FortiOS - FortiSwitch Devices Managed by FortiOS 6.0

Version 6.0.4

October 24, 2019
FortiOS 6.0.4 FortiSwitch Devices Managed by FortiOS 6.0
01-604-481086-20191024

TABLE OF CONTENTS

Change log

Date	Change Description
May 21, 2019	Initial document release for FortiOS 6.0.4
May 23, 2019	Added the “Special notices” section.
July 9, 2019	Updated the “Auto-discovery of the FortiSwitch ports” section.
July 31, 2019	Updated the “Configuring loop guard” section.
August 27, 2019	Updated the “Auto-discovery of the FortiSwitch ports” section.
October 24, 2019	Updated the “Dual-homed servers connected to a pair of FortiSwitch units using an MCLAG” section. Removed the “Banning IP addresses” section.

What’s new in FortiOS 6.0.4

The following list contains new managed FortiSwitch features added in FortiOS 6.0.4. Click on a link to navigate to that section for further information.

- Using quarantines with 802.1x MAC-based authentication on page 65

What’s new in FortiOS 6.0.3

The following list contains new managed FortiSwitch features added in FortiOS 6.0.3. Click on a link to navigate to that section for further information.

- Increased number of devices supported per port for 802.1x MAC-based authentication on page 88

What’s new in FortiOS 6.0.1

The following list contains new managed FortiSwitch features added in FortiOS 6.0.1. Click on a link to navigate to that section for further information.

- Logging violations of the MAC address learning limit on page 77
- Test 802.1x authentication with monitor mode on page 92
- Check FortiSwitch connections on page 108
- CLI changes for quarantining MAC addresses (see Using the FortiGate CLI on page 63)
- CLI changes for releasing MAC addresses from quarantine (see Using the FortiGate CLI on page 69)

What’s new in FortiOS 6.0.0

The following list contains new managed FortiSwitch features added in FortiOS 6.0. Click on a link to navigate to that section for further information.

- Limiting the number of learned MAC addresses on a FortiSwitch interface on page 76
- Sharing FortiSwitch ports between VDOMs on page 73
- Configuring sFlow on page 85
- Restrict the type of frames allowed through IEEE 802.1Q ports on page 92
- Configuring Dynamic ARP inspection (DAI) on page 86
- Configuring FortiSwitch port mirroring on page 87
- Quarantining MAC addresses (see Using the FortiGate CLI on page 63)
- FortiSwitch features configuration on page 56
- Synchronizing the FortiGate unit with the managed FortiSwitch units on page 101
- Enabling the use of HTTPS to download firmware to managed FortiSwitch units (see Using the CLI on page 95)
- RADIUS accounting support on page 93
- FortiLink mode over a layer-3 network on page 26
- Limiting the number of parallel process for FortiSwitch configuration on page 55
- Changes to the `execute switch-controller get-physical-connection`, `execute switch-controller get-conn-status`, and `diagnose switch-controller dump network-upgrade status` CLI commands
- Upgrade the firmware on multiple FortiSwitch units at the same time using the GUI (see View and upgrade the FortiSwitch firmware version on page 95)
- Enabling network-assisted device detection on page 55

FortiSwitch devices managed by FortiOS

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
Up to FortiGate-98 and FortiGate-VM01	8
FortiGate-100 to 280 and FortiGate-VM02	24
FortiGate-300 to 5*xx*	48
FortiGate-600 to 900 and FortiGate-VM04	64
FortiGate-1000 and up	128
FortiGate-3*xxx* and up and FortiGate-VM08 and up	300

Supported models

The following table shows the FortiSwitch models that support FortiLink mode.

FortiGate and FortiWifi Models	FortiSwitch Models
3x, 5x, 6x, 7x, 8x, 9x, 1xx, 2xx, 3xx, 4xx, 5xx, 6xx, 8xx, 9xx, 1xxxx, 2xxxx, 3xxx	**D and E Series**
FortiOS 5.6 GA and later	For FortiSwitch D-series models, FortiSwitchOS 3.6.4 GA or later is required for all managed switches. For FortiSwitch E-series models, FortiSwitchOS 6.0.0 GA or later is required for all managed switches.

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, 1xxE-Series
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)	Not supported on 1xxE-Series
Port Mirroring	D-series, E-series
RADIUS Accounting Support	Not supported on 1xxE-Series
Centralized Configuration	D-series, E-series
Access VLAN	Not supported on 1xxE-Series, 112D-POE
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, 112D-POE
Centralized Firmware Management	D-series, E-series

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.

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).

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-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 (single port or LAG) 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 FortLink port or create a logical FortLink interface.
2. Authorize the managed FortiSwitch unit.

Configure FortiLink as a single link

To configure the FortiLink port on the FortiGate unit:

1. Go to *Network* > *Interfaces*.
2. (Optional) If the FortiLink physical port is currently included in the internal interface, edit it and remove the desired port from the Physical Interface Members.
3. Edit the FortiLink port.
4. Set *Addressing mode* to *Dedicated to FortiSwitch*.
5. Configure the *IP/Network Mask* for your network.
6. Optionally select *Automatically authorize devices* or disable to manually authorize the FortiSwitch.
7. Select *OK*.

Configure FortiLink as a logical interface

You can configure the FortiLink as 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 unit to the FortiSwitch unit. Ensure that you configure auto-discovery on the FortiSwitch ports (unless it is so by default).

1. Go to *Network* > *Interfaces*.
2. (Optional) If the FortiLink physical ports are currently included in the internal interface, edit the internal interface, and remove the desired ports from the Physical Interface Members.
3. Select *Create New* > *Interface*.
4. Enter a name for the interface (11 characters maximum).

5. Set the *Type* to *802.3ad Aggregate*, *Hardware Switch*, or *Software Switch*.
6. Select the FortiGate ports for the logical interface.
7. Set *Addressing mode* to *Dedicated to FortiSwitch*.
8. Configure the *IP/Network Mask* for your network.
9. Optionally select *Automatically authorize devices* or disable to manually authorize the FortiSwitch.
10. Select *OK*.

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).

You must enable the split interface on the FortiLink aggregate interface using the FortiGate CLI:

```
config system interface
   edit <name of the FortiLink interface>
      set fortilink-split-interface enable
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:

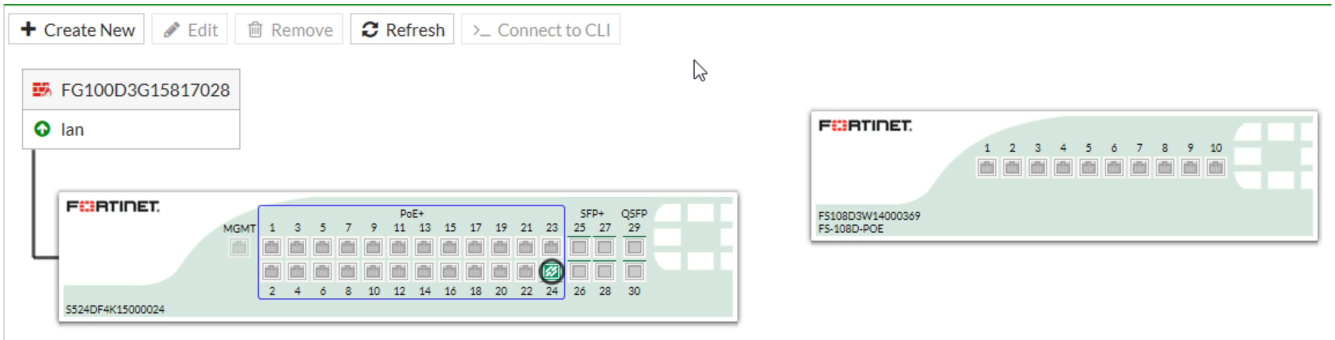
1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. Optionally, click on the FortiSwitch faceplate and click *Authorize*. This step is required only if you disabled the automatic authorization field of the interface.

Adding preauthorized FortiSwitch units

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

To preauthorize a FortiSwitch:

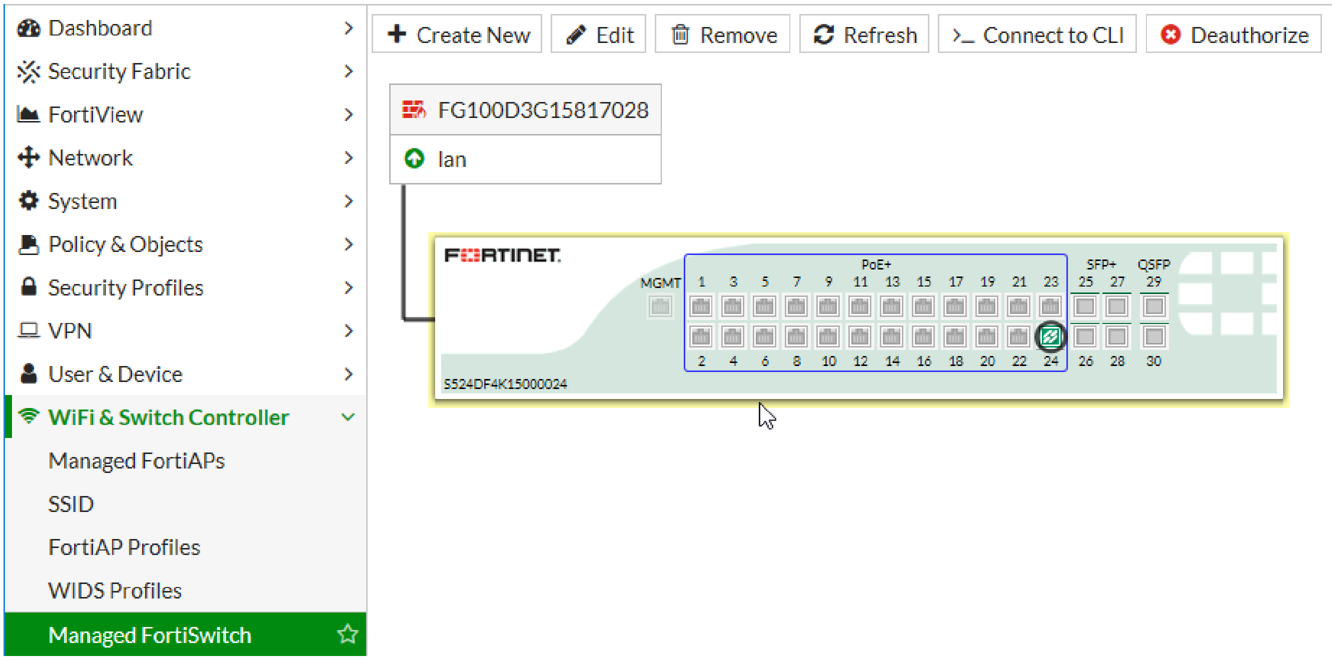
1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. Click *Create New*.
3. In the New Managed FortiSwitch page, enter the serial number, model name, and description of the FortiSwitch.
4. Move the *Authorized* slider to the right.
5. Click *OK*. The Managed FortiSwitch page shows a FortiSwitch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



Managed FortiSwitch display

Go to *WiFi & Switch Controller > Managed FortiSwitch* to see all of the switches being managed by your FortiGate.

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:

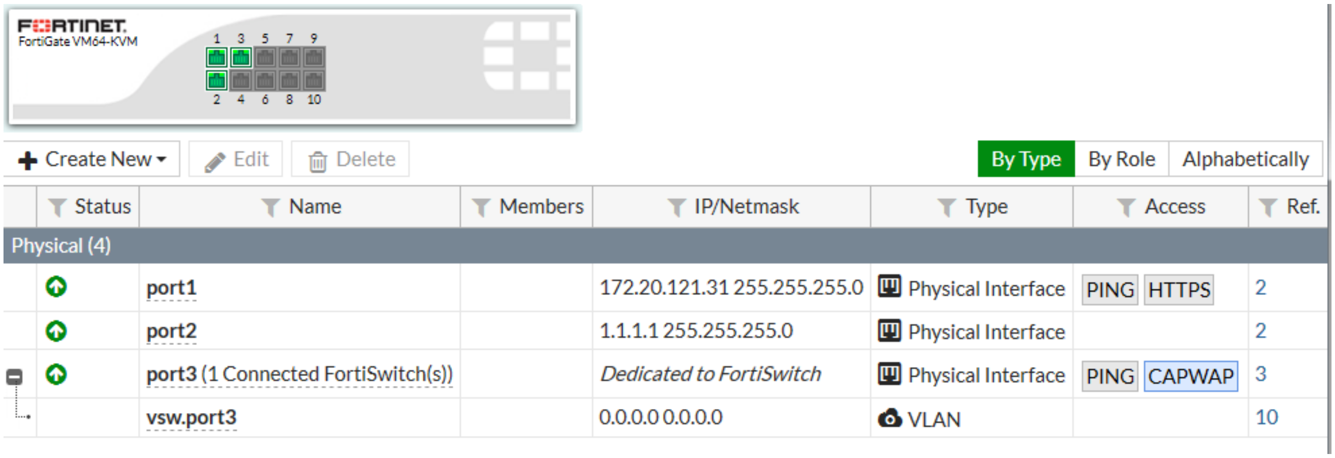
1. Go to *Wifi & Switch Controller* > *Managed FortiSwitch*.
2. Click on the FortiSwitch to and click *Edit*, right-click on a FortiSwitch unit and select *Edit*, or double-click on a FortiSwitch unit.

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.

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.



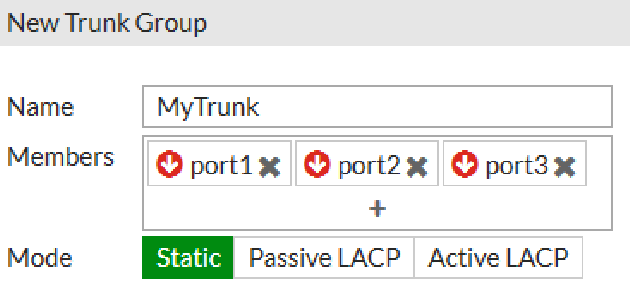
	Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (4)							
	⬆	port1		172.20.121.31 255.255.255.0	Physical Interface	PING HTTPS	2
	⬆	port2		1.1.1.1 255.255.255.0	Physical Interface		2
⊟	⬆	port3 (1 Connected FortiSwitch(s))		*Dedicated to FortiSwitch*	Physical Interface	PING CAPWAP	3
		vsw.port3		0.0.0.0 0.0.0.0	VLAN		10

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.

5. Select the *Mode*: Static, Passive LACP, or Active LACP.
6. Click *OK*.



New Trunk Group

Name: MyTrunk

Members: port1, port2, port3

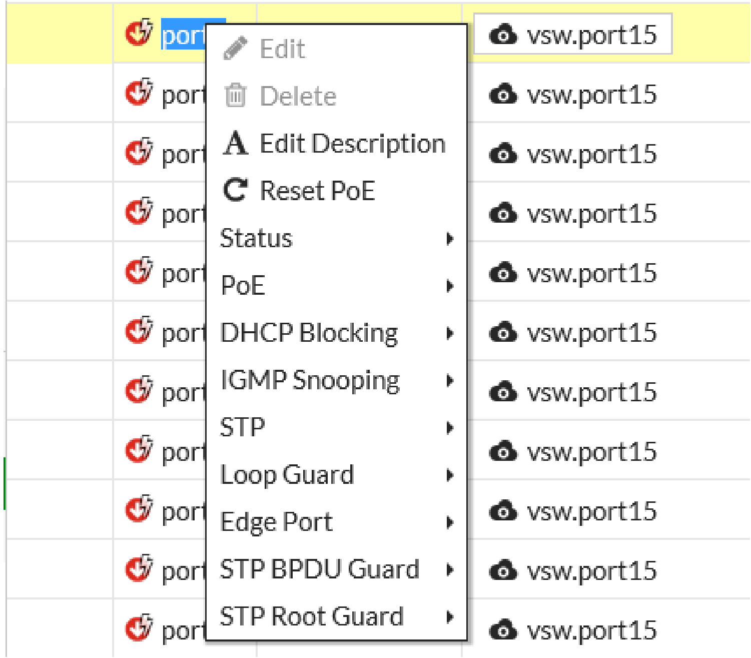
Mode: Static

Configure DHCP blocking, IGMP snooping, 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 blocking*—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.
- *IGMP snooping*—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.
- *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 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 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 is enabled on all ports by default. Loop guard is disabled by default on all ports.


port
vsw.port15
Edit
Delete
Edit Description
Reset PoE
Status
PoE
DHCP Blocking
IGMP Snooping
STP
Loop Guard
Edge Port
STP BPDU Guard
STP Root Guard

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. Ensure that you configure auto-discovery on the FortiSwitch ports (unless it is auto-discovery by default).

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
```

