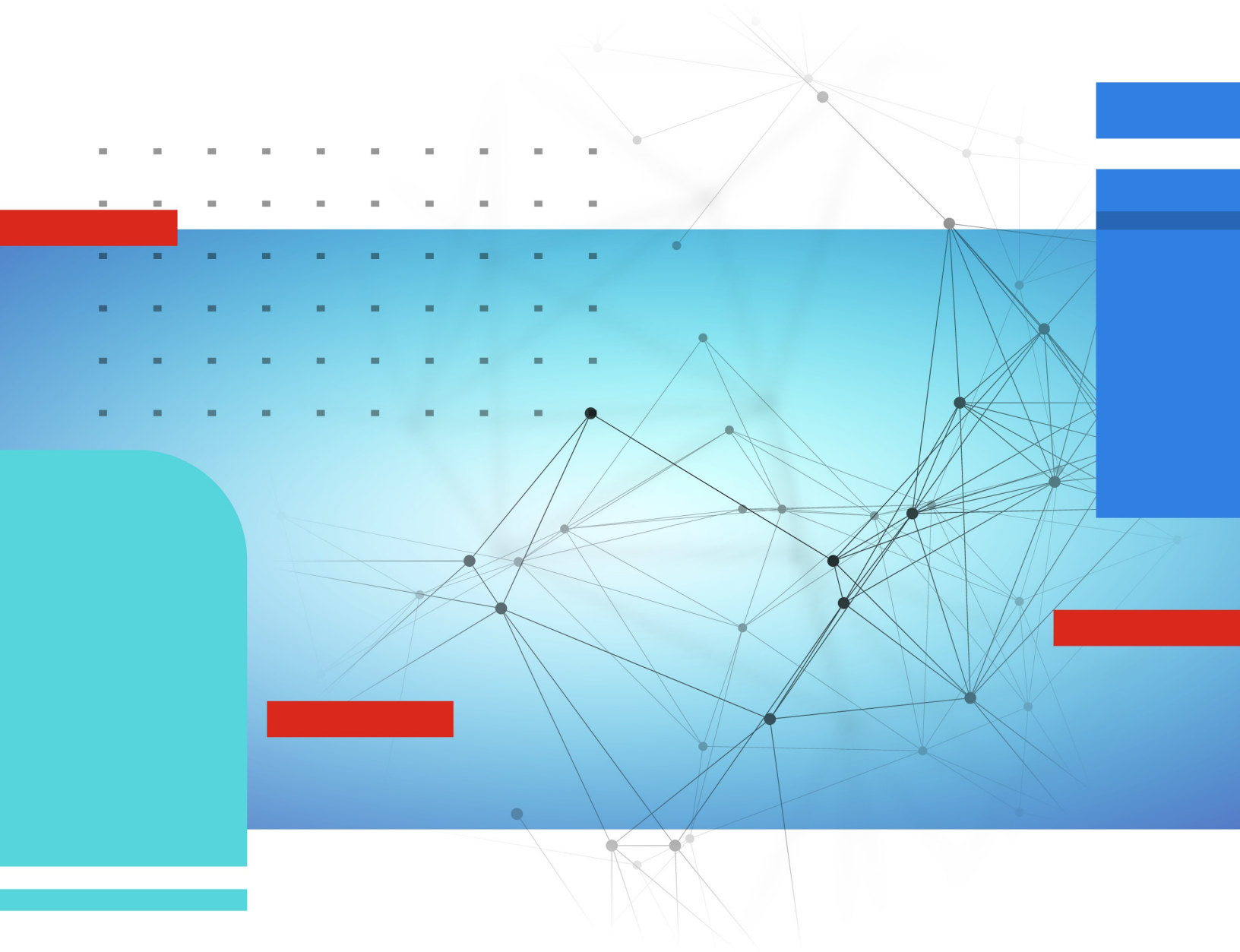
Administration Guide

FortiSwitch Manager 7.2.5



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 3, 2025
FortiSwitch Manager 7.2.5 Administration Guide
11-725-1075125-20250403

TABLE OF CONTENTS

Change log

Date	Change Description
December 10, 2024	Initial release of FortiSwitch Manager 7.2.5
January 24, 2025	Added a note at the beginning of Getting started on page 15 about the necessity of an internet connection.
January 27, 2025	• Removed the note at the beginning of Getting started on page 15 about the necessity of an internet connection. • Added more information to Registering the FortiSwitch Manager license on page 17.
April 3, 2025	Updated System requirements on page 11.

What's new in FortiSwitch Manager 7.2.5

The following new features are available in FortiSwitch Manager 7.2.5:

- The command for enabling VLAN optimization has changed from `set vlan-optimization enable` to `set vlan-optimization configured`; the command is still located under `config switch-controller global`. For more details, see Enabling VLAN optimization on page 37.
- FortiSwitch Manager now supports VLAN pruning. VLAN pruning prevents unnecessary traffic from unused VLANs by only allowing traffic from the VLANs required for the inter-switch link (ISL) trunks. This process makes networks more efficient and preserves bandwidth. In addition, VLAN pruning eliminates the time spent on manual VLAN pruning and reduces the chance of errors. For more details, see VLAN pruning on page 37.
- Two new CLI commands have been added under `config switch-controller system` to improve the FortiSwitch Manager connection:
  - Use the `set caputp-echo-interval <8-600>` command to set the interval for the Control and Provisioning of Unified Termination Points (CAPUTP) ECHO requests from the Scheduling Wide-area Transport Protocol (SWTP). The default value is 30 seconds. Setting the interval to a shorter time means that an offline device is detected quicker.
  - Use the `set caputp-max-retransmit <0-64>` command to set the maximum number of times that CAPUTP tunnel packets are retransmitted. The default value is 4. Setting the retransmission times to a lower number causes the CAPUTP daemon to time out sooner and then restart for faster failover.
- 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. For more details, see LACP fallback mode on page 52.
- The CLI commands for configuring Precision Time Protocol (PTP) transparent-clock mode have changed. FortiSwitch Manager supports the previous CLI commands, as well as the new ones. For more details, see Configuring PTP transparent-clock mode on page 75.
- 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). For more details, see FortiSwitch security policies on page 83.
- You can use new CLI commands to specify how the following RADIUS request attributes are formatted:
  - User-Name
  - User-Password
  - Called-Station-Id
  - Calling-Station-Id

  For more details, see Specifying how RADIUS request attributes are formatted on page 86.
- You can now dynamically assign a different NAS-IP-Address attribute to the managed switches when authenticating users with a RADIUS server. If needed, you can override the dynamic assignment and manually assign the NAS-IP-Address attribute to individual managed switches. **NOTE:** FortiSwitchOS supports only IPv4 addresses for the NAS-IP-Address attribute. For more details, see Dynamically and manually assigning the NAS-IP-Address attribute on page 87.

- The synchronization of the FortiSwitch Manager system interface description to the switch VLAN description (up to the first 63 characters of FortiSwitch VLAN description field in FortiSwitch Manager) is now supported. This allows a more flexible use of the Tunnel-Private-Group-Id RADIUS attribute. For more details, see Dynamic VLAN assignment on page 88.
- You can now assign a priority to each VLAN used in the 802.1X security policy. If there is more than one VLAN with the same name (specified in the `set description` command), FortiSwitchOS selects the VLAN with the lowest `assignment-priority` value (which is the highest priority) of the VLANs with names that match the value of the RADIUS Tunnel-Private-Group-Id or Egress-VLAN-Name attribute. The `assignment-priority` value can be 1-255. By default, the `assignment-priority` is 128. The lowest `assignment-priority` value gets the highest priority. For more details, see Setting the priority for dynamic or egress VLAN assignment on page 89.
- 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. For more details, see Dynamic access control lists on page 90.
- You can now include option-82 data in the DHCP request for DHCP snooping. DHCP option-82 data provides additional security by enabling a controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. You can select a fixed format for the Circuit ID and Remote ID fields or select which values appear in the Circuit ID and Remote ID fields. You can configure the option-82 settings on a global level, or you can override the global option-82 setting to specify plain text strings for the Circuit ID field and the Remote ID field for a specific VLAN on a port. In addition, you can display the DHCP option-82 string in ASCII or hexadecimal format. For more details, see Including option-82 data on page 104.
- 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. For more details, see Monitoring ARP packets on page 107.
- You can now use an access control list (ACL) to configure a policy for the ingress stage of the pipeline for incoming traffic. After creating an ACL group for the ingress policy, you apply the ACL group to a managed switch port. For more details, see Configuring an ACL on page 111.
- You can now use names for managed FortiSwitch units in switch-controller CLI commands. The user-defined name is also used in the FortiSwitch Manager GUI and logs. The FortiSwitch unit's serial number is saved in a new read-only field. For more details, see Defining names for managed switches on page 138.
- You can now export a list of FortiSwitch names, switch groups, status, models, firmware versions, where the switch is connecting from, and the join times. You can also export a list of switch ports with trunk names, port policies, enabled features, native VLANs, allowed VLANs, dynamic VLANs, PoE status, device information, security policies, DHCP-snooping status, transceivers connected to, transceiver power (transmitted or received), and negotiated speed. You can choose to export each list in comma-separated values (CSV) or JSON format. For more details, see Exporting switch information on page 176.

Introduction

FortiSwitch Manager (FSWM) is the on-premise management platform for the FortiSwitch product. FortiSwitch units connect to FSWM over the layer-3 network. You can configure a large number of FortiSwitch units with this FortiSwitch-management-only platform. FortiSwitch Manager provides a user experience consistent with the FortiLink Switch Controller.

Supported models

FortiSwitch Manager 7.2.5 supports the following models:

FortiSwitch 1xx	FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-110G-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124FFPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE
FortiSwitch 2xx	FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE
FortiSwitch 4xx	FS-424E, FS-424E-POE, FS-424E-FPOE, FS-424E-Fiber, FS-M426E-FPOE, FS-448E, FS-448E-POE, FS-448E-FPOE
FortiSwitch 5xx	FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE
FortiSwitch 6xx	FS-624F, FS-624F-FPOE, FS-648F, FS-648F-FPOE
FortiSwitch 1xxx	FS-1024D, FS-1024E, FS-1048E, FS-T1024E, FS-T1024F-FPOE
FortiSwitch 2xxx	FS-2048F
FortiSwitch 3xxx	FS-3032E
FortiSwitch Rugged	FSR-112D-POE, FSR-124D, FSR-216F-POE, FSR-424F-POE

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

Compatibility

FortiSwitch Manager 7.2.5 is compatible with FortiSwitchOS 6.4.6 build 0470 or later.

Web browser support

Web browser	• Microsoft Edge 112 • Mozilla Firefox version 113 • Google Chrome version 113 Other web browsers might function correctly but are not supported by Fortinet.

Virtualization environment support

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.2 Express Edition, CU1
Linux KVM	• Ubuntu 22.04.3 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• Windows Server 2019
Windows Hyper-V Server	• Microsoft Hyper-V Server 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESXi	• Versions 6.5, 6.7, 7.0, and 8.0

System requirements

Number of managed FortiSwitch units	vCPU	Memory (GB)	Hard disk
1-10	8 (minimum 4)	8 (minimum 4)	1 TB (minimum 32 GB)
10-100	16 (minimum 8)	16 (minimum 8)	1 TB (minimum 32 GB)
100-1,000	32 (minimum 16)	32 (minimum 16)	1 TB (minimum 32 GB)
1,000-2,500	32	32 (minimum 16)	1 TB (minimum 32 GB)

Supported Switch Controller features

Switch Controller Features	FortiSwitch Models
Centralized VLAN Configuration	D-series, E-series, F-series
Switch POE Control	D-series, E-series
Link Aggregation Configuration	D-series, E-series, F-series
Spanning Tree Protocol (STP)	D-series, E-series, F-series
LLDP/MED	D-series, E-series, F-series
IGMP Snooping	D-series, E-series, F-series
802.1X Authentication (Port-based, MAC-based, MAB)	D-series, E-series, F-series
Syslog Collection	D-series, E-series, F-series
DHCP Snooping	D-series, E-series, F-series
LAG support	D-series, E-series, F-series
sFlow	Not supported on FS-1xxE Series
Dynamic ARP Inspection (DAI)	D-series, E-series, F-series
Port Mirroring	D-series, E-series
RADIUS Accounting	D-series, E-series, F-series
Centralized Configuration	D-series, E-series, F-series
STP BDPU Guard, Root Guard, Edge Port	D-series, E-series, F-series
Loop Guard	D-series, E-series, F-series
Switch admin Password	D-series, E-series
Storm Control	D-series, E-series, F-series
802.1X-Authenticated Dynamic VLAN Assignment	D-series, E-series, F-series
QoS	Not supported on FSR-112D-POE
Centralized Firmware Management	D-series, E-series, F-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, F-series
NetFlow and IPFIX flow tracking and export	D-series, E-series
MSTP instances	D-series, E-series, F-series
QoS statistics	D-series, E-series
Configuring SNMP	D-series, E-series, F-series

Switch Controller Features	FortiSwitch Models
IPv4 source guard	FSR-124D, FS-224D-FPOE, FS-248D, FS-424D-POE, FS-424D-FPOE, FS-448D-POE, FS-448D-FPOE, FS-424D, FS-448D, FS-2xxE, and FS-4xxE
Point-to-point layer-2 network supported	D-series, E-series, F-series
Dynamic detection of LLDP neighbor devices	D-series, E-series
Explicit congestion notification (ECN)	FS-1024D, FS-1048D, FS-1048E, FS-3032D, FS-3032E, FS-4xxE, and FS-5xxD
Aggregation mode selection for trunk members	D-series, E-series
Multiple attribute values sent in a RADIUS Access-Request	D-series, E-series
PTP transparent-clock mode	FS-1048E, FS-224D, FS-224E, FS-3032D, FS-3032E, FS-424D, FS-4xxE, and FS-5xxD
Rapid PVST interoperation	D-series, E-series, F-series
Flash port LEDs	D-series, E-series
Cable diagnostics	Not supported on FSR-112D-POE, FS-1024D, FS-1048D, FS-1048E, FS-3032D, or FS-3032E
Flow control	D-series, E-series, F-series
Ingress pause metering	200 series, 400D and 400E series, 500 series, FS-1024D, FS-1048D, FS-1048E, and FS-3032D
RVI	448E, 448E-FPOE, 448E-POE, 424E-Fiber, 500 series, 1024D, 1024E,1048E, T1024E, 3032E
Static routing (IPv4/IPv6)	D-series, E-series, F-series (except FSR-112DPOE)
VRF (IPv4/IPv6)	500 series, 1024D, 1024E,1048E, T1024E, 3032E
Automation stitches	D-series, E-series, F-series
Templates for managed-switch configurations	D-series, E-series, F-series
DHCP-snooping static entries (IPv4)	D-series, E-series, F-series
VLAN pruning	D-series, E-series, F-series, G-series
LACP fallback mode	D-series, E-series, F-series (except FS-6xxF), G-series
Dynamic access control lists (DACLs)	FSR-124D, FSR-424F-POE, 1xxE, 1xxF, FS-110G-FPOE, 200 Series, 4xxE, 500 Series, 1024D, 1024E, 1048E, T1024E, T1024F-FPOE, 2048F, 3032E
802.1x: priority for dynamic or egress VLAN assignment	D-series, E-series, F-series, G-series
DHCP-snooping option 82	FSR-124D, FSR-424F-POE, 1xxE, 1xxF, FS-110G-FPOE, 200 Series, 4xxE, 500 Series, 1024D, 1024E, 1048E, T1024E, T1024F-FPOE, 2048F, 3032E

Switch Controller Features	FortiSwitch Models
DAI: monitor ARP packets	D-series, E-series, F-series (except FS-6xxF), G-series
ACL (IPv4 ingress)	FSR-112D-POE, FSR-124D, FSR-216F-POE, FSR-424F-POE, 200 Series, 4xxE, 500 Series, 6xxF, 1024E, 1048E, T1024E, T1024F-FPOE, 2048F, 3032E

NOTE: The following features are not supported:

- High availability (HA)
- FortiLink layer-2 mode
- UTM/security services (These are not needed because FortiSwitch Manager is not in the data path.)
- Network access control (NAC)
- Hardware switch
- Remote SPAN (RSPAN)
- Quarantines
- Integration with FortiAnalyzer
- VDOMs

Getting started

FortiSwitch Manager is offered as a virtual appliance. After you install a hypervisor of your choice, install the FortiSwitch Manager license as per your scale requirements. The FortiSwitch Manager license SKUs can be added together, so you can use more than one of the following available license SKUs:

FortiSwitch Manager subscription license	Description
FC1-10-SWMVM-258-01-DD	Subscription license for 10 FortiSwitch units managed by FortiSwitch Manager VM. 24x7 FortiCare support (for FSWM VM) included.
FC2-10-SWMVM-258-01-DD	Subscription license for 100 FortiSwitch units managed by FortiSwitch Manager VM. 24x7 FortiCare support (for FSWM VM) included.
FC3-10-SWMVM-258-01-DD	Subscription license for 1,000 FortiSwitch units managed by FortiSwitch Manager VM. 24x7 FortiCare support (for FSWM VM) included.

Your licenses control the maximum number of FortiSwitch units that you can manage; however, only authorized switches are counted by FortiSwitch Manager. Switches that have been discovered but not authorized yet do not count toward the maximum number of switches that can be managed.

To check how many FortiSwitch units can be managed:

```
diagnose debug vm-print-license
```

To check how many FortiSwitch units are managed:

```
execute switch-controller licensed-switches counts
```

In the command output, switches are in one of four states:

- *managed*—Authorized switches are counted as *managed*. Deauthorized a switch does not remove it from the count of managed switches.
- *reserved*— Switches are included in the count of managed switches without being discovered or authorized. Reserving a place for a switch prevents another switch from being added to count instead.
- *pending*— A switch that is in the process of becoming managed or being deleted from the configuration. A pending switch is included in the count of managed switches.
- *locked-out*—When a configuration has more authorized switches than are licensed, the system will lock out some switches. Locked-out switches are not included in the count of managed switches.

To delete an authorized switch so that it is no longer included in the count of managed switches:

```
config switch-controller managed-switch
   delete <FortiSwitch-serial-number>
end
```

To remove a FortiSwitch unit from being managed and to reserve space for a different FortiSwitch unit in the count of managed switches:

```
execute switch-controller licensed-switches swap <swap-out-FortiSwitch-serial-number> <swap-
     in-FortiSwitch-serial-number>
```

The command deletes <swap-out-FortiSwitch-serial-number> from the configuration and reserves a place for <swap-in-FortiSwitch-serial-number>.

The swapped-out switch can still be re-discovered. If automatic authorization is enabled, the swapped-out switch can be authorized again.

In the following example, S108DV3A17000033 is deleted from the configuration, and S108DV3A17000034 is authorized and counted by FortiSwitch Manager:

```
execute switch-controller licensed-switches swap S108DV3A17000033 S108DV3A17000034
```

To list the switches that are managed and authorized and reserved switches:

```
execute switch-controller licensed-switches list managed
```

To list reserved switches:

```
execute switch-controller licensed-switches list reserved
```

To delete a reserved switch and remove it from the count of managed switches:

```
execute switch-controller licensed-switches delete-reserved <FortiSwitch-serial-number>
```

Setting up FortiSwitch Manager

To set up FortiSwitch Manager, you need to configure the FortiSwitch Manager VM port1 and configure static routes. By default, port1 has the DHCP client enabled. If necessary, assign a fixed IP address and configure a default route.

The VM platform and hypervisor management environments include a guest console window. On FortiSwitch Manager, the guest console window provides access to the FortiSwitch Manager console. Before you can access the CLI using SSH/Telnet, you must configure the FortiSwitch Manager VM port1 with an IP address and administrative access. For example:

```
config system interface
   edit "port1"
      set ip 192.168.2.1 255.255.255.0
      set allowaccess ping https ssh http telnet
   next
end
```

To configure static routes:

```
   config router static
      edit <ID>
         set dst <router-subnet> <subnet-mask>
```

```
      set gateway <router-IP-address>
      set device "<FortiLink-interface>"
    next
end
```

For example:

```
config router static
  edit 2
    set gateway 192.168.2.11
    set device "port1"
  next
end
```

Registering the FortiSwitch Manager license

You need the following to register the FortiSwitch Manager license:

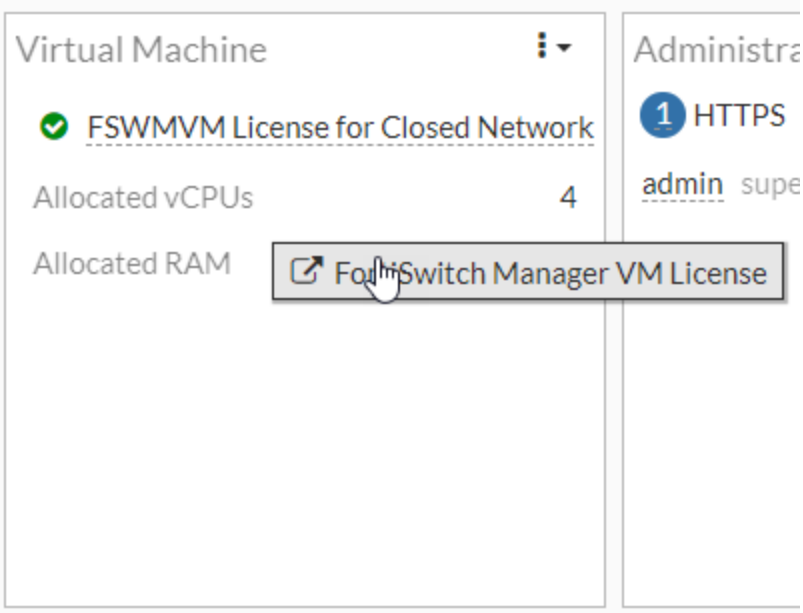
- An internet connection is required for FortiSwitch Manager to contact FortiGuard to validate its license during the initial deployment and periodically during normal operation.
- The UUID is required for registration. Use the following CLI command to obtain the UUID:

```
diagnose hardware sysinfo vm
```

Installing the FortiSwitch Manager license

To upload the license file using the GUI:

1. Go to *Dashboard* > *Status*.
2. Click in the *Virtual Machine* widget.
3. Click *FortiSwitch Manager VM License*.



4. Click *Upload*.
5. After you upload the license file, click *OK*.

To upload the license file:

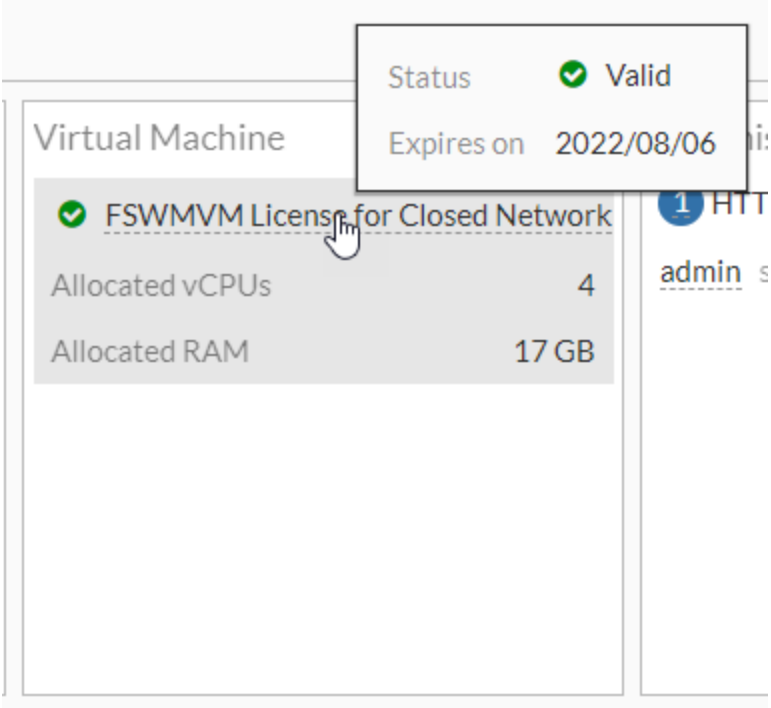
```
execute restore vmlicense {ftp | tftp} <file-name> <FTP-server>[:FTP-port]
```

For example:

```
execute restore vmlicense tftp license.lic 10.0.1.2
```

To check that the license is valid using the GUI:

Go to *Dashboard* > *Status* and hover over the license link in the *Virtual Machine* widget.



To check that the license status is valid using the CLI:

```
get system status
```

Configuring FortiLink

By default, port1 is the FortiLink interface. After the network connectivity is configured, FortiSwitch Manager is ready to manage FortiSwitch units.

Optionally, enable automatic FortiSwitch authorization:

1. Go to *Switch Controller > FortiLink Interface*.
2. Select the FortiLink interface and click *Edit*.
3. Enable *Automatically authorize devices*.
4. Click *Apply*.

Setting up the FortiSwitch units

Starting with FortiSwitchOS 7.2.0, when using DHCP discovery, FortiSwitch units can automatically connect with FortiSwitch Manager, either with “internal” or “mgmt” ports, and the FortiSwitch units can then be authorized and managed. Additional FortiSwitch units connected to another FortiSwitch unit already managed by FortiSwitch Manager are also discovered and authorized.

If you are using an earlier version of FortiSwitchOS or if you are using static discovery, follow the procedures in this section.

You need to configure FortiSwitch units with the FortiSwitch Manager IP address to establish connectivity, and you need to configure the FortiSwitch units to use FortiLink mode over a layer-3 network.

To configure a FortiSwitch unit to operate in a layer-3 network (in-band management):

NOTE: You must enter these commands in the indicated order for this feature to work.

1. Reset the FortiSwitch to factory default settings with the `execute factoryreset` command.
2. Manually set the FortiSwitch unit to FortiLink mode if you are using FortiSwitchOS 7.0.0 or earlier:

```
config system global
   set switch-mgmt-mode fortilink
end
```

3. Configure the discovery setting for the FortiSwitch unit. You can either use DHCP discovery or static discovery to find the IP address of the FortiSwitch Manager. The default `ac-dhcp-option-code` is `138`.

   To use DHCP discovery:

```
config switch-controller global
   set ac-discovery-type dhcp
   set ac-dhcp-option-code <integer>
end
```

   To use static discovery:

```
config switch-controller global
   set ac-discovery-type static
   config ac-list
      edit <id>
         set ipv4-address <IPv4-address>
      next
   end
end
```

4. Configure only one physical port or LAG interface of the FortiSwitch unit as an uplink port. When the FortiSwitch unit is in FortiLink mode, VLAN 4094 is configured on an internal port, which can provide a path to the layer-3 network.
   NOTE: The uplink port cannot be assigned any VLANs.

```
config switch interface
   edit <port-number>
      set fortilink-l3-mode enable
   end
end
```

   The `fortilink-l3-mode` command is only visible after you configure DHCP or static discovery.
5. If you are going to configure another FortiSwitch unit that is connected to the FortiSwitch unit configured in steps 1-4, you only need to configure the discovery settings. You do not need to enable `fortilink-l3-mode` on the uplink port.

To use DHCP discovery:

```
config switch-controller global
   set ac-discovery-type dhcp
   set ac-dhcp-option-code <integer>
end
```

To use static discovery:

```
config switch-controller global
   set ac-discovery-type static
   config ac-list
      edit <id>
         set ipv4-address <IPv4-address>
      next
   end
end
```

To configure a FortiSwitch unit to operate in a layer-3 network (out-of-band management):

1. Configure FortiSwitch Manager as the Network Time Protocol (NTP) server:

```
config system ntp
   set allow-unsync-source enable
      config ntpserver
         edit <ID>
            set server "<FortiSwitch-Manager-IP-address>"
         next
      end
   set ntpsync enable
end
```

For example:

```
config system ntp
   set allow-unsync-source enable
      config ntpserver
         edit 1
            set server "192.168.2.1"
         next
      end
   set ntpsync enable
end
```

2. Configure the management system interface.

NOTE: You can use DHCP mode for the management system interface (`set mode dhcp`). If you do use DHCP mode, configuring NTP and the static route is not necessary.

```
config system interface
   edit "mgmt"
      set ip <IP-address-netmask>
      set allowaccess ping https ssh
      set type physical
   next
```

```
end
```

For example:

```
config system interface
   edit "mgmt"
      set ip 192.168.11.94 255.255.255.0
      set allowaccess ping https ssh
      set type physical
   next
end
```

3. Configure a static route:

```
config router static
   edit <ID>
      set device "mgmt"
      set dst <destination-IP-address-netmask>
      set gateway <gateway-IP-address>
   next
end
```

For example:

```
config router static
   edit 1
      set device "mgmt"
      set dst 0.0.0.0 0.0.0.0
      set gateway 192.168.11.1
   next
end
```

4. Configure the discovery setting for the FortiSwitch unit. You can either use static discovery or DHCP discovery to find the IP address of the FortiSwitch Manager. The default `ac-dhcp-option-code` is 138.

To use static discovery:

```
config switch-controller global
   set ac-discovery-type static
   config ac-list
      edit <id>
         set ipv4-address <IPv4-address>
      next
   end
end
```

To configure DHCP on the management interface:

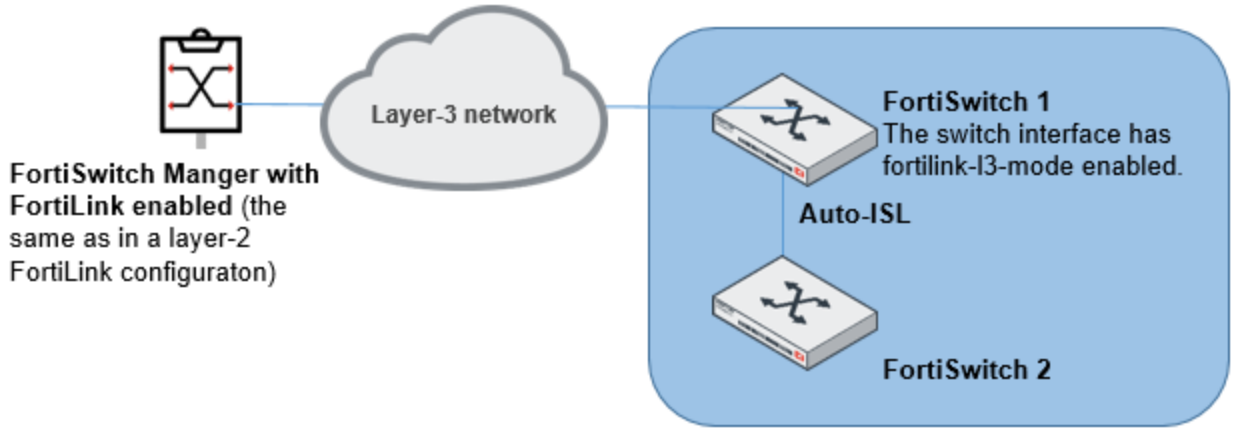
```
config system interface
   edit "mgmt"
      set mode dhcp
      set allowaccess ping https http ssh telnet
      set type physical
   next
end
```

To use DHCP discovery:

```
config switch-controller global
   set ac-discovery-type dhcp
   set ac-dhcp-option-code <integer>
end
```

Connecting additional FortiSwitch units to the first FortiSwitch unit

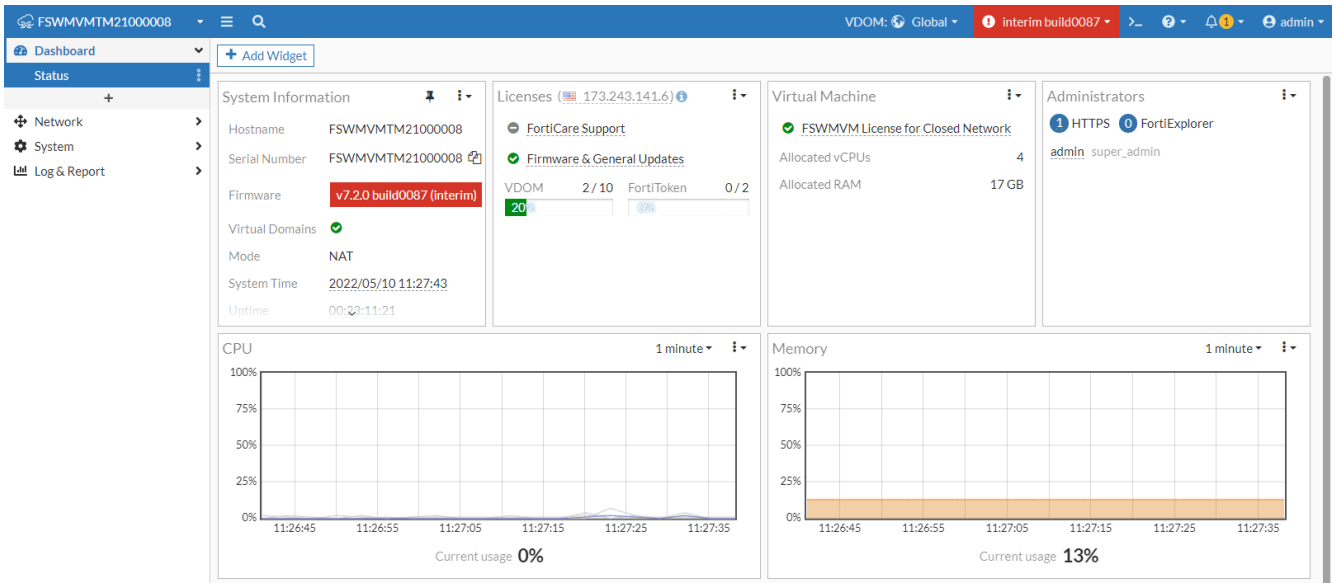
In this scenario, the default FortiLink-enabled port of FortiSwitch 2 is connected to FortiSwitch 1, and the two switches then form an auto-ISL. You only need to configure the discovery settings (see Step 3) for additional switches (FortiSwitch 2 in the following diagram). You do not need to enable `fortilink-l3-mode` on the uplink port. Check that each FortiSwitch unit can reach FortiSwitch Manager.



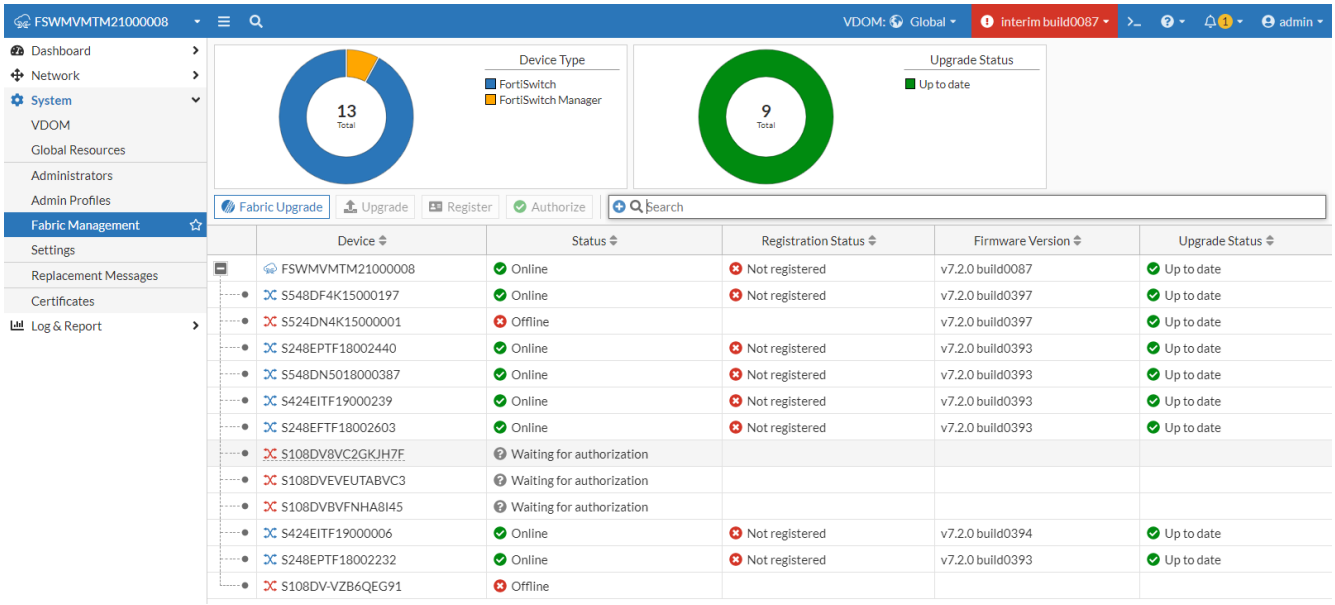
Using FortiSwitch Manager

Go to *Dashboard* > *Status* to see the current values for the following:

- System information
- Licenses
- Allocated vCPUs and RAM
- Administrators
- CPU
- Memory



Go to *System* > *Fabric Management* to see a list of managed FortiSwitch units, as well as the status, registration status, firmware version, and upgrade status for each.



How to authorize a FortiSwitch unit

Using the GUI:

1. Go to *System* > *Fabric Management*.
2. Select an unauthorized FortiSwitch unit.
3. Click *Authorize*.

Using the CLI:

```
config switch-controller managed-switch
   edit <FortiSwitch-serial-number>
      set fsw-wan1-admin enable
   next
end
```

Creating a switch group

Grouping switches makes it easier to manage a large number of switches. For example, a switch group can be all switches in a building, in a city, or in a business unit.

Using the GUI:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Click *Create New* > *FortiSwitch Group*.
3. Enter a name for the switch group.
4. Select the FortiLink interface.
5. Click + and then select the switches to be grouped.
6. Click *Close* to return to the *New FortiSwitch Group* page.
7. Enter a description of the switch group.
8. Click *OK*.

Using the CLI:

```
config switch-controller switch-group
   edit <name-of-FortiSwitch-group>
      set description <description-of-FortiSwitch-group
      set fortilink <name-of-FortiLink-interface>
      set members <FortiSwitch-serial-number1>, <FortiSwitch-serial-number2>, ...
   next
end
```

Upgrading FortiSwitch Manager

To upgrade FortiSwitch Manager in the GUI:

1. Log in to the FortiSwitch Manager GUI as the admin administrative user.
2. Go to *System* > *Firmware*.
3. Select FortiSwitch Manager and click *Upgrade*.
   The *FortiSwitch Manager Upgrade* pane opens.
4. Click the following tabs to view the available firmware:

Latest	Displays the latest, available firmware from FortiGuard.
All Upgrades	Displays all available firmware from FortiGuard.
File Upload	Click the *File Upload* tab to upload a firmware file that you previously downloaded from the Fortinet Customer Service & Support website.

5. Select a firmware version and click *Confirm and Backup Config*.
   If you are upgrading from a mature to a feature firmware version, the *Confirm* pane opens with a warning message.
6. Review the warning and click *Confirm* to continue.
   A warning message is displayed.
7. Click *Continue* to initiate the upgrade.
8. FortiSwitch Manager backs up the current configuration to the management computer, uploads the firmware image file, upgrades to the new firmware version, and restarts.
   This process takes a few minutes.

