FortiSwitch - Managed by FortiOS 6.4

Version 6.4.0

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

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

September 2, 2021
FortiSwitch 6.4.0 Managed by FortiOS 6.4
11-640-591525-20210902

TABLE OF CONTENTS

Change log

Date	Change Description
March 31, 2020	Initial document release for FortiOS 6.4.0
May 4, 2020	Updated the “Configuring storm control” section.
May 8, 2020	Updated the “Sharing FortiSwitch ports between VDOMs” section.
July 7, 2020	Updated the “Configuring dynamic ARP inspection (DAI)” section.
September 1, 2021	Updated the “Support of FortiLink features” section.
September 2, 2021	Updated the “Support of FortiLink features” section.

What's new in FortiOS 6.4.0

The following list contains new managed FortiSwitch features added in FortiOS 6.4.0. Click on a link to navigate to that section for further information.

- An integrated FortiGate network access control (NAC) function is provided to the FortiAP and FortiSwitch networks by using a shared set of NAC policies. The NAC policy can be applied based on data from the user device list. There is also a wizard to help with configuring FortiSwitch NAC settings and defining a FortiSwitch NAC VLAN. See FortiSwitch network access control on page 147.
- To more accurately detect Internet of Things (IoT) devices, a new FortiGuard service is available to provide a large database of device IoT identification. Devices detected on the local FortiGate unit and through the FortiAP and FortiSwitch networks can be queried with the FortiGuard IoT device database to provide enhanced identification. See Configuring IoT detection on page 154.
- A FortiLink topology with an HA cluster of four FortiGate units is now supported. See FortiLink with an HA cluster of four FortiGate units on page 54.
- FortiLink mode can now run over a point-to-point layer-2 network. See FortiLink over a point-to-point layer-2 network on page 56.
- LLDP neighbor devices are now dynamically detected. See Configure LLDP-MED on page 81.
- IPv4 source guard can now be configured in FortiOS for managed FortiSwitch units that support IP source guard. See Configuring IPv4 source guard on page 74.
- The number of FortiSwitch units supported by certain FortiGate models has been increased.
- The quarantine feature on the FortiSwitch unit has been extended by allowing a device to be quarantined but remain with the VLAN where it was detected. You can still quarantine devices to a VLAN. See Quarantining MAC addresses on page 88.
- Administrators can now modify some configuration options of automatically generated VLANs using the `config switch-controller initial-config template` command. These changes are applied at the time of VLAN creation. See Defining a FortiSwitch NAC VLAN on page 147.
- On the Managed FortiSwitch page, you can now view the managed FortiSwitch units in a list, in groups of switches, or in a topology diagram.
- IGMP snooping is now always enabled on managed switch interfaces and cannot be disabled.
- When an inter-switch link (ISL) is formed automatically in FortiLink mode, the `igmps-flood-reports` and `igmps-flood-traffic` options are now disabled by default.
- Storm control is now disabled by default in FortiLink mode.

Introduction

This section provides information about how to set up and configure managed FortiSwitch units using the FortiGate unit (termed “using FortiSwitch in FortiLink mode”).

NOTE: FortiLink is not supported in transparent mode.

The maximum number of supported FortiSwitch units depends on the FortiGate model:

FortiGate Model Range	Number of FortiSwitch Units Supported
FortiGate 91E, FortiGate-VM01	8
FortiGate 6xE, 8xE, 90E	16
FortiGate 100D, FortiGate-VM02	24
FortiGate 100E, 100EF, 101E, 140E, 140E-POE	32
FortiGate 200E, 201E	64
FortiGate 300D to 500D	48
FortiGate 300E to 500E	72
FortiGate 600D to 900D and FortiGate-VM04	64
FortiGate 600E to 900E	96
FortiGate 1000D to 15xxD	128
FortiGate 1100E to 25xxE	196
FortiGate-3*xxx* and up and FortiGate-VM08 and up	300

Supported models

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

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

Support of FortiLink features

The following table lists the FortiSwitch models supported by FortiLink features.

FortiLink Features	FortiSwitch Models
Centralized VLAN Configuration	D-series, E-series
Switch POE Control	D-series, E-series
Link Aggregation Configuration	D-series, E-series
Spanning Tree Protocol (STP)	D-series, E-series
LLDP/MED	D-series, E-series
IGMP Snooping	Not supported on 112D-POE
802.1x Authentication (Port-based, MAC-based, MAB)	D-series, E-series
Syslog Collection	D-series, E-series
DHCP Snooping	Not supported on 1xxE-Series
Device Detection	D-series, E-series
Support FortiLink FortiGate in HA Cluster	D-series, E-series
LAG support for FortiLink Connection	D-series, E-series
Active-Active Split MLAG from FortiGate to FortiSwitch units for Advanced Redundancy	Not supported on FS-1xx Series
sFlow	Not supported on 1xxE-Series
Dynamic ARP Inspection (DAI)	D-series, E-series
Port Mirroring	D-series, E-series
RADIUS Accounting Support	Not supported on 1xxE-Series
Centralized Configuration	D-series, E-series
Access VLAN	D-series, E-series
STP BDPU Guard, Root Guard, Edge Port	D-series, E-series
Loop Guard	D-series, E-series
Switch admin Password	D-series, E-series
Storm Control	D-series, E-series
802.1x-Authenticated Dynamic VLAN Assignment	D-series, E-series
Host Quarantine on Switch Port	D-series, E-series
QoS	Not supported on 1xxE-Series or 112D-POE
Centralized Firmware Management	D-series, E-series

FortiLink Features	FortiSwitch Models
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
NetFlow and IPFIX flow tracking and export	D-series, E-series
FortiSwitch split ports	524D, 524D-FPOE, 548D, 548D-FPOE, 1048E, 3032D
Encapsulated remote switched port analyzer (ERSPAN)	2xx and higher
MSTP instances **NOTE:** In FortiLink mode, the FortiGate unit supports 1-14 instances for all platforms.	D-series, E-series
QoS statistics	D-series, E-series
Configuring SNMP through FortiLink	D-series, E-series
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, and FS-2xxE

Before you begin

Before you configure the managed FortiSwitch unit, the following assumptions have been made in the writing of this manual:

- You have completed the initial configuration of the FortiSwitch unit, as outlined in the QuickStart Guide for your FortiSwitch model, and you have administrative access to the FortiSwitch GUI and CLI.
- You have installed a FortiGate unit on your network and have administrative access to the FortiGate GUI and CLI.

How this guide is organized

This guide contains the following sections:

- What's new in FortiOS 6.2.2 describes the new features for this release.
- Introduction lists supported FortiSwitch models, number of FortiSwitch units supported, and supported FortiLink features.
- Connecting FortiLink ports describes how to connect FortiSwitch ports to FortiGate ports.
- Using the FortiGate GUI describes how to use the FortiGate GUI for FortiLink configuration.
- Using the FortiGate CLI describes how to use the FortiGate CLI for FortiLink configuration.
- Network topologies describes the configuration for various network topologies.
- MCLAG configuration for access ports describes how to set up a multichassis LAG (MCLAG).

- Optional setup tasks describes other setup tasks that are optional.
- FortiSwitch features configuration describes how to configure managed FortiSwitch features, including VLANs.
- FortiSwitch port features describe how to configure ports and PoE from the FortiGate unit.
- FortiSwitch port security policy describes how to set up FortiSwitch security policies.
- Additional capabilities describes more FortiSwitch features.
- Troubleshooting describes techniques for troubleshooting common problems.

Special notices

There is an additional command available only on the FG-92D model:

```
config system global
   set hw-switch-ether-filter {enable | disable}
end
```

By default, the `hw-switch-ether-filter` command is enabled. When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed.
- BPDUs are dropped, and no STP loop results.
- PPPoE packets are dropped.
- IPv6 packets are dropped.
- FortiSwitch devices are not discovered.
- HA might fail to form depending on the network topology.

When the `hw-switch-ether-filter` command is disabled, all packet types are allowed, but, depending on the network topology, an STP loop might result.

To work around this issue:

1. Use either WAN1 or WAN2 as the HA heartbeat device.
2. Disable the `hw-switch-ether-filter` option.

Connecting FortiLink ports

This section contains information about the FortiSwitch and FortiGate ports that you connect to establish a FortiLink connection.

In FortiSwitchOS 3.3.0 and later releases, you can use any of the switch ports for FortiLink. Some or all of the switch ports (depending on the model) support auto-discovery of the FortiLink ports.

You can chose to connect a single FortiLink port or multiple FortiLink ports as a logical interface (link-aggregation group, hardware switch, or software switch).

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

1. Enable the switch controller on the FortiGate unit

Before connecting the FortiSwitch and FortiGate units, ensure that the switch controller feature is enabled on the FortiGate unit with the FortiGate GUI or CLI to enable the switch controller. Depending on the FortiGate model and software release, this feature might be enabled by default.

Using the FortiGate GUI

1. Go to *System* > *Feature Visibility*.
2. Turn on the *Switch Controller* feature, which is in the *Basic Features* list.
3. Select *Apply*.

The menu option *WiFi & Switch Controller* now appears.

Using the FortiGate CLI

Use the following commands to enable the switch controller:

```
config system global
   set switch-controller enable
end
```

2. Connect the FortiSwitch unit and FortiGate unit

FortiSwitchOS 3.3.0 and later provides flexibility for FortiLink:

- Use any switch port for FortiLink
- Provides auto-discovery of the FortiLink ports on the FortiSwitch
- Choice of a single FortiLink port or multiple FortiLink ports in a link-aggregation group (LAG)

Auto-discovery of the FortiSwitch ports

In FortiSwitchOS 3.3.0 and later releases, D-series FortiSwitch models support FortiLink auto-discovery, on automatic detection of the port connected to the FortiGate unit.

You can use any of the switch ports for FortiLink. Before connecting the switch to the FortiGate unit, use the following FortiSwitch CLI commands to configure a port for FortiLink auto-discovery:

```
config switch interface
   edit <port>
   set auto-discovery-fortilink enable
end
```

By default, each FortiSwitch model provides a set of ports that are enabled for FortiLink auto-discovery. If you connect the FortiLink using one of these ports, no switch configuration is required.

In FortiSwitchOS 3.4.0 and later releases, the last four ports are the default auto-discovery FortiLink ports. You can also run the `show switch interface` command on the FortiSwitch unit to see the ports that have auto-discovery enabled.

The following table lists the default auto-discovery ports for each switch model.

NOTE: Any port can be used for FortiLink if it is manually configured.

FortiSwitch Model	Default Auto-FortiLink ports
FS-108D-POE	port9–port10
FS-108E, FS-108E-POE, FS-108E-FPOE	port7–port10
FSR-112D-POE	port5–port12
FS-124D, FS-124D-POE	port23–port26
FSR-124D	port1-port4, port21–port28
FS-124E, FS-124E-POE, FS-124E-FPOE	port21–port28
FS-148E, FS-148E-POE	port21–port52
FS-224D-POE	port21–port24
FS-224D-FPOE	port21–port28
FS-224E, FS-224E-POE	port21–port28
FS-248D, FS-248D-FPOE	port45–port52
FS-248D-POE	port47–port50
FS-248E-POE, FS-248E-FPOE	port45–port52
FS-424D, FS-424D-POE, FS-424D-FPOE	port23–port26
FS-424E-Fiber	port1-port30
FS-426E-FPOE-MG	port23-port30
FS-448D, FS-448D-POE, FS-448D-FPOE	port45–port52
FS-524D, FS-524D-FPOE	port21–port30

FortiSwitch Model	Default Auto-FortiLink ports
FS-548D	port39–port54
FS-548D-FPOE, FS-548DN	port45–port54
FS-1024D	port1–port24
FS-1048D, FS-1048E	port1–port52
FS-3032D, FS-3032E	port1–port32

Choosing the FortiGate ports

The FortiGate unit manages all of the switches through one active FortiLink. The FortiLink can consist of one port or multiple ports (for a LAG).

As a general rule, FortiLink is supported on all ports that are not listed as HA ports.

Using the FortiGate GUI

This section describes how to configure a FortiLink between a FortiSwitch unit and a FortiGate unit.

You can configure FortiLink using the FortiGate GUI or CLI. Fortinet recommends using the GUI because the CLI procedures are more complex (and therefore more prone to error).

If you use one of the auto-discovery FortiSwitch ports, you can establish the FortiLink connection with no configuration steps on the FortiSwitch and with a few simple configuration steps on the FortiGate unit.

Summary of the procedure

1. On the FortiGate unit, configure the FortiLink interface.
2. Authorize the managed FortiSwitch unit manually if you did not select *Automatically authorize devices*.

Configure the FortiLink interface

To configure the FortiLink interface on the FortiGate unit:

1. Go to *WiFi & Switch Controller* > *FortiLink Interface*.
2. Enter a name for the interface (11 characters maximum).
3. Select + in the Interface members field and then select the ports to add to the FortiLink interface. You can create a LAG type or software/hardware switch type of FortiLink interface; these types are more scalable than a physical interface.
   NOTE: If you do not see any ports listed in the Select Entries pane, go to *Network* > *Interfaces*, right-click the FortiLink physical port, select *Edit*, delete the port from the Interface Members field, and then select *OK*.
4. Configure the *IP/Network Mask* for your network.
5. Select *Automatically authorize devices*.
6. Select *Apply*.

FortiLink split interface

You can use the FortiLink split interface to connect the FortiLink aggregate interface from one FortiGate unit to two FortiSwitch units. When the FortiLink split interface is enabled, only one link remains active.

The aggregate interface for this configuration must contain exactly two physical ports (one for each FortiSwitch unit).

The FortiLink split interface is enabled by default. You can configure this feature with the FortiGate GUI and CLI.

Using the FortiGate GUI:

1. Go to *WiFi & Switch Controller* > *FortiLink Interface*.
2. Move the *FortiLink split interface* slider

Using the FortiGate CLI:

```
config system interface
   edit <name of the FortiLink interface>
      set fortilink-split-interface {enable | disable}
end
```

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 *WiFi & Switch Controller* > *Managed FortiSwitch*.
2. Optionally, click on the FortiSwitch faceplate and click *Authorize*. This step is required only if you disabled the automatic authorization field of the interface.

Adding preauthorized FortiSwitch units

After you preauthorize a FortiSwitch unit, you can assign the FortiSwitch ports to a VLAN.

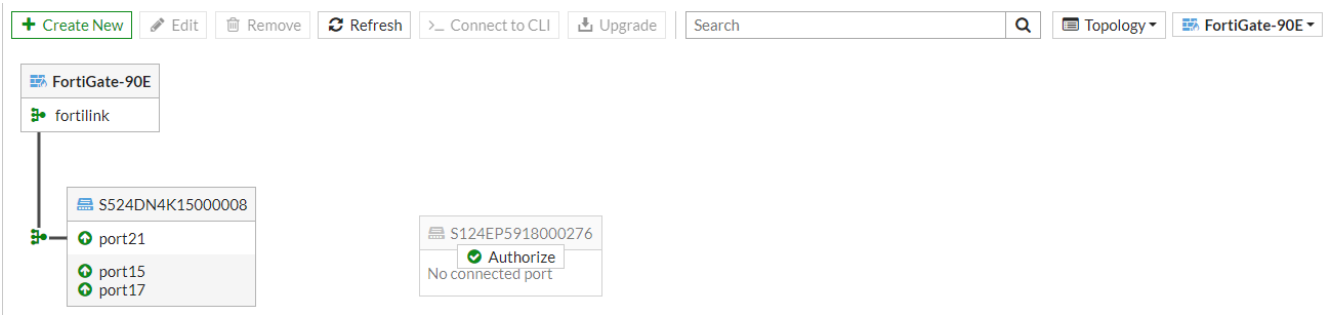
To preauthorize a FortiSwitch:

1. Go to *WiFi & Switch Controller* > *Managed FortiSwitch*.
2. Click *Create New*.
3. In the New Managed FortiSwitch page, enter the serial number, model name, and description of the FortiSwitch.
4. Move the *Authorized* slider to the right.
5. Select *OK*. The Managed FortiSwitch page lists the preauthorized switch.

Managed FortiSwitch display

Go to *WiFi & Switch Controller* > *Managed FortiSwitch* to see all of the switches being managed by your FortiGate. Select *Topology* from the drop-down menu in the upper right corner to see which devices are connected.

When the FortiLink is established successfully, the status is green (next to the FortiGate interface name and on the FortiSwitch faceplate), and the link between the ports is a solid line.



If the link has gone down for some reason, the line will be dashed, and a broken link icon will appear. 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 the FortiGate unit.

From the Managed FortiSwitch 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.

Edit a managed FortiSwitch unit

To edit a managed FortiSwitch unit:

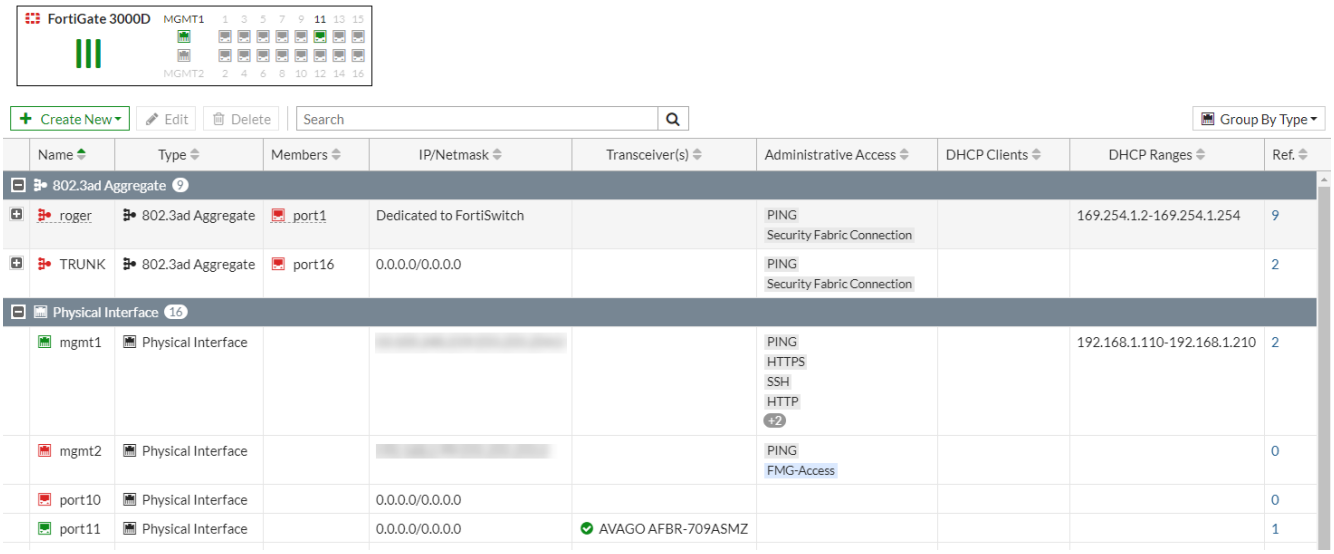
1. Go to *WiFi & Switch Controller* > *Managed FortiSwitch*.
2. Click on the FortiSwitch to and click *Edit*, right-click on a FortiSwitch unit and select *Edit*, or double-click on a FortiSwitch unit.

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.
- *Authorize* or deauthorize the FortiSwitch.
- *Update* the firmware running on the switch.
- Override 802.1x settings, including the reauthentication interval, maximum reauthentication attempts, and link-down action

Network interface display

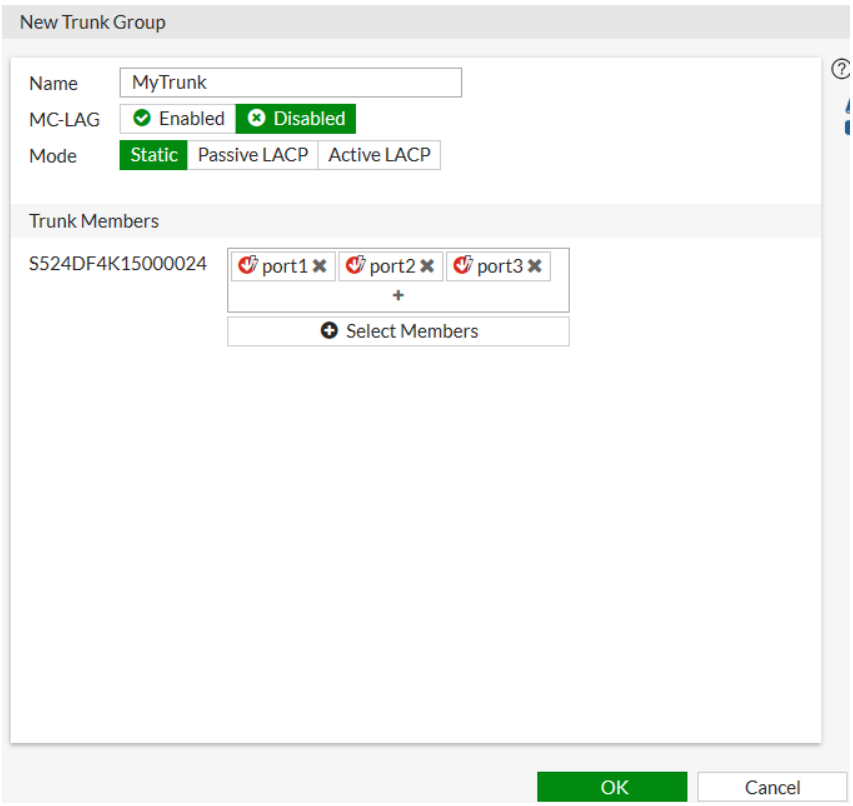
On the *Network* > *Interfaces* page, you can see the FortiGate interface connected to the FortiSwitch unit. The GUI indicates *Dedicated to FortiSwitch* in the IP/Netmask field.



Add link aggregation groups (trunks)

To create a link aggregation group for FortiSwitch user ports:

1. Go to *WiFi & Switch Controller* > *FortiSwitch Ports*.
2. Click *Create New* > *Trunk*.
3. In the New Trunk Group page, enter a *Name* for the trunk group.
4. Select two or more physical ports to add to the trunk group and then select *Apply*.
5. Select the *Mode*: Static, Passive LACP, or Active LACP.
6. Select *Enabled* or *Disabled* for the MC-LAG.
7. Select *OK*.