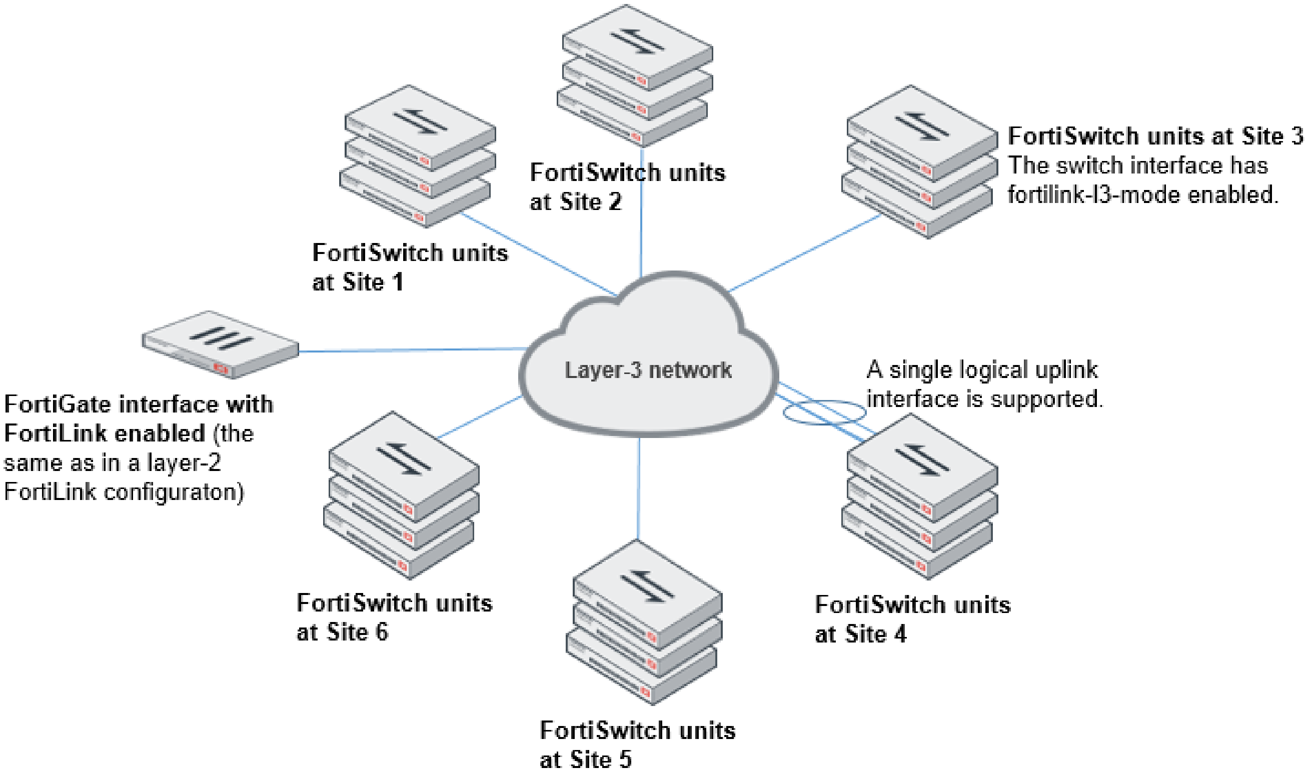
FortiLink mode over a layer-3 network

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


FortiSwitch units at Site 3
The switch interface has fortilink-l3-mode enabled.
FortiSwitch units at Site 2
FortiSwitch units at Site 1
FortiGate interface with FortiLink enabled (the same as in a layer-2 FortiLink configuraton)
Layer-3 network
A single logical uplink interface is supported.
FortiSwitch units at Site 6
FortiSwitch units at Site 4
FortiSwitch units at Site 5

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 dhcp
   set dhcp-option-code <integer>
end
```

   To use static discovery:

```
config switch-controller global
   set ac-discovery 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
   ```

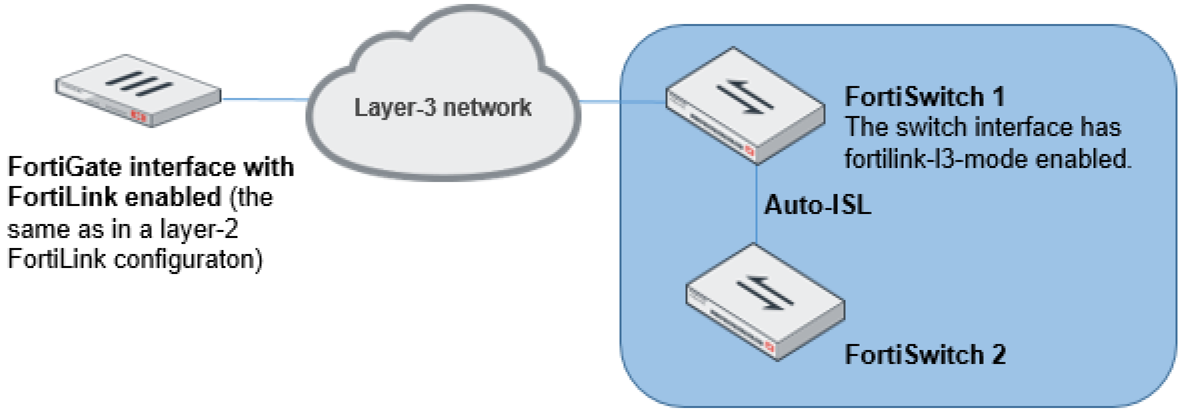
   The `fortilink-l3-mode` command is only visible after you configure DHCP or static discovery.

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 __ FoRtILnk0L3__ 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.

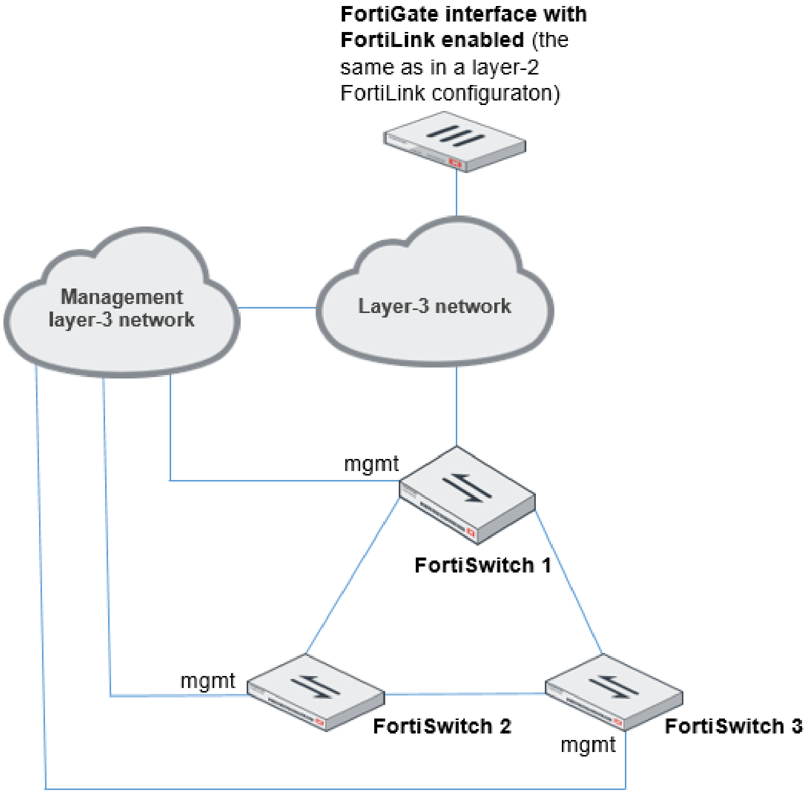
Connecting additional FortiSwitch units to the first FortiSwitch unit

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.


Layer-3 network
FortiGate interface with FortiLink enabled (the same as in a layer-2 FortiLink configuraton)
FortiSwitch 1
The switch interface has fortilink-l3-mode enabled.
Auto-ISL
FortiSwitch 2

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.


FortiGate interface with FortiLink enabled (the same as in a layer-2 FortiLink configuraton)
Management layer-3 network
Layer-3 network
mgmt
FortiSwitch 1
mgmt
FortiSwitch 2
FortiSwitch 3
mgmt

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.

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:

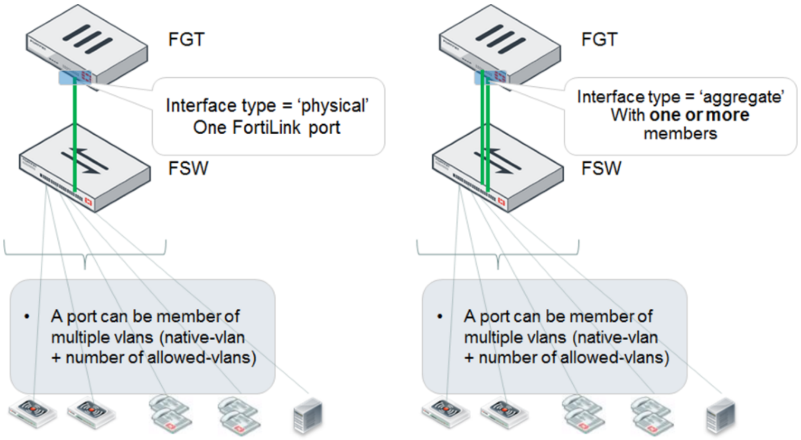
- Single FortiGate managing a single FortiSwitch unit on page 32
- Single FortiGate unit managing a stack of several FortiSwitch units on page 33
- HA-mode FortiGate units managing a single FortiSwitch unit on page 34
- HA-mode FortiGate units managing a stack of several FortiSwitch units on page 35
- HA-mode FortiGate units managing a FortiSwitch two-tier topology on page 36
- Single FortiGate unit managing multiple FortiSwitch units (using a hardware or software switch interface) on page 37
- HA-mode FortiGate units managing two-tier FortiSwitch units with access rings on page 38
- Dual-homed servers connected to a pair of FortiSwitch units using an MCLAG on page 39
- Standalone FortiGate unit with dual-homed FortiSwitch access on page 41
- HA-mode FortiGate units with dual-homed FortiSwitch access on page 42
- Multi-tiered MCLAG with HA-mode FortiGate units on page 43

Single FortiGate managing a single FortiSwitch unit

On the FortiGate unit, the FortiLink interface is configured as physical or aggregate. 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`.


FGT
Interface type = 'physical'
One FortiLink port
FSW
• A port can be member of multiple vlans (native-vlan + number of allowed-vlans)
FGT
Interface type = 'aggregate'
With one or more members
FSW
• A port can be member of multiple vlans (native-vlan + number of allowed-vlans)

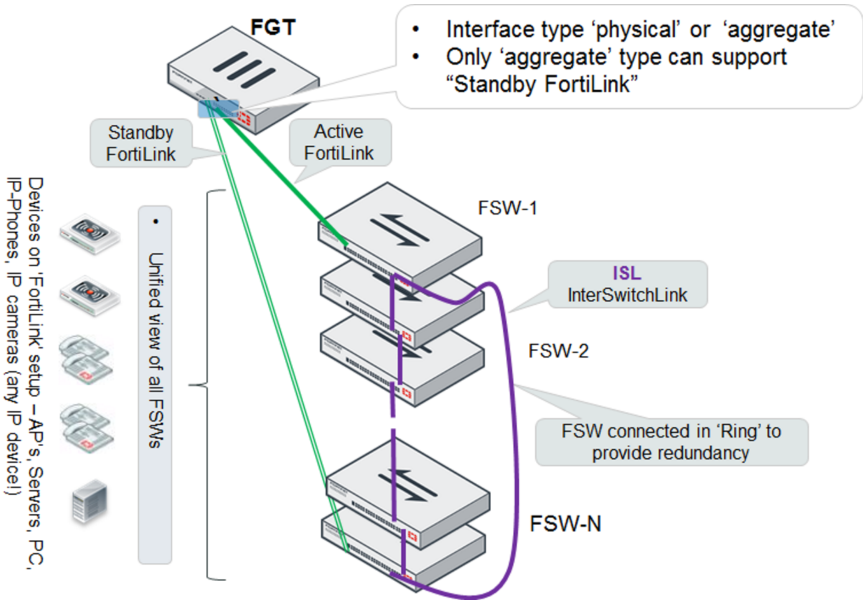
Single FortiGate unit managing a stack of several FortiSwitch units

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:

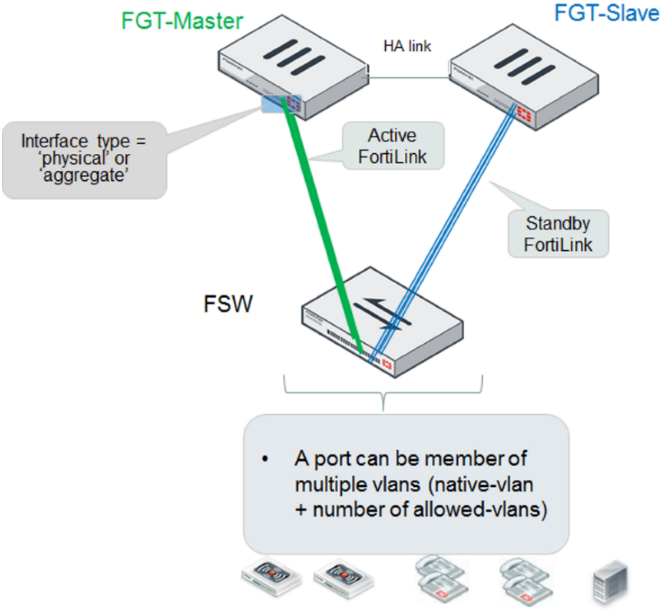
- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface, the `lacp-mode` of the FortiLink aggregate interface must be set to `static`.
- External devices shown in the following topology must be compliant endpoints, such as computers. They cannot be third-party switches or appliances.


FGT
• Interface type 'physical' or 'aggregate'
• Only 'aggregate' type can support "Standby FortiLink"
Standby FortiLink
Active FortiLink
FSW-1
ISL InterSwitchLink
FSW-2
FSW connected in 'Ring' to provide redundancy
FSW-N
• Unified view of all FSWs
Devices on 'FortiLink' setup – AP's, Servers, PC, IP-Phones, IP cameras (any IP device)

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: When using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive.


FGT-Master
HA link
FGT-Slave
Interface type = 'physical' or 'aggregate'
Active FortiLink
Standby FortiLink
FSW
• A port can be member of multiple vlans (native-vlan + number of allowed-vlans)

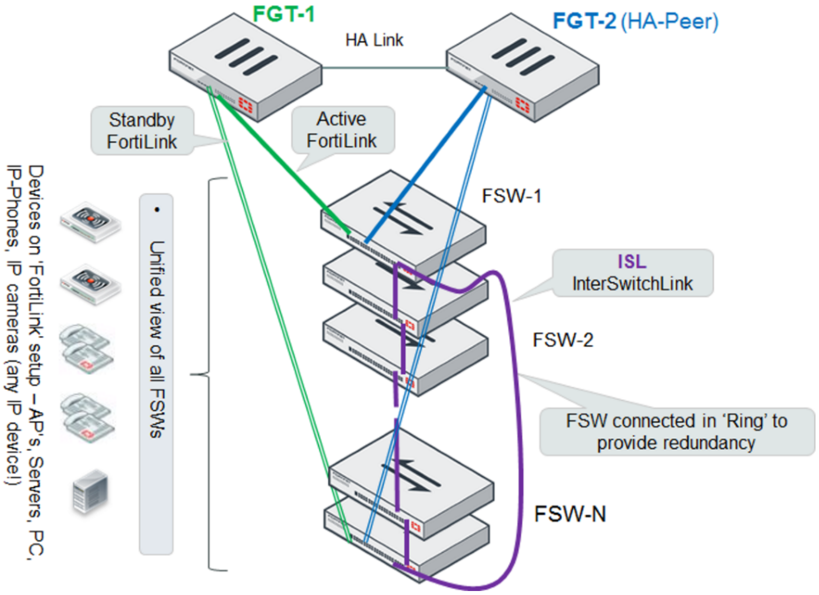
HA-mode FortiGate units managing a stack of several FortiSwitch units