To upgrade FortiSwitch Manager in the CLI:

1. Make sure that the TFTP server is running.
2. Copy the new firmware image file to the root directory of the TFTP server.
3. Log in to the CLI.
4. Ping the TFTP server to ensure that FortiSwitch Manager can connect to it:
   ```
   execute ping <tftp_ipv4>
   ```
5. Enter the following command to copy the firmware image from the TFTP server to FortiSwitch Manager:
   ```
   execute restore image tftp <image_name_on_TFTP_server> <TFTP_sever_Ipv4_IPv6_FQDN>
   ```
   FortiSwitch Manager responds with the message:
   ```
   This operation will replace the current firmware version!
   Do you want to continue? (y/n)
   ```
6. Type `y`.
   FortiSwitch Manager uploads the firmware image file, verifies the signature of the firmware image, and determines the firmware maturity level.
   When you are upgrading to a feature firmware image, you are asked to confirm whether to continue with the upgrade.
   When you proceed with the upgrade, the upgrade image is installed, and FortiSwitch Manager restarts. This process takes a few minutes.
   ```
   Please wait...
   ```

```
Connect to tftp server 172.16.200.55 ...
############################################################################
Get image from tftp server OK.
Verifying the signature of the firmware image.

Warning: Upgrading to an image with Feature maturity notation.
Image file uploaded is marked as a Feature image, are you sure you want to upgrade?
Do you want to continue? (y/n)y
Please confirm again. Are you sure you want to upgrade using uploaded file?
Do you want to continue? (y/n)y
Checking new firmware integrity ... pass
Please wait for system to restart.
Firmware upgrade in progress ...
Done.
The system is going down NOW !!
```

7. Reconnect to the CLI.
8. Update the antivirus and attack definitions:

```
execute update-now
```

To download firmware:

1. Log into Fortinet Customer Service & Support with your user name and password.
2. Go to *Support* > *Firmware Download*.

   A list of Release Notes is shown. If you have not already done so, download and review the Release Notes for the firmware version that you are upgrading to.
3. Select the *Download* tab.
4. Navigate to the folder for the firmware version that you are upgrading to.
5. Find your device model on the list.
6. Click *HTTPS* in the far right column to download the firmware image to your computer.

Firmware can also be downloaded using FTP, but as FTP is not an encrypted file transferring protocol, HTTPS downloading is recommended.

Managing FortiSwitch units

FortiSwitch units, when used in managed mode, support only the default administrative access HTTPS port (443).

Starting in FortiSwitch Manager 7.2.0, zero-touch management is now more efficient for new FortiSwitch units. When a new FortiSwitch unit is started, by default, it will connect to the available manager, which can be FortiSwitch Manager, a FortiGate device, or FortiLAN Cloud. 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.

This section covers the following topics:

Optional configuration required before discovering and authorizing FortiSwitch units

This section covers the following topics:

Migrating the configuration of standalone FortiSwitch units

When a configured standalone FortiSwitch unit is converted to managed mode, the standalone configuration is lost. To save time, use the `fortilinkify.py` utility to migrate your standalone configuration from one or more FortiSwitch units to a combined FortiSwitch-Manager-compatible configuration.

To get the script and instructions, go to:

https://fndn.fortinet.net/index.php?/tools/file/68-fortiswitch-configuration-migration-tool/

VLAN interface templates for FortiSwitch units

NOTE: You can only create VLAN interface templates when FortiSwitch Manager has not authorized any FortiSwitch units yet, so only physically connect the FortiSwitch unit to FortiSwitch Manager after completing this section.

You can create configuration templates that define the VLAN interfaces and are applied to new FortiSwitch devices when they are discovered and managed by FortiSwitch Manager.

You can create templates, and then assign those templates to the automatically created switch VLAN interfaces for six types of traffic. The network subnet that is reserved for the switch controller can also be customized.

To ensure that switch VLAN interface names are unique for each system, the interface names are the same as the template names.

You can also customize the FortiLink management VLAN per FortiLink interface:

```
config system interface
   edit <fortilink interface>
      set fortilink enable
      set switch-controller-mgmt-vlan <integer>
   next
end
```

The management VLAN can be a number from 1 to 4094. the default value is 4094.

Create VLAN interface templates

To configure the VLAN interface templates:

```
config switch-controller initial-config template
   edit <template_name>
      set vlanid <integer>
      set ip <ip/netmask>
      set allowaccess {options}
      set auto-ip {enable | disable}
      set dhcp-server {enable | disable}
   next
end
```

<template_name>	The name, or part of the name, of the template.
vlanid <integer>	The unique VLAN ID for the type of traffic the template is assigned to (1-4094; the default is 4094)
ip <ip/netmask>	The IP address and subnet mask of the switch VLAN interface. This can only be configured when auto-ip is disabled.
allowaccess {options}	The permitted types of management access to this interface.
auto-ip {enable | disable}	When enabled, the switch-controller will pick an unused 24 bit subnet from the switch-controller-reserved-network (configured in config system global).
dhcp-server {enable | disable}	When enabled, the switch-controller will create a DHCP server for the switch VLAN interface

To assign the templates to the specific traffic types:

```
config switch-controller initial-config vlans
   set default-vlan <template>
```

```
   set quarantine <template>
   set rspan <template>
   set voice <template>
   set video <template>
   set nac <template>
end
```

default-vlan <template>	Default VLAN assigned to all switch ports upon discovery.
quarantine <template>	VLAN for quarantined traffic.
rspan <template>	VLAN for RSPAN/ERSPAN mirrored traffic.
voice <template>	VLAN dedicated for voice devices.
video <template>	VLAN dedicated for video devices.
nac <template>	VLAN for NAC onboarding devices.

To configure the network subnet that is reserved for the switch controller:

```
config system global
   set switch-controller-reserved-network <ip/netmask>
end
```

The default value is `169.254.0.0 255.255.0.0`.

Example

In this example, six templates are configured with different VLAN IDs. Except for the default template, all of them have DHCP server enabled. When a FortiSwitch is discovered, VLANs and the corresponding DHCP servers are automatically created.

To configure six templates and apply them to VLAN traffic types:

```
config switch-controller initial-config template
   edit "default"
      set vlanid 1
      set auto-ip disable
   next
   edit "quarantine"
      set vlanid 4093
      set dhcp-server enable
   next
   edit "rspan"
      set vlanid 4092
      set dhcp-server enable
   next
   edit "voice"
      set vlanid 4091
      set dhcp-server enable
   next
   edit "video"
      set vlanid 4090
      set dhcp-server enable
   next
```

```
   edit "onboarding"
      set vlanid 4089
      set dhcp-server enable
   next
end
config switch-controller initial-config vlans
   set default-vlan "default"
   set quarantine "quarantine"
   set rspan "rspan"
   set voice "voice"
   set video "video"
   set nac "onboarding"
end
```

To see the automatically created VLANs and DHCP servers:

```
show system interface
   edit "default"
      set vdom "root"
      set snmp-index 24
      set switch-controller-feature default-vlan
      set interface "fortilink"
      set vlanid 1
   next
   edit "quarantine"
      set vdom "root"
      set ip 169.254.11.1 255.255.255.0
      set description "Quarantine VLAN"
      set security-mode captive-portal
      set replacemsg-override-group "auth-intf-quarantine"
      set device-identification enable
      set snmp-index 25
      set switch-controller-access-vlan enable
      set switch-controller-feature quarantine
      set color 6
      set interface "fortilink"
      set vlanid 4093
   next
   ...
end
show system dhcp server
   edit 2
      set dns-service local
      set ntp-service local
      set default-gateway 169.254.1.1
      set netmask 255.255.255.0
      set interface "fortilink"
      config ip-range
         edit 1
            set start-ip 169.254.1.2
            set end-ip 169.254.1.254
         next
      end
      set vci-match enable
      set vci-string "FortiSwitch" "FortiExtender"
   next
   edit 3
```

```
      set dns-service default
      set default-gateway 169.254.11.1
      set netmask 255.255.255.0
      set interface "quarantine"
      config ip-range
         edit 1
            set start-ip 169.254.11.2
            set end-ip 169.254.11.254
         next
      end
      set timezone-option default
   next
   ...
end
```

Automatic provisioning of FortiSwitch firmware upon authorization

Administrators no longer need to upload the FortiSwitch firmware. Instead, administrators can configure the managed FortiSwitch units to be automatically upgraded to the latest FortiSwitchOS version available in FortiGuard when the switches are authorized by FortiSwitch Manager. If the FortiSwitch units are already running the latest version of FortiSwitchOS when they are authorized, no changes are made.

- You cannot use the one-time automatic upgrade with the automatic provisioning that uses uploaded firmware. When `firmware-provision-latest` is set to `once`, the `firmware-provision` and `firmware-provision-version` commands are unset.
- If a FortiSwitch unit is being upgraded when the one-time automatic upgrade is configured, the upgrade in progress is paused until the one-time automatic upgrade is completed.

To configure the automatic provisioning using uploaded FortiSwitch firmware:

```
config switch-controller managed-switch
       edit <FortiSwitch_serial_number>
               set firmware-provision {enable | disable}
               set firmware-provision-version <version>
       next
end
```

`firmware-provision {enable | disable}`	Enable or disable provisioning firmware to the FortiSwitch unit after authorization (the default is disable).
`firmware-provision-version <version>`	The firmware version to provision the FortiSwitch unit with on bootup. The format is major_version.minor_version.build_number, for example, 6.4.0454.

To set up the one-time automatic upgrade of the FortiSwitch firmware:

1. On FortiSwitch Manager, configure automatic provisioning:

```
config switch-controller global
   set firmware-provision-on-authorization enable
end
```

By default, the `set firmware-provision-latest` command is set to `disable` under `config switch-controller managed-switch` before the FortiSwitch unit is authorized by FortiSwitch Manager.

2. On FortiSwitch Manager, authorize the FortiSwitch unit.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set fsw-wan1-peer <FortiLink_interface_name>
      set fsw-wan1-admin enable
   end
```

Authorizing the FortiSwitch unit changes the setting of the `set firmware-provision-latest` command to `once` under `config switch-controller managed-switch`.

3. When the status of the managed FortiSwitch unit is “Authorized/Up,” FortiSwitch Manager downloads the latest supported version of FortiSwitchOS from FortiGuard and then upgrades the switch.
4. The setting of the `set firmware-provision-latest` command is changed to `disable` under `config switch-controller managed-switch`.

Instead of enabling `firmware-provision-on-authorization`, you can leave the command at its default setting (`set firmware-provision-on-authorization disable`) and change the setting of `firmware-provision-latest` to `once`.

Discovering

This section covers the following topics:

Authorizing

If automatic authorization is disabled, you need to authorize the FortiSwitch unit as a managed switch:

```
config switch-controller managed-switch
   edit FS224D3W14000370
      set fsw-wan1-admin enable
   end
end
```

NOTE: After authorization, the FortiSwitch unit reboots in managed mode.

Preparing the FortiSwitch unit

If the FortiSwitch unit is in the factory default configuration, it is ready to be connected to FortiSwitch Manager. If the FortiSwitch unit is not in the factory default configuration, log in to the FortiSwitch unit with the CLI and use the `execute factoryreset` command to reset the FortiSwitch unit to the factory defaults

Optional management configuration

This section covers the following topics:

Using the FortiSwitch serial number for automatic name resolution

By default, you can check that FortiSwitch unit is accessible from FortiSwitch Manager with the `execute ping <FortiSwitch_IP_address>` command. If you want to use the FortiSwitch serial number instead of the FortiSwitch IP address, use the following commands:

```
config switch-controller global
   set sn-dns-resolution enable
end
```

NOTE: The `set sn-dns-resolution enable` configuration is enabled by default.

Then you can use the `execute ping <FortiSwitch_serial_ number>.<domain_name>` command to check if the FortiSwitch unit is accessible from FortiSwitch Manager. For example:

```
FSWMVMTM21000008 (root) # execute ping S524DF4K15000024.fsw
PING S524DF4K15000024.fsw (123.456.7.8): 56 data bytes
64 bytes from 123.456.7.8: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=3 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=4 ttl=64 time=0.0 ms
```

Now you can use the `execute ping <FortiSwitch_serial_number>` command to check if the FortiSwitch unit is accessible from FortiSwitch Manager. For example:

```
FSWMVMTM21000008 (root) # execute ping S524DF4K15000024
PING S524DF4K15000024.fsw (123.456.7.8): 56 data bytes
64 bytes from 123.456.7.8: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=3 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=4 ttl=64 time=0.0 ms

--- S524DF4K15000024.fsw ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Changing the admin password for all managed FortiSwitch units

By default, each FortiSwitch has an admin account without a password. To replace the admin passwords for all managed FortiSwitch units, use the following commands from FortiSwitch Manager:

```
config switch-controller switch-profile
   edit default
      set login-passwd-override {enable | disable}
      set login-passwd <password>
   next
end
```

If you had already applied a profile with the override enabled and the password set and then decide to remove the admin password, you need to apply a profile with the override enabled and no password set; otherwise, your previously set password will remain in the FortiSwitch. For example:

```
config switch-controller switch-profile
   edit default
      set login-passwd-override enable
      unset login-passwd
   next
end
```

Disabling the FortiSwitch console port login

Administrators can 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.

To change the FortiSwitch profile:

```
config switch-controller switch-profile
   edit {default | <FortiSwitch_profile_name>}
      set login {enable | disable} enabled by default
   end
```

To disable logging in to the managed FortiSwitch consort port in the default FortiSwitch profile:

```
config switch-controller switch-profile
   edit default
      set login disable
   end
```

To change which FortiSwitch profile is used by a managed switch

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set switch-profile {default | <FortiSwitch_profile_name>}
   end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      set switch-profile new_switch_profile
   end
```

Using automatic network detection and configuration

There are three commands that let you use automatic network detection and configuration.

To specify which policies can override the defaults for a specific ISL, ICl, or FortiLink interface:

```
config switch-controller auto-config custom
   edit <automatically configured FortiLink, ISL, or ICL interface name>
      config switch-binding
         edit "switch serial number"
            set policy "custom automatic-configuation policy"
         end
```

To specify policies that are applied automatically for all ISL, ICL, and FortiLink interfaces:

```
config switch-controller auto-config default
   set fgt-policy <default FortiLink automatic-configuration policy>
   set isl-policy <default ISL automatic-configuration policy>
   set icl-policy <default ICL automatic-configuration policy>
end
```

To specify policy definitions that define the behavior on automatically configured interfaces:

```
config switch-controller auto-config policy
   edit <policy_name>
      set qos-policy <automatic-configuration QoS policy>
      set storm-control-policy <automatic-configuation storm-control policy>
      set poe-status {enable | disable}
      set igmp-flood-report {enable | disable}
      set igmp-flood-traffic {enable | disable}
   end
```

Limiting the number of parallel processes for FortiSwitch configuration

Use the following CLI commands to reduce the number of parallel processes that the switch controller uses for configuring FortiSwitch units:

```
config global
   config switch-controller system
      set parallel-process-override enable
      set parallel-process <1-300>
   end
end
```

Configuring access to management and internal interfaces

The `set allowaccess` command configures access to all interfaces on a FortiSwitch unit. If you need to have different access to the FortiSwitch management interface and the FortiSwitch internal interface, you can set up a local-access security policy with the following commands:

```
config switch-controller security-policy local-access
   edit <policy_name>
      set mgmt-allowaccess {https | ping | ssh | snmp | http | telnet | radius-acct}
      set internal-allowaccess {https | ping | ssh | snmp | http | telnet | radius-acct}
   end
config switch-controller managed-switch
```

```
   edit <FortiSwitch_serial_number>
      set access-profile <name_of_policy>
   end
```

For example:

```
config switch-controller security-policy local-access
   edit policy1
      set mgmt-allowaccess https ping ssh radius-acct
      set internal-allowaccess https ssh snmp telnet
   end
config switch-controller managed-switch
   edit S524DF4K15000024
      set access-profile policy1
   end
```

Enabling VLAN optimization

When inter-switch links (ISLs) are automatically formed on trunks, the switch controller allows VLANs 1-4093 on ISL ports. This configuration can increase data processing on the FortiSwitch unit. When VLAN optimization is enabled, the FortiSwitch unit allows only user-defined VLANs on the automatically generated trunks.

NOTE: VLAN optimization is enabled by default.

To enable VLAN optimization on FortiSwitch units from FortiSwitch Manager:

```
config switch-controller global
   set vlan-optimization configured
end
```

NOTE: You cannot use the `set vlan-all-mode all` command with the `set vlan-optimization configured` command.

VLAN pruning

Starting in FortiSwitch Manager 7.2.5 with FortiSwitchOS 7.6.1, FortiSwitch Manager supports VLAN pruning. VLAN pruning prevents unnecessary traffic from unused VLANs by only allowing traffic from the VLANs required for the inter-switch link (ISL) trunks. This process makes networks more efficient and preserves bandwidth. In addition, VLAN pruning eliminates the time spent on manual VLAN pruning and reduces the chance of errors. By default, VLAN pruning is disabled.

To enable VLAN pruning in FortiSwitch Manager:

```
config switch-controller global
   set vlan-optimization prune
end
```

To disable VLAN pruning in FortiSwitch Manager:

```
config switch-controller global
   set vlan-optimization {configured | none}
end
```

To display all VLANs learned using VLAN pruning on a FortiSwitch unit:

```
diagnose switch vlan-pruning dynamic-vlan list [<interface_name>]
```

For example:

```
diagnose switch vlan-pruning dynamic-vlan list port10
```

Although FortiSwitch Manager leverages the Generic VLAN Registration Protocol (GVRP) message format to exchange internal control packets for the VLAN-pruning feature, the firmware is currently not fully compliant with the IEEE 802.1r-based standard GVRP specification.

To display the received and transmitted counters with GVRP-formatted messages on a FortiSwitch unit:

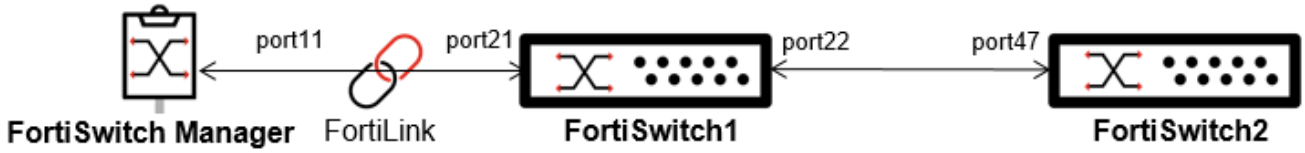
```
diagnose switch vlan-pruning protocol-packet stats [<interface_name>]
```

For example:

```
FS1E48T422005187 # diagnose switch vlan-pruning protocol-packet stats
Receive(RX) and transmit(TX) counters for GVRP vlan states
RX: JE JI LE LI LA E
TX: JE JI LE LI LA E
JE: JoinEmpty JI: JoinIn LE: LeaveEmpty
LI: LeaveIn LA: LeaveAll E: Empty
```

Configuration example

In the following example, FortiSwitch Manager manages two FortiSwitch units.



1. Configure the native VLAN on the managed FortiSwitch port. FortiSwitch1 has vlan1 and vlan11, and FortiSwitch2 has vlan11

```
config switch interface
   edit port21
      set native-vlan vlan1
   next
end

config switch interface
   edit port22
      set native-vlan vlan11
   next
end

config switch interface
   edit port47
      set native-vlan vlan11
   next
```

```
end
```

2. Enable VLAN pruning on FortiSwitch Manager.

```
FGT_A (vdom1) (Interim)# config switch-controller global
FGT_A (global) (Interim)# set vlan-optimization prune
FGT_A (global) (Interim)# end
```

3. Check VLAN pruning on the FortiSwitch1 auto-generated trunk interface. Only vlan11 and vlan4093 (the quarantine VLAN configured in the `set allowed-vlans` command on all FortiSwitch ports) are allowed, and vlan1 is not.

```
config switch trunk
   edit "8EPTF18001384-0"
      set mode lacp-active
      set auto-isl 1
      set members "port22"
   next
end

S524DN4K16000116 # diagnose switch vlan-pruning dynamic-vlan list 8EPTF18001384-0
8EPTF18001384-0 :
vlans  : 11 4093
```

Grouping FortiSwitch units

You can simplify the configuration and management of complex topologies by creating FortiSwitch groups. A group can include one or more FortiSwitch units and you can include different models in a group.

Using the GUI:

1. Go to *Switch Controller* > *Managed FortiSwitch*.
2. Select *Create New* > *FortiSwitch Group*.
3. In the Name field, enter a name for the FortiSwitch group.
4. In the Members field, click + to select which switches to include in the FortiSwitch group.
5. In the Description field, enter a description of the FortiSwitch group.
6. Select *OK*.

Using the CLI:

```
config switch-controller switch-group
   edit <name>
      set description <string>
      set members <serial-number> <serial-number> ...
      end
   end
```

Grouping FortiSwitch units allows you to restart all of the switches in the group instead of individually. For example, you can use the following command to restart all of the FortiSwitch units in a group named `my-sw-group`:

```
execute switch-controller switch-action restart delay switch-group my-sw-group
```

Upgrading the firmware of FortiSwitch groups is easier, too, because fewer commands are needed. See the next section for the procedure.

Improving the FortiSwitch Manager connection

Starting in FortiSwitch Manager 7.2.5, there are two CLI commands under `config switch-controller system` to improve the FortiSwitch Manager connection:

- Use the `set caputp-echo-interval <8-600>` command to set the interval for the Control and Provisioning of Unified Termination Points (CAPUTP) ECHO requests from the Scheduling Wide-area Transport Protocol (SWTP). The default value is 30 seconds. Setting the interval to a shorter time means that an offline device is detected quicker.
- Use the `set caputp-max-retransmit <0-64>` command to set the maximum number of times that CAPUTP tunnel packets are retransmitted. The default value is 4. Setting the retransmission times to a lower number causes the CAPUTP daemon to time out sooner and then restart for faster failover.

Configuring FortiSwitch VLANs and ports

This section covers the following topics:

Configuring VLANs

Use Virtual Local Area Networks (VLANs) to logically separate a LAN into smaller broadcast domains. VLANs allow you to define different policies for different types of users and to set finer control on the LAN traffic. (Traffic is only sent automatically within the VLAN. You must configure routing for traffic between VLANs.)

From FortiSwitch Manager, you can centrally configure and manage VLANs for the managed FortiSwitch units.

The FortiSwitch unit supports untagged and tagged frames in FortiLink mode. The switch supports up to 1,023 user-defined VLANs. You can assign a VLAN number (ranging from 1-4095) to each of the VLANs. For FortiSwitch units in FortiLink mode, you can assign a name to each VLAN.

You can configure the default VLAN for each FortiSwitch port as well as a set of allowed VLANs for each FortiSwitch port.

This section covers the following topics:

Creating VLANs

Setting up a VLAN requires you to create the VLAN and assign FortiSwitch ports to the VLAN. You can do this with either the Web GUI or CLI.

Using the GUI

To create the VLAN:

1. Go to *Switch Controller* > *FortiSwitch VLANs*, click *Create New*, and change the following settings:

Name	VLAN name
VLAN ID	Enter a number (1-4094)
Color	Choose a unique color for each VLAN, for ease of visual display.
Role	Select *LAN*, *WAN*, *DMZ*, or *Undefined*.

2. Enable *DHCP* for IPv4 or IPv6.
3. Set the *Administrative Access* options as required.
4. Click *OK*.

To assign FortiSwitch ports to the VLAN:

1. Go to *Switch Controller* > *FortiSwitch Ports*.
2. Click a port row.
3. Click the pencil icon in the *Native VLAN* column to change the native VLAN.
4. Select a VLAN from the displayed list and then click *Apply*. The new value is assigned to the selected ports.
5. Click the pencil icon in the *Allowed VLANs* column to change the allowed VLANs.
6. Select one or more of the VLANs (or *All*) from the displayed list and then click *Apply*. The new value is assigned to the selected port.

Using the FortiSwitch CLI

1. Create the marketing VLAN.

```
config system interface
   edit <VLAN_name>
      set vlanid <1-4094>
      set color <1-32>
      set interface <FortiLink-enabled interface>
      set vdom <VDOM_name>
   end
```

2. Set the VLAN's IP address.

```
config system interface
   edit <VLAN_name>
      set ip <IP_address> <network_mask>
   end
```

3. Enable a DHCP Server.

```
config system dhcp server
   edit 1
      set default-gateway <IP address>
      set dns-service default
```

```
      set interface <vlan name>
         config ip-range
            set start-ip <IP address>
            set end-ip <IP address>
         end
      set netmask <Network mask>
   end
```

4. Assign ports to the VLAN.

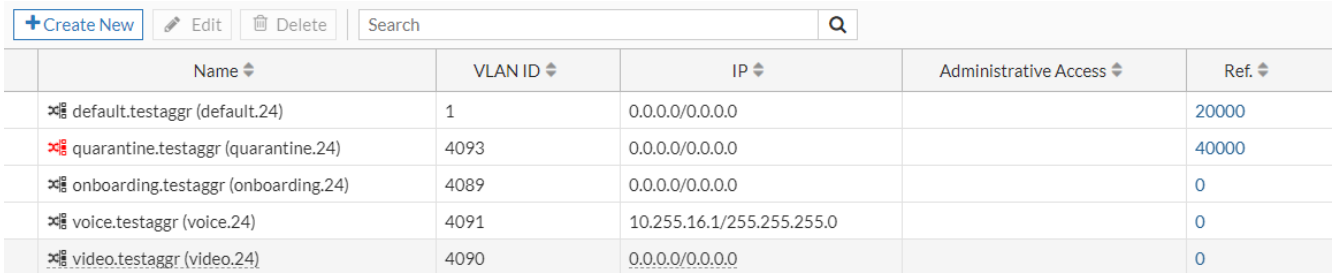
```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port name>
            set vlan <vlan name>
            set allowed-vlans <vlan name>
            or
            set allowed-vlans-all enable
         next
      end
   end
```

5. Assign untagged VLANs to a managed FortiSwitch port:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port>
            set untagged-vlans <VLAN-name>
         next
      end
   next
end
```

Viewing FortiSwitch VLANs

The *Switch Controller* > *FortiSwitch VLANs* page displays VLAN information for the managed switches.



Name	VLAN ID	IP	Administrative Access	Ref.
default.testaggr (default.24)	1	0.0.0.0/0.0.0.0		20000
quarantine.testaggr (quarantine.24)	4093	0.0.0.0/0.0.0.0		40000
onboarding.testaggr (onboarding.24)	4089	0.0.0.0/0.0.0.0		0
voice.testaggr (voice.24)	4091	10.255.16.1/255.255.255.0		0
video.testaggr (video.24)	4090	0.0.0.0/0.0.0.0		0

Each entry in the VLAN list displays the following information:

- *Name*—name of the VLAN
- *VLAN ID*—the VLAN number
- *IP*—address and mask of the subnetwork that corresponds to this VLAN
- *Administrative Access*—administrative access settings for the VLAN
- *Ref.*—number of configuration objects referencing this VLAN

Configuring ports using the GUI

You can use the *Switch Controller* > *FortiSwitch Ports* page to do the following with FortiSwitch switch ports:

- Set the native VLAN and add more VLANs
- Edit the description of the port
- Enable or disable the port
- Set the access mode of the port in *Port* view:
  - *Static*—The port does not use a dynamic port policy or FortiSwitch network access control (NAC) policy.
  - *Assign Port Policy*—The port uses a dynamic port policy.
  - *NAC*—The port uses a FortiSwitch NAC policy.
- Set the LACP mode of the trunk in *Trunk* view:
  - *Static*—In this mode, no control messages are sent, and received control messages are ignored.
  - *Passive LACP*—The port passively uses LACP to negotiate 802.3ad aggregation.
  - *Active LACP*—The port actively used LACP to negotiate 802.3ad aggregation.
- Double-click a port to display the *Port Statistics* pane, 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.
- Clear port counters by right-clicking a port and selecting *Clear port counters*.
- Enable or disable PoE for the port
- Enable or disable DHCP snooping (if supported by the port)
- Enable or disable whether a port is an edge port
- Enable or disable STP (if supported by the port)
- Enable or disable loop guard (if supported by the port)
- Enable or disable STP BPDU guard (if supported by the port)
- Enable or disable STP root guard (if supported by the port)

Configuring port speed and status

To set port speed and other base port settings:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set description <text>
            set speed <speed>
            set status {down | up}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
```

```
            set description "First port"
            set speed auto
            set status up
        end
    end
```

To check the port properties:

```
diagnose switch-controller switch-info port-properties [<FortiSwitch_serial_number>] [<port_
    name>]
```

If the FortiSwitch serial number is not specified, results for all FortiSwitch units are returned. If the port name is not specified, results for all ports are returned.

For example:

```
FSWMVMTM21000005 (vdom1) # diagnose switch-controller switch-info port-properties
S108DVTM20002500 port2

Switch: S108DVTM20002500
Port: port2
PoE           :
Connector     : RJ45
Speed         :
```

Configuring flap guard

A flapping port is a port that changes status rapidly from up to down. A flapping port can create instability in protocols such as Spanning Tree Protocol (STP). If a port is flapping, STP must continually recalculate the role for each port. Flap guard also prevents unwanted access to the physical ports.

Flap guard detects how many times a port changes status during a specified number of seconds, and the system shuts down the port if necessary. You can manually reset the port and restore it to the active state.

Flap guard is configured and enabled on each port through the switch controller. The default setting is disabled.

The flap rate counts how many times a port changes status during a specified number of seconds. The range is 1 to 30 with a default setting of 5.

The flap duration is the number of seconds during which the flap rate is counted. The range is 5 to 300 seconds with a default setting of 30 seconds.

The flap timeout is the number of minutes before the flap guard is reset. The range is 0 to 120 minutes. The default setting of 0 means that there is no timeout.

- If a triggered port times out while the switch is in a down state, the port is initially in a triggered state until the switch has fully booted up and calculated that the timeout has occurred.
- The following models do not store time across reboot; therefore, any triggered port is initially in a triggered state until the switch has fully booted up—at which point the trigger is cleared:
  - FS-1xxE
  - FS-2xxD/E
  - FS-4xxD
  - FS-4xxE

To configure flap guard on a port through the switch controller:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set flapguard {enable | disable}
            set flap-rate <1-30>
            set flap-duration <5-300 seconds>
            set flap-timeout <0-120 minutes>
         next
      end
   end
```

For example:

```
config switch-controller managed-switch
   edit S424ENTF19000007
      config ports
         edit port10
            set flapguard enable
            set flap-rate 15
            set flap-duration 100
            set flap-timeout 30
         next
      end
   end
```

Resetting a port

After flap guard detects that a port is changing status rapidly and the system shuts down the port, you can reset the port and restore it to service.

To reset a port:

```
execute switch-controller flapguard reset <FortiSwitch_serial_number> <port_name>
```

For example:

```
execute switch-controller flapguard reset S424ENTF19000007 port10
```

Configuring PoE

This section covers the following topics:

Enabling PoE on the port

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set poe-status {enable | disable}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set poe-status enable
         end
      end
```

Enabling PoE pre-standard detection

Depending on the FortiSwitch model, you can manually change the PoE pre-standard detection setting on the global level or on the port level. The factory default setting for `poe-pre-standard-detection` is `disable`.

PoE pre-standard detection is a global setting for the following FortiSwitch models: FSR-112D-POE, FS-548DFPOE, FS-524D-FPOE, FS-108D-POE, FS-224D-POE, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, and FS-124EFPOE. For the other FortiSwitch PoE models, PoE pre-standard detection is set on each port.

On the global level, set `poe-pre-standard-detection` with the following commands:

```
config switch-controller managed-switch
       edit <FortiSwitch_serial_number>
               set poe-pre-standard-detection {enable | disable}
       next
end
```

On the port level, set `poe-pre-standard-detection` with the following commands:

```
config switch-controller managed-switch
       edit <FortiSwitch_serial_number>
               config ports
                       edit <port_name>
                               set poe-pre-standard-detection {enable | disable}
                       next
               end
       next
end
```

Configuring PoE port settings

Starting in FortiSwitch Manager 7.2.2, you can configure the following PoE port settings on managed switches:

- Port mode—You can set the port mode to IEEE802.3 AF, IEEE802.3 AT, or IEEE802.3 BT.
- Port priority—You can set the port priority to critical, high, medium, or low. If there is not enough power, power is allotted first to critical-priority ports, then to high-priority ports, then to medium-priority ports, and then to low-priority ports. Medium priority is available only on the following models: FS-224D-FPOE, FS-224E-POE, FS-248E-POE, FS-248E-FPOE, FS-424E-POE, FS-424E-FPOE, FS-M426E-FPOE, FS-448E-POE, FS-448E-FPOE, FS-524DFPOE, and FS-548D-FPOE.
- Port power—You can set the port to use normal, power, perpetual power, or perpetual-fast power. Refer to the FortiSwitchOS feature matrix to see which FortiSwitch models support this feature.

Port power setting	Description
normal	PoE power is not provided while a switch restarts.
perpetual	PoE power is provided during a soft reboot (switch is restarted while powered up).
perpetual-fast	PoE power is provided during a hard reboot (the switch's power is physically turned off and then on again).

To configure the PoE port settings:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set poe-port-mode {ieee802-3af | ieee802-3at | ieee802-3bt}
            set poe-port-priority {critical-priority | high-priority | low-priority | medium-
                 priority}
            set poe-port-power {normal | perpetual | perpetual-fast}
         next
      end
   next
end
```

Resetting the PoE port

Power over Ethernet (PoE) describes any system that passes electric power along with data on twisted pair Ethernet cabling. Doing this allows a single cable to provide both data connection and electric power to devices (for example,

wireless access points, IP cameras, and VoIP phones).

The following command resets PoE on the port:

```
execute switch-controller poe-reset <FortiSwitch_serial_number> <port_name>
```

Displaying general PoE status

```
get switch-controller poe <FortiSwitch_serial_number> <port_name>
```

The following example displays the PoE status for port 6 on the specified switch:

```
# get switch-controller poe FS108D3W14000967 port6
Port(6) Power:3.90W, Power-Status: Delivering Power
Power-Up Mode: Normal Mode
Remote Power Device Type: IEEE802.3AT PD
Power Class: 4
Defined Max Power: 30.0W, Priority:3
Voltage: 54.00V
Current: 78mA
```

Adding 802.3ad link aggregation groups (trunks)

If the trunk is in LACP mode and has ports with different speeds, the ports of the same negotiated speed are grouped in an aggregator.

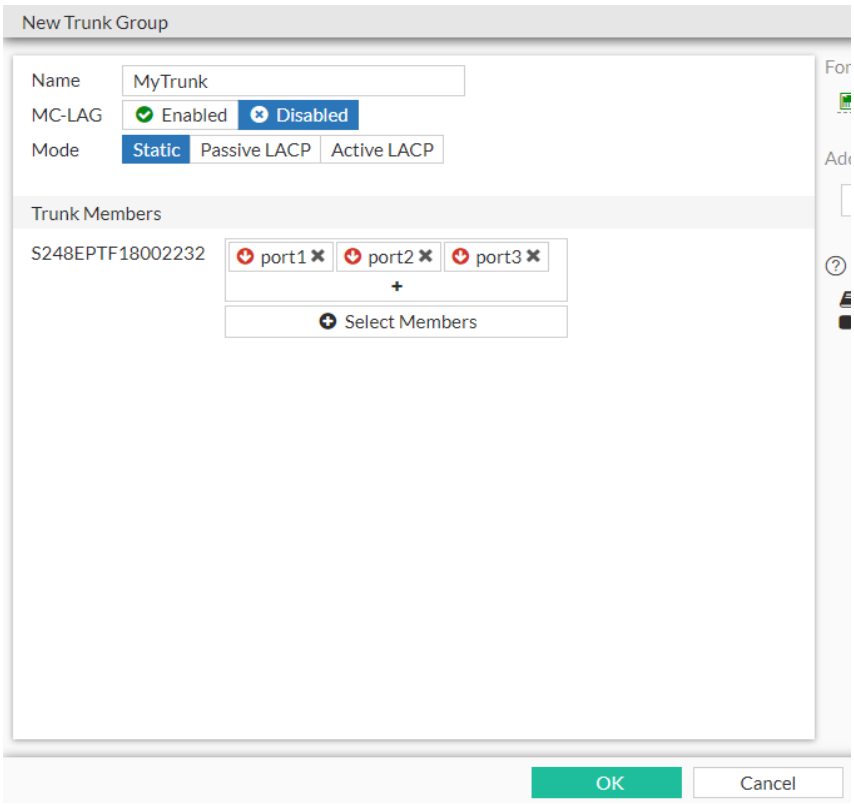
If multiple aggregators exist, one and only one of the aggregators is used by the trunk.

You can use the CLI to specify how the aggregator is selected:

- When the `aggregator-mode` is set to `bandwidth`, the aggregator with the largest bandwidth is selected. This mode is the default.
- When the `aggregator-mode` is set to `count`, the aggregator with the largest number of ports is selected.

Using the FortiSwitch Manager GUI:

1. Go to *Switch Controller* > *FortiSwitch Ports*.
2. Click *Create New* > *Trunk Group*.
3. In the *New Trunk Group* page, enter a *Name* for the trunk group.
4. Select *Enabled* or *Disabled* for the MCLAG.
   - An MCLAG peer group must be configured before adding a trunk with MCLAG enabled.
   - Make sure to select ports from switches that are part of the same MCLAG peer group.
5. Select the *Mode*: Static, Passive LACP, or Active LACP.
6. Select two or more physical ports to add to the trunk group and then click *Apply*.
7. Click *OK*.