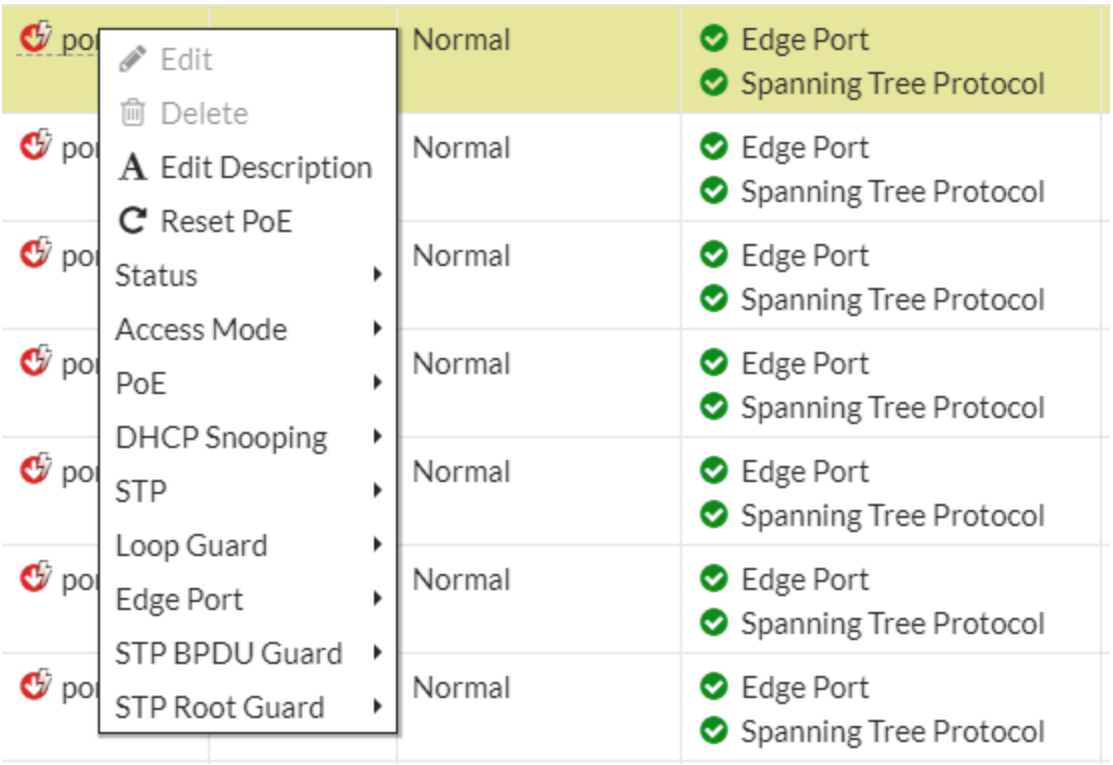
Configure DHCP blocking, STP, and loop guard on managed FortiSwitch ports

Go to *WiFi & 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.



Using the FortiGate CLI

This section describes how to configure FortiLink using the FortiGate CLI. Fortinet recommends using the FortiGate GUI because the CLI procedures are more complex (and therefore more prone to error).

If you use one of the auto-discovery FortiSwitch ports, you can establish the FortiLink connection (single port or LAG) with no configuration steps on the FortiSwitch and with a few simple configuration steps on the FortiGate unit.

You can also configure FortiLink mode over a layer-3 network.

Summary of the procedure

1. Configure FortiLink on a physical port or configure FortiLink on a logical interface.
2. Configure NTP.
3. Authorize the managed FortiSwitch unit.
4. Configure DHCP.

Configure FortiLink on a physical port

Configure FortiLink on any physical port on the FortiGate unit and authorize the FortiSwitch unit as a managed switch.

In the following steps, port 1 is configured as the FortiLink port.

1. If required, remove port 1 from the `lan` interface:

```
config system virtual-switch
   edit lan
      config port
         delete port1
      end
   end
end
```

2. Configure port 1 as the FortiLink interface:

```
config system interface
   edit port1
      set auto-auth-extension-device enable
      set fortilink enable
   end
end
```

3. Configure an NTP server on port 1:

```
config system ntp
   set server-mode enable
   set interface port1
end
```

4. Authorize the FortiSwitch unit as a managed switch:

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

5. The FortiSwitch unit will reboot when you issue the `set fsw-wan1-admin enable` command.

Configure FortiLink on a logical interface

You can configure FortiLink on a logical interface: link-aggregation group (LAG), hardware switch, or software switch.

LAG is supported on all FortiSwitch models and on FortiGate models FGT-100D and above. Hardware switch is supported on some FortiGate models.

Connect any of the FortiLink-capable ports on the FortiGate to the FortiSwitch unit. Ensure that you configure auto-discovery on the FortiSwitch ports (unless it is auto-discovery by default).

NOTE: Starting with FortiOS 6.2.2, you can use the default `fortilink` aggregate interface and then add ports. This configuration is available for all FortiGate E series models, 100 and higher. For FortiGate models lower than 100, you can use the default `fortilink` hardware switch or software switch interface and then add ports.

In the following procedure, port 4 and port 5 are configured as a FortiLink LAG.

1. If required, remove the FortiLink ports from the `lan` interface:

```
config system virtual-switch
   edit lan
      config port
         delete port4
         delete port5
      end
   end
end
```

2. Create a trunk with the two ports that you connected to the switch:

```
config system interface
   edit flink1 (enter a name, 11 characters maximum)
      set ip 169.254.3.1 255.255.255.0
      set allowaccess ping capwap https
      set vlanforward enable
      set type aggregate
      set member port4 port5
      set lacp-mode static
      set fortilink enable
      (optional) set fortilink-split-interface enable
   next
end
```

NOTE: If the members of the aggregate interface connect to more than one FortiSwitch, you must enable `fortilink-split-interface`.

3. Authorize the FortiSwitch unit as a managed switch:

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

NOTE: FortiSwitch will reboot when you issue the `set fsw-wan1-admin enable` command.

Enable multiple FortiLink interfaces

NOTE: Only the first FortiLink interface has GUI support.

Use the following command to enable or disable multiple FortiLink interfaces.

```
config switch-controller global
   set allow-multiple-interfaces {enable | disable}
end
```

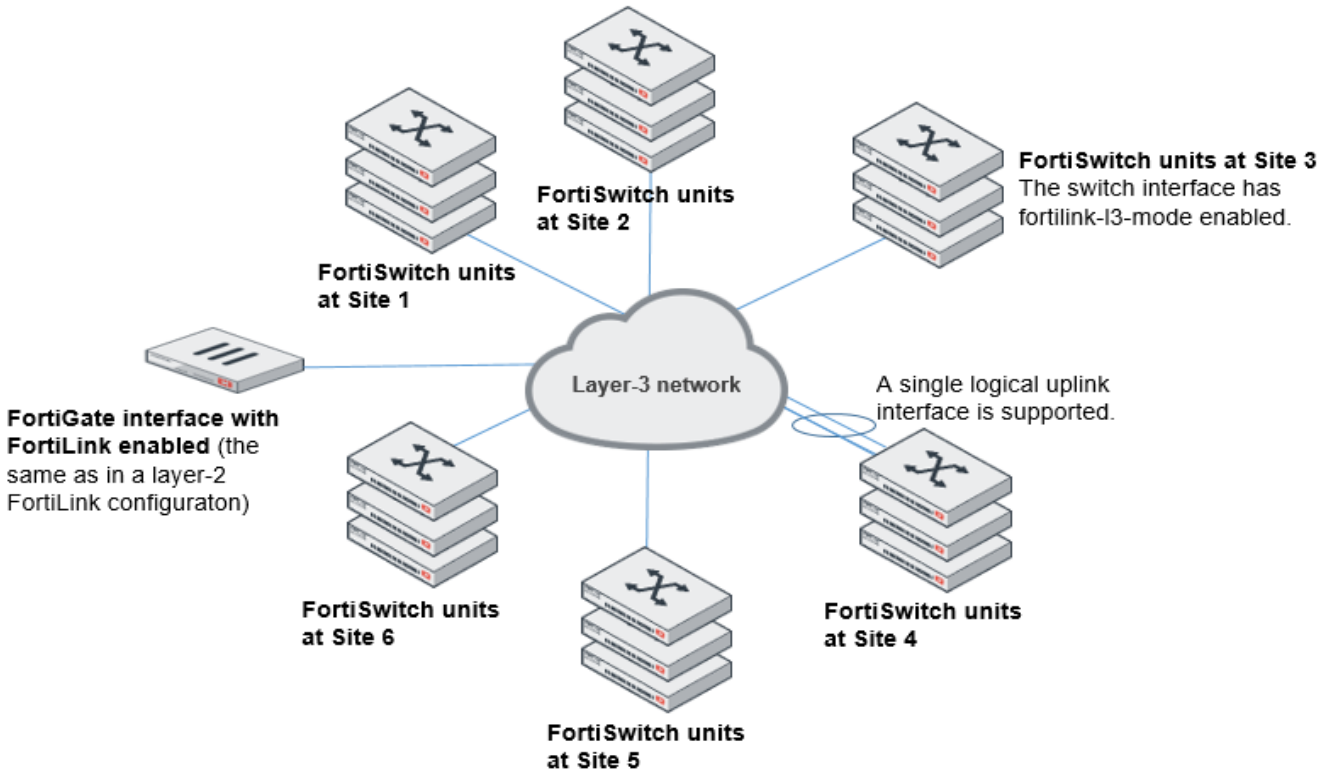
FortiLink mode over a layer-3 network

This feature allows FortiSwitch islands to operate in FortiLink mode over a layer-3 network, even though they are not directly connected to the switch-controller FortiGate unit. FortiSwitch islands contain one or more FortiSwitch units.

There are two main deployment scenarios for using FortiLink mode over a layer-3 network:

- In-band management, which uses the FortiSwitch unit's internal interface to connect to the layer-3 network
- Out-of-band management, which uses the FortiSwitch unit's mgmt interface to connect to the layer-3 network

In-band management



To configure a FortiSwitch unit to operate in a layer-3 network:

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:

```
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 FortiGate unit (switch controller) that manages this switch. The default `dhcp-option-code` is `138`.

   To use DHCP discovery:

```
config switch-controller global
   set ac-discovery-type dhcp
   set 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 with the following commands:

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

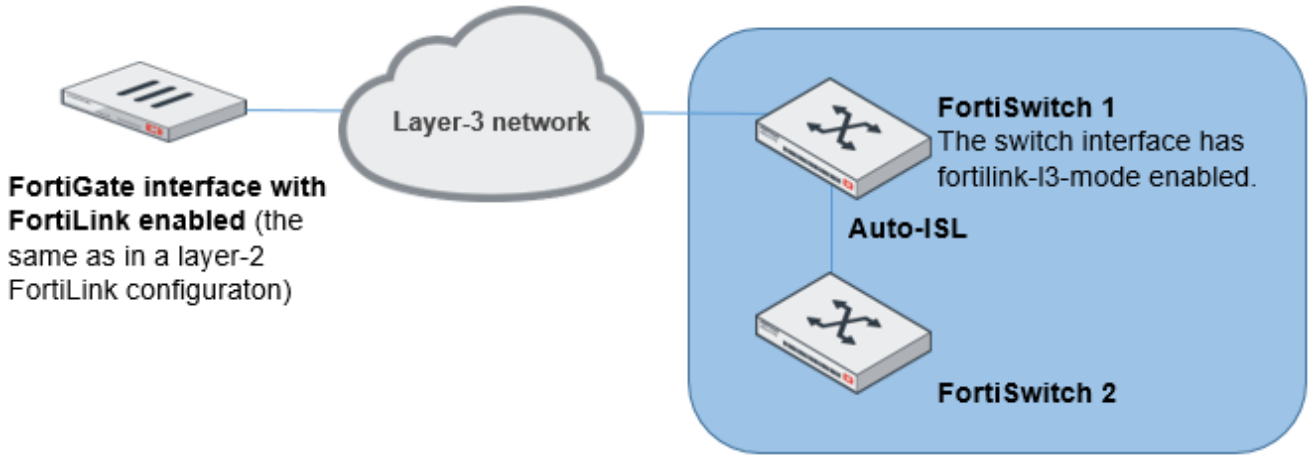
   The `fortilink-l3-mode` command is only visible after you configure DHCP or static discovery.

NOTE:

- Make certain that each FortiSwitch unit can successfully ping the FortiGate unit.
- The NTP server must be configured on the FortiSwitch unit either manually or provided by DHCP. The NTP server must be reachable from the FortiSwitch unit.
- If more than one port (switch interface) has `fortilink-l3-mode` enabled, the FortiSwitch unit automatically forms a link aggregation group (LAG) trunk that contains all `fortilink-l3-mode`-enabled ports as a single logical interface.
- If you have more than one port with `fortilink-l3-mode` enabled, all ports are automatically added to the __FoRtlLnk0L3__ trunk. Make certain that the layer-3 network is also configured as a LAG with a matching LACP mode.
- In addition to the two layer-3 discovery modes (DHCP and static), there is the default layer-2 discovery broadcast mode. The layer-3 discovery multicast mode is unsupported.

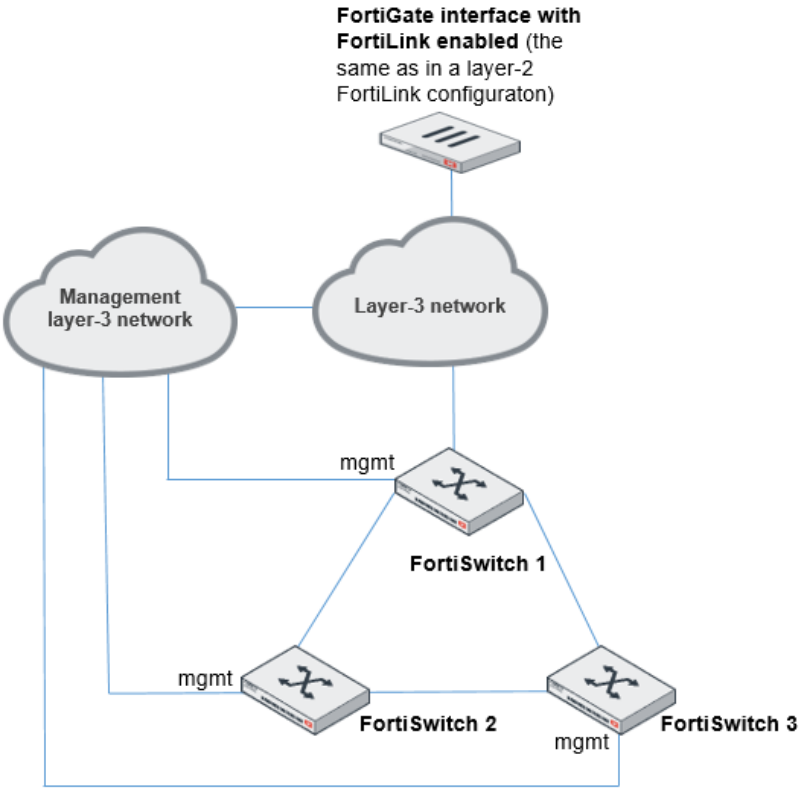
Connecting additional FortiSwitch units to the first FortiSwitch unit

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 the FortiGate unit.



Out-of-band management

If you use the mgmt port to connect to the layer-3 network, you do not need to enable `fortilink-l3-mode` on any physical port because the mgmt port is directly connected to the layer-3 network.



You can use the internal interface for one FortiSwitch island to connect to the layer-3 network and the mgmt interface for another FortiSwitch island to connect to the same layer-3 network. Do not mix the internal interface connection and mgmt interface connection within a single FortiSwitch island.

Other topologies

If you have a layer-2 loop topology, make certain that the alternative path can reach the FortiGate unit and that STP is enabled on the FortiLink layer-3 trunk.

If you have two FortiSwitch units separately connected to two different intermediary routers or switches, the uplink interfaces for both FortiSwitch units must have `fortilink-l3-mode` enabled. If the FortiSwitch units are also connected to each other, an auto-ISL forms automatically, and STP must be enabled to avoid loops.

A single logical interface (which can be a LAG) is supported when they use the internal interface as the FortiLink management interface.

You can use a LAG connected to a single intermediary router or switch. A topology with multiple ports connected to different intermediary routers or switches is not supported.

Limitations

The following limitations apply to FortiSwitch islands operating in FortiLink mode over a layer-3 network:

- All FortiSwitch units using this feature must be included in the FortiGate preconfigured switch table.
- No layer-2 data path component, such as VLANs, can span across layer 3 between the FortiGate unit and the FortiSwitch unit.
- All FortiSwitch units within an FortiSwitch island must be connected to the same FortiGate unit.
- The FortiSwitch unit needs a functioning layer-3 routing configuration to reach the FortiGate unit or any feature-configured destination, such as syslog or 802.1x.
- Do not connect a layer-2 FortiGate unit and a layer-3 FortiGate unit to the same FortiSwitch unit.
- If the FortiSwitch management port is used for a layer-3 connection to the FortiGate unit, the FortiSwitch island can contain only one FortiSwitch unit. All switch ports must remain in standalone mode. If you need more than one physical link, you can group the links as a link aggregation group (LAG).
- Do not connect a FortiSwitch unit to a layer-3 network and a layer-2 network on the same segment.
- If the network has a wide geographic distribution, some features, such as software downloads, might operate slowly.
- After a topology change, make certain that every FortiSwitch unit can reach the FortiGate unit.

MCLAG configuration for access ports

A multichassis LAG (MCLAG) provides node-level redundancy by grouping two FortiSwitch models together so that they appear as a single switch on the network. If either switch fails, the MCLAG continues to function without any interruption, increasing network resiliency and eliminating the delays associated with the Spanning Tree Protocol (STP). For the network topologies, see Dual-homed servers connected to a pair of FortiSwitch units using an MCLAG on page 42 and Standalone FortiGate unit with dual-homed FortiSwitch access on page 44.

MCLAG requirements

- Both peer switches should be of the same hardware model and same software version. Mismatched configurations might work but are unsupported.
- There is a maximum of two FortiSwitch models per MCLAG.
- The routing feature is not available within an MCLAG.
- When min_bundle or max_bundle is combined with MCLAG, the bundle limit properties are applied only to the local aggregate interface.
- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on *all* ICL trunks.

NOTE: If you are going to use IGMP snooping with an MCLAG topology:

- On the global switch level, `mclag-igmp-aware` must be enabled,
- The `igmps-flood-traffic` and `igmps-flood-report` settings must be *disabled* on the ISL and FortiLink trunks; but the `igmps-flood-traffic` and `igmps-flood-report` settings must be *enabled* on ICL trunks.
- IGMP proxy must be enabled.

Using the GUI

1. Go to *WiFi & Switch Controller* > *FortiSwitch Ports*.
2. Select *Create New* > *Trunk*.
3. Enter a name for the MCLAG trunk.
4. For the MC-LAG 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, select *Select Members*, select the ports to include in the MCLAG trunk, and then select *OK* to save the trunk members.
7. Select *OK* to save the MCLAG configuration.
   The ports are listed as part of the MCLAG trunk on the FortiSwitch Ports page.

After the FortiSwitch units are configured as MCLAG peer switches, any port that supports advanced features on the FortiSwitch can become a LAG port. When `mclag` is enabled and the LAG port names match, an MCLAG peer set is automatically formed. The member ports for each FortiSwitch in the MCLAG do not need to be identical to the member ports on the peer FortiSwitch.

If you disable the MCLAG ICL (with the `set mclag-icl disable` command), you need to enable the fortilink-split-interface.

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 "<switch-id>"
      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

Log into each managed FortiSwitch to check the MCLAG configuration with the following command:

```
diagnose switch mclag
```

When an MCLAG is formed, the time on all FortiSwitch units is synchronized with an NTP server. To confirm that each FortiSwitch in the MCLAG is using an NTP server, use the following command:

```
show system ntp
```

Network topologies

The FortiGate unit requires only one active FortiLink to manage all of the subtending FortiSwitch units (called *stacking*).

You can configure the FortiLink as a physical interface or as a logical interface (associated with one or more physical interfaces). Depending on the network topology, you can also configure a standby FortiLink.

NOTE: For any of the topologies:

- All of the managed FortiSwitch units will function as one Layer-2 stack where the FortiGate unit manages each FortiSwitch separately.
- The active FortiLink carries data as well as management traffic.

Supported topologies

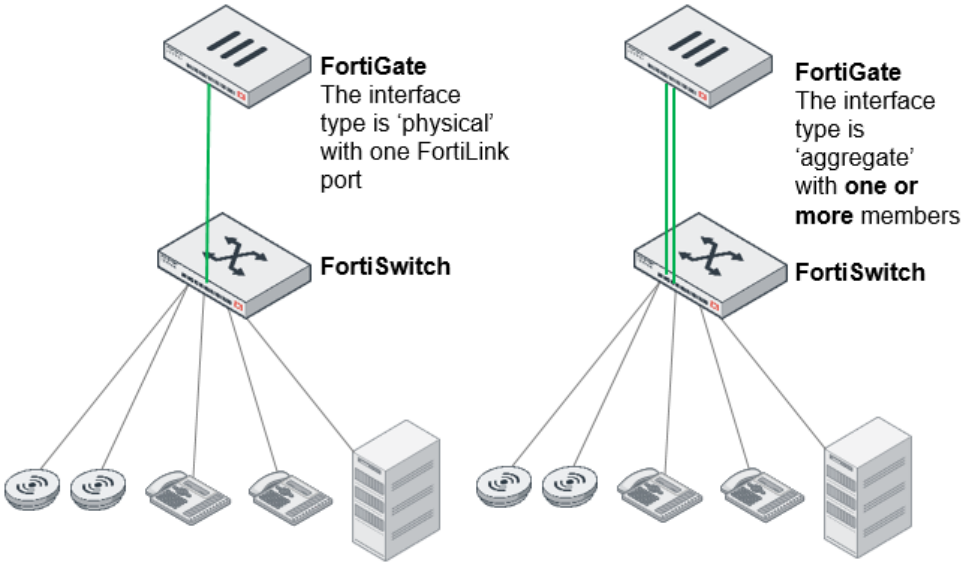
Fortinet recommends the following topologies for managed FortiSwitch units:

Single FortiGate managing a single FortiSwitch unit

On the FortiGate unit, the FortiLink interface is configured as a physical or aggregate interface. The 802.3ad aggregate interface type provides a logical grouping of one or more physical interfaces.

NOTE:

- For the aggregate interface, you must disable the split interface on the FortiGate unit.
- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface, the `lacp-mode` of the FortiLink aggregate interface must be set to `static`. Unless MCLAG is enabled and you are using 6.2.0 or later, see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 64 for details.
- Do not create loops or rings with the FortiSwitch units because the FortiGate unit does not use the STP.



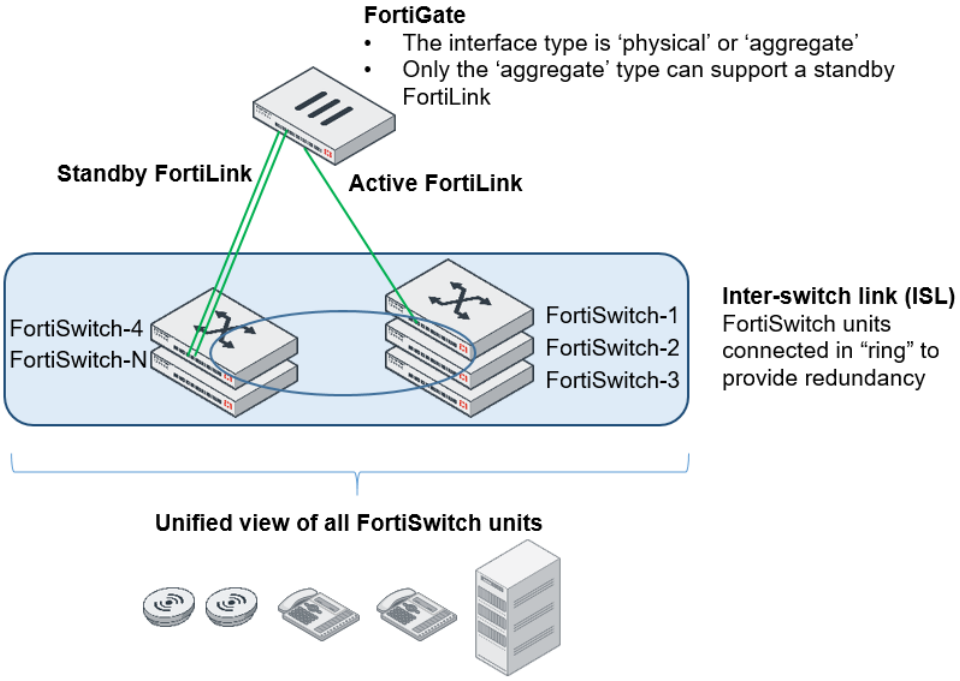
Single FortiGate unit managing a stack of several FortiSwitch units

The FortiGate unit connects directly to one FortiSwitch unit using a physical or aggregate interface. The remaining FortiSwitch units connect in a ring using inter-switch links (that is, ISL).

