FortiLink Guide—FortiSwitch Devices Managed by FortiOS 7.2

FortiSwitchOS 7.2.4

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 6, 2023
FortiSwitchOS 7.2.4 FortiLink Guide—FortiSwitch Devices Managed by FortiOS 7.2
11-724-848364-20230206

TABLE OF CONTENTS

Change log

Date	Change Description
January 31, 2023	Initial document release for FortiOS 7.2.4
February 1, 2023	Updated the “Optimizing the FortiSwitch network” section.
February 6, 2023	Updated the “Transitioning from a FortiLink split interface to a FortiLink MCLAG” section.

What's new in FortiOS 7.2.4

The following list contains new managed FortiSwitchOS features added in FortiOS 7.2.4. Click on a link to navigate to that section for further information:

- A new CLI command reports device statistics when network access control (NAC) is enabled. The `diagnose switch-controller telemetry show mac-stats` command reports the MAC addresses of known devices, the number of packets and bytes received, the number of seconds since the last update, and the age of the MAC counter in seconds. For more details, see Viewing device statistics on page 139.
- NAC now supports more connected devices—up to 48 times the maximum number of managed FortiSwitch units supported on the FortiGate device. You can use the `diagnose switch-controller mac-device nac known` command to check the number of known devices. When 95 percent of the maximum number of devices is reached, a warning icon is displayed in the *Matched NAC Devices* widget in the FortiOS GUI. When the maximum number is reached, a switch-controller event is logged.
- The range and default values for the `set nac-periodic-interval` command (under `config switch-controller system`) have changed. The default value is now 60, and the range of values is now 5-180.
- The range and default values for the `set dynamic-periodic-interval` command (under `config switch-controller system`) have changed. The default value is now 60, and the range of values is now 5-180.
- You can now specify static entries for DHCP snooping and dynamic ARP inspection (DAI) by manually associating an IP address with a MAC address in the FortiOS CLI. For more details, see Configuring DHCP-snooping static entries on page 166.
- The FG-180xF and FG-260xF models can now manage 196 FortiSwitch units.
- There is now a `set link-status` command under `config switch-controller managed-switch` in the FortiOS CLI.
- New tests have been added to the FortiSwitch recommendations in the *Security Fabric* > *Security Rating* page to help optimize your network. The tests check the following:
  - If the `poe-status` has been enabled under the `config switch-controller auto-config policy` command, FortiOS recommends that you disable it to prevent unpredictable problems caused by connecting two power sourcing equipment (PSE) ports.
  - If port 8 of an FS-108E or FS-108 unit is used for an inter-switch link (ISL), FortiOS recommends creating a custom auto-config policy.
  - If the configured speed is less than the maximum speed for a switch port, FortiOS recommends changing the port speed to the maximum amount.
  - Check if the inter-switch links (ISLs) and inter-chassis links (ICLs) are static to increase stability during events such as cable disconnections or power outages.
  - When a multichassis LAG (MCLAG) is recommended between two FortiSwitch units, there is a *Create MCLAG button* available under *WiFi & Switch Controller* > *Managed FortiSwitches* in the *Topology* view.
- A new *FortiView Internal Hubs* monitor in FortiOS will report the IP addresses and the number of bytes collected with flow tracking from devices behind a managed FortiSwitch unit. If you drill down on one of the devices, you can see a chart displaying the devices and how they are connected. For more details, see Configuring flow tracking and export on page 198.
- You can now use the FortiOS CLI to configure the Power over Ethernet (PoE) port mode (IEEE802.3 AF or IEEE802.3 AT), port priority (critical, high, medium, or low), and port power (normal, perpetual, or perpetual fast) on managed switches. For more details, see Configuring PoE port settings on page 83.

Introduction

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

NOTE: FortiLink is not supported in transparent mode.

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

FortiGate Model Range	Number of FortiSwitch Units Supported
FortiGate 40F, FortiGate-VM01	8
FortiGate 6xE, 8xE, 90E, 91E	16
FGR-60F, FG-60F, FGR-60F-3G4G, FG-61F, FG-80F, FG-80FB, FG-80FP, FG-81F, FG-81FP	24
FortiGate 100D, FortiGate-VM02	24
FortiGate 100E, 100EF, 100F, 101E, 140E, 140E-POE	32
FortiGate 200E, 201E	64
FortiGate 300D to 500D	48
FortiGate 300E to 500E	72
FortiGate 600D to 900D and FortiGate-VM04	64
FortiGate 600E to 900E	96
FortiGate 1000D to 15xxD	128
FortiGate 1100E to 26xxF	196
FortiGate-3*xxx* and up and FortiGate-VM08 and up	300

Supported models

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

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

Support of FortiLink features

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

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

Removal of switch-mgmt-mode

Starting in 7.2.0, there is no `switch-mgmt-mode` setting to set the FortiSwitch unit in `local` or `fortilink` mode anymore. The `config switch auto-network` command is used to form the ISL trunk and bring up the switch in FortiLink mode without rebooting the switch. The status of `auto-network` is `enable` by default in 7.2.x.

Additional command for FG-92D

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.

FortiSwitch management

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

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

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

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

This section covers the following topics:

Use the FortiGate GUI or CLI to configure the FortiSwitch units unless this manual specifically says to directly configure the FortiSwitch units. If you make configuration changes directly on the FortiSwitch units, the FortiGate device will not be aware of the changes, resulting in missing configurations when the FortiSwitch units are restarted.

Zero-touch management

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

Only one manager can be used at a time. Although FortiSwitchOS does not prevent more than one manager being chosen, a FortiSwitch unit cannot be authorized for more than one manager in most cases.

The FortiSwitch configuration does not need to be backed up before the FortiSwitch unit is managed, and the FortiSwitch unit does not need to be restarted when it becomes managed.

For a FortiSwitch unit that has already been configured, Fortinet recommends resetting the FortiSwitch unit to the factory defaults with the `execute factoryreset` command before upgrading to FortiSwitchOS 7.2.0 with FortiOS 7.2.0; otherwise, the FortiSwitch unit might not come online or might have a configuration synchronization error.

Under zero-touch management, the following settings are applied as factory defaults:

- All switch interfaces have VLAN 1 as the native VLAN.
- The internal system interface is set to VLAN 1, as well as all front-panel ports.
- The mgmt and internal interfaces have DHCP enabled.
- Auto topology is enabled.

  To disable auto topology, use the following commands:

```
config switch auto-network
   set status disable
end
```

- All ports are enabled for FortiLink auto-discovery.
- FortiLAN Cloud is enabled.
- FortiLink CAPWAP discovery is enabled.
- When a layer-2 network is detected, the Multiple Spanning Tree Protocol (MSTP) is applied to instances 0 and 15., and the internal switch interface is changed to a native VLAN of 4094.
- When a layer-3 network is detected, a static interchassis link (ICL) is created.

When the connection mode is DHCP, the gateway IP address is taken from the DHCP server by default (`set defaultgw enable` under the `config system interface` command) for both the internal and mgmt interfaces, which could prevent FortiLink from working (if multiple default routes are provided, FortiSwitchOS uses equal-cost multi-path routing [ECMP] to determine the route). If you are using DHCP for both mgmt and internal interfaces, Fortinet recommends resolving this conflict by disabling the default gateway on the interface that will not be used for managing FortiSwitch (`set defaultgw disable` under the `config system interface` command).

Configuring FortiLink

You need to physically connect the FortiSwitch unit to the FortiGate unit only *after* completing this section. Some settings are only possible when the FortiGate unit has not authorized any switches.

To configure FortiLink:

1. Enabling the switch controller on the FortiGate unit on page 14

2. Configuring the FortiLink interface on page 15

3. Auto-discovery of the FortiSwitch ports on page 20

1. Enabling 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 *Core 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. Configuring the FortiLink interface

The FortiLink interface is created automatically as an aggregate interface type; if the FortiGate model does not support the aggregate interface type, the FortiLink interface is created automatically as a hardware switch. Fortinet recommends keeping the default type of the FortiLink; however, if a physical interface or soft-switch interface type is required, the interface must be enabled for FortiLink using the FortiOS CLI, and then the default FortiLink interface can be deleted.

The FortiLink interface type is dependent on the network topology to be deployed. See Determining the network topology on page 36.

Using the FortiGate GUI

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

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

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

Configure the FortiLink interface

To configure the FortiLink interface on the FortiGate unit:

1. Go to *WiFi & Switch Controller* > *FortiLink Interface*.
2. Select + in the Interface members field and then select the ports to add to the FortiLink interface.
   NOTE: If you do not see any ports listed in the Select Entries pane, go to *Network* > *Interfaces*, right-click the FortiLink physical port, select *Edit*, delete the port from the Interface Members field, and then select *OK*.
3. Configure the *IP/Network Mask* for your network.
4. Select *Automatically authorize devices*.
5. Select *Apply*.

FortiLink split interface

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

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

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

NOTE: The FortiLink split interface must be enabled before MCLAG is enabled on the FortiSwitch unit. After MCLAG is enabled, you can disable the FortiLink split interface to make both links active. See MCLAG peer groups on page 60.

Using the FortiGate GUI:

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

Using the FortiGate CLI:

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

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

For example, if the IP address, members, and automatic FortiSwitch authorization are enabled:

```
config system interface
   edit "fortilink"
      set ip 172.16.16.254 255.255.255.0
      set member "port9" "port10"
      set auto-auth-extension-device enable
   next
end
```

If required, remove a physical port from the `lan` interface:

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

```
end
```

2.1 Custom FortiLink interfaces

Choosing the FortiGate ports

The FortiLink can consist of a single (physical) or multiple ports (802.3ad aggregate, hardware switch, or software switch).

FortiLink is supported on all Ethernet ports except HA and MGMT.

If the default FortiLink interface was removed, on the FortiGate GUI, edit the interface and select *Dedicated to FortiSwitch*. Optionally, set the IP address and enable auto-authorization. Disable the split-interface if the interface is the aggregate type and is connecting all members to the same FortiSwitch unit.

NOTE: The FortiLink interface type is dependent upon the network topology to be deployed. See Determining the network topology on page 36.

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, port1 is configured as the FortiLink port.

1. Configure port1 as the FortiLink interface with the customer IP address and automatic authorization:

```
config system interface
   edit "port1"
      set fortilink enable
      set ip 172.16.16.254 255.255.255.0
      set auto-auth-extension-device enable
   next
end
```

   If required, remove port1 from the `lan` interface:

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

2. (Optional) Configure an NTP server on port1:

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

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

```
config switch-controller managed-switch
   edit FS224D3W14000370
```

```
      set fsw-wan1-admin enable
   end
end
```

4. 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. Check the FortiGate feature matrix to check which models support the hardware switch and LAG (802.3ad aggregate) interfaces.

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

Using the GUI:

To configure the FortiLink interface on the FortiGate unit:

1. Go to *Network* > *Interfaces* and click *Create New*.
2. Enter a name for the interface (11 characters maximum).
3. For the type, select *802.3ad aggregate*.
4. Select + in the *Interface members* field and then select the ports to add to the FortiLink interface.
   NOTE: If you do not see any ports listed in the *Select Entries* pane, go to *Network* > *Interfaces*, edit the *lan* or *internal* interface, delete the port from the *Interface Members* field, and then click *OK*.
5. Configure the IP/Network Mask for your network.
6. Select *Automatically authorize devices*.
7. Click *Apply*.
   If you want to add a third FortiLink interface, go to *WiFi & Switch Controller* > *FortiLink Interface* and click *Create new*.

Using the CLI:

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 with a maximum of 11 characters)
      set ip 172.16.16.254 255.255.255.0
      set type aggregate
      set member port4 port5
      set fortilink enable
      (optional) set fortilink-split-interface disable
```

```
    next
end
```

NOTE: If the members of the aggregate interface connect to the same FortiSwitch unit, you must disable `fortilink-split-interface`.

Configure a LAG on a FortiLink-enabled software switch

Starting in FortiOS 7.2.0 with FortiSwitchOS 7.2.0, you can configure a link-aggregation group (LAG) as a member of a software switch that is being used for FortiLink. Previously, you could not add a LAG to a software switch that was being used for FortiLink.

- You must set `fortilink-neighbor-detect` to `lldp`.
- Aggregate interfaces do not automatically form an inter-switch link (ISL) within a FortiGate software switch. You must create the aggregate interfaces and add them to the software switch.
- The FortiSwitch unit will automatically form an ISL with correctly configured FortiGate aggregate interfaces.

In the following example, aggregate1 and aggregate2 are FortiGate aggregate interfaces. The third interface, switch3, is a software switch with FortiLink enabled. The three interfaces are configured, and then aggregate1 and aggregate2 are added to the software switch interface.

```
config system interface
   edit "aggregate1"
      set vdom "root"
      set type aggregate
      set member "port11"
      set device-identification enable
      set role lan
      set snmp-index 25
   next
   edit "aggregate2"
      set vdom "root"
      set type aggregate
      set member "port7"
      set device-identification enable
      set role lan
      set snmp-index 34
   next
   edit "switch3"
      set vdom "root"
      set fortilink enable
      set ip 10.255.1.1 255.255.255.0
      set allowaccess ping fabric
      set type switch
      set lldp-reception enable
      set lldp-transmission enable
      set snmp-index 26
      set fortilink-neighbor-detect lldp
      set swc-first-create 64
      config ipv6
         set ip6-send-adv enable
         set ip6-other-flag enable
```

```
      end
   next
end

config system switch-interface
   edit "switch3"
      set vdom "root"
      set member "aggregate1" "aggregate2"
   next
end
```

3. Auto-discovery of the FortiSwitch ports

Starting with FortiSwitch 7.2.0, all ports are enabled for auto-discovery by default.

NOTE: For details on how to connect the FortiSwitch topology, see Determining the network topology on page 36.

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.

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

FortiSwitch Model	Default Auto-FortiLink ports
FS-424E-Fiber	port1-port30
FS-426E-FPOE-MG	port23-port30
FS-448D, FS-448D-POE, FS-448D-FPOE	port45–port52
FS-524D, FS-524D-FPOE	port21–port30
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

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

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
```

Automatic inter-switch links (ISLs)

After a FortiSwitch unit is discovered and in FortiLink mode, all ports are enabled for FortiLink. Connect another FortiSwitch unit to any of the already discovered FortiSwitch ports, and the ISL is formed automatically, and the new unit is discovered by the FortiGate unit.

Static ISL trunks

In some cases, you might want to manually create an ISL trunk, for example, for FortiLink mode over a point-to-point layer-2 network or for FortiLink mode over a layer-3 network. You can also enable or disable automatic VLAN configuration on the manually created (static) ISL trunk. The static ISL feature can also be used to lock down the FortiLink topology after automatic discovery.

To manually create an ISL trunk:

```
config switch trunk
   edit "<trunk_name>"
      set static-isl enable
      set static-isl-auto-vlan {enable | disable}
   end
```

Deleting a FortiLink interface

If you have any problems with deleting a FortiLink interface, disable it first using the CLI:

```
config switch interface
   edit <FortiLink_interface_name>
      set fortilink disable
   end
```

Optional FortiLink configuration required before discovering and authorizing FortiSwitch units

This section covers the following topics:

Migrating the configuration of standalone FortiSwitch units

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

To get the script and instructions, go to:

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

VLAN interface templates for FortiSwitch units

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

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

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

To ensure that switch VLAN interface names are unique for each system, the following naming rules are used:

- root VDOM: The interface names are the same as the template names.
- other VDOMs: The interface name is created from the template name and the SNMP index of the interface. For example, if the template name is `quarantined` and the SNMP index is `29`, the interface name is `quarantined.29`.

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

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

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

Create VLAN interface templates

To configure the VLAN interface templates:

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

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

To assign the templates to the specific traffic types:

```
config switch-controller initial-config vlans
   set default-vlan <template>
   set quarantine <template>
   set rspan <template>
   set voice <template>
   set video <template>
   set nac <template>
end
```

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

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

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

```
end
```

The default value is `169.254.0.0 255.255.0.0`.

Example

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

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

```
config switch-controller initial-config template
   edit "default"
      set vlanid 1
      set auto-ip disable
   next
   edit "quarantine"
      set vlanid 4093
      set dhcp-server enable
   next
   edit "rspan"
      set vlanid 4092
      set dhcp-server enable
   next
   edit "voice"
      set vlanid 4091
      set dhcp-server enable
   next
   edit "video"
      set vlanid 4090
      set dhcp-server enable
   next
   edit "onboarding"
      set vlanid 4089
      set dhcp-server enable
   next
end
config switch-controller initial-config vlans
   set default-vlan "default"
   set quarantine "quarantine"
   set rspan "rspan"
   set voice "voice"
   set video "video"
   set nac "onboarding"
end
```

To see the automatically created VLANs and DHCP servers:

```
show system interface
   edit "default"
      set vdom "root"
      set snmp-index 24
      set switch-controller-feature default-vlan
      set interface "fortilink"
```

```
      set vlanid 1
    next
    edit "quarantine"
      set vdom "root"
      set ip 169.254.11.1 255.255.255.0
      set description "Quarantine VLAN"
      set security-mode captive-portal
      set replacemsg-override-group "auth-intf-quarantine"
      set device-identification enable
      set snmp-index 25
      set switch-controller-access-vlan enable
      set switch-controller-feature quarantine
      set color 6
      set interface "fortilink"
      set vlanid 4093
    next
    ...
end
show system dhcp server
    edit 2
      set dns-service local
      set ntp-service local
      set default-gateway 169.254.1.1
      set netmask 255.255.255.0
      set interface "fortilink"
      config ip-range
        edit 1
          set start-ip 169.254.1.2
          set end-ip 169.254.1.254
        next
      end
      set vci-match enable
      set vci-string "FortiSwitch" "FortiExtender"
    next
    edit 3
      set dns-service default
      set default-gateway 169.254.11.1
      set netmask 255.255.255.0
      set interface "quarantine"
      config ip-range
        edit 1
          set start-ip 169.254.11.2
          set end-ip 169.254.11.254
        next
      end
      set timezone-option default
    next
    ...
end
```

Automatic provisioning of FortiSwitch firmware upon authorization

Starting in FortiOS 7.0.0, administrators can use the FortiOS CLI to upload the FortiSwitch firmware and then configure the managed FortiSwitch units to be automatically upgraded with the uploaded firmware when the switches were

authorized by FortiLink. On FortiGate models that have a hard disk, up to four images for the same FortiSwitch model can be uploaded. For FortiGate models without a hard disk, only one image can be uploaded for each FortiSwitch model.

Starting in FortiOS 7.0.4, administrators no longer need to upload the FortiSwitch firmware. Instead, administrators can configure the managed FortiSwitch units to be automatically upgraded to the latest FortiSwitchOS version available in FortiGuard when the switches are authorized by FortiLink. If the FortiSwitch units are already running the latest version of FortiSwitchOS when they are authorized, no changes are made.

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

To configure the automatic provisioning using uploaded FortiSwitch firmware:

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

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

In the following example, a FortiSwitch 248E-POE is upgraded from FortiSwitchOS 6.4.3 to 6.4.4:

1. Upload the FortiSwitch image to the FortiGate device and confirm that it was uploaded successfully:

```
# execute switch-controller switch-software upload tftp 248-454.out 172.18.60.160

Downloading file 248-454.out from tftp server 172.18.60.160...
##########################
Image checking ...
Image MD5 calculating ...
Image Saving S248EP-IMG.swtp ...
Successful!

File Syncing...
```

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

ImageName                       ImageSize(B)   ImageInfo              Uploaded Time
S248EP-v6.4-build454-IMG.swtp   28579517       S248EP-v6.4-build454   Mon Nov 30
15:06:07 2020
```

2. On the FortiSwitch unit, check the current version:

```
# get system status
Version: FortiSwitch-248E-POE v6.4.3,build0452,201029 (GA)
```

```
Serial-Number: S248EPTF18001842
BIOS version: 04000004
System Part-Number: P22169-02
Burn in MAC: 70:4c:a5:e1:53:f6
Hostname: S248EPTF18001842
Distribution: International
Branch point: 452
System time: Wed Dec 31 16:11:17 1969
```

3. On the FortiGate device, enable firmware provisioning and specify the version:

```
config switch-controller managed-switch
       edit S248EPTF18000000
              set firmware-provision enable
              set firmware-provision-version 6.4.0454
       next
end
```

4. On the FortiGate device, authorize the FortiSwitch unit:

```
config switch-controller managed-switch
       edit S248EPTF18000000
              set fsw-wan1-peer flink
              set fsw-wan1-admin enable
       next
end
```

5. When the authorized FortiSwitch unit is in FortiLink mode, it automatically starts upgrading to the provisioned firmware:

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

================================================================================================
============================
VDOM : vdom1
       FS1D243Z170000XX  FS1D24-v6.4.0-build456,201121 (Interim)        (0/0/0)   N/A  (Idle)
       S248DN3X170002XX  S248DN-v6.4.0-build456,201121 (Interim)        (0/0/0)   N/A  (Idle)
       S248EPTF18000000  S248EP-v6.4.3-build452,201029 (GA)             (14/0/0)   N/A
(Upgrading)
```

6. Check the version when the upgrade is complete:

```
# execute switch-controller get-conn-status
Managed-devices in current vdom vdom1:

FortiLink interface : flink
SWITCH-ID         VERSION           STATUS         FLAG   ADDRESS              JOIN-TIME
          NAME
FS1D243Z17000032  v6.4.0 (456)      Authorized/Up   -   169.254.1.3     Mon Nov 30
11:08:10 2020    -
S248DN3X170002XX  v6.4.0 (456)      Authorized/Up   -   169.254.1.4     Mon Nov 30
11:08:32 2020    -
S248EPTF18000000  v6.4.4 (454)      Authorized/Up   C   169.254.1.6     Mon Nov 30
15:20:53 2020    -
```

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

1. On the FortiGate device, configure automatic provisioning:

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

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

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

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

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

Discovering

This section covers the following topics:

Authorizing

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

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

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

Preparing the FortiSwitch unit

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

Optional FortiLink configuration

This section covers the following topics:

Assigning roles to FortiLink VLAN interfaces

If you are using the FortiGate unit's security rating feature, you need to assign a role of *LAN*, *WAN*, or *DMZ* to your FortiLink VLAN interfaces before referencing them in any firewall policies. If this is not done, the security rating score is lowered until the issue is remedied, due to failing the "Interface Classification" requirement.

Using the FortiSwitch serial number for automatic name resolution

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

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

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

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

```
FG100D3G15817028 (root) # execute ping S524DF4K15000024.fsw
PING S524DF4K15000024.fsw (123.456.7.8): 56 data bytes
64 bytes from 123.456.7.8: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=1 ttl=64 time=0.0 ms
```

```
64 bytes from 123.456.7.8: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=3 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=4 ttl=64 time=0.0 ms
```

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

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

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

```
FG100D3G15817028 (root) # execute ping S524DF4K15000024
PING S524DF4K15000024.fsw (123.456.7.8): 56 data bytes
64 bytes from 123.456.7.8: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=3 ttl=64 time=0.0 ms
64 bytes from 123.456.7.8: icmp_seq=4 ttl=64 time=0.0 ms

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

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
```

Disabling the FortiSwitch console port login

Starting in FortiOS 7.2.0 with FortiSwitchOS 7.2.0, administrators can use the FortiSwitch profile to control whether users can log in with the managed FortiSwitchOS console port. By default, users can log in with the managed

FortiSwitchOS console port.

To change the FortiSwitch profile:

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

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

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

To change which FortiSwitch profile is used by a managed switch

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

For example:

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

Using automatic network detection and configuration

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

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

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

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

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

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

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

```
config switch-controller auto-config policy
   edit <policy_name>
      set qos-policy <automatic-configuration QoS policy>
```

```
      set storm-control-policy <automatic-configuation storm-control policy>
      set poe-status {enable | disable}
      set igmp-snooping-flood-reports {enable | disable}
      set mcast-snooping-flood-traffic {enable | disable}
   end
```

Limiting the number of parallel processes for FortiSwitch configuration

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

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

Configuring access to management and internal interfaces

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

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

For example:

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

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

```
         set min-bundle <int>
         set max-bundle <int>
         set members <port1 port2 ...>
      next
   end
end
```

```
end
```

Enabling FortiLink VLAN optimization

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

NOTE: VLAN optimization is enabled by default.

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

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

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

Configuring 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
```

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 FortiGate 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
```

If provisioned with custom commands on the FortiGate device, the configuration is preserved on the FortiGate device. See Executing custom FortiSwitch scripts on page 241.

Multiple FortiLink interfaces

If you are adding a second FortiLink interface, use the CLI to enable FortiLink. For example:

```
config system interface
   edit "fortilink_2"
      set fortilink enable
   next
end
```

After that, the interface is available in the GUI to complete the settings. Click *Create* to add additional FortiLink interfaces.

Grouping FortiSwitch units

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

Using the GUI:

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

Using the CLI:

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

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

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

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

Disabling 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
```

Determining the network topology

The FortiGate unit requires an active FortiLink interface 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.

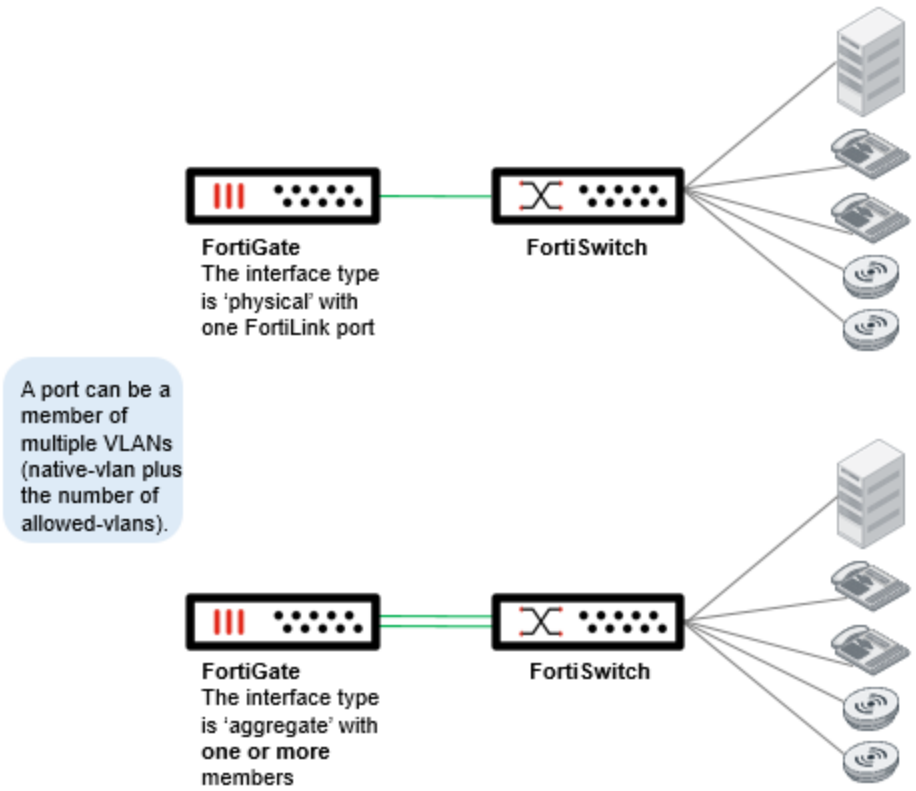
This section covers the following topics:

Single FortiGate managing a single FortiSwitch unit

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

NOTE:

- For the aggregate interface, you must disable the split interface on the FortiGate unit.
- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface, the `lacp-mode` of the FortiLink aggregate interface must be set to `static`. Unless MCLAG is enabled and you are using 6.2.0 or later, see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 60 for details.



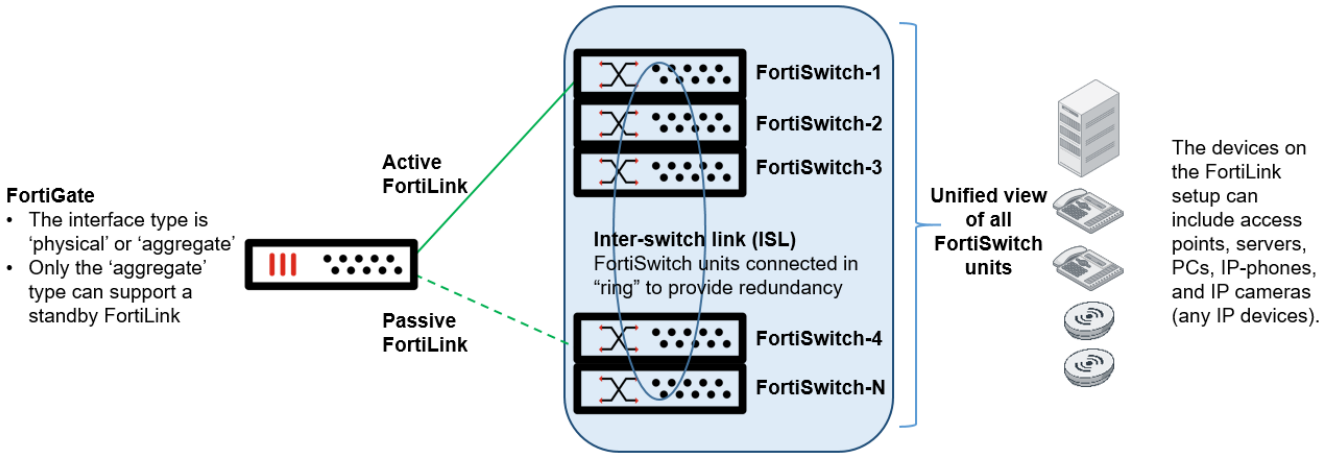
Single FortiGate unit managing a stack of several FortiSwitch units

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

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

NOTE:

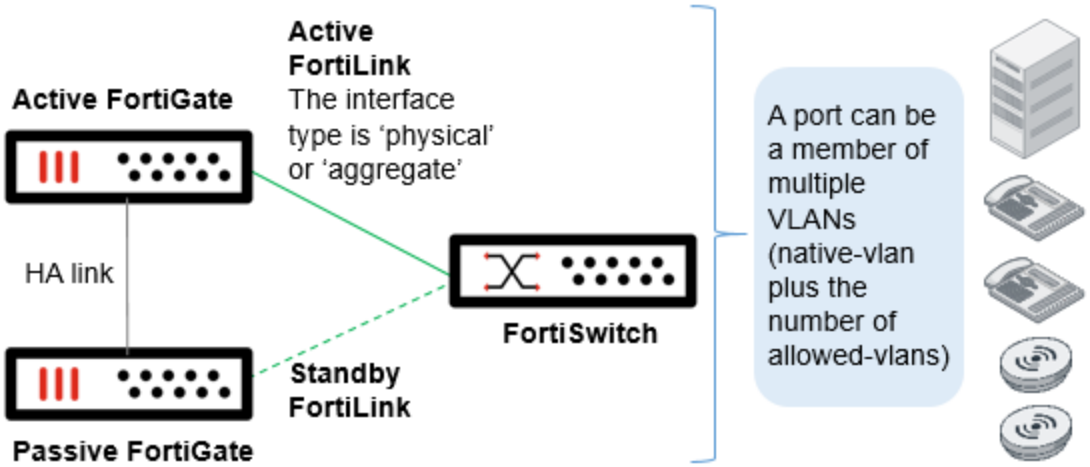
- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface, the `lacp-mode` of the FortiLink aggregate interface must be set to `static`. Unless MCLAG is enabled and you are using 6.2.0 or later, see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 60 for details.
- Do not create loops or rings with the FortiGate unit in the path.



HA-mode FortiGate units managing a single FortiSwitch unit

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

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



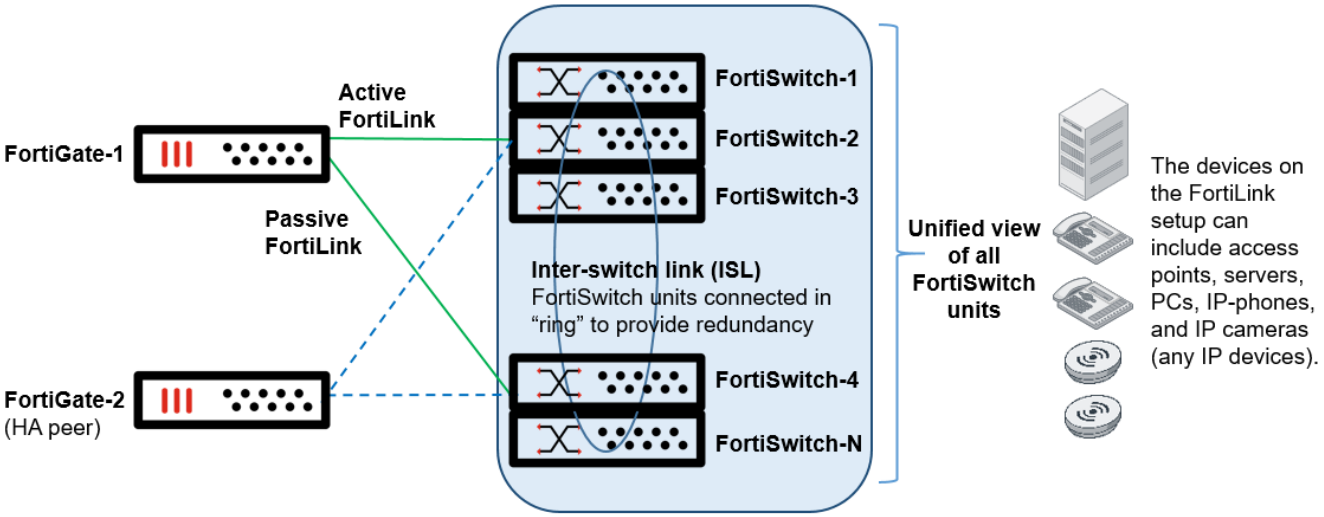
HA-mode FortiGate units managing a stack of several FortiSwitch units

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

When using an aggregate interface for the active/standby FortiLink configuration, make sure the FortiLink split interface is enabled (this forces one link to be active and the rest to be standby links, which avoids loops in the network). This option can be disabled later if you enable an MCLAG. See Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 60.

NOTE:

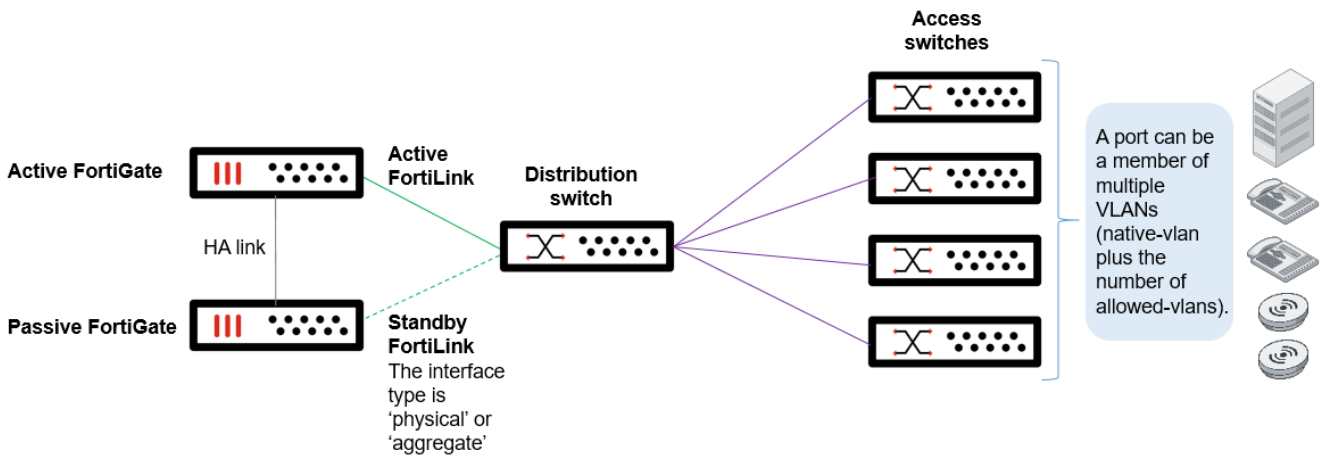
- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface, the `lacp-mode` of the FortiLink aggregate interface must be set to `static`. Unless MCLAG is enabled and you are using 6.2.0 or later, see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 60 for details.
- Before FortiOS 6.2.0, when using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive. Starting in FortiOS 6.2.0, the FortiGate HA mode can be either active-passive or active-active.



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

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

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



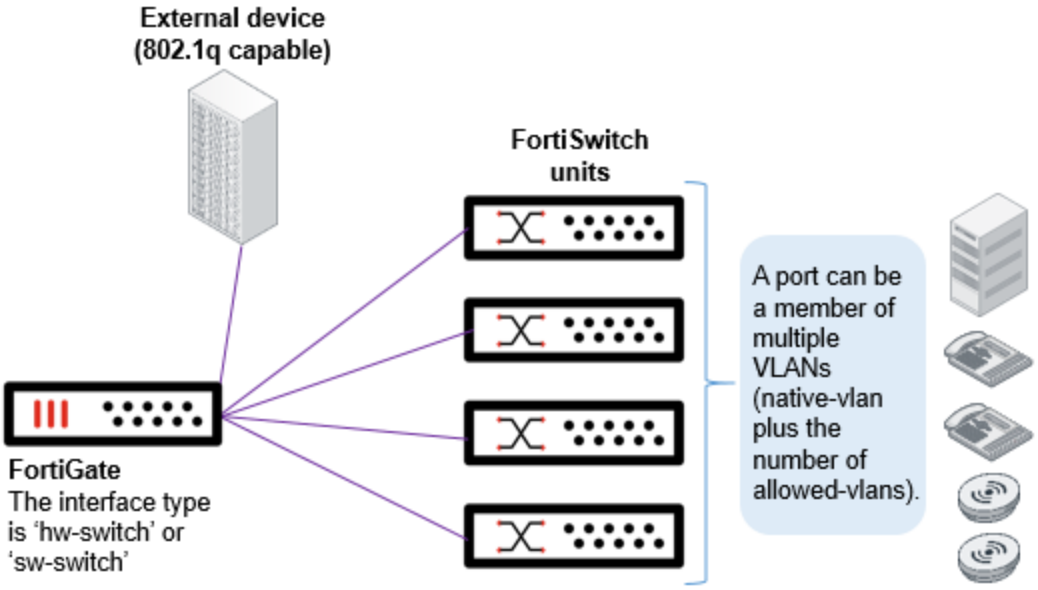
Single FortiGate unit managing multiple FortiSwitch units (using a hardware or software switch interface)

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

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

NOTE:

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



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

In most FortiLink topologies, MCLAG or LAG configurations are used for FortiSwitch redundancy. However, some FortiGate models do not support the FortiLink aggregate interface, or some FortiSwitch models do not support MCLAG.

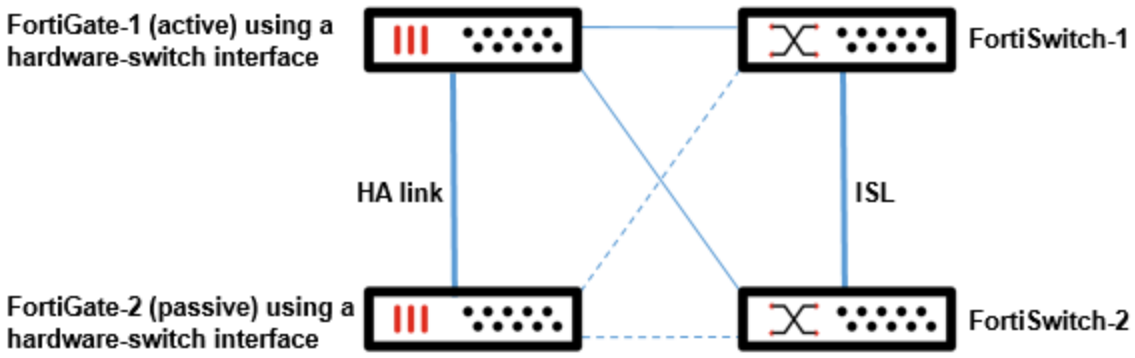
The following network topology uses a hardware-switch interface on each FortiGate unit. Each FortiSwitch unit is connected to a single port of the hardware-switch interface of the FortiGate unit. The inter-switch link (ISL) between the FortiSwitch units provides redundancy.

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

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

NOTE:

- The FortiLink interface uses the Link Layer Discovery Protocol (LLDP) for neighbor detection. LLDP transmission must be enabled with the `set lldp-transmission enable` command before enabling Spanning Tree Protocol (STP).
- STP and STP forwarding are both supported by the FortiLink hardware-switch interface.
- The software-switch interface is not supported.
- If the FortiGate model does not support aggregate interfaces, you need to configure the FortiGate unit to be the Common and Internal Spanning Tree (CIST) by assigning the lowest STP priority to the FortiGate unit and placing each switch in a different region. You can assign the STP priority to the FortiGate unit with the `set switch-priority` command under `config system stp`. You can move a switch to another region with the `set revision` command under `config stp-settings`.



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

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

NOTE:

- The `set fortilink-p2p` command is available in FortiLink mode and standalone mode. The `set fortilink-p2p-tpid` command is available only in FortiLink mode.
- The FS-108E, FS-108E-POE, FS-108E-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE, FS-148F, FS-148F-POE, FS-148F-FPOE, FS-124F, FS-124F-POE, and FS-124F-FPOE models support only the default 0x8100 TPID; TPID changes are not supported.

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

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

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

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

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

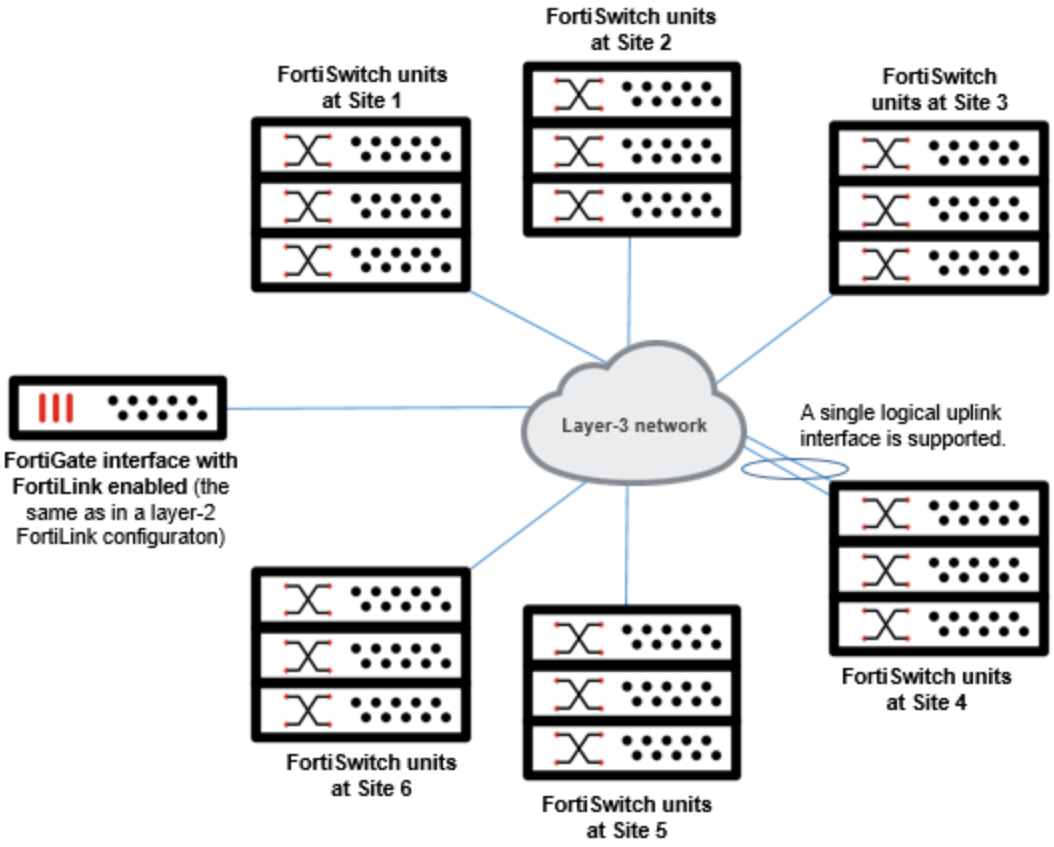
Starting in FortOS 6.4.3, you can now configure a FortiLink-over-layer-3 network to use the FortiLink interface as the source IP address for the communication between the FortiGate unit and the FortiSwitch unit. You can still use the outbound interface as the source IP address if you prefer.

After you have configured FortiLink mode over a layer-3 network, downgrading FortiSwitchOS is not supported.

To use the FortiLink interface as the source IP address:

```
config system interface
   edit <FortiLink_interface>
      set switch-controller-source-ip fixed
   end
```

In-band management



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

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

1. Reset the FortiSwitch to factory default settings with the `execute factoryreset` command.
2. If you are using DHCP discovery with DHCP option 138, the FortiSwitch unit automatically connects to the FortiGate unit and establishes FortiLink. If you are not using DHCP discovery with DHCP option 138, you can configure DHCP discovery with a different `ac-dhcp-option-code` or configure static discovery to find the IP address of the FortiGate unit (switch controller) that manages this switch. If you configure static discovery, you need to create a static inter-switch link (ISL) trunk and then enable or disable automatic VLAN configuration on the manually created (static) ISL trunk.

   To use DHCP discovery:

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

   To use static discovery:

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

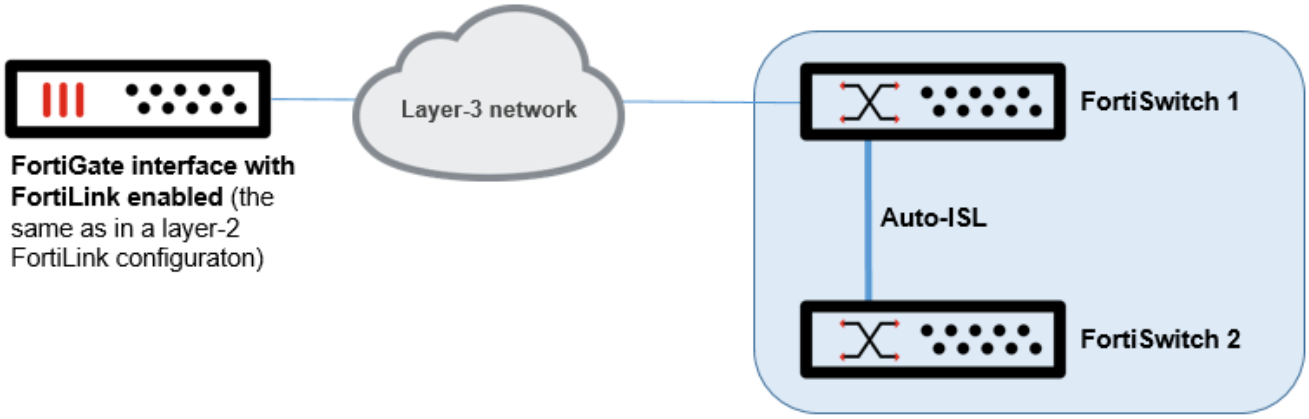
```
      config ac-list
         edit <id>
            set ipv4-address <IPv4_address>
         next
      end
   end
   config switch trunk
      edit <trunk_name>
         set static-isl enable
         set static-isl-auto-vlan {enable | disable}
      next
   end
```

NOTE:

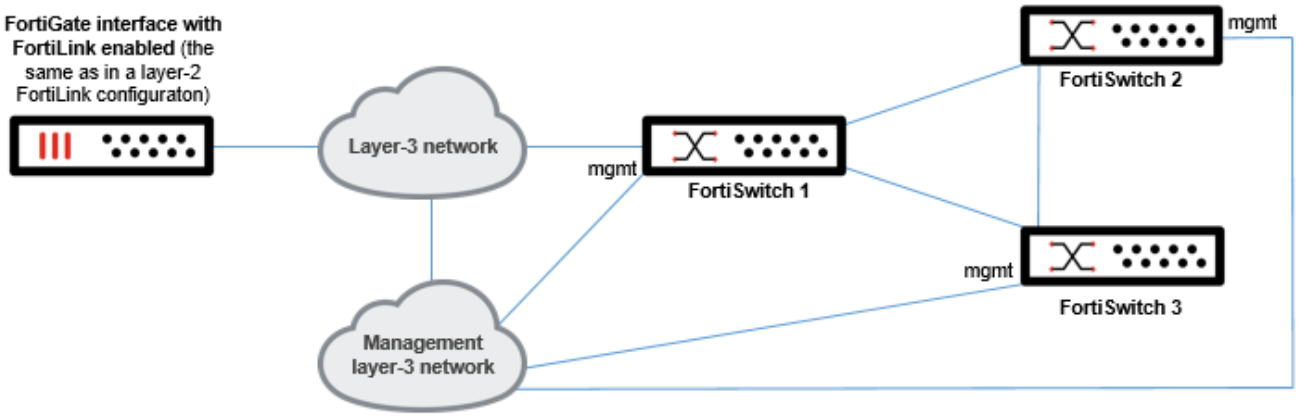
- Make certain that each FortiSwitch unit can successfully ping the FortiGate unit.
- The NTP server must be configured on the FortiSwitch unit either manually or provided by DHCP. The NTP server must be reachable from the FortiSwitch unit.
- In addition to the two layer-3 discovery modes (DHCP and static), 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 2) for additional switches (FortiSwitch 2 in the following diagram). Check that each FortiSwitch unit can reach the FortiGate unit.



Out-of-band management



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 and 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:

- 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.
- NAT is not supported between the FortiSwitch unit and FortiGate unit.

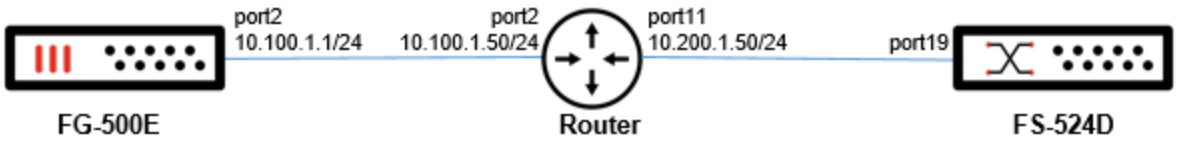
Starting in FortiOS 7.2.1, the `set fortilink-l3-mode` command is deprecated. Instead, you can create a static inter-switch link (ISL) trunk and then enable or disable automatic VLAN configuration on the manually created (static) ISL trunk:

```
config switch trunk
   edit <trunk_name>
      set static-isl enable
      set static-isl-auto-vlan {enable | disable}
   next
end
```

Managing FortiSwitch units on VXLAN interfaces

You can use Virtual Extensible LAN (VXLAN) interfaces to create a layer-2 overlay network when managing a FortiSwitch unit over a layer-3 network. After a VXLAN tunnel is set up between a FortiGate device and a FortiSwitch unit, the FortiGate device can use the VXLAN interface to manage the FortiSwitch unit. Only the management traffic uses the VXLAN tunnel; the FortiSwitch data traffic does not go through the VXLAN tunnel to the FortiGate device.

In the following configuration example, the FG-500E device is connected with a VXLAN tunnel to the FS-524D unit. After FortiLink is enabled on the VXLAN interface, the FortiGate device can manage the FortiSwitch unit.



To manage the FortiSwitch unit with the VXLAN interface:

1. Configure the FortiSwitch unit.
2. Configure the FortiGate device.

Configure the FortiSwitch unit

1. Configure a VLAN to use as the VXLAN interface.

