FortiLink Guide (FortiOS 7.6.5)

FortiSwitchOS 7.6.5

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

February 10, 2026
FortiSwitchOS 7.6.5 FortiLink Guide (FortiOS 7.6.5)
11-765-1195722-20260210

TABLE OF CONTENTS

Change log

Date	Change Description
December 11, 2025	Initial document release for FortiOS 7.6.5
February 6, 2026	Removed “IGMP proxy must be enabled.” from the following sections: • MCLAG requirements on page 85 • Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 85 • Dual-homed servers connected to a pair of FortiSwitch units using an MCLAG on page 89 • Multi-tiered MCLAG with HA-mode FortiGate units on page 90
February 10, 2026	Updated the table in Introduction on page 12.

What’s new in FortiOS 7.6.5

The following list contains new managed FortiSwitchOS features added in FortiOS 7.6.5. Click on a link to navigate to that section for further information:

- When in FortiLink mode, the FSR-108F, FSR-112F-POE, and FSR-216F-POE models now support auto-negotiation in SGMII mode. For more details, see Configuring port speed and status on page 109.
- The switch controller now provides OS image signature verification for dual-signed images.

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”).

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, FG-50G, FortiGate-VM01	8
FGR-50G-5G, FGR-60F, FG-60F, FGR-60F-3G4G, FG-61F, FG-70F, FG-70G, FGR-70G, FG-71F, FG-80F, FG-80FB, FG-80FP, FG-81F, FG-81FP, FG-90G, FG-91G, FortiGate-VM02	24
FortiGate 100F, 101F	32
FG-120G, FG-121G	48
FortiGate 200E, FG-200G, 201E, 200F, 201F, 800D, 900D, FortiGate-VM04	64
FortiGate 300E to 500E	72
FortiGate 600E to 900E, 400F, 401F, 601F	96
FortiGate 1000D, 600F	128
FortiGate 900G, 901G, 1000F, 1001F, 1100E to 26xxF	196
FortiGate-3xxx 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.

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).

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

This section covers the following topics:

- Zero-touch management on page 14
- Zero-touch provisioning automation on page 15
- Configuring FortiLink on page 22
- Optional FortiLink configuration required before discovering and authorizing FortiSwitch units on page 33
- Discovering on page 41
- Optional FortiLink configuration on page 41

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).

Zero-touch provisioning automation

You can use automation stitches on managed switches for zero-touch provisioning. To configure an automation stitch, you specify a trigger and the action that is performed when the trigger occurs.

To use a switch-controller event for zero-touch provisioning:

1. Configure the trigger.
2. Configure the action.
3. Configure the automation stitch.

Configure the trigger

Starting in FortiOS 7.4.4, you can use the following switch-controller events as triggers for zero-touch provisioning:

- Log ID 32618—A switch port was exported to or returned from a virtual switch.
- Log ID 32619—A switch was added to or removed from a virtual port pool.
- Log ID 32620—A switch was added to a switch group.
- Log ID 32621—A switch was removed from a switch group.
- Log ID 32622—A switch was connected using FortiLink mode over a layer-2 or layer-3 network.

- Log ID 32623—The location of a switch changed.
- Log ID 32624—A new switch peer was detected (either a peer to a single switch or an MCLAG).

You can configure multiple fields for the automation trigger when the `event-type` is `event-log` and the `logid` is set. The action is only performed if all conditions are valid (using AND logic). For example, the following automation trigger requires both the log message to include `VRRP` and the interface to be `svi777` before the action is performed.

```
config system automation-trigger
   edit "VRRPlogtrigger"
      set event-type event-log
      set logid 10229
      config fields
         edit 1
            set name "msg"
            set value "*VRRP*"
         next
         edit 2
            set name "interface"
            set value "svi777"
         next
      end
   next
end
```

To configure the trigger:

```
config system automation-trigger
   edit <trigger_name>
      set description <string>
      set trigger-type event-based
      set event-type event-log
      set logid <log_ID>
      config fields
         edit <entry_ID>
            set name <string>
            set value <string>
         next
      end
   next
end
```

Variable	Description	Default
<trigger_name>	Name of the trigger configuration.	No default
description	Description of the trigger.	No default
trigger-type	Select the event-based trigger.	event-based
event-type	Select the use of a log ID as the trigger for the automation-stitch action.	event-log
logid <log_ID>	Enter the log ID to trigger the action. The range of values is 1-65535. If you use the full 10-digit entry, the first four digits are truncated.	0