Optionally, you can connect a standby FortiLink connection to the last FortiSwitch unit. For this configuration, you create a FortiLink Split-Interface (an aggregate interface that contains one active link and one standby link).

NOTE:

- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface, the `lacp-mode` of the FortiLink aggregate interface must be set to `static`. Unless MCLAG is enabled and you are using 6.2.0 or later, see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 64 for details.
- External devices shown in the following topology must be compliant endpoints, such as computers. They cannot be third-party switches or appliances.
- Do not create loops or rings with the FortiGate unit in the path.

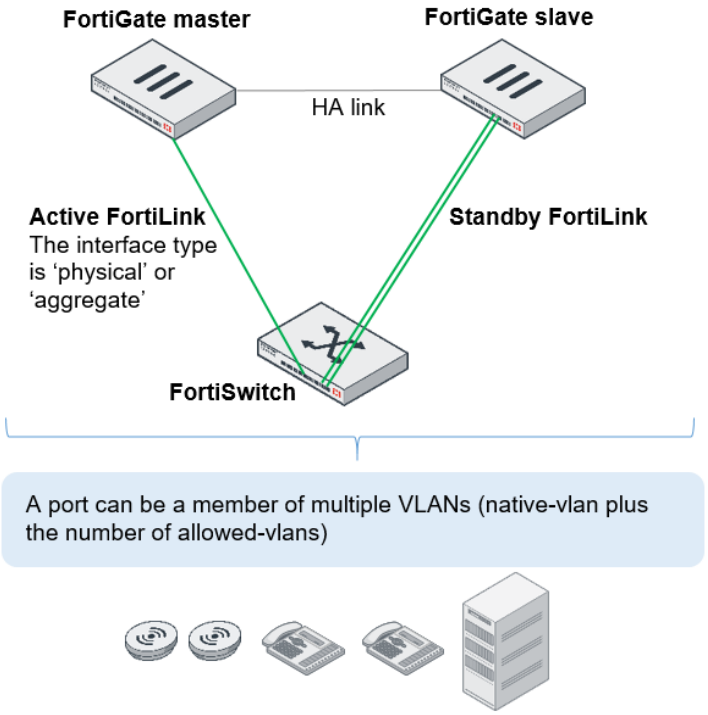


The devices on the FortiLink setup can include access points, servers, PCs, IP-phones, and IP cameras (any IP devices)

HA-mode FortiGate units managing a single FortiSwitch unit

The master and slave FortiGate units both connect a FortiLink to the FortiSwitch unit. The FortiLink port(s) and interface type must match on the two FortiGate units.

NOTE: Before FortiOS 6.2.0, when using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive. Starting in FortiOS 6.2.0, the FortiGate HA mode can be either active-passive or active-active.



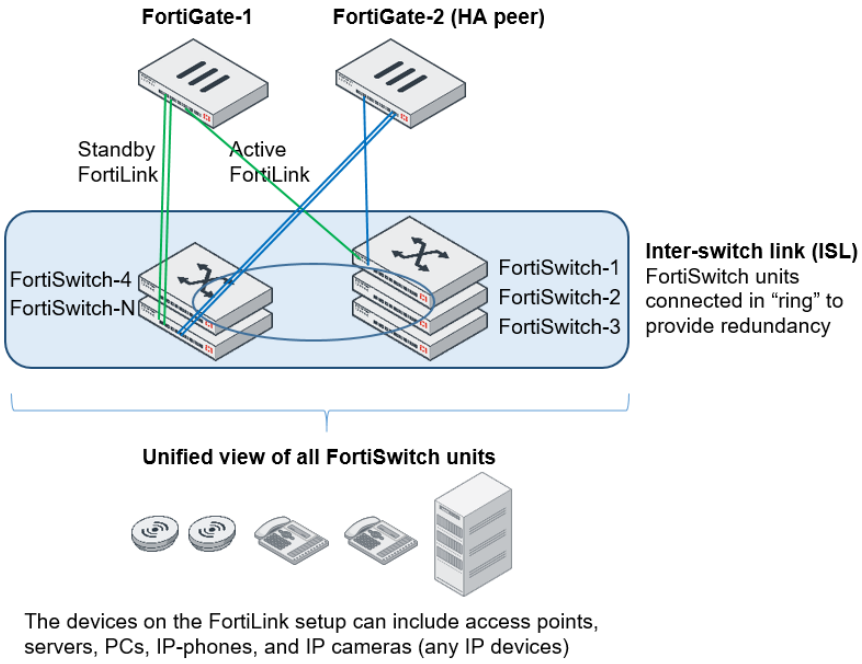
HA-mode FortiGate units managing a stack of several FortiSwitch units

The master and slave FortiGate units both connect a FortiLink to the first FortiSwitch unit and (optionally) to the last FortiSwitch unit. The FortiLink ports and interface type must match on the two FortiGate units.

When using an aggregate interface for the active/standby FortiLink configuration, make sure the FortiLink split interface is enabled (this forces one link to be active and the rest to be standby links, which avoids loops in the network). This option can be disabled later if you enable an MCLAG. See Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 64.

NOTE:

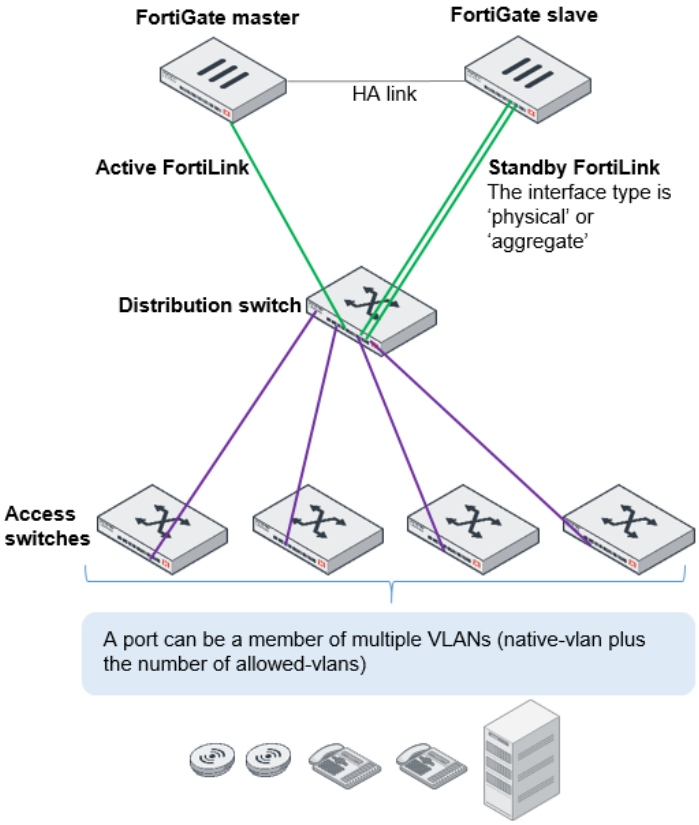
- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface, the `lacp-mode` of the FortiLink aggregate interface must be set to `static`. Unless MCLAG is enabled and you are using 6.2.0 or later, see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 64 for details.
- Before FortiOS 6.2.0, when using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive. Starting in FortiOS 6.2.0, the FortiGate HA mode can be either active-passive or active-active.



HA-mode FortiGate units managing a FortiSwitch two-tier topology

The distribution FortiSwitch unit connects to the master and slave FortiGate units. The FortiLink port(s) and interface type must match on the two FortiGate units.

NOTE: Before FortiOS 6.2.0, when using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive. Starting in FortiOS 6.2.0, the FortiGate HA mode can be either active-passive or active-active.



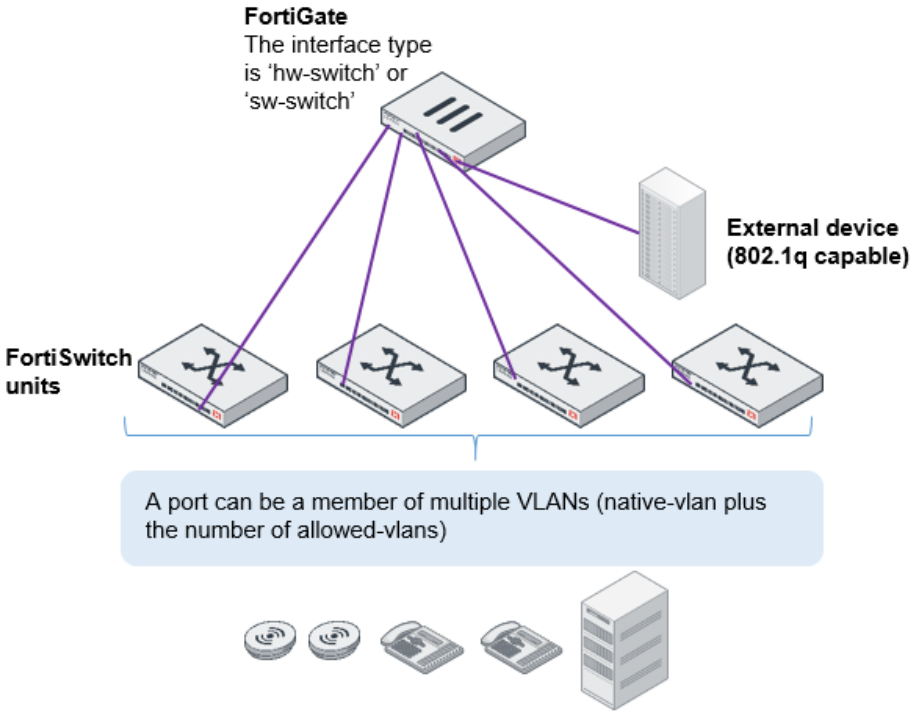
Single FortiGate unit managing multiple FortiSwitch units (using a hardware or software switch interface)

The FortiGate unit connects directly to each FortiSwitch unit. Each of these FortiLink ports is added to the logical hardware-switch or software-switch interface on the FortiGate unit.

Optionally, you can connect other devices to the FortiGate logical interface. These devices, which must support IEEE 802.1q VLAN tagging, will have Layer 2 connectivity with the FortiSwitch ports.

NOTE:

- Using the hardware or software switch interface in FortiLink mode is not recommended in most cases. It can be used when the traffic on the ports is very light because all traffic across the switches moves through the FortiGate unit.
- Do not create loops or rings in this topology.



HA-mode one-tier MCLAG

HA-mode FortiGate units connect to redundant distribution FortiSwitch units. Access FortiSwitch units are arranged in a stack in each IDF, connected to both distribution switches.

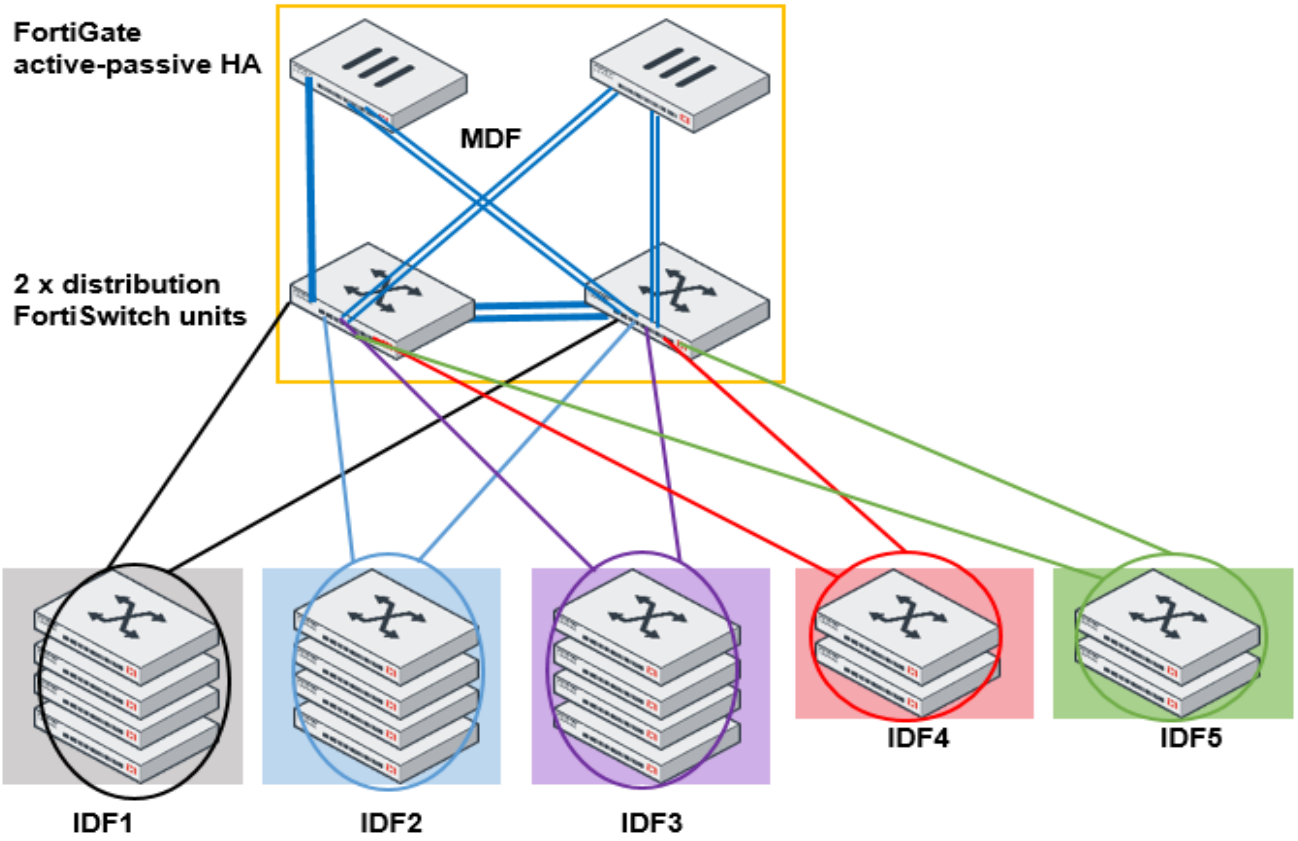
For the FortiLink connection to each distribution switch, you create a FortiLink split interface (an aggregate interface that contains one active link and one standby link).

NOTE:

- Before FortiSwitchOS 3.6.4, MCLAG was not supported when access rings were present. Starting with FortiSwitchOS 3.6.4, MCLAG is supported, even with access rings present.
- Before FortiOS 6.2.0, when using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive. Starting in FortiOS 6.2.0, the FortiGate HA mode can be either active-passive or active-active.
- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface, the `lacp-mode` of the FortiLink aggregate interface must be set to `static`. Unless MCLAG is enabled and you are using 6.2.0 or later, see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 64 for details.
- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks.
- This is only an example topology. Other combinations of FortiGate units and FortiSwitch units can be used to create a similar topology.

NOTE: If you are going to use IGMP snooping with an MCLAG topology:

- On the global switch level, `mclag-igmp-aware` must be enabled,
- The `igmps-flood-traffic` and `igmps-flood-report` settings must be *disabled* on the ISL and FortiLink trunks; but the `igmps-flood-traffic` and `igmps-flood-report` settings must be *enabled* on ICL trunks.
- IGMP proxy must be enabled.


FortiGate
active-passive HA
MDF
2 x distribution
FortiSwitch units
IDF1
IDF2
IDF3
IDF4
IDF5

Dual-homed servers connected to a pair of FortiSwitch units using an MCLAG

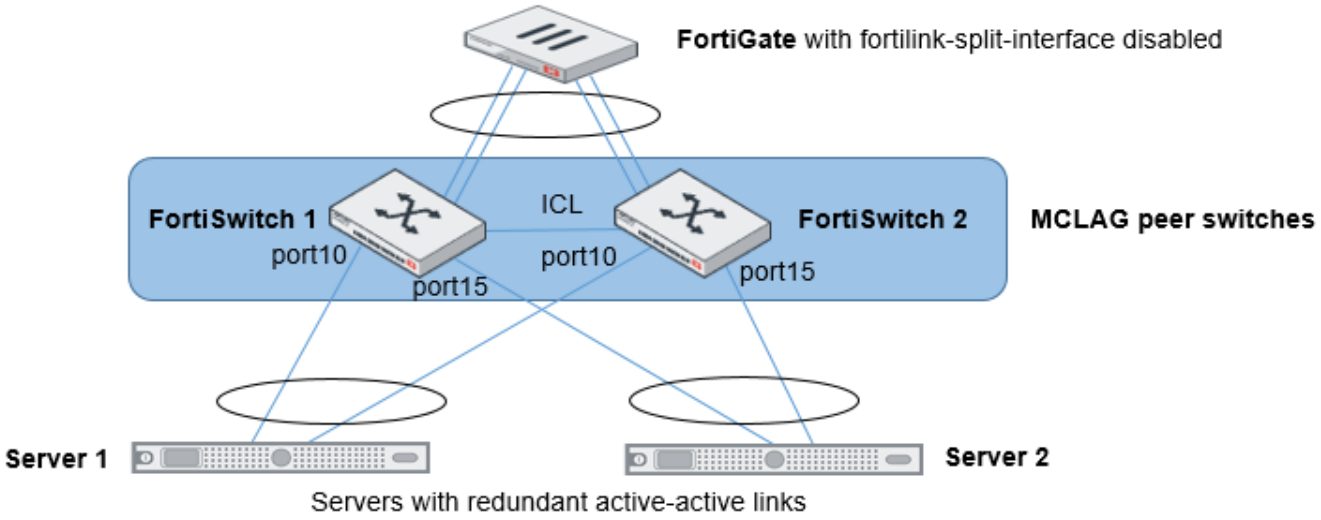
To configure a multichassis LAG, you need to configure FortiSwitch 1 and FortiSwitch 2 as MCLAG peer switches before creating a two-port LAG. Use the `set mclag-icl enable` command to create an inter-chassis link (ICL) on each FortiSwitch unit (see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 64). Then you set up two MCLAGs towards the servers, each MCLAG using one port from each FortiSwitch unit.

This topology is supported when the FortiGate unit is in HA mode.

NOTE: On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks.

NOTE: If you are going to use IGMP snooping with an MCLAG topology:

- On the global switch level, `mclag-igmp-aware` must be enabled,
- The `igmps-flood-traffic` and `igmps-flood-report` settings must be *disabled* on the ISL and FortiLink trunks; but the `igmps-flood-traffic` and `igmps-flood-report` settings must be *enabled* on ICL trunks.
- IGMP proxy must be enabled.



Step 1: Ensure the MCLAG ICL is already configured between FortiSwitch 1 and FortiSwitch 2.

```
diagnose switch mclag icl
```

Step 2: Configure a trunk in FortiSwitch 1 and then configure a trunk in FortiSwitch 2.

The trunk names must match.

Step 3: Set up the servers.

To set up Server 1:

```
config switch trunk
   edit server_1
```

```
      set members port10
      set mclag enable
   next
   edit server_2
      set members port15
      set mclag enable
   next
end
```

To set up Server 2:

```
config switch trunk
   edit server_1
      set members port10
      set mclag enable
   next
   edit server_2
      set members port15
      set mclag enable
   next
end
```

If you disable the MCLAG ICL (with the `set mclag-icl disable` command), you need to enable the fortilink-split-interface.

Standalone FortiGate unit with dual-homed FortiSwitch access

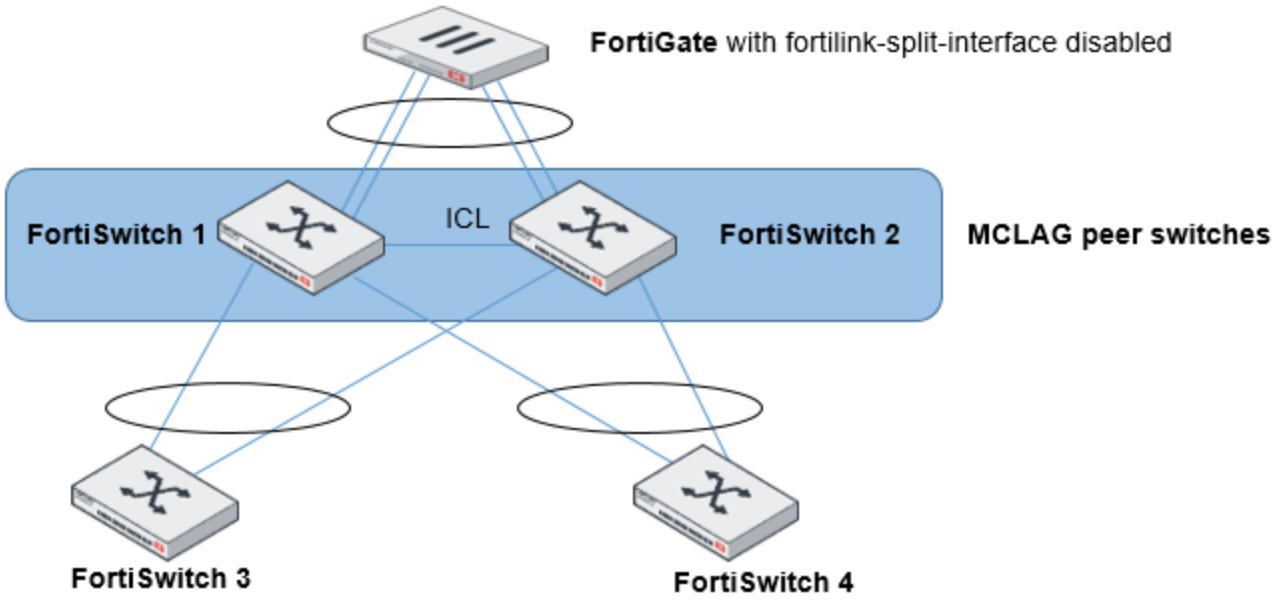
This network topology provides high port density with two tiers of FortiSwitch units.

Use the `set mclag-icl enable` command to create an ICL on each FortiSwitch unit (see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 64).

NOTE: On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks.

NOTE: If you are going to use IGMP snooping with an MCLAG topology:

- On the global switch level, `mclag-igmp-aware` must be enabled,
- The `igmps-flood-traffic` and `igmps-flood-report` settings must be *disabled* on the ISL and FortiLink trunks; but the `igmps-flood-traffic` and `igmps-flood-report` settings must be *enabled* on ICL trunks.
- IGMP proxy must be enabled.



HA-mode FortiGate units with dual-homed FortiSwitch access

In HA mode, only one FortiGate is active at a time. If the active FortiGate unit fails, the backup FortiGate unit becomes active.