```
config system interface
   edit "vlan-1000"
      set ip 10.200.1.2 255.255.255.0
      set allowaccess ping
```

```
      set vlanid 1000
      set interface "internal"
   next
end
```

2. Configure the VXLAN interface with the remote IP address of the FortiGate device.

```
config system vxlan
   edit "vx-4094"
      set vni 123456
      set vlanid 4094
      set interface "vlan-1000"
      set remote-ip "10.100.1.1"
   next
end
```

3. Configure a static route with the VXLAN remote IP address as the destination.

```
config router static
   edit 1
      set device "vlan-1000"
      set dst 10.100.1.1 255.255.255.255
      set gateway 10.200.1.50
   next
end
```

4. Configure the switch trunk to make it static and disable the automatic VLAN provisioning.

```
config switch trunk
   edit "__FoRtILnk0L3__"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port19"
   next
end
```

5. Configure the FortiLink interface to set the native VLAN to match the VLAN used for the VXLAN defined in step 1.

```
config switch interface
   edit "__FoRtILnk0L3__"
      set native-vlan 1000
      set allowed-vlans 1,1000,4088-4094
      set dhcp-snooping trusted
      ....
   next
end
```

6. If you are not using DHCP option 138 to inform the FortiSwitch unit of the FortiGate IP address, enable static discovery.

```
config switch-controller global
   set ac-discovery-type static
   config ac-list
      edit 1
         set ipv4-address 10.255.2.1
      next
   end
end
```

7. Assign VLAN ID 4094 to the “internal” interface, which will be used to establish the FortiLink connection with the FortiGate device over VXLAN.

```
config switch interface
   edit "internal"
      set native-vlan 4094
```

```
   next
end
```

8. Make certain that the FortiSwitch unit can be discovered by the FortiGate device over VXLAN.

```
config switch global
     set auto-fortilink-discovery enable
end
```

Configure the FortiGate device

1. Configure the system interface.

```
config system interface
   edit "port2"
      set vdom "root"
      set ip 10.100.1.1 255.255.255.0
      set allowaccess ping https http
   next
end
```

2. Configure the VXLAN interface.

```
config system vxlan
   edit "flk-vxlan"
      set interface "port2"
      set vni 123456
      set remote-ip "10.200.1.2"
   next
end
```

3. Configure the FortiLink interface as the VXLAN type and set the IP address.

```
config system interface
   edit "flk-vxlan"
      set fortilink enable
      set ip 10.255.2.1 255.255.255.0
   next
end
```

4. Configure a static route.

```
config router static
   edit 0
      set dst 10.200.1.0 255.255.255.0
      set gateway 10.100.1.50
      set distance 5
      set device "port2"
   next
end
```

5. Configure the DHCP server with option 138 to provide the switch-controller IP address to the FortiSwitch unit. DNS and NTP services are provided by the FortiGate device.

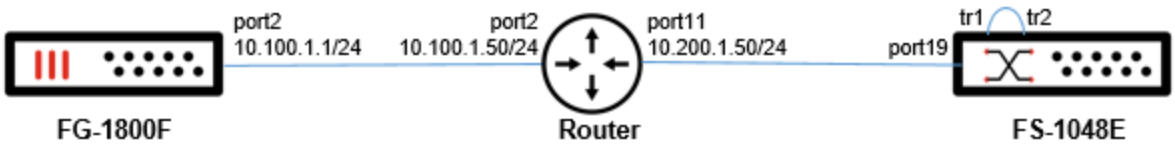
```
config system dhcp server
   edit 0
      set dns-service local
      set ntp-service local
      set default-gateway 10.255.2.1
      set netmask 255.255.255.0
      set interface "flk-vxlan"
      config ip-range
         edit 1
            set start-ip 10.255.2.2
```

```
            set end-ip 10.255.2.254
         next
      end
      config options
         edit 1
            set code 138
            set type ip
            set ip "10.255.2.1"
         next
      end
      set vci-match enable
      set vci-string "FortiSwitch"
   next
end
```

FortiSwitch VLANs over VXLAN

On some FortiSwitch models, you can send user traffic over a VXLAN tunnel, creating a layer-2 overlay over a layer-3 network, allowing Security Fabric functionality to be applied to devices connecting to the FortiSwitch unit.

In the following configuration example, the FG-1800F device is connected with a VXLAN tunnel to the FS-1048E unit. After FortiLink is enabled on the VXLAN interface, the FortiGate device can manage the FortiSwitch unit.



1. Configure a VLAN to use as the VXLAN interface.

```
config system interface
   edit "vlan-1000"
      set ip 10.200.1.2 255.255.255.0
      set vlanid 1000
      set interface "internal"
   next
end
```

2. Configure a static route with the VXLAN remote IP address as the destination.

```
config router static
   edit 1
      set device "vlan-1000"
      set dst 10.100.1.1 255.255.255.255
      set gateway 10.200.1.50
   next
end
```

3. Configure the link monitor to monitor access to the gateway.

```
config system link-monitor
   edit "1"
      set srcintf "vlan-1000"
      set protocol ping
      set gateway-ip 10.200.1.50
      set interval 60
   next
end
```

4. Configure the switch trunk to make it static and disable the automatic VLAN provisioning.

```
config switch trunk
   edit "__FoRtILnk0L3__"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port19"
   next
end
```

5. Configure the FortiLink interface so that the native VLAN matches the VLAN used for the VXLAN defined in step 1.

```
config switch interface
   edit "__FoRtILnk0L3__"
      set native-vlan 1000
   next
end
```

6. Assign VLAN ID 4094 to the “internal” interface that will be used to establish the FortiLink connection with the FortiGate device over VXLAN.

```
config switch interface
   edit "internal"
      set native-vlan 4094
   next
end
```

7. If you are not using DHCP option 138 to inform the FortiSwitch unit of the FortiGate IP address, enable static discovery.

```
config switch-controller global
   set ac-discovery-type static
   config ac-list
      edit 1
         set ipv4-address 10.255.2.1
      next
   end
end
```

8. Connect two physical ports to each other as a loopback. In this example, `port23` and `port24` are connected.
9. Create two trunks, each trunk with one physical link that is connected as a loopback. In this example, trunk `tr1` is created with `port23` as a member. Trunk `tr2` is created with `port24` as a member. `port24` forms a loopback with `port23`.
10. Configure trunk `tr2` as `static-isl`. Leave the rest of the values at the defaults.

```
config switch trunk
   edit "tr2"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port24"
   next
end
```

11. Configure the `tr2` interface with a native VLAN of 4094 and the allowed VLANs as 1-4094.

```
config switch interface
   edit "tr2"
      set native-vlan 4094
      set allowed-vlans 1-4094
   next
end
```

12. Configure trunk `tr1` as `static-isl` and `static-isl-auto-vlan`. Leave the rest of the values at the defaults. This trunk will be used in the VXLAN tunnel-loopback interface. `port23` forms a loopback with `port24`.

```
config switch trunk
   edit "tr1"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port23"
   next
end
```

13. Configure the `tr1` interface with a native VLAN of 4087 and disable STP.

```
config switch interface
   edit "tr1"
      set native-vlan 4087
      set stp-state disabled
   next
end
```

14. Configure the VXLAN interface with `tr1` as the tunnel-loopback interface. Set the interface to a normal SVI from step 1 to reach the Internet. The `remote-ip` address is the remote VTEP; in this case, the remote VTEP is the FortiGate interface being used for the VXLAN tunnel.

    With this configuration, all VLAN traffic from the switch, including all FortiSwitch VLANs, will loop to `tr1` and initiate the VXLAN tunnel to the FortiGate device.

```
config system vxlan
   edit vx1
      set interface vlan-1000
      set vni 4094
      set remote-ip 10.100.1.1
      set tunnel-loopback "tr1"
   next
end
```

Switch redundancy with MCLAG

The following network topologies provide switch redundancy with MCLAG:

Standalone FortiGate unit with dual-homed FortiSwitch access

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

See Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 60.

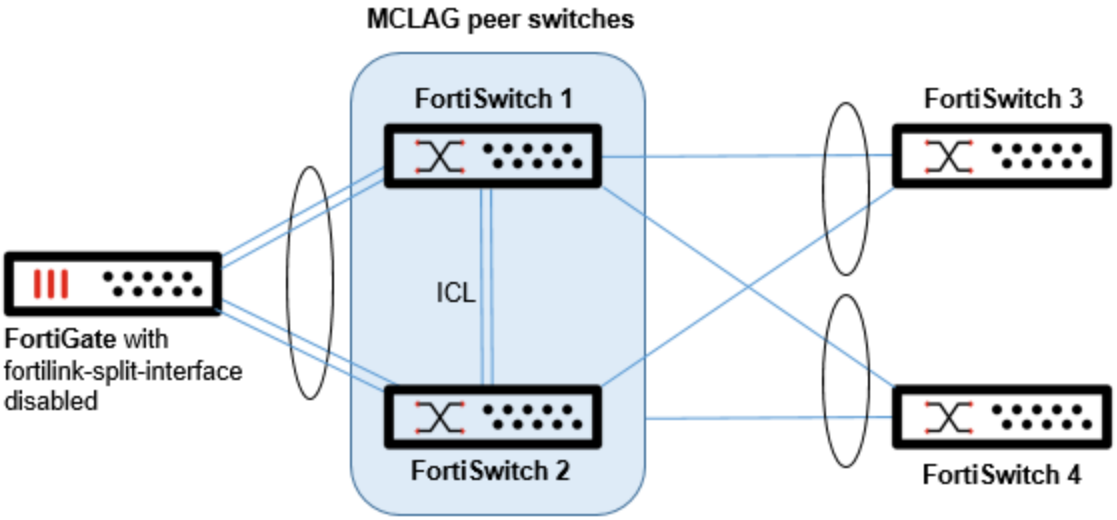
After the MCLAG peer group is created between FortiSwitch 1 and FortiSwitch 2, the MCLAG trunks are automatically established with the access switches (FortiSwitch 3 and FortiSwitch 4).

NOTE:

- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks. They are both enabled by default.
- Fortinet recommends using at least two links for ICL redundancy.

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

- On the global switch level, `mclag-igmpsnooping-aware` must be enabled. It is enabled by default.
- The `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *disabled* on the ISL and FortiLink trunks; but the `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *enabled* on ICL trunks. These settings are enabled by default.
- IGMP proxy must be enabled.



HA-mode FortiGate units with dual-homed FortiSwitch access

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

See Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 60.

After the MCLAG peer group is created between FortiSwitch 1 and FortiSwitch 2, the MCLAG trunks are automatically established with the access switches (FortiSwitch 3, FortiSwitch 4, and FortiSwitch 5).

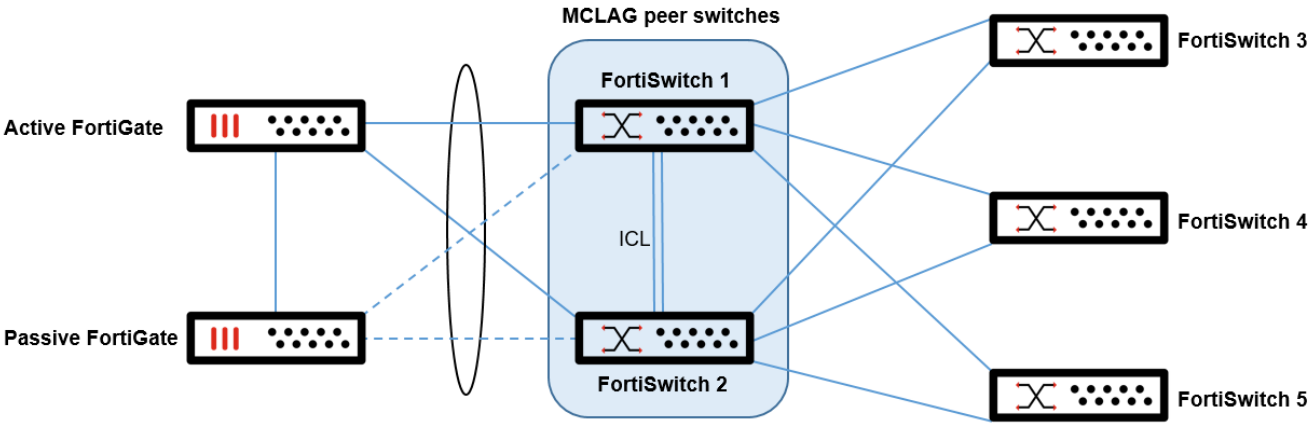
NOTE:

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

- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks. They are both enabled by default.
- Fortinet recommends using at least two links for ICL redundancy.

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

- On the global switch level, `mclag-igmpsnooping-aware` must be enabled. It is enabled by default.
- The `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *disabled* on the ISL and FortiLink trunks; but the `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *enabled* on ICL trunks. These settings are enabled by default.
- IGMP proxy must be enabled.



HA-mode one-tier MCLAG

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

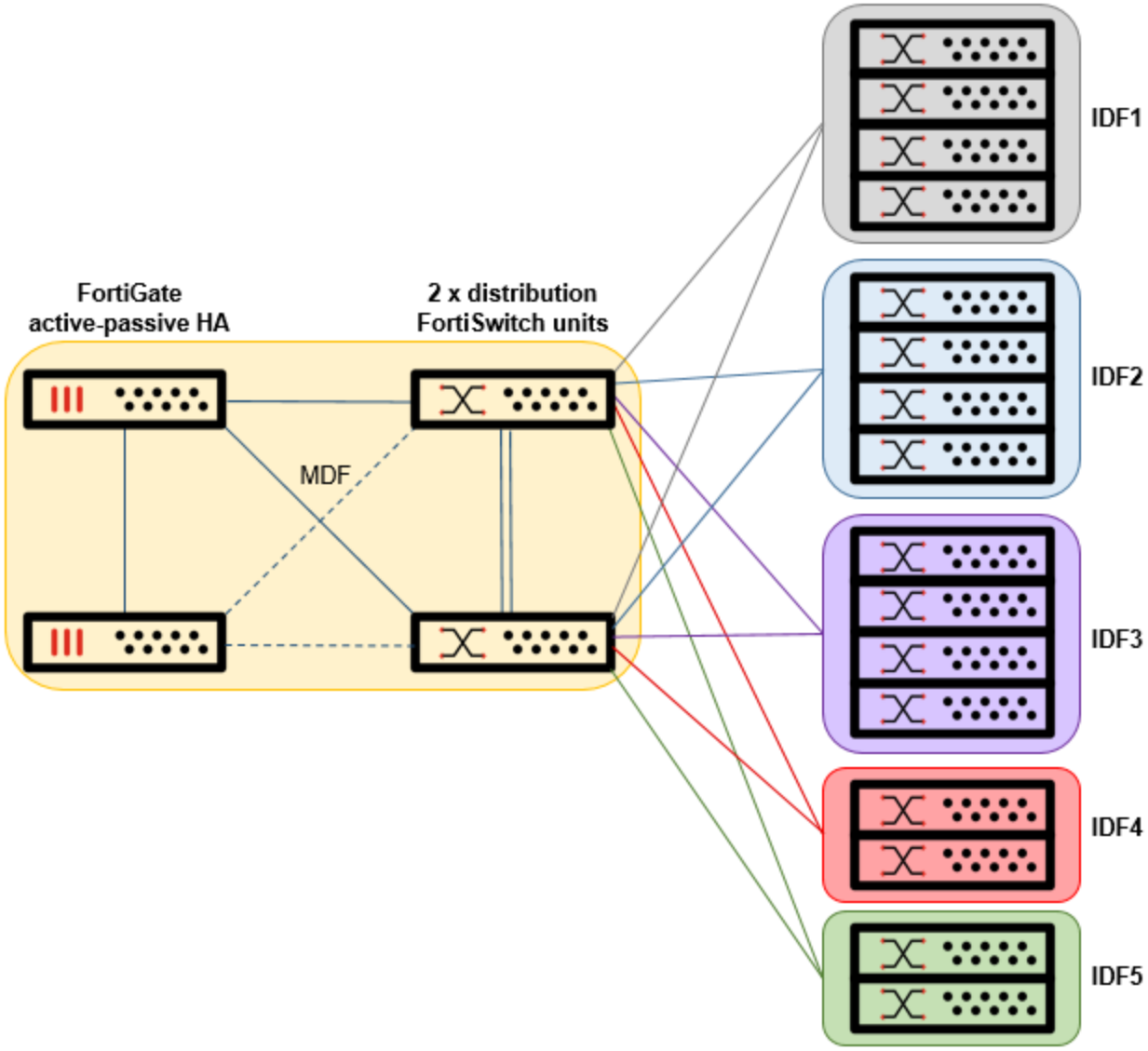
For the FortiLink connection to each distribution switch, you create a FortiLink split interface (an aggregate interface that contains one active link and one standby link).

NOTE:

- Before FortiSwitchOS 3.6.4, MCLAG was not supported when access rings were present. Starting with FortiSwitchOS 3.6.4, MCLAG is supported, even with access rings present.
- Before FortiOS 6.2.0, when using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive. Starting in FortiOS 6.2.0, the FortiGate HA mode can be either active-passive or active-active.
- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface, the `lacp-mode` of the FortiLink aggregate interface must be set to `static`. Unless MCLAG is enabled and you are using 6.2.0 or later, see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 60 for details.
- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks. They are both enabled by default.
- This is only an example topology. Other combinations of FortiGate units and FortiSwitch units can be used to create a similar topology.
- Fortinet recommends using at least two links for ICL redundancy.

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

- On the global switch level, `mclag-igmpsnooping-aware` must be enabled. It is enabled by default.
- The `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *disabled* on the ISL and FortiLink trunks; but the `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *enabled* on ICL trunks. These settings are enabled by default.
- IGMP proxy must be enabled.



FortiLink with an HA cluster of four FortiGate units

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

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

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

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

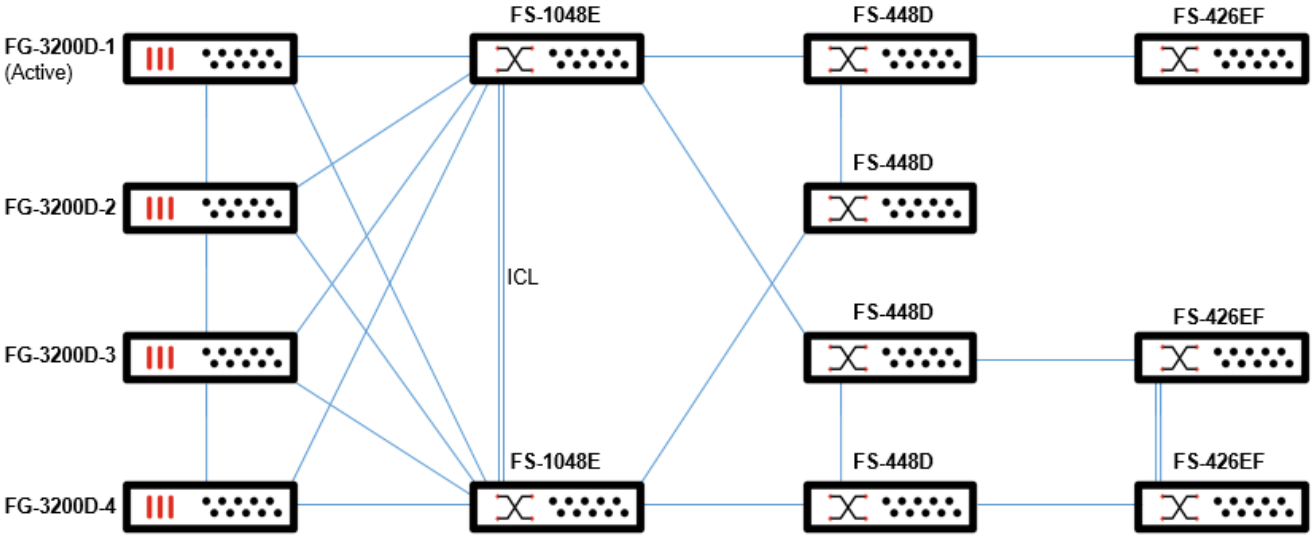
The cluster uses the FGCP to select the primary unit, and to provide device, link, and session failover. The FGCP also manages the two HA modes; active-passive (failover HA) and active-active (load-balancing HA).

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

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

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

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



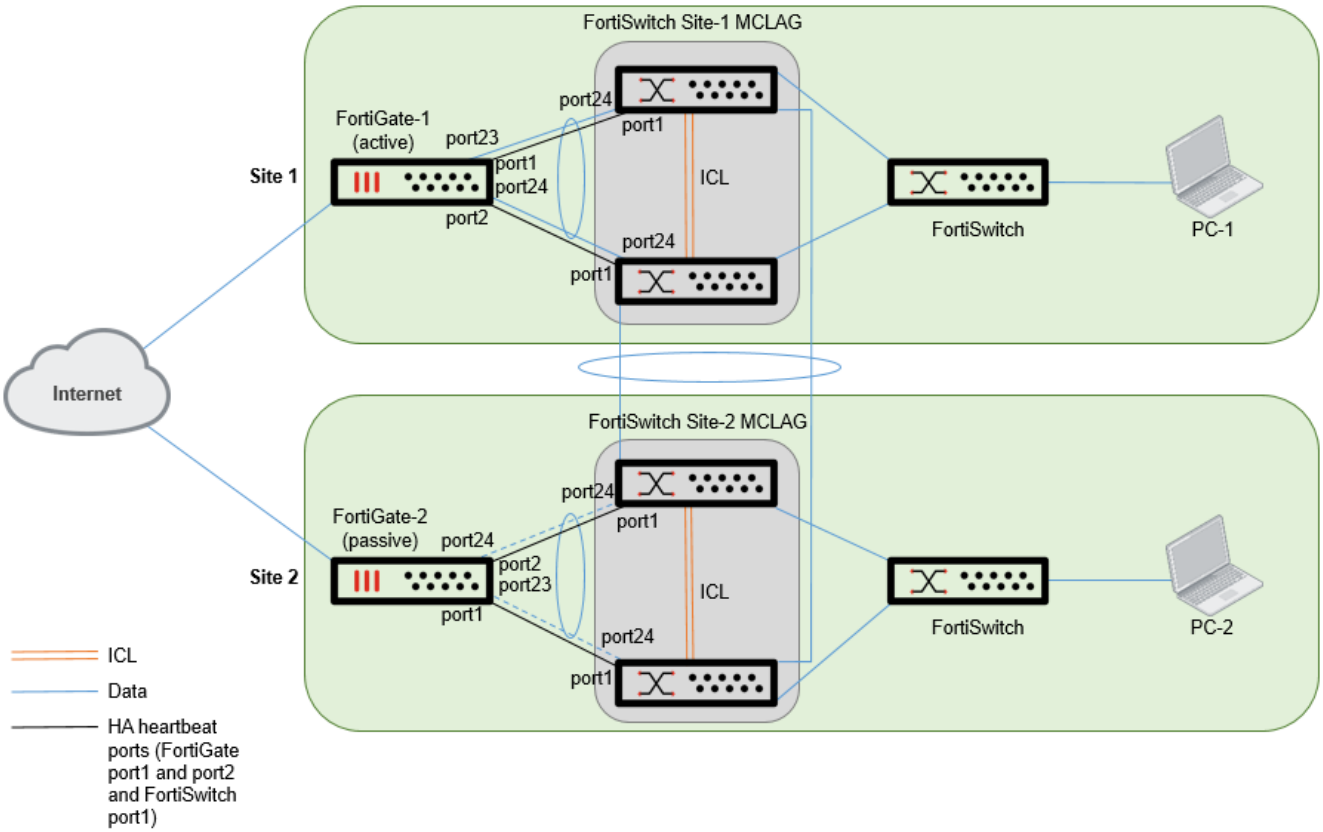
HA-mode FortiGate units in different sites

There are two sites in this topology, each with a FortiGate unit. The two sites share the FortiGate units in active-passive HA mode. The FortiGate units use the FortiSwitch units in FortiLink mode as the heartbeat connections because of limited physical connections between the two sites.

FortiOS 6.4.2 or higher and FortiSwitchOS 6.4.2 or higher are required.

For example steps, refer to Deploying MCLAG topologies on page 63.

NOTE: Fortinet recommends using at least two links for ICL redundancy.

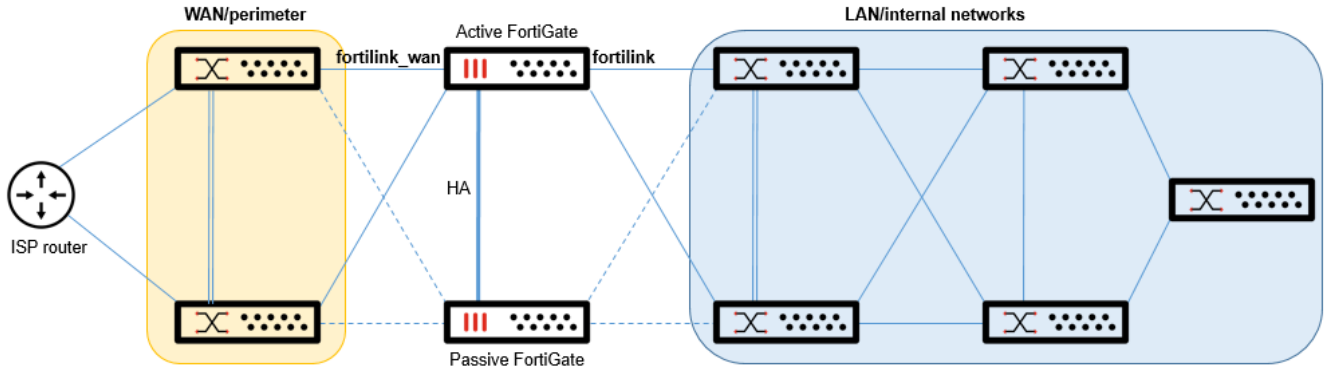


Isolated LAN/WAN with multiple FortiLink interfaces

This topology makes use of two FortiLink interfaces to provide a dedicated switching layer for each part of the network, LAN and WAN. Each FortiLink interface is independent with its own FortiSwitch VLANs, providing two separate FortiLink stacks.

In this specific example, the FortiLink stack for the LAN networks consists of a two-tier MCLAG topology with dual-homed access switches, whereas the WAN FortiLink stack has a one-tier MCLAG peer group connected to the ISP routers.

Starting with FortiOS 6.4.2, you can use the GUI to entirely manage multiple FortiLink stacks.

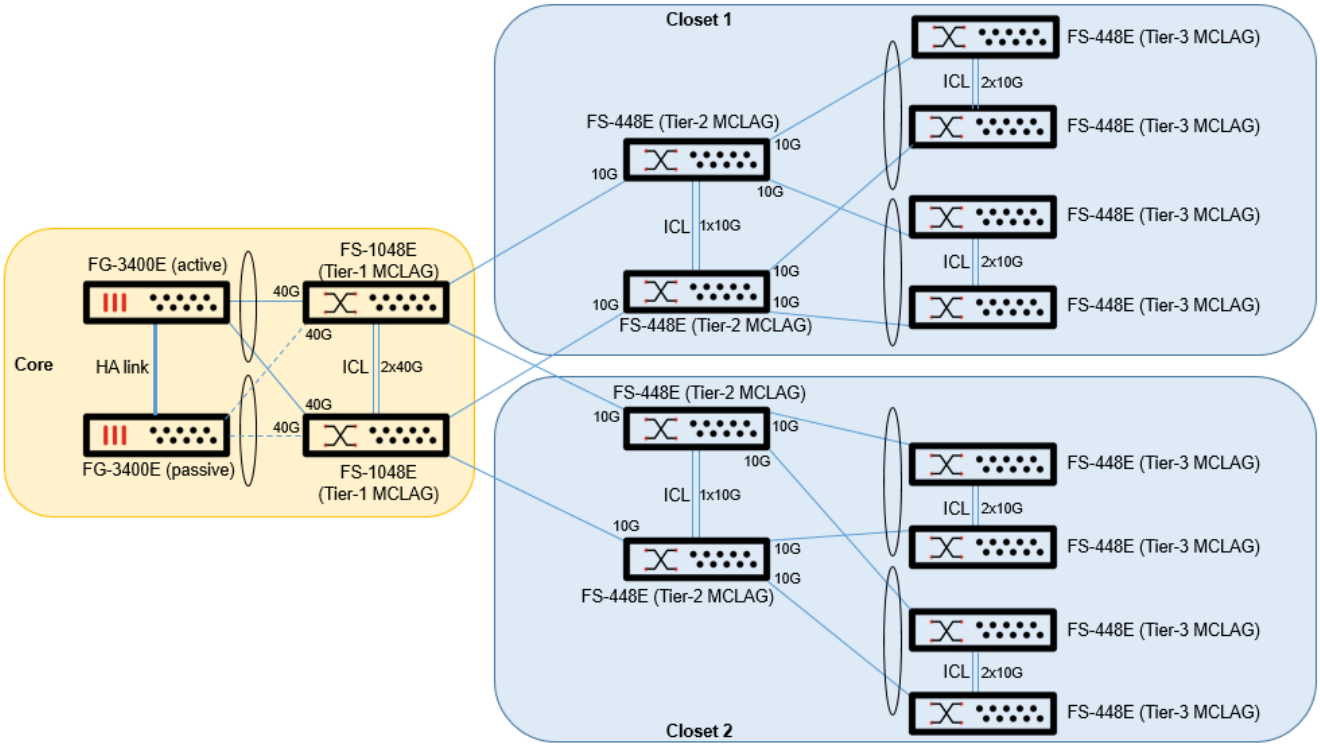


Three-tier FortiLink MCLAG configuration

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

MCLAG can be deployed in up to three tiers to expand the FortiSwitch stack, offering link and switch redundancy with the efficient use of the bandwidth because all links are active.

For the procedure, see Deploying MCLAG topologies on page 63.



NOTE: Fortinet recommends using at least two links for ICL redundancy.

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. Then you set up two MCLAGs towards the servers, each MCLAG using one port from each FortiSwitch unit. For the procedure, see Deploying MCLAG topologies on page 63.

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

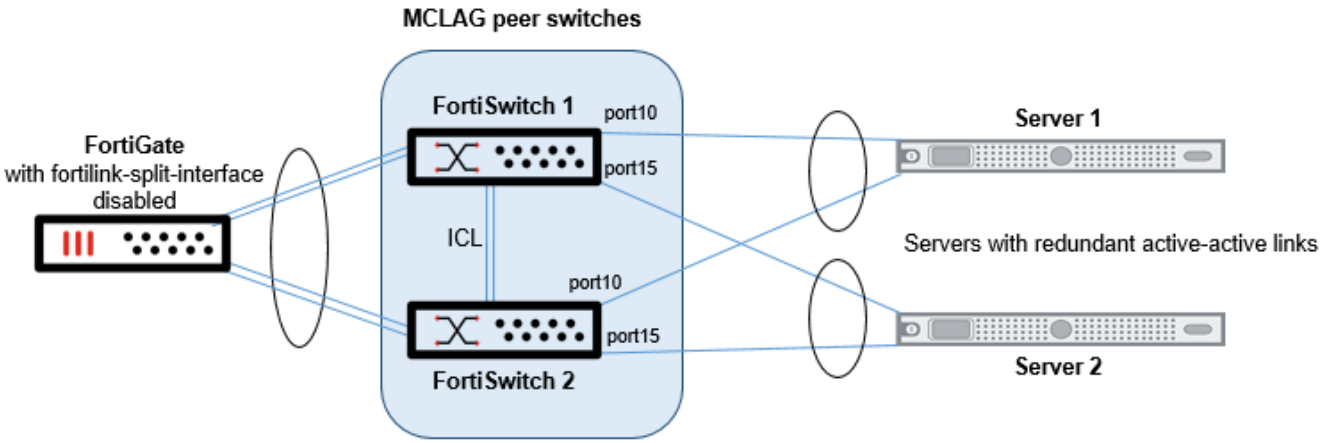
NOTE:

- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks. They are both enabled by default.
- Fortinet recommends using at least two links for ICL redundancy.

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

- On the global switch level, `mclag-igmpsnooping-aware` must be enabled. It is enabled by default.

- The `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *disabled* on the ISL and FortiLink trunks; but the `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *enabled* on ICL trunks. These settings are enabled by default.
- IGMP proxy must be enabled.



MCLAG peer groups

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).

This section covers the following topics:

MCLAG requirements

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

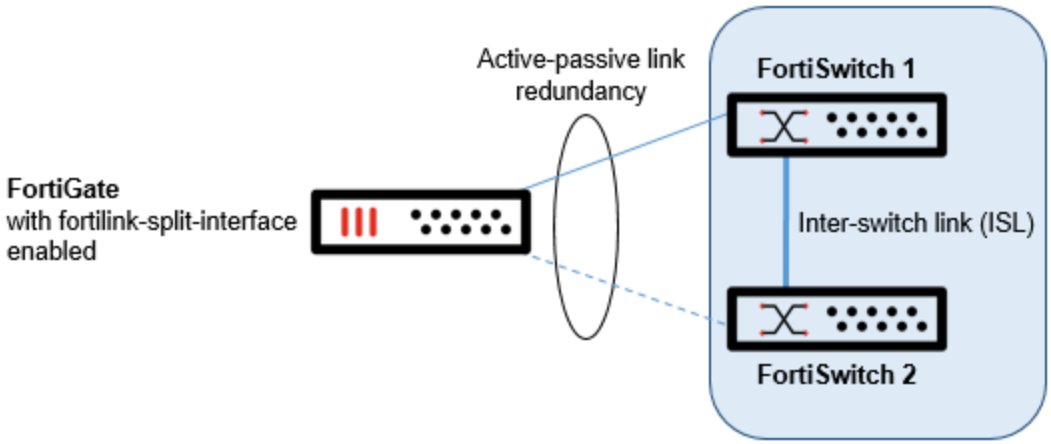
NOTE: If you are going to use IGMP snooping with an MCLAG topology:

- On the global switch level, `mclag-igmpsnooping-aware` must be enabled. By default, `mclag-igmpsnooping-aware` is enabled in the FortiSwitchOS CLI.
- The `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *disabled* on the ISL and FortiLink trunks; but the `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *enabled* on ICL trunks. These settings are enabled by default.
- IGMP proxy must be enabled.

Transitioning from a FortiLink split interface to a FortiLink MCLAG

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

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



NOTE:

- Make sure that the split interface is enabled.
- This procedure also applies to a FortiGate unit in HA mode.
- More links can be added between the FortiGate unit and FortiSwitch unit.
- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks. They are both enabled by default.
- Fortinet recommends using at least two links for ICL redundancy.

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

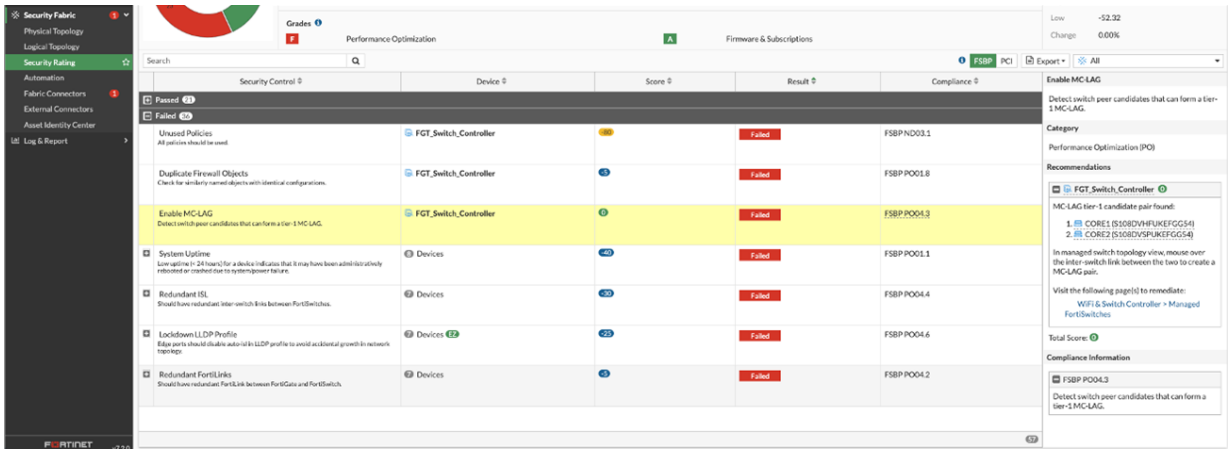
- On the global switch level, `mclag-igmpsnooping-aware` must be enabled. It is enabled by default.
- The `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *disabled* on the ISL and FortiLink trunks; but the `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *enabled* on ICL trunks. These settings are enabled by default.
- IGMP proxy must be enabled.

Use the FortiGate CLI to change the FortiSwitch units' configuration without losing their management from the FortiGate unit. You do not need to change anything on the individual FortiSwitch units.

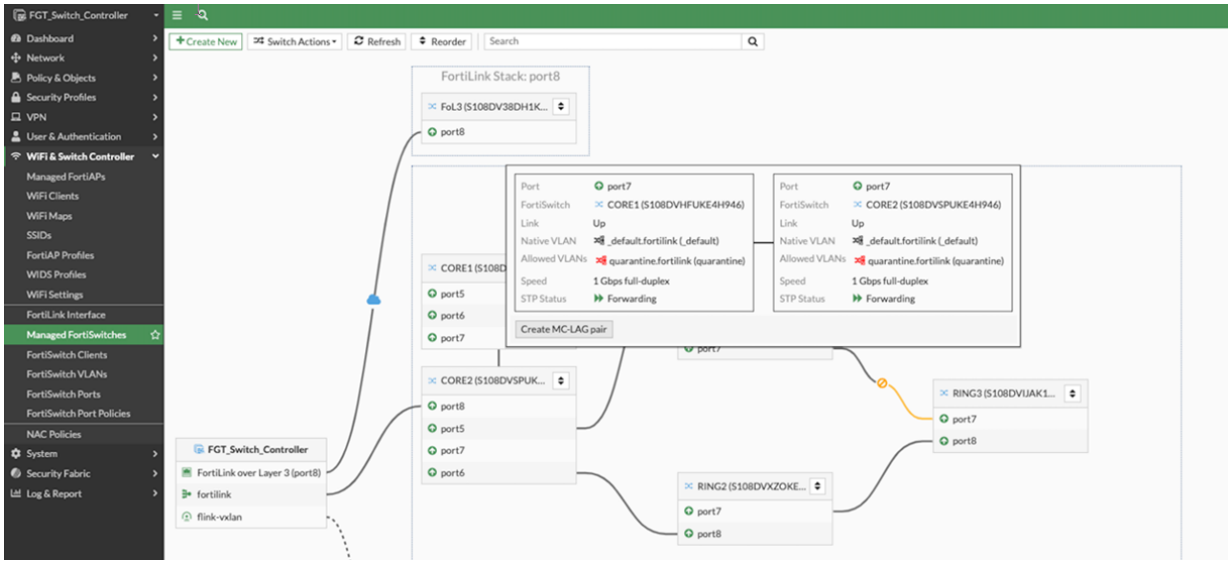
1. You can use the GUI (starting in FortiOS 7.2.4) or CLI to form the MCLAG between two switches.

   To use the FortiGate GUI:

   a. Go to *Security Fabric* > *Security Rating*. Look under *Failed* > *Enable MC-LAG* to find which pair of switches can form a tier-1 MCLAG.



b. Go to *WiFi & Switch Controller* > *Managed FortiSwitches*. In the *Topology* view, hover over the inter-switch link between the pair of switches and then click *Create MC-LAG pair* in the dialog.



To use the FortiGate CLI:

a. Assign the LLDP profile “default-auto-mclag-icl” to the ports that should form the MCLAG ICL in FortiSwitch unit 1. For example:

```
FGT_Switch_Controller # config switch-controller managed-switch
FGT_Switch_Controller (managed-switch) # edit FS1E48T419000051
FGT_Switch_Controller (FS1E48T419000051) # config ports
FGT_Switch_Controller (ports) # edit port49
FGT_Switch_Controller (port49) # set lldp-profile default-auto-mclag-icl
FGT_Switch_Controller (port49) # end
FGT_Switch_Controller (FS1E48T419000051) # end
```

b. Assign the LLDP profile “default-auto-mclag-icl” to the ports that should form the MCLAG ICL in FortiSwitch unit 2. The port numbers can be different.

2. Disable the split interface in the FortiLink interface. For example:

```
config system interface
```

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

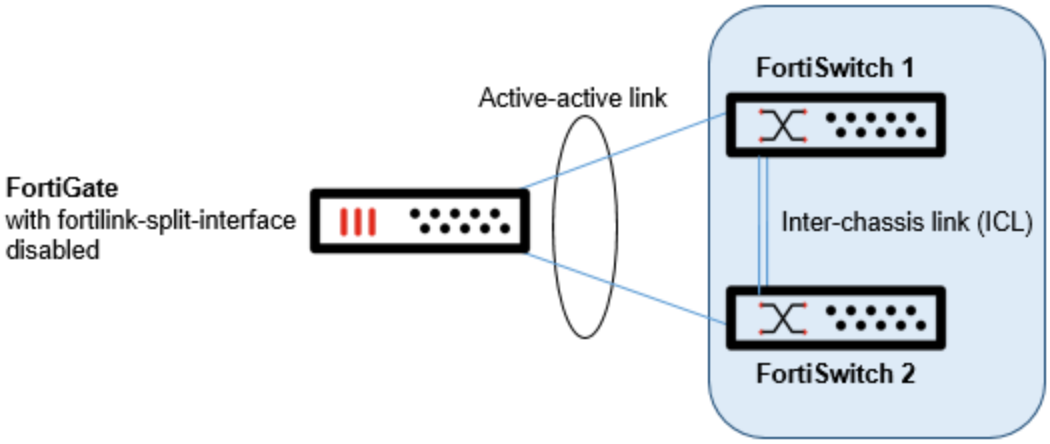
3. From the FortiGate unit, enable the LACP active mode if not already set:

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

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

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

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



If you disable the MCLAG ICL, you need to enable the `fortilink-split-interface`.

Deploying MCLAG topologies

This section covers the following topics:

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. See Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 60. Then you set up two MCLAGs towards the servers, each MCLAG using one port from each FortiSwitch unit.

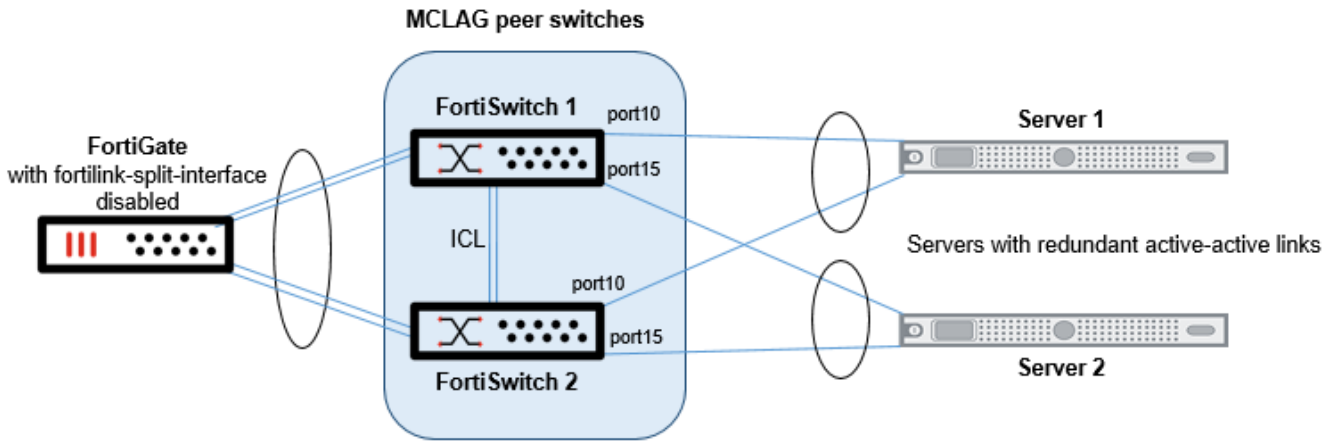
This topology is also supported when the FortiGate unit is in HA mode.

NOTE:

- On the global switch level, `mclag-stp-aware` must be enabled, and STP must be enabled on all ICL trunks. They are both enabled by default.
- Fortinet recommends using at least two links for ICL redundancy.

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

- On the global switch level, `mclag-igmpsnooping-aware` must be enabled. It is enabled by default.
- The `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *disabled* on the ISL and FortiLink trunks; but the `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *enabled* on ICL trunks. These settings are enabled by default.
- IGMP proxy must be enabled.



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

```
diagnose switch-controller switch-info mclag icl
```

Step 2: For each server, configure a trunk with MCLAG enabled. For server 1, select port10 on FortiSwitch 1 and FortiSwitch 2. For server 2, select port15 on FortiSwitch 1 and FortiSwitch 2.

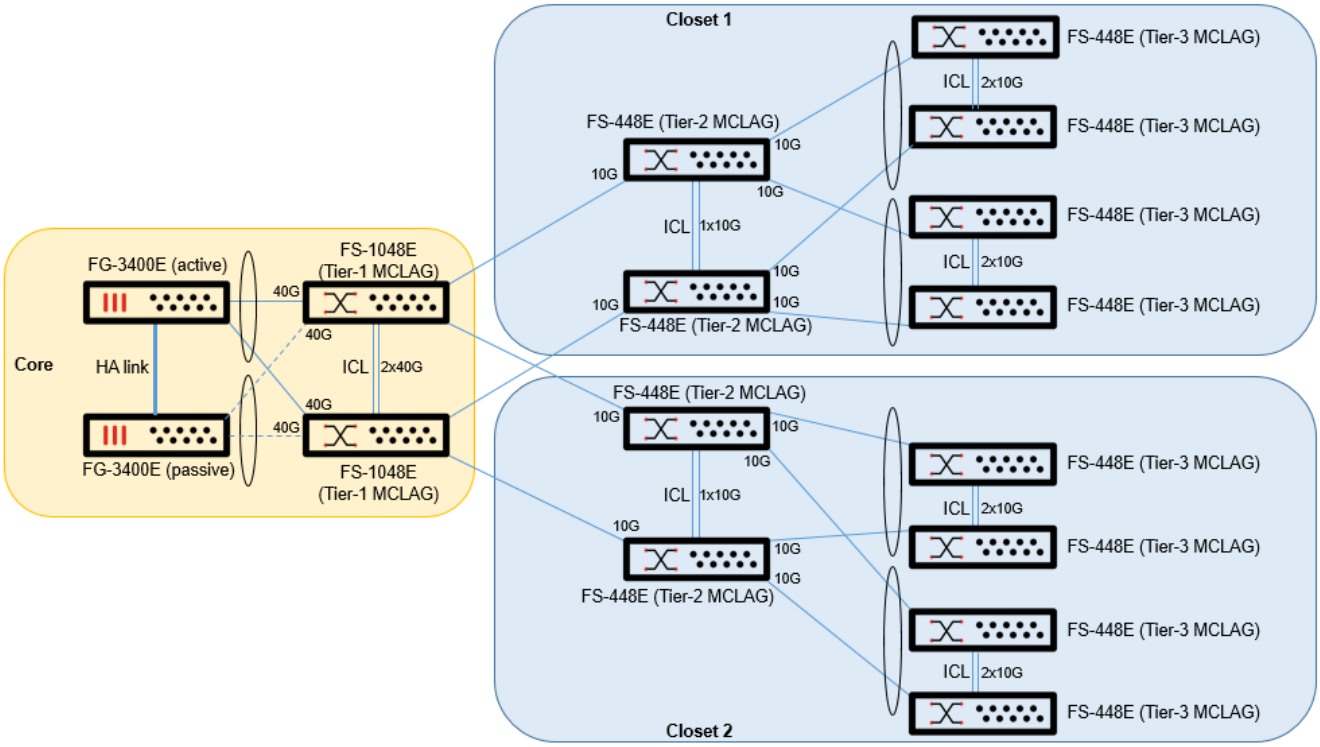
For details, refer to MCLAG trunks on page 86.

Step 3: Verify the MCLAG configuration.

```
diagnose switch-controller switch-info mclag list
```

Multi-tiered MCLAG with HA-mode FortiGate units

Use the following procedure to deploy tier-2 and tier-3 MCLAG peer groups from the FortiGate switch controller without the need for direct console access to the FortiSwitch units.



NOTE:

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

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

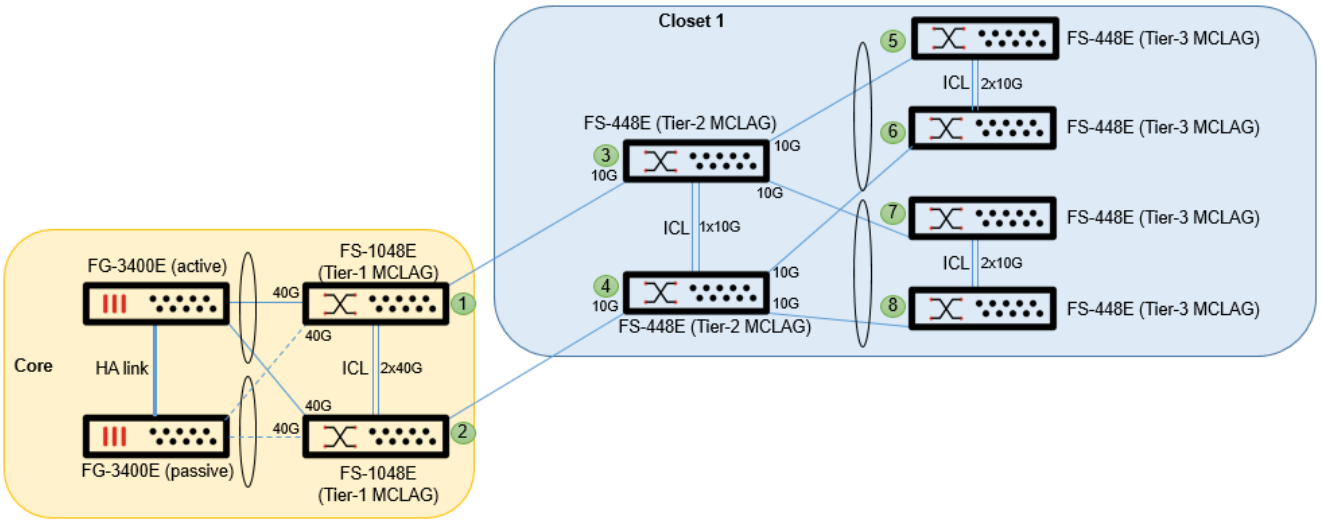
- On the global switch level, `mclag-igmpsnooping-aware` must be enabled. It is enabled by default.
- The `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *disabled* on the ISL and FortiLink trunks; but the `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *enabled* on ICL trunks. These settings are enabled by default.
- IGMP proxy must be enabled.

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

Tier-1 MCLAG

Wire the two core FortiSwitch units to the FortiGate devices. To configure the FortiSwitch units in the core, see Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 60.

Tier-2 and Tier-3 MCLAGs



1. Connect *only* the tier-2 MCLAG FortiSwitch units 3 and 4 to the core units 1 and 2 (leaving the other switches in Closet 1 disconnected). Wait until they are discovered and authorized (authorization must be done manually if auto-authorization is disabled).
2. Using the FortiGate CLI, assign the LLDP profile “default-auto-mclag-icl” to the ports that should form the MCLAG ICL in the tier-2 MCLAG switches 3 and 4. For example:

```
FGT_Switch_Controller # config switch-controller managed-switch
FGT_Switch_Controller (managed-switch) # edit FS1E48T419000051
FGT_Switch_Controller (FS1E48T419000051) # config ports
FGT_Switch_Controller (ports) # edit port49
FGT_Switch_Controller (port49) # set lldp-profile default-auto-mclag-icl
FGT_Switch_Controller (port49) # end
FGT_Switch_Controller (FS1E48T419000051) # end
```

3. For each tier-2 MCLAG peer group, add an `auto-isl-port-group` for the tier-2 MCLAG switches on both switch 1 and switch 2:

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

This configuration is done directly in the FortiSwitch CLI (or by binding a custom script using custom commands on the FortiGate device. See Executing custom FortiSwitch scripts on page 241.

If there is not a tier-3 MCLAG, skip to step 7.

4. Wire the tier-3 MCLAG switches 5, 6, 7, and 8. Wait until they are discovered and authorized (authorization must be done manually if auto-authorization is disabled).
5. For each tier-3 MCLAG peer group, add two `auto-isl-port-group`s for the tier-3 MCLAG switches on both switch 3 and switch 4:

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

This configuration is done directly in the FortiSwitch CLI (or by binding a custom script using custom commands on the FortiGate device. See Executing custom FortiSwitch scripts on page 241.

6. Using the FortiGate CLI, assign the LLDP profile “default-auto-mclag-icl” to the ports that should form the ICL in the tier-3 MCLAG peers switches 5 and 6 and switches 7 and 8. For example:

```
FGT_Switch_Controller # config switch-controller managed-switch
FGT_Switch_Controller (managed-switch) # edit FS1E48T419000051
FGT_Switch_Controller (FS1E48T419000051) # config ports
FGT_Switch_Controller (ports) # edit port49
FGT_Switch_Controller (port49) # set lldp-profile default-auto-mclag-icl
FGT_Switch_Controller (port49) # end
FGT_Switch_Controller (FS1E48T419000051) # end
```

7. Connect the access switches to the MCLAG peer groups, and the inter-switch links are formed automatically. Wait until they are discovered and authorized (authorization must be done manually if auto-authorization is disabled).
8. Wire *only* the tier-2 MCLAG FortiSwitch units from Closet 2 (leaving the other switches in Closet 2 disconnected). Wait until they are discovered and authorized (authorization must be done manually if auto-authorization is disabled). Return to step 3 to complete the process for Closet 2.
9. All FortiSwitch units are now authorized, and all MCLAG peer groups are enabled. Proceed with the configuration of the FortiSwitch units by assigning VLANs to the access ports and any other functionality required.

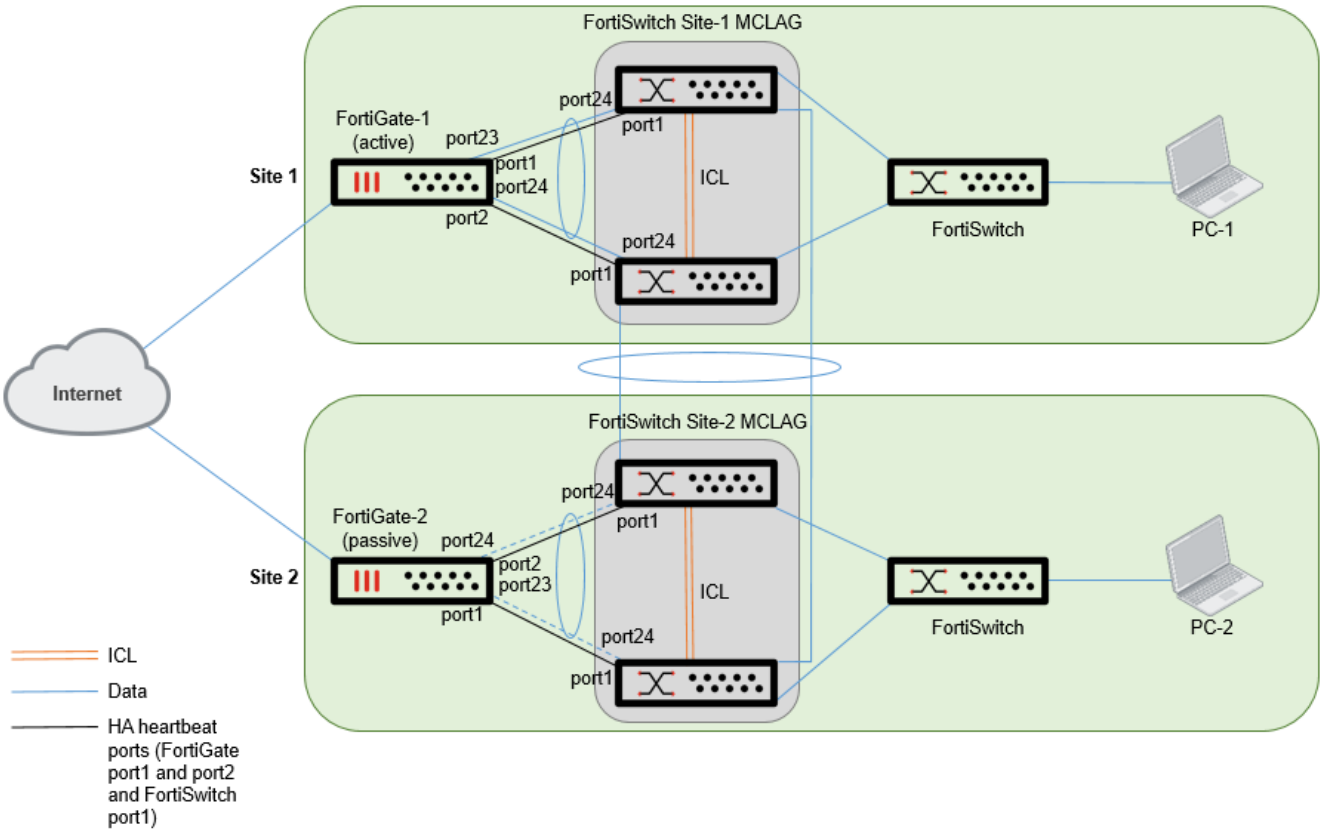
HA-mode FortiGate units in different sites

There are two sites in this topology, each with a FortiGate unit. The two sites share the FortiGate units in active-passive HA mode. The FortiGate units use the FortiSwitch units in FortiLink mode as the heartbeat connections because of limited physical connections between the two sites.

FortiOS 6.4.2 or higher and FortiSwitchOS 6.4.2 or higher are required.

Refer to the other network topologies in Deploying MCLAG topologies on page 63.

NOTE: Fortinet recommends using at least two links for ICL redundancy.



The following steps are an example of how to configure this topology:

1. Disconnect the physical connections between the two sites.
2. On Site 1:
   a. Use the FortiGate unit to establish the FortiLinks on Site 1. See Configuring FortiLink on page 14.
   b. Enable the MCLAG-ICL on the core switches of Site 1. See Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 60.
   c. Enable the HA mode and set the heartbeat ports on FortiGate-1. FortiGate port1 and port2 are used as HA heartbeat ports in this example. For example, `set hbdev "port1" 242 "port2" 25`.
   d. Create a switch VLAN or VLANs dedicated to the FortiGate HA heartbeats between the two FortiGate units. For example:

```
config system interface
   edit "hb1"
      set vdom "vdom name"
      set vlanid 998
   next
   edit "hb2"
      set vdom "vdom name"
      set vlanid 999
   next
end
```

   e. Under the `config switch-controller managed-switch` command, set the native VLAN of the switch ports connected to the heartbeat ports using the VLAN created in step 2d.

      In this example, you need to assign port1 of core-switch1 to vlan998 and connect port1 of the active FortiGate

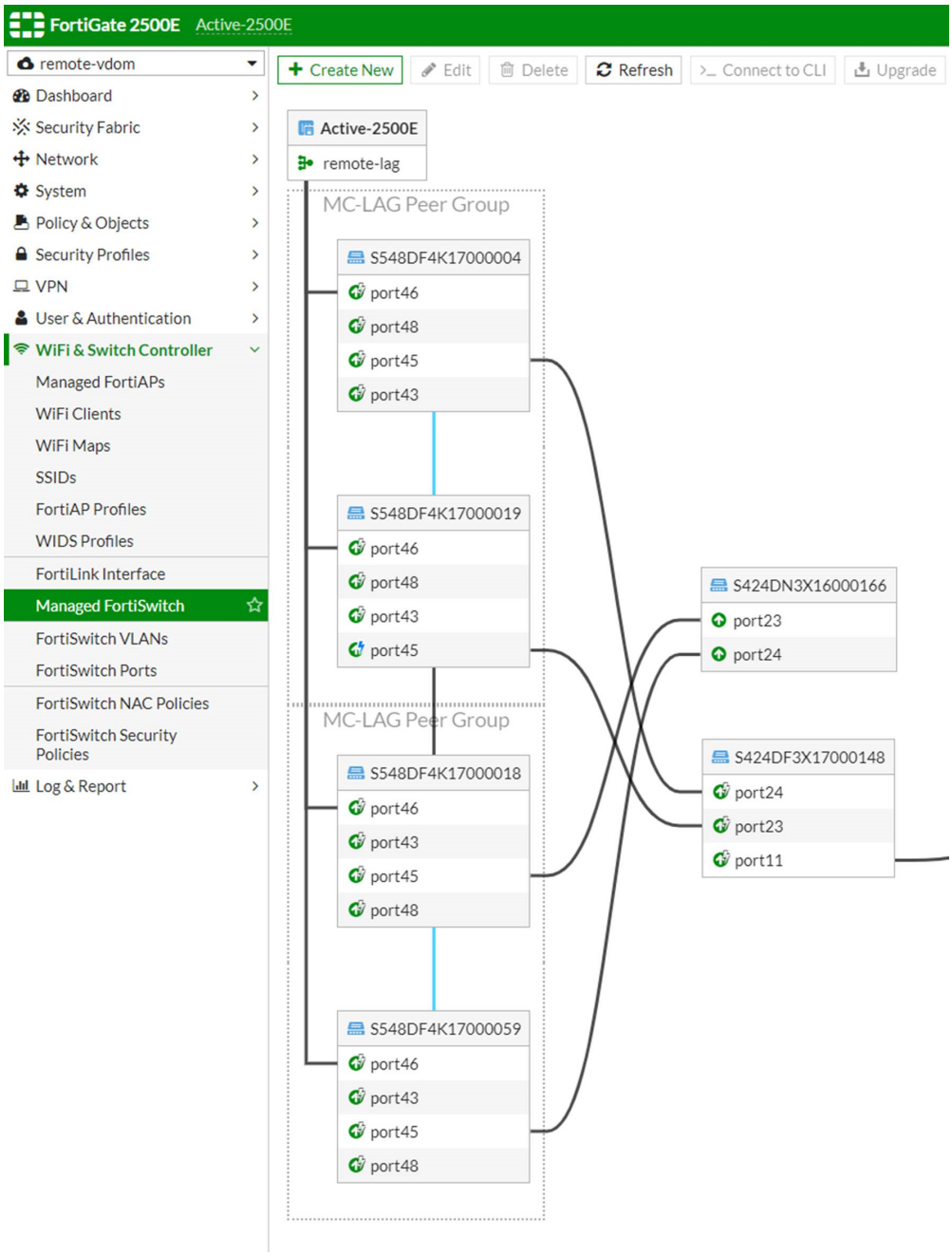
unit to port1 of core-switch1. Then you need to assign port1 of core-switch2 to vlan999 and connect port2 of the active FortiGate unit to port1 of core-switch2.

```
config switch-controller managed-switch
   edit <site1-core-switch1>
      edit "port1"
         set vlan "hb1"
      next
   end
   edit <site1-core-switch2>
      edit "port1"
         set vlan "hb2"
      next
   end
```

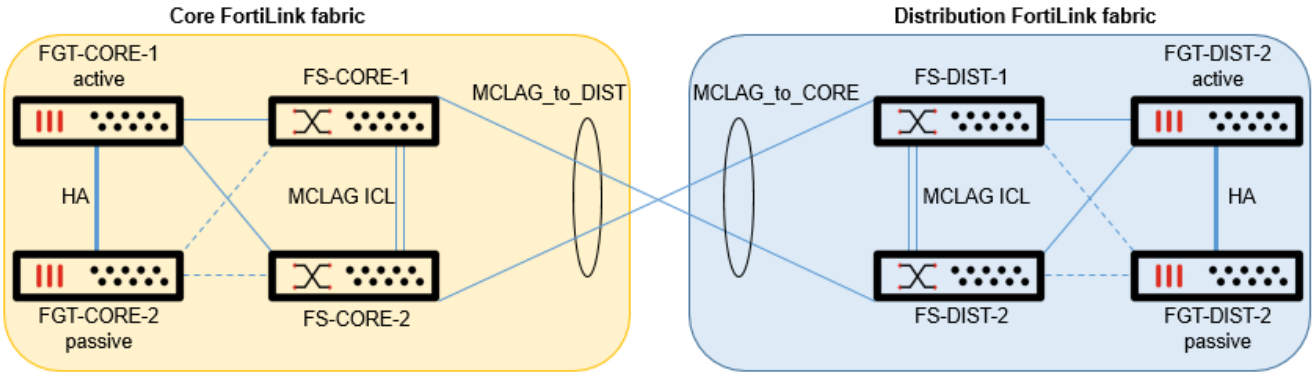
   f. Make sure all FortiLinks are up.

3. On Site 2:
   a. Configure Site 2 using the same configuration as step 2, except for the HA priority.
   b. Make sure all FortiLinks are up.
4. Disconnect the physical connections for the FortiGate HA and FortiLink interface on Site 2.
5. Connect the cables between the two pairs of core switches in Site 1 and Site 2.
6. On both sites:
   a. On the MCLAG Peer Group switches at Site 1, use the `config switch auto-isl-port-group` command in the FortiSwitch CLI to group the ports to Site 2. See Deploying MCLAG topologies on page 63.
   b. On the MCLAG Peer Group switches at Site 2 , use the `config switch auto-isl-port-group` command in the FortiSwitch CLI to group the ports to Site 1. See Deploying MCLAG topologies on page 63.
   c. Make sure all the FortiLinks are up.
7. Connect the FortiGate HA and FortiLink interface connections on Site 2.
8. Check the configuration:
   a. On both sites, enter the `get system ha status` command on the FortiGate unit to check the HA status.
   b. On the active (master) FortiGate unit, enter the `execute switch-controller get-conn-status` command to check the FortiLink state.

9. In the GUI, the example configuration looks like the following:



Interconnecting FortiLink fabrics



Each FortiLink fabric is a set of FortiSwitch units controlled by a FortiGate device. When you interconnect FortiLink fabrics, each FortiGate device manages its own FortiSwitch units. The FortiLink fabric interconnection points are seen as access ports from each FortiGate unit; no inter-switch links are formed.

In this example:

- The interconnecting ports (port15) on FS-CORE-1, FS-CORE-2, FS-DIST-1, and FS-DIST-2 have the LLDP profile set to `default` with `auto-isl` disabled.
- Optionally, you can disable the management of FS-DIST-1 and FS-DIST-2 by the FGT-CORE switch controller.
- FGT-CORE-1 and FGT-CORE-2 have the MCLAG trunk `MCLAG_to_DIST`.
- FGT-DIST-1 and FGT-DIST-2 have the MCLAG trunk `MCLAG_to_CORE`.
- The allowed VLANs on the `MCLAG_to_DIST` and `MCLAG_to_CORE` trunks match.

This topology requires the following:

- Disable `auto-isl` on the interconnection links to avoid one FortiGate device discovering or managing FortiSwitch units that should be discoverd and managed by the other FortiGate device.
- Optionally, on one FortiGate device, disable discovery for the FortiSwitch serial numbers managed by the other FortiGate device.
- Configure matching native VLANs and allowed VLANs on both sides to allow communication between FortiLink fabrics.
- The VLAN IDs must match, but the names can be different.

Deployment steps

1. Deploy each FortiGate device and respective FortiSwitch units separately. See Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 60.
2. (Optional) Disable discovery for the FortiSwitch units from the other FortiGate device.
3. Assign the “default” LLDP profile to the interconnecting ports. See Configuring ports using the GUI on page 79.
4. Create the MCLAG trunk for the interconnection. See Adding 802.3ad link aggregation groups (trunks) on page 85.
5. Assign matching native VLANs and allowed VLANs to the MCLAG trunk. See Configuring ports using the GUI on page 79.
6. Connect the cables to interconnect the FortiLink fabrics.

Configuration example

This configuration example assumes that each FortiLink fabric has been deployed already.

To configure the core FortiLink fabric:

1. Configure the FortiLink interface that will be used to interconnect the two FortiLink fabrics.

```
config system interface
   edit "INTERCON"
      set vdom "root"
      set ip 10.255.255.1 255.255.255.252
      set allowaccess ping ssh
      set color 20
      set interface "fortilink"
      set vlanid 500
   next
end
```

2. Assign the “default” LLDP profile to the switch ports and configure the MCLAG trunk toward the core FortiLink fabric (FS-CORE-1 and FS-CORE-2).

```
config switch-controller managed-switch
   edit "FS-CORE-1"
      config ports
         edit "port15"
            set port-owner "MCLAG_to_DIST"
            set lldp-profile "default"
         next
         edit "port16"
            set port-owner "MCLAG_to_DIST"
            set lldp-profile "default"
         next
         edit "MCLAG_to_DIST"
            set vlan "INTERCON"
            set type trunk
            set mode lacp-active
            set mclag enable
            set members "port15" "port16"
         next
      end
   next
end

config switch-controller managed-switch
   edit "FS-CORE-2"
      config ports
         edit "port15"
            set port-owner "MCLAG_to_DIST"
            set lldp-profile "default"
         next
         edit "port16"
            set port-owner "MCLAG_to_DIST"
            set lldp-profile "default"
```

```
        next
        edit "MCLAG_to_DIST"
           set vlan "INTERCON"
           set type trunk
           set mode lacp-active
           set mclag enable
           set members "port15" "port16"
        next
     end
  next
end
```

3. Optionally, prevent the core FortiGate devices from discovering the distribution FortiSwitch units.

```
config switch-controller global
   set disable-discovery "FS-DIST-1" "FS-DIST-2"
end
```

To configure the distribution FortiLink fabric:

1. Configure the FortiLink interface that will be used to interconnect the two FortiLink fabrics.

```
config system interface
   edit "INTERCON"
      set vdom "root"
      set ip 10.255.255.2 255.255.255.252
      set allowaccess ping ssh
      set color 20
      set interface "fortilink"
      set vlanid 500
   next
end
```

2. Assign the “default” LLDP profile to the switch ports and configure the MCLAG trunk toward the core FortiLink fabric (FS-DIST-1 and FS-DIST-2).

```
config switch-controller managed-switch
   edit "FS-DIST-1"
      config ports
         edit "port15"
            set port-owner "MCLAG_to_CORE"
            set lldp-profile "default"
         next
         edit "port16"
            set port-owner "MCLAG_to_CORE"
            set lldp-profile "default"
         next
         edit "MCLAG_to_CORE"
            set vlan "INTERCON"
            set type trunk
            set mode lacp-active
            set mclag enable
            set members "port15" "port16"
         next
      end
   next
end

config switch-controller managed-switch
   edit "FS-DIST-2"
```

```
      config ports
         edit "port15"
            set port-owner "MCLAG_to_CORE"
            set lldp-profile "default"
         next
         edit "port16"
            set port-owner "MCLAG_to_CORE"
            set lldp-profile "default"
         next
         edit "MCLAG_to_CORE"
            set vlan "INTERCON"
            set type trunk
            set mode lacp-active
            set mclag enable
            set members "port15" "port16"
         next
      end
   next
end
```

3. Optionally, prevent the distribution FortiGate devices from discovering the core FortiSwitch units.

```
config switch-controller global
   set disable-discovery "FS-CORE-1" "FS-CORE-2"
end
```

Configuring FortiSwitch VLANs and ports

This section covers the following topics:

Configuring VLANs

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

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

In FortiSwitchOS 3.3.0 and later releases, the FortiSwitch supports untagged and tagged frames in FortiLink mode. The switch supports up to 1,023 user-defined VLANs. You can assign a VLAN number (ranging from 1-4095) to each of the VLANs. For FortiSwitch units in FortiLink mode (FortiOS 6.2.0 and later), you can assign a name to each VLAN.

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

This section covers the following topics:

Creating VLANs

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

Using the GUI

To create the VLAN:

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

Interface Name	VLAN name
VLAN ID	Enter a number (1-4094)
Color	Choose a unique color for each VLAN, for ease of visual display.
Role	Select *LAN*, *WAN*, *DMZ*, or *Undefined*. **NOTE:** If you are using the FortiGate unit's security rating feature, you need to assign a role of *LAN*, *WAN*, or *DMZ* to your FortiLink VLAN interfaces before referencing them in any firewall policies. If this is not done, the security rating score is lowered until the issue is remedied, due to failing the "Interface Classification" requirement.

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

To assign FortiSwitch ports to the VLAN:

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

Using the FortiSwitch CLI

1. Create the marketing VLAN.

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

2. Set the VLAN's IP address.

```
config system interface
   edit <vlan name>
      set ip <IP address> <Network mask>
   end
```

3. Enable a DHCP server.

```
config system dhcp server
   edit 1
      set default-gateway <IP address>
      set dns-service default
      set interface <vlan name>
         config ip-range
            set start-ip <IP address>
            set end-ip <IP address>
         end
      set netmask <Network mask>
   end
```

4. Assign ports to the VLAN.

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

5. Assign untagged VLANs to a managed FortiSwitch port:

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

Viewing FortiSwitch VLANs

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

Each entry in the VLAN list displays the following information:

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

Changing the VLAN configuration mode

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

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

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

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

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

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

Configuring multiple managed FortiSwitch VLANs to be used in a software switch

Starting in FortiOS 7.2.0 with FortiSwitchOS 7.2.0, you can add multiple managed FortiSwitch VLANs to a software switch using the GUI or CLI. In previous releases, you could add only one managed FortiSwitch VLAN per FortiGate device to a software switch.

Traffic between two VLANs is controlled by the `intra-switch-policy` setting under the `config system switch-interface` command. By default, `intra-switch-policy` is set to `implicit`, which allows traffic between software switch members.

The FortiSwitch VLANs must be configured without IP addresses.

Using the GUI

1. Go to *Network* > *Interfaces*.
2. Create or edit a software switch interface
3. In *Interface members*, select multiple FortiSwitch VLANs.
4. Click *OK*.

Using the CLI

In the following example, you create two managed FortiSwitch VLANs and then add them to a software switch.

```
config system interface
   edit "vlan1"
      set vdom "root"
      set device-identification enable
      set role lan
      set snmp-index 46
      set interface "fortilink"
      set vlanid 3501
   next
   edit "vlan2"
      set vdom "root"
      set device-identification enable
      set role lan
      set snmp-index 47
      set interface "fortilink"
      set vlanid 3502
   next
end

config system switch-interface
   edit "softwareswitch"
      set vdom "root"
      set member "vlan1" "vlan2"
   next
end
```

Configuring ports using the GUI

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

- Set the native VLAN and add more VLANs
- Edit the description of the port
- Enable or disable the port
- Set the access mode of the port in *Port* view:
  - *Static*—The port does not use a dynamic port policy or FortiSwitch network access control (NAC) policy.
  - *Assign Port Policy*—The port uses a dynamic port policy.
  - *NAC*—The port uses a FortiSwitch NAC policy.
- Set the LACP mode of the trunk in *Trunk* view:
  - *Static*—In this mode, no control messages are sent, and received control messages are ignored.
  - *Passive LACP*—The port passively uses LACP to negotiate 802.3ad aggregation.
  - *Active LACP*—The port actively used LACP to negotiate 802.3ad aggregation.
- Double-click a port to display the *Port Statistics* pane, which shows the transmitted and received traffic, frame errors by type, and transmitted and received frames. You can also select a port and then click the *View Statistics* button in the upper right corner. The *Compare with* dropdown list allows you to select another port to compare with the currently selected port. The statistics are refreshed every 15 seconds.
- Clear port counters by right-clicking a port and selecting *Clear port counters*.

- Enable or disable PoE for the port
- Enable or disable DHCP snooping (if supported by the port)
- Enable or disable whether a port is an edge port
- Enable or disable STP (if supported by the port)
- Enable or disable loop guard (if supported by the port)
- Enable or disable STP BPDU guard (if supported by the port)
- Enable or disable STP root guard (if supported by the port)

Configuring port speed and status

To set port speed and other base port settings:

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

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port1
            set description "First port"
            set speed auto
            set status up
         end
      end
```

To check the port properties:

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

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

For example:

```
FortiGate-100F # diagnose switch-controller switch-info port-properties S524DF4K15000024
port18

Vdom: root
Switch: S524DF4K15000024
Port: port18
       PoE           : 802.3af/at,30.0W
```

```
        Connector     : RJ45
        Speed         : 10Mhalf/10Mfull/100Mhalf/100Mfull/1Gauto/auto
```

Configuring flap guard

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

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

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

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

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

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

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

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

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

For example:

```
config switch-controller managed-switch
   edit S424ENTF19000007
```

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

Resetting a port

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

To reset a port:

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

For example:

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

Viewing the flap-guard configuration

To display flap-guard information for all ports of a FortiSwitch unit:

```
diagnose switch-controller switch-info flapguard status <FortiSwitch_serial_number>
```

For example:

```
diagnose switch-controller switch-info flapguard status S424ENTF19000007
```

Configuring PoE

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

This section covers the following topics:

Enabling PoE on the port

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

```
      edit <port_name>
        set poe-status {enable | disable}
      end
    end
```

For example:

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

Enabling PoE pre-standard detection

Depending on the FortiSwitch model, you can manually change the PoE pre-standard detection setting on the global level or on the port level. Starting with FortiOS 6.4.5, the factory default setting for `poe-pre-standard-detection` is `disable`.

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

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

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

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

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

Configuring PoE port settings

Starting in FortiOS 7.2.4 with FortiSwitchOS 7.2.3, you can configure the following PoE port settings on managed switches:

- Port mode—You can set the port mode to IEEE802.3 AF or IEEE802.3 AT.
- Port priority—You can set the port priority to critical, high, medium, or low. If there is not enough power, power is allotted first to critical-priority ports, then to high-priority ports, then to medium-priority ports, and then to low-priority

ports. Medium priority is available only on the following models: FS-224D-FPOE, FS-224E-POE, FS-248E-POE, FS-248E-FPOE, FS-424E-POE, FS-424E-FPOE, FS-M426E-FPOE, FS-448E-POE, FS-448E-FPOE, FS-524D-FPOE, and FS-548D-FPOE.

- Port power—You can set the port to use normal, power, perpetual power, or perpetual-fast power. Refer to the FortiSwitchOS feature matrix to see which FortiSwitch models support this feature.

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

To configure the PoE port settings:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set poe-port-mode {IEEE802_3AF | IEEE802_3AT}
            set poe-port-priority {critical-priority | high-priority | low-priority | medium-
                 priority}
            set poe-port-power {normal | perpetual | perpetual-fast}
         next
      end
   next
end
```

Resetting the PoE port

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

The following command resets PoE on the port:

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

Displaying general PoE status

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

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

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

Adding 802.3ad link aggregation groups (trunks)

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

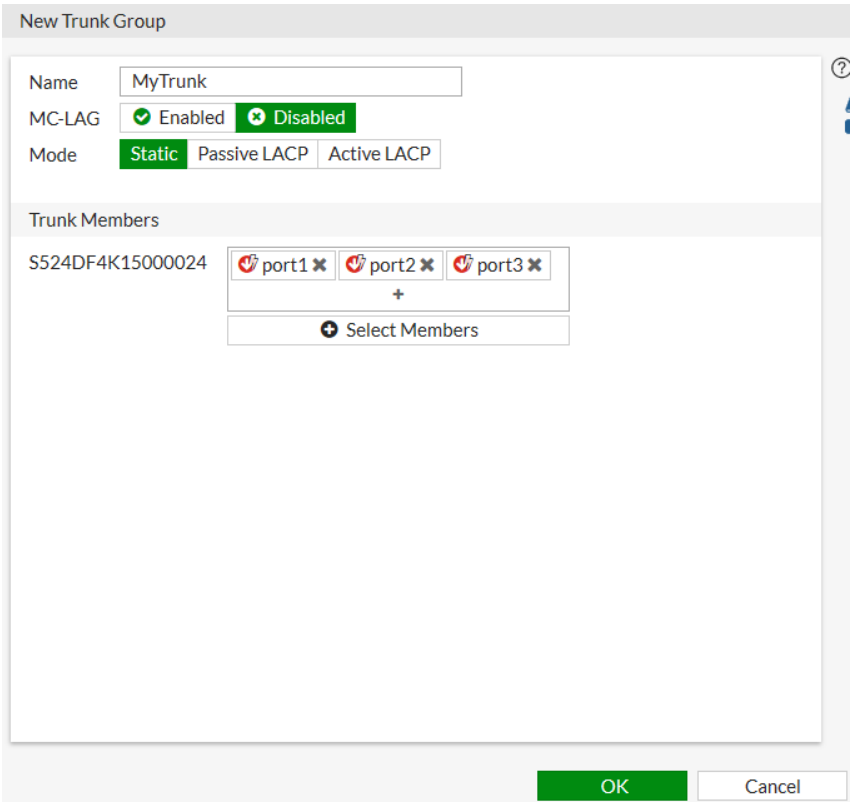
If multiple aggregators exist, one and only one of the aggregators is used by the trunk.

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

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

Using the FortiGate GUI:

1. Go to *WiFi & Switch Controller* > *FortiSwitch Ports*.
2. Click *Create New* > *Trunk*.
3. In the New Trunk Group page, enter a *Name* for the trunk group.
4. Select two or more physical ports to add to the trunk group and then select *Apply*.
5. Select the *Mode*: Static, Passive LACP, or Active LACP.
6. Select *Enabled* or *Disabled* for the MCLAG.
   - An MCLAG peer group must be configured before adding a trunk with MCLAG enabled. See MCLAG peer groups on page 60.
   - Make sure to select ports from switches that are part of the same MCLAG peer group.
7. Select *OK*.

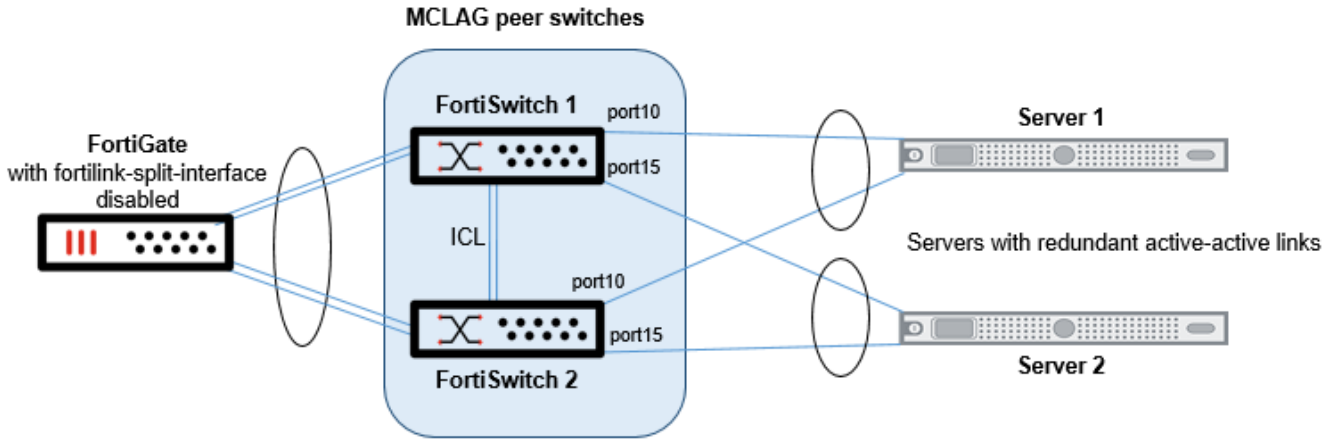


Using the the FortiGate CLI:

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

MCLAG trunks

The MCLAG trunk consists of 802.3ad link aggregation groups with members that belong to different FortiSwitch units. To configure an MCLAG trunk, you need an MCLAG peer group (see MCLAG peer groups on page 60). The MCLAG trunk members are selected from the same MCLAG peer group.



Using the GUI

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

Using the CLI

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

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

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

Variable	Description	Default
<switch-id>	FortiSwitch serial number.	No default
<trunk name>	Enter a name for the MCLAG trunk. **NOTE:** Each FortiSwitch unit that is part of the MCLAG must have the same MCLAG trunk name configured.	No default
type trunk	Set the interface type to a trunk port.	physical

Variable	Description	Default
mode {static | lacp-passive | lacp-active}	Set the LACP mode. —Set to `static` for static aggregation. In this mode, no control messages are sent, and received control messages are ignored. —Set to `lacp-passive` to passively use LACP to negotiate 802.3ad aggregation. —Set to `lacp-active` to actively use LACP to negotiate 802.3ad aggregation.	lacp-active
members "<port>,<port>"	Set the aggregated LAG bundle interfaces.	No default
mclag enable	Enable or disable the MCLAG.	disable

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

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

FortiLink mode supports the FortiSwitch split-port configuration:

- Configuring split ports on a previously discovered FortiSwitch unit on page 89
- Configuring split ports with a new FortiSwitch unit on page 89
- Configuring forward error correction on switch ports on page 89
- Configuring a split port on the FortiSwitch unit on page 90

Notes

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

  Use the `set port-configuration ?` command to check which ports are supported for each model.
- Currently, the maximum number of ports supported in software is 64 (including the management port). Therefore, only 10 QSFP ports can be split. This limitation applies to all of the models, but only the FS-3032D, FS-3032E, and the FS-1048E models have enough ports to encounter this limit.
- Use `10000full` for the general 10G interface configuration. If that setting does not work, use `10000cr` for copper connections (with copper cables such as 10GBASE-CR) or use `10000sr` for fiber connections (fiber optic transceivers such as 10GBASE-SR/-LR/-ER/-ZR).
- Starting in FortiOS 7.2.0 and FortiSwitchOS 7.2.0, the FortiGate device automatically updates the port list after split ports are changed and the FortiSwitch unit restarts. When split ports are added or removed, the changes are logged.

Configuring split ports on a previously discovered FortiSwitch unit

Before FortiSwitchOS 7.2.0:

1. On the FortiSwitch unit, configure the split ports. See Configuring a split port on the FortiSwitch unit on page 90.
2. Restart the FortiSwitch unit.
3. Remove the FortiSwitch from being managed:

```
config switch-controller managed-switch
   delete <FortiSwitch_serial_number>
end
```

4. Discover the FortiSwitch unit.
5. Authorize the FortiSwitch unit.

Starting with FortiSwitchOS 7.2.0:

1. On the FortiSwitch unit, configure the split ports. See Configuring a split port on the FortiSwitch unit on page 90.
2. Restart the FortiSwitch unit.

Configuring split ports with a new FortiSwitch unit

Before FortiSwitchOS 7.2.0:

1. Discover the FortiSwitch unit.
2. Authorize the FortiSwitch unit.
3. On the FortiSwitch unit, configure the split ports. See Configuring a split port on the FortiSwitch unit on page 90.
4. Restart the FortiSwitch unit.
5. Remove the FortiSwitch from being managed:

```
config switch-controller managed-switch
   delete <FortiSwitch_serial_number>
end
```

6. Discover the FortiSwitch unit.
7. Authorize the FortiSwitch unit.

Starting with FortiSwitchOS 7.2.0:

1. Discover the FortiSwitch unit.
2. Authorize the FortiSwitch unit.
3. On the FortiSwitch unit, configure the split ports. See Configuring a split port on the FortiSwitch unit on page 90.
4. Restart the FortiSwitch unit.

Configuring forward error correction on switch ports

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

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

```
                config ports
                        edit <port_name>
                                set fec-capable {0 | 1}
                                set fec-state {disabled | cl74 | cl91}
                        next
                end
        next
end
```

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

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

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

Configuring a split port on the FortiSwitch unit

To configure a split port:

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

The following settings are available:

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

- `6x40G`—For 1048E, enable the maximum speed (40G) of ports 49 through 54.
- `4x4x25G`—For 1048E, enable the maximum speed (100G) of ports 49 through 52; each split port has a maximum speed of 25G. Ports 47 and 48 are disabled.
- `single-port`—Use the port at the full base speed without splitting it.
- `4x25G`—For 100G QSFP only, split one port into four subports of 25 Gbps each.
- `4x10G`—For 40G or 100G QSFP only, split one port into four subports of 10Gbps each.
- `4x1G`—For 40G or 100G QSFP only, split one port into four subports of 1 Gbps each.
- `2x50G`—For 100G QSFP only, split one port into two subports of 50 Gbps each.

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

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

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

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

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

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

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

Restricting the type of frames allowed through IEEE 802.1Q ports

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

Use the following CLI commands:

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

Multitenancy and VDOMs

This section covers the following topics:

FortiSwitch ports dedicated to VDOMs

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

FortiSwitch ports can now be shared between VDOMs.

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

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

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

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

```
FG5H0E3917900081 (bbb) #
   config system interface
      edit "bbb-vlan99"
         set vdom "bbb"
         set allowaccess ping
         set device-identification enable
         set role lan
         set snmp-index 58
         set switch-controller-dhcp-snooping enable
         set interface "flink-lag" // this is the FortiLink interface in the root VDOM
         set vlanid 99
      next
   end

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

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

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

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

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

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

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

claim them before they are used.)