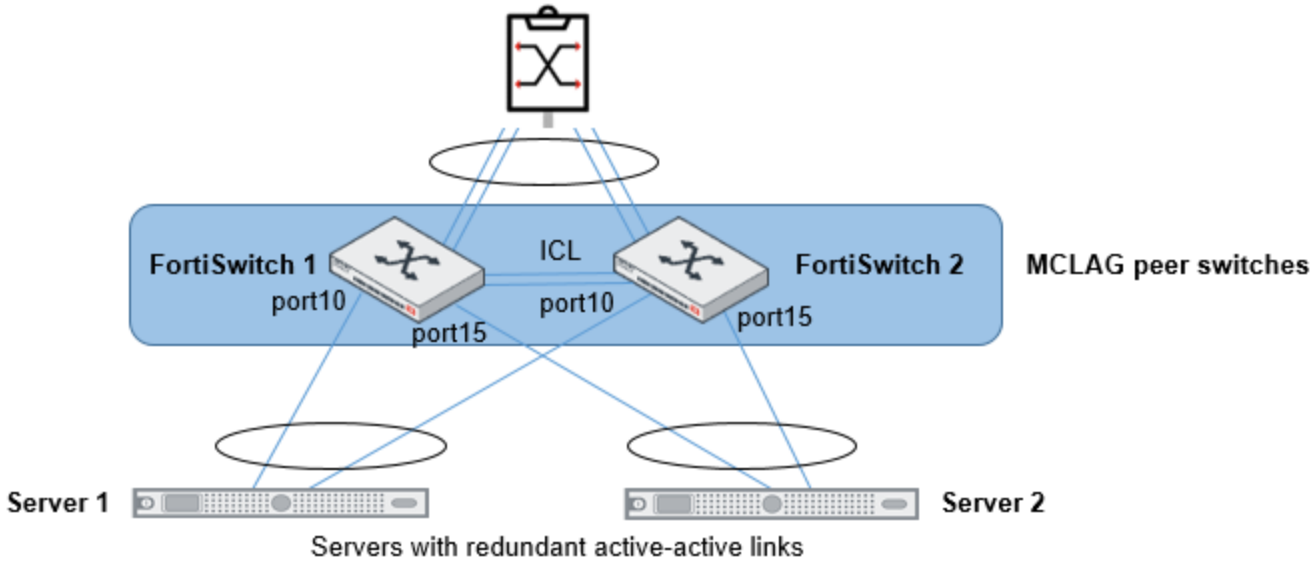


Using the FortiSwitch Manager CLI:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <trunk_name>
            set type trunk
            set mode {static | lacp-passive | lacp-active}
            set mclag {enable | disable}
            set bundle {enable | disable}
            set min-bundle <int>
            set max-bundle <int>
            set members <port1 port2 ...>
         next
      end
   end
end
```

MCLAG trunks

The MCLAG trunk consists of 802.3ad link aggregation groups with members that belong to different FortiSwitch units. To configure an MCLAG trunk, you need an MCLAG peer group. The MCLAG trunk members are selected from the same MCLAG peer group.



Using the GUI

1. Go to *Switch Controller* > *FortiSwitch Ports*.
2. Select *Create New* > *Trunk Group*.
3. Enter a name for the MCLAG trunk.
4. For the MCLAG status, select *Enabled* to create an active MCLAG trunk.
5. For the mode, select *Static*, *Passive LACP*, or *Active LACP*.
   - Set to *Static* for static aggregation. In this mode, no control messages are sent, and received control messages are ignored.
   - Set to *Passive LACP* to passively use LACP to negotiate 802.3ad aggregation.
   - Set to *Active LACP* to actively use LACP to negotiate 802.3ad aggregation.
6. For trunk members, click *Select Members*, select the ports to include in the MCLAG trunk, and then click *Apply* to save the trunk members. **NOTE:** The members must belong to the same MCLAG peer group.
7. Select *OK* to save the MCLAG configuration.
   The ports are listed as part of the MCLAG trunk on the *FortiSwitch Ports* page.

Using the CLI

Configure a trunk in each switch that is part of the MCLAG pair:

- The trunk name for each switch must be the same.
- The port members for each trunk can be different.
- After you enable MCLAG, you can enable LACP if needed.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit "<trunk name>"
            set type trunk
            set mode {static | lacp-passive | lacp-active}
            set members "<port>,<port>"
            set mclag enable
         next
```

```
    end
  next
```

Variable	Description	Default
<switch-id>	FortiSwitch serial number.	No default
<trunk name>	Enter a name for the MCLAG trunk. **NOTE:** Each FortiSwitch unit that is part of the MCLAG must have the same MCLAG trunk name configured.	No default
type trunk	Set the interface type to a trunk port.	physical
mode {static | lacp-passive | lacp-active}	Set the LACP mode. • Set to `static` for static aggregation. In this mode, no control messages are sent, and received control messages are ignored. • Set to `lacp-passive` to passively use LACP to negotiate 802.3ad aggregation. • Set to `lacp-active` to actively use LACP to negotiate 802.3ad aggregation.	lacp-active
members "<port>,<port>"	Set the aggregated LAG bundle interfaces.	No default
mclag enable	Enable or disable the MCLAG.	disable

LACP fallback mode

Starting in FortiSwitch Manager 7.2.5, LACP fallback mode is supported in the CLI. LACP fallback mode allows a selected port to stay up so that a device not running LACP can still connect to the network. LACP fallback mode is useful if you have a preboot execution environment (PXE) and need to download an image from the network before running LACP in active mode.

When you select the fallback port for a switch trunk, the aggregate interface will use the LACP fallback mode if the trunk does not receive any LACP protocol data units (PDUs). The fallback port is set to up, and all other ports are blocked. When the trunk starts receiving LACP PDUs again, the switch trunk changes from fallback mode to LACP active mode.

When the switch trunk is running LACP in active mode and stops receiving LACP PDUs:

- There is a 90-second delay before LACP fallback mode if the `lacp-speed` for the switch trunk is set to slow.
- There is a 30-second delay before LACP fallback mode if the `lacp-speed` for the switch trunk is set to fast.

The following are the requirements and limitations for LACP fallback mode:

- The switch trunk must be running in `lacp-active` mode.
- If you are using MCLAG, do not configure fallback mode on more than one MCLAG switch. If you configure fallback mode on both MCLAG switches, the `diagnose switch mclag peer-consistency-check` command will report it as a mismatch.
- You cannot use fallback mode with the `min_bundle` or `max_bundle` setting.
- You cannot use fallback mode with an MCLAG split-brain state.

To configure LACP fallback mode:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set type trunk
            set mode lacp-active
            set members <port_name_1> <port_name_2> ...
            set fallback-port <port_name>
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit "first-mclag"
            set vlan "_default.39"
            set allowed-vlans "quarantine.39"
            set untagged-vlans "quarantine.39"
            set type trunk
            set mac-addr 80:80:2c:a3:c5:58
            set mode lacp-active
            set mclag enable
            set members "port7" "port8"
            set fallback-port "port8"
         next
      end
   next
end
```

Configuring FortiSwitch split ports (phy-mode) in FortiLink mode

On FortiSwitch models that provide 40G/100G QSFP (quad small form-factor pluggable) interfaces, you can install a breakout cable to convert one 40G/100G interface into four 10G/25G interfaces. See the list of supported FortiSwitch models in the notes in this section.

This section covers the following topics:

Notes

- Split ports are not configured for pre-configured FortiSwitch units.
- Splitting ports is supported on the following FortiSwitch models:
  - FS-3032D (ports 5 to 28 are splittable)
  - FS-3032E (Ports can be split into 4 x 25G when configured in 100G QSFP28 mode or can be split into 4 x 10G when configured in 40G QSFP mode. Use the `set <port_name>-phy-mode disabled command` to disable some 100G ports to allow up to sixty-two 100G/25G/10G ports.)
  - FS-524D and FS-524D-FPOE (ports 29 and 30 are splittable)
  - FS-548D and FS-548D-FPOE (ports 53 and 54 are splittable)
  - FS-1048E (In the 4 x 100G configuration, ports 49, 50, 51, and 52 are splittable as 4 x 25G. In the 6 x 40G configuration, ports 49, 50, 51, 52, 53, 54 are splittable as 4 x 10G.)

  Use the `set port-configuration ?` command to check which ports are supported for each model.
- Currently, the maximum number of ports supported in software is 64 (including the management port). Therefore, only 10 QSFP ports can be split. This limitation applies to all of the models, but only the FS-3032D, FS-3032E, and the FS-1048E models have enough ports to encounter this limit.
- Use `10000full` for the general 10G interface configuration. If that setting does not work, use `10000cr` for copper connections (with copper cables such as 10GBASE-CR) or use `10000sr` for fiber connections (fiber optic transceivers such as 10GBASE-SR/-LR/-ER/-ZR).
- FortiSwitch Manager 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.

Configuring split ports on a previously discovered FortiSwitch unit

1. On the FortiSwitch unit, configure the split ports. See Configuring a split port on the FortiSwitch unit on page 55.
2. Restart the FortiSwitch unit.

Configuring split ports with a new FortiSwitch unit

1. Discover the FortiSwitch unit.
2. Authorize the FortiSwitch unit.
3. On the FortiSwitch unit, configure the split ports. See Configuring a split port on the FortiSwitch unit on page 55.
4. Restart the FortiSwitch unit.

Configuring forward error correction on switch ports

Supported managed-switch ports of the FS-1048E and FS-3032E can be configured with a forward error correction (FEC) state of Clause 74 FC-FEC for 25-Gbps ports and Clause 91 RS-FEC for 100-Gbps ports.

Starting in FortiSwitch Manager 7.2.4, when a managed FortiSwitch unit is capable of FEC, the default setting for `fec-state` is `detect-by-module`, which automatically detects whether FEC is supported by the module.

```
config switch-controller managed-switch
       edit <FortiSwitch_serial_number>
              config ports
                     edit <port_name>
                            set fec-capable {0 | 1}
                            set fec-state {cl74 | cl91 | detect-by-module | disabled}
```

```
                        next
                end
        next
end
```

`fec-capable {0 | 1}`	Set whether the port is FEC capable. • `0`: The port is not FEC capable. • `1`: The port is FEC capable.
`fec-state {cl74 | cl91 | detect-by-module | disabled}`	Set the FEC state: • `cl74`: Enable Clause 74 FC-FEC. This option is only available for on FS-1048E and FS-3032E ports that have been split to 4x25G. • `cl91`: Enable Clause 91 RS-FEC. This option is only available for on FS-1048E and FS-3032E ports that have been split to 4x100G. • `detect-by-module`: Automatically detect whether FEC is supported by the module. • `disabled`: Disable FEC on the port.

In this example, a managed FortiSwitch FS-3032E is configured with Clause 74 FC-FEC on port 16.1 and Clause 91 RS-FEC on port 8.

```
config switch-controller managed-switch
        edit FS3E32T419000000
                config ports
                        edit port16.1
                                set fec-state cl74
                        next
                        edit port8
                                set fec-state cl91
                        next
                end
        next
end
```

Configuring a split port on the FortiSwitch unit

To configure a split port:

```
config switch phy-mode
   set port-configuration <default | disable-port54 | disable-port41-48 | 4x100G | 6x40G |
        4x4x25G}
   set {<port-name>-phy-mode <single-port| 4x25G | 4x10G | 4x1G | 2x50G}
   ...
   (one entry for each port that supports split port)
end
```

The following settings are available:

- `disable-port54`—For 548D and 548D-FPOE, only port53 is splittable; port54 is unavailable.
- `disable-port41-48`—For 548D and 548D-FPOE, port41 to port48 are unavailable, but you can configure port53 and port54 in split-mode.
- `4x100G`—For 1048E, enable the maximum speed (100G) of ports 49 through 52. Ports 53 and 54 are disabled.
- `6x40G`—For 1048E, enable the maximum speed (40G) of ports 49 through 54.

- `4x4x25G`—For 1048E, enable the maximum speed (100G) of ports 49 through 52; each split port has a maximum speed of 25G. Ports 47 and 48 are disabled.
- `single-port`—Use the port at the full base speed without splitting it.
- `4x25G`—For 100G QSFP only, split one port into four subports of 25 Gbps each.
- `4x10G`—For 40G or 100G QSFP only, split one port into four subports of 10Gbps each.
- `4x1G`—For 40G or 100G QSFP only, split one port into four subports of 1 Gbps each.
- `2x50G`—For 100G QSFP only, split one port into two subports of 50 Gbps each.

In the following example, a FortiSwitch 3032D is configured with ports 10, 14, and 28 set to 4x10G:

```
config switch phy-mode
   set port5-phy-mode 1x40G
   set port6-phy-mode 1x40G
   set port7-phy-mode 1x40G
   set port8-phy-mode 1x40G
   set port9-phy-mode 1x40G
   set port10-phy-mode 4x10G
   set port11-phy-mode 1x40G
   set port12-phy-mode 1x40G
   set port13-phy-mode 1x40G
   set port14-phy-mode 4x10G
   set port15-phy-mode 1x40G
   set port16-phy-mode 1x40G
   set port17-phy-mode 1x40G
   set port18-phy-mode 1x40G
   set port19-phy-mode 1x40G
   set port20-phy-mode 1x40G
   set port21-phy-mode 1x40G
   set port22-phy-mode 1x40G
   set port23-phy-mode 1x40G
   set port24-phy-mode 1x40G
   set port25-phy-mode 1x40G
   set port26-phy-mode 1x40G
   set port27-phy-mode 1x40G
   set port28-phy-mode 4x10G
end
```

The system applies the configuration only after you enter the `end` command, displaying the following message:

```
This change will cause a ports to be added and removed, this will cause loss of
     configuration on removed ports. The system will have to reboot to apply this change.
Do you want to continue? (y/n)y
```

To configure one of the split ports, use the notation ".x" to specify the split port:

```
config switch physical-port
   edit "port1"
      set lldp-profile "default-auto-isl"
      set speed 40000full
   next
   edit "port2"
      set lldp-profile "default-auto-isl"
      set speed 40000full
   next
   edit "port3"
      set lldp-profile "default-auto-isl"
      set speed 40000full
```

```
    next
    edit "port4"
      set lldp-profile "default-auto-isl"
      set speed 40000full
    next
    edit "port5.1"
      set speed 10000full
    next
    edit "port5.2"
      set speed 10000full
    next
    edit "port5.3"
      set speed 10000full
    next
    edit "port5.4"
      set speed 10000full
    next
end
```

Restricting the type of frames allowed through IEEE 802.1Q ports

You can now specify whether each FortiSwitch port discards tagged 802.1Q frames or untagged 802.1Q frames or allows all frames access to the port. By default, all frames have access to each FortiSwitch port.

Use the following CLI commands:

```
config switch-controller managed-switch <SN>
   config ports
      edit <port_name>
         set discard-mode <none | all-tagged | all-untagged>
      next
   next
end
```

Configuring switching features

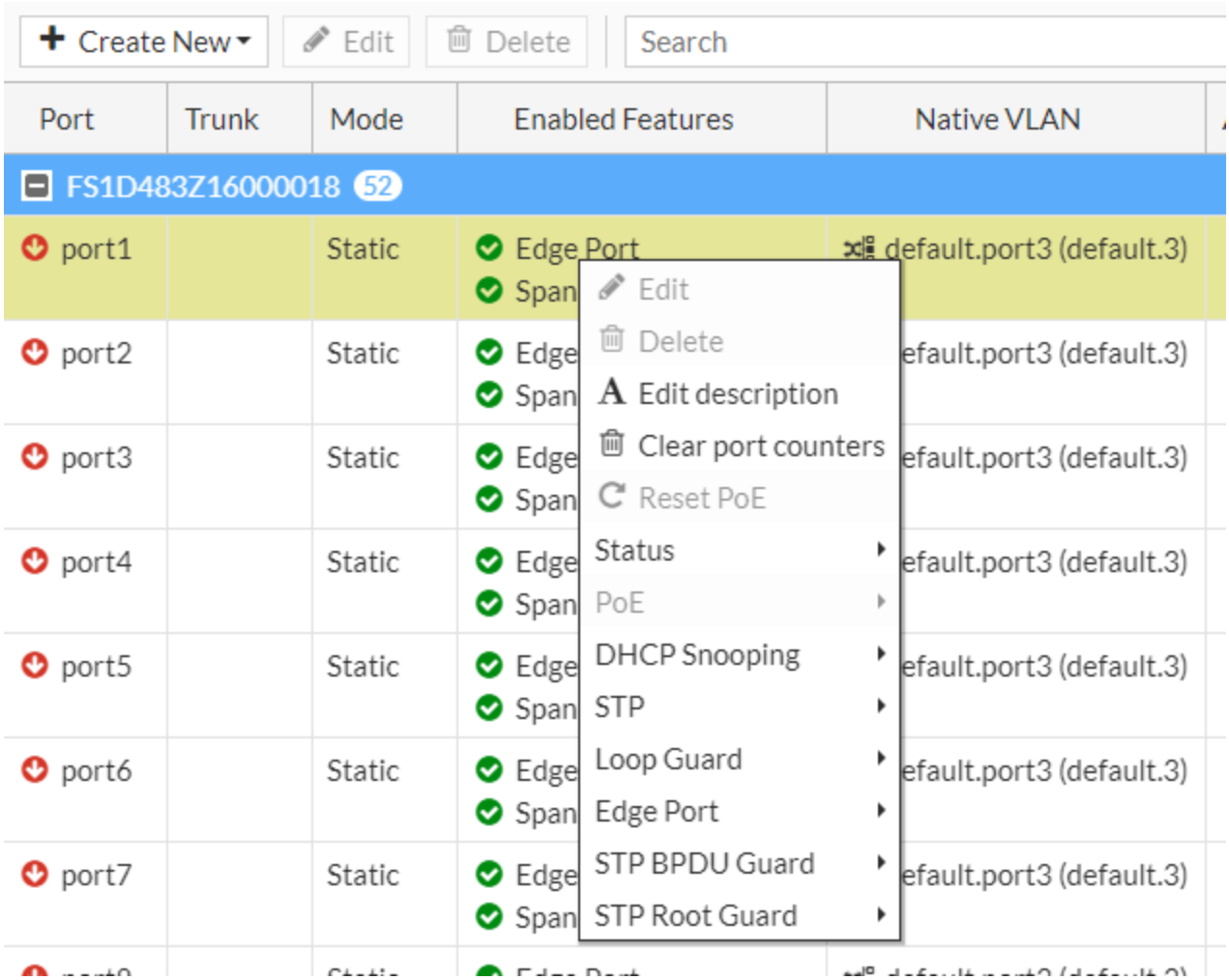
This section covers the following features:

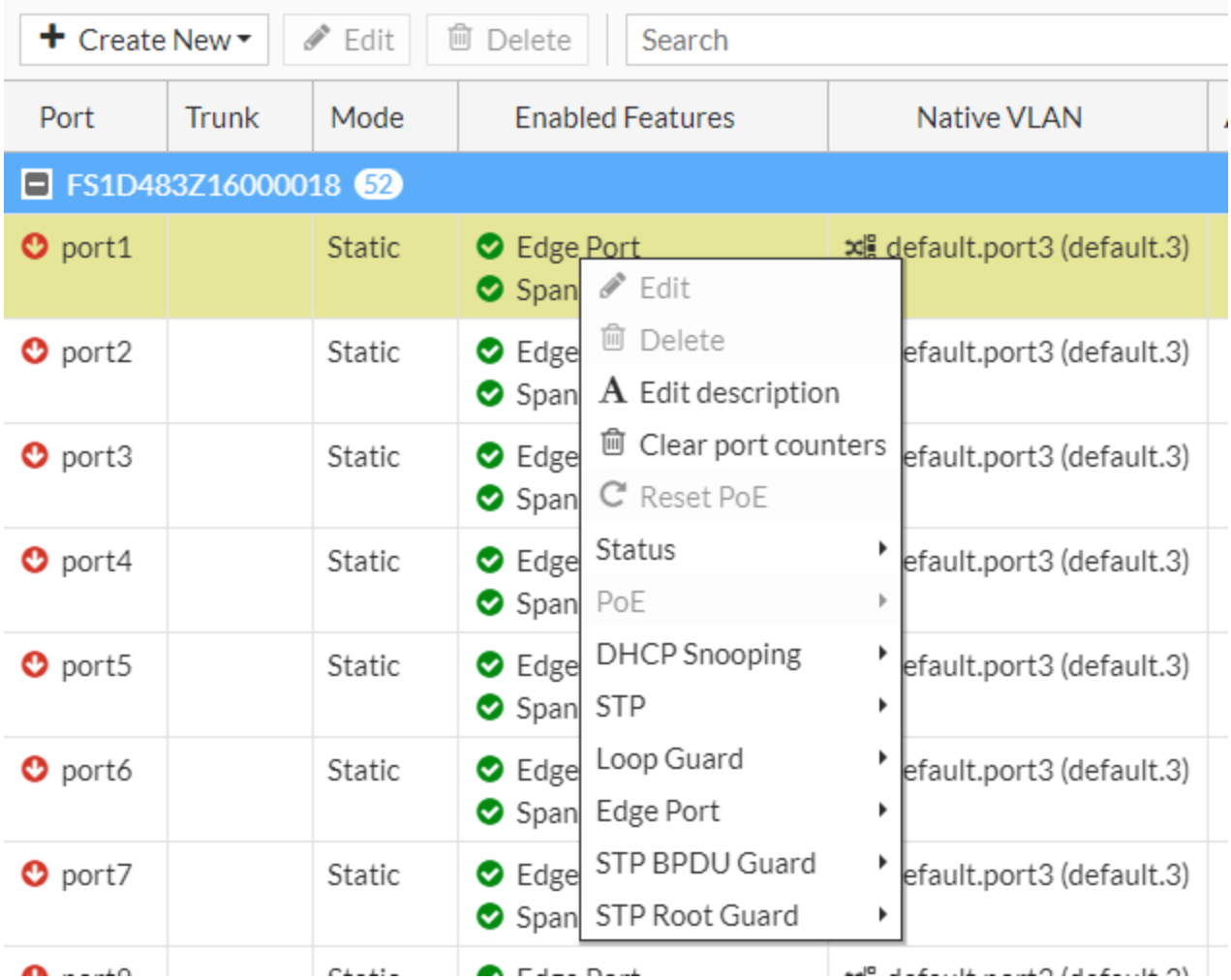
Configuring DHCP blocking, STP, and loop guard on managed FortiSwitch ports

Go to *Switch Controller* > *FortiSwitch Ports*. Right-click any port and then enable or disable the following features:

- *DHCP Snooping*—The DHCP blocking feature monitors the DHCP traffic from untrusted sources (for example, typically host ports and unknown DHCP servers) that might initiate traffic attacks or other hostile actions. To prevent this, DHCP blocking filters messages on untrusted ports.
- *Spanning Tree Protocol (STP)*—STP is a link-management protocol that ensures a loop-free layer-2 network topology.
- *Loop guard*—A loop in a layer-2 network results in broadcast storms that have far-reaching and unwanted effects. Fortinet loop guard helps to prevent loops. When loop guard is enabled on a switch port, the port monitors its subtending network for any downstream loops. The loop guard feature is designed to work in concert with STP rather than as a replacement for STP.
- *STP BPDU guard*—Similar to root guard, BPDU guard protects the designed network topology. When BPDU guard is enabled on STP edge ports, any BPDUs received cause the ports to go down for a specified number of minutes. The BPDUs are not forwarded, and the network edge is enforced.
- *STP root guard*—Root guard protects the interface on which it is enabled from becoming the path to root. When enabled on an interface, superior BPDUs received on that interface are ignored or dropped. Without using root guard, any switch that participates in STP maintains the ability to reroute the path to root. Rerouting might cause your network to transmit large amounts of traffic across suboptimal links or allow a malicious or misconfigured device to pose a security risk by passing core traffic through an insecure device for packet capture or inspection. By enabling root guard on multiple interfaces, you can create a perimeter around your existing paths to root to enforce the specified network topology.

STP and IGMP snooping are enabled on all ports by default. Loop guard is disabled by default on all ports.


Create New
Edit
Delete
Search
Port
Trunk
Mode
Enabled Features
Native VLAN
FS1D483Z16000018 52
port1
Static
Edge Port
default.port3 (default.3)
port2
port3
port4
port5
port6
port7
Edit
Delete
Edit description
Clear port counters
Reset PoE
Status
PoE
DHCP Snooping
STP
Loop Guard
Edge Port
STP BPDU Guard
STP Root Guard



Configuring edge ports

Use the following commands to enable or disable an interface as an edge port:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set edge-port {enable | disable}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set edge-port enable
         end
```

```
    end
```

Configuring loop guard

A loop in a layer-2 network results in broadcast storms that have far-reaching and unwanted effects. Fortinet loop guard helps to prevent loops. When loop guard is enabled on a switch port, the port monitors its subtending network for any downstream loops. Loop guard and STP should be used separately for loop protection. By default, loop guard is disabled on all ports.

Use the following commands to configure loop guard on a FortiSwitch port:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set loop-guard {enabled | disabled}
            set loop-guard-timeout <0-120 minutes>
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set loop-guard enabled
            set loop-guard-timeout 10
         end
      end
```

Configuring STP settings

The managed FortiSwitch unit supports Spanning Tree Protocol (a link-management protocol that ensures a loop-free layer-2 network topology) as well as Multiple Spanning Tree Protocol (MSTP), which is defined in the IEEE 802.1Q standard.

MSTP supports multiple spanning tree instances, where each instance carries traffic for one or more VLANs (the mapping of VLANs to instances is configurable). MSTP is backward-compatible with STP and Rapid Spanning Tree Protocol (RSTP). A layer-2 network can contain switches that are running MSTP, STP, or RSTP. MSTP is built on RSTP, so it provides fast recovery from network faults and fast convergence times.

This section covers the following topics:

To configure STP for all managed FortiSwitch units:

```
config switch-controller stp-settings
   set name <name>
   set revision <stp revision>
   set hello-time <hello time>
   set forward-time <forwarding delay>
   set max-age <maximum aging time>
   set max-hops <maximum number of hops>
end
```

To override the global STP settings for a specific FortiSwitch unit:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>>
      config stp-settings
         set local-override enable
      end
```

To configure MSTP instances:

```
config switch-controller stp-instance
   edit <id>
      config vlan-range <list of VLAN names>
   end
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config stp-instance
         edit <id>
            set priority <0 | 4096 | 8192 | 12288 | 16384 | 20480 | 24576 | 28672 | 32768 |
                 36864 | 40960 | 45056 | 49152 | 53248 | 57344 | 61440>
         next
      end
   next
end
```

For example:

```
config switch-controller stp-instance
   edit 1
      config vlan-range vlan1 vlan2 vlan3
   end
config switch-controller managed-switch
   edit S524DF4K15000024
      config stp-instance
         edit 1
            set priority 16384
         next
      end
   next
end
```

Configuring STP on FortiSwitch ports

STP is enabled by default for the non-FortiLink ports on the managed FortiSwitch units. STP is a link-management protocol that ensures a loop-free layer-2 network topology.

Use the following commands to enable or disable STP on FortiSwitch ports:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set stp-state {enabled | disabled}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set stp-state enabled
         end
      end
```

To check the STP configuration on a FortiSwitch, use the following command:

```
diagnose switch-controller switch-info stp <FortiSwitch_serial_number> <instance_number>
```

For example:

```
FSWMVMTM21000008 # diagnose switch-controller switch-info stp S524DF4K15000024 0
MST Instance Information, primary-Channel:
Instance ID :   0
Switch Priority : 24576
Root MAC Address :    085b0ef195e4
Root Priority:    24576
Root Pathcost:    0
Regional Root MAC Address :   085b0ef195e4
Regional Root Priority:   24576
Regional Root Path Cost:  0
Remaining Hops:       20
This Bridge MAC Address :    085b0ef195e4
This bridge is the root

Port               Speed   Cost       Priority   Role         State       Edge  STP-Status
Loop Protection
_________________  ______  _________  _________  ___________  __________  ____  __________
________

port1              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port2              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port3              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port4              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port5              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
```

```
    NO
port6               -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port7               -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port8               -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port9               -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port10              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port11              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port12              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port13              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port14              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port15              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port16              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port17              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port18              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port19              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port20              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port21              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port22              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port23              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port25              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port26              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port27              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port28              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port29              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
port30              -       200000000  128        DISABLED     DISCARDING   YES    ENABLED
    NO
internal            1G      20000      128        DESIGNATED   FORWARDING   YES    DISABLED
    NO
__FoRtI1LiNk0__     1G      20000      128        DESIGNATED   FORWARDING   YES    DISABLED
    NO
```

Configuring STP root guard

Root guard protects the interface on which it is enabled from becoming the path to root. When enabled on an interface, superior BPDUs received on that interface are ignored or dropped. Without using root guard, any switch that participates in STP maintains the ability to reroute the path to root. Rerouting might cause your network to transmit large amounts of traffic across suboptimal links or allow a malicious or misconfigured device to pose a security risk by passing core traffic through an insecure device for packet capture or inspection. By enabling root guard on multiple interfaces, you can create a perimeter around your existing paths to root to enforce the specified network topology.

Enable root guard on all ports that should not be root bridges. Do not enable root guard on the root port. You must have STP enabled to be able to use root guard.

Use the following commands to enable or disable STP root guard on FortiSwitch ports:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set stp-root-guard {enabled | disabled}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set stp-root-guard enabled
         end
      end
```

Configuring STP BPDU guard

Similar to root guard, BPDU guard protects the designed network topology. When BPDU guard is enabled on STP edge ports, any BPDUs received cause the ports to go down for a specified number of minutes. The BPDUs are not forwarded, and the network edge is enforced.

There are two prerequisites for using BPDU guard:

- You must define the port as an edge port with the `set edge-port enable` command.
- You must enable STP on the switch interface with the `set stp-state enabled` command.

You can set how long the port will go down when a BPDU is received for a maximum of 120 minutes. The default port timeout is 5 minutes. If you set the timeout value to 0, the port will not go down when a BPDU is received, but you will have manually reset the port.

Use the following commands to enable or disable STP BPDU guard on FortiSwitch ports:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set stp-bpdu-guard {enabled | disabled}
            set stp-bpdu-guard-time <0-120>
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set stp-bpdu-guard enabled
            set stp-bpdu-guard-time 10
         end
      end
```

To check the configuration of STP BPDU guard on a FortiSwitch unit, use the following command:

```
diagnose switch-controller switch-info bpdu-guard-status <FortiSwitch_serial_number>
```

For example:

```
FSWMVMTM21000008 # diagnose switch-controller switch-info bpdu-guard-status S524DF4K15000024
Managed Switch : S524DF4K15000024 0

Portname              State      Status       Timeout(m)    Count    Last-Event
____________________  ________   __________   ___________   _____   _______________

port1                enabled      -              10            0            -
port2                disabled     -              -             -            -
port3                disabled     -              -             -            -
port4                disabled     -              -             -            -
port5                disabled     -              -             -            -
port6                disabled     -              -             -            -
port7                disabled     -              -             -            -
port8                disabled     -              -             -            -
port9                disabled     -              -             -            -
port10               disabled     -              -             -            -
port11               disabled     -              -             -            -
port12               disabled     -              -             -            -
port13               disabled     -              -             -            -
port14               disabled     -              -             -            -
port15               disabled     -              -             -            -
port16               disabled     -              -             -            -
port17               disabled     -              -             -            -
port18               disabled     -              -             -            -
port19               disabled     -              -             -            -
port20               disabled     -              -             -            -
port21               disabled     -              -             -            -
port22               disabled     -              -             -            -
port23               disabled     -              -             -            -
port25               disabled     -              -             -            -
port26               disabled     -              -             -            -
port27               disabled     -              -             -            -
port28               disabled     -              -             -            -
port29               disabled     -              -             -            -
port30               disabled     -              -             -            -
__FoRtI1LiNk0__     disabled     -              -             -            -
```

Configuring interoperation with per-VLAN RSTP

Managed FortiSwitch units can interoperate with a network that is running RPVST+. The existing network's configuration can be maintained while adding managed FortiSwitch units as an extended region. By default, interoperation with RPVST+ is disabled.

When an MSTP domain is connected with an RPVST+ domain, FortiSwitch interoperation with the RPVST+ domain works in two ways:

- If the root bridge for the CIST is within an MSTP region, the boundary FortiSwitch unit of the MSTP region duplicates instance 0 information, creates one BPDU for every VLAN, and sends the BPDUs to the RPVST+ domain.

  In this case, follow this rule: If the root bridge for the CIST is within an MSTP region, VLANs other than VLAN 1 defined in the RPVST+ domains must have their bridge priorities worse (numerically greater) than that of the CIST root bridge within MSTP region.

- If the root bridge for the CIST is within an RPVST+ domain, the boundary FortiSwitch unit processes only the VLAN 1 information received from the RPVST+ domain. The other BPDUs (VLANs 2 and above) sent from the connected RPVST+ domain are used only for consistency checks.

  In this case, follow this rule: If the root bridge for the CIST is within the RPVST+ domain, the root bridge priority of VLANs other than VLAN 1 within that domain must be better (numerically less) than that of VLAN 1.

To configure interoperation with RPVST+:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set rpvst-port {enabled | disabled}
         next
      end
```

For example:

```
FSWMVMTM21000008 (testvdom) # config switch-controller managed-switch
FSWMVMTM21000008 (managed-switch) # edit FS3E32T419000006
FSWMVMTM21000008 (FS3E32T419000006) # config ports
FSWMVMTM21000008 (ports) # edit port5
FSWMVMTM21000008 (port5) # set rpvst-port enabled
FSWMVMTM21000008 (port5) # next
FSWMVMTM21000008 (ports) # end
```

To check your configuration and to diagnose any problems:

```
diagnose switch-controller switch-info rpvst <FortiSwitch_serial_number> <port_name>
```

For example:

```
diagnose switch-controller switch-info rpvst FS3E32T419000006 port5
```

Dynamic MAC address learning

You can enable or disable dynamic MAC address learning on a port or VLAN. The existing dynamic MAC entries are flushed when you change this setting. If you disable MAC address learning, you can set the behavior for an incoming packet with an unknown MAC address (to drop or forward the packet).

This section covers the following topics:

Limiting the number of learned MAC addresses on a FortiSwitch interface

You can limit the number of MAC addresses learned on a FortiSwitch interface (port or VLAN). The limit ranges from 1 to 128. If the limit is set to the default value zero, there is no learning limit.

NOTE: Static MAC addresses are not counted in the limit. The limit refers only to learned MAC addresses.

Use the following CLI commands to limit MAC address learning on a VLAN:

```
config switch vlan
   edit <integer>
      set switch-controller-learning-limit <limit>
   end
end
```

For example:

```
config switch vlan
   edit 100
      set switch-controller-learning-limit 20
   end
end
```

Use the following CLI commands to limit MAC address learning on a port:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set learning-limit <limit>
         next
      end
   end
end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port3
            set learning-limit 50
         next
```

```
      end
   end
end
```

Controlling how long learned MAC addresses are saved

You can change how long learned MAC addresses are stored. By default, each learned MAC address is aged out after 300 seconds. After this amount of time, the inactive MAC address is deleted from the FortiSwitch hardware. The value ranges from 10 to 1000,000 seconds. Set the value to 0 to disable MAC address aging.

```
config switch-controller global
   set mac-aging-interval <10 to 1000000>
end
```

For example:

```
config switch-controller global
   set mac-aging-interval 500
end
```

If the mac-aging-interval is disabled by being set to 0, you can still control when inactive MAC addresses are removed from the FortiSwitch hardware. By default, inactive MAC addresses are removed after 24 hours. The value ranges from 0 to 168 hours. Set the value to 0 to use the mac-aging-interval setting to control when inactive MAC addresses are deleted.

```
config switch-controller global
   set mac-retention-period <0 to 168>
end
```

For example:

```
config switch-controller global
   set mac-retention-period 36
end
```

Logging violations of the MAC address learning limit

If you want to see the first MAC address that exceeded the learning limit for an interface or VLAN, you can enable the learning-limit violation log for a managed FortiSwitch unit. Only one violation is recorded per interface or VLAN.

By default, logging is disabled. The most recent violation that occurred on each interface or VLAN is recorded in the system log. After that, no more violations are logged until the log is reset for the triggered interface or VLAN. Only the most recent 128 violations are displayed in the console.

Use the following commands to control the learning-limit violation log and to control how long learned MAC addresses are saved:

```
config switch-controller global
   set mac-violation-timer <0-1500>
   set log-mac-limit-violations {enable | disable}
end
```

For example:

```
config switch-controller global
   set mac-violation-timer 1000
   set log-mac-limit-violations enable
end
```

To view the content of the learning-limit violation log for a managed FortiSwitch unit, use one of the following commands:

- `diagnose switch-controller switch-info mac-limit-violations all <FortiSwitch_serial_number>`
- `diagnose switch-controller switch-info mac-limit-violations interface <FortiSwitch_serial_number> <port_name>`
- `diagnose switch-controller switch-info mac-limit-violations vlan <FortiSwitch_serial_number> <VLAN_ID>`

For example, to set the learning-limit violation log for VLAN 5 on a managed FortiSwitch unit:

```
diagnose switch-controller switch-info mac-limit-violations vlan S124DP3XS12345678 5
```

To reset the learning-limit violation log for a managed FortiSwitch unit, use one of the following commands:

- `execute switch-controller mac-limit-violation reset all <FortiSwitch_serial_number>`
- `execute switch-controller mac-limit-violation reset vlan <FortiSwitch_serial_number> <VLAN_ID>`
- `execute switch-controller mac-limit-violation reset interface <FortiSwitch_serial_number> <port_name>`

For example, to clear the learning-limit violation log for port 5 of a managed FortiSwitch unit:

```
execute switch-controller mac-limit-violation reset interface S124DP3XS12345678 port5
```

Persistent (sticky) MAC addresses

You can make dynamically learned MAC addresses persistent when the status of a FortiSwitch port changes (goes down or up). By default, MAC addresses are not persistent.

Use the following commands to configure the persistence of MAC addresses on an interface:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set sticky-mac {enable | disable}
         next
      end
```

You can also save persistent MAC addresses to the FortiSwitch configuration file so that they are automatically loaded when the FortiSwitch unit is rebooted. By default, persistent entries are lost when a FortiSwitch unit is rebooted. Use the following commands to save persistent MAC addresses for a specific interface or all interfaces:

```
execute switch-controller switch-action sticky-mac save interface <FortiSwitch_serial_
     number> <port_name>
execute switch-controller switch-action sticky-mac save all <FortiSwitch_serial_number>
```

Use one of the following commands to delete the persistent MAC addresses instead of saving them in the FortiSwitch configuration file:

```
execute switch-controller switch-action delete sticky-mac delete-unsaved all <FortiSwitch_
     serial_number>
execute switch-controller switch-action delete sticky-mac delete-unsaved interface
     <FortiSwitch_serial_number> <port_name>
```

Logging changes to MAC addresses

Use the following commands to create syslog entries for when MAC addresses are learned, aged out, and removed. By default, no syslog entries are created.

NOTE: You must set `data-sync-interval` to a non-zero value.

```
config switch-controller system
   set data-sync-interval <30-1800 seconds>
end

config switch-controller global
   set mac-event-logging enable
end
```

Starting in FortiSwitch Manager 7.2.2, you can log dynamic MAC address events.

Go to *Log & Report* > *System Events* to see the log entries.

Configuring storm control

Storm control uses the data rate (packets/sec, default 500) of the link to measure traffic activity, preventing traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port.

When the data rate exceeds the configured threshold, storm control drops excess traffic. You can configure the types of traffic to drop: broadcast, unknown unicast, or multicast. By default, these three types of traffic are not dropped.

To configure storm control for all switch ports (including both FortiLink ports and non-FortiLink ports) on the managed switches, use the following FortiSwitch Manager CLI commands:

```
config switch-controller storm-control
   set rate <rate>
   set unknown-unicast {enable | disable}
   set unknown-multicast {enable | disable}
   set broadcast {enable | disable}
end
```

To configure storm control for a FortiSwitch port, use the FortiSwitch Manager CLI to select the override storm-control-mode in the storm-control policy and then assigning the storm-control policy for the FortiSwitch port.

```
config switch-controller storm-control-policy
   edit <storm_control_policy_name>
      set description <description_of_the_storm_control_policy>
      set storm-control-mode override
      set rate <1-10000000 or 0 to drop all packets>
      set unknown-unicast {enable | disable}
      set unknown-multicast {enable | disable}
      set broadcast {enable | disable}
   next
end

config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit port5
            set storm-control-policy <storm_control_policy_name>
```

```
        next
    end
```

For example:

```
config switch-controller storm-control-policy
   edit stormpol1
      set description "storm control policy for port 5"
      set storm-control-mode override
      set rate 1000
      set unknown-unicast enable
      set unknown-multicast enable
      set broadcast enable
   next
end

config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port5
            set storm-control-policy stormpol1
         next
      end
```

Configuring IGMP-snooping settings

You need to configure global IGMP-snooping settings and IGMP-snooping settings on a FortiSwitch unit before configuring the IGMP-snooping proxy and IGMP-snooping querier.

This section covers the following topics:

Configuring global IGMP-snooping settings

Use the following commands to configure the global IGMP-snooping settings.

Aging time is the maximum number of seconds that the system will retain a multicast snooping entry. Enter an integer value from 15 to 3600. The default value is 300.

The `flood-unknown-multicast` setting controls whether the system will flood unknown multicast messages within the VLAN.