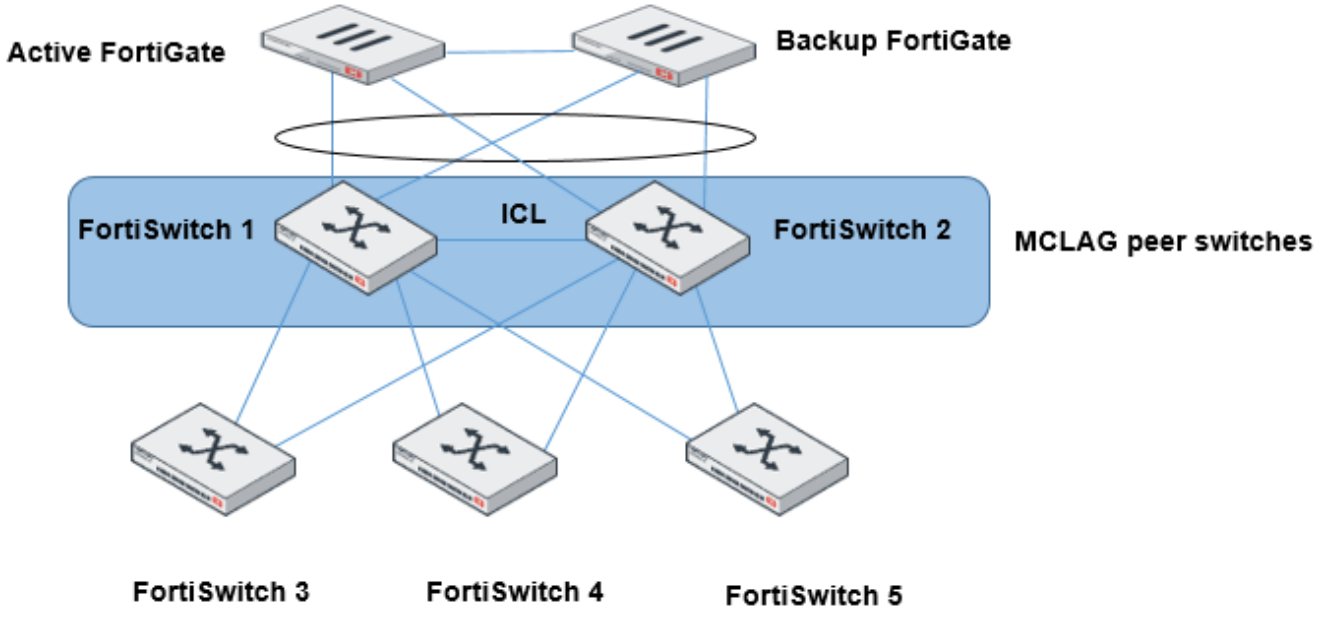
Use the `set mclag-icl enable` command to create an ICL on each FortiSwitch unit (see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 64).

NOTE:

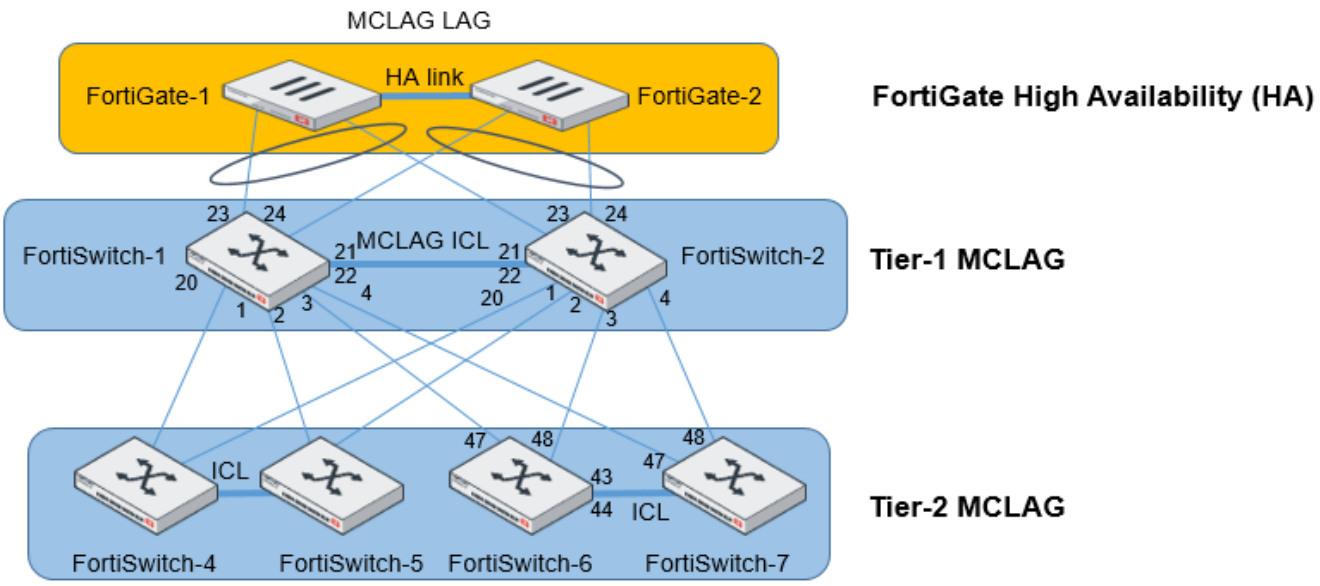
- Before FortiOS 6.2.0, when using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive. Starting in FortiOS 6.2.0, the FortiGate HA mode can be either active-passive or active-active.
- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks.

NOTE: If you are going to use IGMP snooping with an MCLAG topology:

- On the global switch level, `mclag-igmp-aware` must be enabled,
- The `igmps-flood-traffic` and `igmps-flood-report` settings must be *disabled* on the ISL and FortiLink trunks; but the `igmps-flood-traffic` and `igmps-flood-report` settings must be *enabled* on ICL trunks.
- IGMP proxy must be enabled.



Multi-tiered MCLAG with HA-mode FortiGate units



NOTE:

- Before FortiOS 6.2.0, when using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive. Starting in FortiOS 6.2.0, the FortiGate HA mode can be either active-passive or active-active.
- In this topology, you must use the `auto-isl-port-group` setting as described in the following configuration example. This setting instructs the switches to group ports from MCLAG peers together into one MCLAG when the inter-switch link (ISL) is formed.
- The inter-chassis link (ICL) and `auto-isl-port-group` settings must be done directly on the FortiSwitch unit.
- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks.
- CLI commands in red are manually configured.

NOTE: If you are going to use IGMP snooping with an MCLAG topology:

- On the global switch level, `mclag-igmp-aware` must be enabled,
- The `igmps-flood-traffic` and `igmps-flood-report` settings must be *disabled* on the ISL and FortiLink trunks; but the `igmps-flood-traffic` and `igmps-flood-report` settings must be *enabled* on ICL trunks.
- IGMP proxy must be enabled.

To configure a multi-tiered MCLAG with HA-mode FortiGate units:

1. Configure FortiSwitch-1 and FortiSwitch-2 for the tier-1 MCLAG:
   For FortiSwitch-1, enable the ICL on the ISL formed with the MCLAG peer switch:

```
config switch trunk
   edit "D243Z14000288-0" // trunk name derived from FortiSwitch-2 SN
      set mode lacp-active
      set auto-isl 1
      set mclag-icl enable
      set members "port21" "port22"
   end
```

   For FortiSwitch-2, enable the ICL on the ISL formed with the MCLAG peer switch:

```
config switch trunk
```

```
edit "D243Z14000289-0" // trunk name derived from FortiSwitch-1 SN
   set mode lacp-active
   set auto-isl 1
   set mclag-icl enable
   set members "port21" "port22"
end
```

2. Continue to configure FortiSwitch-1 for the tier-1 MCLAG:
   a. Configure the two `auto-isl-port-group`s based on the topology diagram. The group name must match the name that is configured on the peer switch.

```
config switch auto-isl-port-group
   edit "distribute-1"
      set members "port1" "port2"
   next
   edit "distribute-2"
      set members "port3" "port4"
   end
```

   b. After you complete the CLI commands in Steps 1 and 2a, the trunks are automatically formed:

```
config switch trunk
   edit "D243Z14000288-0"
      set mode lacp-active
      set auto-isl 1
      set mclag-icl enable
      set members "port21" "port22"
   next
   edit "FG100D3G15817028" // trunk name derived from FortiGate-1
      set mclag enable
      set members "port24" "port23"
   next
   edit "distribute-1"
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port1" "port2"
   next
   edit "distribute-2"
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port3" "port4"
   next
end
```

3. Continue to configure FortiSwitch-2 for the tier-1 MCLAG:
   a. Configure the two `auto-isl-port-group`s based on the topology diagram. The group name must match the name that is configured on the peer switch.

```
config switch auto-isl-port-group
   edit "distribute-1"
      set members "port1" "port2"
   next
   edit "distribute-2"
      set members "port3" "port4"
   end
```

   b. After you complete the CLI commands in Steps 1 and 3a, the trunks are automatically formed:

```
config switch trunk
   edit "D243Z14000288-0"
```

```
      set mode lacp-active
      set auto-isl 1
      set mclag-icl enable
      set members "port21" "port22"
   next
   edit "FG100D3G15817032" // trunk name derived from FortiGate-2
      set mclag enable
      set members "port24" "port23"
   next
   edit "distribute-1"
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port1" "port2"
   next
   edit "distribute-2"
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port3" "port4"
   next
end
```

4. Tier-2 MCLAGs. Enable the ICL between the MCLAG peer switches. For example, configure FortiSwitch-6 as follows.
   a. Change the tier-2 MCLAG peer switches to FortiLink mode and connect them to each other. Enable the ICL on the ISL formed with the MCLAG peer switches.

```
config switch trunk
   edit "8DN3X15000026-0" // trunk name derived from FortiSwitch-7 SN
      set mode lacp-active
      set auto-isl 1
      set mclag-icl enable
      set members "port43" "port44"
   end
```

   b. The trunks are automatically formed as below:

```
config switch trunk
   edit "8DN3X15000026-0"
      set mode lacp-active
      set auto-isl 1
      set mclag-icl enable
      set members "port43" "port44"
   next
   edit "_FlInK1_MLAG0_"
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port48" "port47"
   next
end
```

5. Access FortiSwitch units. The access switch trunks are formed automatically as below.

   On FortiSwitch-6:

```
config switch trunk
   edit "_FlInK1_MLAG0_"
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port48" "port47"
   next
end
```

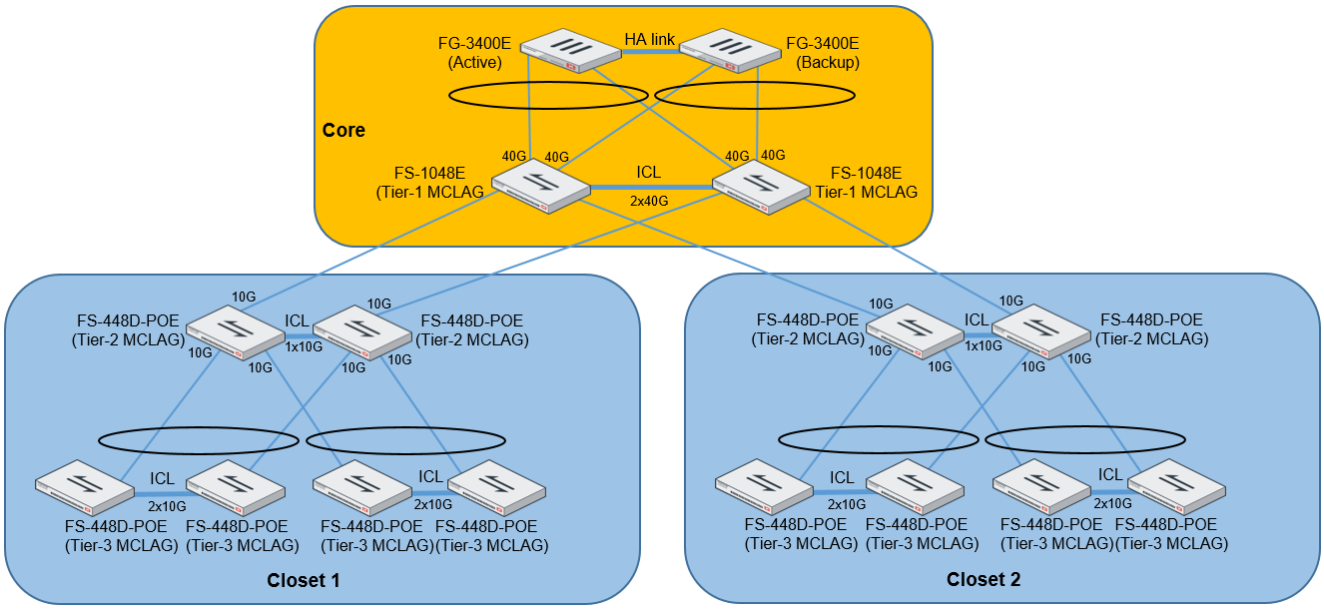
   On FortiSwitch-7:

```
config switch trunk
   edit "_FlInK1_MLAG0_"
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port47" "port48"
   next
end
```

If you disable the MCLAG ICL (with the `set mclag-icl disable` command), you need to enable the fortilink-split-interface.

Three-tier FortiLink MCLAG configuration

To create a three-tier FortiLink MCLAG topology, use FortiOS 6.2.3 GA or later and FortiSwitchOS 6.2.3 GA or later.



To configure the two FortiGate units:

1. Set up an active-passive HA configuration.
2. (Optional) Disable `override` in the HA CLI configuration.
3. Use the GUI or CLI to create the FortiLink interface.
4. Configure the FortiLink interface:

```
config system interface
   edit <FortiLink_interface>
      set lacp-mode active
      set fortilink-neighbor-detect lldp
      set fortilink-split-interface disable
      set lldp-reception enable
      set lldp-transmission enable
   next
end
```

5. Change the default `auto-config` policy:

```
config switch-controller auto-config policy
   edit default
      set poe-status disable
   next
end
```

6. Change the firmware upgrade mode:

```
config switch-controller global
   set https-image-push enable
end
```

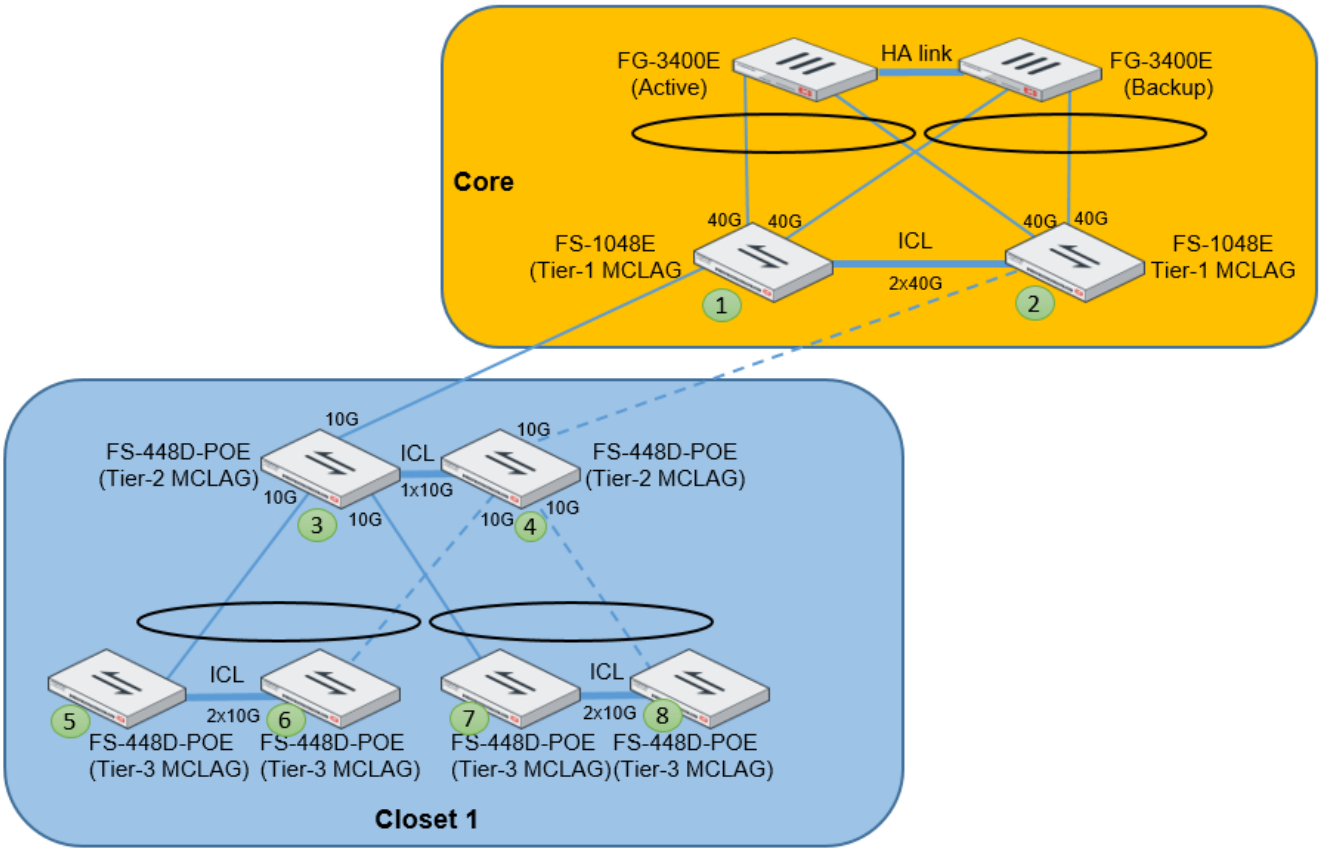
To configure the FortiSwitch units in the core:

1. Find the trunk between the two MCLAG switches. Enable `mclag-icl` on the MCLAG-ICL trunk. The default name of the MCLAG-ICL trunk is the last 13 characters of the peer switch name plus “-0”.

```
config switch trunk
   edit <MCLAG-ICL_trunk_name>
      set mclag-icl enable
   next
end
```

2. Create downlink trunks on the MCLAG-ICL switches.
   Note: Only the trunks from the higher tier MCLAG-ICL switches to the next tier MCLAG-ICL switches need this configuration.

To configure the three-tier MCLAG topology shown in the following figure:



1. Configure the tier-1 MCLAG switches.
   a. Connect switch 1 and switch 2 to the FortiGate units and interconnect switch 1 and switch 2.
   b. Wait for both switches to change to FortiLink mode and for both FortiLinks to be up.
   c. Configure the ICL trunks on the inter-switch trunks to form MCLAG switches in FortiLink mode.
   d. Use the `diagnose switch mclag peer-consistency-check` CLI command to verify that the MCLAG-ICL trunk formed successfully.
   e. Add an `auto-isl-port-group` for the tier-2 MCLAG switches on both switch 1 and switch 2:

```
config switch auto-isl-port-group
   edit tier2-closet-1
      set members port1
   next
   edit tier2-closet-2
      set members port2
   next
end
```

2. Wire all switches in closet 1 by following the figure. Do not make the dotted-line connections for now. Wait for all switches to be up in FortiLink mode.
3. Add two `auto-isl-port-group`s for the tier-3 MCLAG switches on both switch 3 and switch 4:

```
config switch auto-isl-port-group
   edit tier-2-closet-<1>-downlink-trunk-A
      set member <port_name>
   next
   edit tier-2-closet-<1>-downlink-trunk-B
      set member <port_name>
   next
end
```

4. Enable the tier-2 MCLAG-ICL trunk on switch 4 using the FortiOS CLI of the switch console port.
5. Enable the tier-3 MCLAG-ICL trunks on switch 6 and switch 8.
   NOTE: The trunk must be configured from the end of the daisy-chain switch.
6. Enable the tier-3 MCLAG-ICL trunks on switch 5 and switch 7.
7. Enable the tier-2 MCLAG-ICL trunk on switch 3.
8. Verify that all the FortiLinks are up and double-check that the MCLAG-ICL configuration on each MCLAG switch.
9. Connect switch 4 to switch 2.
10. Verify that the FortiLinks are up.
11. Connect switch 6 and switch 8 to switch 4.
12. Verify that the FortiLinks are up.
13. Use the `diagnose switch mclag peer` CLI command to verify that the tier-1, tier-2, and tier-3 MCLAG-switches are formed correctly.
14. Check the traffic on switch 1 and switch 2 during the configuration.
15. Repeat steps 2 to 14 for closet 2.
16. All FortiLinks should be up.

HA-mode FortiGate units using hardware-switch interfaces and STP

In most FortiLink topologies, MCLAG or LAG configurations are used for FortiSwitch redundancy. However, some FortiGate models (such as the FG-60E model) do not support the FortiLink aggregate interface.

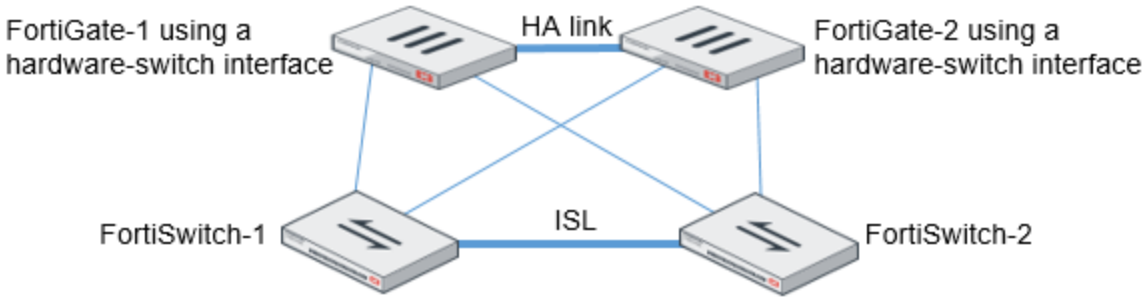
The following network topology uses a hardware-switch interface on each FortiGate unit. Each FortiSwitch unit is connected to a single port of the hardware-switch interface of the FortiGate unit. The inter-switch link (ISL) between the FortiSwitch units provides redundancy.

For this network topology to function, use the following commands on each FortiLink hardware-switch interface:

```
config system interface
   edit <FortiLink_hardware_switch_interface>
      set stp enable
   end
```

NOTE:

- The FortiLink interface uses the Link Layer Discovery Protocol (LLDP) for neighbor detection.
- Spanning Tree Protocol (STP) and STP forwarding are both supported by the FortiLink hardware-switch interface.
- The software-switch interface is not supported.



FortiLink with an HA cluster of four FortiGate units

A FortiGate HA cluster consists of two to four FortiGate units configured for HA operation. Each FortiGate in a cluster is called a cluster unit. All cluster units must be the same FortiGate model with the same FortiOS firmware build installed. All cluster units must also have the same hardware configuration (for example, the same number of hard disk) and be running in the same operating mode (NAT mode or transparent mode).

In addition, the cluster units must be able to communicate with each other through their heartbeat interfaces. This heartbeat communication is required for the cluster to be created and to continue operating. Without it, the cluster acts like a collection of standalone FortiGate units.

On startup, after configuring the cluster units with the same HA configuration and connecting their heartbeat interfaces, the cluster units use the FortiGate Clustering Protocol (FGCP) to find other FortiGate units configured for HA operation and to negotiate to create a cluster. During cluster operation, the FGCP shares communication and synchronization information among the cluster units over the heartbeat interface link. This communication and synchronization is called the FGCP heartbeat or the HA heartbeat. Often, this is shortened to just heartbeat.

NOTE: You can create an FGCP cluster of up to four FortiGate units.