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

4. Check your configuration on the root VDOM:

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

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

5. Check your configuration on the tenant VDOM:

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

```
    end
```

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

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

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

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

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

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

NOTE: Shared ports do not support the following features:

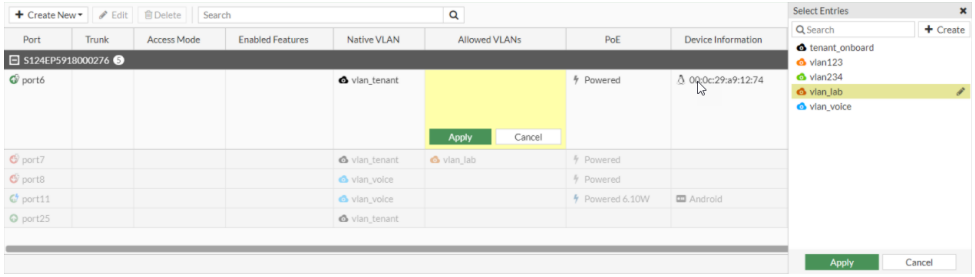
- LLDP
- STP
- BPDU guard
- Root guard
- DHCP snooping
- IGMP snooping
- MCLAG
- Quarantines

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

FortiSwitch VLANs from different VDOMs sharing the same FortiSwitch ports

In this scenario, there is no administrative separation, and all FortiSwitch ports and VLANs are created and assigned by the administrator of the VDOM where the FortiSwitch unit is controlled, usually root.

1. From the root VDOM, create the FortiSwitch VLANs and assign them to their respective VDOMs.
2. From the CLI, assign the VLANs to the FortiSwitch ports. The assigned VLANs are displayed in the GUI (*WiFi & Switch Controller* > *FortiSwitch Ports*) in the root VDOM.



NOTE: FortiSwitch units are not visible in non-root VDOMs.

Configuring switching features

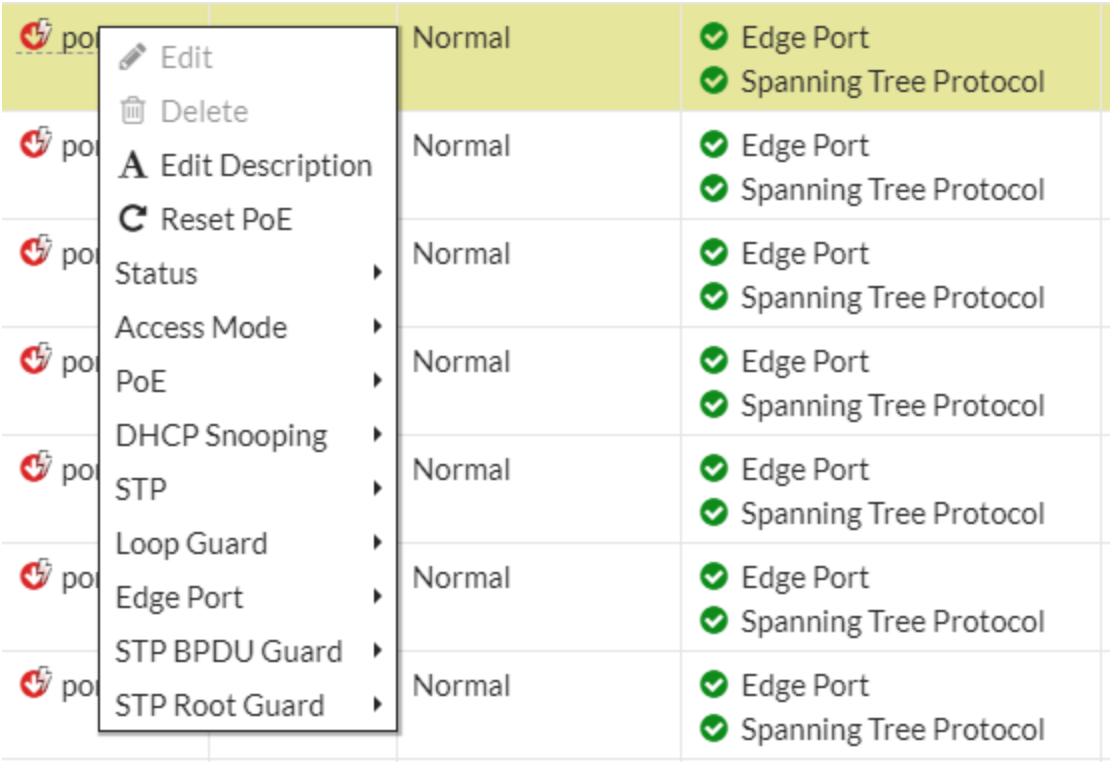
This section covers the following features:

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

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

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

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



Configuring edge ports

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

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

For example:

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

Configuring loop guard

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

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

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

For example:

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

Configuring STP settings

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

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

This section covers the following topics:

To configure STP for all managed FortiSwitch units:

```
config switch-controller stp-settings
   set name <name>
   set revision <stp revision>
   set hello-time <hello time>
```

```
   set forward-time <forwarding delay>
   set max-age <maximum aging time>
   set max-hops <maximum number of hops>
end
```

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

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

To configure MSTP instances:

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

For example:

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

Configuring STP on FortiSwitch ports

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.

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

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

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

For example:

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

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

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

For example:

```
FG100D3G15817028 # diagnose switch-controller switch-info stp S524DF4K15000024 0
MST Instance Information, primary-Channel:
Instance ID :   0
Switch Priority : 24576
Root MAC Address :    085b0ef195e4
Root Priority:    24576
Root Pathcost:    0
Regional Root MAC Address :   085b0ef195e4
Regional Root Priority:   24576
Regional Root Path Cost:  0
Remaining Hops:       20
This Bridge MAC Address :    085b0ef195e4
This bridge is the root

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

port1              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port2              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port3              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port4              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port5              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port6              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port7              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port8              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
port9              -       200000000  128        DISABLED     DISCARDING  YES    ENABLED
    NO
```

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

Configuring STP root guard

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

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

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

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

For example:

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

Configuring STP BPDU guard

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

There are two prerequisites for using BPDU guard:

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

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

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

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

For example:

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

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

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

For example:

```
FG100D3G15817028 # diagnose switch-controller switch-info bpdu-guard-status S524DF4K15000024
Managed Switch : S524DF4K15000024 0

Portname              State      Status       Timeout(m)     Count    Last-Event
____________________  ________   __________   ____________   ______   ________________

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

Configuring interoperation with per-VLAN RSTP

Starting in FortiOS 6.4.2, managed FortiSwitch units can now interoperate with a network that is running RPVST+. The existing network's configuration can be maintained while adding managed FortiSwitch units as an extended region. By default, interoperation with RPVST+ is disabled.

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

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

  In this case, follow this rule: If the root bridge for the CIST is within an MSTP region, VLANs other than VLAN 1

defined in the RPVST+ domains must have their bridge priorities worse (numerically greater) than that of the CIST root bridge within MSTP region.

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

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

To configure interoperation with RPVST+:

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

For example:

```
FGT-1 (testvdom) # config switch-controller managed-switch
FGT-1 (managed-switch) # edit FS3E32T419000006
FGT-1 (FS3E32T419000006) # config ports
FGT-1 (ports) # edit port5
FGT-1 (port5) # set rpvst-port enabled
FGT-1 (port5) # next
FGT-1 (ports) # end
```

A maximum of 16 VLANs is supported; the maximum number of VLANs includes native VLANs. You must configure the same VLANs as those used in the RPVST+ domain.

To check your configuration and to diagnose any problems:

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

For example:

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

Dynamic MAC address learning

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

This section covers the following topics:

Limiting the number of learned MAC addresses on a FortiSwitch interface

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

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

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

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

For example:

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

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

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

For example:

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

Controlling how long learned MAC addresses are saved

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

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

For example:

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

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

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

For example:

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

Logging violations of the MAC address learning limit

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

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

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

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

For example:

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

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

- `diagnose switch-controller switch-info mac-limit-violations all <FortiSwitch_serial_number>`

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

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

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

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

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

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

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

Persistent (sticky) MAC addresses

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

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

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

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

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

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

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

Logging changes to MAC addresses

Use the following commands to create syslog entries for when MAC addresses are learned, aged out, and removed:

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

```
end
```

Configuring storm control

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

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

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

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

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

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

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

For example:

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

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

Configuring IGMP-snooping settings

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

You cannot use IGMP snooping when network access control (NAC) has been enabled on a global scale with `set mode global` under the `config switch-controller nac-settings` command.

This section covers the following topics:

Configuring global IGMP-snooping settings

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

Aging time is the maximum number of seconds that the system will retain a multicast snooping entry. The range of values is 15 to 3,600 seconds. The default value is 300 seconds.

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

Starting in FortOS 7.2.1 with FortiSwitchOS 7.2.1, you can specify how often the managed FortiSwitch unit will send IGMP version-2 queries when the IGMP-snooping querier is configured. The range of values is 10-1,200 seconds. By default, queries are sent every 125 seconds. The value for `aging-time` must be greater than the value for `query-interval`.

```
config switch-controller igmp-snooping
   set aging-time <15-3600>
   set flood-unknown-multicast {enable | disable}
   set query-interval <10-1200>
end
```

Configuring IGMP-snooping settings on a switch

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

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

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

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

For example:

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

Configuring the IGMP-snooping proxy

Before FortiOS 7.0.2, you could use the CLI to enable IGMP proxy on a system-wide basis. Starting in FortiOS 7.0.2, you can use the CLI to enable IGMP proxy per FortiSwitch unit.

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

To enable IGMP snooping and the IGMP-snooping proxy:

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

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

```
config system interface
   edit vlan100
      set switch-controller-igmp-snooping enable
      set switch-controller-igmp-snooping-proxy enable
   next
```

```
end
```

Configuring the IGMP-snooping querier

Starting in FortiOS 7.0.2, you can configure the IGMP-snooping querier version 2 or 3. When the IGMP querier version 2 is configured, the managed FortiSwitch unit will send IGMP version-2 queries when no external querier is present. When the IGMP querier version 3 is configured, the managed FortiSwitch unit will send IGMP version-3 queries when no external querier is present.

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

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

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

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

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

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

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

For example:

```
config switch-controller managed-switch
   edit S524DF4K15000024
   config igmp-snooping
      set local-override enable
      set aging-time 1000
      set flood-unknown-multicast enable
      config vlans
         edit vlan100
            set proxy disable
            set querier enable
            set querier-addr 1.2.3.4
```

```
            set version 3
        next
      end
   end
end
```

Configuring PTP transparent-clock mode

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

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

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

1. Configure the global PTP settings.
   By default, PTP is disabled.
2. Enable the PTP policy.
   By default, the PTP policy is enabled.
3. Apply the PTP policy to a port.
   NOTE: PTP policies are hidden on virtual ports

To configure the global PTP settings:

```
config switch-controller ptp settings
   set mode {disable | transparent-e2e | transparent-p2p}
end
```

To enable the PTP policy:

```
config switch-controller ptp policy
   edit {default | <policy_name>}
      set status {enable | disable}
   next
end
```

To apply the PTP policy to a port:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set ptp-policy {default | <policy_name>}
         end
      end
```

For example:

```
config switch-controller ptp settings
   set mode transparent-p2p
end
```

```
config switch-controller ptp policy
   edit ptppolicy1
      set status enable
   next
end

config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port5
            set ptp-policy ptppolicy1
         end
      end
```

Device detection

This section covers the following topics:

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
```

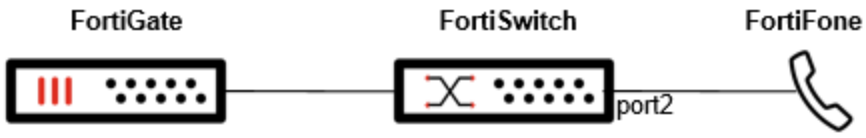
You can display a list of detected devices from the *Device Inventory* menu in the GUI. To list the detected devices in the CLI, enter the following command:

```
diagnose user device list
```

Voice device detection

FortiSwitchOS is able to parse LLDP messages from voice devices such as FortiFone and pass this information to a FortiGate device for device detection. You can use a dynamic port policy to assign a device to an LLDP profile, QoS policy, and VLAN policy. When a detected device is matched to the dynamic port policy, the corresponding policy actions are applied on the switch port.

In the following example, FortiFone is connected to port2 of the FortiSwitch unit. A dynamic port policy is created to apply a VLAN policy, LLDP policy, and QoS policy to the device family FortiFone.

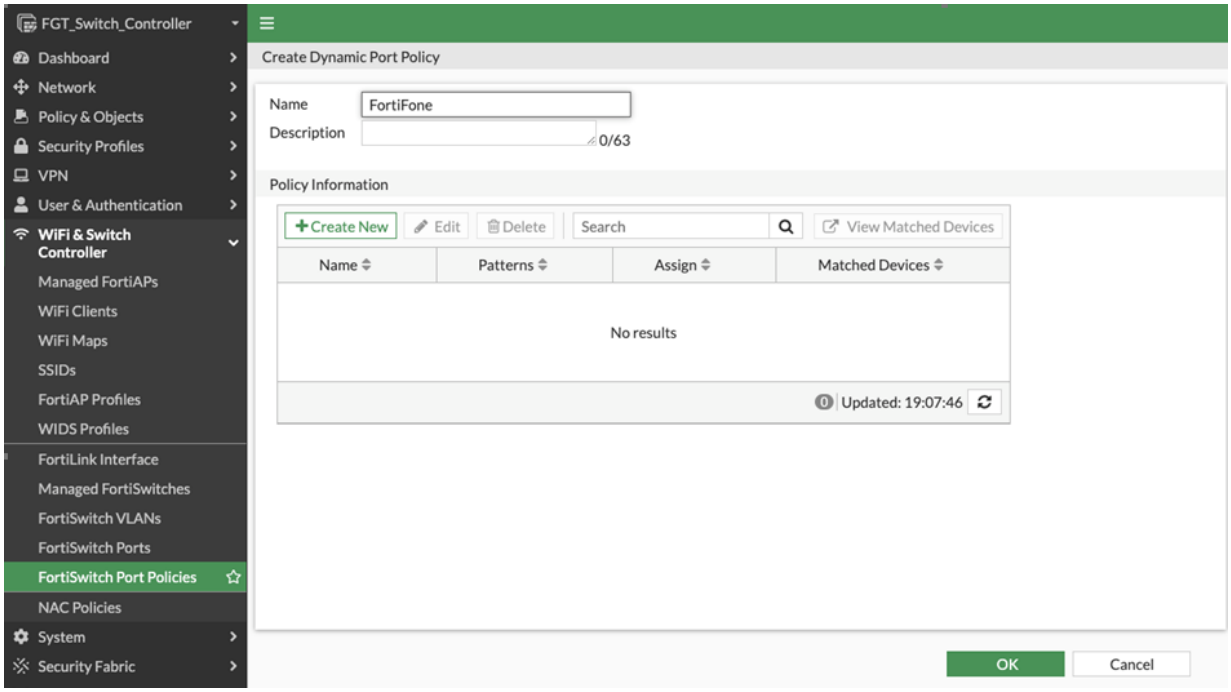


The following is a summary of the procedure:

1. Use the FortiGate CLI to configure the VLAN policy, LLDP profile, and Quality of Service (QoS) policy. You can use the predefined `voice-qos` policy for QoS and the predefined `fortivoice.fortilink` profile for LLDP.
2. Use the FortiGate GUI to configure a dynamic port policy to match the FortiFone device family with the actions from the assigned LLDP profile, QoS policy, and VLAN policy.
3. Use the FortiGate GUI to assign the dynamic port policy to the FortiSwitch port.

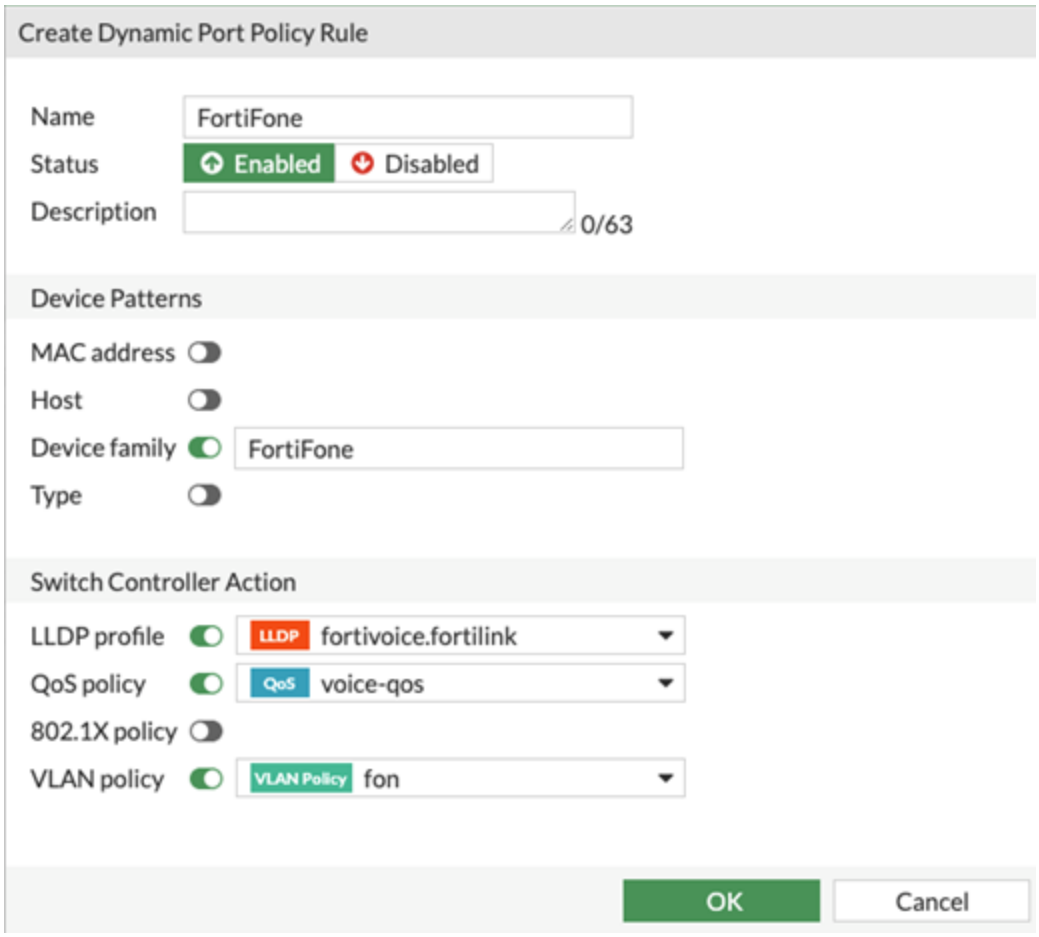
To create a dynamic port policy in the GUI and then assign it to a FortiSwitch port:

1. Go to *WiFi & Switch Controller* > *FortiSwitch Port Policies* and click *Dynamic Port Policies*.
   a. Click *Create New* to create a dynamic port policy.
   b. In the *Name* field, enter `FortiFone`.

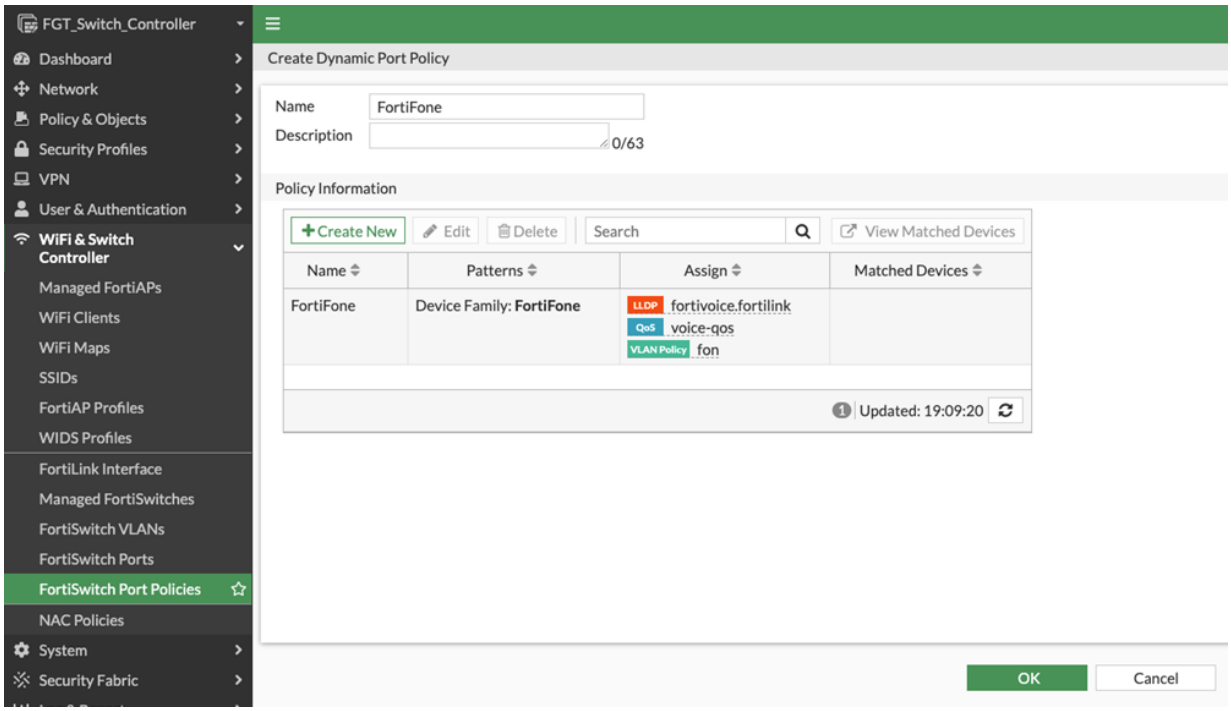


   c. Click *Create new* to create a dynamic port policy rule.
   d. In the Name field, enter `FortiFone`.
   e. Disable *MAC address*.
   f. Enable *Device family* and enter `FortiFone`.
   g. Enable *LLDP profile* and select a voice profile.
   h. Enable *QoS policy* and select a voice policy.

i. Enable *VLAN policy* and select a voice policy.



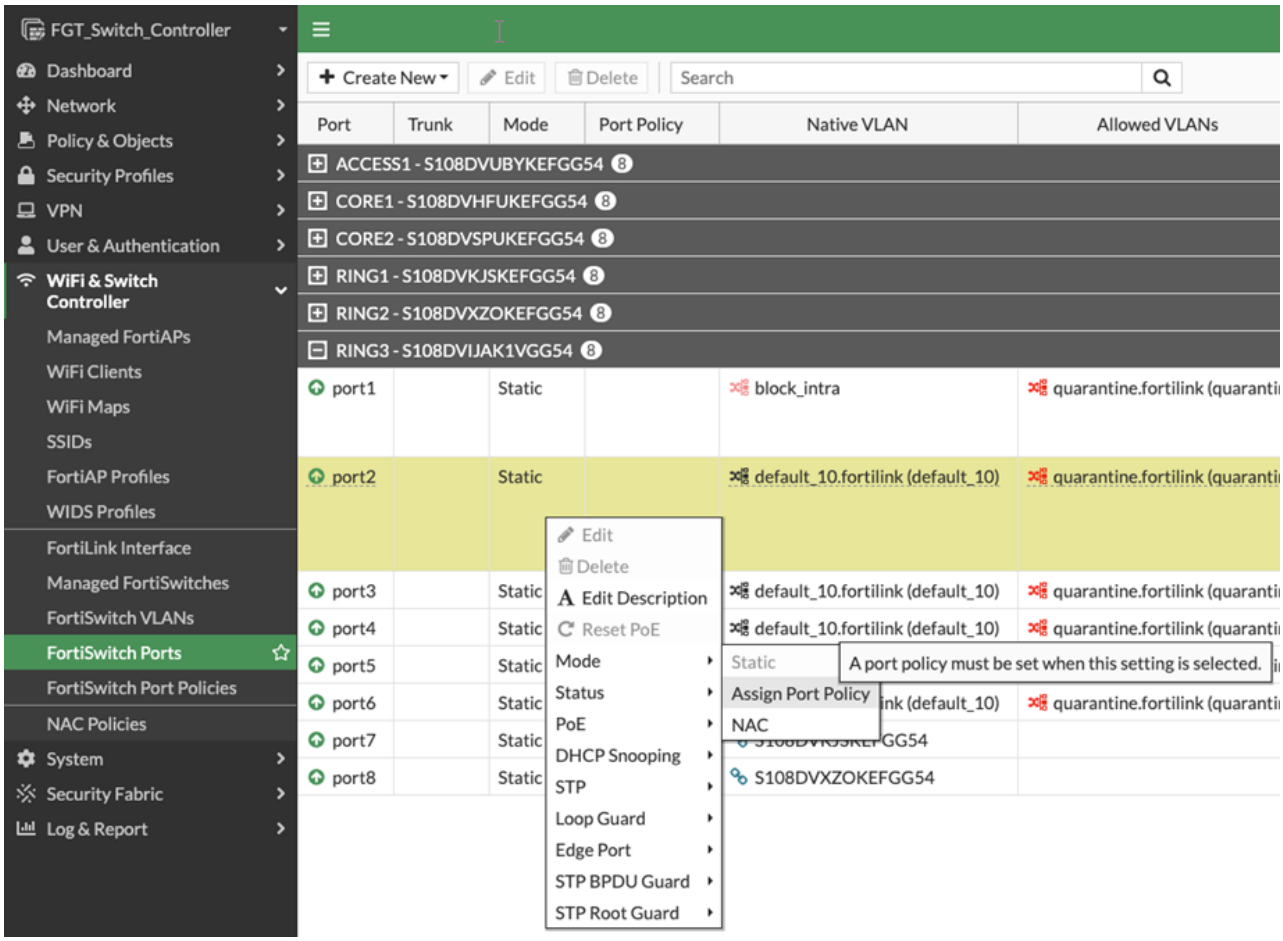
j. Click *OK* to save the dynamic port policy rule.



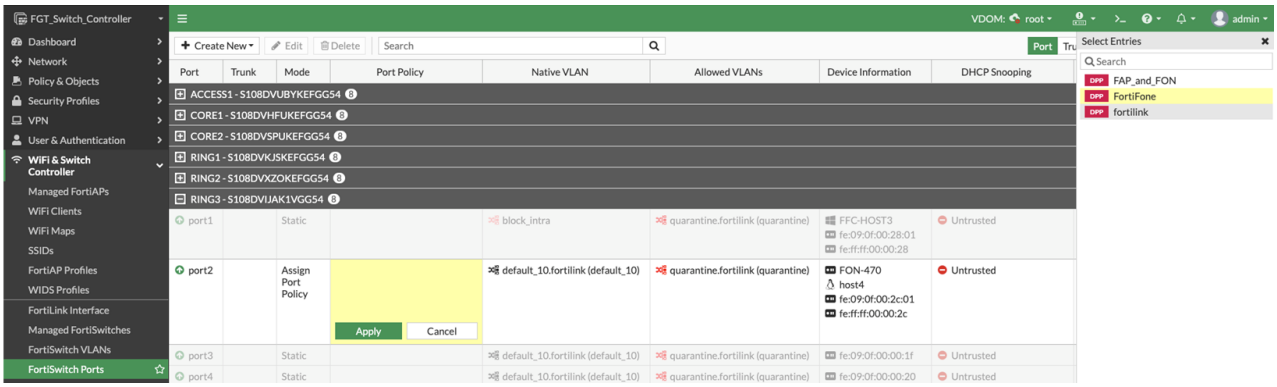
k. Click *OK* to save the dynamic port policy.

2. Go to *WiFi & Switch Controller* > *FortiSwitch Ports*.

3. Right-click *port2* and select *Mode* > *Assign Port Policy*.

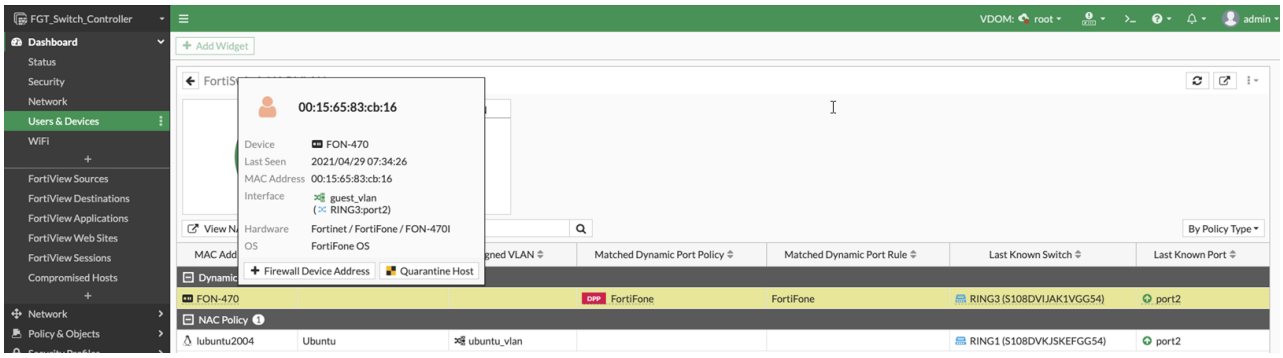


4. Click the pencil icon in the Port Policy column, select the *FortiFone* dynamic port policy, and then click *Apply*.



5. Plug the FortiFone into port2 of the FortiSwitch unit.

6. Go to *Dashboard* > *Users & Devices* and verify that the FortiFone is displayed in the *FortiSwitch NAC VLANs* pane.



To configure voice device detection in the CLI:

1. Use the FortiGate CLI to configure the VLAN policy, LLDP profile, and QoS policy.

```
config switch-controller lldp-profile
   edit "fortivoice.fortilink"
      set med-tlvs inventory-management network-policy location-identification
      set auto-isl disable
      config med-network-policy
         edit "voice"
            set status enable
            set vlan-intf "voice"
            set assign-vlan enable
            set dscp 46
         next
         edit "voice-signaling"
            set status enable
            set vlan-intf "voice"
            set assign-vlan enable
            set dscp 46
         next
         edit "guest-voice"
         next
         edit "guest-voice-signaling"
         next
         edit "softphone-voice"
         next
         edit "video-conferencing"
         next
         edit "streaming-video"
         next
         edit "video-signaling"
         next
      end
      config med-location-service
         edit "coordinates"
         next
         edit "address-civic"
         next
         edit "elin-number"
         next
      end
```

```
   next
end

config switch-controller qos qos-policy
   edit "voice-qos"
      set trust-dot1p-map "voice-dot1p"
      set trust-ip-dscp-map "voice-dscp"
      set queue-policy "voice-egress"
   next
end

config switch-controller vlan-policy
     edit "fon"
        set fortilink "fortilink"
        set vlan "default_10"
        set allowed-vlans "quarantine" "voice"
        set untagged-vlans "quarantine"
     next
end
```

2. Configure a dynamic port policy to match the FortiFone device family with the actions from the assigned LLDP profile, QoS policy, and VLAN policy.

```
   config switch-controller dynamic-port-policy
      edit "FortiFone"
         set fortilink "fortilink"
         config policy
            edit "FortiFone"
               set family "FortiFone"
               set lldp-profile "fortivoice.fortilink"
               set qos-policy "voice-qos"
               set vlan-policy "fon"
            next
         end
      next
   end
```

3. Assign the dynamic port policy to port2 of the FortiSwitch unit.

```
config switch-controller managed-switch
   edit S108DVIJAK1VGG54
   config ports
      edit "port2"
         set vlan "default_10"
         set allowed-vlans "quarantine"
         set untagged-vlans "quarantine"
         set access-mode dynamic
         set port-policy "FortiFone"
         set export-to "root"
         set mac-addr 02:09:0f:00:2c:01
      next
   end
```

4. The FortiSwitch unit receives an LLDP message from FortiFone after it is plugged into port2.
5. Run the `diagnose switch-controller mac-device dynamic` command to check the device information on FortiGate device. The FortiFone is identified.

```
FGT_Switch_Controller (root) # diagnose switch-controller mac-device dynamic
Vdom: root
MAC                LAST-KNOWN-SWITCH  LAST-KNOWN-PORT    DYNAMIC-PORT-POLICY      POLICY
            LAST-SEEN    COMMENTS
00:15:65:83:cb:16  S108DVIJAK1VGG54   port2              FortiFone
FortiFone          148          auto detected @ 2021-04-29 19:12:42
```

Configuring IoT detection

NOTE: This feature requires an IoT Detection Service license.

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

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

You can control how often a FortiSwitch unit scans for IoT devices. The range of values is 2 to 10,080 minutes. By default, the scan interval is 60 minutes. Every MAC address will be scanned for a time interval of 60 minutes followed by 60 minutes when it will not be scanned. The start time of every MAC address's 60-minute scan interval is unique. Set the `iot-scan-interval` value to 0 to disable IoT detection.

A MAC address of an IoT device must be detected by the FortiSwitch unit for more than a specified number of minutes before the MAC address is passed along to the FortiGuard service for IoT identification. The default number of minutes is 5. The range of values is 0 to 10,080 minutes. Set the `iot-holdoff` value to 0 to disable this setting.

If a MAC address entry's last-seen time is greater than the `iot-mac-idle` value, the MAC address entry is not considered for IoT detection. By default, the `iot-mac-idle` value is 1,440 minutes. The range of values is 0 to 10,080 minutes.

To configure system-wide settings for IoT detection:

```
config switch-controller system
   set iot-weight-threshold <0-255>
   set iot-scan-interval <2-10080>
   set iot-holdoff <0-10080>
   set iot-mac-idle <0-10080>
end
```

Starting in FortiOS 6.4.3, IoT detection can be managed per FortiLink interface as well. IoT detection is disabled by default on the FortiLink interface. Use the FortiOS CLI or GUI to enable IoT detection on the FortiLink interface so that the FortiSwitch unit starts scanning for IoT devices.

Using the GUI:

1. Go to *WiFi & Switch Controller* > *FortiLink Interface*.
2. Enable *IoT scanning*.

Using the CLI:

```
config system interface
   edit <FortiLink_interface>
      set switch-controller-iot-scanning enable
   end
```

Configuring LLDP-MED settings

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

This section covers the following topics:

To configure LLDP profiles in FortiOS:

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

```
      end
    next
end
```

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

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

To configure LLDP settings in FortiOS:

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

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

To configure dynamic detection of LLDP neighbor devices in FortiSwitchOS:

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

Creating LLDP asset tags for each managed FortiSwitch

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

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

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

Adding media endpoint discovery (MED) to an LLDP configuration

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

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

Displaying LLDP information

You can use the following commands to display LLDP information:

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

Configuring the LLDP settings

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

Starting in FortiOS 6.4.3, you can also configure the `lldp-status` and `lldp-profile` settings of a virtual switch port in a tenant VDOM. **NOTE:** The `auto-isl` setting in `config switch-controller lldp-profile` is ignored, and the setting remains disabled for the tenant's ports.

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

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

For example:

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

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

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

For example:

```
config vdom
   edit VDOM_1
      config switch-controller managed-switch
         edit "S424ENTF19000007"
            config ports
               edit port28
                  set lldp-status tx-rx
                  set lldp-profile lldpprofile1
               next
            end
         end
```

```
    end
```

FortiSwitch security

This section covers the following topics:

FortiSwitch network access control

You can configure a FortiSwitch network access control (NAC) policy within FortiOS that matches devices with the specified criteria, devices belonging to a specified user group, or devices with a specified FortiClient EMS tag. Devices that match are assigned to a specific VLAN or have port-specific settings applied to them.

NOTE: The FortiSwitch NAC settings must be configured before defining a NAC policy. See Configuring the FortiSwitch NAC settings on page 130.

Summary of the procedure

1. Define a FortiSwitch NAC VLAN. See Defining a FortiSwitch NAC VLAN on page 128.
2. Configure the FortiSwitch NAC settings. See Configuring the FortiSwitch NAC settings on page 130.
3. Create a FortiSwitch NAC policy. See Defining a FortiSwitch NAC policy on page 133.
4. View the devices that match the NAC policy. See Viewing the devices that match the NAC policy on page 139.
5. View device statistics. See Viewing device statistics on page 139.

Defining a FortiSwitch NAC VLAN

When devices are matched by a NAC policy, you can assign those devices to a FortiSwitch NAC VLAN. By default, there are six VLAN templates:

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

- *video*—This VLAN is dedicated for video devices.
- *onboarding*—This VLAN is for NAC onboarding devices.

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

Creating a NAC VLAN

Using the GUI:

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

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

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

Using the CLI:

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

Editing a NAC VLAN

You can edit the default `onboarding` NAC VLAN.

Using the GUI:

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

Using the CLI:

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

```
    set auto-ip {enable | disable}
    set dhcp-server {enable | disable}
end
```

Configuring the FortiSwitch NAC settings

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

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

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

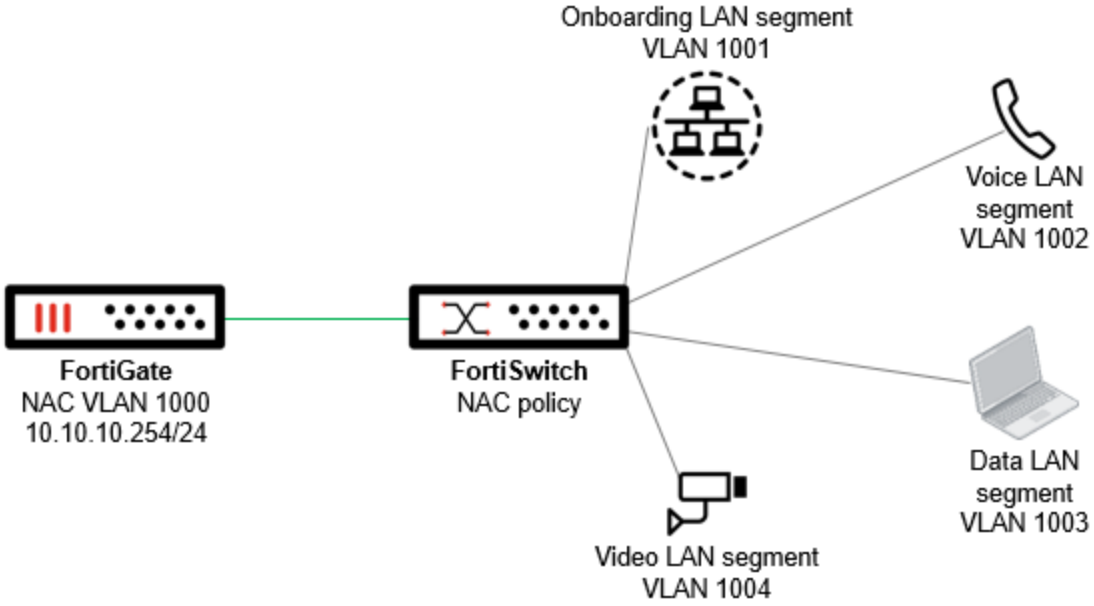
When NAC devices are discovered, they are assigned to the NAC onboarding VLAN. You can specify the default `onboarding` VLAN or specify another existing VLAN. By default, there is no NAC onboarding VLAN assigned.

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

Starting in FortiOS 7.0.0, you can use the `set nac-periodic-interval` command to specify how often the NAC engine runs in case any events are missed. The range is 5 to 180 seconds, and the default setting is 60 seconds.

When NAC mode is configured on a port, the link of a switch port goes down and then up by default, which restarts the DHCP process for that device. When a link goes down, the NAC devices are cleared from the switch port that bounced. Bouncing the switch port and restarting DHCP changes the IP addresses of hosts and invalidates firewall sessions. Starting in FortiOS 7.0.1, you can avoid these problems by assigning each VLAN to a separate LAN segment.

LAN segments prevent the IP addresses of hosts from changing but still provide physical isolation. For example, the following figure shows how four LAN segments have been assigned to four separate VLANs:



The switch controls traffic between LAN segments. Enable *Block Intra-VLAN Traffic* in the GUI or use the `set switch-controller-access-vlan` command to allow or prevent traffic between hosts in a LAN segment.

An RSPAN VLAN interface cannot be a member of a LAN segment group.

LAN segments require the following:

- FortiGate devices running FortiOS 7.0.1 or higher with managed FortiSwitch units running FortiSwitchOS 7.0.1 or higher.
- To see which FortiSwitch models support this feature, refer to the FortiSwitch feature matrix.

The FortiGate device supports only one LAN segment.

LAN segments on the FS-108E, FS-108E-POE, FS-108E-FPOE, FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models have the following limitations:

- After you enable LAN segments, FortiSwitchOS automatically assigns a VLAN for internal use. This VLAN cannot be used for any other purpose. If you want to assign a different internal VLAN, type `set lan-internal-vlan ?` to see a range of VLANs; however, these VLANs might not be available. If no VLANs are available to be used as an internal VLAN, the LAN segment configuration returns an error message.
- These models cannot be directly connected to a FortiGate device; they should be connected using another FortiSwitch model.
- FortiSwitchOS 7.2.0 or later is required.
- All LAN segment VLANs (both primary VLANs and sub-VLANs) must belong to the same STP instance. Multiple STP instances are not supported within the same LAN segment VLANs.
- For packets coming from sub-VLANs or primary VLANs, MAC learning occurs on the internal VLAN, not the primary VLAN or sub-VLAN.

Starting in FortiSwitchOS 7.2.0 and FortiOS 7.2.0, IGMP snooping and MLD snooping are supported on FortiLink NAC LAN segments.

If you want to enable IGMP snooping in a LAN segment, IGMP snooping must be enabled on all VLANs in the segment, including the primary VLAN, sub-VLANs, and onboarding VLANs. Multicast data streams are expected to come in ONLY on the primary VLAN.

To use LAN segments:

- Configure FortiSwitch VLANs without layer-3 properties (unset the IP address, set the access mode to `static`, unset `allowaccess`, and disable the DHCP server).
- Optionally, enable *Block Intra-VLAN Traffic*.
- Enable LAN segments.
- Specify the NAC LAN interface.
- Specify which VLANs belong to that LAN segment.

Do not make changes after assigning a VLAN to a LAN segment. Changing VLANs assigned to LAN segments might have unexpected results.

Configuring NAC settings

Using the CLI:

```
config switch-controller fortilink-settings
   edit <name_of_FortiLink_interface>
      set inactive-timer <integer>
      set link-down-flush {enable | disable}
      config nac-ports
         set onboarding-vlan <string>
         set bounce-nac-port {enable | disable}
         set lan-segment {enabled | disabled}
         set nac-lan-interfaces <string>
         set nac-segment-vlans <VLAN_interface_name>
      end
   next
end

config switch-controller system
   set nac-periodic-interval <5-180 seconds>
end
```

For example:

```
config switch-controller fortilink-settings
   edit "fortilink"
      config nac-ports
         set onboarding-vlan "onboarding"
         set lan-segment enabled
         set nac-lan-interface "nac_segment"
         set nac-segment-vlans "voice" "video"
      end
   next
end

config switch-controller system
   set nac-periodic-interval 100
end
```

Using the GUI:

1. Go to *WiFi & Switch Controller* > *NAC Policies*.
2. Select a NAC LAN and click *Edit*.
3. For the *NAC VLAN segmentation*, click *Enabled*.
4. From the *Primary Interface* dropdown list, select the primary interface. The IP address and DHCP server of the primary interface are shared by the segment VLANs.
5. From the *Onboarding VLAN* dropdown list, select the onboarding VLAN.
6. In the *Segment VLANs* field, click + and select one or more segment VLANs.
7. Click *OK*.

Enabling NAC on a FortiSwitch port

Using the CLI:

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

Using the GUI:

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

Synchronizing MAC events

```
config switch interface
   edit <FortiSwitch_interface>
      set nac enable
   end
```

For example:

```
config switch interface
   edit port20
      set nac enable
   end
```

Defining a FortiSwitch NAC policy

In the FortiOS GUI, you can create three types of NAC policies:

- *Device*—The NAC policy matches devices with the specified MAC address, hardware vendor, device family, type, operating system, and user. Visit https://filestore.fortinet.com/product-downloads/fortilink/HTFO_list.json to see a list of values for hardware vendor, type, device family, and operating system.
- *User*—The NAC policy matches devices belonging to the specified user group.
- *EMS tag*—The NAC policy matches devices with the specified FortiClient EMS tag.

Using the CLI, you can specify a MAC policy to be applied to devices that have been matched by the NAC policy. See Creating a MAC policy on page 138.

Starting in FortiOS 7.0.2, you can specify FortiSwitch groups in NAC policies instead of specifying individual managed FortiSwitch units when creating a NAC policy. In FortiOS 7.0.2, the `set switch-scope` command has been replaced with the `set switch-group` command. You can select more than one FortiSwitch group in the CLI and GUI, and the same FortiSwitch unit can be included in more than one FortiSwitch group. If no FortiSwitch group is specified in the `set switch-group` command, all FortiSwitch groups are used for the NAC policy.

When you upgrade to FortiOS 7.0.2, the individual FortiSwitch units selected for the NAC policy are assigned to a new FortiSwitch group, and the new FortiSwitch group replaces the individual FortiSwitch units in the NAC policy. If you downgrade from FortiOS 7.0.2, the individual FortiSwitch units in the FortiSwitch group are listed in the `set switch-scope` command in the NAC policy, and the `set switch-group` command is removed from the NAC policy.

NOTE: The FortiSwitch NAC settings must be configured before defining a FortiSwitch NAC policy. See Configuring the FortiSwitch NAC settings on page 130.

Starting in FortiOS 7.2.4 with FortiSwitchOS 7.2.2 or later, NAC supports more connected devices—up to 48 times the maximum number of managed FortiSwitch units supported on the FortiGate device. You can use the `diagnose switch-controller mac-device nac known` command to check the number of known devices. When 95 percent of the maximum number of devices is reached, a warning icon is displayed in the *Matched NAC Devices* widget in the FortiOS GUI. When the maximum number is reached, a switch-controller event is logged.

Creating a device policy

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

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

Starting in FortiOS 7.0.1, you can configure a dynamic firewall address for devices and use it in a NAC policy. When a device matches the NAC policy, the MAC address for that device is automatically assigned to the dynamic firewall address, which can be used in firewall policies to control traffic from/to these devices. Configuring a dynamic firewall address requires setting the address type to `dynamic` and the address subtype to `swc-tag`. Using the dynamic firewall address in a NAC policy requires specifying the conditions that a device must match and setting the firewall address to the name of the dynamic firewall address.

To identify devices to add to a device policy, try the following:

- Use the `diagnose user device list` command to see devices connected to your FortiGate device.
- Use the FortiGuard Device Detection service (https://www.fortiguard.com/learnmore#dds) to provide information about an IoT device based on its MAC address.

Using the GUI to configure a NAC policy and a dynamic firewall address:

1. Go to *WiFi & Switch Controller* > *NAC Policies*.
2. Click *Create New*.
3. In the Name field, enter a name for the NAC policy.
4. Make certain that the status is set to *Enabled*.
5. Click *Specify* to select which FortiSwitch groups to apply the NAC policy to or click *All*.
6. Select *Device* for the category.
7. If you want the device to match a MAC address, enable *MAC Address* and enter the MAC address to match. Starting in FortiOS 6.4.6, you can use the wildcard * character when entering the MAC address (for example, `xx:xx:xx:**:**:**`).

8. If you want the device to match a hardware vendor, enable *Hardware Vendor* and enter the name of the hardware vendor to match. Starting in FortiOS 6.4.6, you can use the wildcard * character when entering the hardware vendor.
9. If you want the device to match a device family, enable *Device Family* and enter the name of the device family to match. Starting in FortiOS 6.4.6, you can use the wildcard * character when entering the device family.
10. If you want the device to match a device type, enable *Type* and enter the device type to match. Starting in FortiOS 6.4.6, you can use the wildcard * character when entering the device type.
11. If you want the device to match an operating system, enable *Operating System* and enter the operating system to match. Starting in FortiOS 6.4.6, you can use the wildcard * character when entering the operating system.
12. If you want the device to match a user, enable *User* and enter the user name to match. Starting in FortiOS 6.4.6, you can use the wildcard * character when entering the user name.
13. If you want to assign a specific VLAN to the device that matches the specified criteria, select *Assign VLAN* and enter the VLAN identifier.
14. If you do not want to bounce the switch port (administratively bringing the link down and then up) when NAC mode is configured, disable *Bounce port*.
15. To use a dynamic firewall address for matching a device, enable *Assign device to dynamic address* and, from the dropdown list, click *Create*.
    a. In the *Name* field, enter the name of the dynamic firewall address.
    b. To change the color, click *Change* and select the color used for the corresponding icon in the GUI.
    c. The address type is set to *Dynamic* by default and the subtype is set to *Switch Controller NAC Policy Tag* by default.
    d. For the interface, select the interface whose IP address is to be used.
    e. In the *Comments* field, enter a description of the dynamic firewall address.
    f. Click *OK* to save the dynamic firewall address.
16. Select *OK* to create the new NAC policy.

Using the CLI to configure a dynamic firewall address:

```
config firewall address
   edit <name_of_dynamic_firewall_address>
      set type dynamic
      set sub-type swc-tag
   next
end
```

For example:

```
config firewall address
   edit "office_vm_device"
      set type dynamic
      set sub-type swc-tag
   next
end
```

To view the dynamic MAC addresses attached to the firewall:

```
diagnose firewall dynamic list
```

Using the CLI to configure a NAC policy:

```
config user nac-policy
   edit <policy_name>
      set description <description_of_policy>
```

```
      set category device
      set status enable
      set mac <MAC_address>
      set hw-vendor <hardware_vendor>
      set type <device_type>
      set family <device_family>
      set os <operating_system>
      set hw-version <hardware_version>
      set sw-version <software_version>
      set host <host_name>
      set user <user_name>.
      set src <source>
      set switch-fortilink <FortiLink_interface>
      set switch-group <list_of_FortiSwitch_groups>
      set switch-auto-auth {enable | disable}
      set switch-mac-policy <switch_mac_policy>
      set firewall-address <name_of_dynamic_firewall_address>
   end
```

For example:

```
config user nac-policy
   edit "OFFICE_VM"
      set hw-vendor "VMware"
      set switch-fortilink "fortilink"
      set switch-mac-policy "OFFICE_VM"
      set firewall-address "office_vm_device"
   next
end
```

Creating a user policy

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

Using the GUI:

1. Go to *WiFi & Switch Controller* > *NAC Policies*.
2. Select *Create New*.
3. In the Name field, enter a name for the NAC policy.
4. Make certain that the status is set to *Enabled*.
5. Click *Specify* to select which FortiSwitch groups to apply the NAC policy to or click *All*.
6. Select *User* for the category.
7. Select which user group that devices must belong to.
8. If you want to assign a specific VLAN to a device assigned to the specified user group, select *Assign VLAN* and enter the VLAN identifier.
9. Select *OK* to create the new NAC policy.

Using the CLI:

```
config user nac-policy
   edit <policy_name>
      set description <description_of_policy>
      set category firewall-user user
```

```
    set status enable
    set user-group <name_of_user_group>
    set switch-fortilink <FortiLink_interface>
    set switch-group <list_of_FortiSwitch_groups>
    set switch-auto-auth {enable | disable}
    set switch-mac-policy <switch_mac_policy>
end
```

Creating an EMS-tag policy

An EMS-tag policy matches devices with a specified MAC address and then assigns a specific VLAN to those devices or applies port-level settings to those devices. The MAC address is derived from an Endpoint Management Server (EMS) tag created in FortiClient.

NOTE: The FortiClient EMS server must be 6.4.1 build 1442 or higher. FortiOS must be 6.4.2 build 1709 or higher.

Before creating an EMS-tag policy on a managed FortiSwitch unit:

1. In FortiClient EMS, group FortiClient Fabric Agent endpoints with an EMS tag.
2. In FortiClient EMS, share these endpoint groups with a FortiGate unit over the EMS connector.
3. In FortiOS, add an on-premise FortiClient EMS server to the Security Fabric:

```
config endpoint-control fctems
   edit <ems_name>
      set server <ip_address>
      set certificate <string>
   next
end
```

For example:

```
config endpoint-control fctems
   edit EMS_Server
      set server 1.2.3.4
      set certificate REMOTE_Cert_1
   next
end
```

4. In FortiOS, verify the EMS certificate. For example:

```
execute fctems verify EMS_Server
```

5. In FortiOS, check that the FortiGate unit and FortiClient are connected:

```
diagnose user device get <FortiClient_MAC_address>
```

6. In FortiOS, verify which MAC addresses the dynamic firewall address resolves to:

```
diagnose firewall dynamic list
```

Using the GUI to create an EMS-tag policy:

1. Go to *WiFi & Switch Controller* > *NAC Policies*.
2. Select *Create New*.
3. In the Name field, enter a name for the NAC policy.
4. Make certain that the status is set to *Enabled*.
5. Click *Specify* to select which FortiSwitch groups to apply the NAC policy to or click *All*.
6. Select *EMS Tag* for the category.
7. Select which FortiClient EMS tag that devices must be assigned.
8. If you want to assign a specific VLAN to a device assigned to the specified EMS tag, select *Assign VLAN* and enter the VLAN identifier.
9. Select *OK* to create the new NAC policy.

Using the CLI to create an EMS-tag policy:

```
config user nac-policy
   edit <policy_name>
      set description <description_of_policy>
      set category ems-tag
      set ems-tag <string>
      set status enable
      set switch-fortilink <FortiLink_interface>
      set switch-group <list_of_FortiSwitch_groups>
      set switch-auto-auth {enable | disable}
      set switch-mac-policy <switch_mac_policy>
   next
end
```

For example:

```
config user nac-policy
   edit nac_policy_1
      set category ems-tag
      set ems-tag MAC_FCTEMS0000108427_Low
      set switch-fortilink fortilink1
   next
end
```

Creating a MAC policy

You can apply a MAC policy to the devices that were matched by the NAC policy. You can specify which VLAN is applied, select which traffic policy is used, and enable or disable packet count.

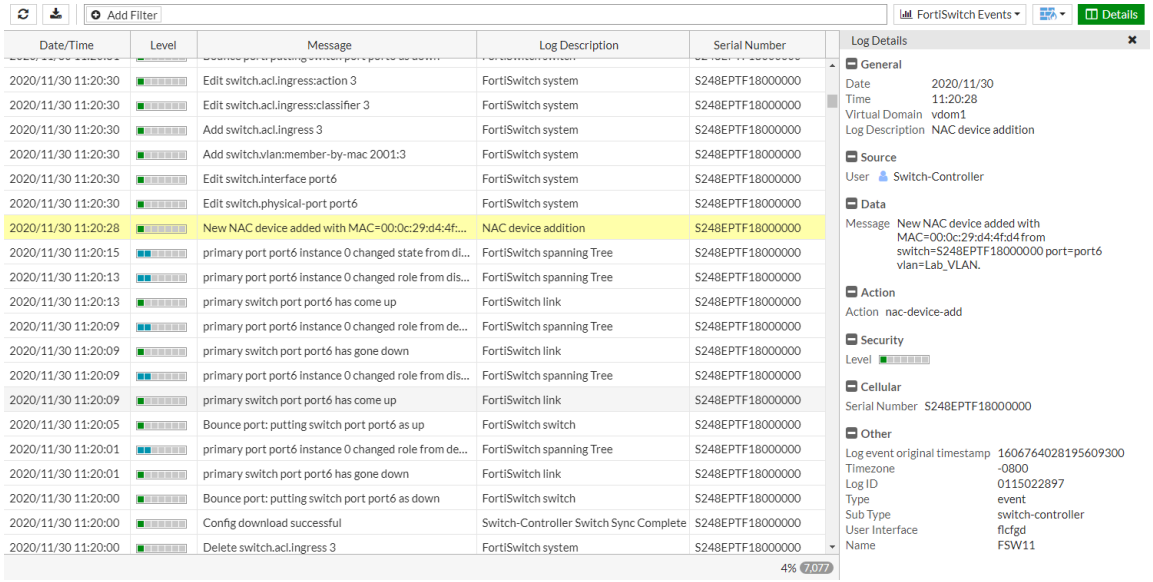
```
config switch-controller mac-policy
   edit <MAC_policy_name>
      set description <policy_description>
      set fortilink <FortiLink_interface>
      set vlan <VLAN_name>
      set traffic-policy <traffic_policy_name>
      set count {enable | disable}
   next
end
```

Viewing the devices that match the NAC policy

Using the GUI:

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

When a NAC device is matched to a NAC policy and assigned to a VLAN, an event log is created.



Using the CLI:

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

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

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

```
diagnose switch-controller mac-device nac onboarding
```

To view the NAC clients:

```
diagnose switch-controller mac-device cache
```

To display the NAC cache of MAC addresses on the FortiSwitch unit:

```
execute switch-controller get-nac-mac-cache
```

Viewing device statistics

Starting in FortiOS 7.2.4 with FortiSwitchOS 7.2.3, you can use the FortiOS CLI to report device statistics when NAC is enabled. The device statistics report the MAC addresses of known devices, the number of packets and bytes received, the number of seconds since the last update, and the age of the MAC counter in seconds.

- Only statistics for receive counters are reported.
- If a device moves to a different FortiSwitch unit, the MAC counters are reallocated.
- If a FortiSwitch unit cannot track both bytes and packets, a zero is displayed for whichever value cannot be tracked. If a FortiSwitch unit cannot track device statistics at all, the entry will be missing from the CLI command output.
- This feature is supported on the following FortiSwitch models: FSR-124D, FSR-224F-FPOE, FS-224D-FPOE, FS-224E, FS-224E-POE, FS-248D, FS-248E-POE, FS-248E-FPOE, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-M426E-FPOE, FS-424E-Fiber, FS-448E, FS-448E-POE, FS-448E-FPOE, FS-524D, FS-524D-FPOE, FS-548D, FS-548D-FPOE, FS-1024D, FS-1024E, FS-T1024E, FS-1048E, and FS-3032E.
- Accuracy is not guaranteed.

To display device statistics:

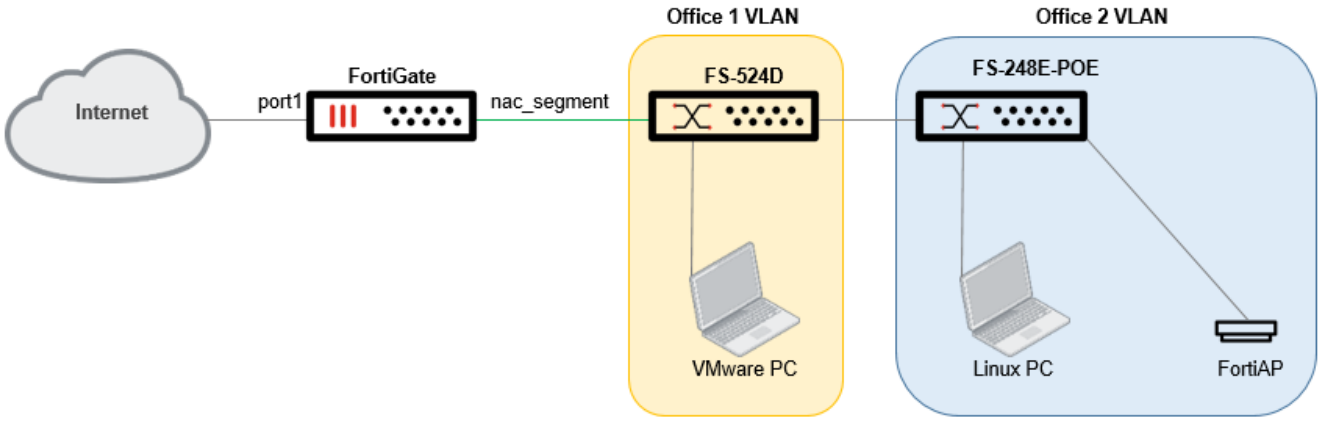
1. Enable NAC.
```
config user nac-policy
   edit <NAC_policy_name>
      set status enable
   next
end
```
2. Enable packet counting in the MAC policy. By default, packet counting is disabled.
```
config switch-controller mac-policy
   edit <MAC_policy_name>
      set count enable
   next
end
```
3. Specify how long inactive MAC addresses are kept before being removed from the client database. By default, MAC addresses are kept for 24 hours. The range of values is 0-168 hours. If you set this option to 0, the value for the `mac-aging-interval` setting is used instead.
```
config switch-controller global
   set mac-retention-period <number_of_hours>
end
```
4. Enter the following command to display the device statistics:
```
diagnose switch-controller telemetry show mac-stats
```

   For example:

```
diagnose switch-controller telemetry show mac-stats

MAC                Packets        Bytes      Last Update (secs ago)  Age
-------------------------------------------------------------------------------
00:00:00:00:00:0f     234562    2356546842           41             23433
00:00:00:00:14:21      44273        456346           68              7477
00:03:7a:a8:82:e7      12346         34545           30            983452
00:04:f2:f3:2b:7f       4357        345345           30             23423
00:04:f2:f6:77:05     463453       4564564          430         362456265
00:04:f2:f6:7a:6a      34535       1312354           30             23423
00:04:f2:f6:7b:66      73821        345345           68            374546
00:05:9a:3c:7a:00         43          9144           68            456725
```

Example of using LAN segments with NAC

In this example, devices are initially placed in the onboarding VLAN and receive IP addresses from the nac_segment DHCP server. Ports connected to the devices are configured with the NAC access mode. NAC policies are used to identify devices by OS and place them into the appropriate VLAN segment and dynamic firewall address. Firewall policies match traffic from the nac_segment interface by the dynamic firewall address and apply the appropriate security profiles to each.



1. Configure the FortiSwitch VLANs for Office 1 and Office 2.

```
config system interface
   edit "Office2"
      set vdom "root"
      set device-identification enable
      set role lan
      set snmp-index 33
      set color 10
      set interface "fortilink"
      set vlanid 2000
   next
   edit "Office1"
      set vdom "root"
      set device-identification enable
      set role lan
      set snmp-index 34
      set color 5
      set interface "fortilink"
      set vlanid 2001
   next
end
```

2. The following is the configuration for the nac_segment interface and its corresponding DHCP server settings. These settings are the default.

```
config system interface
   edit "nac_segment"
   set vdom "root"
   set ip 10.255.13.1 255.255.255.0
   set description "NAC Segment VLAN"
   set alias "nac_segment.fortilink"
```

```
   set device-identification enable
   set snmp-index 32
   set switch-controller-feature nac-segment
   set interface "fortilink"
   set vlanid 4088
   next
end
config system dhcp server
   edit 5
      set lease-time 300
      set dns-service default
      set default-gateway 10.255.13.1
      set netmask 255.255.255.0
      set interface "nac_segment"
      config ip-range
         edit 1
            set start-ip 10.255.13.2
            set end-ip 10.255.13.254
         next
      end
      set timezone-option default
   next
end
```

3. Add the Office 1 VLAN and Office 2 VLAN to the LAN segment VLANs.

```
config switch-controller fortilink-settings
   edit "fortilink"
      config nac-ports
         set onboarding-vlan "onboarding"
         set lan-segment enabled
         set nac-lan-interface "nac_segment"
         set nac-segment-vlans "voice" "video" "Office2" "Office1"
      end
   next
end
```

4. Configure the NAC policy for devices in Office 1 and Office 2.

   If you configure the NAC policy from the GUI, you can create the office2_device and office1_device dynamic firewall addresses inline. However, if you create the NAC policy from the CLI, first create the firewall addresses and then create the MAC policy and NAC policies.

```
config firewall address
   edit "office2_device"
      set type dynamic
      set sub-type swc-tag
      set color 19
   next
   edit "office1_device"
      set type dynamic
      set sub-type swc-tag
      set color 10
   next
end
```

```
config switch-controller mac-policy
   edit "Office2_FAP"
      set fortilink "fortilink"
      set vlan "Office2"
   next
   edit "Office2_PC"
      set fortilink "fortilink"
      set vlan "Office2"
   next
   edit "Office1_PC"
      set fortilink "fortilink"
      set vlan "Office1"
   next
end

config user nac-policy
   edit "OFFICE2_FAP"
      set hw-vendor "Fortinet"
      set family "FortiAP"
      set os "FortiAP OS"
      set switch-fortilink "fortilink"
      set switch-group "Office2switches"
      set switch-mac-policy "Office2_FAP"
      set firewall-address "office2_device"
   next
   edit "OFFICE2_PC"
      set os "Linux"
      set switch-fortilink "fortilink"
      set switch-group "Office2switches"
      set switch-mac-policy "Office2_PC"
      set firewall-address "office2_device"
   next
   edit "OFFICE1_PC"
      set hw-vendor "VMware"
      set switch-fortilink "fortilink"
      set switch-group "Office1switches"
      set switch-mac-policy "Office1_PC"
      set firewall-address "office1_device"
   next
end
```

5. Configure the firewall policy for devices in Office 1 or Office 2.

   The source of all traffic is nac_segment, but the traffic is filtered on the srcaddr by the dynamic firewall address previously assigned by the NAC policies.

```
config firewall policy
   edit 5
      set name "Office1_Device"
      set uuid d3e2bbdc-d9c1-51eb-dbd3-cb534366b58d
      set srcintf "nac_segment"
      set dstintf "port1"
      set action accept
      set srcaddr "office1_device"
      set dstaddr "all"
```

```
      set schedule "always"
      set service "ALL"
      set ssl-ssh-profile "certificate-inspection"
      set logtraffic all
      set nat enable
   next
   edit 4
      set name "Office2_Device"
      set uuid a724c2fc-d9c1-51eb-e8d8-a501419308b3
      set srcintf "nac_segment"
      set dstintf "port1"
      set action accept
      set srcaddr "office2_device"
      set dstaddr "all"
      set schedule "always"
      set service "ALL_ICMP" "FTP" "FTP_GET" "FTP_PUT" "HTTP" "HTTPS" "TFTP"
      set ssl-ssh-profile "certificate-inspection"
      set logtraffic all
      set nat enable
   next
   edit 3
      set name "All_devices"
      set uuid 0accfbae-d9c1-51eb-b0bf-2ba0b00647c0
      set srcintf "nac_segment"
      set dstintf "port1"
      set action accept
      set srcaddr "all"
      set dstaddr "all"
      set schedule "always"
      set service "ALL"
      set utm-status enable
      set ssl-ssh-profile "certificate-inspection"
      set av-profile "default"
      set webfilter-profile "default"
      set dnsfilter-profile "default"
      set ips-sensor "default"
      set application-list "default"
      set logtraffic all
      set nat enable
   next
end
```

6. Place the ports in NAC mode.

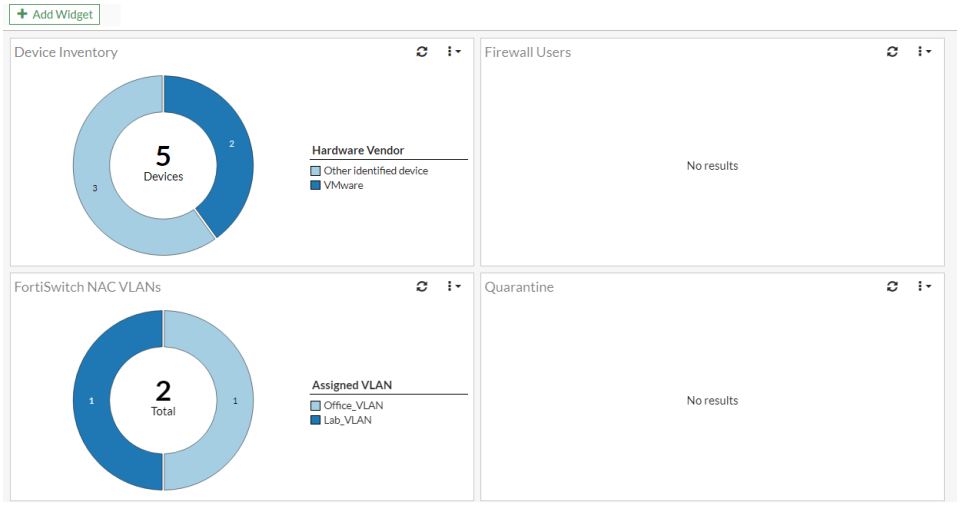
```
config switch-controller managed-switch
   edit "S524DN4K16000116"
      config ports
         edit "port7"
            set vlan "onboarding"
            set allowed-vlans "quarantine" "nac_segment"
            set untagged-vlans "quarantine" "nac_segment"
            set access-mode nac
         next
      end
      next
   edit "S248EPTF18001384"
      config ports
```

```
            edit "port1"
               set vlan "onboarding"
               set allowed-vlans "quarantine" "nac_segment"
               set untagged-vlans "quarantine" "nac_segment"
               set access-mode nac
            next
            edit "port6"
               set vlan "onboarding"
               set allowed-vlans "quarantine" "nac_segment"
               set untagged-vlans "quarantine" "nac_segment"
               set access-mode nac
            next
         end
      next
   end
```

Using the FortiSwitch NAC VLAN widget

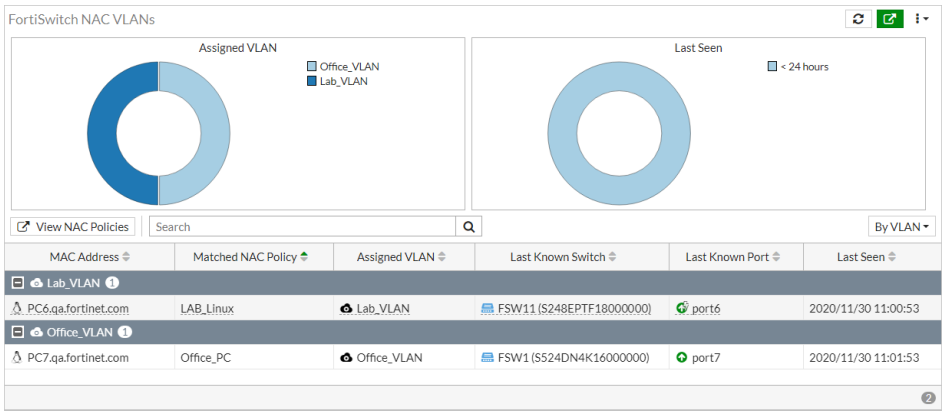
The widget shows a pie chart of the assigned FortiSwitch NAC VLANs. When expanded to the full screen, the widget shows a full list of devices grouped by VLAN, NAC policy, or last seen.

The widget is added to the *Users & Devices* dashboard after a dashboard reset or can be manually added to a dashboard. It can also be accessed by going to *WiFi & Switch Controller* > *NAC Policies* and clicking *View Matched Devices*.



The expanded view of the widget shows Assigned VLAN and Last Seen pie charts and a full device list. The list can be organized *By VLAN*, *By NAC Policy*, or *By Policy Type*.

Click *View NAC Policies* to go to *WiFi & Switch Controller* > *NAC Policies*.



Configuring dynamic port policy rules

Dynamic port policies allow you to specify rules that dynamically determine port policies. After you create the FortiLink policy settings, you define the dynamic port policy rules. When a rule matches the specified device patterns, the switch-controller actions control the port's properties.

NOTE: Visit https://filestore.fortinet.com/product-downloads/fortilink/HTFO_list.json to see a list of values for hardware vendor, type, device family, and operating system.

When you add dynamic port policy rules to the FortiLink policy settings, the rules are processed sequentially, from the first rule to the last rule. The last rule in the FortiLink policy settings should indicate the default properties for any port that has been assigned these FortiLink policy settings.

To identify devices to add to a dynamic port policy rule, try the following:

- Use the `diagnose user device list` command to see devices connected to your FortiGate device.
- Use the FortiGuard Device Detection service (https://www.fortiguard.com/learnmore#dds) to provide information about an IoT device based on its MAC address.

To configure dynamic port policy rules:

1. Set the access mode and port policy for the port on page 146
2. Set the FortiLink policy settings to the FortiLink interface on page 147
3. Create the FortiLink policy settings on page 147
4. Create the dynamic port policy rule on page 148
5. Set how often the dynamic port policy engine runs on page 150

Set the access mode and port policy for the port

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

```
            set access-mode dynamic
            set port-policy <dynamic_port_policy>
          next
        end
      next
   end
```

Set the FortiLink policy settings to the FortiLink interface

Enable the dynamic port policy on the FortiLink interface by specifying the FortilLink policy settings on the FortiLink interface.

```
config system interface
   edit fortilink
      set switch-controller-dynamic <FortiLink_policy_settings>
   next
end
```

Create the FortiLink policy settings

Using the GUI

1. Go to *WiFi & Switch Controller* > *FortiSwitch Port Policies*.
2. Click *Dynamic Port Policies*.
3. Click *Configure Dynamic Port Settings*.
4. Select the onboarding VLAN from the *Onboarding VLAN* dropdown list. The default onboarding VLAN is *onboarding*.
5. Move the *Bounce port* slider to enable it if you want the link to go down and then up when the NAC mode is configured on the port.
6. If you are using the dynamic port policy with FortiSwitch network access control, move the *Apply rule to NAC policies* slider to enable it.
7. Click *Next*.
8. When devices are matched by a dynamic port policy, you can assign those devices to a dynamic port VLAN. By default, there are six VLAN templates:
   - *default*—This VLAN is assigned to all switch ports when the FortiSwitch unit is first discovered.
   - *onboarding*—This VLAN is for NAC onboarding devices.
   - *quarantine*—This VLAN contains quarantined traffic.
   - *rspan*—This VLAN contains RSPAN and ERSPAN mirrored traffic.
   - *video*—This VLAN is dedicated for video devices.
   - *voice*—This VLAN is dedicated for voice devices.

   You can select one of the default VLAN templates, edit one of the default VLAN templates, or create a dynamic port VLAN.
9. Click *Submit*.

Using the CLI

```
config switch-controller fortilink-settings
   edit <name_of_this_FortiLink_configuration>
      set inactive-timer <integer>
      set link-down-flush {enable | disable}
```

```
      config nac-ports
         set onboarding-vlan <string>
         set bounce-nac-port {enable | disable}
      end
   next
end
```

Create the dynamic port policy rule

Using the GUI

1. On the *Dynamic Port Policies* page, select the dynamic port policy that you want to add dynamic port policy rules to.
2. Click *Edit*.
3. Click *Create New*.
4. In the *Name* field, enter a name for the dynamic port policy rule.
5. Make certain that the status is set to *Enabled*.
6. In the *Description* field, enter a description of the dynamic port policy rule.
7. If you want the device to match a MAC address, enable *MAC Address* and enter the MAC address to match.
8. If you want the device to match a host name or IP address, enable *Host* and enter the host name or IP address to match.
9. If you want the device to match a hardware vendor, enable *Hardware vendor* and enter the name of the hardware vendor to match in the *Hardware vendor* field.
   This option is available in FortiOS 7.0.4 and higher.
10. If you want the device to match a device family, enable *Device Family* and enter the name of the device family to match.
11. If you want the device to match a device type, enable *Type* and enter the device type to match.
12. If you want to assign an LLDP profile to the device that matches the specified criteria, enable *LLDP profile* and select the LLDP profile.
13. If you want to assign a QoS policy to the device that matches the specified criteria, enable *QoS policy* and select the QoS policy.
14. If you want to assign an 802.1x policy to the device that matches the specified criteria, enable *802.1X policy* and select the 802.1x policy.
15. If you want to assign a VLAN policy to the device that matches the specified criteria, enable *VLAN policy* and select the VLAN policy.
16. Click *OK*.

Using the CLI

```
config switch-controller dynamic-port-policy
   edit <dynamic_port_policy_name>
      set description <string>
      set fortilink <FortiLink_interface_name>
      config policy
         edit <policy_name>
            set description <string>
            set status {enable | disable}
            set category {device | interface-tag}
            set hw-vendor <hardware_vendor>
            set mac <MAC_address>
            set type <device_type>
            set family <device_family_name>
```

```
            set host <host_name_or_IP_address>
            set lldp-profile <LLDP_profile_name>
            set qos-policy <QoS_policy_name>
            set 802-1x <802.1x_policy_name>
            set vlan-policy <VLAN_policy_name>
            set bounce-port-link {disable | enable}
         next
      end
   next
end
```

For example:

```
config switch-controller dynamic-port-policy
   edit DPP1
      set description "Policy for VMware devices"
      set fortilink "flink"
      config policy
         edit policy1
            set description "Rule applies only to VMware devices"
            set status enable
            set hw-vendor "VMware"
            set lldp-profile "LLDPprofile1"
            set bounce-port-link enable
         next
      end
   next
end
```

Creating a VLAN policy

You can specify a VLAN policy to be used in the port policy. In the VLAN policy, you can specify the native VLAN to be applied, the allowed VLANs, and the untagged VLANs. You can enable or disable all defined VLANs and select whether to discard untagged or tagged frames or to not discard any frames.

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

For example:

```
config switch-controller vlan-policy
   edit vlan_policy_1
      set fortilink fortilink1
      set vlan default
   next
end
```

Set how often the dynamic port policy engine runs

In the FortiOS CLI, you can change how often the dynamic port policy engine runs. By default, it runs every 60 seconds. The range of values is 5-180 seconds.

```
config switch-controller system
   set dynamic-periodic-interval <5-180 seconds>
end
```

FortiSwitch security policies

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

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. If a link goes down, you can select whether the impacted devices must reauthenticate. By default, reauthentication is disabled.

You can configure a guest VLAN for unauthorized users and a VLAN for users whose authentication was unsuccessful. Starting in FortiSwitchOS 6.4.3, if the RADIUS server cannot be reached for 802.1X authentication, you can specify a RADIUS timeout VLAN for users after the authentication server timeout period expires.

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

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

This section covers the following topics:

- RADIUS change of authorization (CoA) support on page 156
- 802.1X authentication deployment example on page 159
- Detailed deployment notes on page 161

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

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

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

Configuring the 802.1X settings 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 link-down-auth {set-unauth | no-action}
   set reauth-period <integer>
   set max-reauth-attempt <integer>
   set tx-period <integer>
   set mab-reauth {enable | disable}
end
```

Option	Description	Default
`link-down-auth {set-unauth | no-action}`	If a link is down, this command determines the authentication state. Choosing `set-unauth` sets the interface to unauthenticated when a link is down, and reauthentication is needed. Choosing `no-action` means that the interface does not need to be reauthenticated when a link is down.	set-unauth

Option	Description	Default
`reauth-period <integer>`	This command sets how often reauthentication is needed. The range is 1-1440 minutes. Setting the value to 0 minutes disables reauthentication. **NOTE:** Setting the `reauth-period` to 0 is supported only in the CLI. The RADIUS dynamic session timeout and CoA session timeout do not support setting the Session Timeout to 0. For MAB authentication, the host entry is automatically reauthenticated after the `reauth-period`. To clear the host entry, you need to clear the entry manually.	60
`max-reauth-attempt <integer>`	This command sets the maximum number of reauthentication attempts. The range is 1-15. Setting the value to 0 disables reauthentication.	3
`tx-period <integer>`	This command sets the 802.1X transmission period in seconds. The range is 4-60.	30
`mab-reauth {enable | disable}`	This command enables or disables MAB reauthentication.	disable

Overriding the 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 FortiSwitches*.
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:

```
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
            set mab-reauth {enable | disable}             // visible if override enabled
        end
    next
end
```

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

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

Using the 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
      set authserver-timeout-vlan {enable | disable}
      set authserver-timeout-period <integer>
      set authserver-timeout-vlanid "<RADIUS-timeout-VLAN-name>"
   end
```

```
end
```

Option	Description
`set security-mode`	You can restrict access with 802.1X port-based authentication or with 802.1X MAC-based authentication.
`set user-group`	You can set a specific group name, Guest-group, or SSO_Guest_Users to have access. This setting is mandatory.
`set mac-auth-bypass`	You can enable or disable MAB on this interface.
`set eap-passthrough`	You can enable or disable EAP pass-through mode on this interface.
`set guest-vlan`	You can enable or disable guest VLANs on this interface to allow restricted access for some users.
`set guest-vlan-id "<guest-VLAN-name>"`	You can specify the name of the guest VLAN.
`set guest-auth-delay`	You can set the authentication delay for guest VLANs on this interface. The range is 1-900 seconds.
`set auth-fail-vlan`	You can enable or disablethe authentication fail VLAN on this interface to allow restricted access for users who fail to access the guest VLAN.
`set auth-fail-vlan-id "<auth-fail-VLAN-name>"`	You can specify the name of the authentication fail VLAN
`set radius-timeout-overwrite`	You can enable or disable whether the session timeout for the RADIUS server will overwrite the local timeout.
`set policy-type 802.1X`	You can set the policy type to the 802.1X security policy.
`set authserver-timeout-vlan`	Enable or disable the RADIUS timeout VLAN on this interface to allow limited access for users when the RADIUS server times out before finishing authentication. By default, this option is disabled.
`set authserver-timeout-period`	You can set how many seconds the RADIUS server has to authenticate users. The range of values is 3-15 seconds; the default time is 3 seconds. This option is only visible when `authserver-timeout-vlan` is enabled.
`set authserver-timeout-vlanid "<RADIUS-timeout-VLAN-name>"`	The VLAN name that is used for users when the RADIUS server times out before finishing authentication. This option is only visible when `authserver-timeout-vlan` is enabled.

Applying an 802.1X security policy to a FortiSwitch port

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

Using the 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
```

Testing 802.1X authentication with monitor mode

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

To enable or disable monitor mode, use the following commands:

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

Clearing authorized sessions

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

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

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

For example:

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

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

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

For example:

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

RADIUS accounting support

The FortiSwitch unit uses 802.1X-authenticated ports to send five types of RADIUS accounting messages to the RADIUS accounting server to support 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.

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

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

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

RADIUS change of authorization (CoA) support

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

Starting in FortiSwitchOS 6.2.1, RADIUS accounting and CoA support EAP and MAB 802.1X authentication.

The FortiSwitch unit supports two types of RADIUS CoA messages:

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

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

RADIUS CoA messages use the following Fortinet proprietary attribute:

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

The format of the value is as follows:

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

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

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

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

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

Configuring CoA and disconnect messages

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

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

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

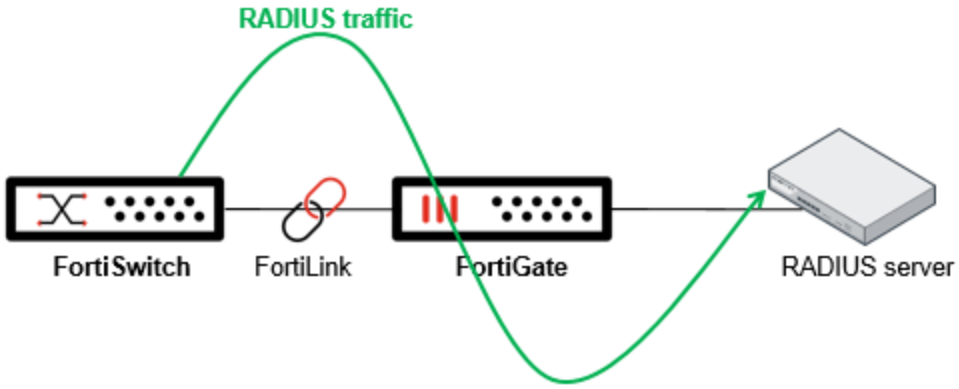
Example: RADIUS CoA

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

```
config switch-controller security-policy local-access
   edit default
      set internal-allowaccess ping https http ssh snmp telnet radius-acct
```

```
   next
end
config user radius
   edit "Radius-188-200"
      set radius-coa enable
      set radius-port 0
      set secret ENC
           +2NyBcp8JF3/OijWl/w5nOC++aDKQPWnlC8Ug2HKwn4RcmhqVYE+q07yI9eSDhtiIw63kR/oMBLGwFQoe
           ZfOQWengIlGTb+YQo/lYJn1V3Nwp9sdkcblfyayfc9gTeqe+mFltKl5IWNI7WRYiJC8sxaF9Iyr2/l4hp
           CiVUMiPOU6fSrj
      set server "10.105.188.200"
   next
end
```

802.1X authentication deployment example



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

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

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

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

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

```
config user radius
   edit "dot1x-radius"
```

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

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

To create an 802.1X security policy:

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

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

To configure the global 802.1X settings:

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

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

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

```
config switch-controller managed-switch
   edit S548DN4K16000360
      config ports
         edit "port1"
            set dhcp-snooping trusted
```

```
        set dhcp-snoop-option82-trust enable
        set port-security-policy "802-1X-policydefault"
    next
end
```

Detailed deployment notes

- Using more than one security group (with the `set security-groups` command) per security profile is not supported.
- CoA and single sign-on are supported only by the CLI in this release.
- RADIUS CoA is supported in standalone mode. In addition, RADIUS CoA is supported in FortiLink mode when NAT is disabled in the firewall policy (`set nat disable` under the `config firewall policy` command), and the interfaces on the link between the FortiGate unit and FortiSwitch unit are assigned routable addresses other than 169.254.1.x.
- The FortiSwitch unit supports using FortiAuthenticator, FortiConnect, Microsoft Network Policy Server (NPS), Aruba ClearPass, and Cisco Identity Services Engine (ISE) as the RADIUS server for CoA and RSSO.
- Each RADIUS CoA server can support only one accounting manager in this release.
- RADIUS accounting/CoA/VLAN-by-name features are supported only with `eap-passthru enable`.
- Fortinet recommends a unique secret key for each accounting server.
- For CoA to correctly function with FortiAuthenticator or FortiConnect, you must include the User-Name attribute (you can optionally include the Framed-IP-Address attribute) *or* the User-Name and Calling-Station-ID attributes in the CoA request.
- To obtain a valid Framed-IP-Address attribute value, you need to manually configure DHCP snooping in the 802.1X-authenticated ports of your VLAN network for both port and MAC modes.
- Port-based basic statistics for RADIUS accounting messages are supported in the Accounting Stop request.
- By default, the accounting server is disabled. You must enable the accounting server with the `set status enable` command.
- The default port for FortiAuthenticator single sign-on is 1813 for the FortiSwitch unit.
- In MAC-based authentication, the maximum number of client MAC addresses is 20. Each model has its own maximum limit.
- Static MAC addresses and sticky MAC addresses are mechanisms for manual/local authorization; 802.1X is a mechanism for protocol-based authorization. Do not mix them.
- Fortinet recommends an 802.1X setup rate of 5 to 10 sessions per second.
- Starting in FortiSwitch 6.2.0, when 802.1X authentication is configured, the EAP pass-through mode (`set eap-passthru`) is enabled by default.
- For information about the RADIUS attributes supported by FortiSwitchOS, refer to the “Supported attributes for RADIUS CoA and RSSO” appendix in the *FortiSwitchOS Administration Guide—Standalone Mode*.
- EAP-MD5 is not supported.

