admin password:

```
config switch-controller switch profile
   edit <FortiSwitch_profile_name>
      set login-passwd-override enable
      set login-passwd <new_password>
   end
```

NAC policies not maintained or converted when upgrading from 6.4 to 7.2

When you upgrade from FortiOS 6.4 to FortiOS 7.2.0, existing NAC policies are not maintained or automatically converted into dynamic port policies. They have to be reconfigured.

Upgrade information

FortiSwitchOS 7.2.0 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 7.2.0 support

The following table lists FortiSwitchOS 7.2.0 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 7.2.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
722781	MAC address flapping on the switch is caused by a connected FortiGate where IPS is enabled in transparent mode.
727301	Unable to quarantine hosts behind a FortiAP unit and FortiSwitch unit.
729324	The *Managed FortiAPs* and *Managed FortiSwitches* pages keep loading when the VDOM administrator has `netgrp` and `wifi` read/write permissions.
766583	A bin/cu_acd crash is generated when cfg-revert is enabled and involves a FortiSwitch unit.
768979	On a FortiGate with many FortiSwitch units and FortiAP units, the *Device Inventory* widget and `user-device- store list` are empty.
774848	Bulk MAC addresses deletions on a FortiSwitch unit is randomly causing all wired clients to disconnect at the same time and reconnect.
776442	FortiSwitch VLANs cannot be created in the FortiGate GUI for a second FortiLink.
777145	The *Managed FortiSwitches* page incorrectly shows a warning about an unregistered FortiSwitch unit even though it is registered. This only impacts transferred or RMAed FortiSwitch units. This is only a display issue with no impact on the FortiSwitch unit's operation.

Common vulnerabilities and exposures

FortiSwitchOS 6.2.0 is no longer vulnerable to the following CVEs:

- CVE-2017-6214

Visit https://fortiguard.com/psirt for more information.

Known issues

The following known issues have been identified with FortiOS 7.2.0. 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`.
781600	There should be a *Create MCLAG pair* button in the Topology view under *WiFi & Switch Controller* > *Managed FortiSwitches*.
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.
802786	Virtual IP addresses cannot be used in a FortiGate device to redirect the public IP address to the private IP address of the FortiSwitch unit.

www.fortinet.com