Variable	Description	Default
trigger-frequency {daily | hourly | monthly | weekly}	Select whether the automation-stitch action is performed on a daily, hourly, monthly, or weekly basis. This option is available only when the `trigger-type` is set to `scheduled`.	daily
config fields	You can configure multiple fields for the automation trigger. The action is only performed if all conditions are valid (using AND logic).	
<entry_ID>	Enter an identifier for this entry.	No default
name <string>	Enter a name for this field.	No default
value <string>	Enter a value for this field. • Use an asterisk to match any character string of any length, including 0-characters long. For example, use `set value "*1567*"` to match values of `81567` and `156789`. • Use square brackets to match one of the multiple characters. For example, use `set value "[aA]dmin"` to match values of `admin` and `Admin`.	No default

Configure the action

You can specify one of the following actions:

- Run a CLI script.
- Send an email message.
- Display an alert in the dashboard.
- Send data to a uniform resource identifier (URI), such as an IP address or URL.

To configure the action:

```
config system automation-action
   edit <name>
      set action-type {alert | cli-script | email | webhook}
      set accprofile <string>
      set email-body <string>
      set email-from <string>
      set email-subject <string>
      set email-to <email_address>
      set http-body <request_body>
      set method {delete | get | patch | post | put}
      set minimum-interval <0-2592000>
      set port <1-65535>
      set protocol {http | https}
      set script <string>
      set uri <request_API_URI>
   next
end
```

Variable	Description	Default
<name>	Name of the action configuration.	No default
action-type {alert | cli-script | email | webhook}	Select the type of action to perform: • `alert`—Display an alert in the dashboard. • `cli-script`—Run a CLI script. • `email`—Send a notification email. • `webhook`—Send data to a uniform resource identifier (URI), such as an IP address or URL.	alert
accprofile <string>	Specify the access profile required to run the CLI script. This option is available only when `action-type` is set to `cli-script`.	No default
email-body <string>	Enter the body of the email. By default, the log message is sent. This option is available only when `action-type` is set to `email`.	%%log%%
email-from <string>	Enter the name of the sender of the email. This option is available only when `action-type` is set to `email`.	No default
email-subject <string>	Enter the subject of the email. This option is available only when `action-type` is set to `email`.	No default
email-to <email_address>	Enter the email address or addresses that the email will be sent to when automation stitch is triggered. This option is available only when `action-type` is set to `email`.	none
http-body <string>	If necessary, enter the request body. Use a serialized JSON string. This option is available only when `action-type` is set to `webhook`.	No default
method {delete | get | patch | post | put}	Select the request method: DELETE, GET, PATCH, POST, or PUT. This option is available only when `action-type` is set to `webhook`.	post
minimum-interval <0-2592000>	Select how many seconds must pass before the action can be performed again.	0
port <1-65535>	Enter the port number that this protocol will use. If the protocol is set to `http`, the default port is `80`. If the protocol is set to `https`, the default port is `443`. This option is available only when `action-type` is set to `webhook`.	80

Variable	Description	Default
protocol {http | https}	Enter the request protocol, either HTTP or HTTPS. This option is available only when `action-type` is set to `webhook`.	http
script <string>	Specify the name and path to the CLI script. This option is available only when `action-type` is set to `cli-script`.	No default
uri <string>	Required. Enter the uniform resource identifier (URI), such as an IP address or URL. This option is available only when `action-type` is set to `webhook`.	No default

Configure the automation stitch

To configure the automation stitch:

```
config system automation-stitch
   edit <name>
      set description <string>
      set status {enable | disable}
      set trigger <trigger_name>
      config actions
         edit <action_ID>
            set action <action_name>
            set delay <0-3600>
            set required {enable | disable}
         next
      end
   next
end
```

Variable	Description	Default
<name>	Name of the automation-stitch configuration.	No default
description <string>	Enter a description of the automation stitch.	No default
status {enable | disable}	Enable or disable this automation stitch.	enable
trigger <trigger_name>	Enter the name of the trigger for this automation stitch.	No default
<action_ID>	Enter an integer to identify the action.	0
action <action_name>	Enter the name of the action configuration for this automation stitch.	none
delay <0-3600>	Enter the number of seconds to delay before executing the automation stitch.	0
required {enable | disable}	Enable this option if the action is required or disable this option if the action is not required.	disable