Configuring the DHCP trust setting

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

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

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

For example:

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

Configuring the DHCP server access list

Starting in FortiOS 7.0.1, you can configure which DHCP servers that DHCP snooping includes in the server access list. These servers on the list are allowed to respond to DHCP requests.

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

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

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

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

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

For example:

```
FGT_A (vdom1) # config switch-controller global
FGT_A (global) # set dhcp-server-access-list enable
FGT_A (global) # end
```

To configure the VLAN settings:

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

For example:

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

To configure the interface settings:

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

For example:

```
config system interface
   edit "_default.13"
      set vdom "vdom1"
      set ip 5.4.4.1 255.255.255.0
      set allowaccess ping https ssh http fabric
      set alias "_default.port11"
      set snmp-index 30
      set switch-controller-dhcp-snooping enable
      config dhcp-snooping-server-list
         edit "server1"
            set server-ip 10.20.20.1
```

```
        next
      end
      set switch-controller-feature default-vlan
      set interface "port11"
      set vlanid 1
   next
end
```

Including option-82 data

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

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

```
Circuit-ID: vlan-mod-port
vlan - [ 2 bytes ]
mod - [ (1 Byte) -> Snoop - 1 , Relay - 0 ]
port - [ 1 byte ]
```

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

```
Remote-ID: mac [ 6 byte ]
```

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

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

For example:

```
config system interface
   edit "user"
      set vdom "root"
      set ip 192.168.101.1 255.255.255.0
      set allowaccess ping
      set device-identification enable
      set role lan
      set snmp-index 42
      set switch-controller-dhcp-snooping enable
      set switch-controller-dhcp-snooping-option82 enable
      set interface "fortilink"
      set vlanid 101
   next
end

config system dhcp server
   edit 7
      set dns-service default
      set default-gateway 192.168.101.1
      set netmask 255.255.255.0
      set interface "user"
      config ip-range
         edit 1
            set start-ip 192.168.101.2
            set end-ip 192.168.101.254
         next
```

```
      end
      config reserved-address
         edit 1
            set type option82
            set ip 192.168.101.201
            set circuit-id "706F7274312C3130312C646863702D73"
            set remote-id "39303a36433a41433a35463a30413a4142"
         next
         edit 2
            set type option82
            set ip 192.168.101.202
            set circuit-id "706F7274322C3130312C646863702D73"
            set remote-id "39303a36433a41433a35463a30413a4142"
         next
      end
   next
end
```

Configuring dynamic ARP inspection (DAI)

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

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

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

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

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

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

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

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

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

Configuring DHCP-snooping static entries

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

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

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

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

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

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

To create a static entry for DHCP snooping and DAI:

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

For example:

```
config switch-controller managed-switch
   edit S524DN4K16000116
      config dhcp-snooping-static-client
         edit DHCPclient
            set vlan 100
```

```
            set ip 192.168.101.1
            set mac 00:21:cc:d2:76:72
            set port port19
        next
    next
end
```

Configuring IPv4 source guard

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

IPv4 source guard allows traffic from the following sources:

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

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

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

IPv4 source guard can be configured in FortiOS only for managed FortiSwitch units that support IP source guard. The following FortiSwitch models support IP source guard:

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

Configuring IPv4 source guard consists of the following steps:

1. Enabling IPv4 source guard on page 167
2. Creating static entries on page 168
3. Checking the IPv4 source-guard entries on page 169

Enabling IPv4 source guard

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

To enable IPv4 source guard:

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

```
      edit <port_name>
         set ip-source-guard enable
      next
   end
end
```

For example:

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

Creating static entries

After you enable IPv4 source guard in the FortiOS CLI, you can create static entries in the FortiOS CLI by binding IPv4 addresses with MAC addresses. For IPv4 source-guard dynamic entries, you need to configure DHCP snooping. See Configuring DHCP blocking, STP, and loop guard on managed FortiSwitch ports on page 96.

To create static entries:

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

For example:

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

Checking the IPv4 source-guard entries

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

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

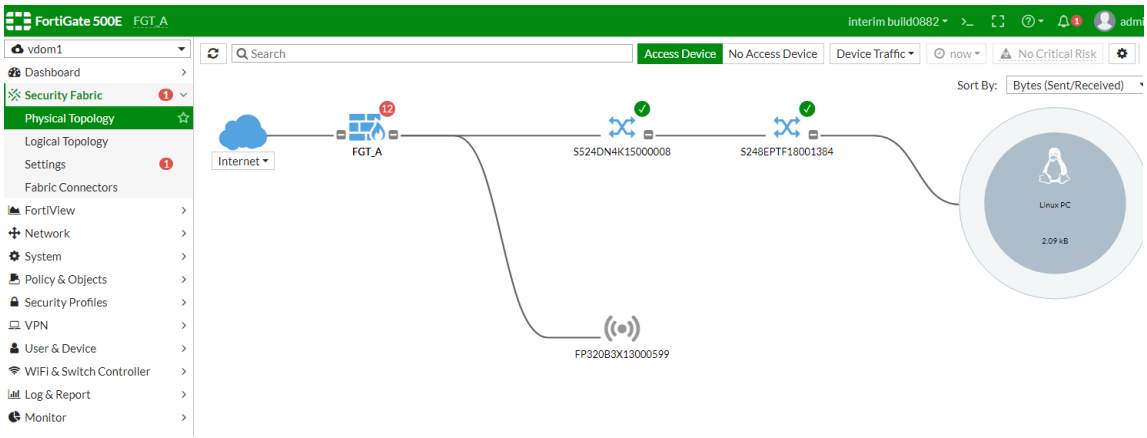
Use this command in the FortiOS CLI to display all IP source-guard entries:

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

Security Fabric showing

This example shows one of the key components in the concept of Security Fabric: FortiSwitches in FortiLink. In the FortiGate GUI, you can see the whole picture of the Security Fabric working for your network security.

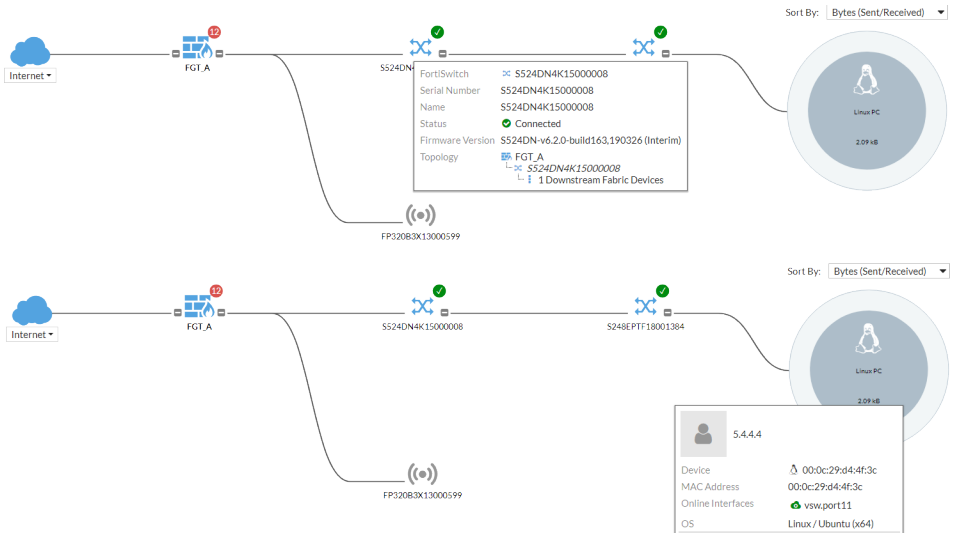
Sample topology



To show Security Fabric information:

1. Go to *Security Fabric* > *Physical Topology*.
2. To see the connection between FortiGates and managed FortiSwitches, hover the pointer over the icons to see

information about each network element.



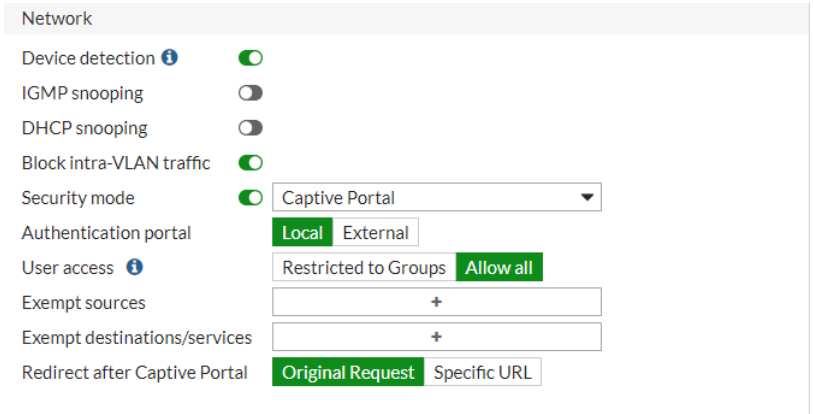
Blocking intra-VLAN traffic

You can block intra-VLAN traffic by aggregating traffic using solely 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 unit, 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, if allowed by a firewall policy and proxy ARP is enabled.

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.

Using the FortiGate GUI

1. Go to *Network* > *Interfaces*.
2. Select the interface and then select *Edit*.
3. In the *Edit Interface* form, enable *Block intra-VLAN traffic* under *Network*.



Using the FortiGate CLI

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

NOTE:

- IPv6 is not supported between clients when intra-VLAN traffic blocking is enabled.
- Intra-VLAN traffic blocking is not supported when the FortiLink interface type is hardware switch or software switch.
- When intra-VLAN traffic blocking is enabled, to allow traffic between hosts, you need to configure the proxy ARP with the `config system proxy-arp` CLI command and configure a firewall policy. 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

config firewall policy
   edit 4
      set name "Allow intra-VLAN traffic"
      set srcintf "V100"
      set dstintf "V100"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set service "ALL"
   next
end
```

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.

This section covers the following topics:

Quarantining MAC addresses

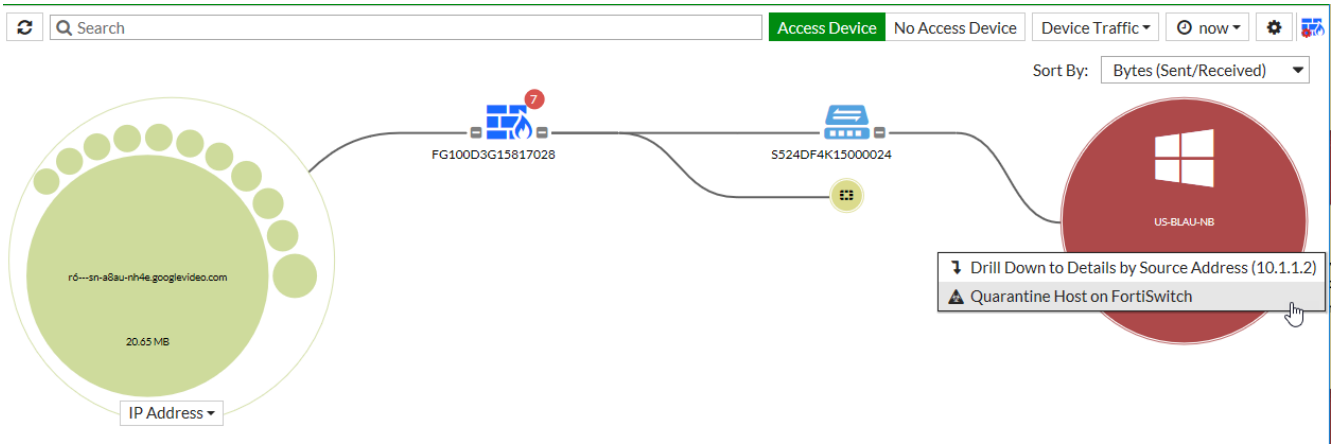
You can use the FortiGate GUI or CLI to quarantine a MAC address.

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

Using the FortiGate GUI

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

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



Using the FortiGate CLI

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

There are two kinds of quarantines:

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

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

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

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

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

Starting in FortiOS 6.4.1, quarantine-by-VLAN is the default. If you have a quarantine-by-VLAN configuration and want to migrate to a quarantine-by-redirect configuration:

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

To set up a quarantine in FortiOS:

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

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

Option	Description
quarantine-mode {by-vlan | by-redirect}	Select the quarantine mode: • `by-vlan` sends quarantined device traffic to the FortiGate unit on a separate quarantine VLAN.This mode is the default. • `by-redirect` redirects quarantined device traffic to a firewall address group on the FortiGate unit.
traffic-policy <traffic_policy_name>	Optional. A name for the traffic policy that controls quarantined devices. If you do add a traffic policy, you need to configure it with the `config switch-controller traffic-policy` command.

Option	Description
firewall-groups <firewall_address_group>	Optional. By default, the firewall address group is `QuarantinedDevices`. If you are using quarantine-by-redirect, you must use the default firewall address group.
quarantine_entry_name	A name for this quarantine entry.
description <string>	Optional. A description of the MAC addresses being quarantined.
MAC_address_1, MAC_address_2, MAC_address_3	A layer-2 MAC address in the following format: `12:34:56:aa:bb:cc`
drop {enable | disable}	Enable to drop quarantined device traffic. Disable to send quarantined device traffic to the FortiGate unit.

For example:

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

config user quarantine
   set quarantine enable
   set traffic-policy qtrafficp
   set firewall-groups QuarantinedDevices
   config targets
      edit quarantine1
      config macs
         set description "infected by virus"
         edit 00:00:00:aa:bb:cc
            set drop disable
         next
         edit 00:11:22:33:44:55
            set drop disable
         next
         edit 00:01:02:03:04:05
            set drop disable
         next
      end
   next
end
```

To configure a traffic policy for quarantined devices in FortiOS:

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

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

For example:

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

Using quarantine with DHCP

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

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

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

Using quarantine with 802.1x MAC-based authentication

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

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

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

```
S448DF3X16000118 # config switch global

S448DF3X16000118 (global) # config port-security

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

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

```
S448DF3X16000118 (port17) # show switch interface port17
config switch interface
   edit "port17"
      set allowed-vlans 4093
      set untagged-vlans 4093
         set security-groups "group1"
      set snmp-index 17
         config port-security
            set auth-fail-vlan disable
            set eap-passthru enable
            set framevid-apply enable
            set guest-auth-delay 30
            set guest-vlan disable
            set mac-auth-bypass enable
            set open-auth disable
            set port-security-mode 802.1X-mac-based
            set quarantine-vlan enable
            set radius-timeout-overwrite disable
            set auth-fail-vlanid 200
            set guest-vlanid 100
         end
      next
   end
```

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

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

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

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

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

```
S448DF3X16000118 # diagnose switch 8 status port17

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

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

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

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

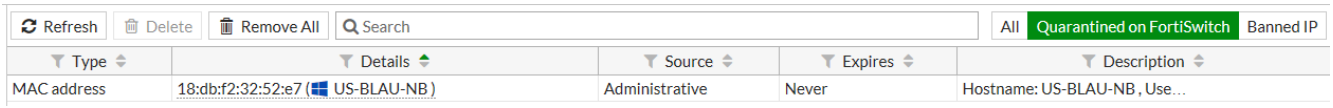
```
S448DF3X16000118 # diagnose switch vlan assignment mac list
00:05:65:ad:15:03 VLAN: 4093 Installed: yes
Source: 802.1X-MAC-Radius
Description: port17

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

Viewing quarantine entries

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

Using the FortiGate GUI

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



Using the FortiGate CLI

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

```
show user quarantine
```

For example:

```
show user quarantine

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

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

Use the following command to view the quarantine VLAN:

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

For example:

```
show system interface qtn.port7

config system interface
   edit "qtn.port7"
      set vdom "vdom1"
      set ip 10.254.254.254 255.255.255.0
      set description "Quarantine VLAN"
      set security-mode captive-portal
      set replacemsg-override-group "auth-intf-qtn.port7"
```

```
      set device-identification enable
      set device-identification-active-scan enable
      set snmp-index 34
      set switch-controller-access-vlan enable
      set color 6
      set interface "port7"
      set vlanid 4093
   next
end
```

Use the following commands to view the quarantine DHCP server:

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

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

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

For example:

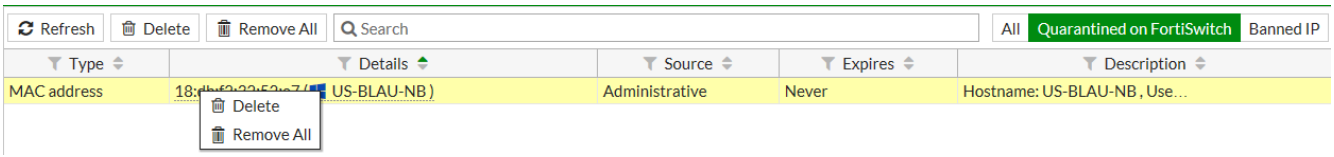
```
show switch-controller managed-switch

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

```
            set allowed-vlans "qtn.port7"
            set untagged-vlans "qtn.port7"
        next
        ...
    end
end
```

Releasing MAC addresses from quarantine

Using the FortiGate GUI

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



Using the FortiGate CLI

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

To delete a single quarantined MAC address:

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

To delete all MAC addresses in a quarantine entry:

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

To disable the quarantine feature:

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

```
end
```

Optimizing the FortiSwitch network

Starting in FortiOS 6.4.2 with FortiSwitchOS 6.4.2, you can check your FortiSwitch network and get recommendations on how to optimize it. If you agree with the configuration recommendations, you can accept them, and they are automatically applied.

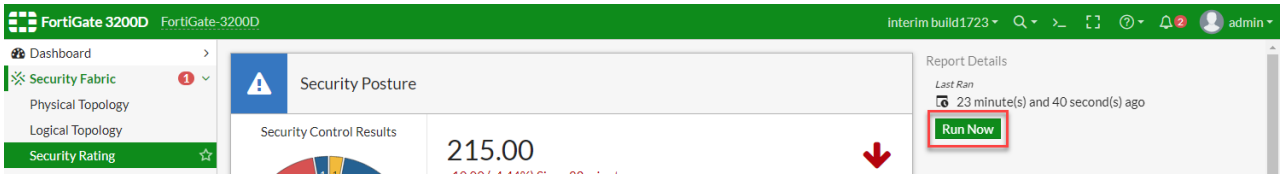
In FortiOS 7.2.4 with FortiSwitchOS 7.2.3, more tests have been added to the FortiSwitch recommendations to help optimize your network:

- If the `poe-status` has been enabled under the `config switch-controller auto-config policy` command, FortiOS recommends that you disable it to prevent unpredictable problems caused by connecting two power sourcing equipment (PSE) ports.
- If port 8 of an FS-108E or FS-108 unit is used for an inter-switch link (ISL), FortiOS recommends creating a custom auto-config policy.
- If the configured speed is less than the maximum speed for a switch port, FortiOS recommends changing the port speed to the maximum amount.
- Check if the inter-switch links (ISLs) and inter-chassis links (ICLs) are static to increase stability during events such as cable disconnections or power outages.
- When a multichassis LAG (MCLAG) is recommended between two FortiSwitch units, there is a *Create MCLAG button* available under *WiFi & Switch Controller* > *Managed FortiSwitches* in the *Topology* view.

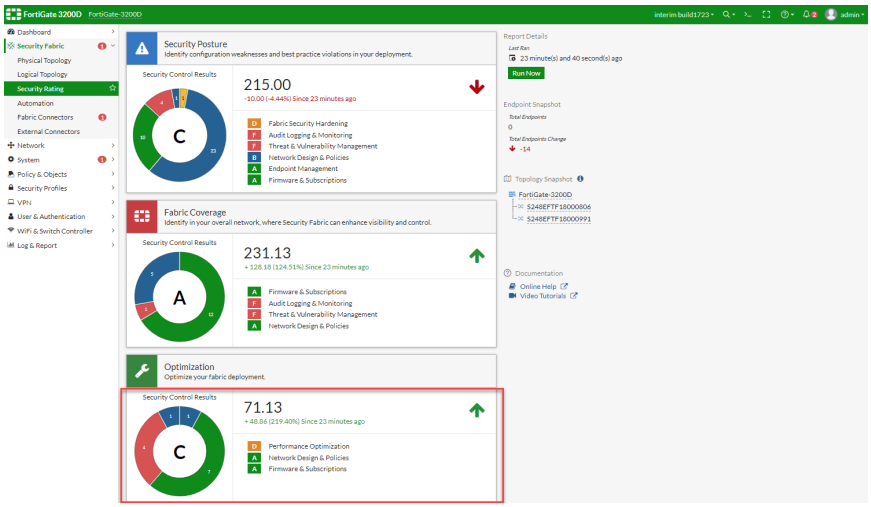
NOTE: The Security Rating feature is available only when VDOMs are disabled.

To optimize your FortiSwitch network:

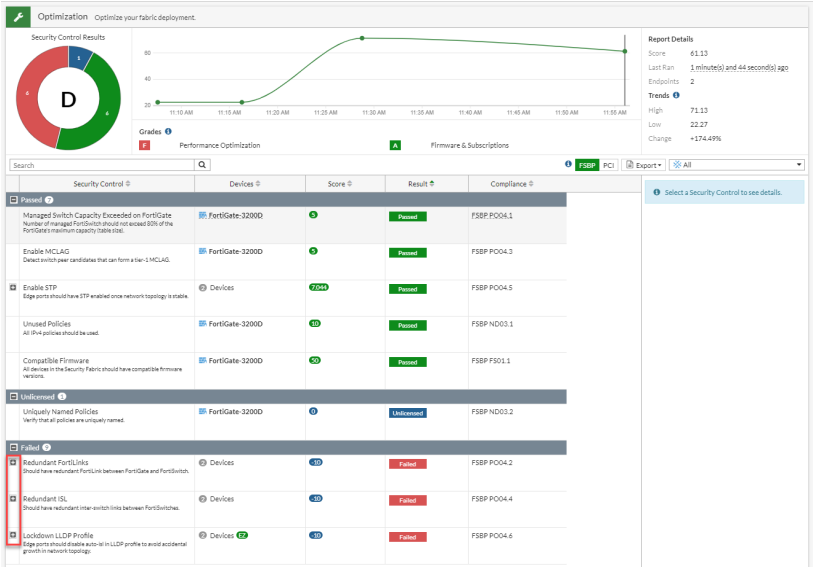
1. Go to *Security Fabric* > *Security Rating*.
2. Select *Run Now* (under *Report Details* in the right pane) to generate the Security Rating report.



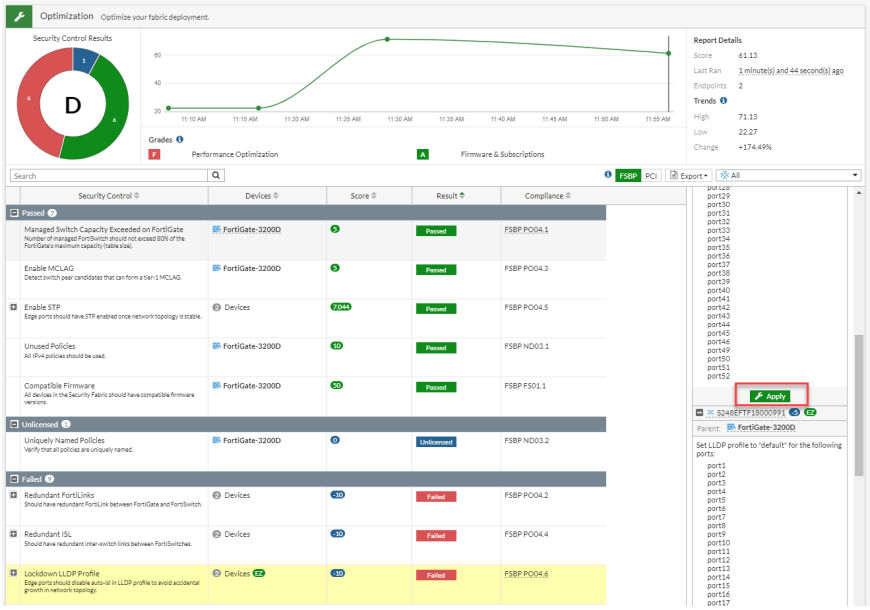
3. Select the *Optimization* section.



4. Under *Failed*, select + next to each item to see more details in the right pane.



5. If you agree with a suggestion in the *Recommendations* section, select *Apply* for the change to be made.


Optimization
Optimize your fabric deployment.
Security Control Results
D
Report Details
Score 61.13
Last Ran 1 minute(s) and 44 second(s) ago
Endpoints 2
Trends
High 71.13
Low 22.27
Change +174.49%
Grades
F Performance Optimization
A Firmware & Subscriptions
Search
FSBP
PCI
Export
All
Security Control
Devices
Score
Result
Compliance
Passed
Managed Switch Capacity Exceeded on FortiGate
Number of managed FortiSwitch should not exceed 80% of the FortiGate's maximum capacity (table size).
FortiGate-3200D
5
Passed
FSBP.PO04.1
Enable MCLAG
Detect switch peer candidates that can form a tier-1 MCLAG.
FortiGate-3200D
5
Passed
FSBP.PO04.3
Enable STP
Edge ports should have STP enabled once network topology is stable.
Devices
7044
Passed
FSBP.PO04.5
Unused Policies
All IPv4 policies should be used.
FortiGate-3200D
10
Passed
FSBP.ND03.1
Compatible Firmware
All devices in the Security Fabric should have compatible firmware versions.
FortiGate-3200D
20
Passed
FSBP.FS01.1
Unlicensed
Uniquely Named Policies
Verify that all policies are uniquely named.
FortiGate-3200D
0
Unlicensed
FSBP.ND03.2
Failed
Redundant FortiLinks
Should have redundant FortiLink between FortiGate and FortiSwitch.
Devices
-10
Failed
FSBP.PO04.2
Redundant ISL
Should have redundant inter-switch links between FortiSwitches.
Devices
-10
Failed
FSBP.PO04.4
Lockdown LLDP Profile
Edge ports should disable auto-isl in LLDP profile to avoid accidental growth in network topology.
Devices 2
-10
Failed
FSBP.PO04.6
Apply
S248EFTF18000991
Parent: FortiGate-3200D
Set LLDP profile to "default" for the following ports:

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.
- If you select `weighted-random-early-detection` for the `drop-policy`, you can enable explicit congestion notification (ECN) marking to indicate that congestion is occurring without just dropping packets.

To configure the QoS for managed FortiSwitch units:

1. Configure a Dot1p map.

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

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

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

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

- priority—Priority
- routine—Routine

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

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

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

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

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

5. Configure each switch port.

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

6. Check the QoS statistics on each switch port.

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

Configuring ECN for managed FortiSwitch devices

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

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

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

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

Logging and monitoring

This section covers the following topics:

FortiSwitch log settings

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

This section covers the following topics:

Exporting logs to FortiGate

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

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

Use the following CLI command syntax:

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

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

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

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

Sending logs to a remote Syslog server

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

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

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

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

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

Configuring FortiSwitch port mirroring

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

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

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

NOTE: RSPAN is supported on FSR-112D-POE, FSR-124D, and on platforms 2xx and higher.

In ERSPAN mode, traffic is encapsulated in Ethernet, IPv4, and generic routing encapsulation (GRE) headers. By focusing on traffic to and from specified ports and traffic to a specified MAC or IP address, ERSPAN reduces the amount of traffic being mirrored. The ERSPAN traffic is sent to a specified IP address, which must be reachable by IPv4 ICMP ping. If no IP address is specified, the traffic is not mirrored.

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

To configure FortiSwitch port-based mirroring:

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

For example:

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

To configure FortiSwitch RSPAN:

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

```
   end
```

For example:

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

To configure FortiSwitch ERSPAN:

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

For example:

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

```
        set in-ports port5 port6 port7
        set out-ports port10
    end
  end
```

To disable FortiSwitch port mirroring:

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

Configuring SNMP

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

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

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

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

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

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

This section covers the following topics:

Configuring SNMP globally

To configure SNMP globally:

1. Configure a firewall policy on the FortiGate device managing the FortiSwitch unit to allow the SNMP server to use the FortiLink interface for SNMP polling.
   For SNMP traps on the managed FortiSwitch unit, you need to configure a firewall policy to allow the managed FortiSwitch unit to communicate with the SNMP server through the FortiLink interface.

2. Add SNMP access on the managed FortiSwitch unit.
   Add SNMP access to the `internal-allowaccess` setting. If you are using FortiLink mode over a layer-3 network with out-of-band management, add SNMP access to the `mgmt-allowaccess` setting.
3. Configure the SNMP system information.
4. Configure the SNMP community.
5. Configure the SNMP trap threshold values.
6. Configure the SNMP user.

To configure a firewall policy for SNMP polling:

```
config firewall policy
   edit <policy_ID>
      set name <policy_name>
      set srcintf <FortiGate port that communicates with the SNMP server>
      set dstintf <FortiLink port that communicates with the managed FortiSwitch unit>
      set action accept
      set srcaddr "all"
      set dstaddr "all"
      set schedule "always"
      set service {"SNMP" | <port_used_for_SNMP_polling>}
      set ssl-ssh-profile "certificate-inspection"
      set logtraffic all
   next
end
```

To add SNMP access on the managed FortiSwitch unit:

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

To configure the SNMP system information globally:

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

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

To configure the SNMP community globally:

```
config switch-controller snmp-community
   edit <SNMP_community_entry_identifier>
      set name <SNMP_community_name>
      set status enable
      set query-v1-status enable
```

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

To configure the SNMP trap threshold values globally:

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

To configure the SNMP user globally:

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

Configuring SNMP locally

To configure SNMP for a specific FortiSwitch unit:

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

Starting in FortiSwitchOS 7.0.0, you can set up one or more SNMP v3 notifications (traps) in the CLI. The following notifications are supported:

- The CPU usage is too high.
- The configuration of an entity was changed.
- The IP address for an interface was changed.

- The available log space is low.
- The available memory is low.

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

To configure the SNMP system information locally:

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

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

To configure the SNMP community locally:

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

To configure the SNMP trap threshold values locally:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set override-snmp-trap-threshold enable
```

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

To configure the SNMP user locally:

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

SNMP OIDs

Three SNMP OIDs have been added to the FortiOS enterprise MIB 2 tables in FortiOS 7.0.1. They report the FortiSwitch port status and FortiSwitch CPU and memory statistics.

SNMP OID	Description
fgSwDeviceInfo.fgSwDeviceTable.fgSwDeviceEntry.fgSwDeviceEntry.fgSwCpu 1.3.6.1.4.1.12356.101.24.1.1.1.11	Percentage of the CPU being used.
fgSwDeviceInfo.fgSwDeviceTable.fgSwDeviceEntry.fgSwDeviceEntry.fgSwMemory 1.3.6.1.4.1.12356.101.24.1.1.1.12	Percentage of memory being used.
fgSwPortInfo.fgSwPortTable.fgSwPortEntry.fgSwPortStatus 1.3.6.1.4.1.12356.101.24.2.1.1.6	Whether a managed FortiSwitch port is up or down.

These OIDs require FortiSwitchOS 7.0.0 or higher. FortiLink and SNMP must be configured on the FortiGate device.

FortiSwitch units update the CPU and memory statistics every 30 seconds. This interval cannot be changed.

FortiOS versions 6.4.2 through 7.0.0 show the port status in the configuration management database (CMDB) for managed ports; FortiOS 7.0.1 and higher show the link status that has been retrieved from the switch port as the port status for managed ports.

Sample queries

To find out how much CPU is being used on a FortiSwitch 1024D with the serial number FS1D243Z17000032:

```
root@PC05:~# snmpwalk -v2c -Cc -c REGR-SYS 172.16.200.1
     1.3.6.1.4.1.12356.101.24.1.1.1.11.2.8.17000032
```

To find out how much memory is being used on a FortiSwitch 1024D with the serial number FS1D243Z17000032:

```
root@PC05:~# snmpwalk -v2c -Cc -c REGR-SYS 172.16.200.1
     1.3.6.1.4.1.12356.101.24.1.1.1.12.2.8.17000032
```

To find out the status of port1 of a FortiSwitch 1024D with the serial number FS1D243Z17000032:

```
root@PC05:~# snmpwalk -v2c -Cc -c REGR-SYS 172.16.200.1
     1.3.6.1.4.1.12356.101.24.2.1.1.6.2.8.17000032.1
```

Configuring sFlow

sFlow is a method of monitoring the traffic on your network to identify areas on the network that might impact performance and throughput. With sFlow, you can export truncated packets and interface counters. FortiSwitch implements sFlow version 5 and supports trunks and VLANs.

NOTE: Because sFlow is CPU intensive, Fortinet does not recommend high rates of sampling for long periods.

sFlow uses packet sampling to monitor network traffic. The sFlow agent captures packet information at defined intervals and sends them to an sFlow collector for analysis, providing real-time data analysis. To minimize the impact on network throughput, the information sent is only a sampling of the data.

The sFlow collector is a central server running software that analyzes and reports on network traffic. The sampled packets and counter information, referred to as flow samples and counter samples, respectively, are sent as sFlow datagrams to a collector. Upon receiving the datagrams, the sFlow collector provides real-time analysis and graphing to indicate the source of potential traffic issues. sFlow collector software is available from a number of third-party software vendors. You must configure a 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
   edit <FortiSwitch_serial_number>
      config ports
```

```
        edit <port_name>
           set sflow-sampler {disabled | enabled}
           set sflow-sample-rate <0-99999>
           set sflow-counter-interval <1-255>
        next
     next
  end
```

For example:

```
config switch-controller sflow
   collector-ip 1.2.3.4
   collector-port 10
end

config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port5
            set sflow-sampler enabled
            set sflow-sample-rate 10
            set sflow-counter-interval 60
         next
      next
   end
```

Configuring flow tracking and export

You can sample IP packets on managed FortiSwitch units and then export the data in NetFlow format or Internet Protocol Flow Information Export (IPFIX) format. You can choose to sample on a single ingress or egress port, on all FortiSwitch units, or on all FortiSwitch ingress ports.

When a new FortiSwitch unit or trunk port is added, the flow-tracking configuration is updated automatically based on the specified sampling mode. When a FortiSwitch port becomes part of an ISL or ICL or is removed, the flow-tracking configuration is updated automatically based on the specified sampling mode.

The maximum number of concurrent flows is defined by the FortiSwitch model. When this limit is exceeded, the oldest flow expires and is exported.

Starting in FortiOS 7.2.0, you can configure multiple flow-export collectors using the `config collectors` command. For each collector, you can specify the collector IP address, the collector port number, and the collector layer-4 transport protocol for exporting packets.

Using multiple flow-export collectors requires FortiSwitchOS 7.0.0 or later. If you are using an earlier version of FortiSwitchOS, only the first flow-export collector is supported.

Starting in FortiOS 7.2.0 with FortiSwitchOS 7.2.0, you can specify how often a template packet is sent using the `set template-export-period` command. By default, a template packet is sent every 5 minutes. The range of values is 1-60 minutes.

Starting in FortiOS 7.2.4 with FortiSwitchOS 7.2.3, you can use the *FortiView Internal Hubs* monitor in FortiOS to report the IP addresses and the number of bytes collected from devices behind a FortiSwitch unit. If you drill down on one of the devices, you can see a chart displaying the devices and how they are connected.

To use the *FortiView Internal Hubs* monitor:

- The IP address for the flow collector (`collector-ip`) must be the same IP address as the FortiLink interface.
- The FortiGate model must have a hard drive, and you must enable historical FortiView and disk logging in the *Log & Report* > *Log Settings* page.
- FortiAnalyzer is not supported.

To enable the *FortiView Internal Hubs* monitor on a managed FortiSwitch unit:

```
config system interface
   edit <FortiLink_interface>
      set ip <IP_address_and_netmask>
      set switch-controller-netflow-collect enable
   next
end
```

To configure flow tracking on managed FortiSwitch units:

```
config switch-controller flow-tracking
   set sample-mode {local | perimeter | device-ingress}
   set sample-rate <0-99999>
   set format {netflow1 | netflow5 | netflow9 | ipfix}
   set level {vlan | ip | port | proto}
   set max-export-pkt-size <512-9216 bytes; default is 512>
   set template-export-period <1-60 minutes, default is 5>
   set timeout-general <60-604800 seconds; default is 3600>
   set timeout-icmp <60-604800 seconds; default is 300>
   set timeout-max <60-604800 seconds; default is 604800>
   set timeout-tcp <60-604800 seconds; default is 3600>
   set timeout-tcp-fin <60-604800 seconds; default is 300>
   set timeout-tcp-rst <60-604800 seconds; default is 120>
   set timeout-udp <60-604800 seconds; default is 300>
   config collectors
      edit <collector_name>
         set ip <IPv4_address>
         set port <0-65535>
         set transport {udp | tcp | sctp}
      end
   config aggregates
      edit <aggregate_ID>
         set <IPv4_address>
      end
end
```

For example:

```
config switch-controller flow-tracking
   config collectors
      edit "Analyzer_1"
         set ip 172.16.201.55
```

```
        set port 4739
        set transport sctp
      next
      edit "Collector_HQ"
        set ip 172.16.116.82
        set port 2055
      next
   end
   set template-export-period 10
end
```

Configure the sampling mode

You can set the sampling mode to local, perimeter, or device-ingress.

- The local mode samples packets on a specific FortiSwitch port.
- The perimeter mode samples packets on all FortiSwitch ports that receive data traffic, except for ISL and ICL ports. For perimeter mode, you can also configure the sampling rate.
- The device-ingress mode samples packets on all FortiSwitch ports that receive data traffic for hop-by-hop tracking. For device-ingress mode, you can also configure the sampling rate.

Configure the sampling rate

For perimeter or device-ingress sampling, you can set the sampling rate, which samples 1 out of the specified number of packets. The default sampling rate is 1 out of 512 packets.

Configure the flow-tracking protocol

You can set the format of exported flow data as NetFlow version 1, NetFlow version 5, NetFlow version 9, or IPFIX sampling.

Configure collector IP address

The default is `0.0.0.0`. Setting the value to “0.0.0.0” or “” disables this feature. The format is xxx.xxx.xxx.xxx.

Configure the transport protocol

You can set exported packets to use UDP, TCP, or SCTP for transport.

Configure the flow-tracking level

You can set the flow-tracking level to one of the following:

- `vlan`—The FortiSwitch unit collects source IP address, destination IP address, source port, destination port, protocol, Type of Service, and VLAN from the sample packet.
- `ip`—The FortiSwitch unit collects source IP address and destination IP address from the sample packet.
- `port`—The FortiSwitch unit collects source IP address, destination IP address, source port, destination port, and protocol from the sample packet.
- `proto`—The FortiSwitch unit collects source IP address, destination IP address, and protocol from the sample packet.

Configure the maximum exported packet size

You can set the maximum size of exported packets in the application level.

To remove flow reports from a managed FortiSwitch unit:

```
execute switch-controller switch-action flow-tracking {delete-flows-all | expire-flows-all}
     <FortiSwitch_serial_number>
```

Expired flows are exported.

To view flow statistics for a managed FortiSwitch unit:

```
diagnose switch-controller switch-info flow-tracking statistics <FortiSwitch_serial_number>
```

To view raw flow records for a managed FortiSwitch unit:

```
diagnose switch-controller switch-info flow-tracking flows-raw <FortiSwitch_serial_number>
```

To view flow record data for a managed FortiSwitch unit:

```
diagnose switch-controller switch-info flow-tracking flows {number_of_records | all} {IP_
     address | all} <FortiSwitch_serial_number> <FortiSwitch_port_name>
```

For example:

```
diagnose switch-controller switch-info flow-tracking flows 100 all S524DF4K15000024 port6
```

To check the status of the flow collector on a managed FortiSwitch unit:

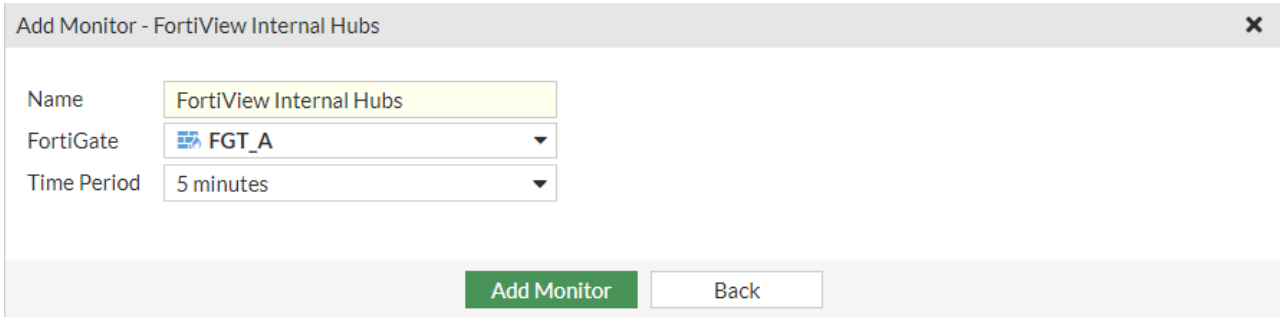
```
diagnose switch-controller flow-collector status
```

For example:

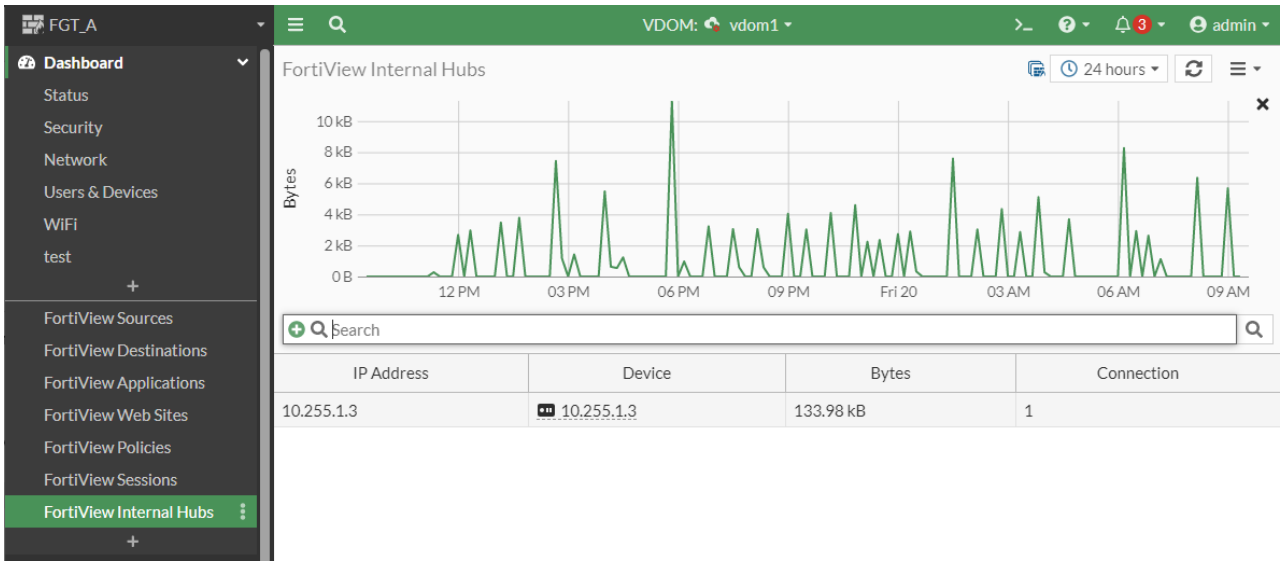
```
FGT_A (vdom1) # diagnose switch-controller flow-collector status
status : enabled
interface : port11
netflow packets : 1300
unknown packets : 0
flows : 42
flows filtered : 201
flowsets skipped : 17129
```

To add the *FortiView Internal Hubs* monitor:

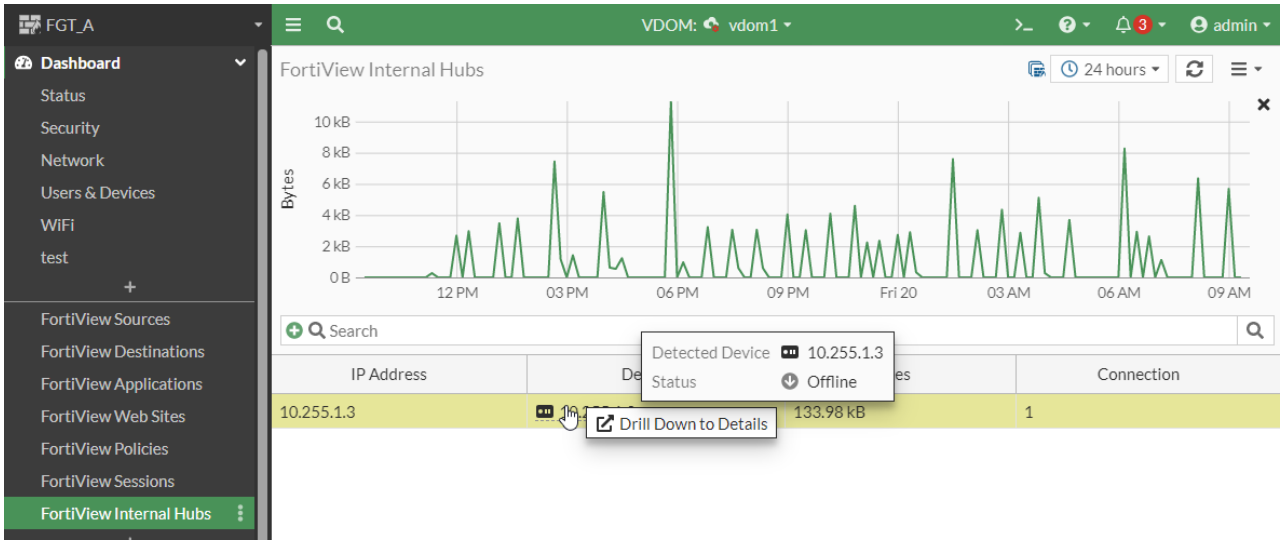
1. Under *Dashboard* and click + to add a monitor.
2. In the *Add Monitor* pane, click the + by *FortiView Internal Hubs*.
3. From the *FortiGate* dropdown list, select which FortiGate device to monitor.
4. From the *Time Period* dropdown list, select how long to monitor (5 minutes, 1 hour, or 24 hours).



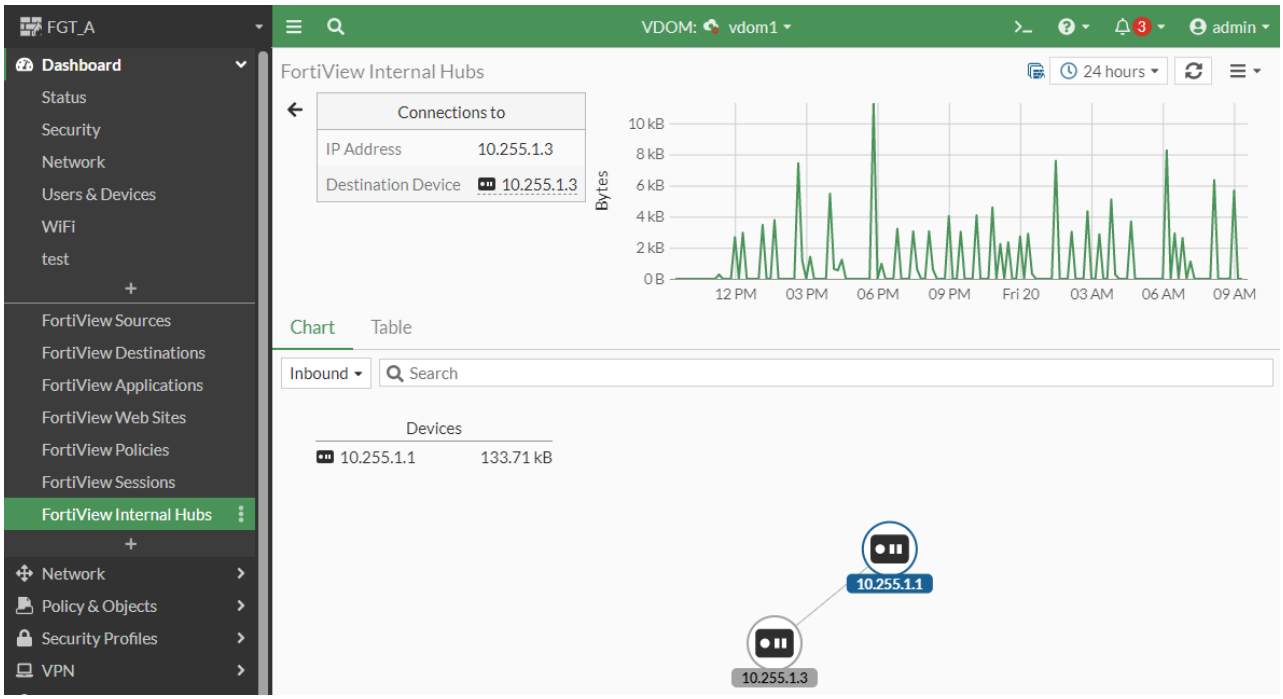
5. Click *Add Monitor*.
6. Under *Dashboard*, select *FortiView Internal Hubs* to display the *FortiView Internal Hubs* page.



7. Right-click on one of the devices and select *Drill Down to Details*.



8. You can select the *Chart* or *Table* tab to change how the details are displayed.



Configuring flow control and ingress pause metering

Flow control allows you to configure a port to send or receive a “pause frame” (that is, a special packet that signals a source to stop sending flows for a specific time interval because the buffer is full). By default, flow control is disabled on all ports.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set flow-control {both | rx | tx | disable}
         next
      end
   end
```

Parameters enable flow control to do the following:

- `rx`—receive pause control frames
- `tx`—transmit pause control frames
- `both`—transmit and receive pause control frames

If you enable flow control to transmit pause control frames or to transmit and receive pause control frames, you can also use ingress pause metering to limit the input bandwidth of an ingress port. Because ingress pause metering stops the traffic temporarily instead of dropping it, ingress pause metering can provide better performance than policing when the port is connected to a server or end station. To use ingress pause metering, you need to set the ingress metering rate in kilobits and set the percentage of the threshold for resuming traffic on the ingress port.