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.

For the active/standby FortiLink configuration, you create a FortiLink Split-Interface (an aggregate interface that contains one active link and one standby link).

NOTE:

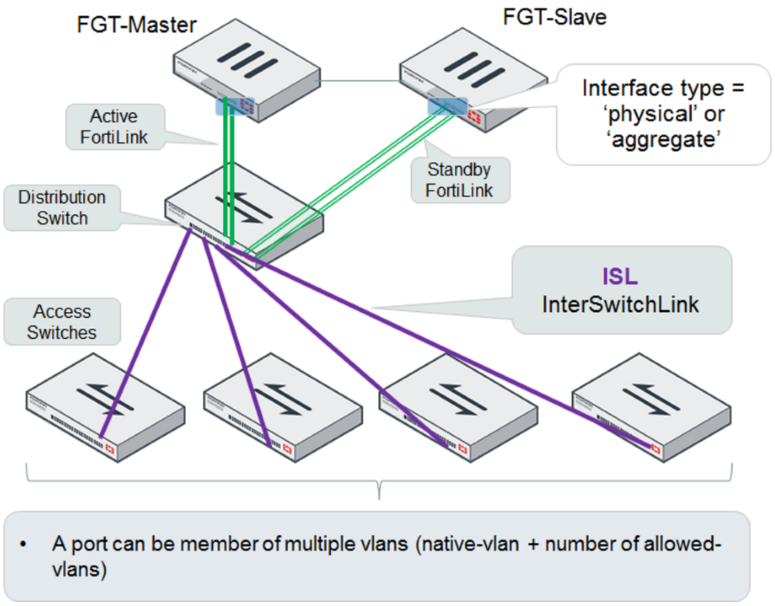
- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface, the `lacp-mode` of the FortiLink aggregate interface must be set to `static`.
- When using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive.


FGT-1
HA Link
FGT-2 (HA-Peer)
Standby FortiLink
Active FortiLink
FSW-1
ISL
InterSwitchLink
FSW-2
FSW connected in 'Ring' to provide redundancy
FSW-N
Unified view of all FSWs
Devices on 'FortiLink' setup – AP's, Servers, PC, IP-Phones, IP cameras (any IP device!)

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: When using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive.

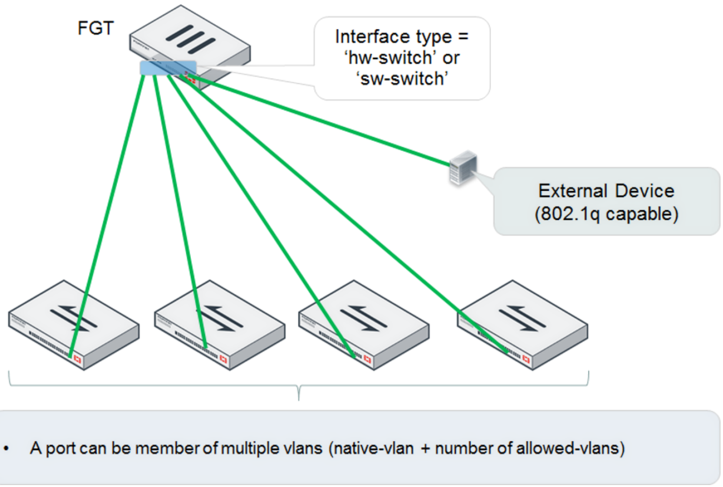

FGT-Master
FGT-Slave
Interface type = 'physical' or 'aggregate'
Active FortiLink
Standby FortiLink
Distribution Switch
ISL
InterSwitchLink
Access Switches
• A port can be member of multiple vlans (native-vlan + number of allowed-vlans)

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.


FGT
Interface type = 'hw-switch' or 'sw-switch'
External Device (802.1q capable)

- A port can be member of multiple vlans (native-vlan + number of allowed-vlans)

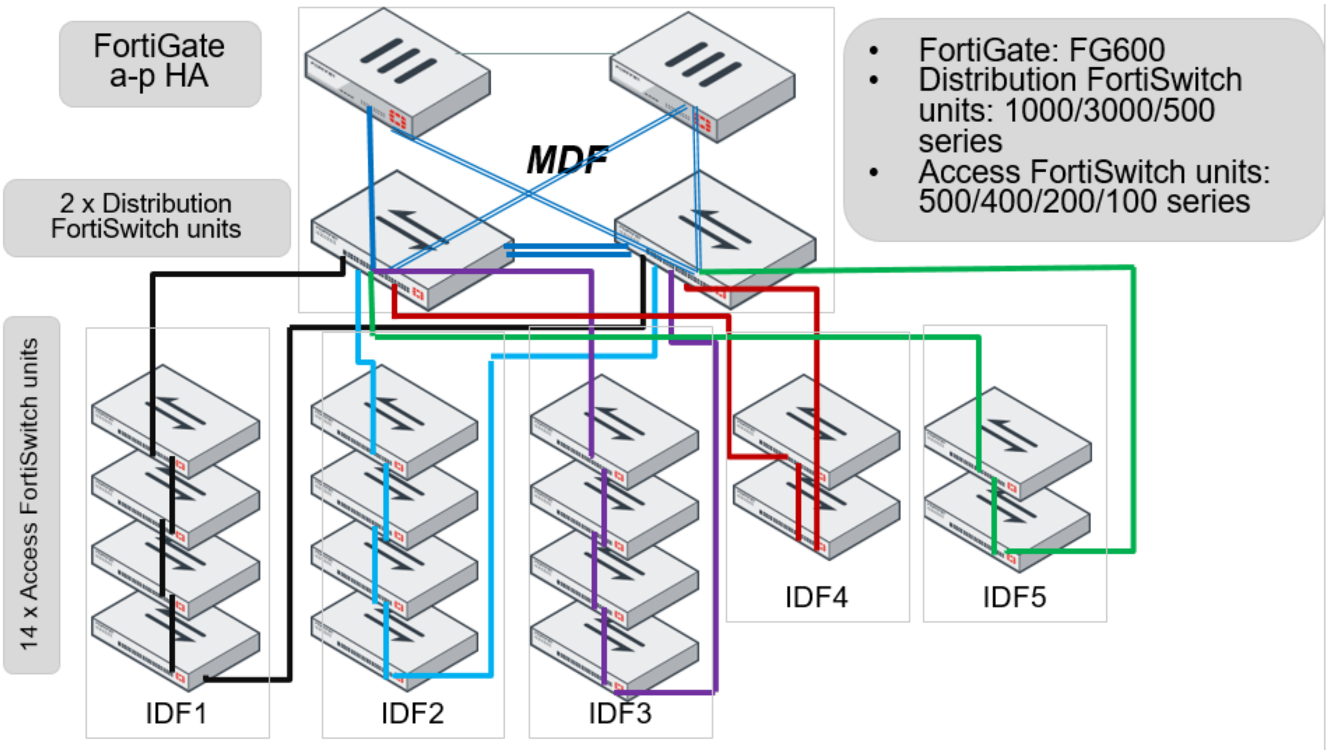
HA-mode FortiGate units managing two-tier FortiSwitch units with access rings

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:

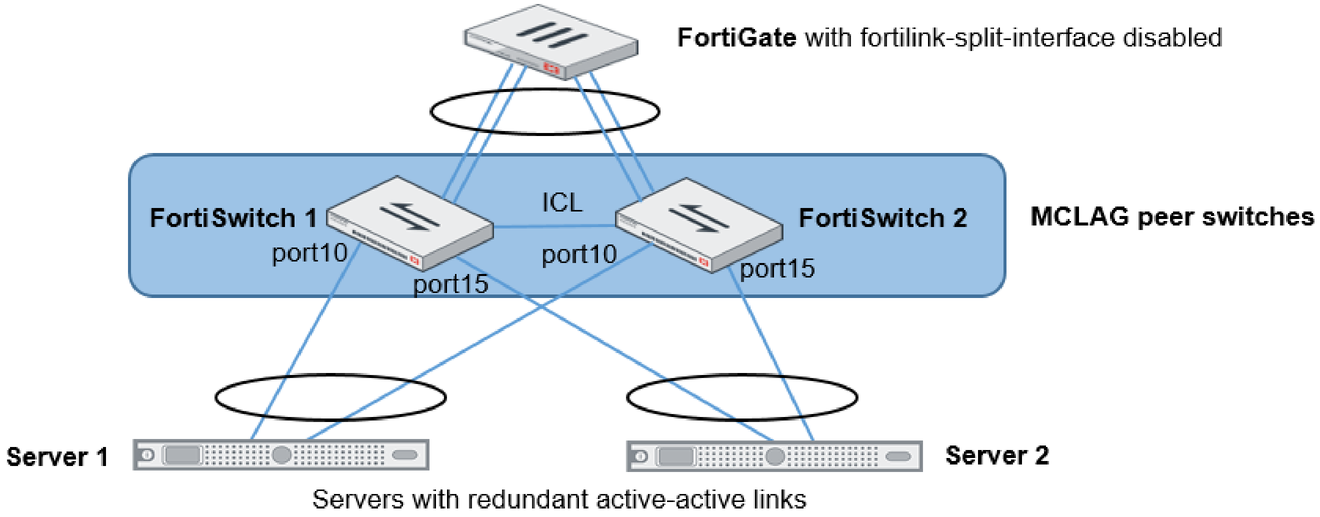
- Before FortiSwitchOS 3.6.4, MCLAG was not supported when access rings were present. Starting with FortiSwitchOS 3.6.4, MCLAG is supported, even with access rings present.
- When using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive.
- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface, the `lacp-mode` of the FortiLink aggregate interface must be set to `static`.
- This is only an example topology. Other combinations of FortiGate units and FortiSwitch units can be used to create a similar topology.


FortiGate a-p HA
2 x Distribution FortiSwitch units
14 x Access FortiSwitch units
MDF
IDF1
IDF2
IDF3
IDF4
IDF5
• FortiGate: FG600
• Distribution FortiSwitch units: 1000/3000/500 series
• Access FortiSwitch units: 500/400/200/100 series

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. 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.


FortiGate with fortilink-split-interface disabled
FortiSwitch 1
port10
port15
ICL
port10
FortiSwitch 2
port15
MCLAG peer switches
Server 1
Server 2
Servers with redundant active-active links

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:

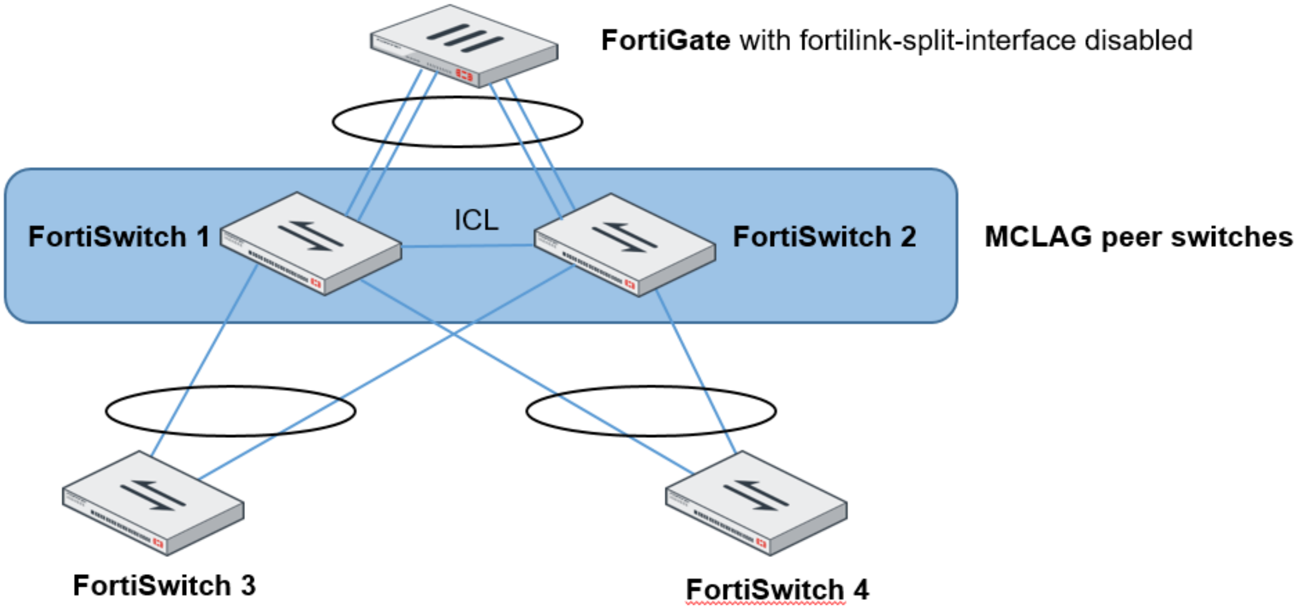
```
config switch trunk
   edit server_1
      set members port10
      set mclag enable
   next
   edit server_2
      set members port15
      set mclag enable
   next
end
```

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.

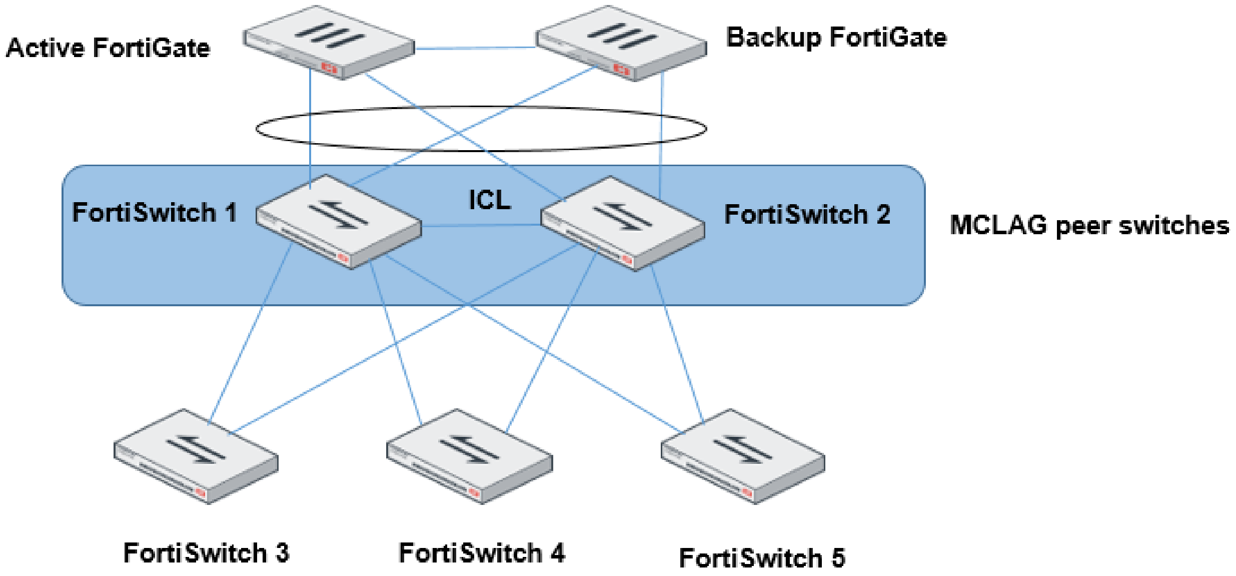


HA-mode FortiGate units with dual-homed FortiSwitch access

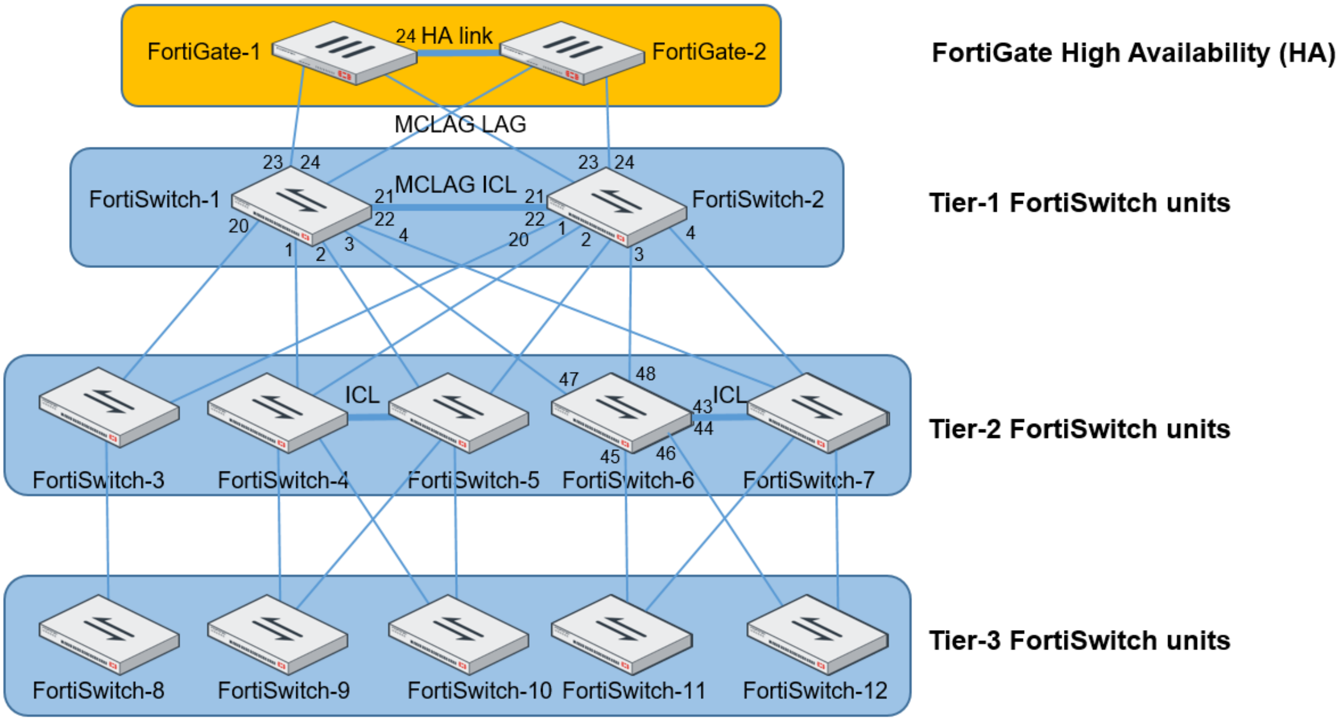
In HA mode, only one FortiGate is active at a time. If the active FortiGate unit fails, the backup FortiGate unit becomes active.

Use the `set mclag-icl enable` command to create an ICL on each FortiSwitch unit.

NOTE: When using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive.



Multi-tiered MCLAG with HA-mode FortiGate units



NOTE:

- When using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive.
- 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.
- CLI commands in red are manually configured.

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

1. Configure FortiSwitch-1 for the tier-1 MCLAG:
   a. 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
```