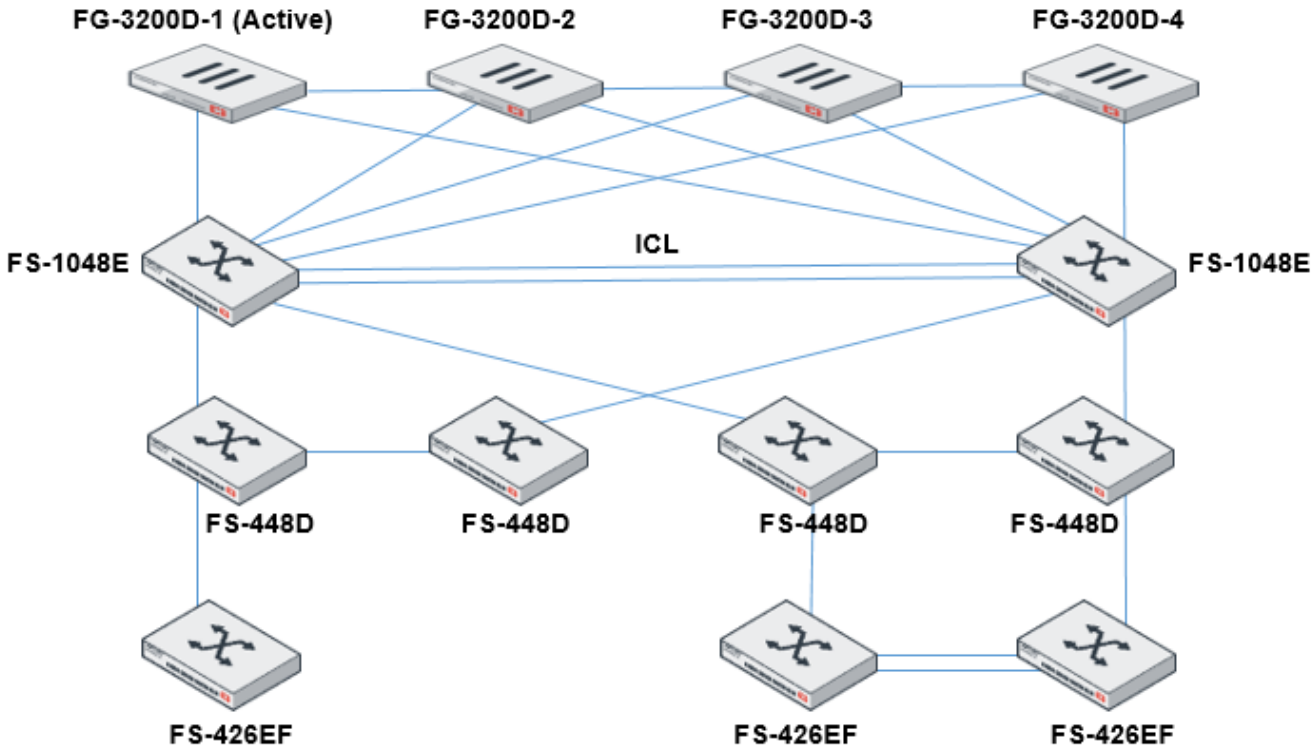
The cluster uses the FGCP to select the primary unit, and to provide device, link, and session failover. The FGCP also manages the two HA modes; active-passive (failover HA) and active-active (load-balancing HA).

The FGCP supports a cluster of two, three, or four FortiGate units. You can add more than two units to a cluster to improve reliability: if two cluster units fail the third will continue to operate and so on. A cluster of three or four units in active-active mode may improve performance because another cluster unit is available for security profile processing. However, active-active FGCP HA results in diminishing performance returns as you add units to the cluster, so the additional performance achieved by adding the third cluster unit might not be worth the cost.

There are no special requirements for clusters of more than two units. Here are a few recommendations though:

- The matching heartbeat interfaces of all of the cluster units must be able to communicate with each other. So each unit's matching heartbeat interface should be connected to the same switch. If the ha1 interface is used for heartbeat communication, the ha1 interfaces of all of the units in the cluster must be connected together so communication can happen between all of the cluster units over the ha1 interface.
- Redundant heartbeat interfaces are recommended. You can reduce the number of points of failure by connecting each matching set of heartbeat interfaces to a different switch. This is not a requirement; however, and you can connect both heartbeat interfaces of all cluster units to the same switch. However, if that switch fails the cluster will stop forwarding traffic.
- For any cluster, a dedicated switch for each heartbeat interface is recommended because of the large volume of heartbeat traffic and to keep heartbeat traffic off of other networks, but it is not required.
- Full mesh HA can scale to three or four FortiGate units. Full mesh HA is not required if you have more than two units in a cluster.
- Virtual clustering can only be done with two FortiGate units.

The following network topology uses four FortiGate units; each is a 3200D model and is running FortiOS 6.4.0 build 1533. The FortiSwitch models are 1048E, 448D, and 426EF; they are running FortiSwitchOS 6.2.0 build 0202:



FortiLink over a point-to-point layer-2 network

Starting in FortiSwitchOS 6.4.0, you can run FortiLink mode over a point-to-point layer-2 network. To create this topology, you form an inter-switch link (ISL) between two FortiSwitch units over a layer-2 device or non-FortiSwitch device (such as a wireless bridge) and configure the tag protocol identifier (TPID) between the two FortiSwitch units.

NOTE:

- The `set fortilink-p2p-tpid` command is not supported on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models.
- The `set fortlink-p2p` command is available in Fortilink mode and standalone mode. The `set fortilink-p2p-tpid` command is available only in FortiLink mode.

1. Enable the FortiLink point-to-point network on each FortiSwitch unit:

```
config switch physical-port
   edit <port_name>
      set fortlink-p2p enable
   end
```

2. Make certain that the FortiLink point-to-point TPID value is the same on each FortiSwitch unit. By default, it is 0x8100.

```
config switch global
   set fortilink-p2p-tpid <0x0001-0xfffe>
end
```

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 *WiFi & 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 Firmware upgrade of stacked or tiered FortiSwitch units on page 58.

Stacking configuration

To set up stacking:

1. Configure the active FortiLink interface on the FortiGate unit.
2. (Optional) Configure the standby FortiLink interface.
3. Connect the FortiSwitch units together, based on your chosen topology.

1. Configure the active FortiLink

Configure the FortiLink interface (as described in the Using the FortiGate GUI chapter).

When you configure the FortiLink interface, the stacking capability is enabled automatically.

2. Configure the standby FortiLink

Configure the standby FortiLink interface. Depending on your configuration, the standby FortiLink might connect to the same FortiGate unit as the active FortiLink or to a different FortiGate unit.

If the FortiGate unit receives discovery requests from two FortiSwitch units, the link from one FortiSwitch unit will be selected as active, and the link from other FortiSwitch unit will be selected as standby.

If the active FortiLink fails, the FortiGate unit converts the standby FortiLink to active.

3. Connect the FortiSwitch units

Refer to the topology diagrams to see how to connect the FortiSwitch units.

Inter-switch links (ISLs) form automatically between the stacked switches.

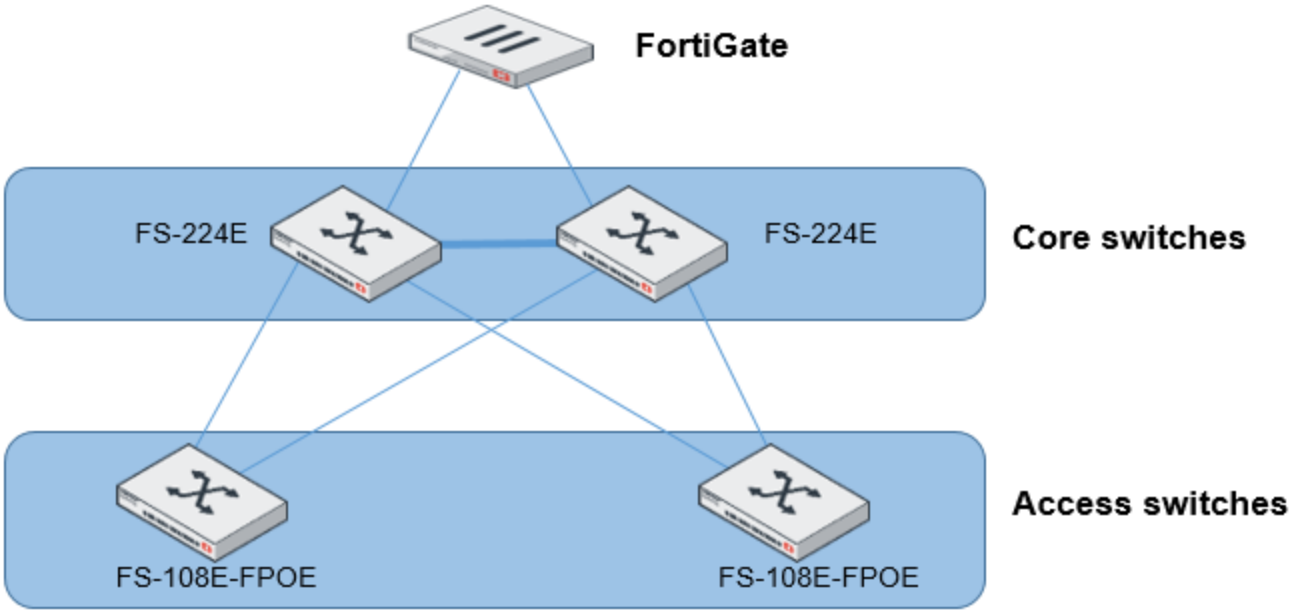
The FortiGate unit will discover and authorize all of the FortiSwitch units that are connected. After this, the FortiGate unit is ready to manage all of the authorized FortiSwitch units.

Disable stacking

To disable stacking, execute the following commands from the FortiGate CLI. In the following example, port4 is the FortiLink interface:

```
config system interface
   edit port4
      set fortilink-stacking disable
   end
end
```

Firmware upgrade of stacked or tiered FortiSwitch units



In this topology, the core FortiSwitch units are model FS-224E, and the access FortiSwitch units are model FS-108E-FPOE. Because the switches are stacked or tiered, the procedure to update the firmware is simpler. The FortiGate unit is running FOS 6.2.2 GA. In the following procedure, the four FortiSwitch units are upgraded from 6.2.1 to 6.2.2.

To upgrade the firmware of stacked or tiered FortiSwitch units:

1. Check that all of the FortiSwitch units are connected and which firmware versions they are running. For example:

```
FGT81ETK19001274 # execute switch-controller get-conn-status
Managed-devices in current vdom root:

STACK-NAME: FortiSwitch-Stack-flink
SWITCH-ID         VERSION           STATUS         FLAG   ADDRESS       JOIN-TIME
NAME
S108EF5918003577  v6.2.1 (176)      Authorized/Up   -   10.105.22.6     Thu Oct 24
10:47:27 2019    -
S108EP5918008265  v6.2.1 (176)      Authorized/Up   -   10.105.22.5     Thu Oct 24
10:47:20 2019    -
S224ENTF18001408  v6.2.1 (176)      Authorized/Up   -   10.105.22.2     Thu Oct 24
10:44:36 2019    -
S224ENTF18001432  v6.2.1 (176)      Authorized/Up   -   10.105.22.3     Thu Oct 24
10:44:49 2019    -

Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=configuration
sync error
Managed-Switches: 4 (UP: 4 DOWN: 0)
```

2. (Optional) To speed up how fast the image is pushed from the FortiGate unit to the FortiSwitch units, enable the HTTPS image push instead of the CAPWAP image push. For example:

```
FGT81ETK19001274 # config switch-controller global
FGT81ETK19001274 (global) # set https-image-push enable
FGT81ETK19001274 (global) # end
```

3. Download the file for the FortiSwitchOS 6.2.2 GA build 194 in the FortiGate unit. For example:

```
FGT81ETK19001274 # execute switch-controller switch-software upload tftp FSW_224E-v6-
build0194-FORTINET.out 10.105.16.15

Downloading file FSW_224E-v6-build0194-FORTINET.out from tftp server 10.105.16.15...
#########################
Image checking ...
Image MD5 calculating ...
Image Saving S224EN-IMG.swtp ...
Successful!

File Syncing...

FGT81ETK19001274 # execute switch-controller switch-software upload tftp FSW_108E_POE-
v6-build0194-FORTINET.out 10.105.16.15

Downloading file FSW_108E_POE-v6-build0194-FORTINET.out from tftp server 10.105.16.15...
##################
Image checking ...
Image MD5 calculating ...
Image Saving S108EP-IMG.swtp ...
Successful!

File Syncing...

FGT81ETK19001274 # execute switch-controller switch-software upload tftp FSW_108E_FPOE-
v6-build0194-FORTINET.out 10.105.16.15

Downloading file FSW_108E_FPOE-v6-build0194-FORTINET.out from tftp server
10.105.16.15...
##################
Image checking ...
Image MD5 calculating ...
Image Saving S108EF-IMG.swtp ...
Successful!

File Syncing...

FGT81ETK19001274 #
```

4. Check the downloaded FortiSwitch image. For example:

```
FGT81ETK19001274 # execute switch-controller switch-software list-available

ImageName              ImageSize(B)   ImageInfo              Uploaded Time
S108EF-IMG.swtp        19574769       S108EF-v6.2-build194   Thu Oct 24 13:03:51 2019
S108EP-IMG.swtp        19583362       S108EP-v6.2-build194   Thu Oct 24 13:03:23 2019
S224EN-IMG.swtp        27159659       S224EN-v6.2-build194   Thu Oct 24 13:03:02 2019

FGT81ETK19001274 #
```

5. Start the image staging. For example:

```
FGT81ETK19001274 #  execute switch-controller switch-software stage all S224EN-IMG.swtp
Staged Image Version S224EN-v6.2-build194
Image staging operation is started for FortiSwitch S224ENTF18001408 ...
Image staging operation is started for FortiSwitch S224ENTF18001432 ...
```

```
FGT81ETK19001274 # execute switch-controller switch-software stage all S108EF-IMG.swtp
Staged Image Version S108EF-v6.2-build194
Image staging operation is started for FortiSwitch S108EF5918003577 ...

FGT81ETK19001274 # execute switch-controller switch-software stage all S108EP-IMG.swtp
Staged Image Version S108EP-v6.2-build194
Image staging operation is started for FortiSwitch S108EP5918008265 ...
```

6. Check the status of the image staging. For example:

```
FGT81ETK19001274 # execute switch-controller get-upgrade-status
Device    Running-version                                Status      Next-boot

================================================================================
===
VDOM : root
S224ENTF18001408  S224EN-v6.2.1-build176,190620 (GA)             (100/0/0)   S224EN-
v6.2-build176       (Staging)
S224ENTF18001432  S224EN-v6.2.1-build176,190620 (GA)             (100/0/0)   S224EN-
v6.2-build176       (Staging)
S108EP5918008265  S108EP-v6.2.1-build176,190620 (GA)             (18/0/0)   S108EP-v6.2-
build176        (Staging)
S108EF5918003577  S108EF-v6.2.1-build176,190620 (GA)             (25/0/0)   S108EF-v6.2-
build176        (Staging)
```

7. Verify that the image staging has completed. For example:

```
FGT81ETK19001274 # execute switch-controller get-upgrade-status
Device    Running-version                                Status      Next-boot

================================================================================
===
VDOM : root
S224ENTF18001408  S224EN-v6.2.1-build176,190620 (GA)             (0/100/100)   S224EN-
v6.2-build194     (Idle)
S224ENTF18001432  S224EN-v6.2.1-build176,190620 (GA)             (0/100/100)   S224EN-
v6.2-build194     (Idle)
S108EP5918008265  S108EP-v6.2.1-build176,190620 (GA)             (0/100/100)   S108EP-
v6.2-build194     (Idle)
S108EF5918003577  S108EF-v6.2.1-build176,190620 (GA)             (0/100/100)   S108EF-
v6.2-build194     (Idle)
```

8. Reboot all switches (or reboot the switches by group). For example:

```
FGT81ETK19001274 # execute switch-controller switch-action restart delay all
Delayed restart operation is requested for FortiSwitch S224ENTF18001408 ...
Delayed restart operation is requested for FortiSwitch S224ENTF18001432 ...
Delayed restart operation is requested for FortiSwitch S108EP5918008265 ...
Delayed restart operation is requested for FortiSwitch S108EF5918003577 ...
```

9. Check the status of the switch reboot. For example:

```
FGT81ETK19001274 # execute switch-controller switch-action restart delay all
Delayed restart operation is requested for FortiSwitch S224ENTF18001408 ...
Delayed restart operation is requested for FortiSwitch S224ENTF18001432 ...
Delayed restart operation is requested for FortiSwitch S108EP5918008265 ...
Delayed restart operation is requested for FortiSwitch S108EF5918003577 ...
```

```
FGT81ETK19001274 # execute switch-controller get-upgrade-status
Device    Running-version                                Status      Next-boot

================================================================================
===
VDOM : root
S224ENTF18001408                        Prepping for delayed restart triggered ...
please wait for switch to reboot in a moment
S224ENTF18001432                        Prepping for delayed restart triggered ...
please wait for switch to reboot in a moment
S108EP5918008265                        Prepping for delayed restart triggered ...
please wait for switch to reboot in a moment
S108EF5918003577                        Prepping for delayed restart triggered ...
please wait for switch to reboot in a moment

FGT81ETK19001274 # execute switch-controller get-conn-status
Managed-devices in current vdom root:

STACK-NAME: FortiSwitch-Stack-flink
SWITCH-ID         VERSION           STATUS         FLAG   ADDRESS      JOIN-TIME
NAME
S108EF5918003577  v6.2.1 ()         Authorized/Down D   0.0.0.0         N/A
 -
S108EP5918008265  v6.2.1 ()         Authorized/Down D   0.0.0.0         N/A
 -
S224ENTF18001408  v6.2.1 ()         Authorized/Down D   0.0.0.0         N/A
 -
S224ENTF18001432  v6.2.1 ()         Authorized/Down D   0.0.0.0         N/A
 -

Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=configuration
sync error
Managed-Switches: 4 (UP: 0 DOWN: 4)

FGT81ETK19001274 #
```

10. Wait for a while before checking that all switches are online. For example:

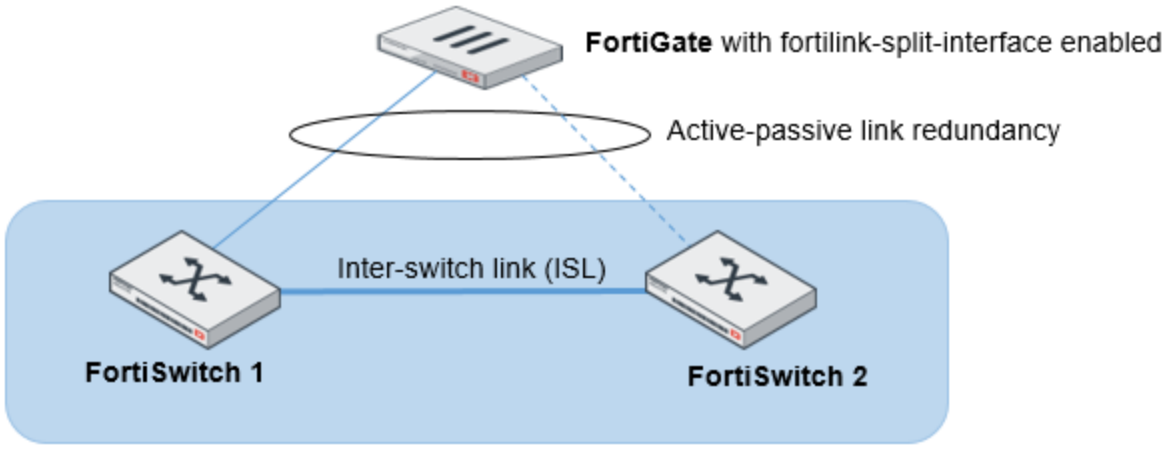
```
FGT81ETK19001274 # execute switch-controller get-upgrade-status
Device    Running-version                                Status      Next-boot

================================================================================
===
VDOM : root
S224ENTF18001408  S224EN-v6.2.2-build194,191018 (GA)             (0/100/100)   S224EN-
v6.2-build194     (Idle)
S224ENTF18001432  S224EN-v6.2.2-build194,191018 (GA)             (0/100/100)   S224EN-
v6.2-build194     (Idle)
S108EP5918008265  S108EP-v6.2.2-build194,191018 (GA)             (0/100/100)   S108EP-
v6.2-build194     (Idle)
S108EF5918003577  S108EF-v6.2.2-build194,191018 (GA)             (0/100/100)   S108EF-
v6.2-build194     (Idle)

FGT81ETK19001274 # execute switch-controller get-conn-status
Managed-devices in current vdom root:

STACK-NAME: FortiSwitch-Stack-flink
```

```
SWITCH-ID         VERSION           STATUS         FLAG   ADDRESS              JOIN-TIME
          NAME
S108EF5918003577  v6.2.2 (194)      Authorized/Up   -   10.105.22.6     Thu Oct 24
13:22:27 2019    -
S108EP5918008265  v6.2.2 (194)      Authorized/Up   -   10.105.22.5     Thu Oct 24
13:22:41 2019    -
S224ENTF18001408  v6.2.2 (194)      Authorized/Up   -   10.105.22.2     Thu Oct 24
13:20:11 2019    -
S224ENTF18001432  v6.2.2 (194)      Authorized/Up   -   10.105.22.3     Thu Oct 24
13:19:58 2019    -

Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=configuration
sync error
Managed-Switches: 4 (UP: 4 DOWN: 0)

FGT81ETK19001274 #
```

Transitioning from a FortiLink split interface to a FortiLink MCLAG

You can use the FortiLink split interface to connect the FortiLink aggregate interface from one FortiGate unit to two FortiSwitch units. When the FortiLink split interface is enabled, only one link remains active.

In this topology, the FortiLink split interface connects a FortiLink aggregate interface from one FortiGate unit to two FortiSwitch units. The aggregate interface of the FortiGate unit for this configuration contains at least one physical port connected to each FortiSwitch unit.



NOTE:

- Make sure that the split interface is enabled.
- This procedure also applies to a FortiGate unit in HA mode.
- More links can be added between the FortiGate unit and FortiSwitch unit.
- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks.

NOTE: If you are going to use IGMP snooping with an MCLAG topology:

- On the global switch level, `mclag-igmp-aware` must be enabled,
- The `igmps-flood-traffic` and `igmps-flood-report` settings must be *disabled* on the ISL and FortiLink trunks; but the `igmps-flood-traffic` and `igmps-flood-report` settings must be *enabled* on ICL trunks.
- IGMP proxy must be enabled.

The following procedure uses zero-touch provisioning to change the configuration of the FortiSwitch units without losing their management from the FortiGate unit. The MCLAG-ICL can also be enabled directly using console cables or management ports.

1. Log into FortiSwitch 2 using the *Connect to CLI* button in the FortiGate GUI, use the `get switch lldp auto-isl-status` command to find out the name of the trunk connecting the peer switches, and change the ISL to an ICL. For example:

```
get switch lldp auto-isl-status

config switch trunk
   edit <trunk_name>
      set
      mclag-icl enable
   next
end
```

2. Log into FortiSwitch 1 using the *Connect to CLI* button in the FortiGate GUI, use the `get switch lldp auto-isl-status` command to find out the name of the trunk connecting the peer switches, and change the ISL to an ICL. For example:

```
get switch lldp auto-isl-status

config switch trunk
   edit <trunk_name>
      set mclag-icl enable
   next
end
```

3. Log into the FortiGate unit and disable the split interface. For example:

```
config system interface
   edit <aggregate_name>
      set fortilink-split-interface disable
   next
end
```

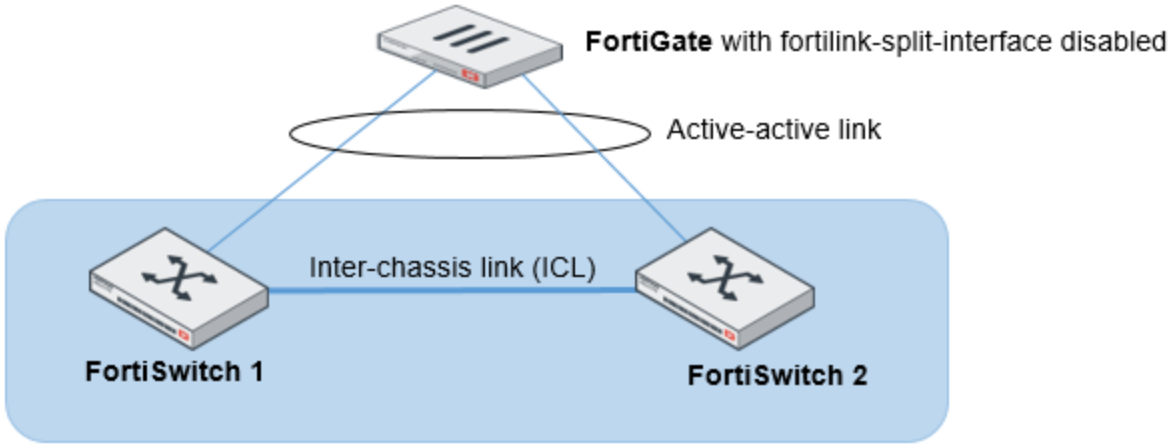
4. From the FortiGate unit, enable the LACP static mode:

```
config system interface
   edit <aggregate_name>
      set lacp-mode static
   next
end
```

NOTE: If you are using FortiOS 6.2 or later, use the `set lacp-mode active` command instead.