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

```
        edit <port_name>
           set flow-control {tx | both}
           set pause-meter <128-2147483647; set to 0 to disable>
           set pause-meter-resume {25% | 50% | 75%}
        next
      end
   end
```

For example:

```
config switch-controller managed-switch
   edit S424ENTF19000007
      config ports
         edit port29
            set flow-control tx
            set pause-meter 900
            set pause-meter-resume 50%
         next
      end
   end
```

Operation and maintenance

This section covers the following topics:

Discovering, authorizing, and deauthorizing FortiSwitch units

This section covers the following topics:

Editing a managed FortiSwitch unit

To edit a managed FortiSwitch unit:

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

From the *Edit Managed FortiSwitch* form, you can:

- Change the *Name* and *Description* of the FortiSwitch unit.
- View the *Status* of the FortiSwitch unit.
- *Restart* the FortiSwitch.
- *Authorize* or deauthorize the FortiSwitch unit.
- *Update* the firmware running on the switch.
- Override 802.1x settings, including the reauthentication interval, maximum reauthentication attempts, and link-down action.

Adding preauthorized FortiSwitch units

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

To preauthorize a FortiSwitch:

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

Using wildcard serial numbers to pre-authorize FortiSwitch units

You can now use asterisks as a wildcard character when you pre-authorize FortiSwitch units. Using a FortiSwitch template, you can name the managed switch and configure the ports. When the FortiSwitch unit is turned on and discovered by the FortiGate device, the wildcard serial number is replaced by the actual serial number and the settings in the FortiSwitch template are applied to the discovered FortiSwitch unit.

When you create the FortiSwitch template, use the following format for the wildcard serial number:

```
PREFIX****nnnnnn
```

PREFIX	The first six digits of a valid FortiSwitch serial number, such as S248EP, S124EN, S548DF, and S524DF.
****	Asterisks are the only wildcard characters allowed. You can have any number of asterisks, as long as ****nnnnnn is no longer than 10 characters.
nnnnnn	You can have any number of valid alphanumeric characters, as long as ****nnnnnn is no longer than 10 characters.

To pre-authorize FortiSwitch units using a FortiSwitch template:

1. Create a FortiSwitch template.

```
config switch-controller managed-switch
   edit <PREFIX****nnnnnn>
      ...
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S248EP****000000"
```

```
        set name "fortilink-FSW248EP1"
        set fsw-wan1-peer "fortilink"
        .......
        config ports
           edit "port1"
              set vlan "onboarding"
              set allowed-vlans "quarantine" "nac_segment"
              set untagged-vlans "quarantine" "nac_segment"
              set access-mode nac
              set export-to "root"
           next
           edit "port2"
              set vlan "_default"
              set allowed-vlans "quarantine"
              set untagged-vlans "quarantine"
              set access-mode dynamic
              set port-policy "aggr1"
              set export-to "root"
           next
        end
     next
  end
```

2. Turn on the FortiSwitch unit so that the FortiGate device will discover it.

   The FortiSwitch unit is matched with the FortiSwitch template using the order of entries in the CMDB table from top to bottom. The settings in the FortiSwitch template are applied to the discovered FortiSwitch unit. Once a match is made for a wildcard entry, that particular entry is consumed.

Authorizing the FortiSwitch unit

If you configured the FortiLink interface to manually authorize the FortiSwitch unit as a managed switch, perform the following steps:

1. Go to *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.

Deauthorizing FortiSwitch units

A device can be deauthorized to remove it from the Security Fabric.

To deauthorize a device:

1. On the root FortiGate, go to Security Fabric > Fabric Connectors
2. In the topology tree, click the device and select Deauthorize.

After devices are deauthorized, the devices' serial numbers are saved in a trusted list that can be viewed in the CLI using the `show system csf` command. For example, this result shows a deauthorized FortiSwitch:

```
show system csf
   config system csf
      set status enable
      set group-name "Office-Security-Fabric"
      set group-password ENC 1Z2X345V678
```

```
      config trusted-list
         edit "FGT6HD391806070"
         next
         edit "S248DF3X17000482"
            set action deny
         next
      end
   end
end
```

Converting to FortiSwitch standalone mode

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

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

You can disable FortiLink auto-discovery on multiple FortiSwitch units using the following commands:

```
config switch-controller global
   set disable-discovery <switch-id>
end
```

For example:

```
config switch-controller global
   set disable-discovery S1234567890
end
```

You can also add or remove entries from the list of FortiSwitch units that have FortiLink auto-discovery disabled using the following commands:

```
config switch-controller global
   append disable-discovery <switch-id>
   unselect disable-discovery <switch-id>
end
```

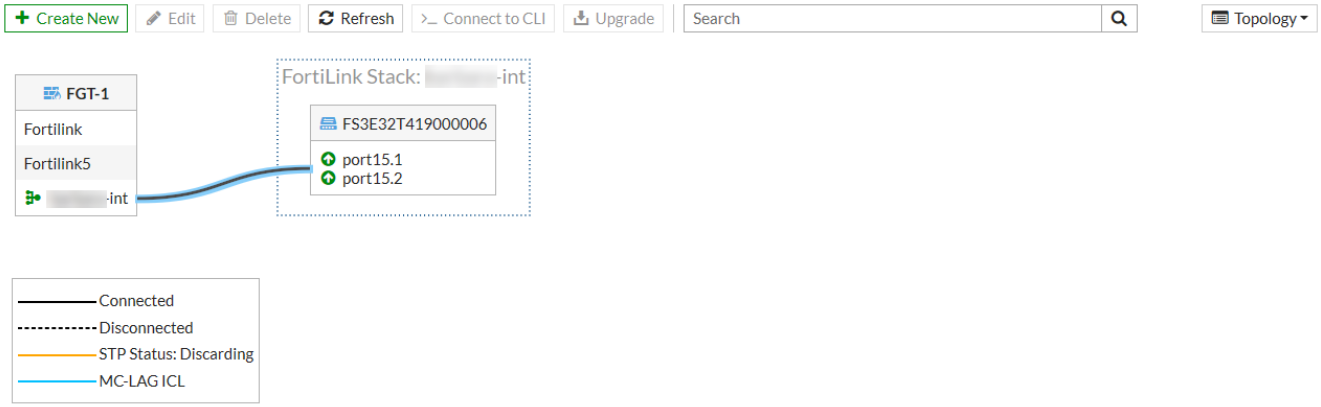
For example:

```
config switch-controller global
   append disable-discovery S012345678
   unselect disable-discovery S1234567890
end
```

Managed FortiSwitch display

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

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



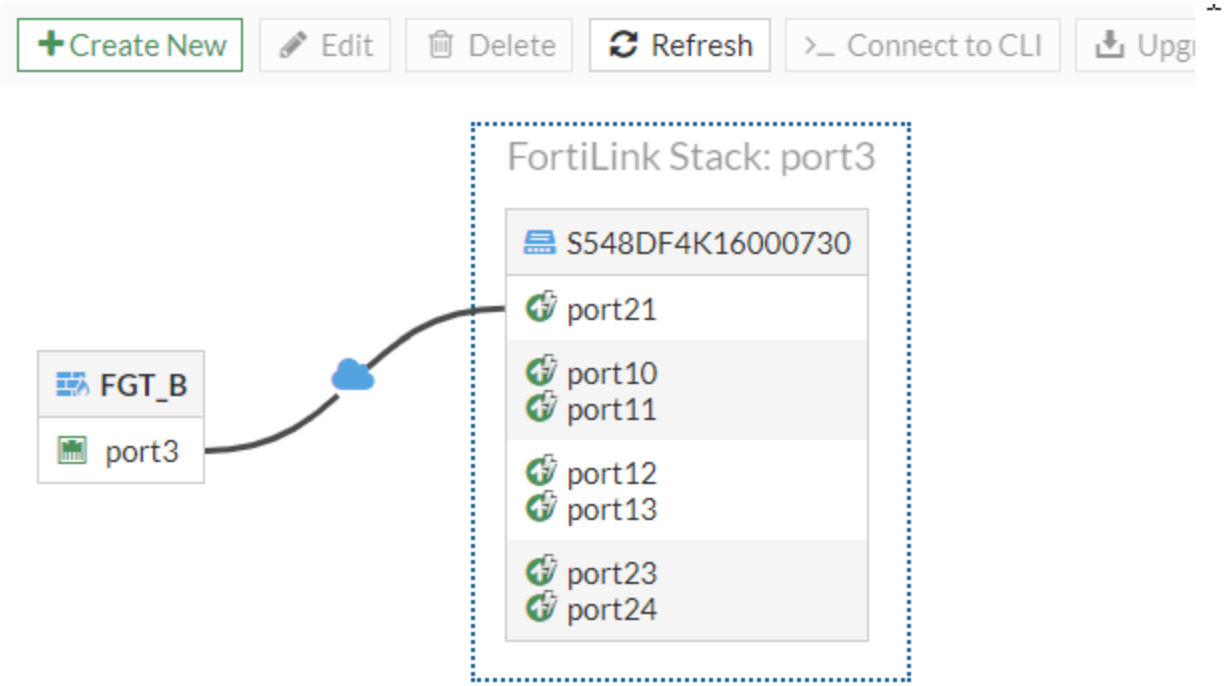
If the link has gone down for some reason, the line will be dashed, and a broken link icon will appear. You can still edit the FortiSwitch unit though and find more information about the status of the switch. The link to the FortiSwitch unit might be down for a number of reasons; for example, a problem with the cable linking the two devices, firmware versions being out of synch, and so on. You need to make sure the firmware running on the FortiSwitch unit is compatible with the firmware running on the FortiGate unit.

From the Managed FortiSwitch page, you can edit any of the managed FortiSwitch units, remove a FortiSwitch unit from the configuration, refresh the display, connect to the CLI of a FortiSwitch unit, or deauthorize a FortiSwitch unit.

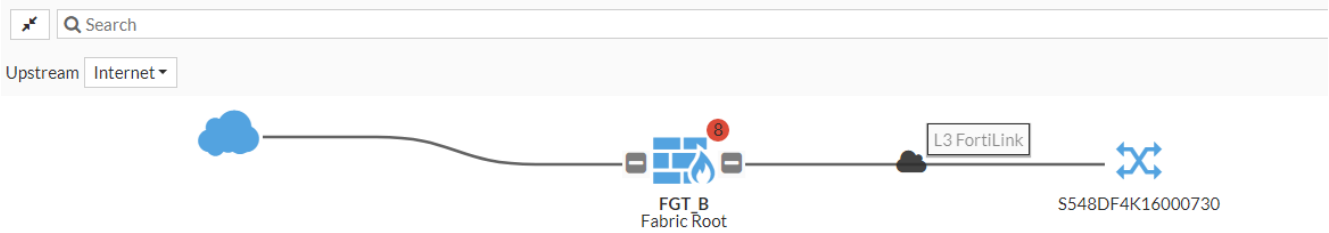
Cloud icon indicates that the FortiSwitch unit is managed over layer 3

A new cloud icon indicates when the FortiSwitch unit is being managed over layer 3. The cloud icon is displayed in two places in the GUI.

Go to *WiFi Controller* > *Managed FortiSwitch* and select *Topology*. In the following figure, the cloud icon over the connection line indicates that S548DF4K16000730 is being managed over layer 3.



Go to *Security Fabric* > *Physical Topology*. In the following figure, the cloud icon over the connection line indicates that S548DF4K16000730 is being managed over layer 3.



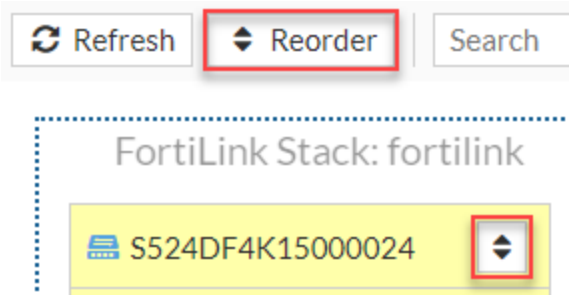
Re-ordering FortiSwitch units in the Topology view

Starting in FortiOS 7.0.1, you can change the order in which FortiSwitch units are displayed in the Topology view.

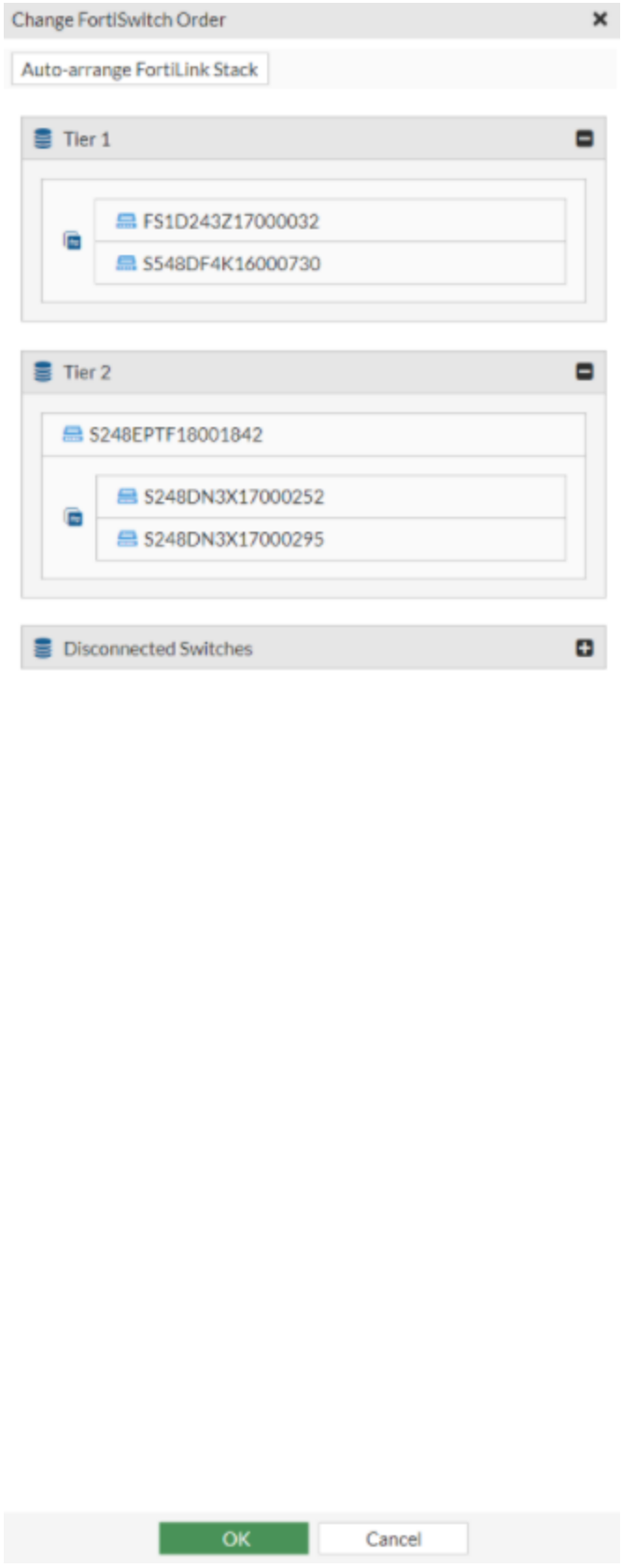
To rearrange the FortiSwitch units in the GUI:

1. Go to *WiFi & Switch Controller* > *Managed FortiSwitches*.
2. In the *View* dropdown list, select *Topology*.

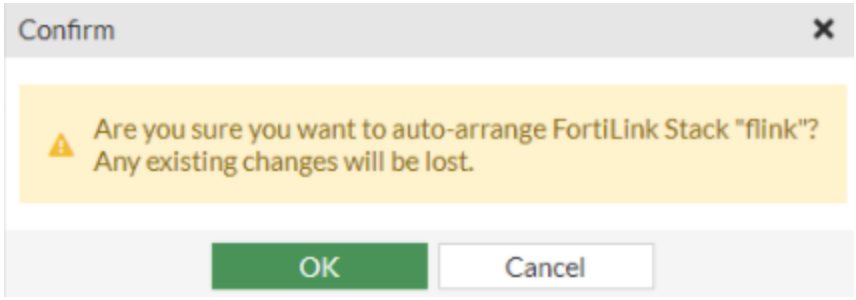
3. Click *Reorder* or the double-arrow button next to the FortiSwitch serial number.



4. In the *Change FortiSwitch Order* window, drag-and-drop each FortiSwitch unit to change the order.



5. If you want FortiOS to determine the arrangement with the fewest edge crossings, click *Auto-arrange FortiLink Stack* in the *Change FortiSwitch Order* window and then click *OK* in the *Confirm* window.



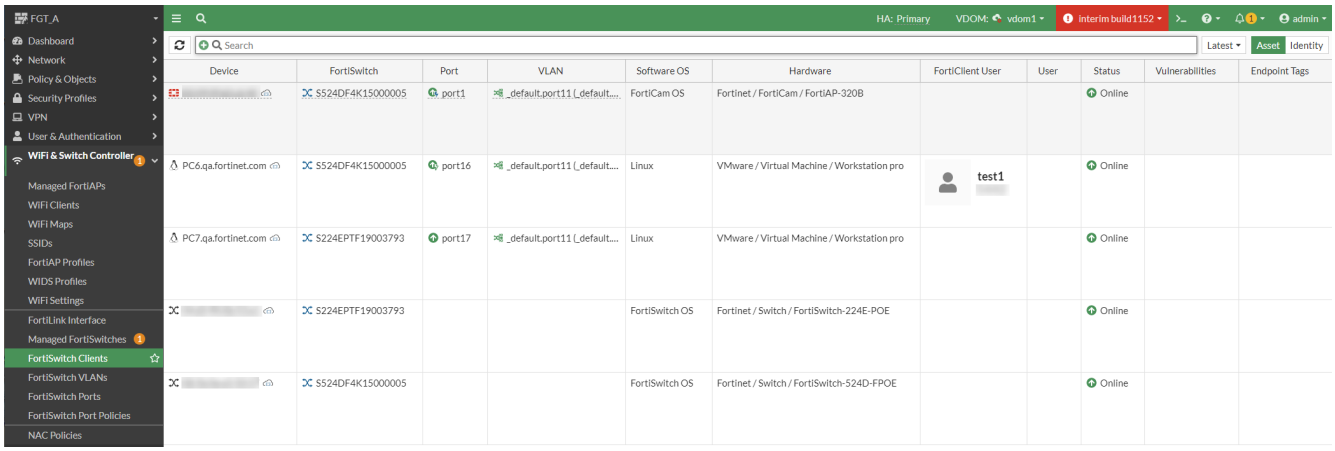
To rearrange the FortiSwitch units in the FortiOS CLI:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      move <FortiSwitch_serial_number1> before <FortiSwitch_serial_number2>
   next
end
```

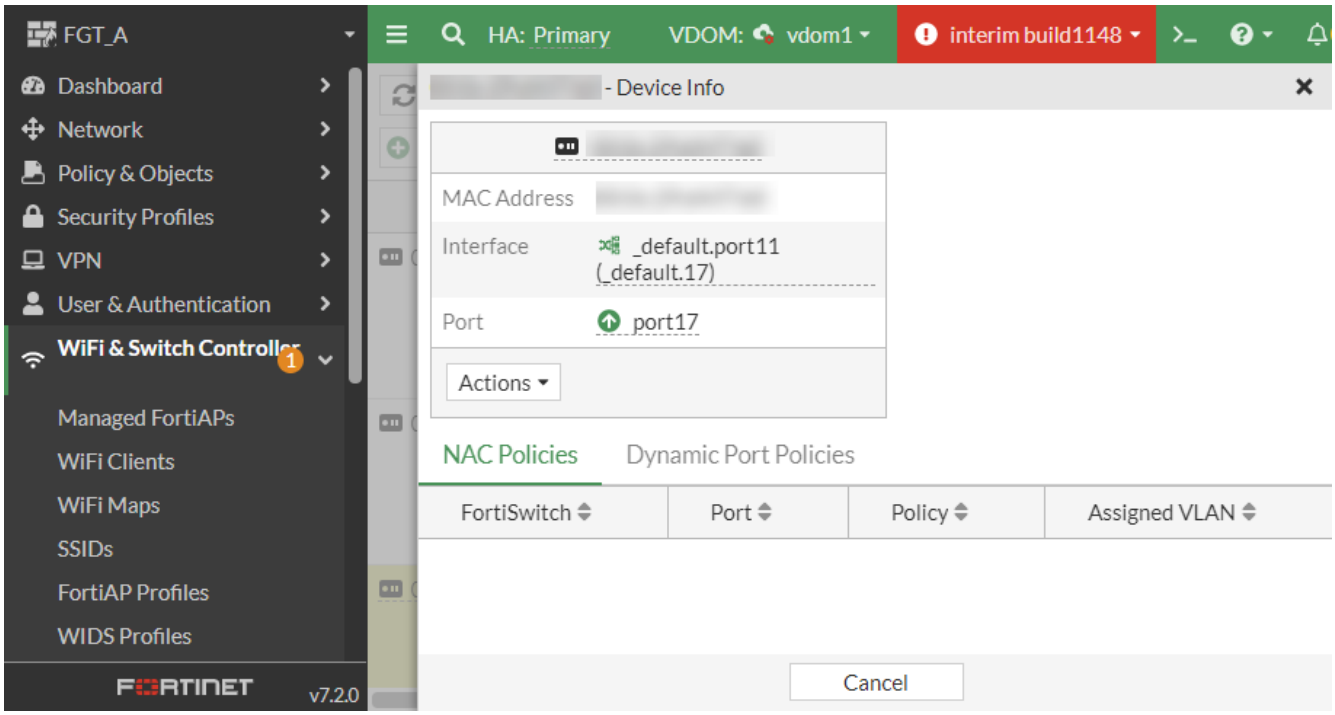
FortiSwitch_serial_number1 is now listed above FortiSwitch_serial_number2.

FortiSwitch clients

Starting in FortiOS 7.2.0, new *WiFi & Switch Controller* > *FortiSwitch Clients* page lists all devices connected to the FortiSwitch unit for a particular VDOM.



Double-click a row to display the *Device Info* pane.

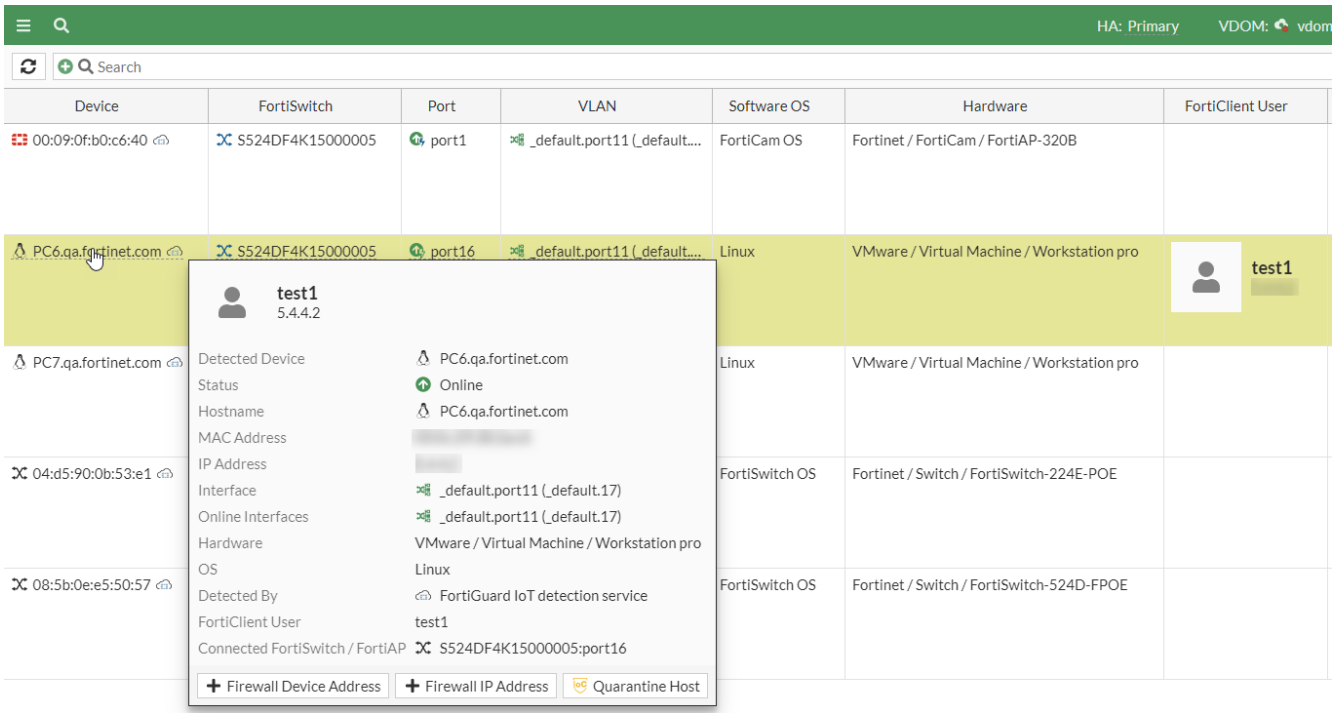


The *Device Info* pane displays the NAC policies and dynamic port policies that the device matches.

From the Actions dropdown menu, you can do the following:

- Create a firewall device address.
- Quarantine the host.

Hover over the device name in the *FortiSwitch Clients* page to get more details.



From the detail window, you can do the following:

- Create a firewall device address.
- Create a firewall IP address.
- Quarantine the host.

To create the firewall device address:

1. Click *Firewall Device Address*.
2. In the *Name* field, enter a name for the firewall device address.
3. Click *Change* if you want a different color for the icon on the GUI.
4. If you want a different MAC address or range of MAC addresses, click + and then enter the MAC address or range of MAC addresses.
5. From the *Interface* dropdown list, select an interface.
6. In the *Comments* field, enter a description of the firewall device address.
7. Click *OK*.

To create the firewall IP address:

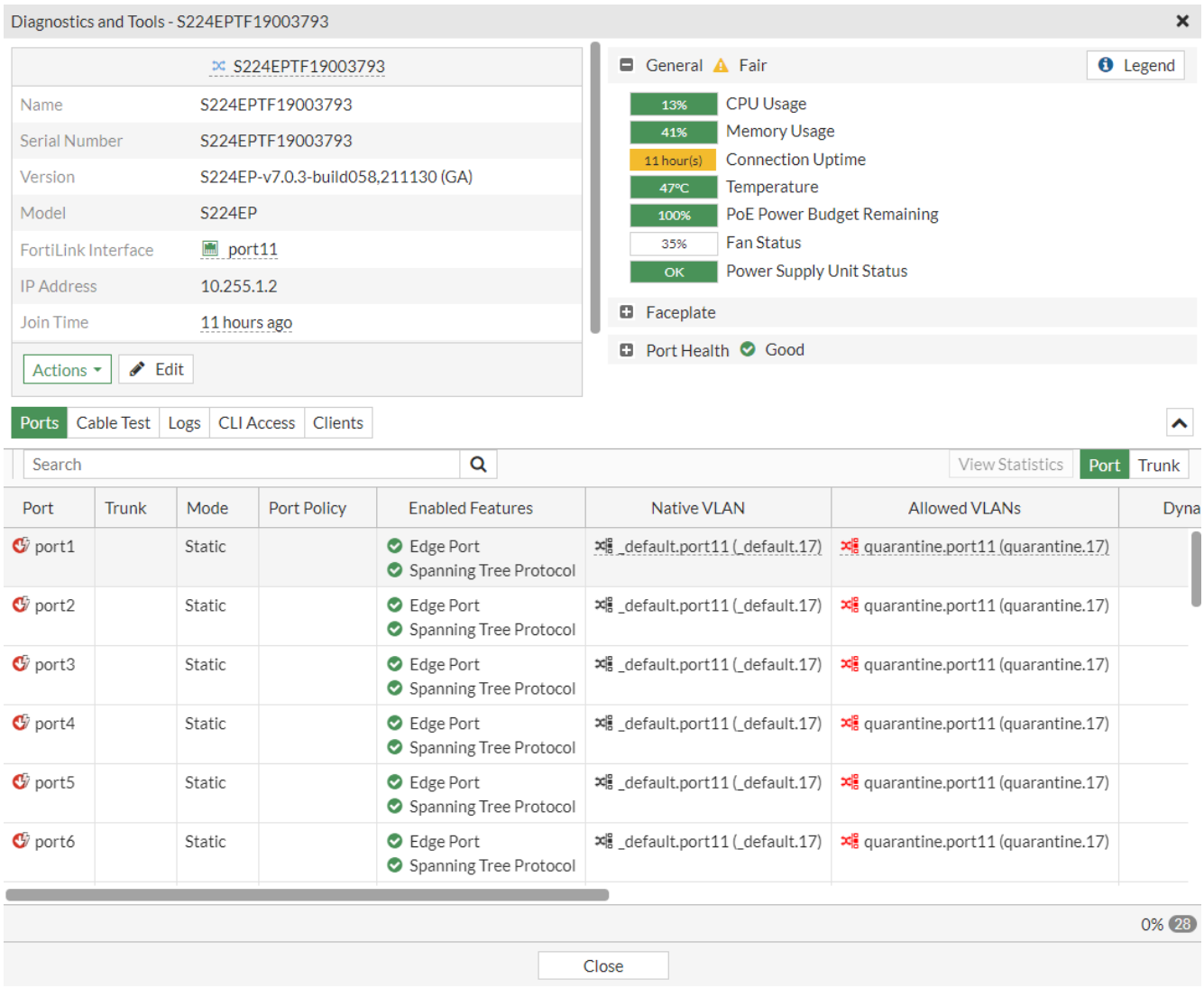
1. Click *Firewall IP Address*.
2. In the *Name* field, enter a name for the firewall IP address.
3. Click *Change* if you want a different color for the icon on the GUI.
4. In the *IP/Netmask* field, change the value as needed.
5. From the *Interface* dropdown list, select an interface.
6. Enable or disable *Static route configuration*.
7. In the *Comments* field, enter a description of the firewall device address.
8. Click *OK*.

To quarantine the host:

1. Click *Quarantine Host*.
2. In the *Description* field, enter the reason for quarantining the host.
3. Click *OK*.

Diagnostics and tools

The *Diagnostics and Tools* pane reports the general health of the FortiSwitch unit, displays details about the FortiSwitch unit, and allows you to run diagnostic tests.



To view the Diagnostics and Tools pane:

1. Go to *WiFi & Switch Controller* > *Managed FortiSwitch*.
2. Click on the FortiSwitch unit and then click *Diagnostics and Tools*.

From the *Diagnostics and Tools* pane, you can do the following:

- *Authorize* or deauthorize the FortiSwitch.
- *Upgrade* the firmware running on the switch.
- *Restart* the FortiSwitch unit.
- *Connect to CLI* to run CLI commands.
- *Show in List* to return to the *WiFi & Switch Controller* > *Managed FortiSwitch* page.
- Go to the *Edit Managed FortiSwitch* form.
- Start or stop the *LED Blink* to identify a specific FortiSwitch unit. See Making the LEDs blink on page 217.
- Display a list of FortiSwitch ports and trunks and configuration details.
- Run a *Cable Test* on a selected port. See Running the cable test on page 217.
- View the *Logs* for the FortiSwitch unit.
- Use the *Clients* tab to list the clients connected to each port of the selected FortiSwitch unit.

- Click the *Legend* button in the *General* pane to display the *Health Thresholds* pane, which lists the thresholds for the good, fair, and poor ratings of the general health, port health, and MC-LAG health.

You can also access the *Diagnostics and Tools* pane from the *Security Fabric > Physical Topology* page.

Making the LEDs blink

When you have multiple FortiSwitch units and need to locate a specific switch, you can flash all port LEDs on and off for a specified number of minutes.

To identify a specific FortiSwitch unit:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. Click on the FortiSwitch unit and then click *Diagnostics and Tools*.
3. Select *LED Blink > Start* and then select *5 minutes*, *15 minutes*, *30 minutes*, or *60 minutes*.
4. After you locate the FortiSwitch unit, select *LED Blink > Stop*.

NOTE: For the 5xx switches, LED Blink flashes only the SFP port LEDs, instead of all the port LEDs.

Running the cable test

NOTE: Running cable diagnostics on a port that has the link up interrupts the traffic for several seconds.

You can check the state of cables connected to a specific port. The following pair states are supported:

- Open
- Short
- Ok
- Open_Short
- Unknown
- Crosstalk

If no cable is connected to the specific port, the state is Open, and the cable length is 0 meters.

Using the GUI:

1. Go to *WiFi & Switch Controller > Managed FortiSwitch*.
2. Click on the FortiSwitch unit and then click *Diagnostics and Tools*.
3. Select *Cable Test*.
4. Select a port.
5. Select *Diagnose*.

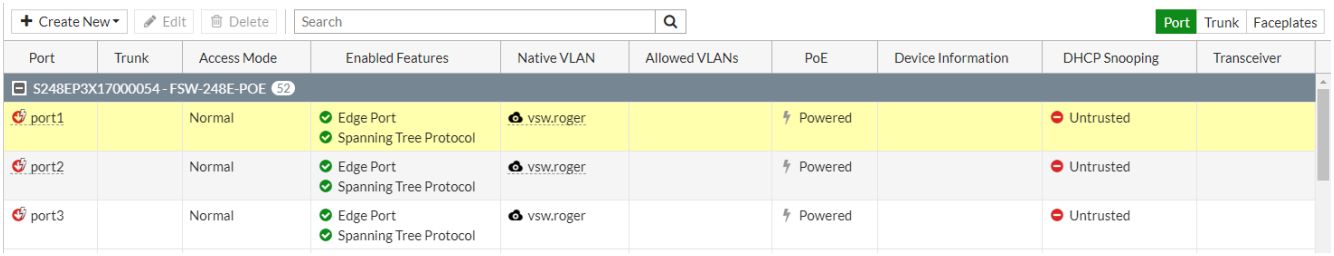
NOTE: There are some limitations for cable diagnostics on the FS-108E, FS-124E, FS-108E-POE, FS-108E-FPOE, FS-124E-POE, FS-124E-FPOE, FS-148E, and FS-148E-POE models:

- Crosstalk cannot be detected.
- There is a 5-second delay before results are displayed.
- The value for the cable length is inaccurate.
- The results are inaccurate for open and short cables.

FortiSwitch ports display

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

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



Select *Faceplates* to get the following information:

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

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

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

Each entry in the port list displays the following information:

- Port status (red for down, green for up)
- Port name
- If the port is a member of a trunk
- Access mode
- Enabled features
- Native VLAN
- Allowed VLANs
- PoE status
- Device information
- DHCP snooping status
- Transceiver information

FortiSwitch per-port device visibility

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

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

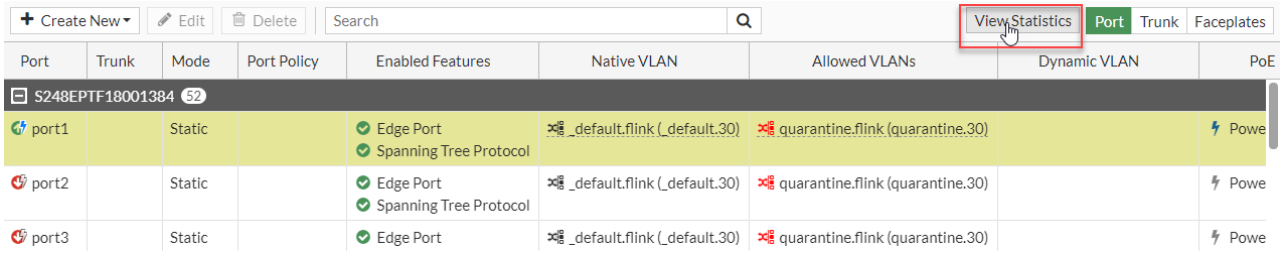
```
diagnose switch-controller mac-cache show <switch-id>
```

Displaying, resetting, and restoring port statistics

For the following commands, if the managed FortiSwitch unit is not specified, the command is applied to all ports of all managed FortiSwitch units.

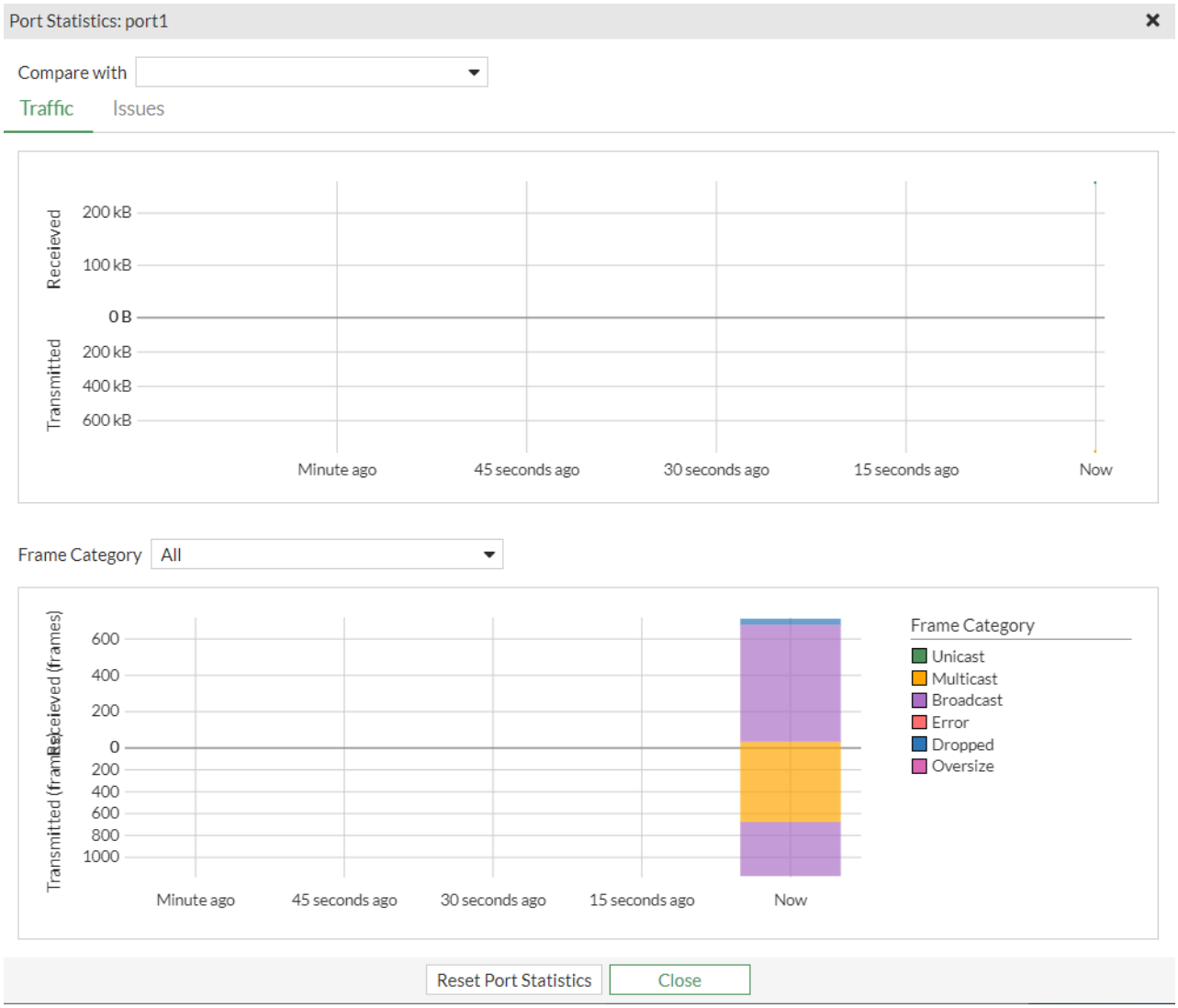
To display port statistics using the GUI:

1. Go to *WiFi & Switch Controller* > *FortiSwitch Ports*.
2. Select a port.
3. Click *View Statistics*.



4. Click the *Traffic* tab to see transmitted and received traffic and transmitted and received frames. Click the *Issues* tab

to see frame errors by type.



To display port statistics using the CLI:

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

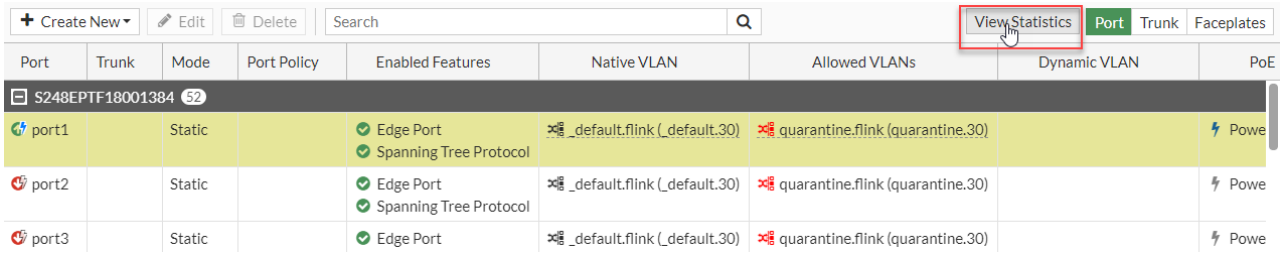
For example:

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

S524DF4K15000024:
Port(port8) is Admin up, line protocol is down
Interface Type is Serial Gigabit Media Independent Interface(SGMII/SerDes)
Address is 08:5B:0E:F1:95:ED, loopback is not set
MTU 9216 bytes, Encapsulation IEEE 802.3/Ethernet-II
half-duplex, 0 Mb/s, link type is auto
```