Starting in FortiSwitch Manager 7.2.2, you can specify how often the managed FortiSwitch unit will send IGMP version-2 queries when the IGMP-snooping querier is configured. The range of values is 10-1,200 seconds. By default, queries are sent every 125 seconds. The value for `aging-time` must be greater than the value for `query-interval`.

```
config switch-controller igmp-snooping
   set aging-time <15-3600>
   set flood-unknown-multicast {enable | disable}
```

```
      set query-interval <10-1200>
   end
```

Configuring IGMP-snooping settings on a switch

IGMP snooping allows the FortiSwitch to passively listen to the Internet Group Management Protocol (IGMP) network traffic between hosts and routers. The switch uses this information to determine which ports are interested in receiving each multicast feed. FortiSwitch can reduce unnecessary multicast traffic on the LAN by pruning multicast traffic from links that do not contain a multicast listener.

NOTE: When an inter-switch link (ISL) is formed automatically in FortiLink mode, the `igmps-flood-reports` and `igmps-flood-traffic` options are disabled by default.

Use the following commands to configure IGMP settings on a FortiSwitch port:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set igmps-flood-reports {enable | disable}
            set igmps-flood-traffic {enable | disable}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port3
            set igmps-flood-reports enable
            set igmps-flood-traffic enable
         end
      end
```

Configuring the IGMP-snooping proxy

You can use the CLI to enable IGMP proxy per FortiSwitch unit.

By default, IGMP snooping is disabled. You need to enable IGMP snooping on FortiSwitch Manager before you can enable the IGMP-snooping proxy.

To enable IGMP snooping and the IGMP-snooping proxy:

```
config system interface
   edit <VLAN_interface>
      set switch-controller-igmp-snooping enable
      set switch-controller-igmp-snooping-proxy enable
   next
end
```

For example, you can enable IGMP snooping and the IGMP-snooping proxy on VLAN 100:

```
config system interface
   edit vlan100
```

```
      set switch-controller-igmp-snooping enable
      set switch-controller-igmp-snooping-proxy enable
   next
end
```

Configuring the IGMP-snooping querier

You can configure the IGMP-snooping querier version 2 or 3. When the IGMP querier version 2 is configured, the managed FortiSwitch unit will send IGMP version-2 queries when no external querier is present. When the IGMP querier version 3 is configured, the managed FortiSwitch unit will send IGMP version-3 queries when no external querier is present.

If you have IGMP snooping and the IGMP-snooping proxy enabled on a VLAN, you can then configure the IGMP-snooping querier on the same VLAN on a managed switch. By default, the IGMP-snooping querier is disabled.

You must enable the overriding of the global IGMP-snooping configuration with the `set local-override enable` command.

By default, the maximum time (`aging-time`) that multicast snooping entries without any packets are kept is for 300 seconds. This value can be in the range of 15-3,600 seconds.

By default, `flood-unknown-multicast` is disabled, and unregistered multicast packets are forwarded only to mRouter ports. If you enable `flood-unknown-multicast`, unregistered multicast packets are forwarded to all ports in the VLAN.

The IGMP-snooping proxy uses the global IGMP-snooping configuration by default. You can enable or disable the IGMP-snooping on the VLAN.

You can optionally specify the IPv4 address that IGMP reports are sent to. You can also set the IGMP-snooping querier version. The default IGMP querier version is 2.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
   config igmp-snooping
      set local-override enable
      set aging-time <15-3600>
      set flood-unknown-multicast {enable | disable}
      config vlans
         edit <VLAN_interface>
            set proxy {disable | enable | global}
            set querier enable
            set querier-addr <IPv4_address>
            set version {2 | 3}
         next
      end
   end
end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
   config igmp-snooping
      set local-override enable
      set aging-time 1000
      set flood-unknown-multicast enable
      config vlans
         edit vlan100
```

```
            set proxy disable
            set querier enable
            set querier-addr 1.2.3.4
            set version 3
         next
      end
   end
end
```

Configuring PTP transparent-clock mode

Use the Precision Time Protocol (PTP) transparent-clock mode to measure the overall path delay for packets in a network to improve the time precision. There are two transparent-clock modes:

- End-to-end measures the path delay for the entire path
- Peer-to-peer measures the path delay between each pair of nodes

Use the following steps to configure PTP transparent-clock mode:

1. Configure a PTP profile or use the `default` profile.
2. Configure the PTP settings.

   By default, PTP is disabled. Enable PTP and select which PTP profile will use these PTP settings. The default profile is automatically selected. If you have multiple PTP profiles, each managed switch can use a different PTP profile.
3. Configure the default PTP policy or create a custom PTP policy.

   Select which VLAN will use the PTP policy and the priority of the VLAN. The default PTP policy is applied to all ports. If you want to select which ports to apply the PTP policy to, you need to create a custom PTP policy. Each switch port can be configured with a different PTP policy.
4. If you are not using the default PTP policy, select which port to apply your custom PTP policy to.

   By default, the PTP status is enabled.

   NOTE: Setting `ptp-policy` on a switch interface is valid only in peer-to-peer mode.

To configure a PTP profile:

```
config switch-controller ptp profile
   edit {default | name_of_PTP_profile}
      set description <description_of_PTP_profile>
      set mode {transparent-e2e | transparent-p2p}
      set ptp-profile C37.238-2017
      set transport l2-mcast
      set domain <0-255> // the default is 254
      set pdelay-req-interval {1sec | 2sec | 4sec | 8sec | 16sec | 32sec} // 1sec default
   next
end
```

For example:

```
config system ptp profile
   edit newPTPprofile
      set description "New PTP profile"
      set mode transparent-p2p
      set ptp-profile C37.238-2017
```

```
      set transport l2-mcast
      set domain 1
      set pdelay-req-interval 2sec
   next
end
```

To configure the PTP settings:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set ptp-status {enable | disable} // the default is disable
      set ptp-profile {default | name_of_PTP_profile} // the default is "default"
   next
end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      set ptp-status enable
      set ptp-profile newPTPprofile
   next
end
```

To configure the default PTP policy or create a custom PTP policy:

```
config switch-controller ptp interface-policy
   edit {default | <policy_name>}
      set description <description_of_PTP_policy>
      set vlan <VLAN_name> //no default
      set vlan-pri <0-7> // the default is 4
   next
end
```

For example:

```
config switch-controller ptp interface-policy
   edit ptppolicy1
      set description "New custom PTP policy"
      set vlan vlan10
      set vlan-pri 3
   next
end
```

To apply your custom PTP policy to a port:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set ptp-status {enable | disable} // the default is enable
            set ptp-policy {default | <policy_name>} // the default is "default"
         end
      end
```

For example:

```
config switch-controller managed-switch
```

```
edit S524DF4K15000024
   config ports
      edit port5
         set ptp-status enable
         set ptp-policy ptppolicy1
      end
   end
```

Device detection

This section covers the following topics:

Configuring LLDP-MED settings

LLDP neighbor devices are dynamically detected. By default, this feature is enabled in FortiSwitch Manager but disabled in managed FortiSwitch units. Dynamic detection must be enabled in both FortiSwitch Manager and FortiSwitchOS for this feature to work.

This section covers the following topics:

To configure LLDP profiles in FortiSwitch Manager:

```
config switch-controller lldp-profile
   edit <profile_name>
      set med-tlvs (inventory-management | network-policy | power-management | location-
           identification)
      set 802.1-tlvs port-vlan-id
      set 802.3-tlvs {max-frame-size | power-negotiation}
      set auto-isl {enable | disable}
      set auto-isl-hello-timer <1-30>
      set auto-isl-port-group <0-9>
      set auto-isl-receive-timeout <3-90>
      config med-network-policy
         edit {guest-voice | guest-voice-signaling | softphone-voice | streaming-video |
              video-conferencing | video-signaling | voice | voice-signaling}
            set status {enable | disable}
            set vlan-intf <string>
            set priority <0-7>
            set dscp <0-63>
         next
      end
      config med-location-service
         edit {address-civic | coordinates | elin-number}
            set status {enable | disable}
            set sys-location-id <string>
         next
      end
      config-tlvs
         edit <TLV_name>
            set oui <hexadecimal_number>
            set subtype <0-255>
            set information-string <0-507>
```

```
        next
      end
    next
end
```

Variable	Description
<profile_name>	Enable or disable
med-tlvs (inventory-management | network-policy | power-management | location-identification)	Select which LLDP-MED type-length-value descriptions (TLVs) to transmit: inventory-managment TLVs, network-policy TLVs, power-management TLVs for PoE, and location-identification TLVs. You can select one or more option. Separate multiple options with a space.
802.1-tlvs port-vlan-id	Transmit the IEEE 802.1 port native-VLAN TLV.
802.3-tlvs {max-frame-size | power-negotiation}	Select whether to transmit the IEEE 802.3 maximum frame size TLV, the power-negotiation TLV for PoE, or both. Separate multiple options with a space.
auto-isl {enable | disable}	Enable or disable the automatic inter-switch LAG.
auto-isl-hello-timer <1-30>	If you enabled auto-isl, you can set the number of seconds for the automatic inter-switch LAG hello timer. The default value is 3 seconds.
auto-isl-port-group <0-9>	If you enabled auto-isl, you can set the automatic inter-switch LAG port group identifier.
auto-isl-receive-timeout <3-90>	If you enabled auto-isl, you can set the number of seconds before the automatic inter-switch LAG times out if no response is received. The default value is 9 seconds.
config med-network-policy	
{guest-voice | guest-voice-signaling | softphone-voice | streaming-video | video-conferencing | video-signaling | voice | voice-signaling}	Select which Media Endpoint Discovery (MED) network policy type-length-value (TLV) category to edit.
status {enable | disable}	Enable or disable whether this TLV is transmitted.
vlan-intf <string>	If you enabled the status, you can enter the VLAN interface to advertise. The maximum length is 15 characters.
priority <0-7>	If you enabled the status, you can enter the advertised Layer-2 priority. Set to 7 for the highest priority.
dscp <0-63>	If you enabled the status, you can enter the advertised Differentiated Services Code Point (DSCP) value to indicate the level of service requested for the traffic.
config med-location-service	
{address-civic | coordinates | elin-number}	Select which Media Endpoint Discovery (MED) location type-length-value (TLV) category to edit.
status {enable | disable}	Enable or disable whether this TLV is transmitted.

Variable	Description
sys-location-id <string>	If you enabled the status, you can enter the location service identifier. The maximum length is 63 characters.
config-tlvs	
<TLV_name>	Enter the name of a custom TLV entry.
oui <hexadecimal_number>	Ener the organizationally unique identifier (OUI), a 3-byte hexadecimal number, for this TLV.
subtype <0-255>	Enter the organizationally defined subtype.
information-string <0-507>	Enter the organizationally defined information string in hexadecimal bytes.

To configure LLDP settings in FortiSwitch Manager:

```
config switch-controller lldp-settings
   set tx-hold <int>
   set tx-interval <int>
   set fast-start-interval <int>
   set management-interface {internal | management}
   set device-detection {enable | disable}
end
```

Variable	Description
tx-hold	Number of tx-intervals before the local LLDP data expires. Therefore, the packet TTL (in seconds) is `tx-hold` times `tx-interval`. The range for tx-hold is 1 to 16, and the default value is 4.
tx-interval	How often the FortiSwitch transmits the LLDP PDU. The range is 5 to 4095 seconds, and the default is 30 seconds.
fast-start-interval	How often the FortiSwitch transmits the first 4 LLDP packets when a link comes up. The range is 2 to 5 seconds, and the default is 2 seconds. Set this variable to zero to disable fast start.
management-interface	Primary management interface to be advertised in LLDP and CDP PDUs.
device-detection {enable | disable}	Enable or disable whether LLDP neighbor devices are dynamically detected. By default, this setting is disabled.

To configure dynamic detection of LLDP neighbor devices in FortiSwitchOS:

```
config switch lldp settings
   set device-detection enable
end
```

Adding media endpoint discovery (MED) to an LLDP configuration

You can use the following commands to add media endpoint discovery (MED) features to an LLDP profile:

```
config switch-controller lldp-profile
```

```
edit <lldp-profle>
      config med-network-policy
         edit guest-voice
            set status {disable | enable}
         next
         edit guest-voice-signaling
            set status {disable | enable}
         next
         edit guest-voice-signaling
            set status {disable | enable}
         next
         edit softphone-voice
            set status {disable | enable}
         next
         edit streaming-video
            set status {disable | enable}
         next
         edit video-conferencing
            set status {disable | enable}
         next
         edit video-signaling
            set status {disable | enable}
         next
         edit voice
            set status {disable | enable}
         next
         edit voice-signaling
            set status {disable | enable}
         end
      config custom-tlvs
         edit <name>
            set oui <identifier>
            set subtype <subtype>
            set information-string <string>
         end
   end
```

Displaying LLDP information

You can use the following commands to display LLDP information:

```
diagnose switch-controller switch-info lldp stats <switch> <port>
diagnose switch-controller switch-info lldp neighbors-summary <switch>
diagnose switch-controller switch-info lldp neighbors-detail <switch>
```

Configuring the LLDP settings

The Fortinet data center switches support the Link Layer Discovery Protocol (LLDP) for transmission and reception wherein the switch will multicast LLDP packets to advertise its identity and capabilities. A switch receives the equivalent information from adjacent layer-2 peers.

Use the following commands to configure LLDP on a FortiSwitch port:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
```

```
config ports
   edit <port_name>
      set lldp-status {rx-only | tx-only | tx-rx | disable}
      set lldp-profile <profile_name>
   end
end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port2
            set lldp-status tx-rx
            set lldp-profile default
         end
      end
```

Use the following commands to configure LLDP on a virtual FortiSwitch port:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set lldp-status {rx-only | tx-only | tx-rx | disable}
            set lldp-profile <profile_name>
         next
      end
   end
end
```

For example:

```
config switch-controller managed-switch
   edit "S424ENTF19000007"
      config ports
         edit port28
            set lldp-status tx-rx
            set lldp-profile lldpprofile1
         next
      end
   end
end
```

FortiSwitch security

This section covers the following topics:

For more information on remote authentication, see the following:

- LDAP authentication
- RADIUS authentication
- TACACS+ authentication

FortiSwitch security policies

To control network access, the managed FortiSwitch unit supports IEEE 802.1X authentication. A supplicant connected to a port on the switch must be authenticated by a RADIUS/Diameter server to gain access to the network. The supplicant and the authentication server communicate using the switch using the EAP protocol. The managed FortiSwitch unit supports EAP-PEAP, EAP-TTLS, EAP-TLS, and EAP-MD5.

To use the RADIUS server for authentication, you must configure the server before configuring the users or user groups on the managed FortiSwitch unit.

NOTE: In FortiLink mode, you must manually create a firewall policy to allow RADIUS traffic for 802.1X authentication from the FortiSwitch unit (for example, from the FortiLink interface) to the RADIUS server through FortiSwitch Manager.

The managed FortiSwitch unit implements MAC-based authentication. The switch saves the MAC address of each supplicant's device. The switch provides network access only to devices that have successfully been authenticated.

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 configure a guest VLAN for unauthorized users and a VLAN for users whose authentication was unsuccessful. If the RADIUS server cannot be reached for 802.1X authentication, you can specify a RADIUS timeout VLAN for users after the authentication server timeout period expires.

Starting in FortiSwitch Manager 7.2.5, you can specify a tagged VLAN for users to be assigned to when the authentication server is unavailable. This feature is available with 802.1x MAC-based authentication. It is compatible with both EAP and MAB.

When you are testing your system configuration for 802.1X authentication, you can use the monitor mode to allow network traffic to flow, even if there are configuration problems or authentication failures.

Fortinet recommends an 802.1X setup rate of 5 to 10 sessions per second.

This section covers the following topics:

Number of devices supported per port for 802.1X MAC-based authentication

The FortiSwitch unit supports up to 20 devices per port for 802.1X MAC-based authentication. System-wide, the FortiSwitch unit now supports a total of 10 times the number of interfaces for 802.1X MAC-based authentication. See the following table.

Model	Total number of devices supported per switch
108	80
112	60
124/224/424/524/1024	240
148/248/448/548/1048	480
3032	320

Configuring the 802.1X settings

To configure the 802.1X security policy:

```
config switch-controller 802-1X-settings
   set link-down-auth {set-unauth | no-action}
   set reauth-period <integer>
```

```
    set max-reauth-attempt <integer>
    set tx-period <integer>
    set mab-reauth {enable | disable}
end
```

Option	Description	Default
`link-down-auth {set-unauth | no-action}`	If a link is down, this command determines the authentication state. Choosing `set-unauth` sets the interface to unauthenticated when a link is down, and reauthentication is needed. Choosing `no-action` means that the interface does not need to be reauthenticated when a link is down.	set-unauth
`reauth-period <integer>`	This command sets how often reauthentication is needed. The range is 1-1440 minutes. Setting the value to 0 minutes disables reauthentication. **NOTE:** Setting the reauth-period to 0 is supported only in the CLI. The RADIUS dynamic session timeout and CoA session timeout do not support setting the Session Timeout to 0.	60
`max-reauth-attempt <integer>`	This command sets the maximum number of reauthentication attempts. The range is 1-15. Setting the value to 0 disables reauthentication.	3
`tx-period <integer>`	This command sets the 802.1X transmission period in seconds. The range is 4-60.	30
`mab-reauth {enable | disable}`	This command enables or disables MAB reauthentication.	disable

Overriding the settings

You can override the settings for the 802.1X security policy.

Using the FortiSwitch Manager GUI

To override the 802.1X settings:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Right-click on a switch name and select *Edit*.
3. In the *Edit Managed FortiSwitch* page, enable *Override 802-1X settings*.
4. In the *Reauthentication Interval* field, enter the number of minutes before reauthentication is required. The maximum interval is 1,440 minutes. Setting the value to 0 minutes disables reauthentiction.
5. In the *Max Reauthentication Attempts* field, enter the maximum times that reauthentication is attempted. The maximum number of attempts is 15. Setting the value to 0 disables reauthentication.
6. Select *Deauthenticate* or *None* for the link down action. Selecting *Deauthenticate* sets the interface to unauthenticated when a link is down, and reauthentication is needed. Selecting *None* means that the interface does not need to be reauthenticated when a link is down.
7. Click *OK*.

Using the FortiSwitch Manager CLI

To override the 802.1X settings:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config 802-1X-settings
         set local-override {enable | *disable}
            set reauth-period <integer>                  // visible if override enabled
            set max-reauth-attempt <integer>             // visible if override enabled
            set link-down-auth {*set-unauth | no-action}   // visible if override enabled
            set mab-reauth {enable | disable}             // visible if override enabled
         end
      next
   end
```

For a description of the options, see Configuring the 802.1X settings.

Specifying how RADIUS request attributes are formatted

Starting in FortiSwitch Manager 7.2.5 with FortiSwitchOS 7.4.1, you can specify how the following RADIUS request attributes are formatted when they are sent to the RADIUS server:

- User-Name

  You can select a colon, hyphen, or single hyphen to use as a delimiter, or you can select `none` for no delimiter. By default, you can use a hyphen as the delimiter.
- User-Password

  You can select a colon, hyphen, or single hyphen to use as a delimiter, or you can select `none` for no delimiter. By default, you can use a hyphen as the delimiter.
- Called-Station-Id

  You can select a colon, hyphen, or single hyphen to use as a delimiter, or you can select `none` for no delimiter. By default, you can use a hyphen as the delimiter.
- Calling-Station-Id

  You can select a colon, hyphen, or single hyphen to use as a delimiter, or you can select `none` for no delimiter. By default, you can use a hyphen as the delimiter.

The following are examples of MAC addresses with the different delimiters:

- Using a colon as a delimiter: `00:11:22:33:44:55`
- Using a hyphen as a delimiter: `00-11-22-33-44-55`
- Using a single hyphen as a delimiter: `001122-334455`
- Using `none` for no delimiter: `001122334455`

You can also select whether to use lowercase or uppercase letters in MAC addresses. By default, lowercase letters are used.

To specify how RADIUS request attributes are formatted:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config 802-1X-settings
         set local-override enable
```

```
        set mac-username-delimiter {colon| hyphen | none | single-hyphen}
        set mac-password-delimiter {colon| hyphen | none | single-hyphen}
        set mac-calling-station-delimiter {colon| hyphen | none | single-hyphen}
        set mac-called-station-delimiter {colon| hyphen | none | single-hyphen}
        set mac-case {lowercase | uppercase}
      end
   next
end
```

Dynamically and manually assigning the NAS-IP-Address attribute

Starting in FortiSwitch Manager 7.2.5, you can dynamically assign a different NAS-IP-Address attribute to the managed switches when authenticating users with a RADIUS server. When this feature is enabled, the NAS-IP-Address attribute is based on the FortiLink IP address when the IP address is IPv4.

If needed, you can override the dynamic NAS-IP-Address attribute and manually assign the NAS-IP-Address attribute to individual managed switches.

- FortiSwitchOS supports only IPv4 addresses for the NAS-IP-Address attribute.
- You can enable `switch-controller-nas-ip-dynamic` only when the `nas-ip` value is not set (under the `config user radius` command).
- When `radius-nas-ip-override` is enabled and the `radius-nas-ip` value is set, the IP address is assigned to the NAS-IP-Address attribute, even if `switch-controller-nas-ip-dynamic` is not enabled and the `nas-ip` value is not set.

To dynamically assign a different NAS-IP-Address attribute on FortiSwitch Manager to all managed switches:

```
config user radius
   edit <RADIUS_server_name>
      set switch-controller-nas-ip-dynamic enable
   next
end
```

To override the dynamic NAS-IP-Address attribute on FortiSwitch Manager for a specific managed switch:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set radius-nas-ip-override enable
      set radius-nas-ip <IPv4_address>
   next
end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      set radius-nas-ip-override enable
      set radius-nas-ip 1.2.3.4
   next
end
```

Dynamic VLAN assignment

You can configure the RADIUS server to return a VLAN in the authentication reply message.

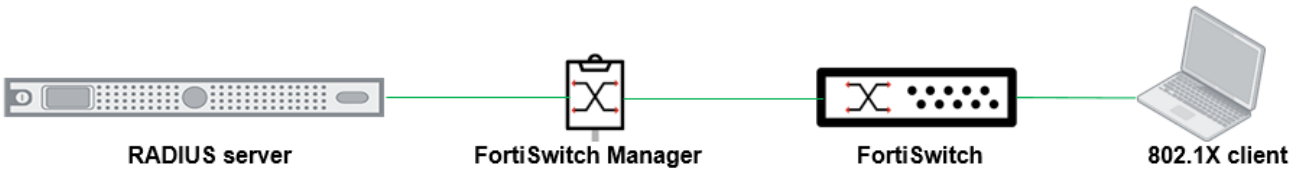
When the FortiSwitch unit receives a VLAN assignment from RADIUS, it determines if the data is an integer or string representation. If the representation is an integer, the FortiSwitch unit assigns the VLAN. If the representation is a string, the 802.1X agent will search each VLAN's description field for all VLANs (names defined by the FortiSwitch Manager VLAN name). If found, the 802.1X agent will make the assignment.

On FortiSwitch Manager, all VLANs are specified as a system interface. Each system interface has a well-defined and unique name. The switch controller synchronizes the FortiSwitch Manager system interface name (maximum of 15 characters) to the FortiSwitch VLAN description.

FortiSwitch Manager 7.2.5 and later also supports the synchronization of the FortiSwitch Manager system interface description to the switch VLAN description (up to the first 63 characters of FortiSwitch VLAN description field in FortiSwtich Manager). This allows a more flexible use of the Tunnel-Private-Group-Id RADIUS attribute. To use the maximum length of 63 characters, set the `vlan-identity` command to `description` (under `config switch-controller global`).

Configuration examples

To configure dynamic VLAN name assignment:



1. Configure a RADIUS server. In this example, the Tunnel-Private-Group-Id is set to the VLAN name, instead of the VLAN identifier.
   - Set Tunnel-Type to "VLAN".
   - Set Tunnel-Medium-Type to "IEEE-802".
   - Set Tunnel-Private-Group-Id to "my.vlan.10".
2. Configure FortiSwitch Manager:

```
config system interface
   edit "my.vlan.10"
      set vdom "root"
      set ip 1.1.1.254 255.255.255.0
      set allowaccess ping
      set interface "my.fortlink"
      set vlanid 10
   next
end
```

3. Check the FortiSwitch unit. The VLAN name is stored in the value for the `set description` command.

```
# show switch vlan
config switch vlan
   edit 10
      set description "my.vlan.10"
   next
end
```

To synchronize the FortiSwitch Manager system interface description to the switch VLAN description:

1. Configure the FortiSwitch VLAN on FortiSwitch Manager:

```
config system interface
   edit "vlan11"
   set vdom "vdom1"
      set ip 6.6.6.1 255.255.255.0
      set allowaccess ping https ssh http fabric
      set description "Test VLAN"
      set device-identification enable
      set role lan
      set snmp-index 45
      set interface "port11"
      set vlanid 111
   next
end
```

2. On the FortiSwitch unit, check that the FortiLink interface name is stored in the value for the `set description` command.

```
config switch vlan
   edit 11
      set description "Test VLAN"
   next
end
```

Setting the priority for dynamic or egress VLAN assignment

Starting in FortiSwitch Manager 7.2.5 with FortiSwitchOS 7.4.2, you can change how a managed FortiSwitch unit searches for VLANs with names (specified in the `set description` command) that match the Tunnel-Private-Group-Id or Egress-VLAN-Name attribute.

Before FortiSwitch Manager 7.2.5 with FortiSwitchOS 7.4.2, if there was more than one VLAN with the same name (specified in the `set description` command), the managed FortiSwitch unit selected the VLAN with the lowest VLAN ID that matched the Tunnel-Private-Group-Id or Egress-VLAN-Name attribute.

In the following example, the Tunnel-Private-Group-Id attribute is set to `testVLAN`, and three VLANs have the same name of `testVLAN`. The managed FortiSwitch unit matches the Tunnel-Private-Group-Id attribute with the VLAN with the lowest ID, VLAN 4.

VLAN ID	VLAN name
4	testVLAN
5	testVLAN
6	testVLAN

In FortiSwitch Manager 7.2.5 with FortiSwitchOS 7.4.2, you can assign a priority to each VLAN. If there is more than one VLAN with the same name (specified in the `set description` command), the managed FortiSwitch unit selects the VLAN with the lowest `assignment-priority` value (which is the highest priority) of the VLANs with names that match the RADIUS Tunnel-Private-Group-Id or Egress-VLAN-Name attribute. The `assignment-priority` value can be 1-255. By default, the `assignment-priority` is 128. The lowest `assignment-priority` value gets the highest priority.

In the following example, the Tunnel-Private-Group-Id attribute is set to `localVLAN`, and four VLANs have the same name of `localVLAN`. The managed FortiSwitch unit matches the Tunnel-Private-Group-Id attribute with the VLAN with the lowest priority, VLAN 5.

VLAN ID	VLAN name	VLAN priority
4	localVLAN	50
5	localVLAN	25
6	localVLAN	75
7	localVLAN	100

To set the priority on the managed FortiSwitch unit for matching VLAN names:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config vlan
         edit <VLAN_name>
            set assignment-priority <1-255>
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S524DF4K15000024"
      config vlan
         edit vlan5
            set assignment-priority 200
         next
      end
   next
end
```

Dynamic access control lists

Starting in FortiSwitch Manager 7.2.5, you can 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.

You can use DACLs with 802.1X port-based authentication and 802.1X MAC-based authentication. IPv4 is supported, but IPv6 is not supported. You can use DACLs with monitor mode (`open-auth`) and with static ACLs.

DACLs are disabled by default. After you enable DACL in an 802.1X security policy, you must apply the 802.1X security policy to a managed FortiSwitch port. See Applying an 802.1X security policy to a FortiSwitch port on page 96.

The maximum number of ACL entries per port is 45. The maximum number of entries includes both static ACL entries and DACL entries. Duplicate entries might cause an error.

FortiSwitch models	Maximum number of static ACL and DACL entries
124D	896
2xxD/2xxE	896
4xxD	896
424E/426E	1,792
448E/424E-Fiber	2,816
5xx	3,584
1024D/1048D	1,792
1024E	3,034
1048E	6,144
3032D	3,072
3032E	986

Two RADIUS attributes are supported:

- Filter-Id —You need to use a custom command to use the Filter-Id attribute.
- NAS-Filter-Rule—The NAS-Filter-Rule attribute defines the filter rules at the RADIUS server. After authentication, the DACL applies to the port.
  - The NAS-Filter-Rule supports a maximum of 80 characters, and you can specify a maximum of 45 entries per authentication session or a maximum of 45 entries per port.
  - Do not include blank spaces in the NAS-Filter-Rule. Commas and dashes are allowed.
  - A syntax error in one NAS-Filter-Rule causes the entire DACL to fail.

The following is the Filter-Id format:

```
Filter-Id += "<filter-name>"
```

For example:

```
Filter-Id += "filter-id-service1"
```

Changing the name of Filter-Id after authentication causes errors in the output of the `diagnose switch-controller switch-info 802.1X-dacl` command when the session is using Filter-Id.

The following is the NAS-Filter-Rule format:

```
NAS-Filter-Rule = " <deny|permit> in <ip|ip-protocol-value> from <any|<ip-addr>|ipv4-
     addr/mask> [<tcp/udp-port|tcp/udp min-max port>] to <any|<ip-addr>|ipv4-addr/mask>
     [<tcp/udp-port|tcp/udp min-max port>] [cnt] "
```

The following table explains the syntax of the NAS-Filter-Rule:

Option	Description
<deny|permit>	Select one of the following: • `permit`—Allow packets that match the rule. • `deny`—Drop packets that match the rule.
in	The `in` keyword specifies that the ACL applies only to the inbound traffic from the authenticated client.
<ip|ip-protocol-value>	Specify one of the following for the type of traffic to filter: • `ip`—Any protocol will match. • `ip-protocol-value`—IP traffic specified by either a protocol number or by `tcp`, `udp`, `icmp`, or (for IPv4 only) `igmp`. The range of protocol numbers is 0-255.
from <any|<ip-addr>|ipv4-addr/mask>	Required. Specify one of the following for the authenticated client source: • `any`—Specifies any IPv4 source address • `<ip-addr>|ipv4-addr/mask>`—Enter a series of contiguous source addresses or all source addresses in a subnet. The <mask> is the number of leftmost bits in a packet's source IPv4 address that must match the corresponding bits in the source IPv4 address. For example, `10.100.24.1/24` will match an inbound traffic from the authenticated client that has a source IPv4 address where the first three octets are 10.100.24.
[<tcp/udp-port|tcp/udp min-max port>] to	Specify the TCP or UDP port or range of ports. Used when the access control entry is intended to filter client TCP or UDP traffic with one or more specific TCP or UDP source port numbers. You can specify a single port or a single port range, such as 10.105.0.1/24 80 or 10.105.0.1/24 80-100.
<any|<ip-addr>|ipv4-addr/mask>	Specify one of the following: • `any`—Specifies any IPv4 destination address • `<ip-addr>|ipv4-addr/mask>`—Enter a series of contiguous destination addresses or all destination addresses in a subnet. The <mask> is the number of leftmost bits in a packet's destination IPv4 address that must match the corresponding bits in the destination IPv4 address. For example, `10.100.24.1/24` will match an inbound traffic from the authenticated client that has a destination IPv4 address where the first three octets are 10.100.24.
[<tcp/udp-port|tcp/udp min-max port>]	Specify the TCP or UDP port or range of ports. Used when the access control entry is intended to filter client TCP or UDP traffic with one or more specific TCP or UDP destination port numbers. You can specify a single port or a single port range, such as 10.105.0.1/24 80 or 10.105.0.1/24 80-100. For example, to deny any UDP traffic from an authenticated client that has a destination address of any address and a UDP destination port of 357-457: `deny in udp from any to any 357-457`

Option	Description
[cnt]	Specify the counter for a RADIUS-assigned access control entry.

For example:

- `NAS-Filter-Rule += "permit in 20 from any to any cnt"`
- `NAS-Filter-Rule += "deny in tcp from any to 10.10.10.1 23"`
- `NAS-Filter-Rule += "permit in tcp from any to any 23"`

When you use the NAS-Filter-Rule attribute, follow these guidelines:

- You can use 8 port ranges (source or destination ports) on the FS-148E, FS-148E-POE, and FS-148E-FPOE models.
- You can use 16 port ranges (source or destination ports) 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-124F, FS-124F-POE, FS-124F-FPOE, FS-148F, FS-148F-POE, and FS-148F-FPOE models.
- You can use up to 32 port ranges (source or destination ports) on the FS-1024D, FS-1024E, FS-T1024E, FS-1048E, FS-3032E, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-M426E-FPOE, FSR-124D, FS-224D-FPOE, FS-248D, FS-224E, FS-224E-POE, FS-248E-POE, FS-248E-FPOE, FS-424E-Fiber, FS-448E, FS-448E-POE, FS-448E-FPOE, FS-524D, FS-524D-FPOE, FS-548D, and FS-548D-FPOE models.
- Port ranges must have the smaller port number as the first number in the range and the larger port number as the second number in the range. For example, you can specify a port range of `8-10` but not `10-8`.
- If you specify a layer-4 port or layer-4 port range (for example, `permit in TCP from any to any 100-200 cnt`) when defining the source or destination in a dynamic ACL entry, FortiSwitchOS discards any port configurations made after the layer-4 configuration.

To enable DACL:

```
config switch-controller security-policy 802-1X
   edit <policy_name>
      set dacl enable
   next
end
```

For example:

```
config switch-controller security-policy 802-1X
   edit "802-1X-policy-default"
      set user-group "radius-users"
      set mac-auth-bypass enable
      set open-auth disable
      set eap-passthru enable
      set eap-auto-untagged-vlans enable
      set guest-vlan disable
      set auth-fail-vlan disable
      set framevid-apply enable
      set radius-timeout-overwrite disable
      set authserver-timeout-vlan disable
```

```
      set dacl enable
   next
end
```

To configure a value for NAS-Filter-Rule:

```
config switch acl service custom
   edit <ACL_service>
      set comment <string>
      set color <0-32>
      set protocol {ICMP | IP | TCP/UDP/SCTP}
      set protocol-number <IP protocol number>
      set tcp-portrange <port_number>-<port_number>
      set udp-portrange <port_number>-<port_number>
   next
end
```

For example:

```
config switch acl service custom
   edit nas-filter-rule-service1
      set comment "NAS filter rule for service 1"
      set udp-portrange 10000-20000
   next
end
```

To use a custom command to configure Filter-Id:

1. Define the Filter-Id attribute.
2. Define the action and classifier.

For example:

```
set command "config switch acl 802-1X %0a edit 403 %0a set filter-id %22 111111 %22 %0a next
     %0a edit 403 %0a config access-list-entry %0a edit 1 %0a config action %0a set count
     enable %0a end %0a config classifier %0a set ether-type 0x800 %0a end %0a end %0a"
```

To display the status of DACLs on a specific FortiSwitch unit:

```
diagnose switch-controller switch-info 802.1X-dacl <FortiSwitch_serial_number>
```

For example:

```
diagnose switch-controller switch-info 802.1X-dacl S548DF5018000776
```

To display the status of DACLs on a specified 802.1X port:

```
diagnose switch-controller switch-info 802.1X-dacl <FortiSwitch_serial_number> <port_name>
```

For example:

```
diagnose switch-controller switch-info 802.1X-dacl S548DF5018000776 port10
```

Defining an 802.1X security policy

You can define multiple 802.1X security policies.

Using the FortiSwitch Manager GUI

To create an 802.1X security policy:

1. Go to *Switch Controller* > *FortiSwitch Port Policies*.
2. Under *Security Policies*, click *Create New*.
3. Enter a name for the new FortiSwitch security policy.
4. For the security mode, click *Port-based* or *MAC-based*.
5. Select + to select which user groups will have access.
6. Enable or disable guest VLANs on this interface to allow restricted access for some users.
7. Enter the number of seconds for authentication delay for guest VLANs. The range is 1-900 seconds.
8. Enable or disable authentication fail VLAN on this interface to allow restricted access for users who fail to access the guest VLAN.
9. Enable or disable MAC authentication bypass (MAB) on this interface.
10. Enable or disable EAP pass-through mode on this interface.
11. Enable or disable whether the session timeout for the RADIUS server will overwrite the local timeout.
12. Select *OK*.

Using the FortiSwitch Manager CLI

To create an 802.1X security policy, use the following commands:

```
config switch-controller security-policy 802-1X
   edit "<policy.name>"
      set security-mode {802.1X | 802.1X-mac-based}
      set user-group <*group_name | Guest-group | SSO_Guest_Users>
      set mac-auth-bypass {enable | *disable}
      set eap-passthru {enable | disable}
      set guest-vlan {enable | *disable}
      set guest-vlan-id "<guest-VLAN-name>"
      set guest-auth-delay <integer>
      set auth-fail-vlan  {enable | *disable}
      set auth-fail-vlan-id "<auth-fail-VLAN-name>"
      set radius-timeout-overwrite {enable | *disable}
      set policy-type 802.1X
      set authserver-timeout-vlan {enable | disable}
      set authserver-timeout-period <integer>
      set authserver-timeout-tagged {lldp-voice | static | disable}
      set authserver-timeout-tagged-vlanid <1-4094>
      set authserver-timeout-vlanid "<RADIUS-timeout-VLAN-name>"
   end
end
```

Option	Description
`set security-mode`	You can restrict access with 802.1X port-based authentication or with 802.1X MAC-based authentication.
`set user-group`	You can set a specific group name, Guest-group, or SSO_Guest_Users to have access. This setting is mandatory.
`set mac-auth-bypass`	You can enable or disable MAB on this interface.

Option	Description
`set eap-passthrough`	You can enable or disable EAP pass-through mode on this interface.
`set guest-vlan`	You can enable or disable guest VLANs on this interface to allow restricted access for some users.
`set guest-vlan-id "<guest-VLAN-name>"`	You can specify the name of the guest VLAN.
`set guest-auth-delay`	You can set the authentication delay for guest VLANs on this interface. The range is 1-900 seconds.
`set auth-fail-vlan`	You can enable or disablethe authentication fail VLAN on this interface to allow restricted access for users who fail to access the guest VLAN.
`set auth-fail-vlan-id "<auth-fail-VLAN-name>"`	You can specify the name of the authentication fail VLAN
`set radius-timeout-overwrite`	You can enable or disable whether the session timeout for the RADIUS server will overwrite the local timeout.
`set policy-type 802.1X`	You can set the policy type to the 802.1X security policy.
`set authserver-timeout-period`	You can set how many seconds the RADIUS server has to authenticate users. The range of values is 3-15 seconds; the default time is 3 seconds. This option is only visible when `authserver-timeout-vlan` is enabled.
`set authserver-timeout-tagged {lldp-voice | static | disable}`	Select whether users are assigned to the specified VLAN when the authentication server times out: • `lldp-voice`—Users are assigned to the VLAN specified in the `set lldp-profile` command (under `config switch-controller managed-switch`). • `static`—Users are assigned to the tagged VLAN specified in the `set authserver-timeout-tagged-vlanid` command. • `disable`—Users are not assigned to a specified VLAN when the authentication server times out. The default is `disable`.
`set authserver-timeout-tagged-vlanid <1-4094>`	Enter the identifier for the tagged VLAN that the system assigns to users when the authentication server times out.
`set authserver-timeout-vlan`	Enable or disable the RADIUS timeout VLAN on this interface to allow limited access for users when the RADIUS server times out before finishing authentication. By default, this option is disabled.
`set authserver-timeout-vlanid "<RADIUS-timeout-VLAN-name>"`	The VLAN name that is used for users when the RADIUS server times out before finishing authentication. This option is only visible when `authserver-timeout-vlan` is enabled.