   b. 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 "mclag-core1"
      set members "port1" "port2"
   next
   edit "mclag-core2"
      set members "port3" "port4"
   end
```

c. After you complete the CLI commands in Steps 1a and 1b, 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 "__FoRtI1LiNk0__"
      set mclag enable
      set members "port24" "port23"
   next
   edit "8DN4K16000360-0" // trunk name derived from FortiSwitch-3 SN
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port20"
   next
   edit "mclag-core1"
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port1" "port2"
   next
   edit "mclag-core2"
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port3" "port4"
   next
end
```

2. Configure FortiSwitch-2 for the tier-1 MCLAG:

a. 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
```

b. 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 "mclag-core1"
      set members "port1" "port2"
   next
   edit "mclag-core2"
      set members "port3" "port4"
   end
```

c. After you complete the CLI commands in Steps 2a and 2b, 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 "__FoRtI1LiNk0__"
      set mclag enable
      set members "port24" "port23"
   next
   edit "8DN4K16000360-0" // trunk name derived from FortiSwitch-3 SN
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port20"
   next
   edit "mclag-core1"
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port1" "port2"
   next
   edit "mclag-core2"
      set mode lacp-active
      set auto-isl 1
      set mclag enable
      set members "port3" "port4"
   next
end
```

3. Tier-2 MCLAGs. Enable the ICL between the MCLAG peers. 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 "8EP3X17000051-0" // trunk name derived from FortiSwitch-11 SN
         set mode lacp-active
         set auto-isl 1
         set mclag enable
         set members "port45"
      next
   ```

```
      edit "_FlInK1_MLAG0_"
         set mode lacp-active
         set auto-isl 1
         set mclag enable
         set members "port48" "port47"
      next
      edit "8EP3X17000069-0" // trunk name derived from FortiSwitch-12 SN
         set mode lacp-active
         set auto-isl 1
         set mclag enable
         set members "port46"
      next
   end
```

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

   On FortiSwitch-11:

   ```
   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-12:

   ```
   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.

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.

```
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 restart-swtp my-switch-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 48.

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.

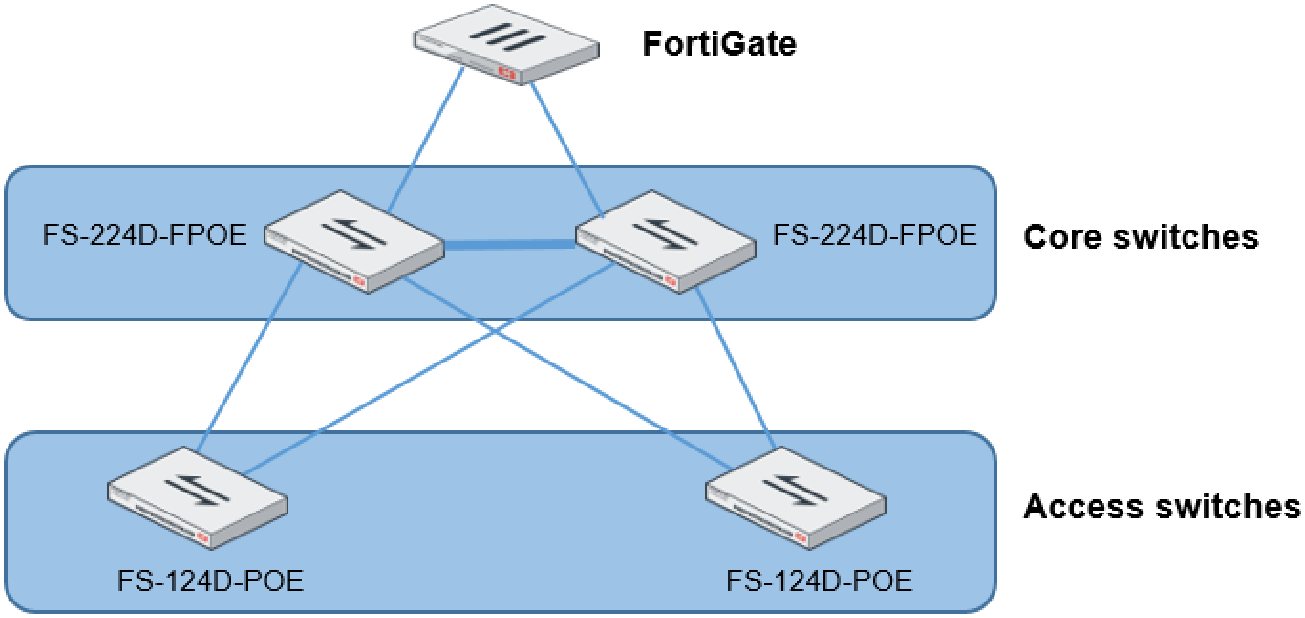
The FortiGate unit will discover and authorize all of the FortiSwitch units that are connected. After this, the FortiGate unit is ready to manage all of the authorized FortiSwitch units.

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-224D-FPOE, and the access FortiSwitch units are model FS-124D-POE. Because the switches are stacked or tiered, the procedure to update the firmware is simpler. In the following procedure, the four FortiSwitch units are upgraded from 3.6.1 to 3.6.2.

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:

```
execute switch-controller get-conn-status
STACK-NAME: FortiSwitch-Stack-port2
SWITCH-ID VERSION STATUS ADDRESS JOIN-TIME NAME
S108DV2EJZDAC42F v3.6.0 Authorized/Up 169.254.2.4 Thu Feb 8 17:07:35 2018 -
S108DV4FQON40Q07 v3.6.0 Authorized/Up 169.254.2.5 Thu Feb 8 17:08:37 2018 -
S108DVBWVLH4QGEB v3.6.0 Authorized/Up 169.254.2.6 Thu Feb 8 17:09:13 2018 -
```

```
S108DVCY19SA0CD8 v3.6.0 Authorized/Up 169.254.2.2 Thu Feb 8 17:04:41 2018 -
S108DVD98KMQGC44* v3.6.0 Authorized/Up 169.254.2.7 Thu Feb 8 17:10:50 2018 -
S108DVGGBJLQQO48* v3.6.0 Authorized/Up 169.254.2.3 Thu Feb 8 17:06:57 2018 -
S108DVKM5T2QEA92 v3.6.0 Authorized/Up 169.254.2.8 Thu Feb 8 17:11:00 2018 -
S108DVZX3VTAOO45 v3.6.0 Authorized/Up 169.254.2.9 Thu Feb 8 17:11:00 2018 -
Managed-Switches: 8 UP: 8 DOWN: 0
```

2. Upload the firmware image for each FortiSwitch model (FS-224D-FPOE and FS-124D-POE) from either an FTP or TFTP server. If you are using a virtual domain (VDOM), you must enter the `config global` command before entering the `upload-swtp-image` command. For example:

```
FG100E4Q16004478 (global) # execute switch-controller upload-swtp-image tftp FSW_124D_POE-
     v3-build0382-FORTINET.out 172.30.12.18
Downloading file FSW_124D_POE-v3-build0382-FORTINET.out from tftp server 172.30.12.18...
##################
Image checking ...
Image MD5 calculating ...
Image Saving S124DP-IMG.swtp ...
Successful!
File Syncing...
FG100E4Q16004478 (global) # execute switch-controller upload-swtp-image tftp FSW_224D_FPOE-
     v3-build0382-FORTINET.out 172.30.12.18
Downloading file FSW_224D_FPOE-v3-build0382-FORTINET.out from tftp server 172.30.12.18...
######################
Image checking ...
Image MD5 calculating ...
Image Saving S224DF-IMG.swtp ...
Successful!
File Syncing...
```

3. Check which firmware images are available. For example:

```
FG100E4Q16004478 (root) # execute switch-controller list-swtp-image
SWTP Images on AC:
ImageName ImageSize(B) ImageInfo ImageMTime
S124DP-IMG.swtp 19174985 S124DP-v3.6-build382 Mon Oct 2 14:40:54 2017
S224DF-IMG.swtp 23277106 S224DF-v3.6-build382 Mon Oct 2 14:42:55 2017
```

4. Stage the firmware image for each FortiSwitch model (FS-224D-FPOE and FS-124D-POE). For example:

```
FG100E4Q16004478 (root) # execute switch-controller stage-tiered-swtp-image ALL S124DP-
     IMG.swtp
Staged Image Version S124DP-v3.6-build382

FG100E4Q16004478 (root) # execute switch-controller stage-tiered-swtp-image ALL S224DF-
     IMG.swtp
Staged Image Version S224DF-v3.6-build382
```

5. Check that the correct firmware image is staged for each FortiSwitch unit. For example:

```
diagnose switch-controller dump network-upgrade status
Running Status Next boot
__________________ ________________________________________ _________ _____________________
     ______
VDOM : root
S108DVCY19SA0CD8 S108DV-v3.6.0-build4277,171207 (Interim) (0/0/0) S108DV-v3.7.0-
     build4277,171207 (Interim)
S108DV2EJZDAC42F S108DV-v3.6.0-build4277,171207 (Interim) (0/0/0)
```

6. Restart the FortiSwitch units after a 2-minute delay. For example: `execute switch-controller restart-swtp-delayed ALL`

7. When the FortiSwitch units are running again, check that they are running the new firmware version. For example:

```
execute switch-controller get-conn-status
```

```
STACK-NAME: FortiSwitch-Stack-port2
SWITCH-ID VERSION STATUS ADDRESS JOIN-TIME NAME
S108DV2EJZDAC42F v3.6.0 Authorized/Up 169.254.2.4 Thu Feb 8 17:07:35 2018 -
S108DV4FQON40Q07 v3.6.0 Authorized/Up 169.254.2.5 Thu Feb 8 17:08:37 2018 -
S108DVBWVLH4QGEB v3.6.0 Authorized/Up 169.254.2.6 Thu Feb 8 17:09:13 2018 -
S108DVCY19SA0CD8 v3.6.0 Authorized/Up 169.254.2.2 Thu Feb 8 17:04:41 2018 -
S108DVD98KMQGC44* v3.6.0 Authorized/Up 169.254.2.7 Thu Feb 8 17:10:50 2018 -
S108DVGGBJLQQO48* v3.6.0 Authorized/Up 169.254.2.3 Thu Feb 8 17:06:57 2018 -
S108DVKM5T2QEA92 v3.6.0 Authorized/Up 169.254.2.8 Thu Feb 8 17:11:00 2018 -
S108DVZX3VTAOO45 v3.6.0 Authorized/Up 169.254.2.9 Thu Feb 8 17:11:00 2018 -
Managed-Switches: 8 UP: 8 DOWN: 0
```

Transitioning from a FortiLink split interface to a FortiLink MCLAG

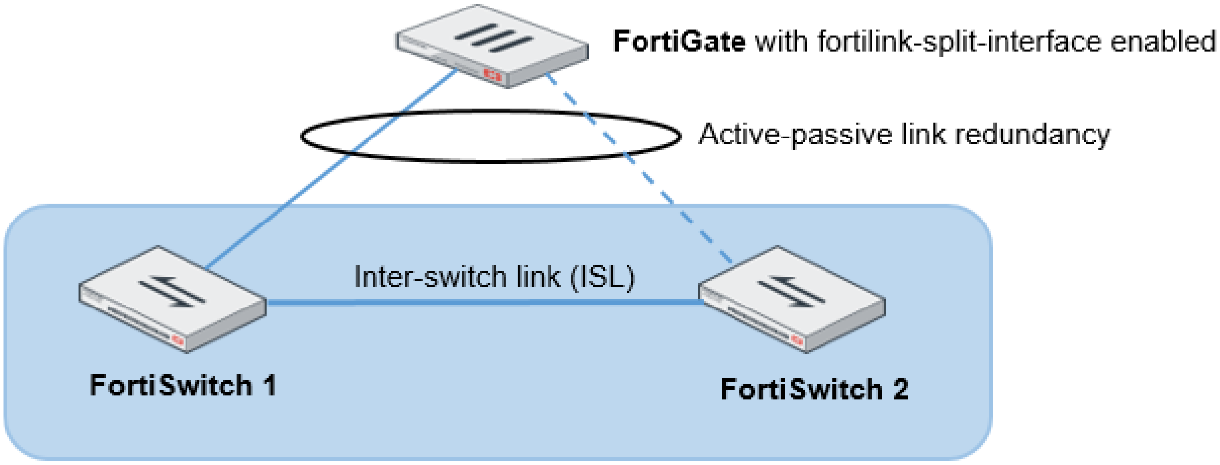
In this topology, the FortiLink split interface connects a FortiLink aggregate interface from one FortiGate unit to two FortiSwitch units.

NOTE:

- This procedure also applies to a FortiGate unit in HA mode.
- More links can be added between the FortiGate unit and FortiSwitch unit.
- After the MCLAG is set up, only connect the tier-2 FortiSwitch units.
- 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`.

1. Enable the split interface on the FortiLink aggregate interface. By default, the split interface is enabled. For example:

```
config system interface
   edit flinksplit1
      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
      set fortilink-split-interface enable
   next
end
```


FortiGate with fortilink-split-interface enabled
Active-passive link redundancy
Inter-switch link (ISL)
FortiSwitch 1
FortiSwitch 2

2. 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
```

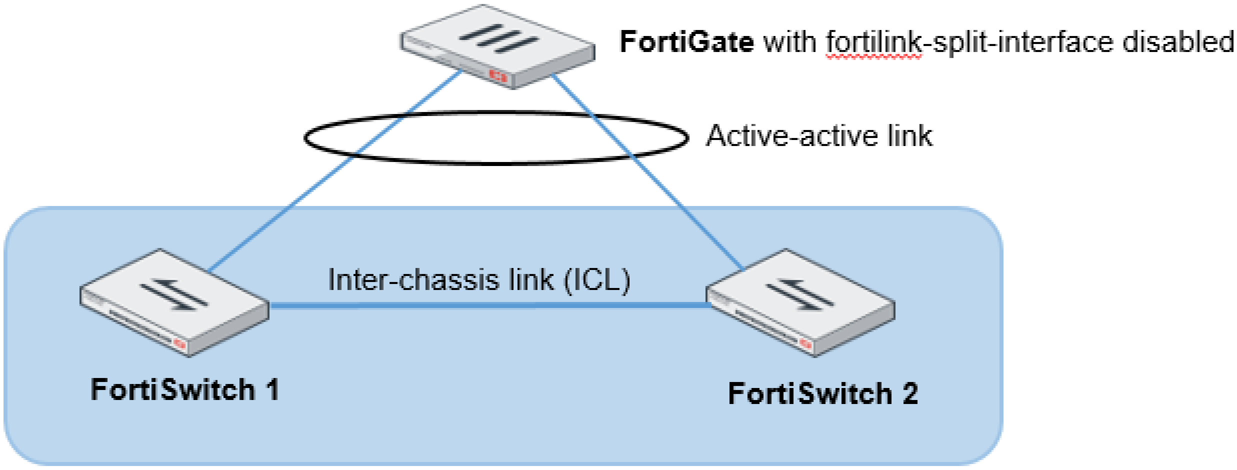
3. Log into FortiSwitch 1 using the *Connect to CLI* button in the FortiGate GUI, use the `get switch lldp auto-isl-status` command to find out the name of the trunk connecting the peer switches, and change the ISL to an ICL. For example:

```
get switch lldp auto-isl-status

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

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

```
config system interface
   edit flinksplit1
      set fortilink-split-interface disable
   next
end
```

5. Enable the LACP active mode.
6. Check that the LAG is working correctly. For example:
7. `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 on page 53
- Converting to FortiSwitch standalone mode on page 54
- Changing the admin password on the FortiGate for all managed FortiSwitch units on page 54
- Enabling network-assisted device detection on page 55
- Limiting the number of parallel process for FortiSwitch configuration on page 55

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
```

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 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
```

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
```

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 on page 56
- Configure IGMP settings on page 60
- Configure LLDP-MED on page 60
- Configure the MAC sync interval on page 62
- Configure STP settings on page 62
- Quarantines on page 63

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.)

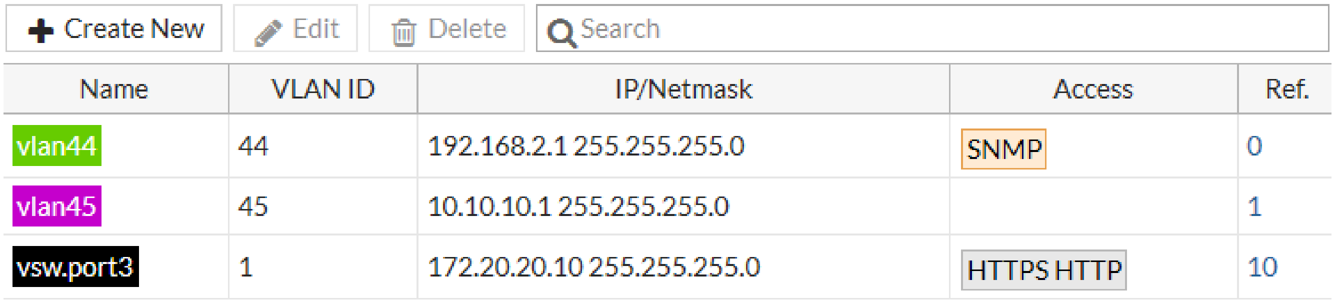
From the FortiGate unit, you can centrally configure and manage VLANs for the managed FortiSwitch units.

In FortiSwitchOS 3.3.0 and later releases, the FortiSwitch unit supports untagged and tagged frames in FortiLink mode. The switch supports up to 1,023 user-defined VLANs. You can assign a VLAN number (ranging from 1-4095) to each of the VLANs.

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

FortiSwitch VLANs display

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



Name	VLAN ID	IP/Netmask	Access	Ref.
vlan44	44	192.168.2.1 255.255.255.0	SNMP	0
vlan45	45	10.10.10.1 255.255.255.0		1
vsw.port3	1	172.20.20.10 255.255.255.0	HTTPS HTTP	10