5. Check that the LAG is working correctly. For example:

```
diagnose netlink aggregate name <aggregate_name>
```



If you disable the MCLAG ICL (with the `set mclag-icl disable` command), you need to enable the fortilink-split-interface.

Optional setup tasks

This section describes the following tasks:

Configuring the FortiSwitch management port

If the FortiSwitch model has a dedicated management port, you can configure remote management to the FortiSwitch. In FortiLink mode, the FortiGate is the default gateway, so you need to configure an explicit route for the FortiSwitch management port.

Using the Web administration GUI

1. Go to *Network* > *Static Routes* > *Create New* > *Route*.
2. Set *Destination* to *Subnet* and enter a subnetwork and mask.
3. Set *Device* to the management interface.
4. Add a *Gateway* IP address.

Using the FortiSwitch CLI

Enter the following commands:

```
config router static
   edit 1
      set device mgmt
      set gateway <router IP address>
      set dst <router subnet> <subnet mask>
   end
end
```

In the following example, the FortiSwitch management port is connected to a router with IP address 192.168.0.10:

```
config router static
   edit 1
```

```
      set device mgmt
      set gateway 192.168.0.10
      set dst 192.168.0.0 255.255.0.0
   end
end
```

Migrating the configuration of standalone FortiSwitch units

When a configured standalone FortiSwitch unit is converted to FortiLink 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 FortiGate-compatible configuration.

To get the script and instructions, go to:

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

Converting to FortiSwitch standalone mode

Use one of the following commands to convert a FortiSwitch from FortiLink mode to standalone mode so that it will no longer be managed by a FortiGate:

- `execute switch-controller factory-reset <switch-id>`—This command returns the FortiSwitch to the factory defaults and then reboots the FortiSwitch. If the FortiSwitch is configured for FortiLink auto-discovery, FortiGate can detect and automatically authorize the FortiSwitch. For example:`execute switch-controller factory-reset S1234567890`
- `execute switch-controller switch-action set-standalone <switch-id>`—This command returns the FortiSwitch to the factory defaults, reboots the FortiSwitch, and prevents the FortiGate 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 <switch-id>
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 <switch-id>
   unselect disable-discovery <switch-id>
end
```

For example:

```
config switch-controller global
   append disable-discovery S012345678
```

```
   unselect disable-discovery S1234567890
end
```

Changing the admin password on the FortiGate for all managed FortiSwitch units

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

```
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
```

Enabling network-assisted device detection

Network-assisted device detection allows the FortiGate unit to use the information about connected devices detected by the managed FortiSwitch unit.

To enable network-assisted device detection on a VDOM:

```
config switch-controller network-monitor-settings
   set network-monitoring enable
end
```

You can display a list of detected devices from the *Device Inventory* menu in the GUI. To list the detected devices in the CLI, enter the following command:

```
diagnose user device list
```

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, ICI, 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
```

NOTE: The ICL automatic-configuration policy requires FortiOS 6.2.0 or later.

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 process for FortiSwitch configuration

Use the following CLI commands to reduce the number of parallel process 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
```

Using the FortiSwitch serial number for automatic name resolution

By default, you can check that FortiSwitch unit is accessible from the FortiGate unit 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
```

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

```
FG100D3G15817028 (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
```

Optionally, you can omit the domain name (`.fsw`) from the command by setting the default DNS domain on the FortiGate unit.

```
config system dns
   set domain "fsw"
end
```

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

```
FG100D3G15817028 (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
```

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
```

NOTE: After you upgrade to FortiOS 6.2, the allowaccess settings for the FortiSwitch mgmt and internal interfaces are overridden by the default local-access security policy.

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.

Configuring SNMP globally

To configure SNMP globally, configure the following settings:

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

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 <FortiGate_location>
end
```

To configure the SNMP community globally:

```
config switch-controller snmp-community
   edit <SNMP_community_ID>
```

```
      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
      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 | sha}
      set auth-pwd <password_for_authentication_protocol>
      set priv-proto {aes | des}
      set priv-pwd <password_for_encryption_protocol>
   end
```

Configuring SNMP locally

To configure SNMP for a specific FortiSwitch unit, configure the following settings:

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

To configure the SNMP system information locally:

```
config switch-controller managed-switch
   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 <FortiGate_location>
   end
end
```

To configure the SNMP community locally:

```
config switch-controller managed-switch
   set override-snmp-community enable
   config snmp-community
      edit <SNMP_community_ID>
         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
         end
```

To configure the SNMP trap threshold values locally:

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

To configure the SNMP user locally:

```
config switch-controller managed-switch
   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 | sha}
         set auth-pwd <password_for_authentication_protocol>
         set priv-proto {aes | des}
         set priv-pwd <password_for_encryption_protocol>
      end
```

```
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 a FortiGate unit, 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 FortiOS only for managed FortiSwitch units that support IP source guard. 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. Enable IPv4 source guard in the FortiOS CLI.
2. Create static entries on the FortiSwitch unit by binding IPv4 addresses with MAC addresses.
3. Check the IPv4 source-guard entries on the FortiSwitch unit.

Enabling IPv4 source guard

You must enable IPv4 source guard in the FortiOS 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 FortiOS CLI, you can create static entries in the FortiOS CLI by binding IPv4 addresses with MAC addresses. For IPv4 source-guard dynamic entries, you need to configure DHCP snooping. See Using the FortiGate GUI on page 17.

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 FortiOS CLI to display all IP source-guard entries:

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

FortiSwitch features configuration

This section describes how to configure global FortiSwitch settings using FortiGate CLI commands. These settings will apply to all of the managed FortiSwitch units. You can also override some of the settings on individual FortiSwitch units.

This chapter covers the following topics:

Configure 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 the FortiGate unit, you can centrally configure and manage VLANs for the managed FortiSwitch units.

In FortiSwitchOS 3.3.0 and later releases, the FortiSwitch 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 (FortiOS 6.2.0 and later), 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.

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 *WiFi & Switch Controller* > *FortiSwitch VLANs*, select *Create New*, and change the following settings:

Interface 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 *Undefine*d.

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

To assign FortiSwitch ports to the VLAN:

1. Go to *WiFi & Switch Controller* > *FortiSwitch Ports*.
2. Click a port row.
3. Click the *Native VLAN* column in one of the selected entries to change the native VLAN.
4. Select a VLAN from the displayed list. The new value is assigned to the selected ports.
5. Click the + icon in the *Allowed VLANs* column to change the allowed VLANs.
6. Select one or more of the VLANs (or the value *all*) from the displayed list. 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>
   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 <Switch ID>
      config ports
         edit <port name>
            set vlan <vlan name>
            set allowed-vlans <vlan name>
            or
            set allowed-vlans-all enable
         next
      end
   end
```

Assign untagged VLANs to a managed FortiSwitch port:

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

Viewing FortiSwitch VLANs

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

Each entry in the VLAN list displays the following information:

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

Enabling and disabling switch-controller access VLANs through the FortiGate unit

Access VLANs are VLANs that aggregate client traffic solely to the FortiGate unit. This prevents direct client-to-client traffic visibility at the layer-2 VLAN layer. Clients can only communicate with the FortiGate unit. After the client traffic reaches the FortiGate, the FortiGate unit can then determine whether to allow various levels of access to the client by shifting the client's network VLAN as appropriate.

NOTE: IPv6 is not supported between clients within a switch-controller access VLAN.

Use `enable` to allow traffic only to and from the FortiGate and to block FortiSwitch port-to-port traffic on the specified VLAN. Use `disable` to allow normal traffic on the specified VLAN.

```
config system interface
   edit <VLAN name>
      set switch-controller-access-vlan {enable | disable}
   next
end
```

NOTE: You must configure the proxy ARP with the `config system proxy-arp` CLI command to be able to use the access VLANs. For example:

```
config system proxy-arp
   edit 1
      set interface "V100"
      set ip 1.1.1.1
      set end-ip 1.1.1.200
   next
end
```

Changing the VLAN configuration mode

You can change which VLANs the `set allowed-vlans` command affects.

If you want the `set allowed-vlans` command to apply to all user-defined VLANs, use the following CLI commands:

```
config switch-controller global
   set vlan-all-mode defined
end
```

If you want the `set allowed-vlans` command to apply to all possible VLANs (1-4094), use the following CLI commands:

```
config switch-controller global
   set vlan-all-mode all
end
```

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

Enabling FortiLink 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. By default, VLAN optimization is disabled.

To enable FortiLink VLAN optimization on FortiSwitch units from the FortiGate unit:

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

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

Configure 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.

Flood-unknown-multicast controls whether the system will flood unknown multicast messages within the VLAN.

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

Configure LLDP-MED

Starting in FortiOS 6.4.0 and FortiSwitchOS 6.4.0, LLDP neighbor devices are dynamically detected. By default, this feature is enabled in FortiOS but disabled in managed FortiSwitch units. Dynamic detection must be enabled in both FortiOS and FortiSwitchOS for this feature to work.

To configure LLDP profiles in FortiOS:

```
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.

Variable	Description
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.
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 FortiOS:

```
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
```

Create LLDP asset tags for each managed FortiSwitch

You can use the following commands to add an LLDP asset tag for a managed FortiSwitch:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set switch-device-tag <string>
end
```

Add 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
```

Display 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>
```

Configure the MAC sync interval

Use the following commands to configure the global MAC synch interval.

The MAC sync interval is the time interval between MAC synchronizations. The range is 30 to 600 seconds, and the default value is 60.

```
config switch-controller mac-sync-settings
   set mac-sync-interval <30-600>
end
```

Configure STP settings

NOTE: STP is not supported between a FortiGate unit and a FortiSwitch unit in FortiLink mode.

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.

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 <switch-id>
```

```
      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
```

Configure 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.

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 collector-ip <collector IP address>
    set collector-port <0-65535; default is 0>
    set transport {udp | tcp | sctp}
    set level {vlan | ip | port | proto}
    set filter <string>
    set max-export-pkt-size <512-9216 bytes; default is 512>.
    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>
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 filter

Use the Berkeley Packet Filter to specify what packets to sample.

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
```

Quarantines

Administrators can use MAC addresses to quarantine hosts and users connected to a FortiSwitch unit. Quarantined MAC addresses are isolated from the rest of the network and LAN.

Quarantining MAC addresses

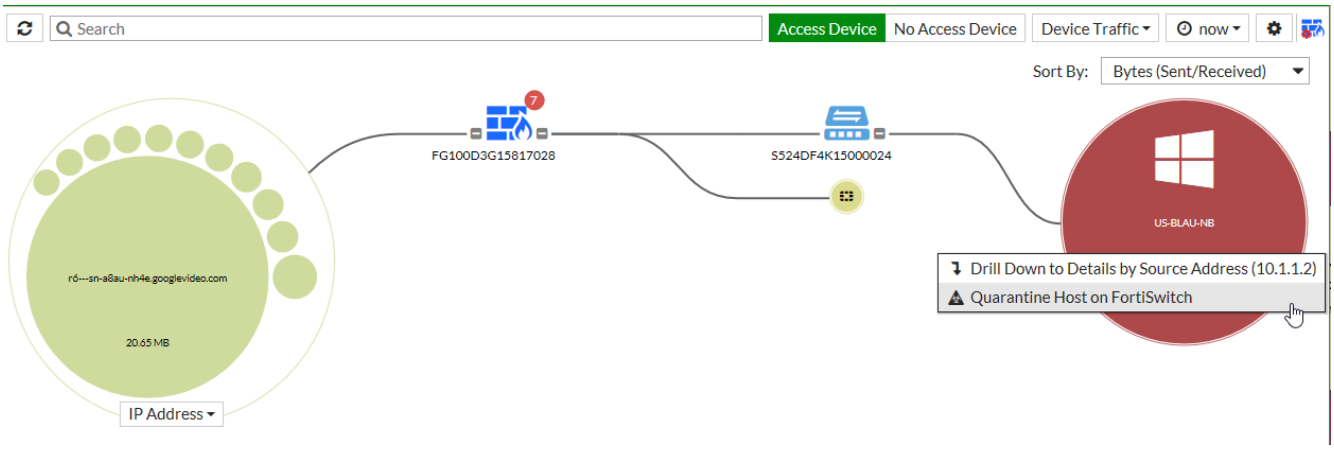
You can use the FortiGate GUI or CLI to quarantine a MAC address.

NOTE: If you have multiple FortiLink interfaces, only the first quarantine VLAN is created successfully (with an IP address of 10.254.254.254). Additional quarantine VLANs will have an empty IP address.

Using the FortiGate GUI

In the FortiGate GUI, the quarantine feature is automatically enabled when you quarantine a host.

1. Select the host to quarantine.
   - Go to *Security Fabric* > *Physical Topology*, right-click on a host, and select *Quarantine Host on FortiSwitch*.
   - Go to *Security Fabric* > *Logical Topology*, right-click on a host, and select *Quarantine Host on FortiSwitch*.
   - Go to *FortiView* > *Sources*, right-click on an entry in the Source column, and select *Quarantine Host on FortiSwitch*.
2. Select *Accept* to confirm that you want to quarantine the host.



Using the FortiGate CLI

NOTE: Previously, this feature used the `config switch-controller quarantine` CLI command.

There are two kinds of quarantines:

- Quarantine-by-VLAN sends quarantined device traffic to the FortiGate unit on a separate quarantine VLAN (starting in FortiOS 6.0.0 and FortiSwitchOS 6.0.0).
- Quarantine-by-redirect redirects quarantined device traffic to a firewall address group on the FortiGate unit (starting in FortiOS 6.4.0 and FortiSwitchOS 6.4.0).

By default, the quarantine feature is enabled. When you upgrade a FortiGate unit from an older to a newer firmware version, the FortiGate unit uses the quarantine feature status from the older configuration. If the quarantine feature was disabled in the older configuration, it will be disabled after the upgrade.

You can add MAC addresses to be quarantined even when the quarantine feature is disabled. The MAC addresses are only quarantined when the quarantine feature is enabled.

The table size limit for the quarantine entry is 512. There is no limit for how many MAC addresses can be quarantined per quarantine entry.

Optionally, you can configure a traffic policy for quarantined devices to control how much bandwidth and burst they use and which class of service (CoS) queue they are assigned to. Without a traffic policy, you cannot control how much network resources quarantined devices use.

Quarantine-by-redirect is the default. If you are upgrading to FortiOS 6.4.0 or higher and already have a quarantine-by VLAN configuration, the quarantine mode does not change during the upgrade.

If you have a quarantine-by-VLAN configuration and want to migrate to a quarantine-by-redirect configuration:

1. Disable quarantine.
2. Change the quarantine-mode to `by-direct`.
3. Remove the quarantine VLAN from the switch ports.
4. Enable quarantine.

To set up a quarantine in FortiOS:

```
config switch-controller global
   set quarantine-mode {by-vlan | by-redirect}
end
```

```
config user quarantine
   set quarantine enable
   set traffic-policy <traffic_policy_name>
   set firewall-groups <firewall_address_group>
   config targets
      edit <quarantine_entry_name>
         set description <string>
         config macs
            edit <MAC_address_1>
               set drop {enable | disable}
            next
            edit <MAC_address_2>
               set drop {enable | disable}
            next
            edit <MAC_address_3>
               set drop {enable | disable}
            next
      end
   end
end
```

Option	Description
quarantine-mode {by-vlan | by-redirect}	Select the quarantine mode: • `by-vlan` sends quarantined device traffic to the FortiGate unit on a separate quarantine VLAN. • `by-redirect` redirects quarantined device traffic to a firewall address group on the FortiGate unit. This mode is the default.
traffic-policy <traffic_policy_name>	Optional. A name for the traffic policy that controls quarantined devices. If you do add a traffic policy, you need to configure it with the `config switch-controller traffic-policy` command.
firewall-groups <firewall_address_group>	Optional. By default, the firewall address group is `QuarantinedDevices`. If you are using quarantine-by-redirect, you must use the default firewall address group.
quarantine_entry_name	A name for this quarantine entry.
description <string>	Optional. A description of the MAC addresses being quarantined.
MAC_address_1, MAC_address_2, MAC_address_3	A layer-2 MAC address in the following format: `12:34:56:aa:bb:cc`
drop {enable | disable}	Enable to drop quarantined device traffic. Disable to send quarantined device traffic to the FortiGate unit.

For example:

```
config switch-controller global
   set quarantine-mode by-redirect
end

config user quarantine
   set quarantine enable
   set traffic-policy qtrafficp
   set firewall-groups QuarantinedDevices
```

```
   config targets
      edit quarantine1
      config macs
         set description "infected by virus"
         edit 00:00:00:aa:bb:cc
            set drop disable
         next
         edit 00:11:22:33:44:55
            set drop disable
         next
         edit 00:01:02:03:04:05
            set drop disable
         next
      end
   next
end
```

To configure a traffic policy for quarantined devices in FortiOS:

```
config switch-controller traffic-policy
   edit <traffic_policy_name>
      set description <string>
      set policer-status enable
      set guaranteed-bandwidth <0-524287000>
      set guaranteed-burst <0-4294967295>
      set maximum-burst <0-4294967295>
      set cos-queue <0-7>
   end
```

Option	Description
traffic-policy <traffic_policy_name>	Enter a name for the traffic policy that controls quarantined devices.
description <string>	Enter an optional description of the traffic policy.
policer-status enable	Enable the policer configuration to control quarantined devices. It is enabled by default.
guaranteed-bandwidth <0-524287000>	Enter the guaranteed bandwidth in kbps. The maximum value is 524287000. The default value is 0.
guaranteed-burst <0-4294967295>	Enter the guaranteed burst size in bytes. The maximum value is 4294967295. The default value is 0.
maximum-burst <0-4294967295>	The maximum burst size is in bytes. The maximum value is 4294967295. The default value is 0.
set cos-queue <0-7>	Set the class of service for the VLAN traffic. Use the `unset cos-queue` command to disable this setting.

For example:

```
config switch-controller traffic-policy
   edit qtrafficp
      set description "quarantined traffic policy"
      set policer-status enable
      set guaranteed-bandwidth 10000
      set guaranteed-burst 10000
```

```
    set maximum-burst 10000
    unset cos-queue
  end
```

Using quarantine with DHCP

When a device using DHCP is quarantined, the device becomes inaccessible until the DHCP is renewed. To avoid this problem, enable the bounce-quarantined-link option, which shuts down the switch port where the quarantined device was last seen and then brings it back up again. Bouncing the port when the device is quarantined and when the device is released from quarantine causes the DHCP to be renewed so that the device is connected to the correct network. By default, the bounce-quarantined-link option is disabled.

To bounce the switch port where a quarantined device was last seen:

```
config switch-controller global
   set bounce-quarantined-link {enable | disable}
end
```

Using quarantine with 802.1x MAC-based authentication

After a device is authorized with IEEE 802.1x MAC-based authentication, you can quarantine that device. If the device was quarantined before 802.1x MAC-based authentication was enabled, the device's traffic remains in the quarantine VLAN 4093 after 802.1x MAC-based authentication is enabled.

To use quarantines with IEEE 802.1x MAC-based authentication:

1. By default, detecting the quarantine VLAN is enabled on a global level on the managed FortiSwitch unit. You can verify that quarantine-vlan is enabled with the following commands:

```
S448DF3X16000118 # config switch global

S448DF3X16000118 (global) # config port-security

S448DF3X16000118 (port-security) # get
link-down-auth : set-unauth
mab-reauth : disable
quarantine-vlan : enable
reauth-period : 60
max-reauth-attempt : 0
```

2. By default, 802.1x MAC-based authentication and quarantine VLAN detection are enabled on a port level on the managed FortiSwitch unit. You can verify the settings for the port-security-mode and quarantine-vlan. For example:

```
S448DF3X16000118 (port17) # show switch interface port17
config switch interface
   edit "port17"
      set allowed-vlans 4093
      set untagged-vlans 4093
         set security-groups "group1"
      set snmp-index 17
         config port-security
            set auth-fail-vlan disable
```

```
            set eap-passthru enable
            set framevid-apply enable
            set guest-auth-delay 30
            set guest-vlan disable
            set mac-auth-bypass enable
            set open-auth disable
            set port-security-mode 802.1X-mac-based
            set quarantine-vlan enable
            set radius-timeout-overwrite disable
            set auth-fail-vlanid 200
            set guest-vlanid 100
         end
      next
   end
```

3. On the FortiGate unit, quarantine a MAC address. For example:

```
config user quarantine
   edit "quarantine1"
      config macs
         edit 00:05:65:ad:15:03
         next
      end
   next
end
```

4. The FortiGate unit pushes the MAC-VLAN binding to the managed FortiSwitch unit. You can verify that the managed FortiSwitch unit received the MAC-VLAN binding with the following command:

```
S448DF3X16000118 # show switch vlan 4093
config switch vlan
   edit 4093
      set description "qtn.FLNK10"
      set dhcp-snooping enable
      set access-vlan enable
         config member-by-mac
            edit 1
               set mac 00:05:65:ad:15:03
            next
         end
      next
   end
```

5. The 802.1x session shows that the MAC address is quarantined in VLAN 4093. You can verify that the managed FortiSwitch port has the quarantined MAC address. For example:

```
S448DF3X16000118 # diagnose switch 8 status port17

port17: Mode: mac-based (mac-by-pass enable)
Link: Link up
Port State: authorized: ( )
EAP pass-through mode : Enable
Quarantine VLAN (4093) detection : Enable
Native Vlan : 1
Allowed Vlan list: 1,4093
Untagged Vlan list: 1,4093
```

```
Guest VLAN :
Auth-Fail Vlan :

Switch sessions 3/480, Local port sessions:1/20
Client MAC Type Vlan Dynamic-Vlan
Quarantined
00:05:65:ad:15:03 802.1x 1 4093

Sessions info:
00:50:56:ad:51:81 Type=802.1x,PEAP,state=AUTHENTICATED,etime=0,eap_cnt=41
     params:reAuth=1800
```

6. The MAC address table also shows the MAC address in VLAN 4093. You can verify the entries in the MAC address table with the following commands:

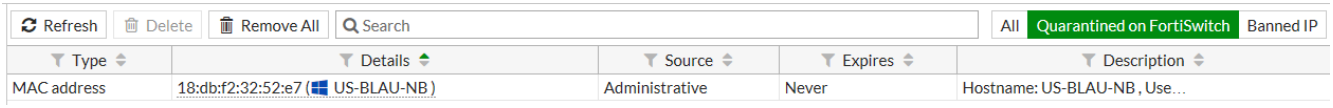
```
S448DF3X16000118 # diagnose switch vlan assignment mac list
00:05:65:ad:15:03 VLAN: 4093 Installed: yes
Source: 802.1X-MAC-Radius
Description: port17

S448DF3X16000118 # diagnose switch mac list | grep "VLAN: 4093"
MAC: 00:05:65:ad:15:03 VLAN: 4093 Port: port17(port-id 17)
```

Viewing quarantine entries

Quarantine entries are created on the FortiGate unit that is managing the FortiSwitch unit.