Applying an 802.1X security policy to a FortiSwitch port

You can apply a different 802.1X security policy to each FortiSwitch port.

Using the FortiSwitch Manager GUI

To apply an 802.1X security policy to a managed FortiSwitch port:

1. Go to *Switch Controller* > *FortiSwitch Ports*.
2. Select the + next to a FortiSwitch unit to expand it.
3. In the *Security Policy* column for a port, click the pencil icon to select a security policy.
4. Click *Apply* to apply the security policy to that port.

Using the FortiSwitch Manager CLI

To apply an 802.1X security policy to a managed FortiSwitch port, use the following commands:

```
config switch-controller managed-switch
   edit <managed-switch>
      config ports
         edit <port>
            set port-security-policy <802.1x-policy>
         next
      end
   next
end
```

Testing 802.1X authentication with monitor mode

Use the monitor mode to test your system configuration for 802.1X authentication. You can use monitor mode to test port-based authentication, MAC-based authentication, EAP pass-through mode, and MAC authentication bypass. Monitor mode is disabled by default. After you enable monitor mode, the network traffic will continue to flow, even if the users fail authentication.

To enable or disable monitor mode:

```
config switch-controller security-policy 802-1X
   edit "<policy_name>"
      set open-auth {enable | disable}
   next
end
```

Clearing authorized sessions

You can clear authorized sessions associated with a specific interface or a specific MAC address.

To clear the 802.1X-authorized session associated with a specific MAC address:

```
execute switch-controller switch-action 802-1X clear-auth-mac <FortiSwitch_serial_number>
     <MAC_address>
```

For example:

```
execute switch-controller switch-action 802-1X clear-auth-mac S548DF5018000776
     4f:8d:c2:73:dd:fe
```

To clear the 802.1X-authorized sessions associated with a specific interface:

```
execute switch-controller switch-action 802-1X clear-auth-port <FortiSwitch_serial_number>
     <port_name>
```

For example:

```
execute switch-controller switch-action 802-1X clear-auth-port S524DF4K15000024 port1
```

RADIUS accounting support

The FortiSwitch unit uses 802.1X-authenticated ports to send five types of RADIUS accounting messages to the RADIUS accounting server to support FortiSwitch Manager RADIUS single sign-on:

- START—The FortiSwitch unit has been successfully authenticated, and the session has started.
- STOP—The FortiSwitch session has ended.
- INTERIM—Periodic messages sent based on the value set using the `set acct-interim-interval` command.
- ON—The FortiSwitch unit will send this message when the switch is turned on.
- OFF—The FortiSwitch unit will send this message when the switch is shut down.

You can specify more than one value to be sent in the RADIUS Service-Type attribute. Use a space between multiple values.

Use the following commands to set up RADIUS accounting so that FortiSwitch Manager can send accounting messages to managed FortiSwitch units:

```
config user radius
   edit <RADIUS_server_name>
      set acct-interim-interval <seconds>
      set switch-controller-service-type {administrative | authenticate-only | callback-
           administrative | callback-framed | callback-login | callback-nas-prompt | call-
           check | framed | login | nas-prompt | outbound}
      config accounting-server
         edit <entry_ID>
            set status {enable | disable}
            set server <server_IP_address>
            set secret <secret_key>
            set port <port_number>
         next
      end
   next
end
```

RADIUS change of authorization (CoA) support

For increased security, each subnet interface that will be receiving CoA requests must be configured with the `set allowaccess radius-acct` command.

RADIUS accounting and CoA support EAP and MAB 802.1X authentication.

The FortiSwitch unit supports two types of RADIUS CoA messages:

- CoA messages to change session authorization attributes (such as data filters and the session-timeout setting) during an active session.

- Disconnect messages (DMs) to flush an existing session. For MAC-based authentication, all other sessions are unchanged, and the port stays up. For port-based authentication, only one session is deleted.

RADIUS CoA messages use the following Fortinet proprietary attribute:

```
Fortinet-Host-Port-AVPair 42 string
```

The format of the value is as follows:

Attribute	Value	Description
Fortinet-Host-Port-AVPair	action=bounce-port	The FortiSwitch unit disconnects all sessions on a port. The port goes down for 10 seconds and then up again.
Fortinet-Host-Port-AVPair	action=disable-port	The FortiSwitch unit disconnects all session on a port. The port goes down until the user resets it.
Fortinet-Host-Port-AVPair	action=reauth-port	The FortiSwitch unit forces the reauthentication of the current session.

In addition, RADIUS CoA use the session-timeout attribute:

Attribute	Value	Description
session-timeout	<session_timeout_value>	The FortiSwitch unit disconnects a session after the specified number of seconds of idleness. This value must be more than 60 seconds. **NOTE:** To use the session-timeout attribute, you must enable the `set radius-timeout-overwrite` command first.

The FortiSwitch unit sends the following Error-Cause codes in RADIUS CoA-NAK and Disconnect-NAK messages.

Error Cause	Error Code	Description
Unsupported Attribute	401	This error is a fatal error, which is sent if a request contains an attribute that is not supported.
NAS Identification Mismatch	403	This error is a fatal error, which is sent if one or more NAS-Identifier Attributes do not match the identity of the NAS receiving the request.
Invalid Attribute Value	407	This error is a fatal error, which is sent if a CoA-Request or Disconnect-Request message contains an attribute with an unsupported value.
Session Context Not Found	503	This error is a fatal error if the session context identified in the CoA-Request or Disconnect-Request message does not exist on the NAS.

Configuring CoA and disconnect messages

Use the following commands to enable a FortiSwitch unit to receive CoA and disconnect messages from a RADIUS server:

```
config system interface
   edit "mgmt"
      set ip <address> <netmask>
      set allowaccess <access_types>
      set type physical
   next
config user radius
   edit <RADIUS_server_name>
      set radius-coa {enable | disable}
      set radius-port <port_number>
      set secret <secret_key>
      set server <server_name_IPv4>
   end
```

Variable	Description
config system interface	
ip <address> <netmask>	Enter the interface IP address and netmask.
allowaccess <access_types>	Enter the types of management access permitted on this interface. Valid types are as follows: `http https ping snmp ssh telnet radius-acct`. Separate each type with a space. You must include `radius-acct` to receive CoA and disconnect messages.
<RADIUS_server_name>	Enter the name of the RADIUS server that will be sending CoA and disconnect messages to the FortiSwitch unit. By default, the messages use port 3799.
config user radius	
radius-coa {enable | disable}	Enable or disable whether the FortiSwitch unit will accept CoA and disconnect messages. The default is disable.
radius-port <port_number>	Enter the RADIUS port number. By default, the value is 0 for FortiSwitch Manager, which uses port 1812 for the FortiSwitch unit in FortiLink mode.
secret <secret_key>	Enter the shared secret key for authentication with the RADIUS server. There is no default.
server <server_name_IPv4>	Enter the domain name or IPv4 address for the RADIUS server. There is no default.

Example: RADIUS CoA

The following example uses the FortiSwitch Manager CLI to enable the FortiSwitch unit to receive CoA and disconnect messages from the specified RADIUS server:

```
config switch-controller security-policy local-access
```

```
    edit default
      set internal-allowaccess ping https http ssh snmp telnet radius-acct
    next
end
config user radius
    edit "Radius-188-200"
      set radius-coa enable
      set radius-port 0
      set secret ENC
           +2NyBcp8JF3/OijWl/w5nOC++aDKQPWnlC8Ug2HKwn4RcmhqVYE+q07yI9eSDhtiIw63kR/oMBLGwFQoe
           ZfOQWengIlGTb+YQo/lYJn1V3Nwp9sdkcblfyayfc9gTeqe+mFltKl5IWNI7WRYiJC8sxaF9Iyr2/l4hp
           CiVUMiPOU6fSrj
      set server "10.105.188.200"
    next
end
```

Detailed deployment notes

- Using more than one security group (with the `set security-groups` command) per security profile is not supported.
- CoA and single sign-on are supported only by the CLI in this release.
- RADIUS CoA is supported in standalone mode. In addition, RADIUS CoA is supported in FortiLink mode when NAT is disabled in the firewall policy (`set nat disable` under the `config firewall policy` command), and the interfaces on the link between FortiSwitch Manager and FortiSwitch unit are assigned routable addresses other than 169.254.1.x.
- The FortiSwitch unit supports using FortiAuthenticator, FortiConnect, Microsoft Network Policy Server (NPS), Aruba ClearPass, and Cisco Identity Services Engine (ISE) as the RADIUS server for CoA and RSSO.
- Each RADIUS CoA server can support only one accounting manager in this release.
- RADIUS accounting/CoA/VLAN-by-name features are supported only with `eap-passthru enable`.
- Fortinet recommends a unique secret key for each accounting server.
- For CoA to correctly function with FortiAuthenticator or FortiConnect, you must include the User-Name attribute (you can optionally include the Framed-IP-Address attribute) *or* the User-Name and Calling-Station-ID attributes in the CoA request.
- To obtain a valid Framed-IP-Address attribute value, you need to manually configure DHCP snooping in the 802.1X-authenticated ports of your VLAN network for both port and MAC modes.
- Port-based basic statistics for RADIUS accounting messages are supported in the Accounting Stop request.
- By default, the accounting server is disabled. You must enable the accounting server with the `set status enable` command.
- The default port for FortiAuthenticator single sign-on is 1813 for the FortiSwitch unit.
- In MAC-based authentication, the maximum number of client MAC addresses is 20. Each model has its own maximum limit.
- Static MAC addresses and sticky MAC addresses are mechanisms for manual/local authorization; 802.1X is a mechanism for protocol-based authorization. Do not mix them.
- Fortinet recommends an 802.1X setup rate of 5 to 10 sessions per second.
- When 802.1X authentication is configured, the EAP pass-through mode (`set eap-passthru`) is enabled by default.
- For information about the RADIUS attributes supported by FortiSwitchOS, refer to the “Supported attributes for RADIUS CoA and RSSO” appendix in the *FortiSwitchOS Administration Guide—Standalone Mode*.

Configuring the DHCP trust setting

The DHCP blocking feature monitors the DHCP traffic from untrusted sources (for example, typically host ports and unknown DHCP servers) that might initiate traffic attacks or other hostile actions. To prevent this, DHCP blocking filters messages on untrusted ports.

Set the port as a trusted or untrusted DHCP-snooping interface:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set dhcp-snooping {trusted | untrusted}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set dhcp-snooping trusted
         end
      end
```

Configuring the DHCP server access list

You can configure which DHCP servers that DHCP snooping includes in the server access list. These servers on the list are allowed to respond to DHCP requests.

NOTE: You can add 255 servers per table. The maximum number of DHCP servers that can be added to all instances of the table is 2,048. This maximum is a global limit and applies across all VLANs.

Configuring the DHCP server access list consists of the following steps:

1. Enable the DHCP server access list on a VDOM level or switch-wide level.
   By default, the server access list is disabled, which means that all DHCP servers are allowed. When the server access list is enabled, only the DHCP servers in the server access list are allowed.
2. Configure the VLAN settings for the managed switch port.
   You can set the DHCP server access list to `global` to use the VDOM or system-wide setting, or you can set the DHCP server access list to `enable` to override the global settings and enable the DHCP server access list.
   In the managed FortiSwitch unit, all ports are untrusted by default, and DHCP snooping is disabled on all untrusted ports. You must set the managed switch port to be trusted to allow DHCP snooping.
3. Configure DHCP snooping and the DHCP access list for the managed FortiSwitch interface.
   By default, DHCP snooping is disabled on the managed FortiSwitch interface.

To enable the DHCP sever access list on a global level:

```
config switch-controller global
   set dhcp-server-access-list enable
end
```

For example:

```
FSWMVMTM21000008 (root) # config switch-controller global
FSWMVMTM21000008 (global) # set dhcp-server-access-list enable
FSWMVMTM21000008 (global) # end
```

To configure the VLAN settings:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set dhcp-server-access-list {global | enable | disable}
      config ports
         edit <port_name>
            set vlan <VLAN_name>
            set dhcp-snooping trusted
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S524DN4K16000116"
      set fsw-wan1-peer "port11"
      set fsw-wan1-admin enable
      set dhcp-server-access-list enable
      config ports
         edit "port19"
            set vlan "_default.13"
            set allowed-vlans "quarantine.13"
            set untagged-vlans "quarantine.13"
            set dhcp-snooping trusted
            set export-to "vdom1"
         next
      end
   next
end
```

To configure the interface settings:

```
config system interface
   edit <VLAN_name>
      set switch-controller-dhcp-snooping enable
      config dhcp-snooping-server-list
         edit <DHCP_server_name>
            set server-ip <IPv4_address_of_DHCP_server>
         next
      end
   next
end
```

For example:

```
config system interface
   edit "_default.13"
      set vdom "vdom1"
      set ip 5.4.4.1 255.255.255.0
      set allowaccess ping https ssh http fabric
```

```
      set alias "_default.port11"
      set snmp-index 30
      set switch-controller-dhcp-snooping enable
      config dhcp-snooping-server-list
         edit "server1"
            set server-ip 10.20.20.1
         next
      end
      set switch-controller-feature default-vlan
      set interface "port11"
      set vlanid 1
   next
end
```

Including option-82 data

This feature requires FortiSwitch Manager 7.2.5 and FortiSwitchOS 7.2.2 or later.

You can now include option-82 data in the DHCP request for DHCP snooping. DHCP option-82 data provides additional security by enabling a controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. You can select a fixed format (`set dhcp-option82-format legacy`) for the Circuit ID and Remote ID fields or select which values appear in the Circuit ID and Remote ID fields (`set dhcp-option82-format ascii`).

The following is the fixed format for the option-82 Circuit ID field:

```
hostname-[<vlan:16><mod:8><port:8>].32bit
```

The following is the fixed format for the option-82 Remote ID field:

```
[mac(0..6)].48bit
```

If you want to select which values appear in the Circuit ID and Remote ID fields:

- For the Circuit ID field, you can include the interface name, VLAN name, host name, mode, and description.
- For the Remote ID field, you can include the MAC address, host name, and IP address.

You can specify whether the DHCP-snooping client only broadcasts packets on trusted ports in the VLAN (`set dhcp-snoop-client-req drop-untrusted`) or broadcasts packets on all ports in the VLAN (`set dhcp-snoop-client-req forward-untrusted`).

You can set a limit for how many entries are in the DHCP-snooping binding database for each port with the `set dhcp-snoop-db-per-port-learn-limit` command. By default, the number of entries is 64. The range of values depends on the switch model.

Before configuring the learning limit, check the range for your switch model by typing `set dhcp-snoop-db-per-port-learn-limit ?`.

You can also specify how long entries are kept in the DHCP-snooping server database with the `set dhcp-snoop-client-db-exp` command. By default, the entries are kept for 86,400 seconds. The range of values is 300-259,200 seconds.

You can use the `diagnose switch-controller switch-info option82-mapping snooping` command to display option-82 Circuit ID and Remote ID values in ASCII or hexadecimal format. This command requires the serial number of the managed switch unit and VLAN identifier. Specifying the port name is optional.

If you have included option-82 data in the DHCP request, it applies globally. You can override the global option-82 setting to specify plain text strings for the Circuit ID field and the Remote ID field for a specific VLAN on a port. If `dhcp-snoop-option82-override` is not configured for the incoming VLAN and switch interface, the settings for the Circuit ID and Remote ID fields are taken from the global option-82 configuration.

NOTE: The values for the Circuit ID and Remote ID field are either both taken from the global option-82 configuration or both taken from the `dhcp-snoop-option82-override` settings. The system cannot take one value at the global level and the other value from the override settings.

Each plain text string can be a maximum of 256 characters long. Together, the combined length of both plain text strings can be a maximum of 256 characters long.

NOTE: You can override the option-82 settings for DHCP snooping but not for DHCP relay.

To configure the option-82 data on a global level:

```
config switch-controller global
   set dhcp-option82-format {ascii | legacy}
   set dhcp-option82-circuit-id {intfname <interface_name> | vlan <VLAN_name> | hostname
        <host_name> | mode <mode> | description <string>}
   set dhcp-option82-remote-id {mac <MAC_address> | hostname <host_name> | ip <IP_address>}
   set dhcp-snoop-client-req {drop-untrusted | forward-untrusted}
   set dhcp-snoop-client-db-exp <300-259200>
   set dhcp-snoop-db-per-port-learn-limit <integer>
end
```

To display option-82 Circuit ID and Remote ID values in ASCII format:

```
diagnose switch-controller  switch-info option82-mapping snooping ascii <FortiSwitch_serial_
     number> <VLAN_ID> <port_name>
```

For example:

```
diagnose switch-controller  switch-info option82-mapping snooping ascii S524DN4K16000116
     vlan11 port3
```

To display option-82 Circuit ID and Remote ID values in hexadecimal format:

```
diagnose switch-controller  switch-info option82-mapping snooping hex <FortiSwitch_serial_
     number> <VLAN_ID> <port_name>
```

For example:

```
diagnose switch-controller  switch-info option82-mapping snooping hex S524DN4K16000116
     vlan11 port5
```

To override the option-82 global settings for a specific VLAN on a port:

```
config switch-controller managed-switch
   edit "<FortiSwitch_serial_number>"
```

```
      config ports
         edit "<port_name>"
            config dhcp-snoop-option82-override
               edit <VLAN_name>
                  set remode-id <string>
                  set circuit-id <string>
               next
            end
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S524DF4K15000024"
      config ports
         edit "port10"
            config dhcp-snoop-option82-override
               edit vlan15
                  set remode-id "remote-id test"
                  set circuit-id "circuit-id test"
               next
            end
         next
      end
   next
end
```

Configuring dynamic ARP inspection (DAI)

DAI prevents man-in-the-middle attacks and IP address spoofing by checking that packets from untrusted ports have valid IP-MAC-address binding. DAI allows only valid ARP requests and responses to be forwarded.

To use DAI, you must first enable the DHCP-snooping feature, enable DAI, and then enable DAI for each VLAN. By default, DAI is disabled on all VLANs.

After enabling DHCP snooping with the `set switch-controller-dhcp-snooping enable` command, use the following CLI commands to enable DAI and then enable DAI for a VLAN:

```
config system interface
   edit vsw.test
      set switch-controller-arp-inpsection {enable | disable}
   end

config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set arp-inspection-trust <untrusted | trusted>
         next
      end
   next
end
```

Use the following CLI command to check DAI statistics for a FortiSwitch unit:

```
diagnose switch-controller switch-info arp-inspection stats <FortiSwitch_serial_number>
```

Use the following CLI command to delete DAI statistics for a specific VLAN:

```
diagnose switch-controller switch-info arp-inspection stats-clear <VLAN_ID> <FortiSwitch_
     serial_number>
```

Monitoring ARP packets

Starting in FortiSwitch Manager 7.2.5, you can monitor ARP packets for a specific VLAN on a DHCP-snooping trusted port of a managed switch and save the VLAN ID, MAC addresses, and IP addresses in the DHCP-snooping database. The static IP addresses can be used in RADIUS accounting.

To monitor ARP packets:

1. Enable DHCP snooping and enable the monitoring of ARP packets for a specific VLAN.

```
config system interface
   edit <VLAN_ID>
      set switch-controller-dhcp-snooping enable
      set switch-controller-arp-inspection monitor
   next
end
```

2. Enable the monitoring of ARP packets on a DHCP-snooping trusted port.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set dhcp-snooping trusted
            set allow-arp-monitor enable
         next
      end
   next
end
```

Configuring DHCP-snooping static entries

After you enable DHCP snooping for a VLAN, you can configure static entries by binding an IPv4 address with a MAC address for a specific switch interface:

- Specify a VLAN that has DHCP snooping enabled. The VLAN must be a native VLAN or allowed VLAN for the port.
- Specify a port that is not defined as trusted.
- Specify the MAC address in the form of xx:xx:xx:xx:xx:xx.
- Bind a single MAC address to a single IPv4 address. Multiple IP addresses cannot be bound to the same MAC address. The MAC address cannot be used in more than one static entry. Duplicate static entries are not supported on a VLAN.

DHCP-snooping static entries must be configured to be able to use DAI for IP/MAC entries not discovered by DHCP snooping.

Specifying the VLAN, IP address, MAC address, and interface name is required.

You can specify a maximum of 64 DHCP static entries for the entire FortiSwitch unit.

- You cannot use a DHCP trusted switch interface or an 802.1X interface for the static entry's switch interface.
- After you configure a DHCP-snooping static entry for a VLAN, you cannot remove that VLAN from the switch interface.
- After you configure a DHCP-snooping static entry for a switch interface, the switch interface cannot be included as a member of a trunk until the DHCP-snooping static entry is deleted.
- If you configure a DHCP-snooping static entry for a trunk, the trunk cannot be deleted until the DHCP-snooping static entry is deleted.

To create a static entry for DHCP snooping and DAI:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config dhcp-snooping-static-client
         edit <DHCP_static_client_name>
            set vlan <VLAN_ID>
            set ip <DHCP_static_client_static_IP_address>
            set mac <DHCP_static_client_MAC_address>
            set port <interface_name>
         next
      next
   end
```

For example:

```
config switch-controller managed-switch
   edit S524DN4K16000116
      config dhcp-snooping-static-client
         edit DHCPclient
            set vlan 100
            set ip 192.168.101.1
            set mac 00:21:cc:d2:76:72
            set port port19
         next
      next
   end
```

Configuring IPv4 source guard

IPv4 source guard protects a network from IPv4 spoofing by only allowing traffic on a port from specific IPv4 addresses. Traffic from other IPv4 addresses is discarded. The discarded addresses are not logged.

IPv4 source guard allows traffic from the following sources:

- Static entries—IP addresses that have been manually associated with MAC addresses.
- Dynamic entries—IP addresses that have been learned through DHCP snooping.

By default, IPv4 source guard is disabled. You must enable it on each port that you want protected.

If you add more than 2,048 IP source guard entries from FortiSwitch Manager, you will get an error. When there is a conflict between static entries and dynamic entries, static entries take precedence over dynamic entries.

IPv4 source guard can be configured in FortiSwitch Manager. The following FortiSwitch models support IP source guard:

- FSR-124D
- FS-224D-FPOE
- FS-248D
- FS-424D-POE
- FS-424D-FPOE
- FS-448D-POE
- FS-448D-FPOE
- FS-424D
- FS-448D
- FSW-2xxE

Configuring IPv4 source guard consists of the following steps:

1. Enabling IPv4 source guard on page 109
2. Creating static entries on page 110
3. Checking the IPv4 source-guard entries on page 110

Enabling IPv4 source guard

You must enable IPv4 source guard in the FortiSwitch Manager CLI before you can configure it.

To enable IPv4 source guard:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number
      config ports
         edit <port_name>
            set ip-source-guard enable
         next
      end
   end
```

For example:

```
config switch-controller managed-switch
   edit S424DF4K15000024
      config ports
         edit port20
            set ip-source-guard enable
         next
      end
   end
```

Creating static entries

After you enable IPv4 source guard in the FortiSwitch Manager CLI, you can create static entries in the FortiSwitch Manager CLI by binding IPv4 addresses with MAC addresses. For IPv4 source-guard dynamic entries, you need to configure DHCP snooping. See Configuring DHCP blocking, STP, and loop guard on managed FortiSwitch ports on page 58.

To create static entries:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ip-source-guard
         edit <port_name>
            config binding-entry
               edit <id>
                  set ip <xxx.xxx.xxx.xxx>
                  set mac <XX:XX:XX:XX:XX:XX>
               next
            end
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit S424DF4K15000024
      config ip-source-guard
         edit port4
            config binding-entry
               edit 1
                  set ip 172.168.20.1
                  set mac 00:21:cc:d2:76:72
               next
            end
         next
      end
   next
end
```

Checking the IPv4 source-guard entries

After you configure IPv4 source guard , you can check the entries.

Static entries are manually added by the `config switch ip-source-guard` command. Dynamic entries are added by DHCP snooping.

Use this command in the FortiSwitch Manager CLI to display all IP source-guard entries:

```
diagnose switch-controller switch-info ip-source-guard hardware <FortiSwitch_serial_number>
```

Configuring an ACL

Starting in FortiSwitch Manager 7.2.5, you can use an access control list (ACL) to configure a policy for the ingress stage of the pipeline for incoming traffic. After creating an ACL group for the ingress policy, you apply the ACL group to a managed switch port.

A user-configurable ACL might conflict with or be overridden by an ACL implemented by other managed FortiSwitch features. If a user-configurable ACL and an internal ACL do not conflict, the resulting behavior depends on the FortiSwitch model. Fortinet recommends validating user-configurable ACLs to make certain that they operate correctly with other enabled features.

To use an ACL:

1. Create an ACL ingress policy.
2. Create an ACL group and add the ingress policy to it.
3. Apply the ACL group to a managed switch port.
4. View the counters on page 113.

Create an ACL ingress policy

The ACL ingress policy includes the following key attributes:

- *Interface*—The port on which traffic arrives at the switch. The policy applies to ingress traffic only (not egress traffic).
- *Classifier*—The classifier identifies the packets that the policy will act on. Each packet can be classified based on one or more criteria. The supported criteria are source and destination MAC address, VLAN identifier, and source and destination IP address.
- *Actions*—If a packet matches the classifier criteria for a given ACL, the following types of action can be applied to the packet:
  - Allow or block the packet
  - Count the number of ingress packets

The switch uses specialized TCAM memory to perform ACL matching.

The order of the classifiers provided during group creation (or during an ACL update in a group when new classifiers are added) matter. Hardware resources are allocated as best fit at the time of creation, which can cause some fragmentation and segmentation of hardware resources because not all classifiers are available at all times. Because the availability of classifiers is order dependent, some allocations succeed or fail at different times.

To create an ACL ingress policy in the CLI:

```
config switch-controller acl ingress
   edit <policy_identifier>
      config action
         set count {enable | disable}
         set drop {enable | disable}
      end
```

```
      config classifier
         set dst-ip-prefix <IPv4_address> <netmask>
         set dst-mac <destination_MAC_address>
         set src-ip-prefix <IPv4_address> <netmask>
         set src-mac <source_MAC_address>
         set vlan <1-4094>
      end
   next
end
```

Create an ACL group

An ACL group contains one or more ACLs.

The ACL ingress policies are assigned to ACL group 3 in the managed FortiSwitch unit. If the managed FortiSwitch unit does not support ACL group 3, the user-configurable ACL is not supported.

To create an ACL group in the CLI:

```
config switch-controller acl group
   edit "<ACL_group_name>"
      set ingress <policy_identifier1> <policy_identifier2> ...
   next
end
```

For example:

```
config switch-controller acl group
   edit "ACLgroup1"
      set ingress 2 3 4
   next
end
```

Apply the ACL group to a managed switch port

You can apply one or more ACL groups to a managed switch port.

To apply an ACL group to a managed switch port in the CLI:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <managed_switch_port_name>
            set acl-group "<ACL_group_name1> <ACL_group_name2> ..."
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
```

```
   edit FS1D243Z14000016
      config ports
         edit port10
            set acl-group "ACLgroup1 ACLgroup2 ACLgroup3"
         next
      end
   next
end
```

View the counters

On the FS-4xxE, FS-1xxE, and FS-1xxF platforms, the ACL byte counters are not available (they will always show as 0 on the CLI). The packet counters are available.

You can use the CLI to view the counters associated with the ingress policies.

To view the counters in the CLI:

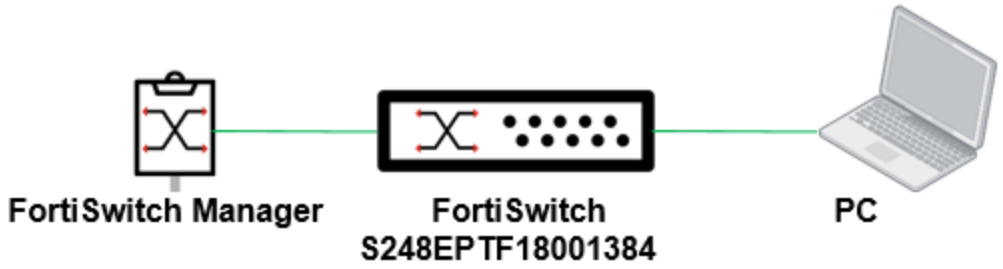
```
diagnose switch-controller switch-info acl-counters <FortiSwitch_serial_number>
```

For example:

```
diagnose switch-controller switch-info acl-counters FS1D243Z14000016
```

Configuration example

In the following example, the ingress ACL policy prevents a PC connected to S248EPTF18001384 (which is managed by FortiSwitch Manager) from accessing `8.8.8.8 255.255.255.255`.




```
config switch-controller acl ingress
   edit 1
      config action
         set drop enable
      end
      config classifier
         set dst-ip-prefix 8.8.8.8 255.255.255.255
         set src-mac 00:0c:29:d4:4f:3c
      end
   next
end

config switch-controller acl group
```

```
    edit "group1"
      set ingress 1
    next
  end

  config switch-controller managed-switch
    edit "S248EPTF18001384"
      config ports
        edit "port6"
          set acl-group "group1"
        next
      end
    next
  end
```

Configuring layer-3 routing on FortiSwitch units

To use layer-3 routing on FortiSwitch units, the managed switches must be running FortiSwitchOS 7.2.0 or later.

You can configure the following layer-3 routing on FortiSwitch units:

- Static routes for IPv4 traffic on page 116

  You add static routes to manually control traffic exiting the FortiSwitch unit. You configure routes by specifying destination IP addresses and network masks and adding gateways for these destination addresses. Gateways are the next-hop routers to which traffic that matches the destination addresses in the route are forwarded.
- Switch virtual interfaces on page 117

  A switch virtual interface (SVI) is a logical interface that is associated with a VLAN and supports routing and switching protocols.

  You can assign an IP address to the SVI to enable routing between VLANs. For example, SVIs can route between two different VLANs connected to a switch (no need to connect through a layer-3 router).
- Routed VLAN interfaces on page 120

  A routed VLAN interface (RVI) is a physical port or trunk interface that supports layer-3 routing protocols. When the physical port or trunk is administratively down, the RVI for that physical port or trunk goes down as well. All RVIs use the same VLAN, 4095.

  RVIs support ECMP, multiple IP addresses, IPv4 addresses, IPv6 addresses, BFD, VRRP, DHCP server, DHCP relay, RIP, OSPF, ISIS, BGP, and PIM. VRF support of RVIs on managed switches requires FortiSwitchOS 7.2.1 or later.
- Virtual routing and forwarding on page 120

  You can use the virtual routing and forwarding (VRF) feature to create multiple routing tables within the same router.

  After you create a VRF instance, you can assign the VRF instance to an SVI or RVI when you create the SVI or RVI or assign the VRF instance to an IPv4 static route when you create the static route.

  You need to configure VRF before using the VRF instance in an SVI or RVI configuration.

Static routes for IPv4 traffic

If you use the same sequence number for a static route in FortiSwitch Manager and an existing route on a managed switch, the FortiSwitch Manager static route will overwrite the managed switch static route. Managed switches might have existing static routes that are necessary for the management connection or for networking, such as VXLAN. To avoid overwriting any existing static routes on managed switches, use higher numbers (such as 100 and higher) for the sequence numbers for FortiSwitch Manager static routes.

You cannot use the management port of a FortiSwitch unit in the `set device` command. FortiSwitch Manager cannot create static routes that use the management port of a FortiSwitch unit as the device. If static routes must include the management port, add the routes using custom commands or add the static route directly on the FortiSwitch unit.

```
config switch-controller managed-switch
   edit <FortiSwitch-serial-number>
      config router-static
         edit <sequence_number>
            set switch-id <FortiSwitch-serial-number>
            set blackhole {enable | disable}
            set comment <string>
            set device <interface_name>
            set distance <1-255>
            set dst <destination-address_IPv4mask>
            set dynamic-gateway {enable | disable}
            set gateway <gateway-address_IPv4>
            set status {enable | disable}
            set vrf <VRF_name>
         next
      end
   next
end
```

Variable	Description	Default
<sequence_number>	Enter a sequence number for the static route. **NOTE:** To avoid overwriting any existing static routes on managed switches, use higher numbers (such as 100 and higher) for the sequence numbers for FortiSwitch Manager static routes.	No default
switch-id <FortiSwitch-serial-number>	Enter the serial number for the managed FortiSwitch unit.	No default
blackhole {enable | disable}	Enable or disable dropping all packets that match this route.	disable
comment <string>	Optionally enter a descriptive comment.	No default

Variable	Description	Default
device <interface_name>	Enter the name of the interface through which to route traffic. Enter '?' to see a list of interfaces. **NOTE:** You cannot use the management port of a FortiSwitch unit in the `set device` command	No default
distance <1-255>	Enter the administrative distance for the route.	10
dst <destination-address_IPv4mask>	Enter the destination IPv4 address and network mask for this route. You can enter `0.0.0.0/0` to create a new static default route.	0.0.0.0 0.0.0.0
dynamic-gateway {enable | disable}	When enabled, the route gateway IP is obtained using DHCP running on the provided route's device interface.	disable
gateway <gateway-address_IPv4>	Enter the IPv4 address of the next-hop router to which traffic is forwarded.	0.0.0.0
status {enable | disable}	Enable this setting for the route to be added to the routing table.	enable
vrf <VRF_name>	Enter the name of the VRF instance.	No default

For example:

```
config switch-controller managed-switch
   edit S548DF5018000776
      config router-static
         edit 1
            set switch-id "S108DVM4HDA47J08"
            set comment "staticroute1.1.1.1"
            set device "vlan101"
            set distance 101
            set dst 5.5.5.0 255.255.255.0
            set gateway 101.1.1.2
            set vrf "vpn1"
         next
      end
   next
end
```

Switch virtual interfaces

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config system-interface
         edit <SVI_name>
            set switch-id <FortiSwitch_serial_number>
            set allowaccess {https | http | ping | radius-acct | snmp | ssh | telnet}
            set distance
            set interface <interface_name>
            set ip <IP_address_and_mask>
            set mode {static | dhcp}
            set status {up | down}
```

```
            set type vlan
            set vlan <id_number>
            set vrf <VRF_name>
        next
    end
  next
end
```

Variable	Description	Default
<SVI_name>	Enter the name for the new SVI. **NOTE:** Avoid reserved names or system-created names, such as those listed in Reserved names on page 119.	No default
switch-id <FortiSwitch-serial-number>	Enter the serial number for the managed FortiSwitch unit.	No default
allowaccess {https | http | ping | radius-acct | snmp | ssh | telnet}	Enter the types of management access permitted on this interface or secondary IP address. Separate each type with a space. To add or remove an option from the list, retype the complete list as required.	No default
distance <1-255>	Enter the distance for routes learned through PPPoE or DHCP, with the lowest number indicating the preferred route. This option is available when `mode` is set to `dhcp`.	5
interface <interface_name>	Enter the name of the interface. This option is only available when `vlanid` is set.	internal
ip <IP_address_and_mask>	Enter the interface IP address and netmask. This option is available when `mode` is set to `static`. You can set the IP and netmask, but they are not displayed. This is only available in NAT/Route mode. The IP address cannot be on the same subnet as any other interface.	0.0.0.0 0.0.0.0
mode {static | dhcp}	Configure the connection mode for the interface as one of: • `static` — configure a static IP address for the interface. • `dhcp` — configure the interface to receive its IP address from an external DHCP server.	static
status {up | down}	Start or stop the interface. If the interface is stopped, it does not accept or send packets. If you stop a physical interface, associated virtual interfaces such as VLAN interfaces will also stop.	up
type vlan	Enter `vlan` for a virtual LAN interface. This is the type of interface created by default on any existing physical interface. VLANs increase the number of network interfaces beyond the physical connections on the system. VLANs cannot be configured on a switch mode interface in Transparent mode.	vlan

Variable	Description	Default
vlan <id_number>	**NOTE:** This VLAN must have been created in FortiSwitch Manager using the `config system interface` command. Enter a VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface. The VLAN ID can be any number between 1 and 4094, as 0 and 4095 are reserved, but it must match the VLAN ID added by the IEEE 802.1Q-compliant router on the other end of the connection. Two VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID. However, you can add two or more VLAN subinterfaces with the same VLAN ID to different physical interfaces, and you can add more multiple VLANs with different VLAN IDs to the same physical interface. This is available only when editing an interface with a type of `vlan`.	No default
vrf <VRF_name>	Enter the name of the VRF instance.	No default

For example:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config system-interface
         edit "svi1"
            set switch-id "S108DVM4HDA47J08"
            set ip 101.1.1.2 255.255.255.0
            set distance 100
            set allowaccess ping https http ssh snmp telnet radius-acct
            set type vlan
            set vlan "vlan101"
            set vrf "vpn2"
         next
      end
   next
end
```

Reserved names

Using FortiSwitch reserved names or system-created names for RVI, SVI, or VRF names can cause synchronization errors. Avoid using the following names:

- flink.sniffer
- flink
- rpsan
- internal
- mgmt
- mgmt*n*, such as mgmt1, mgmt2, mgmt3, …, mgmt10, mgmt11, mgmt12, …
- sp*n*, such as sp1, sp2, sp3, …, sp10, sp11, sp12, …
- ppp
- p*n*, such as p1, p2, p3, …, p10, p11, p12,…
- __port__*n*, such as __port__1, __port__2, __port__3, …, __port__10, __port__11, __port__12, …

Routed VLAN interfaces

Avoid using a reserved name or system-created name for the RVI name. See Reserved names on page 119.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config system-interface
         edit <RVI_name>
            set switch-id <FortiSwitch_serial_number>
            set allowaccess {https | http | ping | radius-acct | snmp | ssh | telnet}
            set ip <IP_address_and_netmask>
            set type physical
            set interface <existing_interface_name>
            set vrf <VRF_name>
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config system-interface
         edit "RVI31"
            set switch-id "S548DF4K17000019"
            set ip 50.31.1.2 255.255.255.0
            set allowaccess ping https http ssh snmp telnet radius-acct
            set type physical
            set interface "port21"
            set vrf "vpn31"
         next
      end
   next
end
```

Virtual routing and forwarding

You need to configure VRF before using the VRF instance in an SVI or RVI configuration.

Use the following steps to configure VRF:

1. Create a VRF instance.
2. Assign the VRF instance to an SVI or RVI or assign the VRF to an IPv4 static route.

NOTE:

- The VRF name cannot be the same as a reserved name or system-created name, such as those listed in Reserved names on page 119.

  The VRF name cannot match any SVI name.
- The VRF identifier is a number in the range of 1-1023, except for 252, 253, 254, and 255. You cannot assign the same VRF identifier to more than one VRF instance. After the VRF instance is created, the VRF identifier cannot be changed.
- After the SVI or RVI is created, the VRF instance cannot be changed or unset. You can assign the same VRF instance to more than one SVI or RVI. The VRF instance cannot be assigned to an internal SVI.
- After the static route is created, the VRF instance cannot be changed or unset. You can assign the same VRF instance to more than one static route.