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
```

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 Web administration GUI

To create the VLAN:

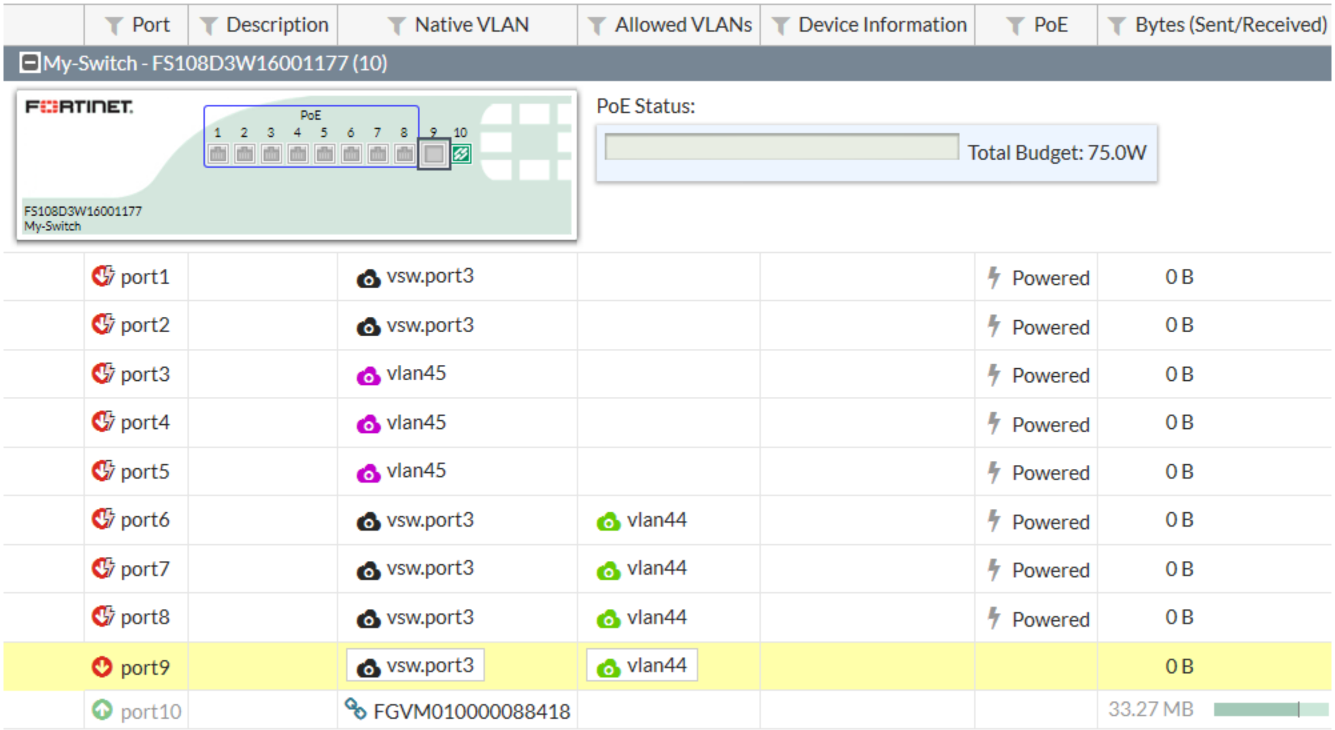
1. Go to *WiFi & Switch Controller > FortiSwitch VLANS*, select *Create New*, and change the following settings:

Interface Name	VLAN name
VLAN ID	Enter a number (1-4094)
Color	Choose a unique color for each VLAN, for ease of visual display.
IP/Network Mask	IP address and network mask for this VLAN.

2. Enable *DHCP Server* and set the IP range.
3. Set the *Admission Control* options as required.
4. Select *OK*.

To assign FortiSwitch ports to the VLAN:

1. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
2. Click the desired 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.



My-Switch - FS108D3W16001177 (10)

PoE Status:

Total Budget: 75.0W

Port	Description	Native VLAN	Allowed VLANs	Device Information	PoE	Bytes (Sent/Received)
port1		vsw.port3			Powered	0 B
port2		vsw.port3			Powered	0 B
port3		vlan45			Powered	0 B
port4		vlan45			Powered	0 B
port5		vlan45			Powered	0 B
port6		vsw.port3	vlan44		Powered	0 B
port7		vsw.port3	vlan44		Powered	0 B
port8		vsw.port3	vlan44		Powered	0 B
port9		vsw.port3	vlan44			0 B
port10		FGVM010000088418				33.27 MB

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
```

Configure IGMP settings

Use the following command to configure the global IGMP 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

To configure LLDP profiles:

```
config switch-controller lldp-profile
   edit <profile number>
      set 802.1-tlvs port-vlan-id
      set 802.3-tlvs max-frame-size
      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>
      set med-tlvs (inventory-management | network-policy)
end
```

To configure LLDP settings:

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

Variable	Description
status	Enable or disable
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.

Variable	Description
tx-interval	How often the FortiSwitch unit transmits the LLDP PDU. The range is 5 to 4095 seconds, and the default is 30 seconds.
fast-start-interval	How often the FortiSwitch unit 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.

Create LLDP asset tags for each managed FortiSwitch unit

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

```
config switch-controller managed-switch
   edit <fsw>
      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 dump lldp stats <switch> <port>
diagnose switch-controller dump lldp neighbors-summary <switch>
diagnose switch-controller dump 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.

Use the following CLI commands for global STP configuration. This configuration applies to 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
```

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

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

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 by using a separate VLAN.

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.

Quarantining MAC addresses

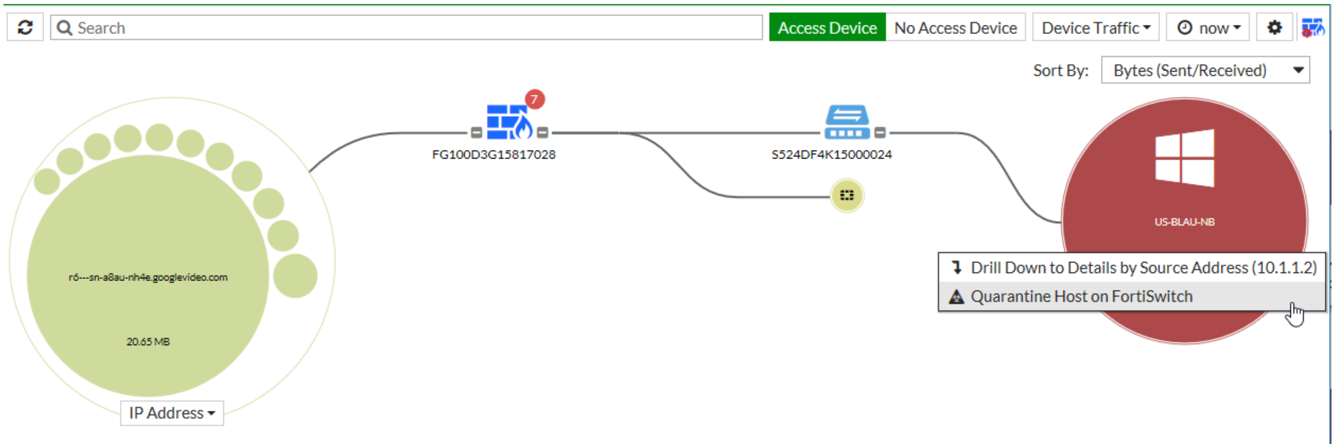
You can use the FortiGate GUI or CLI to quarantine a MAC address.

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.

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.

```
config user quarantine
   set quarantine enable
   config targets
      edit <quarantine_entry_name>
         set description <string>
         config macs
            edit <MAC_address_1>
            next
            edit <MAC_address_2>
            next
            edit <MAC_address_3>
            next
      end
   end
end
```

Option	Description
quarantine_entry_name	A name for this quarantine entry.
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`

For example:

```
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
```

Using quarantines 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
```

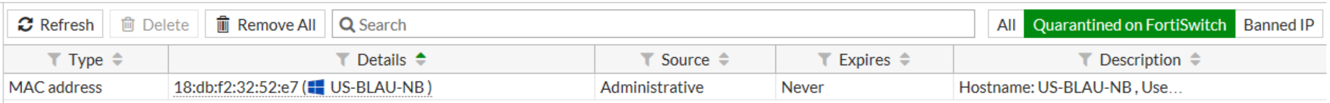
```
S448DF3X16000118 # diagnose switch mac list | grep "VLAN: 4093"
MAC: 00:05:65:ad:15:03 VLAN: 4093 Port: port17(port-id 17)
```

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.



Type	Details	Source	Expires	Description
MAC address	18:db:f2:32:52:e7 (US-BLAU-NB)	Administrative	Never	Hostname: US-BLAU-NB , Use...

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
```

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:

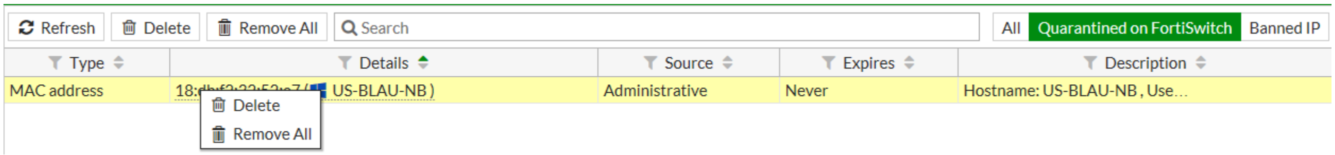
```
show switch-controller managed-switch

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.



Type	Details	Source	Expires	Description
MAC address	18:db:f2:22:52:e7 (US-BLAU-NB)	Administrative	Never	Hostname: US-BLAU-NB , Use...

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
```

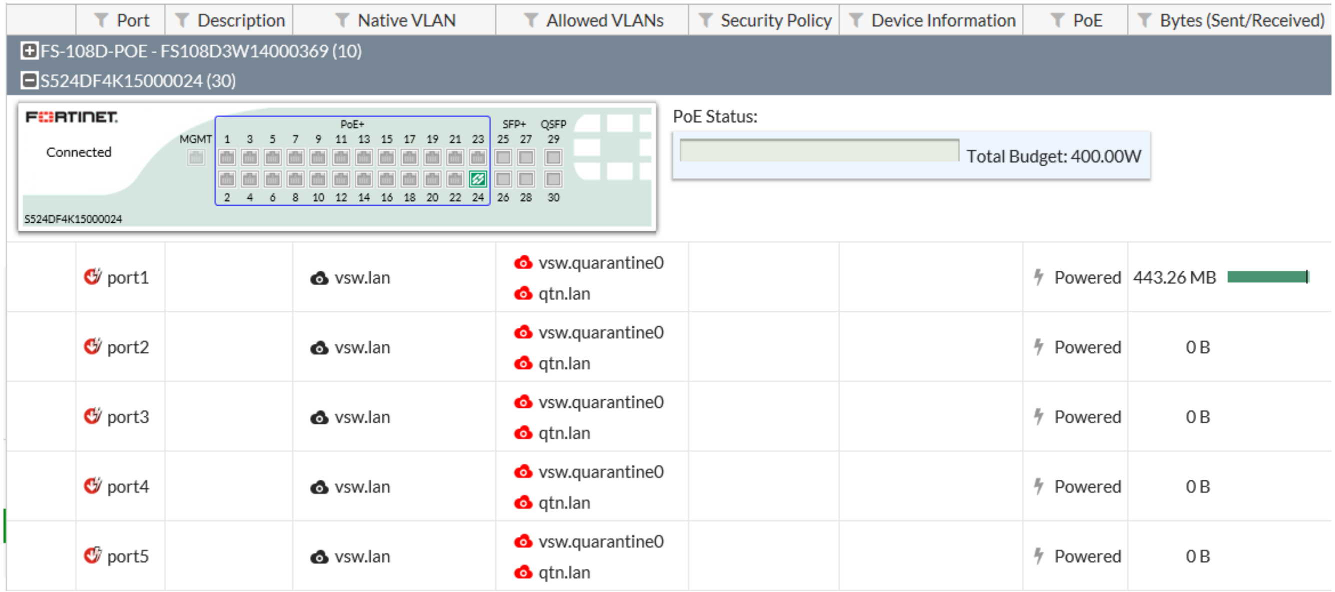
FortiSwitch port features

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 524D-FPOE:



	Port	Description	Native VLAN	Allowed VLANs	Security Policy	Device Information	PoE	Bytes (Sent/Received)
FS-108D-POE - FS108D3W14000369 (10)								
S524DF4K15000024 (30)								
	port1		vsw.lan	vsw.quarantine0 qtn.lan			Powered	443.26 MB
	port2		vsw.lan	vsw.quarantine0 qtn.lan			Powered	0 B
	port3		vsw.lan	vsw.quarantine0 qtn.lan			Powered	0 B
	port4		vsw.lan	vsw.quarantine0 qtn.lan			Powered	0 B
	port5		vsw.lan	vsw.quarantine0 qtn.lan			Powered	0 B

PoE Status:

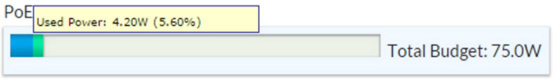
Total Budget: 400.00W

The switch faceplate displays:

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

PoE Status displays the total power budget and the actual power currently allocated.