Configuration example

In the following example, CLI scripts are used to configure new switches.

```
config system automation-trigger
   edit "SwitchAuthorized.Model.ALL"
      set event-type event-log
      set logid 32602
   next
   edit "SwitchAuthorized.Model.S108DV"
      set event-type event-log
      set logid 32602
      config fields
         edit 1
            set name "sn"
            set value "S108DV*"
         next
      end
   next
   edit "SwitchAuthorized.Model.FS1E48"
      set event-type event-log
      set logid 32602
      config fields
         edit 1
            set name "sn"
            set value "FS1E48*"
         next
      end
   next
end

config system automation-action
   edit "swc.assign.port.vlans"
      set action-type cli-script
      set script "config switch-controller managed-switch
         edit %%log.sn%%
            config ports
               edit \"port8\"
                  set vlan \"vlan.20\"
               next
            end
         next
      end"
      set accprofile "super_admin"
   next
   edit "swc.add.switch2.group-core"
      set action-type cli-script
      set script "config switch-controller switch-group
         edit \"core\"
            append members %%log.sn%%
         next
      end"
      set accprofile "super_admin"
   next
   edit "swc.setswitch.syslog"
      set action-type cli-script
      set script "config switch-controller managed-switch
         edit %%log.sn%%
            config remote-log
               edit \"syslogd\"
                  set status enable
                  set server \"192.168.0.111\"
               next
            end
         end"
      set accprofile "super_admin"
   next
   edit "swc.add.switch2.group-edge"
      set action-type cli-script
      set script "config switch-controller switch-group
         edit \"edge\"
            append members %%log.sn%%
         next
      end"
      set accprofile "super_admin"
   next
end

config system automation-stitch
   edit "ZT.OnboardNewSwitch.Global"
      set trigger "SwitchAuthorized.Model.ALL"
      config actions
         edit 1
            set action "swc.setswitch.syslog"
            set required enable
         next
      end
   next
   edit "ZT.OnboardNewSwitch.Edge"
      set trigger "SwitchAuthorized.Model.S108DV"
      config actions
         edit 1
            set action "swc.assign.port.vlans"
            set required enable
         next
         edit 2
            set action "swc.add.switch2.group-edge"
            set required enable
         next
      end
   next
   edit "ZT.OnboardNewSwitch.Core"
      set trigger "SwitchAuthorized.Model.FS1E48"
      config actions
         edit 2
            set action "swc.add.switch2.group-core"
            set required enable
         next
      end
   next
end
```

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 22

2. Configuring the FortiLink interface on page 22

3. Auto-discovery of the FortiSwitch ports on page 30

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 54.

This section covers the following topics:

- Using the FortiGate GUI on page 23
- Using the FortiGate CLI on page 24
- Custom FortiLink interfaces on page 25
- FortiLink interfaces using IPv6 on page 28

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. Click *Create New*.
3. 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*.
4. Configure the *IP/Network Mask* for your network.
5. Select *Automatically authorize devices*.
6. Click *OK*.

FortiLink split interface

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

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

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 85.

When the split interface is enabled and FortiLink neighbor detection is set to `fortilink`, the standby interface link is down. When FortiLink neighbor detection is set to `lldp`, the standby interface link is up, and LACP is inactive.

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
```

FortiLink neighbor detection

The FortiGate device can detect FortiSwitch units using two methods: FortiLink and LLDP. Starting in FortiOS 7.6.1, FortiLink neighbor detection uses LLDP by default.

To configure FortiLink neighbor detection:

```
config system interface
   edit "fortilink"
      set fortilink-neighbor-detect {fortilink | lldp}
   next
end
```

When you use LLDP, make sure that LLDP reception and transmission are enabled in the FortiLink interface:

```
config system interface
   edit "fortilink"
      set lldp-reception enable
      set lldp-transmission enable
   next
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
```

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.

> The FortiLink interface type is dependent upon the network topology to be deployed. See Determining the network topology on page 54.

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
```

FortiLink interfaces using IPv6

Starting in FortiOS 7.6.3 with FortiSwitchOS 7.2.3, you can use FortiLink to manage FortiSwitch units using IPv6 addresses. Previously, only IPv4 addresses were supported.