To create the VRF instance:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config router-vrf
         edit <VRF_name>
            set vrfid <VRF_identifier>
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   set switch-id "S548DF4K17000019"
      config router-vrf
         edit vrfv4
            set vrfid 1
         next
         edit vrfv6
            set vrfid 2
         next
      end
   next
end
```

Configuring QoS with managed FortiSwitch units

Quality of Service (QoS) provides the ability to set particular priorities for different applications, users, or data flows.

NOTE: FortiSwitch Manager does not support QoS for hard or soft switch ports.

The FortiSwitch unit supports the following QoS configuration capabilities:

- Mapping the IEEE 802.1p and Layer 3 QoS values (Differentiated Services and IP Precedence) to an outbound QoS queue number.
- Providing eight egress queues on each port.
- Policing the maximum data rate of egress traffic on the interface.
- If you select `weighted-random-early-detection` for the `drop-policy`, you can enable explicit congestion notification (ECN) marking to indicate that congestion is occurring without just dropping packets.

To configure the QoS for managed FortiSwitch units:

1. Configure a Dot1p map.

   A Dot1p map defines a mapping between IEEE 802.1p class of service (CoS) values (from incoming packets on a trusted interface) and the egress queue values. Values that are not explicitly included in the map will follow the default mapping, which maps each priority (0-7) to queue 0. If an incoming packet contains no CoS value, the switch assigns a CoS value of zero.

   NOTE: Do not enable trust for both Dot1p and DSCP at the same time on the same interface. If you do want to trust both Dot1p and IP-DSCP, the FortiSwitch uses the latter value (DSCP) to determine the queue. The switch will use the Dot1p value and mapping only if the packet contains no DSCP value.

   ```
   config switch-controller qos dot1p-map
      edit <Dot1p map name>
         set description <text>
         set priority-0 <queue number>
         set priority-1 <queue number>
         set priority-2 <queue number>
         set priority-3 <queue number>
         set priority-4 <queue number>
         set priority-5 <queue number>
         set priority-6 <queue number>
         set priority-7 <queue number>
      next
   end
   ```

2. Configure a DSCP map. A DSCP map defines a mapping between IP precedence or DSCP values and the egress queue values. For IP precedence, you have the following choices:
   - `network-control`—Network control
   - `internetwork-control`—Internetwork control
   - `critic-ecp`—Critic and emergency call processing (ECP)
   - `flashoverride`—Flash override
   - `flash`—Flash
   - `immediate`—Immediate

- priority—Priority
- routine—Routine

```
config switch-controller qos ip-dscp-map
   edit <DSCP map name>
      set description <text>
      configure map <map_name>
         edit <entry name>
            set cos-queue <COS queue number>
            set diffserv {CS0 | CS1 | AF11 | AF12 | AF13 | CS2 | AF21 | AF22 | AF23 | CS3
                 | AF31 | AF32 | AF33 | CS4 | AF41 | AF42 | AF43 | CS5 | EF | CS6 | CS7}
            set ip-precedence {network-control | internetwork-control | critic-ecp |
                 flashoverride | flash | immediate | priority | routine}
            set value <DSCP raw value>
         next
      end
   end
```

3. Configure the egress QoS policy. In a QoS policy, you set the scheduling mode for the policy and configure one or more CoS queues. Each egress port supports eight queues, and three scheduling modes are available:
   - With strict scheduling, the queues are served in descending order (of queue number), so higher number queues receive higher priority.
   - In simple round-robin mode, the scheduler visits each backlogged queue, servicing a single packet from each queue before moving on to the next one.
   - In weighted round-robin mode, each of the eight egress queues is assigned a weight value ranging from 0 to 63.

```
config switch-controller qos queue-policy
   edit <QoS egress policy name>
      set schedule {strict | round-robin | weighted}
      config cos-queue
      edit queue-<number>
         set description <text>
         set min-rate <rate in kbps>
         set max-rate <rate in kbps>
         set drop-policy {taildrop | weighted-random-early-detection}
         set ecn {enable | disable}
         set weight <weight value>
         next
      end
   next
end
```

4. Configure the overall policy that will be applied to the switch ports.

```
config switch-controller qos qos-policy
   edit <QoS egress policy name>
      set default-cos <default CoS value 0-7>
      set trust-dot1p-map <Dot1p map name>
      set trust-ip-dscp-map <DSCP map name>
      set queue-policy <queue policy name>
   next
end
```

5. Configure each switch port.

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port>
            set qos-policy <CoS policy>
         next
      end
   next
end
```

6. Check the QoS statistics on each switch port.

```
diagnose switch-controller switch-info qos-stats <FortiSwitch_serial_number> <port_name>
```

Configuring ECN for managed FortiSwitch devices

Explicit Congestion Notification (ECN) allows ECN enabled endpoints to notify each other when they are experiencing congestion. It is supported on the following FortiSwitch models: FS-3032E, FS-3032D, FS-1048E, FS-1048D, FS-5xxD series, and FS-4xxE series.

On FortiSwitch Manager, ECN can be enabled for each class of service (CoS) queue to enable packet marking to drop eligible packets. The command is only available when the dropping policy is weighted random early detection. It is disabled by default.

To configure FortiSwitch to enable ECN packet marking to drop eligible packets:

```
config switch-controller qos queue-policy
   edit "ECN_marking"
      set schedule round-robin
      set rate-by kbps
      config cos-queue
         edit "queue-0"
            set drop-policy weighted-random-early-detection
            set ecn enable
         next
         edit "queue-1"
         next
         edit "queue-2"
         next
         ...
      end
   next
end
```

Logging and monitoring

This section covers the following topics:

FortiSwitch log settings

You can export the logs of managed FortiSwitch units to FortiSwitch Manager or send FortiSwitch logs to a remote Syslog server.

This section covers the following topics:

Exporting logs to FortiSwitch Manager

You can enable and disable whether the managed FortiSwitch units export their logs to FortiSwitch Manager. The setting is global, and the default setting is enabled.

To allow a level of filtering, FortiSwitch Manager sets the user field to “fortiswitch-syslog” for each entry.

Use the following CLI command syntax:

```
config switch-controller switch-log
   set status {*enable | disable}
   set severity {emergency | alert | critical | error | warning | notification |
        *information | debug}
end
```

You can override the global log settings for a FortiSwitch unit, using the following commands:

```
config switch-controller managed-switch
   edit <switch-id>
      config switch-log
         set local-override enable
```

At this point, you can configure the log settings that apply to this specific switch.

Sending logs to a remote Syslog server

Instead of exporting FortiSwitch logs to FortiSwitch Manager, you can send FortiSwitch logs to one or two remote Syslog servers. After enabling this option, you can select the severity of log messages to send, whether to use comma-separated values (CSVs), and the type of remote Syslog facility. By default, FortiSwitch logs are sent to port 514 of the remote Syslog server.

Use the following CLI command syntax to configure the default syslogd and syslogd2 settings:

```
config switch-controller remote-log
   edit {syslogd | syslogd2}
      set status {enable | *disable}
      set server <IPv4_address_of_remote_syslog_server>
      set port <remote_syslog_server_listening_port>
      set severity {emergency | alert | critical | error | warning | notification |
           *information | debug}
      set csv {enable | *disable}
      set facility {kernel | user | mail | daemon | auth | syslog | lpr | news | uucp | cron
           | authpriv | ftp | ntp | audit | alert | clock | local0 | local1 | local2 |
           local3 | local4 | local5 | local6 | *local7}
   next
end
```

You can override the default syslogd and syslogd2 settings for a specific FortiSwitch unit, using the following commands:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config remote-log
         edit {edit syslogd | syslogd2}
            set status {enable | *disable}
            set server <IPv4_address_of_remote_syslog_server>
            set port <remote_syslog_server_listening_port>
            set severity {emergency | alert | critical | error | warning | notification |
                 *information | debug}
            set csv {enable | *disable}
            set facility {kernel | user | mail | daemon | auth | syslog | lpr | news | uucp |
                 cron | authpriv | ftp | ntp | audit | alert | clock | local0 | local1 |
                 local2 | local3 | local4 | local5 | local6 | *local7}
         next
      end
   next
end
```

Configuring FortiSwitch port mirroring

The FortiSwitch unit can send a copy of any ingress or egress packet on a port to egress on another port of the same FortiSwitch unit. The original traffic is unaffected. This process is known as port-based mirroring and is typically used for external analysis and capture.

Using encapsulated RSPAN (ERSPAN) allows you to send the collected packets across layer-2 domains for analysis. You can have only one ERSPAN session.

In ERSPAN mode, traffic is encapsulated in Ethernet, IPv4, and generic routing encapsulation (GRE) headers. By focusing on traffic to and from specified ports and traffic to a specified MAC or IP address, ERSPAN reduces the amount

of traffic being mirrored. The ERSPAN traffic is sent to a specified IP address, which must be reachable by IPv4 ICMP ping. If no IP address is specified, the traffic is not mirrored.

NOTE: ERSPAN is supported on FSR-124D and platforms 2xx and higher. ERSPAN cannot be used with the other FortiSwitch port-mirroring method.

To configure FortiSwitch port-based mirroring:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config mirror
         edit <mirror_name>
            set status {active | inactive} // Required
            set dst <port_name> // Required
            set switching-packet {enable | disable}
            set src-ingress <port_name>
            set src-egress <port_name>
         next
      end
   next
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config mirror
         edit 2
            set status active
            set dst port1
            set switching-packet enable
            set src-ingress port2 port3
            set src-egress port4 port5
         next
      end
   next
end
```

To configure FortiSwitch ERSPAN:

```
config switch-controller traffic-sniffer
   set mode erspan-auto
   set erspan-ip <xxx.xxx.xxx.xxx> // IPv4 address where ERSPAN traffic is sent
   config target-mac
      edit <MM:MM:MM:SS:SS:SS> // mirror traffic sent to this MAC address
         set description <string>
      end
   config target-ip
      edit <xxx.xxx.xxx.xxx> // mirror traffic sent to this IPv4 address
         set description <string>
      end
   config target-port
      edit <FortiSwitch_serial_number>
         set description <string>
         set in-ports <portx porty portz ...> // mirror traffic sent to these ports
         set out-ports <portx porty portz ...> // mirror traffic sent from these ports
      end
   end
```

For example:

```
config switch-controller traffic-sniffer
   set mode erspan-auto
   set erspan-ip 10.254.254.254
   config target-mac
      edit 00:00:00:aa:bb:cc
         set description MACtarget1
      end
   config target-ip
      edit 10.254.254.192
         set description IPtarget1
      end
   config target-port
      edit S524DF4K15000024
         set description PortTargets1
         set in-ports port5 port6 port7
         set out-ports port10
      end
   end
```

To disable FortiSwitch port mirroring:

```
config switch-controller traffic-sniffer
   set mode none
end
```

Configuring SNMP

Simple Network Management Protocol (SNMP) enables you to monitor hardware on your network.

The managed FortiSwitch SNMP implementation is read-only. SNMP v1-compliant and v2c-compliant SNMP managers have read-only access to FortiSwitch system information through queries and can receive trap messages from the managed FortiSwitch unit.

To monitor FortiSwitch system information and receive FortiSwitch traps, you must first compile the Fortinet and FortiSwitch management information base (MIB) files. A MIB is a text file that describes a list of SNMP data objects that are used by the SNMP manager. These MIBs provide information that the SNMP manager needs to interpret the SNMP trap, event, and query messages sent by the FortiSwitch SNMP agent.

FortiSwitch core MIB files are available for download by going to *System* > *Config* > *SNMP* > *Settings* and selecting the *FortiSwitch MIB File* download link.

You configure SNMP on a global level so that all managed FortiSwitch units use the same settings. If you want one of the FortiSwitch units to use different settings from the global settings, configure SNMP locally.

The maximum number of hosts for SNMP traps on a FortiSwitch unit is 8.

This section covers the following topics:

Configuring SNMP globally

To configure SNMP globally:

1. Add SNMP access on the switch-management interface.
2. Configure the SNMP system information.
3. Configure the SNMP community.
4. Configure the SNMP trap threshold values.
5. Configure the SNMP user.

To add SNMP access on the switch-management interface:

```
config switch-controller security-policy local-access
   edit "{default | <policy_name>}"
      set mgmt-allowaccess <options> snmp
      set internal-allowaccess <options>
   next
end
```

To configure the SNMP system information globally:

```
config switch-controller snmp-sysinfo
   set status enable
   set engine-id <local_SNMP_engine_ID (the maximum is 24 characters)>
   set description <system_description>
   set contact-info <contact_information>
   set location <FortiSwitch_location>
end
```

NOTE: Each SNMP engine maintains a value, snmpEngineID, which uniquely identifies the SNMP engine. This value is included in each message sent to or from the SNMP engine. The engine-id is part of the snmpEngineID but does not include the Fortinet prefix 0x8000304404.

To configure the SNMP community globally:

```
config switch-controller snmp-community
   edit <SNMP_community_entry_identifier>
      set name <SNMP_community_name>
      set status enable
      set query-v1-status enable
      set query-v1-port <0-65535; the default is 161>
      set query-v2c-status enable
      set query-v2c-port <0-65535; the default is 161>
      set trap-v1-status enable
      set trap-v1-lport <0-65535; the default is 162>
      set trap-v1-rport <0-65535; the default is 162>
      set trap-v2c-status enable
```

```
      set trap-v2c-lport <0-65535; the default is 162>
      set trap-v2c-rport <0-65535; the default is 162>
      set events {cpu-high mem-low log-full intf-ip ent-conf-change}
      config hosts
         edit <host_entry_ID>
            set ip <IPv4_address_of_the_SNMP_manager>
         end
      next
   end
```

To configure the SNMP trap threshold values globally:

```
config switch-controller snmp-trap-threshold
   set trap-high-cpu-threshold <percentage_value; the default is 80>
   set trap-low-memory-threshold <percentage_value; the default is 80>
   set trap-log-full-threshold <percentage_value; the default is 90>
end
```

To configure the SNMP user globally:

```
config switch-controller snmp-user
   edit <SNMP_user_name>
      set queries enable
      set query-port <0-65535; the default is 161>
      set security-level {auth-priv | auth-no-priv | no-auth-no-priv}
      set auth-proto {md5 | sha1 | sha224 | sha256 | sha384 | sha512}
      set auth-pwd <password_for_authentication_protocol>
      set priv-proto {aes128 | aes192 | aes192c | aes256 | aes256c | des}}
      set priv-pwd <password_for_encryption_protocol>
   end
```

Configuring SNMP locally

To configure SNMP for a specific FortiSwitch unit:

1. Configure the SNMP system information.
2. Configure the SNMP community.
3. Configure the SNMP trap threshold values.
4. Configure the SNMP user.

You can set up one or more SNMP v3 notifications (traps) in the CLI. The following notifications are supported:

- The CPU usage is too high.
- The configuration of an entity was changed.
- The IP address for an interface was changed.
- The available log space is low.
- The available memory is low.

By default, all SNMP notifications are enabled. Notifications are sent to one or more IP addresses.

To configure the SNMP system information locally:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
```

```
      set override-snmp-sysinfo enable
      config snmp-sysinfo
         set status enable
         set engine-id <local_SNMP_engine_ID (the maximum is 24 characters)>
         set description <system_description>
         set contact-info <contact_information>
         set location <FortiSwitch_location>
      end
   next
end
```

NOTE: Each SNMP engine maintains a value, snmpEngineID, which uniquely identifies the SNMP engine. This value is included in each message sent to or from the SNMP engine. The engine-id is part of the snmpEngineID but does not include the Fortinet prefix 0x8000304404.

To configure the SNMP community locally:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set override-snmp-community enable
      config snmp-community
         edit <SNMP_community_entry_identifier>
            set name <SNMP_community_name>
            set status enable
            set query-v1-status enable
            set query-v1-port <0-65535; the default is 161>
            set query-v2c-status enable
            set query-v2c-port <0-65535; the default is 161>
            set trap-v1-status enable
            set trap-v1-lport <0-65535; the default is 162>
            set trap-v1-rport <0-65535; the default is 162>
            set trap-v2c-status enable
            set trap-v2c-lport <0-65535; the default is 162>
            set trap-v2c-rport <0-65535; the default is 162>
            set events {cpu-high mem-low log-full intf-ip ent-conf-change}
            config hosts
               edit <host_entry_ID>
                  set ip <IPv4_address_of_the_SNMP_manager>
               end
            next
         end
```

To configure the SNMP trap threshold values locally:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set override-snmp-trap-threshold enable
      config snmp-trap-threshold
         set trap-high-cpu-threshold <percentage_value; the default is 80>
         set trap-low-memory-threshold <percentage_value; the default is 80>
         set trap-log-full-threshold <percentage_value; the default is 90>
      end
   next
end
```

To configure the SNMP user locally:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set override-snmp-user enable
      config snmp-user
         edit <SNMP_user_name>
            set queries enable
            set query-port <0-65535; the default is 161>
            set security-level {auth-priv | auth-no-priv | no-auth-no-priv}
            set auth-proto {md5 | sha1 | sha224 | sha256 | sha384 | sha512}
            set auth-pwd <password_for_authentication_protocol>
            set priv-proto {aes128 | aes192 | aes192c | aes256 | aes256c | des}
            set priv-pwd <password_for_encryption_protocol>
         end
      next
   end
```

SNMP OIDs

Three SNMP OIDs report the FortiSwitch port status and FortiSwitch CPU and memory statistics.

SNMP OID	Description
fgSwDeviceInfo.fgSwDeviceTable.fgSwDeviceEntry.fgSwDeviceEntry.fgSwCpu 1.3.6.1.4.1.12356.101.24.1.1.1.11	Percentage of the CPU being used.
fgSwDeviceInfo.fgSwDeviceTable.fgSwDeviceEntry.fgSwDeviceEntry.fgSwMemory 1.3.6.1.4.1.12356.101.24.1.1.1.12	Percentage of memory being used.
fgSwPortInfo.fgSwPortTable.fgSwPortEntry.fgSwPortStatus 1.3.6.1.4.1.12356.101.24.2.1.1.6	Whether a managed FortiSwitch port is up or down.

These OIDs require FortiSwitchOS 7.0.0 or higher. FortiLink and SNMP must be configured on FortiSwitch Manager.

FortiSwitch units update the CPU and memory statistics every 30 seconds. This interval cannot be changed.

Sample queries

To find out how much CPU is being used on a FortiSwitch 1024D with the serial number FS1D243Z17000032:

```
root@PC05:~# snmpwalk -v2c -Cc -c REGR-SYS 172.16.200.1
     1.3.6.1.4.1.12356.101.24.1.1.1.11.2.8.17000032
```

To find out how much memory is being used on a FortiSwitch 1024D with the serial number FS1D243Z17000032:

```
root@PC05:~# snmpwalk -v2c -Cc -c REGR-SYS 172.16.200.1
     1.3.6.1.4.1.12356.101.24.1.1.1.12.2.8.17000032
```

To find out the status of port1 of a FortiSwitch 1024D with the serial number FS1D243Z17000032:

```
root@PC05:~# snmpwalk -v2c -Cc -c REGR-SYS 172.16.200.1
     1.3.6.1.4.1.12356.101.24.2.1.1.6.2.8.17000032.1
```

Configuring sFlow

sFlow is a method of monitoring the traffic on your network to identify areas on the network that might impact performance and throughput. With sFlow, you can export truncated packets and interface counters. FortiSwitch implements sFlow version 5 and supports trunks and VLANs.

NOTE: Because sFlow is CPU intensive, Fortinet does not recommend high rates of sampling for long periods.

sFlow uses packet sampling to monitor network traffic. The sFlow agent captures packet information at defined intervals and sends them to an sFlow collector for analysis, providing real-time data analysis. To minimize the impact on network throughput, the information sent is only a sampling of the data.

The sFlow collector is a central server running software that analyzes and reports on network traffic. The sampled packets and counter information, referred to as flow samples and counter samples, respectively, are sent as sFlow datagrams to a collector. Upon receiving the datagrams, the sFlow collector provides real-time analysis and graphing to indicate the source of potential traffic issues. sFlow collector software is available from a number of third-party software vendors. You must configure a FortiSwitch Manager policy to transmit the samples from the FortiSwitch unit to the sFlow collector.

sFlow can monitor network traffic in two ways:

- Flow samples—You specify the percentage of packets (one out of *n* packets) to randomly sample.
- Counter samples—You specify how often (in seconds) the network device sends interface counters.

Use the following CLI commands to specify the IP address and port for the sFlow collector. By default, the IP address is 0.0.0.0, and the port number is 6343.

```
config switch-controller sflow
   collector-ip <x.x.x.x>
   collector-port <port_number>
end
```

Use the following CLI commands to configure sFlow:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set sflow-sampler {disabled | enabled}
            set sflow-sample-rate <0-99999>
            set sflow-counter-interval <1-255>
         next
      next
   end
```

For example:

```
config switch-controller sflow
   collector-ip 1.2.3.4
   collector-port 10
end
```

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port5
            set sflow-sampler enabled
            set sflow-sample-rate 10
            set sflow-counter-interval 60
         next
      next
   end
```

Configuring flow tracking and export

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.

When a new FortiSwitch unit or trunk port is added, the flow-tracking configuration is updated automatically based on the specified sampling mode. When a FortiSwitch port becomes part of an ISL or ICL or is removed, the flow-tracking configuration is updated automatically based on the specified sampling mode.

The maximum number of concurrent flows is defined by the FortiSwitch model. When this limit is exceeded, the oldest flow expires and is exported.

You can 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.

Using multiple flow-export collectors requires FortiSwitchOS 7.0.0 or later. If you are using an earlier version of FortiSwitchOS, only the first flow-export collector is supported.

You can specify how often a template packet is sent using the `set template-export-period` command. By default, a template packet is sent every 5 minutes. The range of values is 1-60 minutes.

To configure flow tracking on managed FortiSwitch units:

```
config switch-controller flow-tracking
   set sample-mode {local | perimeter | device-ingress}
   set sample-rate <0-99999>
   set format {netflow1 | netflow5 | netflow9 | ipfix}
   set level {vlan | ip | port | proto}
   set max-export-pkt-size <512-9216 bytes; default is 512>
   set template-export-period <1-60 minutes, default is 5>
   set timeout-general <60-604800 seconds; default is 3600>
   set timeout-icmp <60-604800 seconds; default is 300>
   set timeout-max <60-604800 seconds; default is 604800>
   set timeout-tcp <60-604800 seconds; default is 3600>
   set timeout-tcp-fin <60-604800 seconds; default is 300>
   set timeout-tcp-rst <60-604800 seconds; default is 120>
   set timeout-udp <60-604800 seconds; default is 300>
   config collectors
```

```
      edit <collector_name>
      set ip <IPv4_address>
      set port <0-65535>
      set transport {udp | tcp | sctp}
      end
   config aggregates
      edit <aggregate_ID>
         set <IPv4_address>
      end
end
```

For example:

```
config switch-controller flow-tracking
   config collectors
      edit "Analyzer_1"
         set ip 172.16.201.55
         set port 4739
         set transport sctp
      next
      edit "Collector_HQ"
         set ip 172.16.116.82
         set port 2055
      next
   end
   set template-export-period 10
end
```

Configure the sampling mode

You can set the sampling mode to local, perimeter, or device-ingress.

- The local mode samples packets on a specific FortiSwitch port.
- The perimeter mode samples packets on all FortiSwitch ports that receive data traffic, except for ISL and ICL ports. For perimeter mode, you can also configure the sampling rate.
- The device-ingress mode samples packets on all FortiSwitch ports that receive data traffic for hop-by-hop tracking. For device-ingress mode, you can also configure the sampling rate.

Configure the sampling rate

For perimeter or device-ingress sampling, you can set the sampling rate, which samples 1 out of the specified number of packets. The default sampling rate is 1 out of 512 packets.

Configure the flow-tracking protocol

You can set the format of exported flow data as NetFlow version 1, NetFlow version 5, NetFlow version 9, or IPFIX sampling.

Configure collector IP address

The default is `0.0.0.0`. Setting the value to “0.0.0.0” or “” disables this feature. The format is xxx.xxx.xxx.xxx.

Configure the transport protocol

You can set exported packets to use UDP, TCP, or SCTP for transport.

Configure the flow-tracking level

You can set the flow-tracking level to one of the following:

- `vlan`—The FortiSwitch unit collects source IP address, destination IP address, source port, destination port, protocol, Type of Service, and VLAN from the sample packet.

- ip—The FortiSwitch unit collects source IP address and destination IP address from the sample packet.
- port—The FortiSwitch unit collects source IP address, destination IP address, source port, destination port, and protocol from the sample packet.
- proto—The FortiSwitch unit collects source IP address, destination IP address, and protocol from the sample packet.

Configure the maximum exported packet size

You can set the maximum size of exported packets in the application level.

To remove flow reports from a managed FortiSwitch unit:

```
execute switch-controller switch-action flow-tracking {delete-flows-all | expire-flows-all}
     <FortiSwitch_serial_number>
```

Expired flows are exported.

To view flow statistics for a managed FortiSwitch unit:

```
diagnose switch-controller switch-info flow-tracking statistics <FortiSwitch_serial_number>
```

To view raw flow records for a managed FortiSwitch unit:

```
diagnose switch-controller switch-info flow-tracking flows-raw <FortiSwitch_serial_number>
```

To view flow record data for a managed FortiSwitch unit:

```
diagnose switch-controller switch-info flow-tracking flows {number_of_records | all} {IP_
     address | all} <FortiSwitch_serial_number> <FortiSwitch_port_name>
```

For example:

```
diagnose switch-controller switch-info flow-tracking flows 100 all S524DF4K15000024 port6
```

Configuring flow control and ingress pause metering

Flow control allows you to configure a port to send or receive a “pause frame” (that is, a special packet that signals a source to stop sending flows for a specific time interval because the buffer is full). By default, flow control is disabled on all ports.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set flow-control {both | rx | tx | disable}
         next
      end
   end
```

Parameters enable flow control to do the following:

- rx—receive pause control frames
- tx—transmit pause control frames
- both—transmit and receive pause control frames

If you enable flow control to transmit pause control frames or to transmit and receive pause control frames, you can also use ingress pause metering to limit the input bandwidth of an ingress port. Because ingress pause metering stops the traffic temporarily instead of dropping it, ingress pause metering can provide better performance than policing when the port is connected to a server or end station. To use ingress pause metering, you need to set the ingress metering rate in kilobits and set the percentage of the threshold for resuming traffic on the ingress port.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set flow-control {tx | both}
            set pause-meter <128-2147483647; set to 0 to disable>
            set pause-meter-resume {25% | 50% | 75%}
         next
      end
   end
```

For example:

```
config switch-controller managed-switch
   edit S424ENTF19000007
      config ports
         edit port29
            set flow-control tx
            set pause-meter 900
            set pause-meter-resume 50%
         next
      end
   end
```

Operation and maintenance

This section covers the following topics:

Defining names for managed switches

Starting in FortiSwitch Manager 7.2.5, you can use names for managed FortiSwitch units in switch-controller CLI commands. The user-defined name is also used in the FortiSwitch Manager GUI and logs. The FortiSwitch unit's serial number is saved in a new read-only field.

Follow these rules for defining a managed FortiSwitch name:

- The name can be a maximum of 16 characters in length.
- Use numbers (0-9), letters (a-z and A-Z), dashes, and underscores for the managed FortiSwitch name.

When you upgrade from FortiSwitch Manager 7.2.5, the FortiSwitch unit's serial number is used as the managed FortiSwitch name if a managed FortiSwitch name has not been defined. If you downgrade from FortiSwitch Manager 7.2.5, the managed FortiSwitch name is changed to the FortiSwitch unit's serial number.

Using the GUI

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Select an unauthorized FortiSwitch unit and then click *Edit*.
3. In the *Name* field, enter a name for the managed FortiSwitch unit.
4. Click *OK* to save the new name.

Using the CLI

```
config switch-controller managed-switch
   rename <FortiSwitch_serial_number> to <managed_FortiSwitch_name>
end
```

For example:

```
config switch-controller managed-switch
   rename S524DN4K16000116 to Distribution
end
```

Other CLI changes in FortiSwitch Manager 7.2.5

- When you pre-configure a managed switch, you must use the `set sn` command (as well as the `set fsw-wan1-peer` command) under `config switch-controller managed-switch` to store the FortiSwitch serial number. For example:

  ```
  config switch-controller managed-switch
     edit switch1
        set sn S524DNTV21000212
        set fsw-wan1-peer fortilink
        set fsw-wan1-admin enable
     next
  end
  ```

- The `execute switch-controller get-sync-status switch-id <managed_FortiSwitch_name>` command uses the user-defined switch name, and the `execute switch-controller get-sync-status serial <FortiSwitch_serial_number>` command uses the FortiSwitch serial number. For example:
  - `execute switch-controller get-sync-status serial S524DN4K16000116`
  - `execute switch-controller get-sync-status switch-id Racktray-127`
- There is a new `set isl-peer-device-sn` command under `config switch-controller managed-switch` to store the serial number of the ISL peer device. For example:

  ```
  config switch-controller managed-switch
     edit Distribution
        config ports
           edit port2
              set isl-local-trunk-name isltrunk1
              set isl-peer-port-name port23
              set isl-peer-device-name islpeerswitch
              set isl-peer-device-sn S124EN5918003682
           next
        end
     next
  end
  ```

- Some of the `switch-controller` commands now use the user-defined FortiSwitch name, for example:
  - `diagnose switch-controller trigger config-sync <managed_FortiSwitch_name>`
  - `execute switch-controller get-conn-status`
  - `execute switch-controller get-physical-conn standard <port_name>`
  - `execute switch-controller get-sync-status all`
  - `execute switch-controller get-upgrade-status`
- The following `execute switch-controller` templating commands now use the user-defined FortiSwitch name:

- `execute switch-controller templating apply-config`
- `execute switch-controller templating copy-dynamic-capability`
- `execute switch-controller templating reapply-config`
- `execute switch-controller templating switch-group-apply-members`
- `execute switch-controller templating switch-group-apply-template`

Discovering, authorizing, and deauthorizing FortiSwitch units

This section covers the following topics:

Editing a managed FortiSwitch unit

To edit a managed FortiSwitch unit:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Click on the FortiSwitch unit and then click *Edit* or right-click on a FortiSwitch unit and select *Edit*.

From the *Edit Managed FortiSwitch* form, you can:

- Change the *Name* and *Description* of the FortiSwitch unit.
- View the *Status* of the FortiSwitch unit.
- *Restart* the FortiSwitch unit.
- *Authorize* or deauthorize the FortiSwitch unit.
- *Upgrade* the firmware running on the switch.
- Override 802.1x settings, including the reauthentication interval, maximum reauthentication attempts, and link-down action.

Adding preauthorized FortiSwitch units

After you preauthorize a FortiSwitch unit, you can assign the FortiSwitch ports to a VLAN.

To preauthorize a FortiSwitch:

1. Go to *Switch Controller* > *Managed FortiSwitch*.
2. Click *Create New* > *FortiSwitch*.
3. In the *New Managed FortiSwitch* page, enter the serial number, model name, and description of the FortiSwitch.
4. Click *Authorize*.
5. Click *OK*. The *Managed FortiSwitches* page lists the preauthorized switch.

Using wildcard serial numbers to pre-authorize FortiSwitch units

You can 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 FortiSwitch Manager, 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.

When you create the FortiSwitch template, use the following format for the wildcard serial number:

```
PREFIX****nnnnnn
```

PREFIX	The first six digits of a valid FortiSwitch serial number, such as S248EP, S124EN, S548DF, and S524DF.
****	Asterisks are the only wildcard characters allowed. You can have any number of asterisks, as long as ****nnnnnn is no longer than 10 characters.
nnnnnn	You can have any number of valid alphanumeric characters, as long as ****nnnnnn is no longer than 10 characters.

To pre-authorize FortiSwitch units using a FortiSwitch template:

1. Create a FortiSwitch template.

```
config switch-controller managed-switch
   edit <PREFIX****nnnnnn>
      ...
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S248EP****000000"
      set name "fortilink-FSW248EP1"
      set fsw-wan1-peer "fortilink"
      .......
      config ports
         edit "port1"
            set vlan "onboarding"
            set allowed-vlans "quarantine" "nac_segment"
            set untagged-vlans "quarantine" "nac_segment"
            set access-mode nac
            set export-to "root"
         next
         edit "port2"
            set vlan "_default"
            set allowed-vlans "quarantine"
            set untagged-vlans "quarantine"
            set access-mode dynamic
            set port-policy "aggr1"
            set export-to "root"
         next
      end
   next
end
```

2. Turn on the FortiSwitch unit so that FortiSwitch Manager will discover it.

The FortiSwitch unit is matched with the FortiSwitch template using the order of entries in the CMDB table from top to bottom. The settings in the FortiSwitch template are applied to the discovered FortiSwitch unit. Once a match is made for a wildcard entry, that particular entry is consumed.

Authorizing the FortiSwitch unit

If you configured the FortiLink interface to manually authorize the FortiSwitch unit as a managed switch, perform the following steps:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Right-click on the FortiSwitch name and select *Authorization* > *Authorize*. This step is required only if you disabled the automatic authorization field of the interface.

Deauthorizing FortiSwitch units

A device can be deauthorized to remove it from the Security Fabric.

To deauthorize a device:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Right-click on the FortiSwitch name and select *Authorization* > *Deauthorize*.

After devices are deauthorized, the devices' serial numbers are saved in a trusted list that can be viewed in the CLI using the `show system csf` command. For example, this result shows a deauthorized FortiSwitch:

```
show system csf
   config system csf
      set status enable
      set group-name "Office-Security-Fabric"
      set group-password ENC 1Z2X345V678
      config trusted-list
         edit "FSWMVMTM21000008"
         next
         edit "S248DF3X17000482"
            set action deny
         next
      end
   end
end
```

Converting to FortiSwitch standalone mode

Use one of the following commands to convert a FortiSwitch unit from managed mode to standalone mode so that it will no longer be managed by FortiSwitch Manager:

- `execute switch-controller factory-reset <FortiSwitch_serial_number>`—This command returns the FortiSwitch unit to the factory defaults and then reboots the FortiSwitch unit. By default, the FortiSwitch unit will connect to the available manager, which can be FortiSwitch Manager, a FortiGate device, or FortiLAN Cloud. For example:`execute switch-controller factory-reset S1234567890`
- `execute switch-controller switch-action set-standalone <FortiSwitch_serial_number>`—This command returns the FortiSwitch unit to the factory defaults, reboots the FortiSwitch, and prevents FortiSwitch

Manager from automatically detecting and authorizing the FortiSwitch. For example:`execute switch-controller set-standalone S1234567890`

You can disable FortiLink auto-discovery on multiple FortiSwitch units using the following commands:

```
config switch-controller global
   set disable-discovery <FortiSwitch_serial_number>
end
```

For example:

```
config switch-controller global
   set disable-discovery S1234567890
end
```

You can also add or remove entries from the list of FortiSwitch units that have FortiLink auto-discovery disabled using the following commands:

```
config switch-controller global
   append disable-discovery <FortiSwitch_serial_number>
   unselect disable-discovery <FortiSwitch_serial_number>
end
```

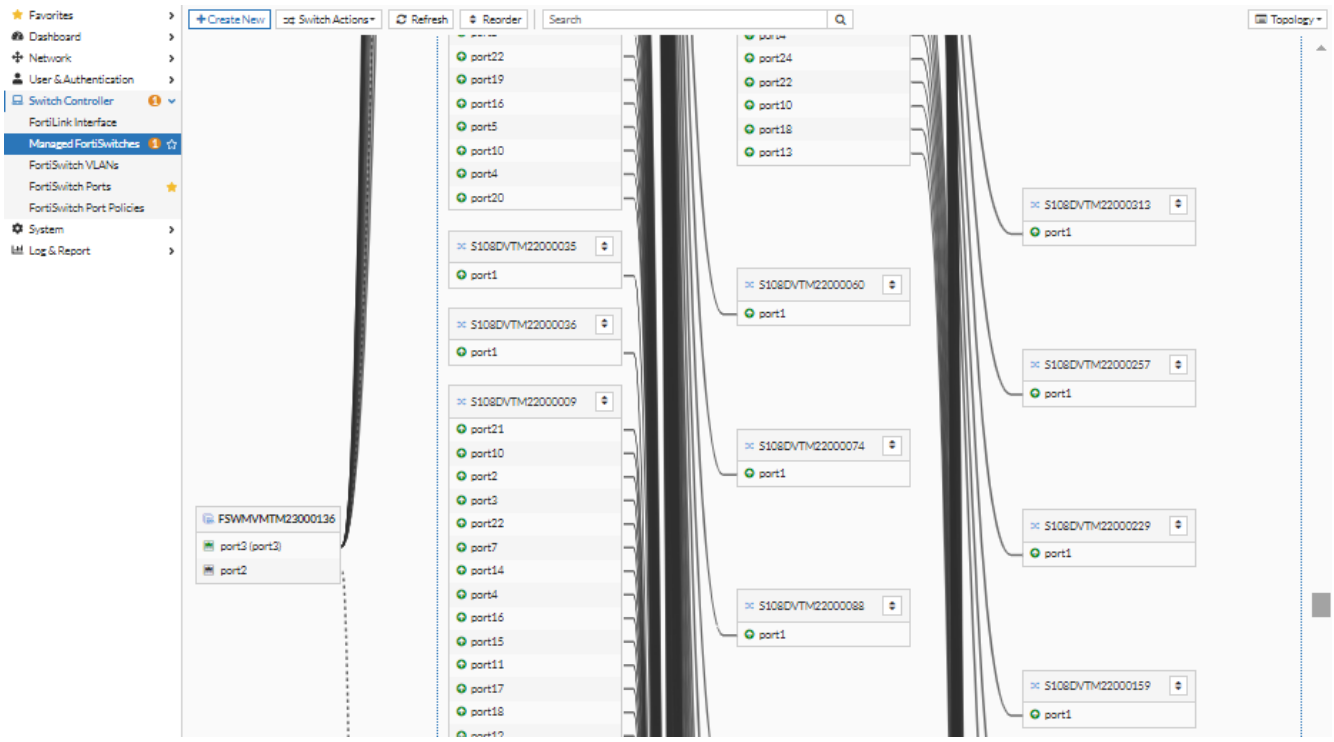
For example:

```
config switch-controller global
   append disable-discovery S012345678
   unselect disable-discovery S1234567890
end
```

Managed FortiSwitch display

The Topology view is recommended for deployments with up to 300 FortiSwitch units.

Go to *Switch Controller* > *Managed FortiSwitches* to see all of the switches being managed by FortiSwitch Manager. Select *Topology* from the drop-down menu in the upper right corner to see which devices are connected.



If the link has gone down for some reason, the line will be dashed. You can still edit the FortiSwitch unit though and find more information about the status of the switch. The link to the FortiSwitch unit might be down for a number of reasons; for example, a problem with the cable linking the two devices, firmware versions being out of synch, and so on. You need to make sure the firmware running on the FortiSwitch unit is compatible with the firmware running on FortiSwitch Manager.

From the *Managed FortiSwitches* page, you can edit any of the managed FortiSwitch units, remove a FortiSwitch unit from the configuration, refresh the display, connect to the CLI of a FortiSwitch unit, or deauthorize a FortiSwitch unit.