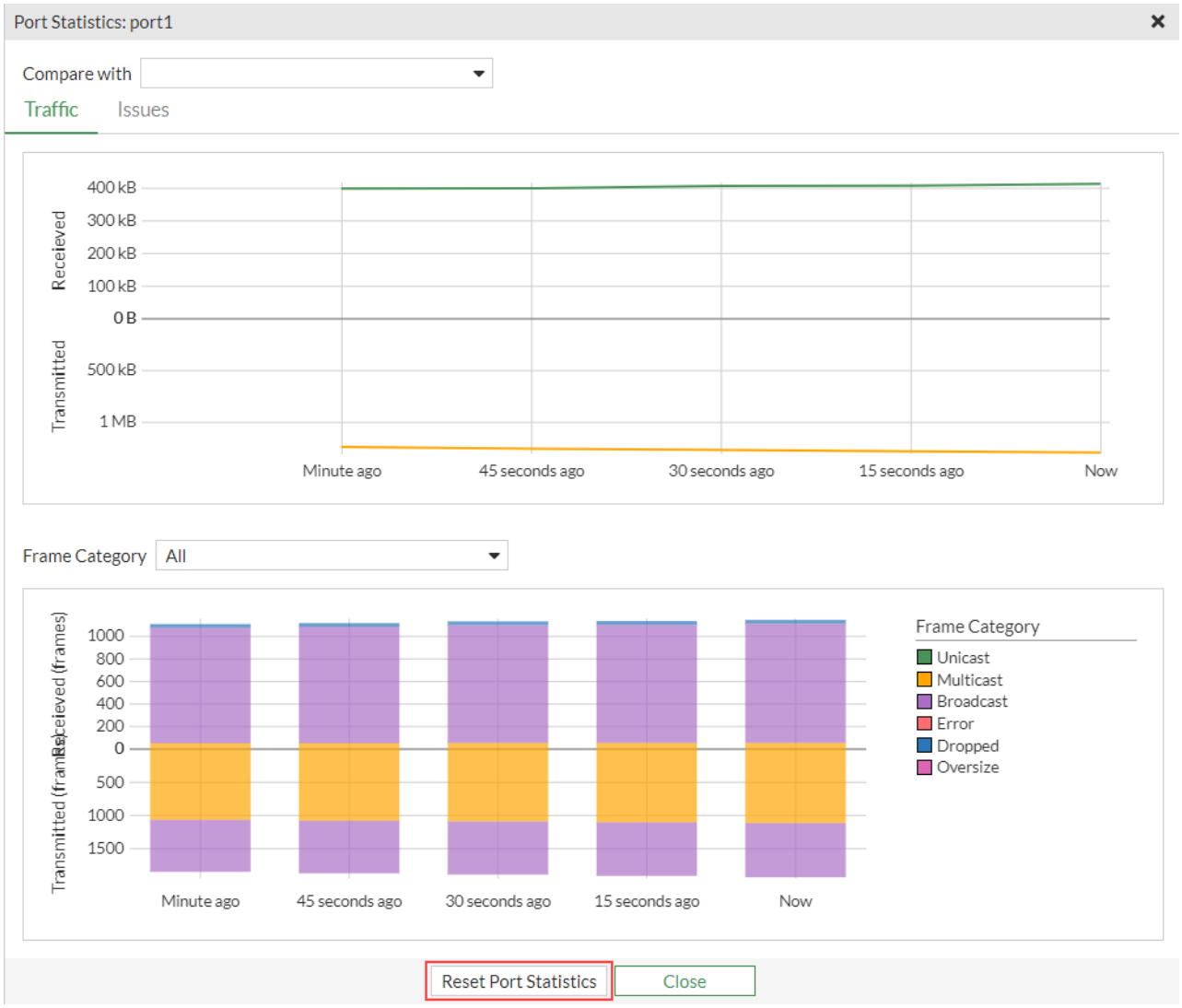
```
input : 0 bytes, 0 packets, 0 errors, 0 drops, 0 oversizes
0 unicasts, 0 multicasts, 0 broadcasts, 0 unknowns
output : 0 bytes, 0 packets, 0 errors, 0 drops, 0 oversizes
0 unicasts, 0 multicasts, 0 broadcasts
0 fragments, 0 undersizes, 0 collisions, 0 jabbers


Vdom: vdom-1
```

To reset the port statistics counters using the GUI:

1. Go to *WiFi & Switch Controller* > *FortiSwitch Ports*.
2. Select a port.
3. Click *View Statistics*.



4. Click *Reset Port Statistics*.



To reset the port statistics counters using the CLI:

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

For example:

```
FG100D3G15817028 (global) # diagnose switch-controller trigger reset-hardware-counters
     S524DF4K15000024 1,3,port6-7
```

NOTE: This command is provided for debugging; accuracy is not guaranteed when the counters are reset. Resetting the counters might have a negative effect on monitoring tools, such as SNMP and FortiGate. The statistics gathered during the time when the counters are reset might be discarded.

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

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

For example:

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

Managing DSL transceivers (FN-TRAN-DSL)

A Procend 180-T DSL transceiver (FN-TRAN-DSL) that is plugged in to a FortiGate-managed FortiSwitch port can now be managed by a FortiGate unit. The management of the DSL transceiver and the FortiSwitch port includes the ability to program the physical-layer attributes on the DSL module, retrieve the status and statistics from the module, upgrade the module's firmware, and reset the module.

You can use the following FortiGate models to manage FN-TRAN-DSL: FG-80F, FG-81F, FG-80F-BP, FGR-60F, FGR-60F-3G4G, FG-60F, and FG-40F-3G4G. The FortiSwitch unit must be running FortiSwitchOS 7.0.1, build 0038 or later. A FortiSwitch unit running in standalone mode cannot program the physical-layer attributes on the DSL module.

To create a DSL policy:

```
config switch-controller dsl policy
   edit <DSL_policy_name>
      set type Procend
      set us-bitswap {enable | disable}
      set ds-bitswap {enable | disable}
      set profile {auto-30a | auto-17a | auto-12ab}
      set cs {A43, B43, A43C, V43}
      set pause-frame {enable | disable}
      set cpe_aele {enable | disable}
      set cpe_aele-mode  {ELE_M0 | ELE_DS | ELE_PB | ELE_MIN}
      set append_padding {enable | disable}
   next
end
```

Option	Description	Default value
<DSL_policy_name>	Enter a name for the DSL policy.	No default
type Procend	You can only select the `Procend` type.	Procend
us-bitswap {enable | disable}	Enable or disable whether the upstream bits are exchanged.	enable
ds-bitswap {enable | disable}	Enable or disable whether the downstream bits are exchanged.	enable
profile {auto-30a | auto-17a | auto-12ab}	Select which very-high-bit-rate digital subscriber line (VDSL) customer premises equipment (CPE) profile to use.	auto-30a
cs {A43, B43, A43C, V43}	Select which CPE carrier set to use.	A43 B43 A43C
pause-frame {enable | disable}	Enable or disable device pause frames.	enable

Option	Description	Default value
cpe_aele {enable | disable}	Enable or disable CPE alternative electrical length estimation (AELE) mode.	enable
cpe_aele-mode {ELE_M0 | ELE_DS | ELE_PB | ELE_MIN}	Select the CPE AELE mode to use.	ELE_MIN
append_padding {enable | disable}	Enable or disable whether to append padding.	enable

To specify the DSL policy to use:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port>
            set dsl-profile <DSL_policy_name>
         next
      end
   next
end
```

To display DSL statistics:

```
get switch-controller dsl link-time <FortiSwitch_serial_number> <port_name>
get switch-controller dsl pkt-count <FortiSwitch_serial_number> <port_name>
get switch-controller dsl pm-line-curr <FortiSwitch_serial_number> <port_name>
get switch-controller dsl policy
get switch-controller dsl rate <FortiSwitch_serial_number> <port_name>
get switch-controller dsl status <FortiSwitch_serial_number> <port_name>
get switch-controller dsl summary <FortiSwitch_serial_number> <port_name>
get switch-controller dsl version <FortiSwitch_serial_number> <port_name>
```

Option	Description
link-time <FortiSwitch_serial_number> <port_name>	Display the link time for the DSL module plugged in to the specified FortiSwitch port.
pkt-count <FortiSwitch_serial_number> <port_name>	Display the packet count for the DSL module plugged in to the specified FortiSwitch port.
pm-line-curr <FortiSwitch_serial_number> <port_name>	Display the line current for the DSL module plugged in to the specified FortiSwitch port.
policy	List the available DSL policies and their settings.
rate <FortiSwitch_serial_number> <port_name>	Display the rate for the DSL module plugged in to the specified FortiSwitch port.
status <FortiSwitch_serial_number> <port_name>	Display the status of the DSL module plugged in to the specified FortiSwitch port.

Option	Description
summary <FortiSwitch_serial_number> <port_name>	Display a summary for the DSL module plugged in to the specified FortiSwitch port.
version <FortiSwitch_serial_number> <port_name>	Display the version of the DSL module plugged in to the specified FortiSwitch port.

To reset the DSL module on a FortiSwitch port:

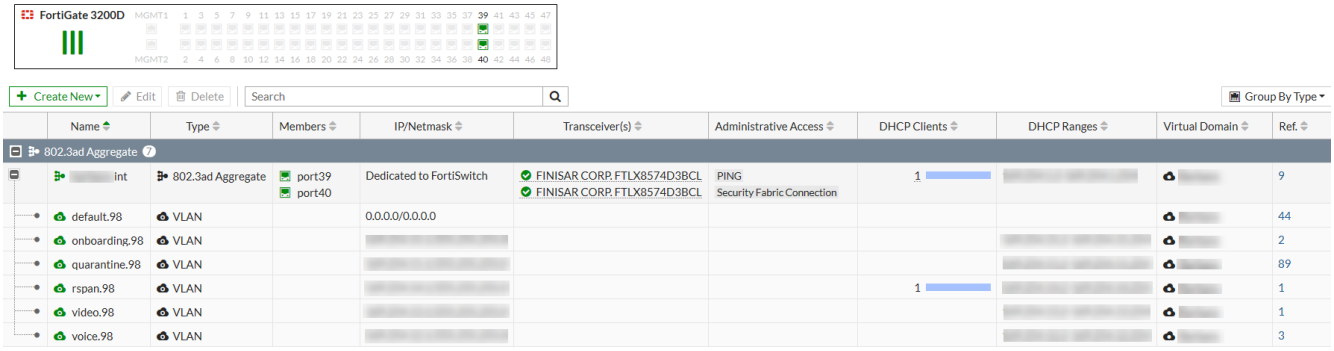
```
execute switch-controller dsl reset <FortiSwitch_serial_number> <port_name>
```

To upload a FortiSwitch image to the FortiGate local storage:

```
execute switch-controller dsl update ftp <DSL_image_name_on_FTP_server> <FTP_server>[:<FTP_
     port>] <FTP_user_name> <FTP_password> <FortiSwitch_serial_number> <port_name>
execute switch-controller dsl update tftp <DSL_image_name_on_TFTP_server> <TFTP_server>
     <FortiSwitch_serial_number> <port_name>
```

Network interface display

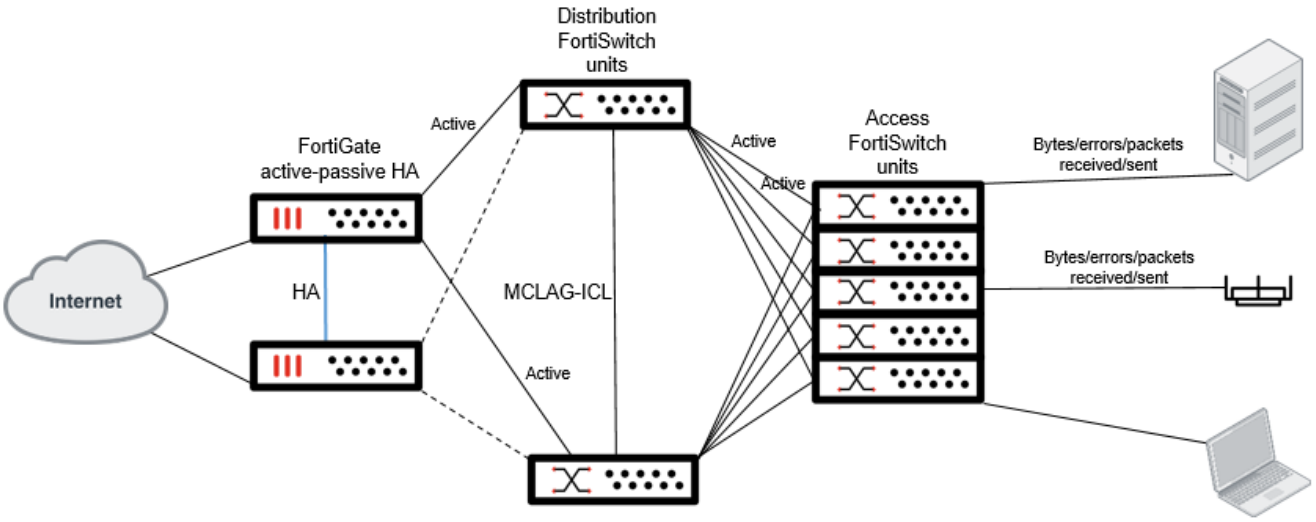
On the *Network* > *Interfaces* page, you can see the FortiGate interface connected to the FortiSwitch unit. The GUI indicates *Dedicated to FortiSwitch* in the IP/Netmask field.



Data statistics

This example shows a FortiLink scenario where the FortiGate acts as the switch controller that collects the data statistics of managed FortiSwitch ports. This is counted by each FortiSwitch and concentrated in the controller.

Sample topology



To show data statistics using the GUI:

1. Go to *WiFi & Switch Controller* > *FortiSwitch Ports*.
2. Select *Configure Table*.
3. Select *Bytes, Errors and Packets* to make them visible.

The related data statistic of each managed FortiSwitch port is shown.

To show data statistics using the CLI:

```
# diagnose switch-controller switch-info port-stats S248EPTF180XXXX
       ......

         Port(port50) is Admin up, line protocol is down
           Interface Type is Gigabit Media Independent Interface(GMII)
         Address is 70:4C:A5:E0:F3:8D, loopback is not set
         MTU 9216 bytes, Encapsulation IEEE 802.3/Ethernet-II
         full-duplex, 1000 Mb/s, link type is manual
         input  : 0 bytes, 0 packets, 0 errors, 0 drops, 0 oversizes
             0 unicasts, 0 multicasts, 0 broadcasts, 0 unknowns
         output : 0 bytes, 0 packets, 0 errors, 0 drops, 0 oversizes
             0 unicasts, 0 multicasts, 0 broadcasts
         0 fragments, 0 undersizes, 0 collisions, 0 jabbers
           ......
```

Synchronizing the FortiGate unit with the managed FortiSwitch units

You can synchronize the FortiGate unit with the managed FortiSwitch units to check for synchronization errors on each managed FortiSwitch unit.

Use the following command to synchronize the full configuration of a FortiGate unit with a managed FortiSwitch unit:

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

Viewing and upgrading the FortiSwitch firmware version

You can view the current firmware version of a FortiSwitch unit and upgrade the FortiSwitch unit to a new firmware version. The FortiGate unit will suggest an upgrade when a new version is available in FortiGuard.

Using the FortiGate GUI

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 FortiGate CLI

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

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

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

```
execute switch-controller switch-software upgrade <switch id> <image id>
```

Use the following CLI commands to enable the use of HTTPS to download firmware to managed FortiSwitch units:

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

NOTE: The HTTPS download is enabled by default.

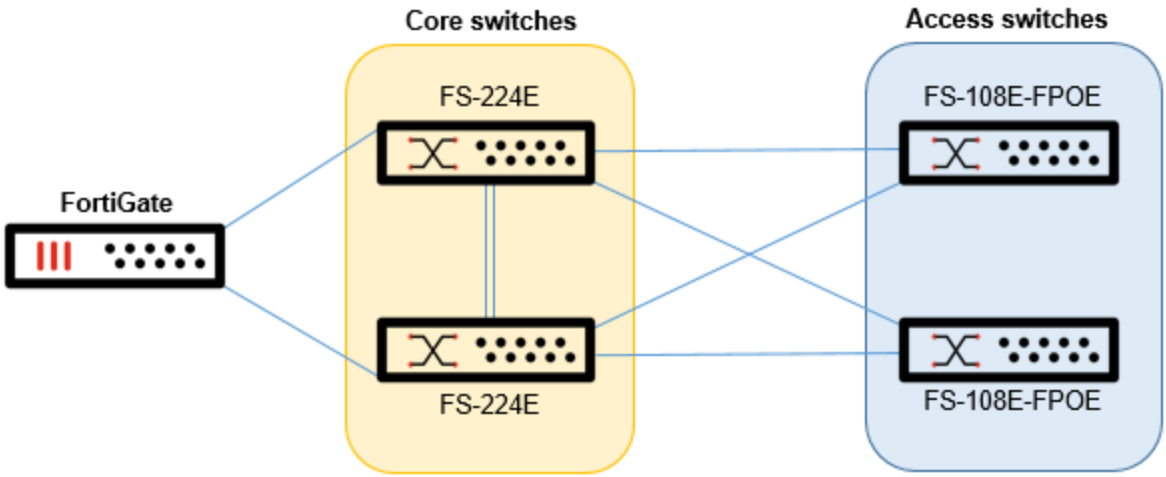
From your FortiGate CLI, you can upgrade the firmware of all of the managed FortiSwitch units of the same model using a single `execute` command. The command includes the name of a firmware image file and all of the managed FortiSwitch units compatible with that firmware image file are upgraded. For example:

```
execute switch-controller switch-software stage all <firmware-image-file>
```

You can also use the following command to restart all of the managed FortiSwitch units after a 2-minute delay.

```
execute switch-controller switch-action restart delay all
```

Firmware upgrade of stacked or tiered FortiSwitch units



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

To upgrade the firmware of stacked or tiered FortiSwitch units:

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

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

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

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

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

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

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

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

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

File Syncing...

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

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

File Syncing...

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

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

File Syncing...

FGT81ETK19001274 #
```

4. Check the downloaded FortiSwitch image. For example:

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

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

FGT81ETK19001274 #
```

5. Start the image staging. For example:

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

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

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

6. Check the status of the image staging. The *Status* column reports (from left to right) the percentage of the new firmware downloaded, the percentage of data erased to make space in the switch's local storage, and the percentage of the new firmware saved to the switch's local storage. For example:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FGT81ETK19001274 #
```

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

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

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

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

STACK-NAME: FortiSwitch-Stack-flink
SWITCH-ID         VERSION           STATUS         FLAG   ADDRESS              JOIN-TIME
           NAME
```

```
    S108EF5918003577  v6.2.2 (194)      Authorized/Up    -   10.105.22.6     Thu Oct 24
    13:22:27 2019    -
    S108EP5918008265  v6.2.2 (194)      Authorized/Up    -   10.105.22.5     Thu Oct 24
    13:22:41 2019    -
    S224ENTF18001408  v6.2.2 (194)      Authorized/Up    -   10.105.22.2     Thu Oct 24
    13:20:11 2019    -
    S224ENTF18001432  v6.2.2 (194)      Authorized/Up    -   10.105.22.3     Thu Oct 24
    13:19:58 2019    -

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

    FGT81ETK19001274 #
```

```
config switch-controller global
   append disable-discovery S012345678
   unselect disable-discovery S1234567890
end
```

Canceling pending or downloading FortiSwitch upgrades

A FortiSwitch device in FortiLink mode can be upgrade using the FortiGate device.

If a connectivity issue occurs during the upgrade process and the FortiSwitch unit loses contact with the FortiGate device, the FortiSwitch upgrade status can get stuck at `Upgrading`. Use the following CLI command to cancel the process:

```
execute switch-controller switch-software cancel {all | sn <FortiSwitch_serial_number> |
     switch-group <switch_group ID>}
```

`all`	Cancel the firmware upgrade for all FortiSwitch units.
`sn <FortiSwitch_serial_number>`	Cancel the firmware upgrade for the FortiSwitch unit with the specified serial number.
`switch-group <switch_group ID>`	Cancel the firmware upgrade for the FortiSwitch units belonging to the specified switch group.

For example, to cancel the upgrade of a FortiSwitch unit with the specified serial number:

```
execute switch-controller switch-software cancel sn S248EPTF180018XX
```

Configuring automatic backups

Starting in FortiOS 7.2.1, you can specify whether your managed FortiSwitch configuration is automatically backed up each time a user logs out or before a system upgrade is started. By default, both options are disabled.

To specify that the managed FortiSwitch unit creates a revision configuration file each time a user logs out:

```
config switch-controller switch-profile
   edit {default | FortiSwitch_profile_name}
      set revision-backup-on-logout enable
   next
end
```

To specify that the managed FortiSwitch unit creates a revision configuration file before a system upgrade is started:

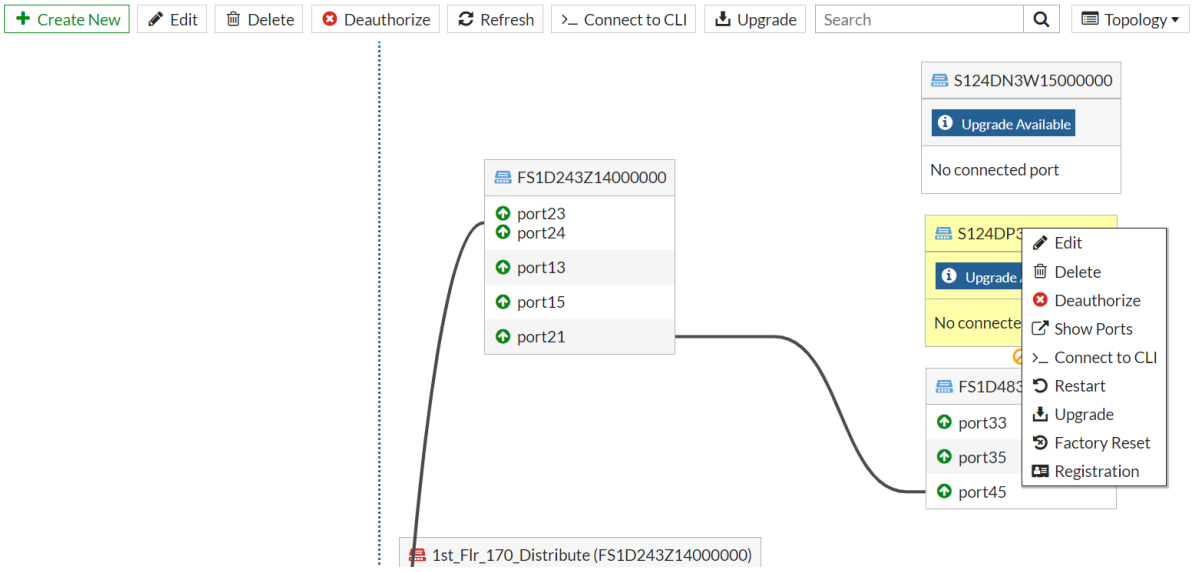
```
config switch-controller switch-profile
   edit {default | FortiSwitch_profile_name}
      set revision-backup-on-upgrade enable
   next
end
```

Registering FortiSwitch to FortiCloud

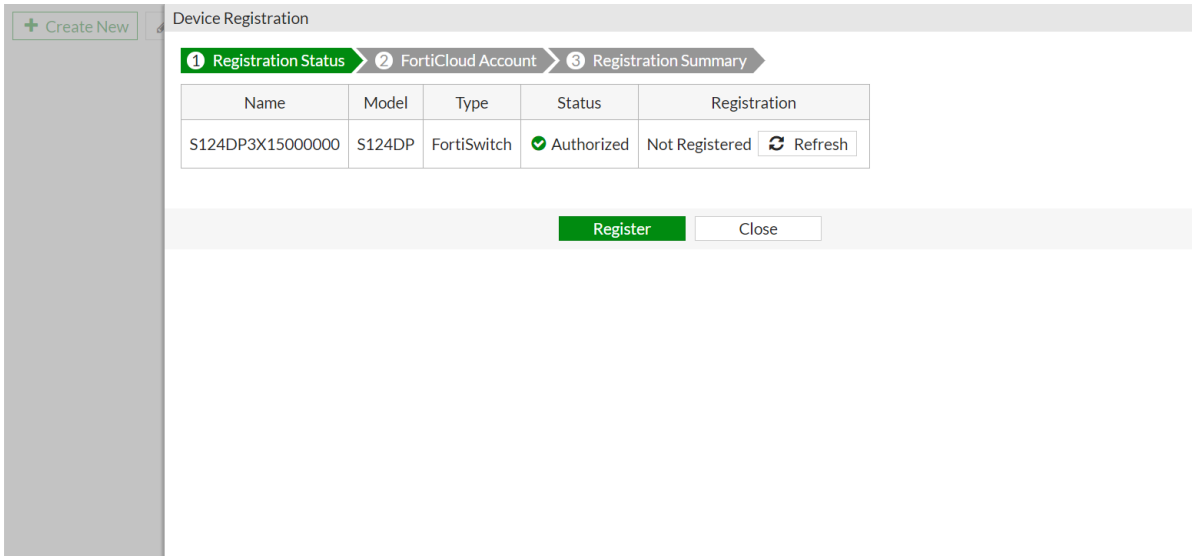
After authorizing a FortiSwitch, administrators can register the FortiSwitch to FortiCloud directly from the FortiOS GUI.

To register the FortiSwitch in the GUI:

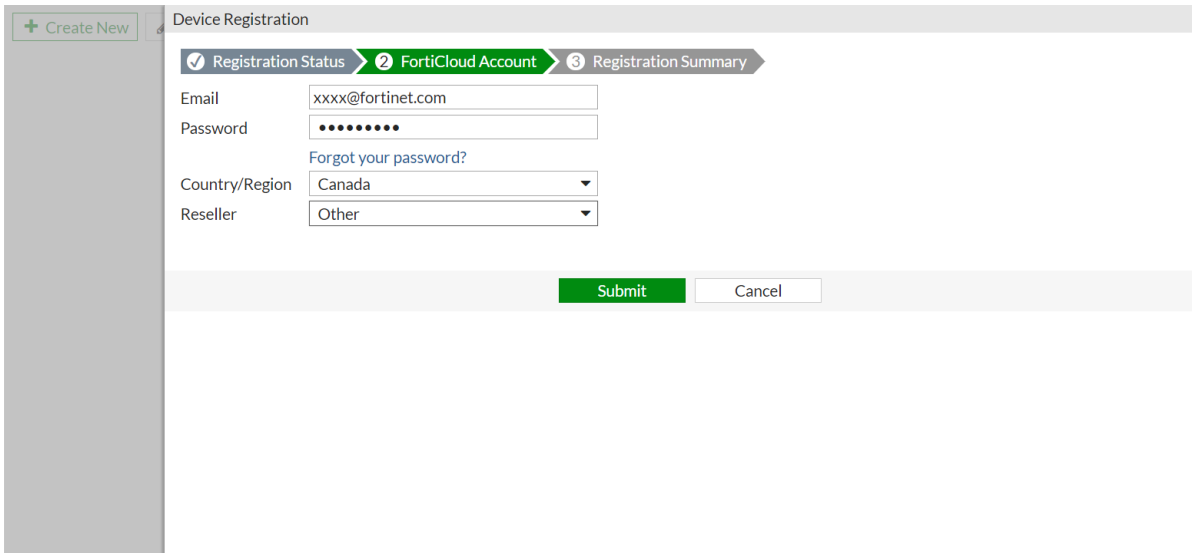
1. Go to *WiFi & Switch Controller* > *Managed FortiSwitch* and ensure the *Topology* view is selected.
2. In the topology, right-click on an unregistered device and click *Registration*.



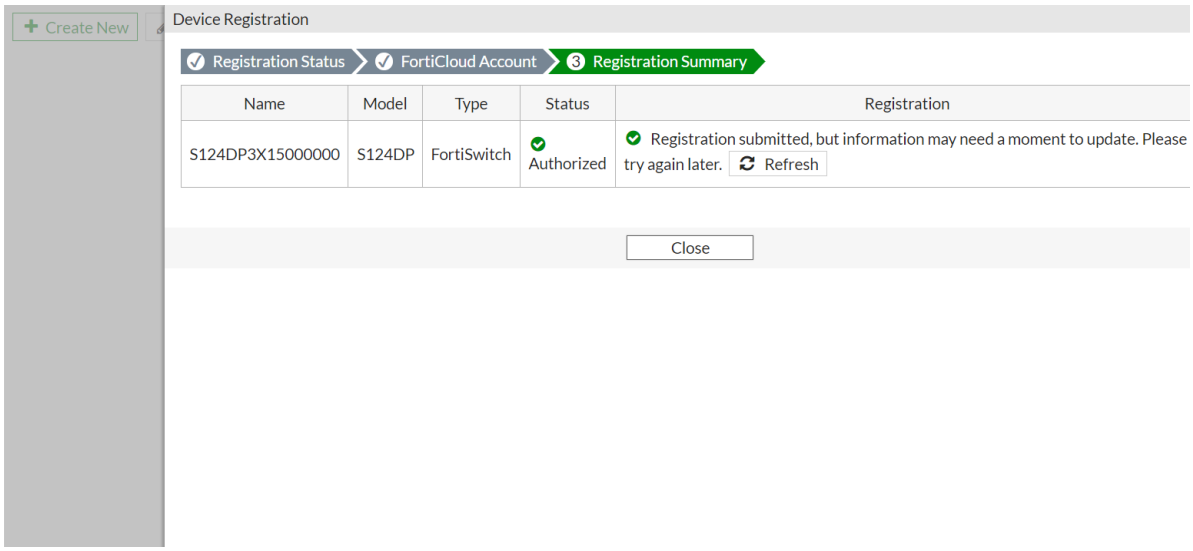
3. Complete the device registration wizard:
   a. Click *Register* to proceed.



   b. Enter the FortiCloud account information and click *Submit*.

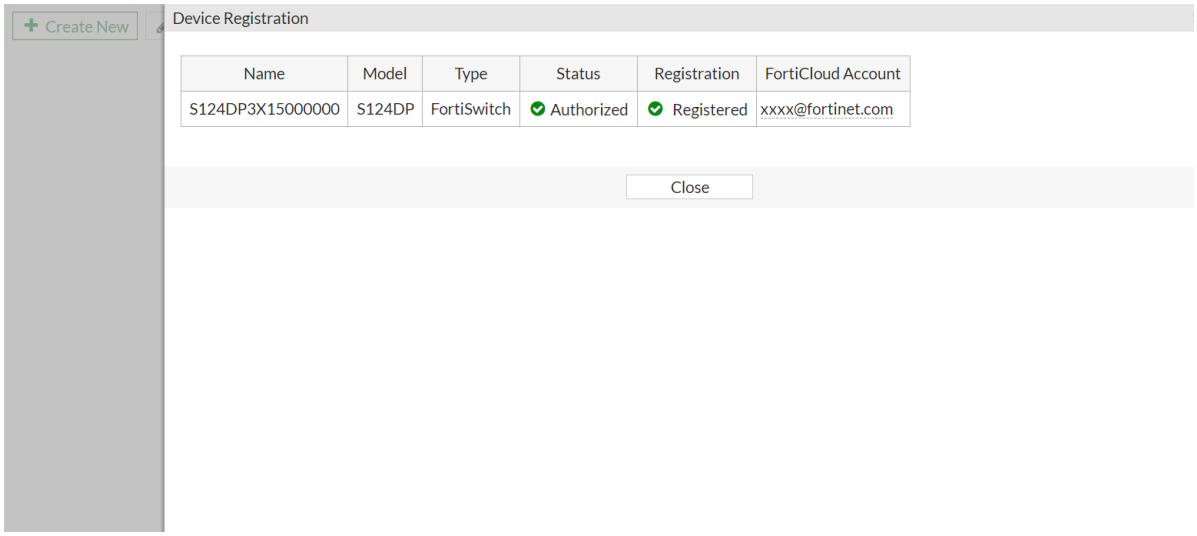


   The registration information is submitted to FortiCare, and FortiOS attempts to collect the registration status from FortiGuard. Since FortiGuard and FortiCare synchronize periodically, the registration status may not update immediately (it may take up to a few hours).



c. Click *Close*.

4. After a while, go back to *WiFi & Switch Controller > Managed FortiSwitch*.
5. Right-click on the device and click *Registration*. The device is shown as *Registered* to the corresponding *FortiCloud* account.



To register the FortiSwitch in the CLI:

```
# diagnose forticare direct-registration product-registration -N S124DP3X15000000 -a
xxxx@fortinet.com -p LDAP -T "CA" -R "other" -e 1
Account info:
       contract_number=[] account_id=[xxxx@fortinet.com] password=[***]
       reseller_id=0 reseller=[other]
       first_name=[] last_name=[] company=[]
       title=[] address=[] city=[]
       state=[] state_code=[] country_code=0
       post_code=[] phone=[] fax=[]
       industry=[] industry_id=0 orgsize=[] orgsize_id=0
       version=0 SN=[S124DP3X15000000] existing=1
Prepare to register product into this account.
```

```
Do you want to continue? (y/n)y
Registration successful
```

Replacing a managed FortiSwitch unit

If a managed FortiSwitch unit fails, you can replace it with another FortiSwitch unit that is managed by the same FortiGate unit. The replacement FortiSwitch unit will inherit the configuration of the FortiSwitch unit that it replaces. The failed FortiSwitch unit is no longer managed by a FortiGate unit or discovered by FortiLink.

NOTE:

- Both FortiSwitch units must be of the same model.
- The replacement FortiSwitch unit must be discovered by FortiLink but not authorized.
- If the replacement FortiSwitch unit is one of an MCLAG pair, you need to manually reconfigure the MCLAG-ICL trunk.
- After replacing the failed FortiSwitch unit, the automatically created trunk name does not change. If you want different trunk name, you need to delete the trunk. The new trunk is created automatically with an updated name. At the end of this section is a detailed procedure for renaming the MCLAG-ICL trunk.
- If the replaced managed FortiSwitch unit is part of an MCLAG, only the ICL should be connected to the new switch to avoid any traffic loops. The other interfaces should be connected only to the switch that is fully managed the FortiGate unit with the correct configuration.
- The best way to replace a MCLAG FortiSwitch unit in FortiLink:
  a. Back up the configuration of the failed FortiSwitch unit.
  b. Restore the configuration to the replaced Fortiswitch unit while it is offline.
  c. Enter the `replace-device` command in FortiOS.
  d. Physically replace the failed FortiSwitch unit.

To replace a managed FortiSwitch unit:

1. Unplug the failed FortiSwitch unit.
2. Plug in the replacement FortiSwitch unit.
3. Upgrade the firmware of the replacement FortiSwitch unit to the same version as the firmware on the failed FortiSwitch unit. See Viewing and upgrading the FortiSwitch firmware version on page 227.
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.
   NOTE: If the replaced managed FortiSwitch unit is part of an MCLAG, only the ICL should be connected to the new switch to avoid any traffic loops. The other interfaces should be connected only to the switch that is fully managed the FortiGate unit with the correct configuration.
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.

11. Authorize the replaced managed FortiSwitch unit.
12. Connect the rest of the cables required for the uplinks and downlinks for the MCLAG FortiSwitch units.

To rename the MCLAG-ICL trunk:

After replacing the failed FortiSwitch unit, the automatically created trunk name does not change. If you want different trunk name, you need to delete the trunk. The new trunk is created automatically with an updated name.

Changing the name of the MCLAG-ICL trunk must be done on both 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 igmp-snooping-flood-reports enable
set mcast-snooping-flood-traffic enable
set snmp-index 57
next
end

icl-sw1 # diag switch mclag icl
D483Z17000282-0
icl-ports 27-28
egress-block-ports 3-4,7-12,47-48
interface-mac 70:4c:a5:86:6d:e5
lacp-serial-number FS1D483Z17000348
peer-mac 70:4c:a5:49:50:53
peer-serial-number FS1D483Z17000282
Local uptime 0 days 1h:49m:24s
Peer uptime 0 days 1h:49m:17s
```

```
MCLAG-STP-mac 70:4c:a5:49:50:52
keepalive interval 1
keepalive timeout 60

Counters
received keepalive packets 4852
transmited keepalive packets 5293
received keepalive drop packets 20
receive keepalive miss 1

icl-sw1 # diagnose switch trunk sum D483Z17000282-0
Trunk Name Mode PSC MAC Status Up Time
_____________ _____________________ ___________ _________________ _______
____ ___________________________________
D483Z17000282-0 lacp-active(auto-isl,mclag-icl) src-dst-ip 70:4C:A5:86:6E:00 up
(2/2) 0 days,0 hours,16 mins,4 secs
```

c. Shut down the ICL member ports using the `config switch physical-port`, `edit <member port#>`, `set status down`, `next`, and `end` commands. For example:

```
icl-sw1 # config switch physical-port
icl-sw1 (physical-port) # edit port27
icl-sw1 (port27) # set status down
icl-sw1 (port27) # n // repeat for each ICL member port
icl-sw1 (physical-port) # edit port28
icl-sw1 (port28) # set status down
icl-sw1 (port28) # next
icl-sw1 (physical-port) # end
```

d. Delete the original MCLAG-ICL trunk name on the switch using the `config switch trunk`, `delete <mclag-icl-trunk-name>`, and `end` commands. For example:

```
icl-sw1 # config switch trunk
icl-sw1 (trunk) # delete D483Z17000282-0
```

e. Use the `show switch trunk` command to verify that the trunk is deleted.

f. Create a new trunk for the MCLAG ICL using the original ICL trunk configuration collected in step 2b and the `set auto-isl 0` command in the configuration. For example:

```
icl-sw1 # config switch trunk

icl-sw1 (trunk) # edit MCLAG-ICL
new entry 'MCLAG-ICL' added
icl-sw1 (MCLAG-ICL) #set mode lacp-active
icl-sw1 (MCLAG-ICL) #set members "port27" "port28"
icl-sw1 (MCLAG-ICL) #set mclag-icl enable
icl-sw1 (MCLAG-ICL) # end
```

g. Use the `show switch trunk` command to check the trunk configuration.

h. Start the trunk member ports by using the `config switch physical-port`, `edit <member port#>`, `set status up`, `next`, and `end` commands. For example:

```
icl-sw1 # config switch physical-port
```

```
icl-sw1 (physical-port) # edit port27
icl-sw1 (port27) # set status up
icl-sw1 (port27) # next // repeat for each trunk member port
icl-sw1 (physical-port) # edit port28
icl-sw1 (port28) # set status up
icl-sw1 (port28) # end
```

NOTE: Follow steps 2a through 2h on both switches.

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

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

4. Check the configuration and status on both MCLAG-ICL switches
   a. Enter the `show switch trunk`, `diagnose switch mclag icl`, and `diagnose switch trunk summary <new-trunk-name>` commands. For example:

```
icl-sw1 # show switch trunk
 config switch trunk
 <snip>
 edit "MCLAG-ICL"
 set mode lacp-active
 set mclag-icl enable
 set members "port27" "port28"
 next
 end

 icl-sw1 # show switch interface MCLAG-ICL
 config switch interface
 edit "MCLAG-ICL"
 set native-vlan 4094
 set allowed-vlans 1,100,2001-2060,4093
 set dhcp-snooping trusted
 set stp-state disabled
 set igmp-snooping-flood-reports enable
 set mcast-snooping-flood-traffic enable
 set snmp-index 56
 next
 end

 icl-sw1 # diagnose switch mclag icl
 MCLAG-ICL
 icl-ports 27-28
 egress-block-ports 3-4,7-12,47-48
 interface-mac 70:4c:a5:86:6d:e5
 lacp-serial-number FS1D483Z17000348
```

```
peer-mac 70:4c:a5:49:50:5
peer-serial-number FS1D483Z17000282
Local uptime 0 days 2h:11m:13s
Peer uptime 0 days 2h:11m: 7s
MCLAG-STP-mac 70:4c:a5:49:50:52
keepalive interval 1
keepalive timeout 60

Counters
received keepalive packets 5838
transmited keepalive packets 6279
received keepalive drop packets 27
receive keepalive miss 1

icl-sw1 # diagnose switch trunk summary MCLAG-ICL

Trunk Name Mode PSC MAC Status Up Time
_____ _____ _____ _____ _____ _____
_____ _____

MCLAG-ICL lacp-active(auto-isl,mclag-icl) src-dst-ip 70:4C:A5:86:6E:00 up(2/2)
0 days,1 hours,4 mins,57 secs
```

b. Compare the command results in step 4a with the command results in step 2b.

Executing custom FortiSwitch scripts

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

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

This section covers the following topics:

Creating a custom script

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

```
config switch-controller custom-command
   edit <cmd-name>
      set command "<FortiSwitch_command>"
   end
```

NOTE: You need to use `%0a` to indicate a return.

For example, use the custom script to set the STP max-age parameter on a managed FortiSwitch unit:

```
config switch-controller custom-command
   edit "stp-age-10"
      set command "config switch stp setting %0a set max-age 10 %0a end %0a"
   end
```

Executing a custom script once

After you have created a custom script, you can manually execute it on any managed FortiSwitch unit. Because the custom script is not bound to any switch, the FortiSwitch unit might reset some parameters when it is restarted.

Use the following syntax on the FortiGate unit to execute the custom script once on a specified managed FortiSwitch unit:

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

For example, you can execute the `stp-age-10` script on the specified managed FortiSwitch unit:

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

Binding a custom script to a managed switch

If you want the custom script to be part of the managed switch's configuration, the custom script must be bound to the managed switch. If any of the commands in the custom script are locally controlled by a switch, the commands might be overwritten locally.

Use the following syntax to bind a custom script to a managed switch:

```
config switch-controller managed-switch
   edit "<FortiSwitch_serial_number>"
      config custom-command
         edit <custom_script_entry>
            set command-name "<name_of_custom_script>"
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S524DF4K15000024"
      config custom-command
         edit 1
            set command-name "stp-age-10"
         next
      end
   next
end
```

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.

www.fortinet.com