Using the FortiGate GUI

1. Go to *Monitor* > *Quarantine Monitor*.
2. Click *Quarantined on FortiSwitch*.The Quarantined on FortiSwitch button is only available if a device is detected behind the FortiSwitch unit, which requires Device Detection to be enabled.



Using the FortiGate CLI

Use the following command to view the quarantine list of MAC addresses:

```
show user quarantine
```

For example:

```
show user quarantine

config user quarantine
   set quarantine enable
   config targets
      edit quarantine1
      config macs
```

```
        set description "infected by virus"
        edit 00:00:00:aa:bb:cc
        next
        edit 00:11:22:33:44:55
        next
        edit 00:01:02:03:04:05
        next
      end
   end
end
```

When the quarantine feature is enabled on the FortiGate unit, it creates a quarantine VLAN (qtn.<FortiLink_port_name>) and a quarantine DHCP server (with the quarantine VLAN as default gateway) on the virtual domain. The quarantine VLAN is applied to the allowed and untagged VLANs on all connected FortiSwitch ports.

Use the following command to view the quarantine VLAN:

```
show system interface qtn.<FortiLink_port_name>
```

For example:

```
show system interface qtn.port7

config system interface
   edit "qtn.port7"
      set vdom "vdom1"
      set ip 10.254.254.254 255.255.255.0
      set description "Quarantine VLAN"
      set security-mode captive-portal
      set replacemsg-override-group "auth-intf-qtn.port7"
      set device-identification enable
      set device-identification-active-scan enable
      set snmp-index 34
      set switch-controller-access-vlan enable
      set color 6
      set interface "port7"
      set vlanid 4093
   next
end
```

Use the following commands to view the quarantine DHCP server:

```
show system dhcp server
config system dhcp server
   edit 2
      set dns-service default
      set default-gateway 10.254.254.254
      set netmask 255.255.255.0
      set interface "qtn.port7"
      config ip-range
         edit 1
            set start-ip 10.254.254.192
            set end-ip 10.254.254.253
         next
      end
      set timezone-option default
   next
```

```
end
```

Use the following command to view how the quarantine VLAN is applied to the allowed and untagged VLANs on all connected FortiSwitch ports:

```
show switch-controller managed-switch
```

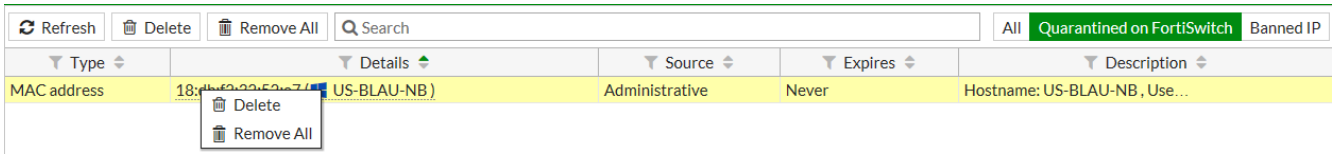
For example:

```
show switch-controller managed-switch

config switch-controller managed-switch
   edit "FS1D483Z15000036"
      set fsw-wan1-peer "port7"
      set fsw-wan1-admin enable
      set version 1
      set dynamic-capability 503
      config ports
         edit "port1"
            set vlan "vsw.port7"
            set allowed-vlans "qtn.port7"
            set untagged-vlans "qtn.port7"
         next
         edit "port2"
            set vlan "vsw.port7"
            set allowed-vlans "qtn.port7"
            set untagged-vlans "qtn.port7"
         next
         edit "port3"
            set vlan "vsw.port7"
            set allowed-vlans "qtn.port7"
            set untagged-vlans "qtn.port7"
         next
         ...
   end
end
```

Releasing MAC addresses from quarantine

Using the FortiGate GUI

1. Go to *Monitor* > *Quarantine Monitor*.
2. Click *Quarantined on FortiSwitch*.
3. Right-click on one of the entries and select *Delete* or *Remove All*.
4. Click *OK* to confirm your choice.



Using the FortiGate CLI

To release MAC addresses from quarantine, you can delete a single MAC address or delete a quarantine entry, which will delete all of the MAC addresses listed in the entry. You can also disable the quarantine feature, which releases all quarantined MAC addresses from quarantine.

To delete a single quarantined MAC address:

```
config user quarantine
   config targets
      edit <quarantine_entry_name>
         config macs
            delete <MAC_address_1>
         end
      end
   end
```

To delete all MAC addresses in a quarantine entry:

```
config user quarantine
   config targets
      delete <quarantine_entry_name>
   end
end
```

To disable the quarantine feature:

```
config user quarantine
   set quarantine disable
end
```

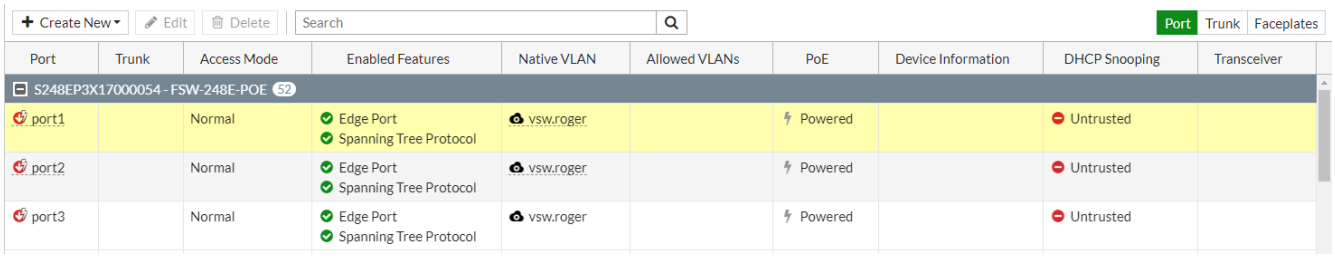
FortiSwitch port features

You can configure the FortiSwitch port feature settings from the FortiGate using the FortiSwitch CLI or web administration GUI.

FortiSwitch ports display

The *WiFi & Switch Controller* > *FortiSwitch Ports* page displays port information about each of the managed switches.

The following figure shows the display for a FortiSwitch 248E-FPOE:



Select *Faceplates* to get the following information:

- active ports (green)
- PoE-enabled ports (blue rectangle)
- FortiLink port (link icon)

If you device has PoE, the Faceplates page displays the total power budget and the actual power currently allocated.

The allocated power displays a blue bar for the used power (currently being consumed) and a green bar for the reserved power (power available for additional devices on the POE ports).

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
- Enabled features
- Native VLAN
- Allowed VLANs
- PoE status
- Device information
- DHCP snooping status
- Transceiver information

Configuring ports using the GUI

You can use the *WiFi & 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 to network access control (NAC) or normal
- 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)

Resetting PoE-enabled ports

If you need to reset PoE-enabled ports, go to *WiFi & Switch Control* > *FortiSwitch Ports*, right-click on one or more PoE-enabled ports and select *Reset PoE* from the context menu.

You can also go to *WiFi & Switch Control* > *Managed FortiSwitch* and click on a port icon for the FortiSwitch of interest. In the FortiSwitch Ports page, right-click on one or more PoE-enabled ports and select *Reset PoE* from the context menu.

Configuring ports using the FortiGate CLI

You can configure the following FortiSwitch port settings using the FortiGate CLI:

- Configuring port speed and status on page 100
- Configure a VLAN on the port (see Configure VLANs)
- Sharing FortiSwitch ports between VDOMs on page 100
- Dynamic MAC address learning on page 103
- Configuring the DHCP trust setting on page 106
- Configuring PoE on page 106
- Configuring edge ports on page 107
- Configuring STP on page 108
- Configuring STP root guard on page 110
- Configuring STP BPDU guard on page 110
- Configuring loop guard on page 112
- Configuring LLDP settings on page 112
- Configuring IGMP snooping settings on page 113
- Configuring sFlow on page 113
- Configuring dynamic ARP inspection (DAI) on page 114

- Configuring FortiSwitch port mirroring on page 115
- Configuring FortiSwitch split ports (phy-mode) in FortiLink mode on page 117

Configuring port speed and status

Use the following commands to set port speed and other base port settings:

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

Sharing FortiSwitch ports between VDOMs

Virtual domains (VDOMs) are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units. VDOMs provide separate security domains that allow separate zones, user authentication, security policies, routing, and VPN configurations.

FortiSwitch ports can now be shared between VDOMs.

Starting in FortiOS 6.2.0, the following features are supported on FortiSwitch ports shared between VDOMs:

- POE pre-standard detection (on a per-port basis if the FortiSwitch model supports this feature)
- Learning limit for dynamic MAC addresses on ports, trunks, and VLANs (if the FortiSwitch unit supports this feature)
- QoS egress CoS queue policy (if the FortiSwitch unit supports this feature)
- Port security policy

The following example shows how to share FortiSwitch ports between VDOMs:

1. In the tenant VDOM named `bbb`, create a VLAN interface using the following CLI commands (not supported in the GUI):

```
FG5H0E3917900081 (bbb) #
   config system interface
      edit "bbb-vlan99"
         set vdom "bbb"
         set allowaccess ping
```

```
        set device-identification enable
        set role lan
        set snmp-index 58
        set switch-controller-dhcp-snooping enable
        set interface "flink-lag" // this is the FortiLink interface in the root VDOM
        set vlanid 99
    next
  end

config switch-controller global
  set default-virtual-switch-vlan "bbb-vlan99"
end
```

2. Go back to the root VDOM. Pick a switch port to share between VDOMs, port10 in this case.

```
FG5H0E3917900081 (vdom) # edit root
current vf=root:0
FG5H0E3917900081 (root) # config switch-controller managed-switch
FG5H0E3917900081 (managed-switch) # edit S548DF4K15000276
FG5H0E3917900081 (S548DF4K15000276) # config ports
FG5H0E3917900081 (ports) # edit port10
FG5H0E3917900081 (port10) # set export-to bbb
```

If you want to use the virtual-pool feature instead:

```
FG5H0E3917900081 (root) # config switch-controller virtual-port-pool
  edit "bbb-pool"
    set description "bbb-vlan-pool"
  end

FG5H0E3917900081 (root) # config switch-controller managed-switch
FG5H0E3917900081 (managed-switch) # edit S548DF4K15000276
FG5H0E3917900081 (S548DF4K15000276) # config port
FG5H0E3917900081 (ports) # edit port11
FG5H0E3917900081 (port11) # set export-to-pool bbb-pool
```

3. Go back to the bbb VDOM to claim port11 because it is in the virtual pool but not directly exported to the VDOM yet. (The administrator might want to pre-assign some ports in the tenant VDOM and let the tenant VDOM administrator claim them before they are used.)

```
FG5H0E3917900081 (bbb) # execute switch-controller virtual-port-pool request
    S548DF4K15000276 port11
FG5H0E3917900081 (bbb) # config switch-controller managed-switch // The switch port is
    now in the bbb VDOM even though there is no FortiLink interface in the bbb VDOM.
FG5H0E3917900081 (managed-switch) # show
config switch-controller managed-switch
  edit "S548DF4K15000276"
    set poe-detection-type 1
    set type virtual
    set owner-vdom "root"
    config ports
      edit "port10"
        set poe-capable 1
        set vlan "bbb-vlan99"
      next
      edit "port11"
```

```
            set poe-capable 1
            set vlan "bbb-vlan99"
         next
      end
   next
end
```

4. Check your configuration on the root VDOM:

```
FG5H0E3917900081 (port10) # show
config ports
   edit "port10"
      set poe-capable 1
      set export-to "bbb"
   next
end

FG5H0E3917900081 (port11) # show
config ports
   edit "port11"
      set poe-capable 1
      set export-to-pool "bbb-pool"
      set export-to "bbb"
   next
end
```

5. Check your configuration on the tenant VDOM:

```
FG5H0E3917900081 (ports) # show
config ports
   edit "port10"
      set poe-capable 1
      set vlan "bbb-vlan99"
   next
   edit "port11"
      set poe-capable 1
      set vlan "bbb-vlan99"
   next
end
```

You can create your own export tags using the following CLI commands:

```
config switch-controller switch-interface-tag
   edit <tag_name>
end
```

Use the following CLI command to list the contents of a specific VPP:

```
execute switch-controller virtual-port-pool show-by-pool <VPP_name>
```

Use the following CLI command to list all VPPs and their contents:

```
execute switch-controller virtual-port-pool show
```

NOTE: Shared ports do not support the following features:

- LLDP
- STP

- BPDU guard
- Root guard
- DHCP snooping
- IGMP snooping
- MCLAG
- Quarantines

NOTE: After you export a switch port to a pool, if you need to export the switch port to a different pool, you need to exit/abort and then re-enter into the FortiSwitch CLI port configuration.

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).

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 save:

```
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:

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

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 PoE

The following PoE CLI commands are available starting in FortiSwitchOS 3.3.0.

Enable 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
```

Reset 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>
```

Display general PoE status

```
get switch-controller <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
```

Configuring edge ports

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

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

Starting with FortiSwitch Release 3.4.2, 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.

NOTE: STP is not supported between a FortiGate unit and a FortiSwitch unit in FortiLink mode.

To configure global STP settings, see Configure STP settings on page 85.

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:

```
FG100D3G15817028 # 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:

```
FG100D3G15817028 # 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 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 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
```

Configuring IGMP snooping settings

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 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 FortiGate 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
   set collector-ip <x.x.x.x>
   set 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 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>
           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>
```

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 remote SPAN (RSPAN) or encapsulated RSPAN (ERSPAN) allows you to send the collected packets across layer-2 domains for analysis. You can have multiple RSPAN sessions but only one ERSPAN session.

In RSPAN mode, traffic is encapsulated in VLAN 4092. The FortiSwitch unit assigns the uplink port and the dst port. The switching functionality is enabled on the dst interface when mirroring.

NOTE: RSPAN is supported on FSR-112D-POE and on platforms 2xx and higher.

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 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
```

To configure FortiSwitch RSPAN:

```
config switch-controller traffic-sniffer
   set mode rspan
   config target-mac
      edit <MM:MM:MM:SS:SS:SS> // mirror traffic sent FROM this source MAC address
         set description <string>
      end
   config target-ip
      edit <xxx.xxx.xxx.xxx> // mirror traffic sent FROM this source IP address
         set description <string>
      end
   config target-port
      edit <FortiSwitch_serial_number>
         set description <string>
         set in-ports <portx porty portz ...> // mirror any traffic sent to these ports
         set out-ports <portx porty portz ...> // mirror any traffic sent from these ports
      end
   end
```

For example:

```
config switch-controller traffic-sniffer
   set mode rspan
   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 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 FortiSwitch split ports (phy-mode) in FortiLink mode

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

FortiLink mode supports the FortiSwitch split-port configuration:

- Configuring split ports on a previously discovered FortiSwitch unit on page 118
- Configuring split ports with a new FortiSwitch unit on page 118
- Configuring ports using the FortiGate CLI on page 99

Notes

- Split ports are not configured for pre-configured FortiSwitch units.
- Splitting ports is supported on the following FortiSwitch models:
  - 3032D (ports 5 to 28 are splittable)
  - 524D, 524D-FPOE (ports 29 and 30 are splittable)
  - 548D, 548D-FPOE (ports 53 and 54 are splittable)
  - 1048E (In the 4 x 100G configuration, ports 49, 50, 51, and 52 are splittable as 4 x 25G.)
  - 1048E (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 3032D and the 1048E models have enough ports to encounter this limit.

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 118.
2. Restart the FortiSwitch unit.
3. Remove the FortiSwitch from being managed:
```
config switch-controller managed-switch
   delete <FortiSwitch_serial_number>
end
```
4. Discover the FortiSwitch unit.
5. Authorize the FortiSwitch unit.

Configuring split ports with a new FortiSwitch unit

1. Discover the FortiSwitch unit.
2. Authorize the FortiSwitch unit.
3. Restart the FortiSwitch unit.
4. On the FortiSwitch unit, configure the split ports. See Configuring a split port on the FortiSwitch unit on page 118.
5. Restart the FortiSwitch unit.
6. Remove the FortiSwitch from being managed:
```
config switch-controller managed-switch
   delete <FortiSwitch_serial_number>
end
```
7. Discover the FortiSwitch unit.
8. Authorize the FortiSwitch unit.

Configuring a split port on the FortiSwitch unit

Use the following commands to configure a split port:

```
config switch phy-mode
   set port-configuration <default | disable-port54 | disable-port41-48 | 4x100G | 6x40G>
   set <port_name>-phy-mode <1x40G | 4x10G>
   ...
   (one entry for each port that supports split port)
end
```

The following settings are available:

- `disable-port54`—For 548D and 548D-FPOE, only port 53 is splittable; port 54 is unavailable.
- `disable-port41-48`—For 548D and 548D-FPOE, ports 41 to 48 are unavailable, but you can configure ports 53 and 54 in split-port 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.

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
```

FortiSwitch port security policy

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 the FortiGate.

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.

Optionally, you can configure a guest VLAN for unauthorized users. Alternatively, you can specify a VLAN for users whose authentication was unsuccessful.

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 chapter covers the following topics:

Increased 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:

Model	Total number of devices supported per switch
108	80
112	120
124/224/424/524/1024	240
148/248/448/548/1048	480
3032	320

Configure the 802.1X settings for a virtual domain

To configure the 802.1X security policy for a virtual domain, use the following commands:

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

Option	Description
`set link-down-auth`	If a link is down, this command determines the authentication state. Choosing `set-auth` sets the interface to unauthenticated when a link is down, and reauthentication is needed. Choosing `no-auth` means that the interface does not need to be reauthenticated when a link is down.
`set reauth-period`	This command sets how often reauthentication is needed. The range is 1-1440 minutes. The default is 60 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.
`set max-reauth-attempt`	This command sets the maximum number of reauthentication attempts. The range is 1-15. The default is 3. Setting the value to 0 disables reauthentication.

Override the virtual domain settings

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

Using the FortiGate GUI

To override the 802.1X settings for a virtual domain:

1. Go to *WiFi & Switch Controller* > *Managed FortiSwitch*.
2. Click on a FortiSwitch faceplate and select *Edit*.
3. In the Edit Managed FortiSwitch page, move the *Override 802-1X settings* slider to the right.
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. Select *OK*.

Using the FortiGate CLI

To override the 802.1X settings for a virtual domain, use the following commands:

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

For a description of the options, see Configure the 802.1X settings for a virtual domain.

Define an 802.1X security policy

You can define multiple 802.1X security policies.

Using the FortiGate GUI

To create an 802.1X security policy:

1. Go to *WiFi & Switch Controller* > *FortiSwitch Security Policies*.
2. Select *Create New*.
3. Enter a name for the new FortiSwitch security policy.
4. For the security mode, select *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 FortiGate 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
   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.
`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 disable authentication fail VLAN on this interface to allow restricted access for users who fail to access the guest VLAN.

Option	Description
`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.

Apply an 802.1X security policy to a FortiSwitch port

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

Using the FortiGate GUI

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

1. Go to *WiFi & Switch Controller* > *FortiSwitch Ports*.
2. Select the + next to a FortiSwitch unit.
3. In the Security Policy column for a port, click + to select a security policy.
4. Select *OK* to apply the security policy to that port.

Using the FortiGate 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
```

Test 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, use the following commands:

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

```
end
```

Restrict 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
```

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 FortiGate RADIUS single sign-on:

- START—The FortiSwitch 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—FortiSwitch will send this message when the switch is turned on.
- OFF—FortiSwitch will send this message when the switch is shut down.

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

```
config user radius
   edit <RADIUS_server_name>
      set acct-interim-interval <seconds>
      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.

Starting in FortiSwitchOS 6.2.1, 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

Error Cause	Error Code	Description
		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 FortiOS, 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.

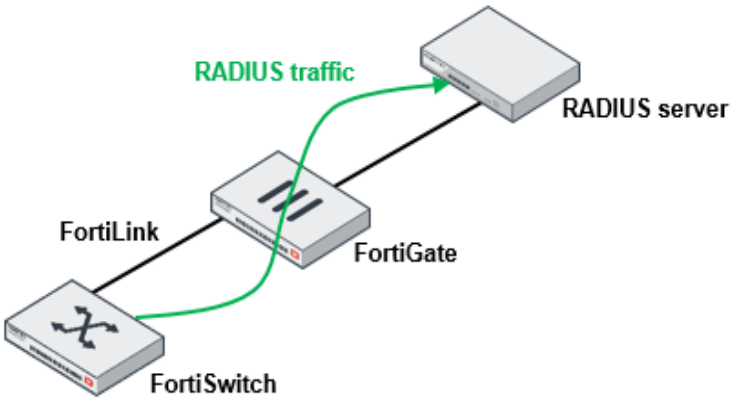
Variable	Description
server <server_name_IPv4>	Enter the domain name or IPv4 address for the RADIUS server. There is no default.

Example: RADIUS CoA

The following example uses the FortiOS 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
```

802.1x authentication deployment example



To control network access, you can configure 802.1x authentication from a FortiGate unit managing FortiSwitch units. A supplicant connected to a port on the switch must be authenticated by a RADIUS/Diameter server to gain access to the network.

To use the RADIUS server for authentication, you must configure the server before configuring the users or user groups on the FortiSwitch unit. You also need a firewall policy on the FortiGate unit to allow traffic from the FortiSwitch unit to the RADIUS server.

To create a firewall policy to allow the FortiSwitch unit to reach the RADIUS server:

```
config firewall policy
   edit 1
      set name "fortilink-to-radius"
      set srcintf "fortilink"
      set dstintf "accounting-server"
      set action accept
      set service "ALL"
      set nat enable
   end
```

To create a group for users who will be authenticated by 802.1x:

```
config user radius
   edit "dot1x-radius"
      set server "192.168.174.10"
      set secret ENC ***
      set radius-port 1812
      config accounting-server
         edit 1
            set status enable
            set server "192.168.174.10"
            set secret ENC ***
            set port 1813
         next
      end
   next
end

config user group
   edit "radius users"
      set member "dot1x-radius"
   next
end
```

To create an 802.1X security policy:

You can create an 802.1X security policy using the FortiGate GUI by going to *WiFi & Switch Controller* > *FortiSwitch Security Policies* and selecting *Create New*.

```
config switch-controller security-policy 802-1X
   edit "802-1X-policy-default"
      set security-mode 802.1X-mac-based
      set user-group "dot1x-local"
      set mac-auth-bypass enable
      set eap-passthru enable
      set guest-vlan enable
      set guest-vlan-id "guest-VLAN"
      set auth-fail-vlan enable
      set auth-fail-vlan-id "auth-fail-VLAN"
      set radius-timeout-overwrite disable
   next
end
```

To configure the global 802.1X settings:

```
config switch-controller 802-1X-settings
   set link-down-auth no-action
   set reauth-period 90
   set max-reauth-attempt 4
end
```

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

You can apply an 802.1X security policy to a managed FortiSwitch port using the FortiGate GUI by going to *WiFi & Switch Controller* > *FortiSwitch Ports*.

```
config switch-controller managed-switch
   edit S548DN4K16000360
      config ports
         edit "port1"
            set dhcp-snooping trusted
            set dhcp-snoop-option82-trust enable
            set port-security-policy "802-1X-policydefault"
         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 the FortiGate unit 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.
- Starting in FortiSwitch 6.2.0, 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*.

Additional capabilities

This chapter covers the following topics:

Execute custom FortiSwitch scripts

From the FortiGate unit, you can execute a custom script on a managed FortiSwitch unit. The custom script contains generic FortiSwitch commands.

NOTE: FortiOS 5.6.0 introduces additional capabilities related to the managed FortiSwitch unit.

Create a custom script

Use the following syntax to create a custom script from the FortiGate unit:

```
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
```

Execute 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 the FortiGate unit 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
```

Bind 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
```

View and upgrade 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. The FortiGate unit will suggest an upgrade when a new version is available in FortiGuard.

Using the FortiGate web interface

To view the FortiSwitch firmware version:

1. Go to *WiFi & Switch Controller* > *Managed FortiSwitch*.
2. In the main panel, select the FortiSwitch faceplate and click **Edit**.
3. In the *Edit Managed FortiSwitch* panel, the *Firmware* section displays the current build on the FortiSwitch.

To upgrade the firmware on multiple FortiSwitch units at the same time:

1. Go to *WiFi & Switch Controller* > *Managed FortiSwitch*.
2. Select the faceplates of the FortiSwitch units that you want to upgrade.
3. Click *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 CLI

Use the following command to stage a firmware image on all FortiSwitch units:

```
diagnose switch-controller switch-software stage all <image id>
```

Use the following command to upgrade the firmware image on one FortiSwitch unit:

```
diagnose 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
```

From your FortiGate 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
```

FortiSwitch log settings

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

Exporting logs to FortiGate

You can enable and disable whether the managed FortiSwitch units export their logs to the FortiGate unit. The setting is global, and the default setting is enabled. Starting in FortiOS 5.6.3, more details are included in the exported FortiSwitch logs.