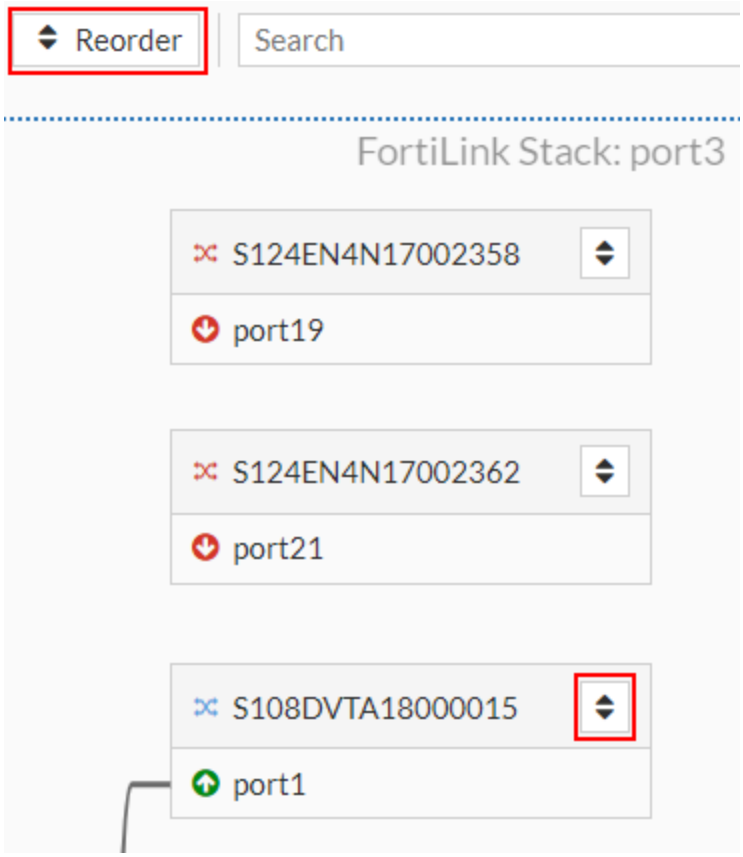
Re-ordering FortiSwitch units in the Topology view

You can change the order in which FortiSwitch units are displayed in the Topology view.

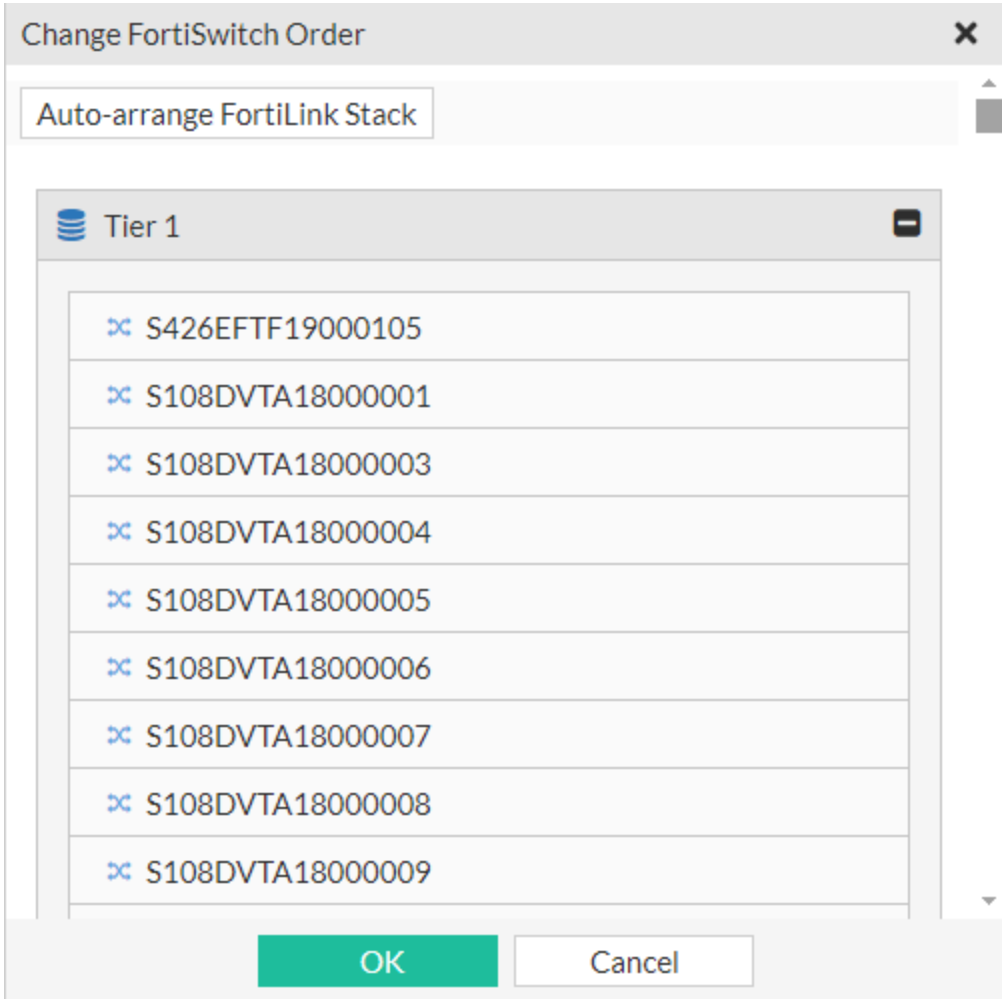
To rearrange the FortiSwitch units in the GUI:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. In the *View* dropdown list, select *Topology*.

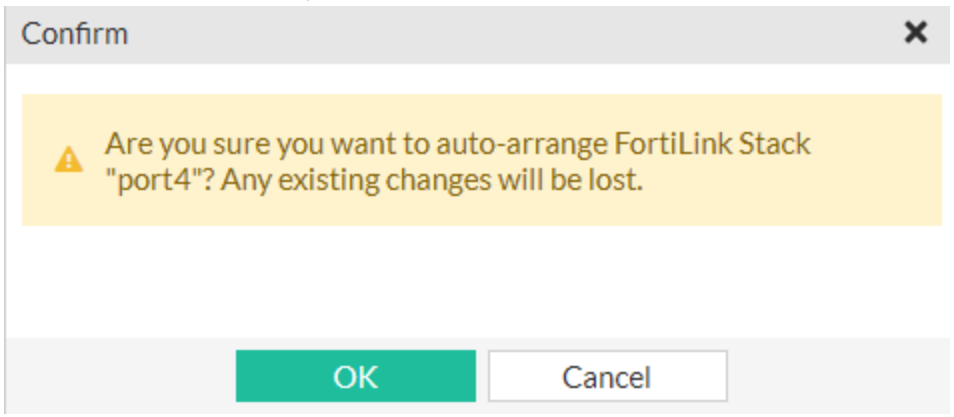
3. Click *Reorder* or the double-arrow button next to the FortiSwitch serial number.



4. In the *Change FortiSwitch Order* window, drag-and-drop each FortiSwitch unit to change the order.

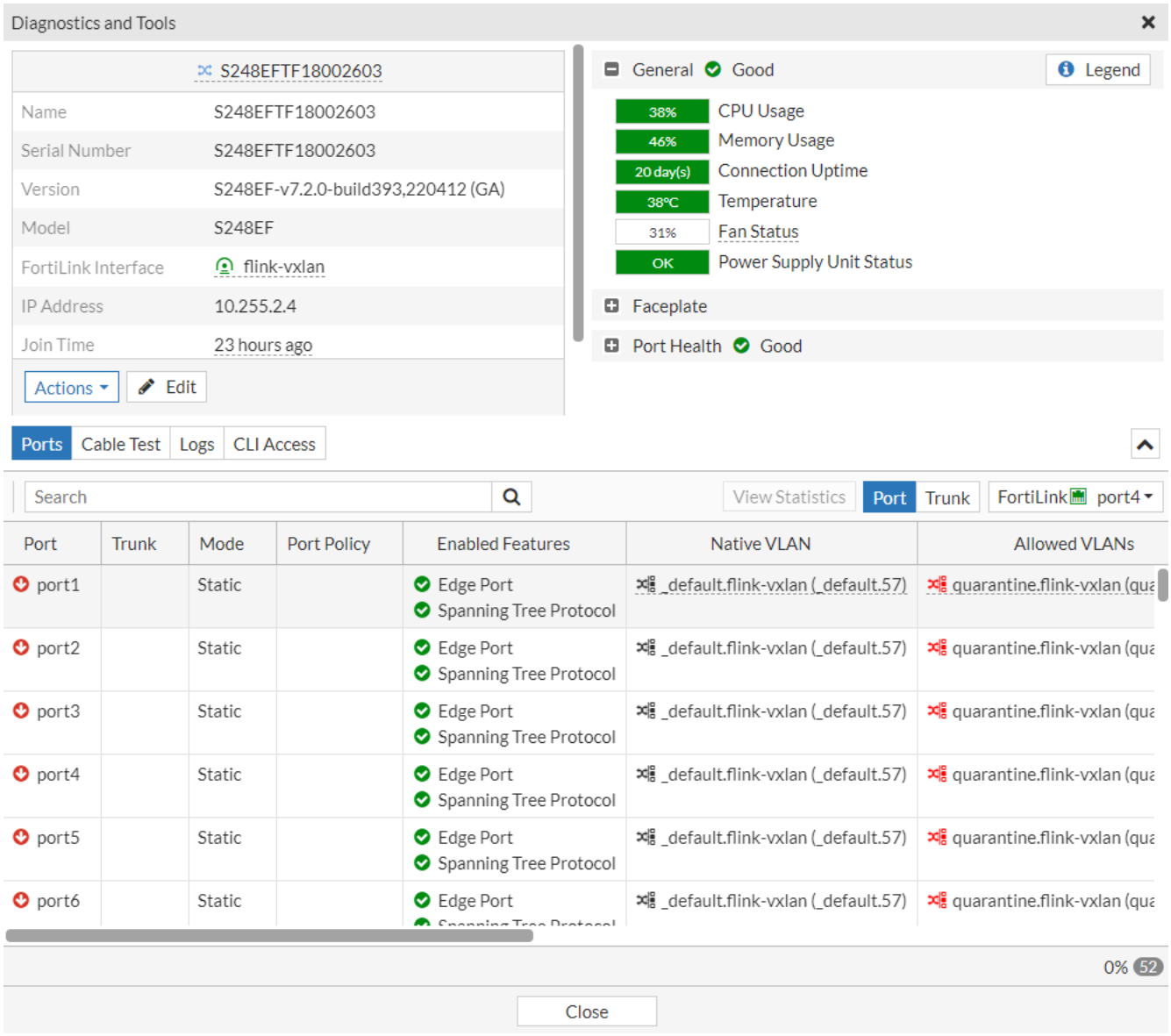


5. If you want FortiSwitch Manager to determine the arrangement with the fewest edge crossings, click *Auto-arrange FortiLink Stack* in the *Change FortiSwitch Order* window and then click *OK* in the *Confirm* window.



Diagnostics and tools

The *Diagnostics and Tools* pane reports the general health of the FortiSwitch unit, displays details about the FortiSwitch unit, and allows you to run diagnostic tests.



To view the Diagnostics and Tools pane:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Right-click the FortiSwitch unit and then select *Diagnostics and Tools*.

From the *Diagnostics and Tools* pane, you can do the following:

- *Authorize* or deauthorize the FortiSwitch.
- *Upgrade* the firmware running on the switch.
- *Restart* the FortiSwitch unit.

- *Connect to CLI* to run CLI commands.
- *Show in List* to return to the *Switch Controller* > *Managed FortiSwitches* page.
- Go to the *Edit Managed FortiSwitch* form.
- Start or stop the *LED Blink* to identify a specific FortiSwitch unit. See Making the LEDs blink on page 148.
- Display a list of FortiSwitch ports and trunks and configuration details.
- Run a *Cable Test* on a selected port. See Running the cable test on page 148.
- View the *Logs* for the FortiSwitch unit.
- Click the *Legend* button in the *General* pane to display 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.

Making the LEDs blink

When you have multiple FortiSwitch units and need to locate a specific switch, you can flash all port LEDs on and off for a specified number of minutes.

To identify a specific FortiSwitch unit:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Right-click the FortiSwitch unit and then select *Diagnostics and Tools*.
3. Select *LED Blink* > *Start* and then select *5 minutes*, *15 minutes*, *30 minutes*, or *60 minutes*.
4. After you locate the FortiSwitch unit, select *LED Blink* > *Stop*.

NOTE: For the 5xx switches, LED Blink flashes only the SFP port LEDs, instead of all the port LEDs.

Running the cable test

NOTE: Running cable diagnostics on a port that has the link up interrupts the traffic for several seconds.

You can check the state of cables connected to a specific port. The following pair states are supported:

- Open
- Short
- Ok
- Open_Short
- Unknown
- Crosstalk

If no cable is connected to the specific port, the state is Open, and the cable length is 0 meters.

Using the GUI:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Right-click the FortiSwitch unit and then select *Diagnostics and Tools*.
3. Select *Cable Test*.
4. Select a port.
5. Select *Diagnose*.

NOTE: There are some limitations for cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models:

- Crosstalk cannot be detected.
- There is a 5-second delay before results are displayed.
- The value for the cable length is inaccurate.
- The results are inaccurate for open and short cables.

FortiSwitch ports display

The *Switch Controller* > *FortiSwitch Ports* page displays port information about each of the managed switches.

Starting in FortiSwitch Manager 7.2.2, the *Device Information* column on the *Switch Controller* > *FortiSwitch Ports* page displays the MAC address connected to that port after you specify in the CLI how often FortiSwitch Manager collects device information from FortiSwitch units.

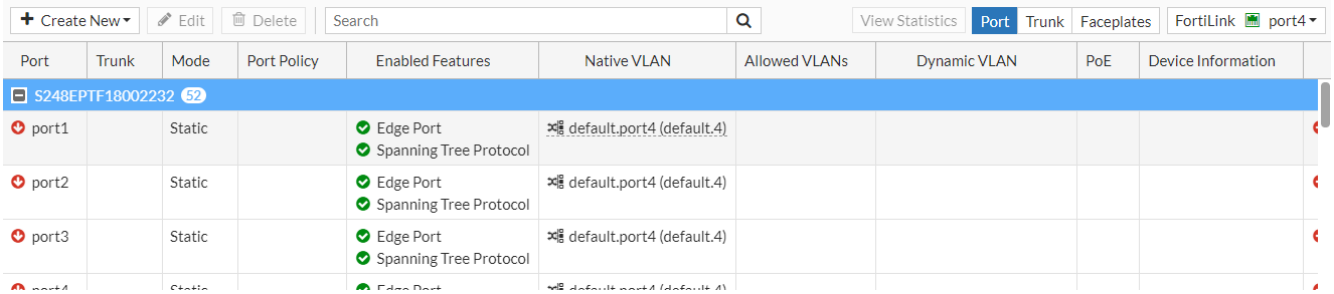
To enable device information collection:

```
config switch-controller system
   set data-sync-interval <30-1800 seconds>
end
```

By default, the `data-sync-interval` is set to 0, and no device information is collected from FortiSwitch units.

Collecting data from the FortiSwitch units is a resource-intensive process. Setting the `data-sync-interval` to a lower value increases the resource requirements, will slow down some management operations, and can lead to instability in large deployments when the value is too low.

Fortinet recommends getting your network running and stabilized before enabling device information collection.



Click *Faceplates* to get the following information:

- Active ports (green)
- FortiLink port (link icon)

Each entry in the port list displays the following information:

- Port status (red for down, green for up)
- Port name
- If the port is a member of a trunk

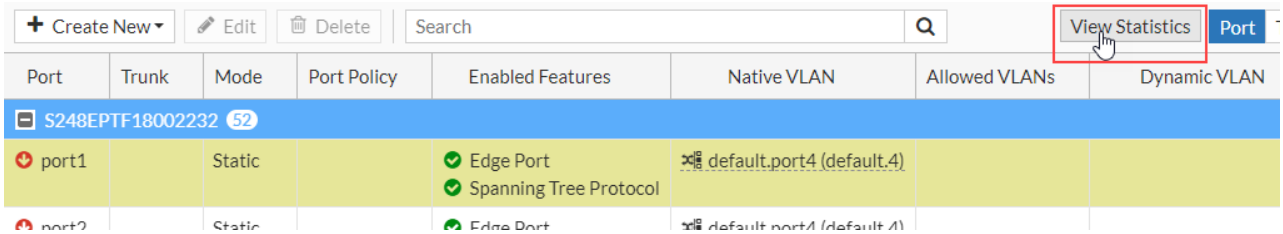
- Access mode
- Port policy
- Enabled features
- Native VLAN
- Allowed VLANs
- Dynamic VLANs
- PoE status
- Device information
- DHCP snooping status
- Transceiver information

Displaying, resetting, and restoring port statistics

For the following commands, if the managed FortiSwitch unit is not specified, the command is applied to all ports of all managed FortiSwitch units.

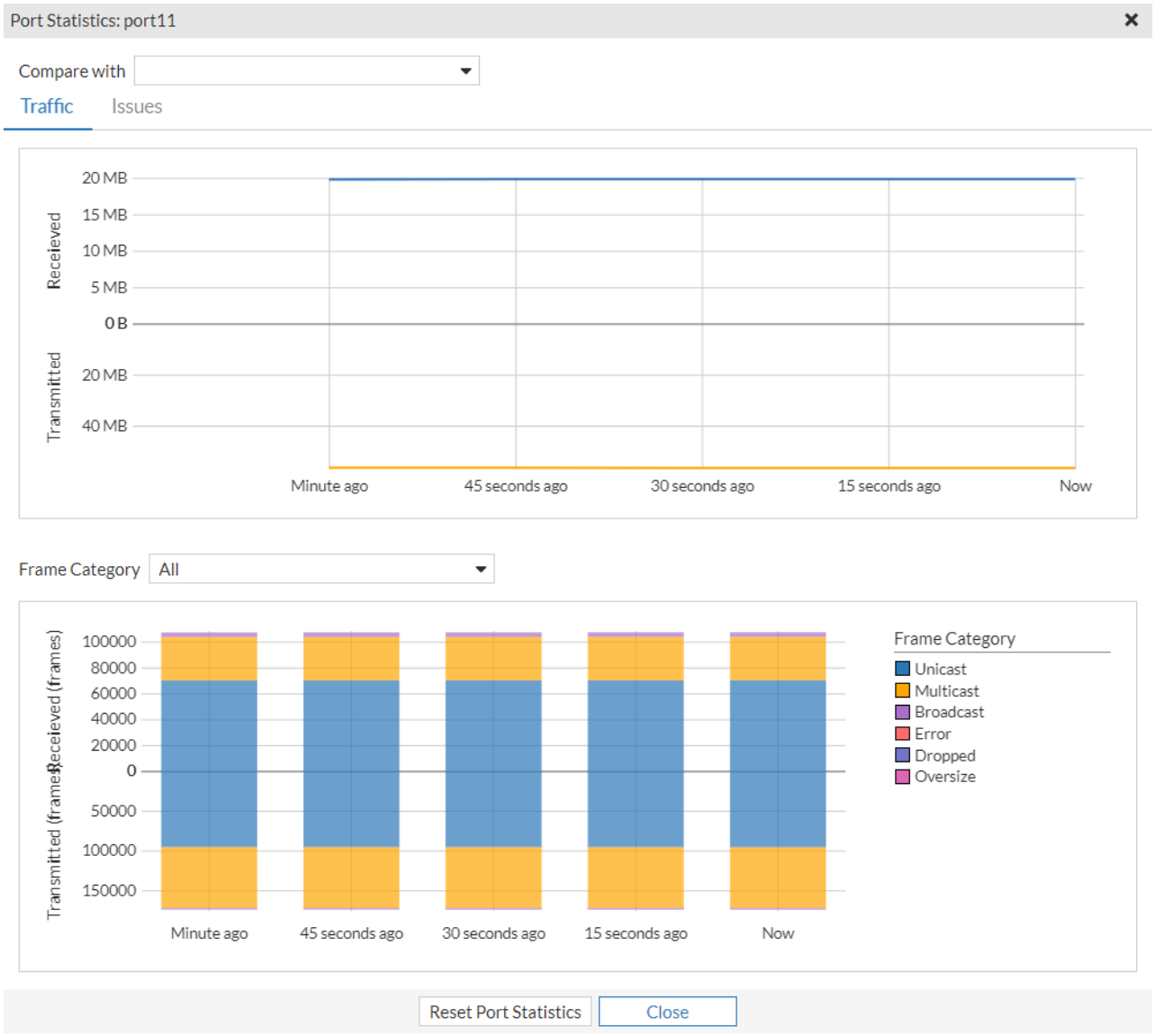
To display port statistics using the GUI:

1. Go to *Switch Controller* > *FortiSwitch Ports*.
2. Select a port.
3. Click *View Statistics*.



4. Click the *Traffic* tab to see transmitted and received traffic and transmitted and received frames. Click the *Issues* tab

to see frame errors by type.



To display port statistics using the CLI:

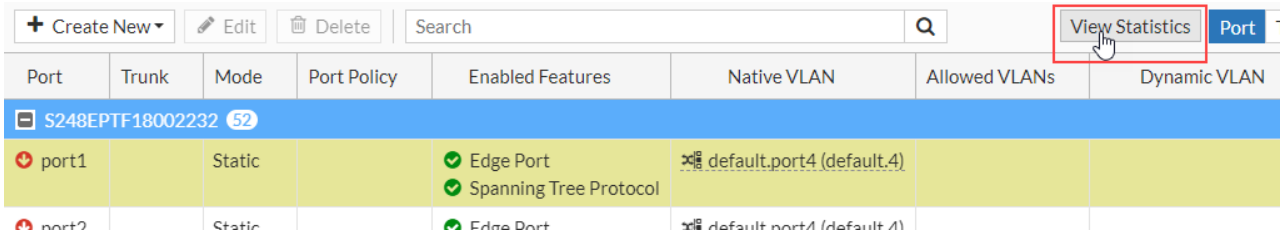
```
diagnose switch-controller switch-info port-stats <managed FortiSwitch device ID> <port_
    name>
```

For example:

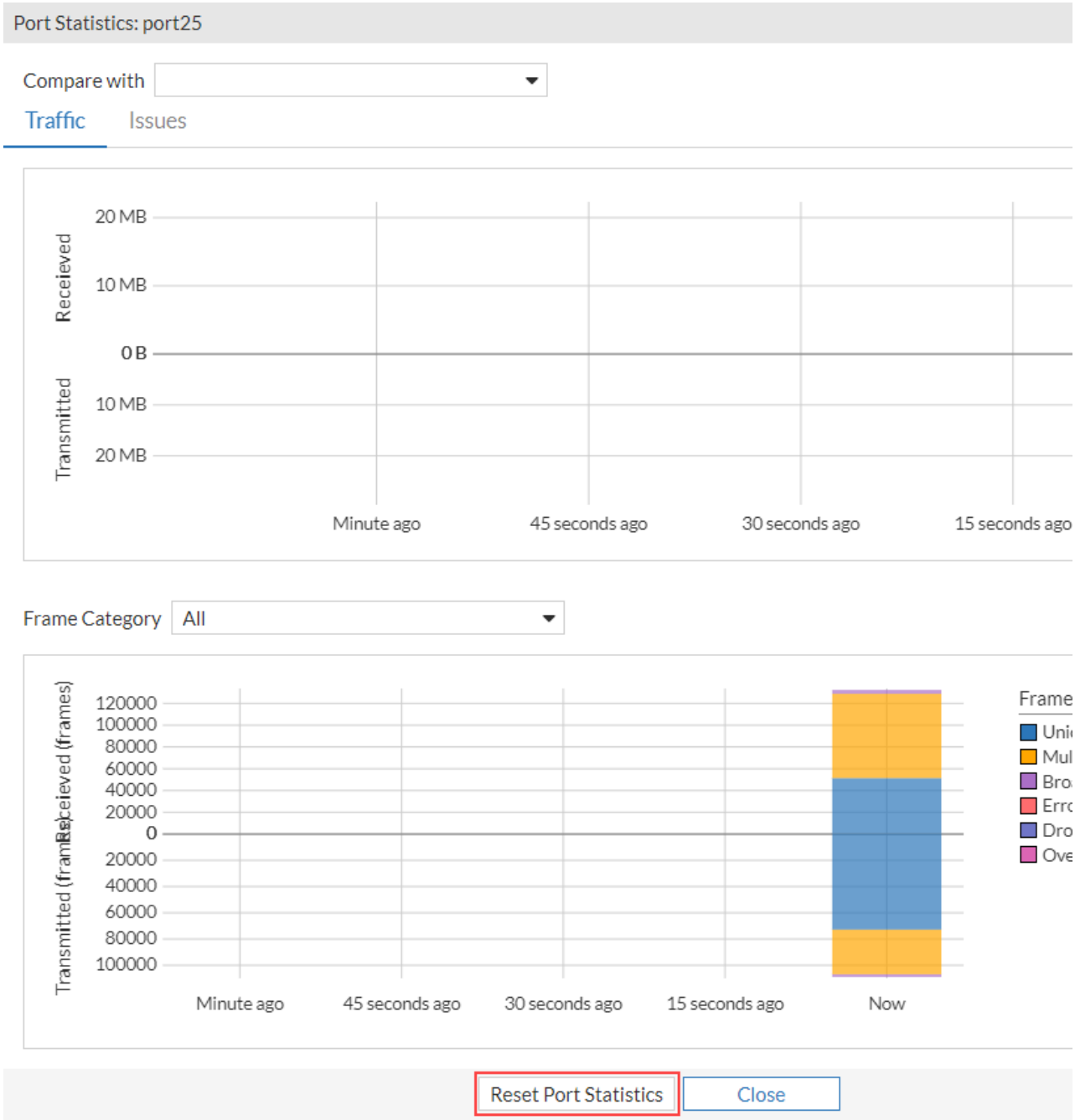
```
diagnose switch-controller switch-info port-stats S524DF4K15000024 port8
```

To reset the port statistics counters using the GUI:

1. Go to *Switch Controller* > *FortiSwitch Ports*.
2. Select a port.
3. Click *View Statistics*.



4. Click *Reset Port Statistics*.



To reset the port statistics counters using the CLI:

```
diagnose switch-controller trigger reset-hardware-counters <managed FortiSwitch device ID>
     <port_name>
```

For example:

```
diagnose switch-controller trigger reset-hardware-counters S524DF4K15000024 1,3,port6-7
```

NOTE: This command is provided for debugging; accuracy is not guaranteed when the counters are reset. Resetting the counters might have a negative effect on monitoring tools, such as SNMP and FortiSwitch Manager. The statistics gathered during the time when the counters are reset might be discarded.

To restore the port statistics counters of a managed FortiSwitch unit:

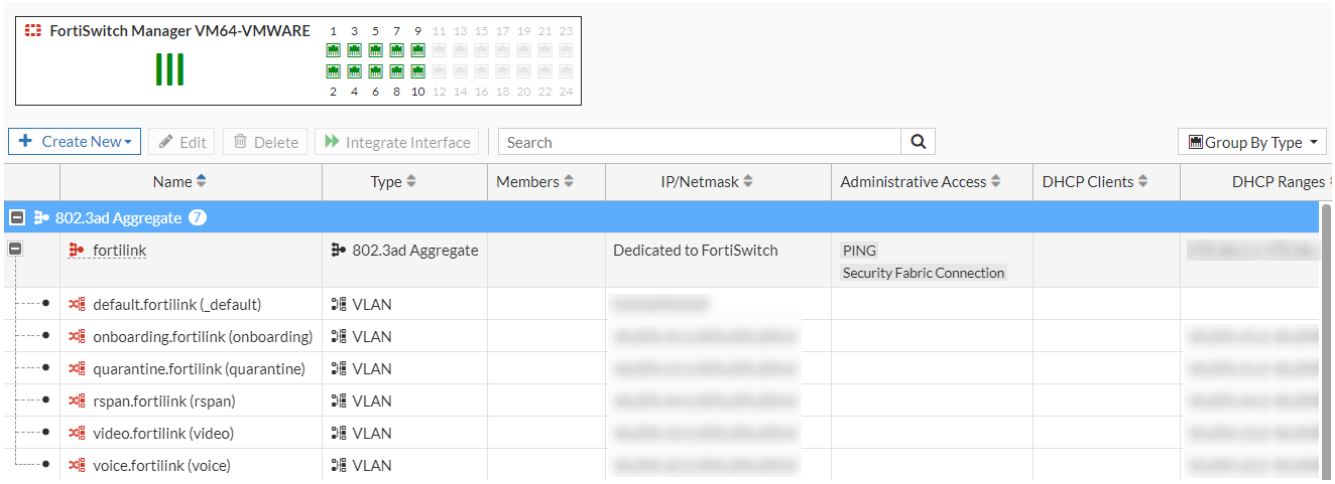
```
diagnose switch-controller trigger restore-hardware-counters <managed FortiSwitch device ID>
     <port_name>
```

For example:

```
diagnose switch-controller trigger restore-hardware-counters S524DF4K15000024 port10-
     port11,internal
```

Network interface display

On the *Network* > *Interfaces* page, you can see the FortiSwitch Manager interface connected to the FortiSwitch unit. The GUI indicates *Dedicated to FortiSwitch* in the IP/Netmask field.



Synchronizing FortiSwitch Manager with the managed FortiSwitch units

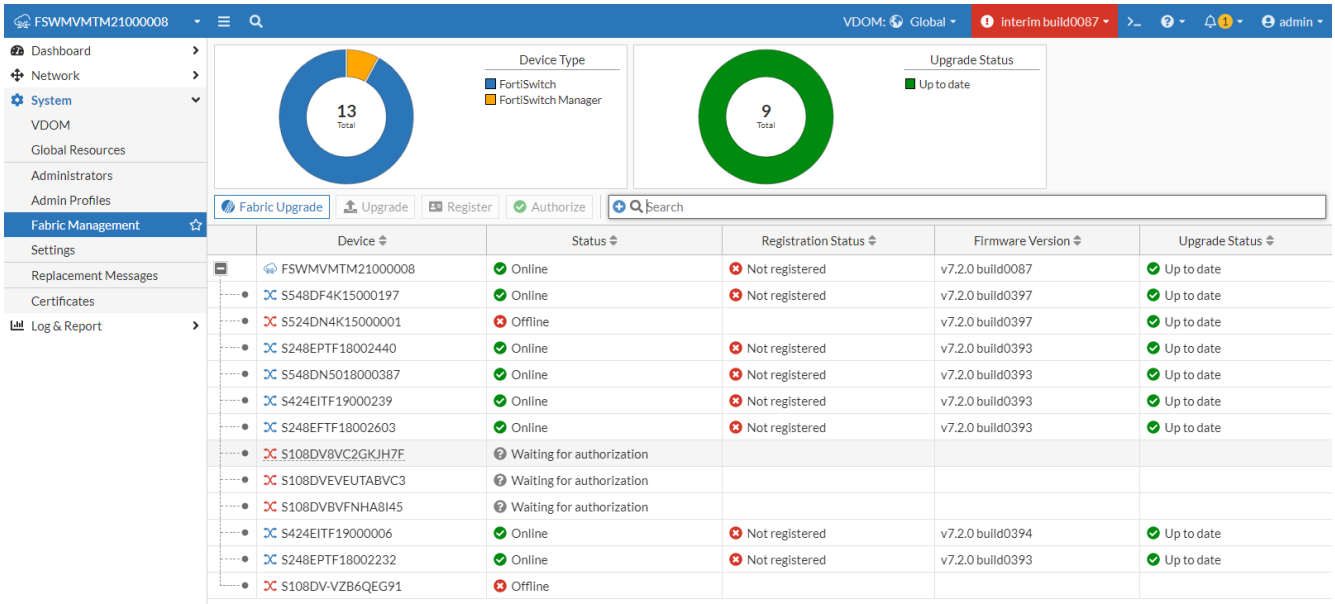
You can synchronize FortiSwitch Manager with the managed FortiSwitch units to check for synchronization errors on each managed FortiSwitch unit.

Use the following command to synchronize the full configuration of FortiSwitch Manager with a managed FortiSwitch unit:

```
diagnose switch-controller trigger config-sync <FortiSwitch_serial_number>
```

Fabric management

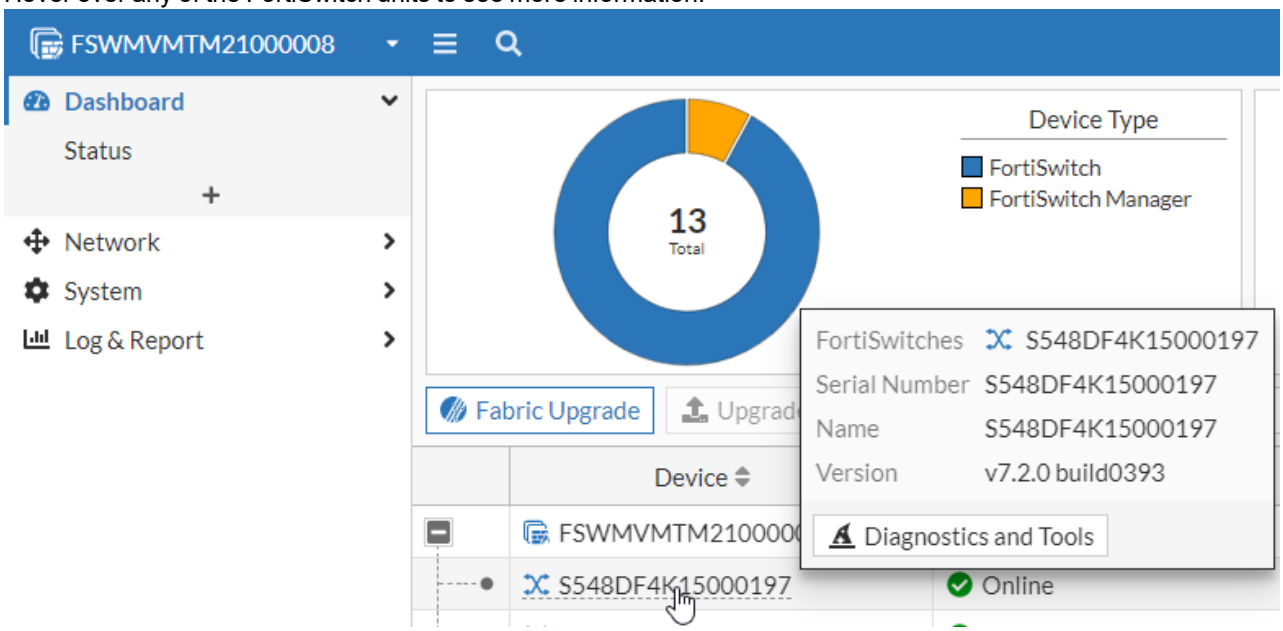
Using fabric management, you can see the whole picture of your network security. The pie charts show what type of devices are in the fabric and whether any of the online switches need to be upgraded.



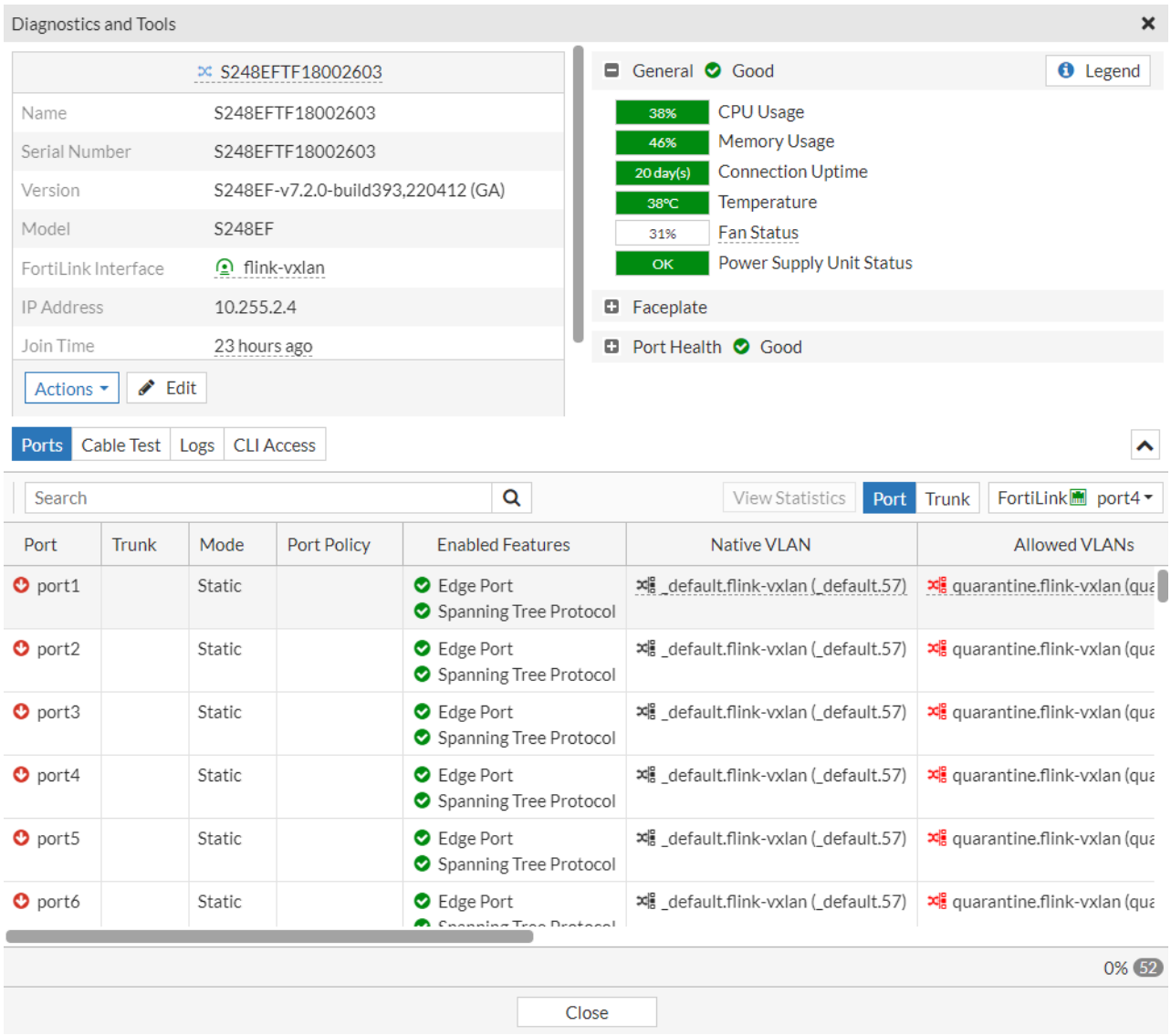
To use fabric management:

1. Go to *System* > *Fabric Management*.
2. Click *Fabric Upgrade* to upgrade FortiSwitch Manager.
3. Select one or more FortiSwitch units and then click *Upgrade* to update the FortiSwitchOS firmware.
4. If the registration status is *Not registered*, select the FortiSwitch unit and click *Register*.
5. If the status is *Waiting for authorization*, select the FortiSwitch unit and click *Authorize*.

6. Hover over any of the FortiSwitch units to see more information.



7. Click *Diagnostics and Tools* to open the *Diagnostics and Tools* pane.



Viewing and upgrading the FortiSwitch firmware version

You can view the current firmware version of a FortiSwitch unit and upgrade the FortiSwitch unit to a new firmware version. FortiSwitch Manager will suggest an upgrade when a new version is available in FortiGuard.

Using the FortiSwitch Manager GUI

To view the FortiSwitch firmware version:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Select the FortiSwitch name and click *Edit*.
3. In the *Edit Managed FortiSwitch* panel, the *Firmware* section displays the current build on the FortiSwitch unit.