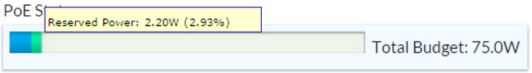
The allocated power displays a blue bar for the used power (currently being consumed) and a green bar for the reserved power (power available for additional devices on the POE ports). See the following figures:



PoE

Used Power: 4.20W (5.60%)

Total Budget: 75.0W



PoE S

Reserved Power: 2.20W (2.93%)

Total Budget: 75.0W

Each entry in the port list displays the following information:

- Port status (red for down, green for up)
- Port name
- Native VLAN
- Allowed VLANs
- Device information
- PoE status
- Bytes sent and received by the port

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
- Enable or disable PoE for the port
- Enable or disable DHCP blocking (if supported by the port)
- Enable or disable IGMP 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 73
- Configure a VLAN on the port (see Configure VLANs)
- Sharing FortiSwitch ports between VDOMs on page 73
- Limiting the number of learned MAC addresses on a FortiSwitch interface on page 76
- Configuring the DHCP trust setting on page 78

- Configuring PoE on page 78
- Configuring edge ports on page 79
- Configuring STP on page 79
- Configuring STP root guard on page 82
- Configuring STP BPDU guard on page 82
- Configuring loop guard on page 84
- Configuring LLDP settings on page 84
- Configuring IGMP settings on page 85
- Configuring sFlow on page 85
- Configuring Dynamic ARP inspection (DAI) on page 86
- Configuring FortiSwitch port mirroring on page 87

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>
            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.

NOTE: You cannot use the quarantine feature while sharing FortiSwitch ports between VDOMs.

To share FortiSwitch ports between VDOMs:

1. Create one or more VDOMs.
2. Assign VLANs to each VDOM as required.

3. From these VLANs, select one VLAN to be the default VLAN for the ports in the virtual switch:

   ```
   config switch-controller global
      set default-virtual-switch-vlan <VLAN>
   ```

   NOTE: You must execute these commands from the VDOM that the default VLAN belongs to. When you add a new port to the VDOM, the new port will be automatically assigned to the default VLAN. You can reassign the ports to other VLANs later.
4. Create a virtual port pool (VPP) to contain the ports to be shared:

   ```
   config switch-controller virtual-port-pool
      edit <VPP_name>
         description <string>
      next
   end
   ```

   NOTE: You must execute these commands from the VDOM that the default VLAN belongs to.

   For example:

   ```
   config switch-controller virtual-port-pool
      edit "pool3"
         description "pool for port3"
      next
   end
   ```
5. Share a FortiSwitch port from the VDOM that the FortiSwitch belongs to with another VDOM or export the FortiSwitch port to a VPP where it can be used by any VDOM:

   ```
   config switch-controller managed-switch
      edit <switch.id>
         config ports
            edit <port_name>
               set {export-to-pool <VPP_name> | export-to <VDOM_name>}
               set export-tags <string1,string2,string3,...>
            next
         end
      next
   end
   ```

   NOTE: You must execute these commands from the VDOM that the default VLAN belongs to.

   For example, if you want to export a port to the VPP named `pool3`:

   ```
   config switch-controller managed-switch
      edit "S524DF4K15000024"
         config ports
            edit port3
               set export-to-pool "pool3"
               set export-tags "Pool 3"
            next
         end
      next
   end
   ```

For example, if you want to export a port to the VDOM named `vdom3`:

```
config switch-controller managed-switch
   edit "S524DF4K15000024"
      config ports
         edit port3
            set export-to "vdom3"
            set export-tags "VDOM 3"
         next
      end
   next
end
```

6. Request a port in a VPP:

   ```
   execute switch-controller virtual-port-pool request <FortiSwitch_device_ID> <port_name>
   ```

   NOTE: You must execute this command from the VDOM that is requesting the port.

   For example:

   ```
   execute switch-controller virtual-port-pool request S524DF4K15000024h port3
   ```

7. Return a port to a VPP:

   ```
   execute switch-controller virtual-port-pool return <FortiSwitch_device_ID> <port_name>
   ```

   NOTE: You must execute this command from the VDOM that owns the port.

   For example:

   ```
   execute switch-controller virtual-port-pool return S524DF4K15000024h port3
   ```

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
- 802.1x
- STP
- BPDU guard
- Root guard
- DHCP snooping

- IGMP snooping
- QoS
- Port security
- MCLAG

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>
            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
```

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
```

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 dump mac-limit-violations all <FortiSwitch_serial_number>`
- `diagnose switch-controller dump mac-limit-violations interface <FortiSwitch_serial_number> <port_name>`
- `diagnose switch-controller dump 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 dump 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
```

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 <switch-id>
      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 <switch-id>
      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-id> <port>
```

Display general PoE status

```
get switch-controller <fortiswitch-id> <port>
```

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>
            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 62.

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

```
config switch-controller managed-switch
   edit <switch-id>
      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 dump stp <FortiSwitch_serial_number> <instance_number>
```

For example:

```
FG100D3G15817028 # diagnose switch-controller dump 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 <switch-id>
    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 <switch-id>
    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 dump bpdu-guard-status <FortiSwitch_serial_number>
```

For example:

```
FG100D3G15817028 # diagnose switch-controller dump 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 <switch-id>
      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 <switch-id>
      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 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.

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

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set igmp-snooping {enable | disable}
            set igmps-flood-reports {enable | disable}
         end
      end
```

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port3
            set igmp-snooping enable
            set igmps-flood-reports 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
   collector-ip <x.x.x.x>
   collector-port <port_number>
end
```

Use the following CLI commands to configure sFlow:

```
config switch-controller managed-switch <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 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 <sn>
      config ports
         edit <VLAN_ID>
            arp-inspection-trust <untrusted | trusted>
         next
      end
   next
end
```

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

```
diagnose switch arp-inspection stats <FortiSwitch_Serial_Number>
```

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

```
diagnose switch 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 mirroring and is typically used for external analysis and capture.

Use the following CLI commands to configure FortiSwitch port mirroring:

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

NOTE: The `set status` and `set dst` commands are mandatory for port mirroring.

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
```

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 on page 88
- Configure the 802.1X settings for a virtual domain on page 89
- Override the virtual domain settings on page 89
- Define an 802.1X security policy on page 90
- Apply an 802.1X security policy to a FortiSwitch port on page 91
- Test 802.1x authentication with monitor mode on page 92
- Restrict the type of frames allowed through IEEE 802.1Q ports on page 92
- RADIUS accounting support on page 93

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
124/224/424/524/1024124/224/424/524/1024	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 < int >
   set max-reauth-attempt < int >
   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 reauthenticaion.
`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.
`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
```

Additional capabilities

This chapter covers the following topics:

- Execute custom FortiSwitch commands on page 94
- View and upgrade the FortiSwitch firmware version on page 95
- FortiSwitch log export on page 96
- FortiSwitch per-port device visibility on page 96
- FortiGate CLI support for FortiSwitch features (on non-FortiLink ports) on page 96
- Synchronizing the FortiGate unit with the managed FortiSwitch units on page 101
- Replacing a managed FortiSwitch unit on page 102

Execute custom FortiSwitch commands

From the FortiGate, you can execute FortiSwitch commands on the managed FortiSwitch.

This feature adds a simple scripting mechanism for users to execute generic commands on the switch.

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

Create a command

Use the following syntax to create a command file:

```
config switch-controller custom-command
   edit <cmd-name>
      set command "<FortiSwitch commands>"
```

Next, create a command file to set the STP max-age parameter:

```
config switch-controller custom-command
   edit "stp-age-10"
      set command "config switch stp setting
         set max-age 10
      end
   next
end
```

Execute a command

After you have created a command file, use the following command on the FortiGate to execute the command file on the target switch:

```
exec switch-controller custom-command <cmd-name> <target-switch>
```

The following example runs the `stp-age-10` command on the specified target FortiSwitch:

```
exec switch-controller custom-command stp-age-10 S124DP3X15000118
```

View and upgrade the FortiSwitch firmware version

You can view the current firmware version of a FortiSwitch unit and upgrade the FortiSwitch 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 display the latest version:

```
diagnose fdsm fortisw-latest-ver <model>
```

Use the following command to download the image:

```
diagnose fdsm fortisw-download <image id>
```

The following example shows how to download the latest image for FS224D:

```
FG100D3G15801204 (global) # diagnose fdsm fortisw-latest-ver FS224D
FS224D - 3.4.2 b192 03004000FIMG0900904002FG100D3G15801204 (global) #

diagnose fdsm fortisw-download 03004000FIMG0900904002

Download image-03004000FIMG0900904002:
#################################################################################
Result=Success
```

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 stage-tiered-swtp-image 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 restart-swtp-delayed ALL
```

FortiSwitch log export

You can enable and disable the managed FortiSwitch units to export their syslogs to the FortiGate. 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, FortiGate sets the user field to "fortiswitch-syslog” for each entry.

The following is the 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, 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.

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 dump mac-hosts_switch-ports
```

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
         it <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 an MCLAG with managed FortiSwitch units

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 topology, see Dual-homed servers connected to a pair of FortiSwitch units using an MCLAG on page 39 and Standalone FortiGate unit with dual-homed FortiSwitch access on page 41.

Notes

- 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.
- For static MAC addresses within an MCLAG, if one FortiSwitch learns the MAC address, the second FortiSwitch will automatically learn the MAC address.

To configure an MCLAG with managed FortiSwitch unis:

1. For each MCLAG peer switch, log into the FortiSwitch to create a LAG:
```
config switch trunk
   edit "LAG-member"
      set mode lacp-active
      set mclag-icl enable
      set members "<port>" "<port>"
   next
```
2. Enable the MCLAG on each managed FortiSwitch:
```
config switch-controller managed-switch
   edit "<switch-id>"
      config ports
```

```
         edit "<trunk name>"
            set type trunk
            set mode {static | lacp-passive | lacp-active}
            set bundle {enable | disable}
            set members "<port>,<port>"
            set mclag {enable | disable}
         next
      end
   next
```

3. Log into each managed FortiSwitch to check the MCLAG configuration:

   ```
   diagnose switch mclag
   ```

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.

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.

The storm control settings are global to all of the non-FortiLink ports on the managed switches. Use the following CLI commands to configure storm control:

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

You can override the global storm control settings for a FortiSwitch using the following commands:

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

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

Displaying port statistics

Port statistics will be accessed using the following FortiSwitch CLI command:

```
FG100D3G15804763 # diagnose switch-controller dump port-stats
S124DP3X16000413 port8
```

```
S124DP3X16000413 0 :
{
   "port8":{
      "tx-bytes":823526672,
      "tx-packets":1402390,
      "tx-ucast":49047,
      "tx-mcast":804545,
      "tx-bcast":548798,
      "tx-errors":0,
      "tx-drops":3,
      "tx-oversize":0,
      "rx-bytes":13941793,
      "rx-packets":160303,
      "rx-ucast":148652,
      "rx-mcast":7509,
      "rx-bcast":4142,
      "rx-errors":0,
      "rx-drops":720,
      "rx-oversize":0,
      "undersize":0,
      "fragments":0,
      "jabbers":0,
      "collisions":0,
      "crc-alignments":0,
      "l3packets":0
   }
}
```

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
```

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 the managed FortiSwitch unit:

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

Use one of the following commands to display the synchronization state of a FortiGate unit with a specific managed FortiSwitch unit:

```
execute switch-controller get-sync-status switch-id <FortiSwitch_serial_number>
execute switch-controller get-sync-status name <FortiSwitch_name>
```

Use the following command to display the synchronization state of a FortiGate unit with a group of managed FortiSwitch units:

```
execute switch-controller get-sync-status group <FortiSwitch_group_name>
```

Use the following command to check the synchronization state of all managed FortiSwitch units in the current VDOM:

```
execute switch-controller get-sync-status all
```

For example:

```
Managed-devices in current vdom root:

STACK-NAME: FortiSwitch-Stack-port15
```

SWITCH (NAME)	STATUS	CONFIG	MAC-SYNC	UPGRADE
S448DNTF18001048	Down	Idle	Idle	Idle

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.

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 95.
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 trunk configuration collected in step 2b. 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 auto-isl 1
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 auto-isl 1
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.

Troubleshooting

Troubleshooting FortiLink issues

If the FortiGate does not establish the FortiLink connection with the FortiSwitch, 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 interfaces
   ```
3. Verify that you can ping the FortiGate IP address:
   ```
   exec 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:
   ```
   exec switch-controller get-conn-status
   ```
2. Verify that ports for a specific FortiSwitch stack are connected to the correct locations:
   ```
   exec switch-controller get-physical-conn <FortiSwitch-Stack-ID>
   ```
3. Verify that all the ports for a specific FortiSwitch are up:
   ```
   exec 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.