To allow a level of filtering, the FortiGate unit 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 a FortiGate unit, 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
```

FortiSwitch per-port device visibility

In the FortiGate GUI, *User & Device* > *Device List* displays a list of devices attached to the FortiSwitch ports. For each device, the table displays the IP address of the device and the interface (FortiSwitch name and port).

From the CLI, the following command displays information about the host devices:

```
diagnose switch-controller mac-cache show <switch-id>
```

FortiGate CLI support for FortiSwitch features (on non-FortiLink ports)

You can configure the following FortiSwitch features from the FortiGate CLI.

Configuring a link aggregation group (LAG)

You can configure a link aggregation group (LAG) for non-FortiLink ports on a FortiSwitch. You cannot configure ports from different FortiSwitch units in one LAG.

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <trunk name>
            set type trunk
            set mode {static | lacp} Link Aggregation mode
            set bundle (enable | disable)
            set min-bundle <int>
            set max-bundle <int>
            set members < port1 port2 ...>
         next
      end
   end
end
```

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 FortiOS 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 FortiOS 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
```

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 of a managed FortiSwitch unit:

```
diagnose switch-controller switch-info port-stats <managed FortiSwitch device ID> <port_
      name>
```

For example:

```
FG100D3G15817028 (global) # diagnose switch-controller switch-info port-stats
     S524DF4K15000024 port8
Vdom: dmgmt-vdom
Vdom: roort
Vdom: root

S524DF4K15000024:
Port(port8) is Admin up, line protocol is down
Interface Type is Serial Gigabit Media Independent Interface(SGMII/SerDes)
Address is 08:5B:0E:F1:95:ED, loopback is not set
MTU 9216 bytes, Encapsulation IEEE 802.3/Ethernet-II
half-duplex, 0 Mb/s, link type is auto
input : 0 bytes, 0 packets, 0 errors, 0 drops, 0 oversizes
0 unicasts, 0 multicasts, 0 broadcasts, 0 unknowns
output : 0 bytes, 0 packets, 0 errors, 0 drops, 0 oversizes
0 unicasts, 0 multicasts, 0 broadcasts
0 fragments, 0 undersizes, 0 collisions, 0 jabbers


Vdom: vdom-1
```

To reset the port statistics counters of a managed FortiSwitch unit:

```
diagnose switch-controller trigger reset-hardware-counters <managed FortiSwitch device ID>
     <port_name>
```

For example:

```
FG100D3G15817028 (global) # 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 FortiGate. 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:

```
FG100D3G15817028 (global) # diagnose switch-controller trigger restore-hardware-counters
     S524DF4K15000024 port10-port11,internal
```

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: The FortiGate unit 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.

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 | random-early-detection}
         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>
```

Synchronizing the FortiGate unit with the managed FortiSwitch units

You can synchronize the FortiGate unit 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 a FortiGate unit with a managed FortiSwitch unit:

```
diagnose switch-controller trigger config-sync <FortiSwitch_serial_number>
```

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 FortiGate unit. The replacement FortiSwitch unit will inherit the configuration of the FortiSwitch unit that it replaces. The failed FortiSwitch unit is no longer managed by a FortiGate unit 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 avoide any traffic loops. The other interfaces should be connected only to the swithc that is fully managed the FortiGate unit with the correct configuration.

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 View and upgrade the FortiSwitch firmware version on page 134.
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 the FortiGate unit, go to *WiFi & Switch Controller* > *Managed FortiSwitch*.
7. Select the faceplate of the failed FortiSwitch unit.
8. Select *Deauthorize*.
9. Connect the replacement FortiSwitch unit to the FortiGate unit that was managing the failed FortiSwitch unit.
10. If the failed FortiSwitch unit was part of a VDOM, enter the following commands:

```
config vdom
  edit <VDOM_name>
    execute replace-device fortiswitch <failed_FortiSwitch_serial_number> <replacement_
        FortiSwitch_serial_number>
```

For example:

```
config vdom
   edit vdom_new
      execute replace-device fortiswitch S124DN3W16002025 S124DN3W16002026
```

If the failed FortiSwitch unit was not part of a VDOM, 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.

To rename the MCLAG-ICL trunk:

Changing the name of the MCLAG-ICL trunk must be done on both the FortiGate unit and the MCLAG-ICL switches. You need a maintenance window for the change.

1. Shut down the FortiLink interface on the FortiGate unit.
   a. On the FortiGate unit, execute the `show system interface` command. For example:

```
FG3K2D3Z17800156 # 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:

```
FG3K2D3Z17800156 # config system interface
FG3K2D3Z17800156 (interface) # edit port48
FG3K2D3Z17800156 (port48) # set status down
FG3K2D3Z17800156 (port48) # next // repeat for each member port
FG3K2D3Z17800156 (interface) # edit port45
FG3K2D3Z17800156 (port45) # set status down
FG3K2D3Z17800156 (port45) # end
```

   d. Verify that FortiLink is down with the `exec switch-controller get-conn-status` command. For example:

```
FG3K2D3Z17800156 # 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 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 the FortiGate unit. Enter the `config system interface`, `edit <interface-member-port>`, `set status up`, `next`, and `end` commands. For example:

```
FG3K2D3Z17800156 # config system interface
 FG3K2D3Z17800156 (interface) # edit port45
 FG3K2D3Z17800156 (port45) # set status up
 FG3K2D3Z17800156 (port45) # next // repeat on all member ports
 FG3K2D3Z17800156 (interface) # edit port48
 FG3K2D3Z17800156 (port48) # set status up
 FG3K2D3Z17800156 (port48) # next
 FG3K2D3Z17800156 (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.

FortiSwitch network access control

You can configure a FortiSwitch network access control (NAC) policy within FortiOS that applies to devices within a specific VLAN. You can create NAC policies for user groups or for devices.

NOTE: The FortiSwitch NAC settings must be configured before defining a NAC policy. You can either manually configure the NAC settings or use the NAC wizard. See Configuring the FortiSwitch NAC settings on page 149 and Using the NAC wizard on page 154.

Summary of the procedure

1. Define a FortiSwitch NAC VLAN.
2. Configure the FortiSwitch NAC settings.
3. Create a FortiSwitch user or device NAC policy.
4. View the devices that match the NAC policy.

Defining a FortiSwitch NAC VLAN

A FortiSwitch NAC VLAN includes all the devices that you want to manage with a specific FortiSwitch NAC policy. By default, there are six VLAN templates:

- *default*—This VLAN is assigned to all switch ports when the FortiSwitch unit is first discovered.
- *quarantine*—This VLAN contains quarantined traffic.
- *rspan*—This VLAN contains RSPAN and ERSPAN mirrored traffic.
- *voice*—This VLAN is dedicated for voice devices.
- *video*—This VLAN is dedicated for video devices.
- *onboarding*—This VLAN is for NAC onboarding devices.

You can use the default onboarding VLAN, edit it, or create a new NAC VLAN. If you want to use the default onboarding NAC VLAN, specify it when you configure the FortiSwitch NAC settings. If you want to edit the default onboarding VLAN or create a new NAC VLAN, use the following procedures.

Creating a NAC VLAN

Using the GUI:

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

Interface 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 *Admission access* options as required.
4. Select *OK*.

Using the CLI:

```
config system interface
   edit <vlan name>
      set vlanid <1-4094>
      set color <1-32>
      set interface <FortiLink-enabled interface>
   end
```

Editing a NAC VLAN

You can edit the default `onboarding` NAC VLAN.

Using the GUI:

1. Go to *WiFi & Switch Controller* > *FortiSwitch VLANs*.
2. Select the `onboarding` NAC VLAN.
3. Select *Edit*.
4. Make your changes.
5. Select *OK* to save your changes.

Using the CLI:

```
config switch-controller initial-config template
   edit onboarding
      set vlanid <1-4094>
      set allowaccess {ping | https |ssh | snmp | http | telnet | fgfm | radius-acct |
           probe-response | fabric | ftm}
      set auto-ip {enable | disable}
      set dhcp-server {enable | disable}
   end
```

Configuring the FortiSwitch NAC settings

NOTE: The FortiSwitch NAC settings must be configured before defining a NAC policy. You can either manually configure the NAC settings or use the NAC wizard. See Using the NAC wizard on page 154.

The local mode uses the local port-level settings of managed FortiSwitch units. The global mode applies the NAC to all managed FortiSwitch ports. Be default, the mode is local.

You can set how many minutes that NAC devices are allowed to be inactive. By default, NAC devices can be inactive for 15 minutes. The range of values is 0 to 1 440 minutes. If you set the inactive-timer to 0, there is no limit to how long the NAC devices can be inactive for.

When NAC devices are discovered, they are assigned to the NAC onboarding VLAN. You can specify the default `onboarding` VLAN or specify another existing VLAN. By default, there is no NAC onboarding VLAN assigned.

When NAC devices are discovered and match a NAC policy, they are automatically authorized by default.

When NAC mode is configured on a port, the link of a switch port goes down and then up by default, which restarts the DHCP process for that switch.

When a link goes down, the NAC devices are cleared from all switch ports by default.

Configuring NAC on a global level

Using the GUI:

1. Go to *WiFi & Switch Controller* > *FortiLink Interface*.
2. Move the *NAC Settings* slider to expand the NAC Settings section.
3. Select the onboarding VLAN from the Onboarding VLAN drop-down list. The default onboarding VLAN is *onboarding*.
4. Move the *Bounce port* slider to enable it if you want the link to go down and then up when the NAC mode is configured on the port.
5. Select *All* or *Specify* to apply NAC policies to all FortiSwitch ports.
6. Select *Apply* to save your changes.

Using the CLI:

```
config switch-controller nac-settings
   edit <name_of_this_NAC_configuration>
      set mode global
      set inactive-timer <integer>
      set onboarding-vlan <string>
      set auto-auth {enable | disable}
      set bounce-nac-port {enable | disable}
      set link-down-flush {enable | disable}
   end
```

Configuring NAC on a local level

Using the GUI:

1. Go to *WiFi & Switch Controller* > *FortiLink Interface*.
2. Move the *NAC Settings* slider to expand the NAC Settings section.

3. Select the onboarding VLAN from the Onboarding VLAN drop-down list. The default onboarding VLAN is *onboarding*.
4. Move the *Bounce port* slider to enable it if you want the link to go down and then up when the NAC mode is configured on the port.
5. Select *Specify* to apply NAC policies to specific FortiSwitch ports.
6. Select one or more FortiSwitch units and specify which FortiSwitch ports to apply the NAC policies to.
7. Select *Apply* to save your changes.

Using the CLI:

```
config switch-controller nac-settings
   edit <name_of_this_NAC_configuration>
      set mode local
      set inactive-timer <integer>
      set onboarding-vlan <string>
      set auto-auth {enable | disable}
      set bounce-nac-port {enable | disable}
      set link-down-flush {enable | disable}
   end

config switch-controller managed-switch
      edit <FortiSwitch_serial_number>
         config ports
            edit <port_name>
               set access-mode nac
            next
         end
      next
   end
```

Using the GUI:

1. Go to *WiFi & Switch Controller* > *FortiSwitch Ports*.
2. Right-click a port.
3. Select *Access Mode* > *NAC*.

Defining a FortiSwitch NAC policy

A user NAC policy matches devices that are assigned to the specified user group and then assigns a specific VLAN to those devices or applies port-level settings to those devices.

NOTE: The FortiSwitch NAC settings must be configured before defining a FortiSwitch NAC policy. You can either manually configure the NAC settings or use the NAC wizard. See Configuring the FortiSwitch NAC settings on page 149 and Using the NAC wizard on page 154.

Creating a user NAC policy

A user NAC policy matches devices that are assigned to the specified user group and then assigns a specific VLAN to those devices or applies port-level settings to those devices. You can also use the CLI to create a port policy and MAC policy.

Using the GUI:

1. Go to *WiFi & Switch Controller* > *FortiSwitch NAC Policies*.
2. Select *Create New*.
3. In the Name field, enter a name for the NAC policy.
4. Select which FortiSwitch units to apply the NAC policy to or select *All*.
5. Select *User* for the category.
6. Select which user group that devices must belong to.
7. If you want to assign a specific VLAN to a device assigned to the specified user group, select *Assign VLAN*, enter the VLAN identifier, and select *Allow* or *Block*.
8. If you want to assign port-level settings for devices assigned to the specific user group, select *Apply Port Specific Settings*. You can specify the LLDP profile, QoS profile, 802.1x policy, and VLAN policy.
9. Select *OK* to create the new NAC policy.

Using the CLI:

```
config user nac-policy
   edit <policy_name>
      set description <description_of_policy>
      set category user
      set status enable
      set user-group <name_of_user_group>
      set switch-fortilink <FortiLink_interface>
      set switch-scope <list_of_managed_FortiSwitch_serial_numbers>
      set switch-auto-auth {enable | disable}
      set switch-port-policy <switch_port_policy>
      set switch-mac-policy <switch_mac_policy>
   end
```

Creating a device NAC policy

A device NAC policy matches devices with the specified criteria and then assigns a specific VLAN to those devices or applies port-level settings to those devices. You can specify the MAC address, hardware vendor, device family, type, and operating system for the devices to match. You can also use the CLI to create a port policy and MAC policy.

By default, there is a default device NAC policy, `Onboarding VLAN`, which uses the default `onboarding` NAC VLAN. You can use the default `Onboarding VLAN` policy, edit it, or create a new NAC policy.

Using the GUI:

1. Go to *WiFi & Switch Controller* > *FortiSwitch NAC Policies*.
2. Select *Create New*.
3. In the Name field, enter a name for the NAC policy.
4. Select which FortiSwitch units to apply the NAC policy to or select *All*.
5. Select *Device* for the category.
6. If you want the device to match a MAC address, move the MAC Address slider and enter the MAC address to match.
7. If you want the device to match a hardware vendor, move the Hardware Vendor slider and enter the name of the hardware vendor to match.

8. If you want the device to match a device family, move the Device Family slider and enter the name of the device family to match.
9. If you want the device to match a device type, move the Type slider and enter the device type to match.
10. If you want the device to match an operating system, move the Operating System slider and enter the operating system to match.
11. If you want the device to match a user, move the User slider and enter the user name to match.
12. If you want to assign a specific VLAN to the device that matches the specified criteria, select *Assign VLAN*, enter the VLAN identifier, and select *Allow* or *Block*.
13. If you want to assign port-level settings to the device that matches the specified criteria select *Apply Port Specific Settings*. You can specify the LLDP profile, QoS profile, 802.1x policy, and VLAN policy.
14. Select *OK* to create the new NAC policy.

Using the CLI:

```
config user nac-policy
   edit <policy_name>
      set description <description_of_policy>
      set category device
      set status enable
      set mac <MAC_address>
      set hw-vendor <hardware_vendor>
      set type <device_type>
      set family <device_family>
      set os <operating_system>
      set hw-version <hardware_version>
      set sw-version <software_version>
      set host <host_name>
      set user <user_name>.
      set src <source>
      set switch-fortilink <FortiLink_interface>
      set switch-scope <list_of_managed_FortiSwitch_serial_numbers>
      set switch-auto-auth {enable | disable}
      set switch-port-policy <switch_port_policy>
      set switch-mac-policy <switch_mac_policy>
   end
```

Creating a MAC policy

When the NAC policy is applied to managed FortiSwitch units, the MAC policy is also applied. You can specify which VLAN is applied and which traffic policy is used, enable or disable packet count, and drop or allow NAC device traffic.

```
config switch-controller mac-policy
   edit <MAC_policy_name>
      set description <policy_description>
      set fortilink <FortiLink_interface>
      set vlan <VLAN_name>
      set traffic-policy <traffic_policy_name>
      set count {enable | disable}
      set drop {enable | disable}
   next
end
```

Creating a port policy

When the NAC policy is applied to managed FortiSwitch units, the port policy is also applied. You can specify which LLDP profile, QoS policy, 802.1x policy, and VLAN policy are used on the port.

```
config switch-controller port-policy
   edit <port_policy_name>
      set description <policy_description>
      set fortilink <FortiLink_interface>
      set lldp-profile <LLDP_profile>
      set qos-policy <QoS_policy>
      set 802-1x <802.1x_policy>
      set vlan-policy <VLAN_policy>
      set bounce-port-link {enable | disable}
   next
end
```

Creating a VLAN policy

When the port policy is applied to a managed FortiSwitch port, the VLAN policy is also applied. You can specify the native VLAN to be applied, the allowed VLANs, and the untagged VLANs. You can enable or disable all defined VLANs and select whether to discard untagged or tagged frames or to not discard any frames.

```
config switch-controller vlan-policy
   edit <VLAN_policy_name>
      set description <policy_description>
      set fortilink <FortiLink_interface>
      set vlan <VLAN_name>
      set allowed-vlans <lists_of_VLAN_names>
      set untagged-vlans <lists_of_VLAN_names>
      set allowed-vlans-all {enable | disable}
      set discard-mode {none | all-untagged | all-tagged}
   next
end
```

Viewing the devices that match the NAC policy

Using the GUI:

1. Go to *WiFi & Switch Controller* > *FortiSwitch NAC Policies*.
2. Select *View Matched Devices*.
3. Select *Refresh* to update the results.

Using the CLI:

To show known NAC devices with a known location that match a NAC policy:

```
diagnose switch-controller nac-device known
```

To show pending NAC devices with an unknown location that match a NAC policy:

```
diagnose switch-controller nac-device pending
```

Using the NAC wizard

The NAC wizard helps with configuring the FortiSwitch NAC settings and defining a FortiSwitch NAC VLAN. If you do not want to manually configure the FortiSwitch NAC settings, use the NAC wizard instead.

NOTE: The FortiSwitch NAC settings must be configured before defining a NAC policy.

1. Go to *WiFi & Switch Controller* > *FortiSwitch NAC Policies*.
2. Select *Configure NAC Settings*.
3. Select the onboarding VLAN from the Onboarding VLAN drop-down list. The default onboarding VLAN is *onboarding*.
4. Move the *Bounce port* slider to enable it if you want the link to go down and then up when the NAC mode is configured on the port.
5. Select *All* or *Specify* to apply NAC policies to all FortiSwitch ports or to specific FortiSwitch ports.
6. If you selected *Specify*, select one or more FortiSwitch units and specify which FortiSwitch ports to apply the NAC policies to.
7. Select *Next*.
8. Select one of the default NAC VLANs to be the onboarding VLAN, create a new NAC VLAN, or edit one of the default NAC VLANs. The default onboarding VLAN is `onboarding`. See Creating a NAC VLAN on page 148 and Editing a NAC VLAN on page 148.
9. Select *Submit*.

Configuring IoT detection

Starting in FortiOS 6.4, FortiSwitch units can use a new FortiGuard service to identify Internet of things (IoT) devices. FortiOS can use the identified devices for storage and display. You can use the FortiOS CLI to configure the IoT detection.

Each detected MAC address of an IoT device has a confidence level assigned to it. If the confidence level is less than the `iot-weight-threshold` value, the MAC address is scanned. The default value is 1. Set the `iot-weight-threshold` value to 0 to disable IoT detection.

You can control how often a FortiSwitch unit scans for IoT devices. The range of values is 2 to 4,294,967,295 minutes. The default is a scan interval of 60 minutes. Every MAC address will be scanned for a time interval of 60 minutes followed by 60 minutes when it will not be scanned. The start time of every MAC address's 60-minute scan interval is unique. Set the `iot-scan-interval` value to 0 to disable IoT detection.

A MAC address of an IoT device must be detected by the FortiSwitch unit for more than a specified number of minutes before the MAC address is passed along to the FortiGuard service for IoT identification. The default number of minutes is 5. The range of values is 0 to 4,294,967,295 minutes. Set the `iot-holdoff` value to 0 to disable this setting.

If a MAC address entry's last-seen time is greater than the `iot-mac-idle` value, the MAC address entry is not considered for IoT detection. By default, the `iot-mac-idle` value is 1,440 minutes. The range of values is 0 to 4,294,967,295 minutes.

```
config switch-controller system
   set iot-weight-threshold <0-4294967295>
   set iot-scan-interval <2-4294967295>
   set iot-holdoff <0-4294967295>
   set iot-mac-idle <0-4294967295>
end
```

Troubleshooting

If the FortiGate unit does not establish the FortiLink connection with the FortiSwitch unit, perform the following troubleshooting checks.

Check the FortiGate configuration

To use the FortiGate GUI to check the FortiLink interface configuration:

1. In *Network* > *Interfaces*, double-click the interface used for FortiLink.
2. Ensure that *Dedicated to FortiSwitch* is set for this interface.

To use the FortiGate CLI to verify that you have configured the DHCP and NTP settings correctly:

1. Verify that the NTP server is enabled and that the FortiLink interface has been added to the list:
   ```
   show system ntp
   ```
2. Ensure that the DHCP server on the FortiLink interface is configured correctly:
   ```
   show system dhcp
   ```

Check the FortiSwitch configuration

To use FortiSwitch CLI commands to check the FortiSwitch configuration:

1. Verify that the switch system time matches the time on the FortiGate:
   ```
   get system status
   ```
2. Verify that FortiGate has sent an IP address to the FortiSwitch (anticipate an IP address in the range 169.254.x.x):
   ```
   get system interface
   ```
3. Verify that you can ping the FortiGate IP address:
   ```
   execute ping x.x.x.x
   ```

To use FortiGate CLI commands to check the FortiSwitch configuration:

1. Verify that the connections from the FortiGate to the FortiSwitch units are up:
   ```
   execute switch-controller get-conn-status
   ```
2. Verify that ports for a specific FortiSwitch stack are connected to the correct locations:
   ```
   execute switch-controller get-physical-conn standard <FortiSwitch-Stack-ID>
   ```
3. Verify that all the ports for a specific FortiSwitch are up:
   ```
   execute switch-controller get-conn-status <FortiSwitch-device-ID>
   ```

Check FortiSwitch connections

Use the following CLI command for detailed diagnostic information on the managed FortiSwitch connections:

```
execute switch-controller diagnose-connection <FortiSwitch_serial_number>
```

If the FortiSwitch serial number is omitted, only the FortiLink configuration is checked.