To upgrade the firmware on multiple FortiSwitch units at the same time:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Select the FortiSwitch units that you want to upgrade.
3. Right-click and select *Upgrade*.The *Upgrade FortiSwitches* page opens.
4. Select *FortiGuard* or select *Upload* and then select the firmware file to upload. If you select *FortiGuard*, all FortiSwitch units that can be upgraded are upgraded. If you select *Upload*, only one firmware image can be used at a time for upgrading.
5. Select *Upgrade*.

Using the FortiSwitch Manager CLI

Use the following command to stage a firmware image on all FortiSwitch units:

```
execute switch-controller switch-software stage all <image id>
```

Use the following command to upgrade the firmware image on one FortiSwitch unit:

```
execute switch-controller switch-software upgrade <switch id> <image id>
```

Use the following CLI commands to enable the use of HTTPS to download firmware to managed FortiSwitch units:

```
config switch-controller global
   set https-image-push enable
end
```

NOTE: The HTTPS download is enabled by default.

From your FortiSwitch Manager CLI, you can upgrade the firmware of all of the managed FortiSwitch units of the same model using a single `execute` command. The command includes the name of a firmware image file and all of the managed FortiSwitch units compatible with that firmware image file are upgraded. For example:

```
execute switch-controller switch-software stage all <firmware-image-file>
```

You can also use the following command to restart all of the managed FortiSwitch units after a 2-minute delay.

```
execute switch-controller switch-action restart delay all
```

Canceling pending or downloading FortiSwitch upgrades

A managed FortiSwitch unit can be upgraded using FortiSwitch Manager.

If a connectivity issue occurs during the upgrade process and the FortiSwitch unit loses contact with FortiSwitch Manager, the FortiSwitch upgrade status can get stuck at `Upgrading`. Use the following CLI command to cancel the process:

```
execute switch-controller switch-software cancel {all | sn <FortiSwitch_serial_number> |
     switch-group <switch_group ID>}
```

`all`	Cancel the firmware upgrade for all FortiSwitch units.
`sn <FortiSwitch_serial_number>`	Cancel the firmware upgrade for the FortiSwitch unit with the specified serial number.
`switch-group <switch_group ID>`	Cancel the firmware upgrade for the FortiSwitch units belonging to the specified switch group.

For example, to cancel the upgrade of a FortiSwitch unit with the specified serial number:

```
execute switch-controller switch-software cancel sn S248EPTF180018XX
```

Configuring automatic backups

Starting in FortiSwitch Manager 7.2.2, you can specify whether your managed FortiSwitch configuration is automatically backed up each time a user logs out or before a system upgrade is started. By default, both options are disabled.

To specify that the managed FortiSwitch unit creates a revision configuration file each time a user logs out:

```
config switch-controller switch-profile
   edit {default | FortiSwitch_profile_name}
      set revision-backup-on-logout enable
   next
end
```

To specify that the managed FortiSwitch unit creates a revision configuration file before a system upgrade is started:

```
config switch-controller switch-profile
   edit {default | FortiSwitch_profile_name}
      set revision-backup-on-upgrade enable
   next
end
```

Replacing a managed FortiSwitch unit

If a managed FortiSwitch unit fails, you can replace it with another FortiSwitch unit that is managed by the same FortiSwitch Manager. The replacement FortiSwitch unit will inherit the configuration of the FortiSwitch unit that it replaces. The failed FortiSwitch unit is no longer managed by FortiSwitch Manager or discovered by FortiLink.

NOTE:

- Both FortiSwitch units must be of the same model.
- The replacement FortiSwitch unit must be discovered by FortiLink but not authorized.
- If the replacement FortiSwitch unit is one of an MCLAG pair, you need to manually reconfigure the MCLAG-ICL trunk.
- After replacing the failed FortiSwitch unit, the automatically created trunk name does not change. If you want different trunk name, you need to delete the trunk. The new trunk is created automatically with an updated name. At the end of this section is a detailed procedure for renaming the MCLAG-ICL trunk.
- If the replaced managed FortiSwitch unit is part of an MCLAG, only the ICL should be connected to the new switch to avoid any traffic loops. The other interfaces should be connected only to the switch that is fully managed by FortiSwitch Manager with the correct configuration.
- The best way to replace a MCLAG FortiSwitch unit in FortiLink:
  a. Back up the configuration of the failed FortiSwitch unit.
  b. Restore the configuration to the replaced FortiSwitch unit while it is offline.

c. Enter the `replace-device` command.
d. Physically replace the failed FortiSwitch unit.

To replace a managed FortiSwitch unit:

1. Unplug the failed FortiSwitch unit.
2. Plug in the replacement FortiSwitch unit.
3. Upgrade the firmware of the replacement FortiSwitch unit to the same version as the firmware on the failed FortiSwitch unit. See Viewing and upgrading the FortiSwitch firmware version on page 156.
4. Reset the replacement FortiSwitch unit to factory default settings with the `execute factoryreset` command.
5. Check the serial number of the replacement FortiSwitch unit.
6. From FortiSwitch Manager, go to *Switch Controller* > *Managed FortiSwitches*.
7. Right-click the name of the failed FortiSwitch unit.
8. Select *Authorization* > *Deauthorize*.
9. Connect the replacement FortiSwitch unit to FortiSwitch Manager.
   NOTE: If the replaced managed FortiSwitch unit is part of an MCLAG, only the ICL should be connected to the new switch to avoid any traffic loops. The other interfaces should be connected only to the switch that is fully managed by FortiSwitch Manager with the correct configuration.
10. Enter the following command:
    ```
    execute replace-device fortiswitch <failed_FortiSwitch_serial_number> <replacement_
         FortiSwitch_serial_number>
    ```
    An error is returned if the replacement FortiSwitch unit is authorized.
11. Authorize the replaced managed FortiSwitch unit.
12. Connect the rest of the cables required for the uplinks and downlinks for the MCLAG FortiSwitch units.

To rename the MCLAG-ICL trunk:

After replacing the failed FortiSwitch unit, the automatically created trunk name does not change. If you want different trunk name, you need to delete the trunk. The new trunk is created automatically with an updated name.

Changing the name of the MCLAG-ICL trunk must be done on both FortiSwitch Manager and the MCLAG-ICL switches. You need a maintenance window for the change.

1. Shut down the FortiLink interface on FortiSwitch Manager.
   a. On FortiSwitch Manager, execute the `show system interface` command. For example:

      ```
      FSWMVMTM21000008 # show system interface root-lag
       config system interface
       edit "root-lag"
       set vdom "root"
       set fortilink enable
       set ip 10.105.60.254 255.255.255.0
       set allowaccess ping capwap
       set type aggregate
       set member "port45" "port48"
       config managed-device
      ```

   b. Write down the member port information. In this example, port45 and port48 are the member ports.
   c. Shut down the member ports with the `config system interface`, `edit <member-port#>`, `set status down`, and `end` commands. For example:

```
FSWMVMTM21000008 # config system interface
FSWMVMTM21000008 (interface) # edit port48
FSWMVMTM21000008 (port48) # set status down
FSWMVMTM21000008 (port48) # next // repeat for each member port
FSWMVMTM21000008 (interface) # edit port45
FSWMVMTM21000008 (port45) # set status down
FSWMVMTM21000008 (port45) # end
```

d. Verify that FortiLink is down with the `exec switch-controller get-conn-status` command. For example:

```
FSWMVMTM21000008 # exec switch-controller get-conn-status
Managed-devices in current vdom root:
 STACK-NAME: FortiSwitch-Stack-root-lag
 SWITCH-ID VERSION STATUS ADDRESS JOIN-TIME NAME
 FS1D483Z17000282 v6.0.0 Authorized/Down 0.0.0.0 N/A icl-sw2
 FS1D483Z17000348 v6.0.0 Authorized/Down 0.0.0.0 N/A icl-sw1
```

2. Rename the MCLAG-ICL trunk name on both MCLAG-ICL switches.

a. Execute the `show switch trunk` command on both MCLAG-ICL switches. Locate the ICL trunk that includes the `set mclag-icl enable` command in its configuration and write down the member ports and configuration information. For example:

```
icl-sw1 # show switch trunk
config switch trunk
...
edit "D483Z17000282-0"
set mode lacp-active
set auto-isl 1
set mclag-icl enable // look for this line
set members "port27" "port28" // note the member ports
next
end
```

b. Note the output of the `show switch interface <MCLAG-ICL-trunk-name>`, `diagnose switch mclag icl`, and `diagnose switch trunk summary <MCLAG-ICL-trunk-name>` commands. For example:

```
icl-sw1 # show switch interface D483Z17000282-0
config switch interface
edit "D483Z17000282-0"
set native-vlan 4094
set allowed-vlans 1,100,2001-2060,4093
set dhcp-snooping trusted
set stp-state disabled
set edge-port disabled
set igmps-flood-reports enable
set igmps-flood-traffic enable
set snmp-index 57
next
end

icl-sw1 # diag switch mclag icl
```

```
D483Z17000282-0
icl-ports 27-28
egress-block-ports 3-4,7-12,47-48
interface-mac 70:4c:a5:86:6d:e5
lacp-serial-number FS1D483Z17000348
peer-mac 70:4c:a5:49:50:53
peer-serial-number FS1D483Z17000282
Local uptime 0 days 1h:49m:24s
Peer uptime 0 days 1h:49m:17s
MCLAG-STP-mac 70:4c:a5:49:50:52
keepalive interval 1
keepalive timeout 60

Counters
received keepalive packets 4852
transmited keepalive packets 5293
received keepalive drop packets 20
receive keepalive miss 1

icl-sw1 # diagnose switch trunk sum D483Z17000282-0
Trunk Name Mode PSC MAC Status Up Time
_____ _____ _____ _____ _____ _____
____ _____
D483Z17000282-0 lacp-active(auto-isl,mclag-icl) src-dst-ip 70:4C:A5:86:6E:00 up
(2/2) 0 days,0 hours,16 mins,4 secs
```

c. Shut down the ICL member ports using the `config switch physical-port`, `edit <member port#>`, `set status down`, `next`, and `end` commands. For example:

```
icl-sw1 # config switch physical-port
icl-sw1 (physical-port) # edit port27
icl-sw1 (port27) # set status down
icl-sw1 (port27) # n // repeat for each ICL member port
icl-sw1 (physical-port) # edit port28
icl-sw1 (port28) # set status down
icl-sw1 (port28) # next
icl-sw1 (physical-port) # end
```

d. Delete the original MCLAG-ICL trunk name on the switch using the `config switch trunk`, `delete <mclag-icl-trunk-name>`, and `end` commands. For example:

```
icl-sw1 # config switch trunk
icl-sw1 (trunk) # delete D483Z17000282-0
```

e. Use the `show switch trunk` command to verify that the trunk is deleted.

f. Create a new trunk for the MCLAG ICL using the original ICL trunk configuration collected in step 2b and the `set auto-isl 0` command in the configuration. For example:

```
icl-sw1 # config switch trunk

icl-sw1 (trunk) # edit MCLAG-ICL
new entry 'MCLAG-ICL' added
icl-sw1 (MCLAG-ICL) #set mode lacp-active
```

```
icl-sw1 (MCLAG-ICL) #set members "port27" "port28"
icl-sw1 (MCLAG-ICL) #set mclag-icl enable
icl-sw1 (MCLAG-ICL) # end
```

g. Use the `show switch trunk` command to check the trunk configuration.

h. Start the trunk member ports by using the `config switch physical-port`, `edit <member port#>`, `set status up`, `next`, and `end` commands. For example:

```
icl-sw1 # config switch physical-port
icl-sw1 (physical-port) # edit port27
icl-sw1 (port27) # set status up
icl-sw1 (port27) # next // repeat for each trunk member port
icl-sw1 (physical-port) # edit port28
icl-sw1 (port28) # set status up
icl-sw1 (port28) # end
```

NOTE: Follow steps 2a through 2h on both switches.

3. Set up the FortiLink interface on FortiSwitch Manager. Enter the `config system interface`, `edit <interface-member-port>`, `set status up`, `next`, and `end` commands. For example:

```
FSWMVMTM21000008 # config system interface
 FSWMVMTM21000008 (interface) # edit port45
 FSWMVMTM21000008 (port45) # set status up
 FSWMVMTM21000008 (port45) # next // repeat on all member ports
 FSWMVMTM21000008 (interface) # edit port48
 FSWMVMTM21000008 (port48) # set status up
 FSWMVMTM21000008 (port48) # next
 FSWMVMTM21000008 (interface) # end
```

4. Check the configuration and status on both MCLAG-ICL switches

a. Enter the `show switch trunk`, `diagnose switch mclag icl`, and `diagnose switch trunk summary <new-trunk-name>` commands. For example:

```
icl-sw1 # show switch trunk
 config switch trunk
 <snip>
 edit "MCLAG-ICL"
 set mode lacp-active
 set mclag-icl enable
 set members "port27" "port28"
 next
 end

 icl-sw1 # show switch interface MCLAG-ICL
 config switch interface
 edit "MCLAG-ICL"
 set native-vlan 4094
 set allowed-vlans 1,100,2001-2060,4093
 set dhcp-snooping trusted
 set stp-state disabled
 set igmps-flood-reports enable
 set igmps-flood-traffic enable
 set snmp-index 56
```

```
next
end

icl-sw1 # diagnose switch mclag icl
MCLAG-ICL
icl-ports 27-28
egress-block-ports 3-4,7-12,47-48
interface-mac 70:4c:a5:86:6d:e5
lacp-serial-number FS1D483Z17000348
peer-mac 70:4c:a5:49:50:5
peer-serial-number FS1D483Z17000282
Local uptime 0 days 2h:11m:13s
Peer uptime 0 days 2h:11m: 7s
MCLAG-STP-mac 70:4c:a5:49:50:52
keepalive interval 1
keepalive timeout 60

Counters
received keepalive packets 5838
transmited keepalive packets 6279
received keepalive drop packets 27
receive keepalive miss 1

icl-sw1 # diagnose switch trunk summary MCLAG-ICL

Trunk Name Mode PSC MAC Status Up Time
_____ _____ _____ _____ _____
_____ _____

 MCLAG-ICL lacp-active(auto-isl,mclag-icl) src-dst-ip 70:4C:A5:86:6E:00 up(2/2)
0 days,1 hours,4 mins,57 secs
```

b. Compare the command results in step 4a with the command results in step 2b.

Executing custom FortiSwitch scripts

From FortiSwitch Manager, you can execute a custom script on a managed FortiSwitch unit. The custom script contains generic FortiSwitch commands.

This section covers the following topics:

- Creating a custom script on page 163
- Executing a custom script once on page 164
- Binding a custom script to a managed switch on page 164

Creating a custom script

Use the following syntax to create a custom script from FortiSwitch Manager:

```
config switch-controller custom-command
   edit <cmd-name>
      set command "<FortiSwitch_command>"
   end
```

NOTE: You need to use `%0a` to indicate a return.

For example, use the custom script to set the STP max-age parameter on a managed FortiSwitch unit:

```
config switch-controller custom-command
   edit "stp-age-10"
      set command "config switch stp setting %0a set max-age 10 %0a end %0a"
   end
```

Executing a custom script once

After you have created a custom script, you can manually execute it on any managed FortiSwitch unit. Because the custom script is not bound to any switch, the FortiSwitch unit might reset some parameters when it is restarted.

Use the following syntax on FortiSwitch Manager to execute the custom script once on a specified managed FortiSwitch unit:

```
execute switch-controller custom-command <cmd-name> <target-switch>
```

For example, you can execute the `stp-age-10` script on the specified managed FortiSwitch unit:

```
execute switch-controller custom-command stp-age-10 S124DP3X15000118
```

Binding a custom script to a managed switch

If you want the custom script to be part of the managed switch's configuration, the custom script must be bound to the managed switch. If any of the commands in the custom script are locally controlled by a switch, the commands might be overwritten locally.

Use the following syntax to bind a custom script to a managed switch:

```
config switch-controller managed-switch
   edit "<FortiSwitch_serial_number>"
      config custom-command
         edit <custom_script_entry>
            set command-name "<name_of_custom_script>"
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S524DF4K15000024"
      config custom-command
         edit 1
            set command-name "stp-age-10"
         next
      end
   next
end
```

Configuring automation stitches

Starting in FortiSwitch Manager 7.2.2, you can configure automation stitches.

To configure an automation stitch, you specify a trigger and the action that is performed when the trigger occurs and then associate the trigger and action in the automation stitch.

You can specify one of the following triggers:

- An event was logged.

  NOTE: When you specify the log ID, the range of values is 1-65535. If you use the full 10-digit entry, the first four digits are truncated.
- FortiSwitch Manager was rebooted.
- The memory is low.
- There is high CPU usage.
- The FortiCare license is near its expiration date.
- The configuration changed.
- The scheduled time occurred.

You can use the following wildcard characters in the `set value` command for the automation trigger:

- Use an asterisk to match any character string of any length, including 0-characters long. For example, use `set value "*1567*"` to match values of `81567` and `156789`.
- Use square brackets to match one of multiple characters. For example, use `set value "[aA]dmin"` to match values of `admin` and `Admin`.

You can also configure multiple fields for the automation trigger when `event-type` is `event-log` and `logid` is set. The action is only performed if all conditions are valid (using AND logic). For example, the following automation trigger requires both the log message to include `VRRP` and the interface to be `svi777` before the action is performed.

```
config system automation-trigger
   edit "VRRPlogtrigger"
      set event-type event-log
      set logid 10200
      config fields
         edit 1
            set name "msg"
            set value "*VRRP*"
         next
         edit 2
            set name "interface"
            set value "svi777"
         next
      end
   next
end
```

You can specify one of the following actions:

- Send an email message.
- Display an alert in the console (CLI only).
- Send data to a uniform resource identifier (URI), such as an IP address or URL.

- Run a CLI script.
- Perform an immediate system operation on this FortiSwitch Manager unit.

To configure an automation stitch in the CLI:

1. Create an automation trigger.

```
config system automation-trigger
   edit <automation_trigger_name>
      set description <string>
      set trigger-type {event-based | scheduled}
      set event-type {event-log | reboot | low-memory | high-cpu | license-near-expiry |
           config-change }
      set license-type forticare-support
      set logid <1-65535>
      set trigger-frequency {hourly | daily | weekly | monthly | once}
      set trigger-hour <0-23>
      set trigger-minute <0-59>
      set trigger-day <1-31>
      set trigger-weekday <sunday | monday | tuesday | wednesday | thursday | friday |
           saturday>
      config fields
         edit <entry_ID>
            set name <string>
            set value <string>
         next
      end
   next
end
```

2. Create an automation action.

```
config system automation-action
   edit <automation_action_name>
      set description <string>
      set action-type {email | alert | webhook | cli-script | system-actions}
      set accprofile <string>
      set email-from <string>
      set email-subject <string>
      set email-to <email_address>
      set execute-security-fabric {enable | disable}
      set http-body <request_body>
      set method {delete | get | patch | post | put}
      set message <string>
      set minimum-interval <0-2592000>
      set output-size <1-1024 megabytes>
      set port <1-65535>
      set protocol {http | https}
      set replacement-message {enable | disable}
      set replacemsg-group <string>
      set script <string>
      set system-action {reboot | shutdown | backup-config}
      set timeout <0-300 seconds>
      set uri <request_API_URI>
   next
end
```

3. Create the automation stitch.

   NOTE: The `set required` command is only available when the *Sequential* button has been selected in the GUI.

```
config system automation-stitch
   edit <automation_stitch_name>
      set description <st
      set status {enable | disable}
      set trigger <trigger_name>
      set destination <serial_number_of_destination_devices>
      config actions
         edit <entry_identifier>
            set action <automation_action_name>
            set delay <0-3600 seconds>
            set required {enable | disable}
         next
      end
   next
end
```

4. Test the automation stitch.

   NOTE: If the trigger is the log identifier, you must add values for `logid`, `level`, and `vd`.

   ```
   diagnose automation test <automation-stitch-name> ["logid=<log_ID> type=event
        level=information vd=root"]
   ```

   For example:

   ```
   diagnose automation test interfacedown-stitch "logid=0100044547 type=event
        level=information vd=root"
   ```

To configure an automation stitch in the GUI:

1. Create an automation trigger.
   a. Go to *System* > *Automation*.
   b. Click the *Trigger* tab.
   c. Click *Create New*.
   d. Select *Configuration Change*, *Conserve Mode*, *High CPU*, *License Expiry*, *Reboot*, *FortiSwitchManagerOS Event Log*, or *Schedule*.

e. Fill out the fields for the trigger you selected.

Trigger	Fields
Configuration Change	• *Name*—Enter a name for the trigger. • *Description*—Enter a description of the trigger.
Conserve Mode	• *Name*—Enter a name for the trigger. • *Description*—Enter a description of the trigger.
High CPU	• *Name*—Enter a name for the trigger. • *Description*—Enter a description of the trigger.
License Expiry	• *Name*—Enter a name for the trigger. • *Description*—Enter a description of the trigger. • *License*—Select *FortiCare Support*. **NOTE:** The other license types are not supported.
Reboot	• *Name*—Enter a name for the trigger. • *Description*—Enter a description of the trigger.
FortiSwitchManagerOS Event Log	• *Name*—Enter a name for the trigger. • *Description*—Enter a description of the trigger. • *Event*—Click +, select one or more events, and then click *Close*. • *Field filter(s)*—Click + and enter the field name and value. If you want to add another filter, click +. **NOTE:** All configured filters must match before the stitch is triggered.
Schedule	• *Name*—Enter a name for the trigger. • *Description*—Enter a description of the trigger. • *Frequency*—Select how often the stitch is triggered: *Hourly*, *Daily*, *Weekly*, *Monthly*, or *Once*. Enter the values in the fields that correspond to the frequency you selected.

f. Click *OK*.

2. Create an automation action.

a. Go to *System* > *Automation*.

b. Click the *Action* tab.

c. Click *Create New*.

d. Select *Email*, *CLI Script*, *Webhook*, or *System Action*.

e. Fill out the fields for the action you selected.

Action	Fields
Email	• *Name*—Enter a name for the action. • *Minimum interval*—Select the units for the time interval: *second(s)*, *minute(s)*, or *hour(s)*. Enter the number for the time interval. **NOTE:** The action will only be allowed to trigger once within this time interval. • *Description*—Enter a description of the action.

Action	Fields
	• *From*—Enter an email address. • *To*—Enter an email address. Click + if you want the email sent to more than one address. • *Subject*—Enter the subject of the email. • *Body*—Enter the text for the email or use action parameters, such as the log message or source IP address. Click % for more information about the available action parameters. • *Replacement message*—If you want to use a replacement message, enable *Replacement message* and then click *Edit*. You can use text, HTML, and action parameters in the replacement message. When you are done, click *Save*.
CLI Script	• *Name*—Enter a name for the action. • *Minimum interval*—Select the units for the time interval: *second(s)*, *minute(s)*, or *hour(s)*. Enter the number for the time interval. **NOTE:** The action will only be allowed to trigger once within this time interval. • *Description*—Enter a description of the action. • *CLI Script*—You can enter the CLI commands in the *Script* field, click *Upload* to select a file with your CLI script, or click *Record in CLI console* to enter the CLI commands in the console. • *Administrator profile*—You can select one of the available administrator profiles to use when executing the CLI script or click *Create* to configure a new administrator profile. The administrator profile selected determines which CLI commands can be executed. • *Execute on Security Fabric*—Enable if you want to execute the CLI script on all FortiSwitch Managers in the Security Fabric. Disable if you want to execute the CLI script on just the current FortiSwitch Manager.
Webhook	• *Name*—Enter a name for the action. • *Minimum interval*—Select the units for the time interval: *second(s)*, *minute(s)*, or *hour(s)*. Enter the number for the time interval. **NOTE:** The action will only be allowed to trigger once within this time interval. • *Description*—Enter a description of the action. • *Protocol*—Select HTTP or HTTPS for the protocol. • *URL*—Enter the URL for the webhook to use. • *Custom port*—If you want to specify the port for the webhook to use, enable *Custom port* and enter the port number. • *Method*—Select *POST*, *PUT*, *GET*, *PATCH*, or *DELETE*. • *HTTP body*—Enter the HTTP request. • *HTTP header*—Enter the header name and value. Click + if you want to add another header. • *TLS certificate*—If you selected *HTTPS* for the protocol, you can enable *TLS certificate* and select which TLS certificate to use for security. If you do not select a TLS certificate, the HTTPS request uses the BIOS certificate.

Action	Fields
	• *Verity remote host*—If you selected *HTTPS* for the protocol, you can verify that the remote host certificate matches the host URL.
System Action	• *Name*—Enter a name for the action. • *Minimum interval*—Select the units for the time interval: *second(s)*, *minute(s)*, or *hour(s)*. Enter the number for the time interval. **NOTE:** The action will only be allowed to trigger once within this time interval. • *Description*—Enter a description of the action. • *Action*—Select the system action: *Reboot*, *Shutdown*, or *Backup configuration*.

   f. Click *OK*.

3. Create the automation stitch.
   a. Go to *System* > *Automation*.
   b. Click *Create New* under the *Stitch* tab.
   c. Select *Sequential* if you want the actions to be executed one after another unless an action fails. Select *Parallel* if you want all actions to be executed immediately when the stitch is triggered. **NOTE:** Action parameters do not work with parallel execution.
   d. In the *Description* field, enter a description of the stitch.
   e. Click +, select a trigger, and then click *Apply*.
   f. Click +, select an action, and then click *Apply*.
   g. If you want to add more actions, click +.
   h. Click *OK*.
4. Test the automation stitch.
   NOTE: Only some of the automation stitches can be tested.
   a. Go to *System* > *Automation*.
   b. Right-click on the automation stitch.
   c. Click *Test Automation Stitch*.

Examples

The following example shows how to create an automation stitch that will display an alert in the console every hour.

```
config system automation-trigger
   edit testtrigger
      set trigger-type scheduled
      set trigger-frequency hourly
      set trigger-minute 30
   next
end

config system automation-action
   edit testaction
      set action-type alert
      set minimum-interval 1200
   next
end
```

```
config system automation-stitch
   edit teststitch
      set status enable
      set trigger testtrigger
      config actions
         edit 1
            set required enable
            set delay 0
            set action testaction
         next
      end
   next
end
```

In the following example, the specified log identifier (32002) causes the FortiSwitch unit to send the log message to the server.

```
config system automation-action
   edit "Send log to server"
      set action-type webhook
      set uri "172.16.200.44"
      set http-body "%%log%%"
      set port 80
   next
end

config system automation-trigger
   edit "badLogin"
      set event-type event-log
      set logid 32002
   next
end

config system automation-stitch
   edit "webhookstitch"
      set trigger "badLogin"
      config actions
         edit 2
            set action "Send log to server"
         next
      end
   next
end
```

In the following example, the administrator receives an email whenever FortiSwitch Manager is restarted.

```
config system automation-trigger
   edit "Reboot"
      set event-type reboot
   next
end

config system automation-action
   edit "emailtest"
      set action-type email
      set email-to "admin@fortinet.com"
   next
end
```

```
config system automation-stitch
   edit "rebootdashboard"
      set trigger "Reboot"
      config actions
         edit 1
            set action "emailtest"
         next
      end
   next
end
```

Creating and applying templates for managed-switch configurations

Starting in FortiSwitch Manager 7.2.2, you can use the CLI to do the following:

- Create a template.
- Copy a managed-switch configuration to a template.
- Apply the template to a managed switch.
- Apply the configuration of one managed switch to another managed switch.

You can manually apply configuration changes to up to 10 FortiSwitch units at a time or automatically apply changes to an unlimited number of switches using switch groups. Using templates makes it easier to configure new switches and to ensure that the same changes are made consistently to all switches of the same model.

Configuration changes are logged as system events. Use the `execute log display` command to view the logs.

You need to configure the following in the template:

- `fsw-wan1-peer` by specifying the FortiLink interface
- `sn` by specifying the FortiSwitch serial number. **NOTE:** The first six characters of `sn` must match the first six characters of the switch model that you will use the template to configure.

Starting in FortiSwitch Manager 7.2.5, the value of the `set sn` command is used to match the FortiSwitch models of the templates and switches so that the commands are applied correctly.

After you create a template for a specific model, you can copy the flags for dynamic capabilities to the template and then copy the configuration from a managed switch to the template.

To create a template:

```
config switch-controller managed-switch
   edit "<name_of_template>"
      set fsw-wan1-peer <FortiLink_interface>
      set sn <managed-switch serial number>
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S248EP@112233445"
```

```
      set fsw-wan1-peer port3
      set sn S248EPTV21000212
      set fsw-wan1-admin enable
    next
end
```

You can use the template in the example to configure FS-248E-POE models.

To copy a managed-switch configuration to a template:

1. Copy the flags for the dynamic capabilities from a managed switch to the template:
   `execute switch-controller templating copy-dynamic-capability <serial_number> <template>`
   For example, to copy the dynamic-capability flags for `S248EP3X17000002` to `S248EP@112233445`:
   `execute switch-controller templating copy-dynamic-capability S248EP3X17000002 S248EP@112233445`
2. Copy the configuration from a managed switch to the template:
   `execute switch-controller templating apply-config <FortiSwitch_serial_number> <template>`
   For example, to copy from `S248EP3X17000003` to `S248EP@112233445`:
   `execute switch-controller templating apply-config S248EP3X17000003 S248EP@112233445`
   Enter `C` to make the changes or enter `A` to make no changes.
3. If you entered `C`, you can enter `V` to see a summary of the changes made and whether the command was successful.
4. If you entered `V`, you can enter `y` to display the log file with details of all changes made.
5. If you entered `y`, you can press any key to return to the summary and then enter `E` to exit the command.

To manually apply a template to up to 10 managed switches of the same model:

NOTE: You can also this command to apply the configuration from one managed switch to another managed switch of the same model.

1. Apply a template to up to 10 managed switches:
   `execute switch-controller templating apply-config <template> <serial_number_1> ... <serial_number_10>`
   For example, to copy from `S248EP@112233445` to `S248EP3X17000003` and `S248EP3X17000002`:
   `execute switch-controller templating apply-config S248EP@112233445 S248EP3X17000003 S248EP3X17000002`
2. If there are any warnings or errors, enter `C` to continue with the command, enter `S` to skip the switch with the warnings or errors, enter `A` to make no changes, or enter `V` to see the details for all changes made for this command.
3. If you entered `C` to continue, you can enter `C` to make the changes or enter `A` to make no changes.
4. If you entered `C`, you can enter `V` to see a summary of the changes made and whether the command was successful or enter `E` to exit the command.

To automatically apply a template to new switch group members:

Create a FortiSwitch group with one or more FortiSwitch units. You can include different switch models as members of the switch group. You can include a managed FortiSwitch unit or template for each switch model for the `set templates` command. A switch can be listed as a value for both the `set members` command and `set templates` command. By default, `template-auto-apply` is enabled, and the templates are automatically applied to new switch group members of the same switch model when they are added to the switch group. If there are any errors, no changes are made to the switch group. Use the `enable-allow-warnings` setting if you want to continue with applying the template for a switch-group members that gives warnings but no errors.

If there is an error when applying a template to a new switch group member, you can manually apply the template to the new switch group member using the `execute switch-controller templating apply-config` command. This command allows you to interactively monitor the template being applied and then examine the output to see which command is failing and if there are any relevant CLI error messages.

```
config switch-controller switch-group
   edit <switch_group_name>
      set fortilink <FortiLink_interface>
      set members "<serial_number_1>" "<serial_number_2>" ...
      set templates "<template_name_or_serial_number>" "<template_name_or_serial_number>"
           ...
      set template-auto-apply {enable | disable | enable-allow-warnings}
   next
end
```

For example, this switch group includes two templates for two different switch models:

```
config switch-controller switch-group
   edit switchgroup1
      set fortilink "port3"
      set members S524DF4K150000482 S248EP3X17000003 S248EP3X17000002
      set templates S248EP@BBBBBBBBB S524DF@123456789
      set template-auto-apply enable
   next
end
```

The template is applied quietly when a new switch member is added with a model that matches one of the templates. An error message is returned if there are any problems.

To manually copy a template to a switch group:

- To apply all templates to the switch group members that match the model of the template:
  `execute switch-controller templating switch-group-apply-all <switch_group_name>`
  For example, the templates in `switchgroup1` are applied to the group members if the switch models match:
  `execute switch-controller templating switch-group-apply-all switchgroup1`
  Enter `C` to save the changes or enter `A` to undo the changes. Enter `V` to see the details for all changes made for this command.
- To apply any matching templates to the specified members of the specified switch group. You can list up to 10 members.
  `execute switch-controller templating switch-group-apply-members <switch_group_name> <serial_number_1> ... <serial_number_10>`
  For example, one of the templates in `switchgroup1` is applied to `S248EP3X17000003` and `S248EP3X17000002` if the switch model matches:
  `execute switch-controller templating switch-group-apply-members switchgroup1 S248EP3X17000003 S248EP3X17000002`
- To apply the specified template to any matching members of the specified switch group:
  `execute switch-controller templating switch-group-apply-template <switch_group_name> <template_name>`
  For example, the configuration in `S524DF@123456789` is applied to matching members in `switchgroup1`:
  `execute switch-controller templating switch-group-apply-template switchgroup1 S524DF@123456789`

- To find switches that list the specified switch or template for the `set last-template-applied` value (under the `config switch-controller managed-switch` command) and re-apply the same configuration to those switches:
  `execute switch-controller templating reapply-config <serial_number_or_template_name>`
  For example, `S248EP@BBBBBBBBB` is re-applied to any managed switches that list them as the `set last-template-applied` value:
  `execute switch-controller templating reapply-config S248EP@BBBBBBBBB`

To get troubleshooting information:

```
diagnose debug application fswmtemplate <debug_level>
```

This command enables more detailed output in the console and in the command logs when you run the `execute templating` commands and when templates are automatically applied to new switch group members.

Limitations

The following limitations apply to this feature:

- The source and destination managed FortiSwitch models must be the same.
- The name of the switch is not copied.
- Read-only settings are not copied.
- Dynamic capabilities are not copied.
- Templates do not support switches with split-port configurations or other nondefault layouts. To work around this issue, configure the source switch with a split-port configuration, manually configure the destination switch with the same split-port configuration, and then apply the managed-switch configuration from the source switch to the destination switch.
- IP addresses for system interfaces are not copied when templates are applied; this prevents IP conflicts.
- Port speeds and other configurations that are determined at run-time might not be filtered when creating a template. Use caution or consult a managed switch to determine the acceptable values.
- You cannot apply the managed-switch configuration from and to the same FortiSwitch unit.
- When applying a template or managed-switch configuration to another switch, the system cannot delete entries that are not present in the source template or managed-switch configuration. These leftover entries might cause conflicts. To avoid configuration conflicts, Fortinet recommends first resetting an existing managed-switch configuration to the factory default configuration before applying a template.
- If you change a template, it does not automatically update all switches that have had that template applied. Use the `execute switch-controller templating reapply-config <template_name>` command to re-apply the template to all managed switches that list the template in the `set last-template-applied` field. **NOTE:** If you applied a managed-switch configuration to other managed switches and then later change that managed-switch configuration, you can also use the `execute switch-controller templating reapply-config <template_name>` command to re-apply the managed-switch configuration to all managed switches that list that switch in the `set last-template-applied` field.

Resetting PoE-enabled ports

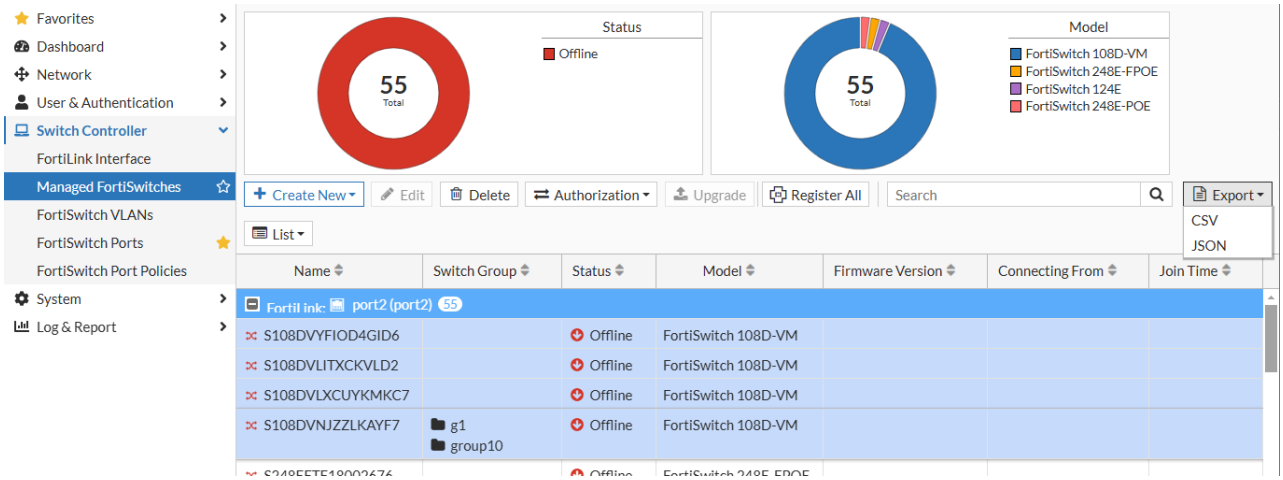
If you need to reset PoE-enabled ports, go to *Switch Controller* > *FortiSwitch Ports*, right-click on one or more PoE-enabled ports and select *Reset PoE* from the context menu.

Exporting switch information

Starting in FortiSwitch Manager 7.2.5, you can export a list of FortiSwitch names, switch groups, status, models, firmware versions, where the switch is connecting from, and the join times. You can also export a list of switch ports with trunk names, port policies, enabled features, native VLANs, allowed VLANs, dynamic VLANs, PoE status, device information, security policies, DHCP-snooping status, transceivers connected to, transceiver power (transmitted or received), and negotiated speed. You can choose to export each list in comma-separated values (CSV) or JSON format.

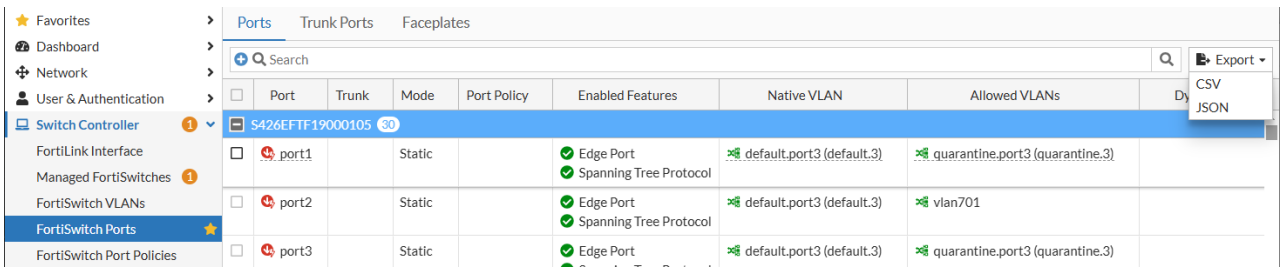
To export a list of FortiSwitch information:

1. Go to *Switch Controller* > *Managed FortiSwitches*.
2. Select the switch rows that you want to export.
3. From the *Export* menu, select *CSV* or *JSON*.



To export a list of all FortiSwitch port information:

1. Go to *Switch Controller* > *FortiSwitch Ports*.
2. From the *Export* menu, select *CSV* or *JSON*.



3. In the *Export to CSV* pane or the *Export to JSON* pane, click *Export*.
   NOTE: Filters entered in *Search* field do not affect the exported port information.

www.fortinet.com