To use this feature, the following is required on the FortiGate device:

- FortiOS 7.6.3 or later
- You need to manually configure the IPv6 address for the FortiLink interface.
- You need to manually configure the DHCP pool.

To use this feature, the following is required on the managed FortiSwitch unit:

- FortiSwitchOS 7.2.3 or later
- You need to set the IPv4 mode for DHCP to static or to a similar setting because the DHCP IP acquisition for IPv4 occurs before IPv6. If the IPv6 DHCP IP address is acquired on an internal interface first, it takes precedence during the discovery phase broadcast.
- You need to configure the IPv6 NTP server.
- In layer-3 mode, only the static AC discovery mode (under the `config switch-controller global` command) is supported for IPv6.

FortiLink interfaces using IPv6 do not support zero-touch provisioning.

To configure a FortiLink interface with IPv6 in the FortiGate GUI:

1. Go to *System > Feature Visibility*, enable *IPv6*, and click *Apply*.
2. Go to *WiFi & Switch Controller > FortiLink Interface*.
3. Click *Create New*.
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*, right-click the FortiLink physical port, select *Edit*, delete the port from the *Interface members* field, and then select *OK*.
5. Configure the *IPv6 Address/Prefix* for your network.
6. Select *Automatically authorize devices*.
7. Click *OK*.

To configure a FortiLink interface with IPv6 in the FortiGate CLI:

Use the IPv6 options for configuring the system interface with the `config system interface` command. For example:

```
config system interface
   edit "fortilink"
      set vdom "root"
      set fortilink enable
      set ip 10.255.1.1 255.255.255.0
      set allowaccess ping fabric
      set type aggregate
      set member "a" "b"
      set lldp-reception enable
      set lldp-transmission enable
      set snmp-index 18
      set auto-auth-extension-device enable
      set fortilink-split-interface disable
      set switch-controller-nac "fortilink"
      set switch-controller-dynamic "fortilink"
      set swc-first-create 255
      config ipv6
         set ip6-address 2001:10:255:1::1/64
         set ip6-allowaccess ping https ssh http fabric
         set ip6-send-adv enable
         set ip6-other-flag enable
         set ip6-max-interval 60
         set ip6-min-interval 10
         config ip6-prefix-list
            edit 2001:10:255:1::/64
               set valid-life-time 86400
               set preferred-life-time 43200
            next
         end
      end
   next
end
```

To configure a DHCP server with IPv6 in the FortiGate GUI:

1. Go to *System > Feature Visibility*, enable *IPv6*, and click *Apply*.
2. Go to *WiFi & Switch Controller > FortiLink Interface*.
3. Select the FortiLink interface and click *Edit*.
4. Enable *DHCPv6 Server*.
5. Complete the fields as needed.
6. Click *OK*.

To configure a DHCP server with IPv6 in the FortiGate CLI:

You can configure a DHCP server using the `config system dhcp6 server` command. For example:

```
config system dhcp6 server
   edit 1
      set dns-service default
      set subnet 2001:db8:d0c:1::/64
      set interface "port5"
      config ip-range
```

```
            edit 1
               set start-ip 2001:db8:d0c:1::a
               set end-ip 2001:db8:d0c:1::f
            next
         end
      next
   end
```

3. Auto-discovery of the FortiSwitch ports

All FortiSwitch ports are enabled for auto-discovery by default. For details on how to connect the FortiSwitch topology, see Determining the network topology on page 54.

In FortiSwitchOS 7.0 and earlier releases, only 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-108F, FS-108F-POE, FS-108F-FPOE	port7-port10
FSR-216F-POE	port5-port12
FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE	port21-port28
FS-148E, FS-148E-POE	port21-port52
FS-148F, FS-148F-POE, FS-148F-FPOE	port48-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-424E-Fiber	port1-port30
FS-426E-FPOE-MG	port23-port30
FS-524D, FS-524D-FPOE	port21-port30
FS-548D	port39-port54
FS-548D-FPOE, FS-548DN	port45-port54
FS-1024E, FS-T1024E, FS-T1024F-FPOE	port1-port26
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.

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

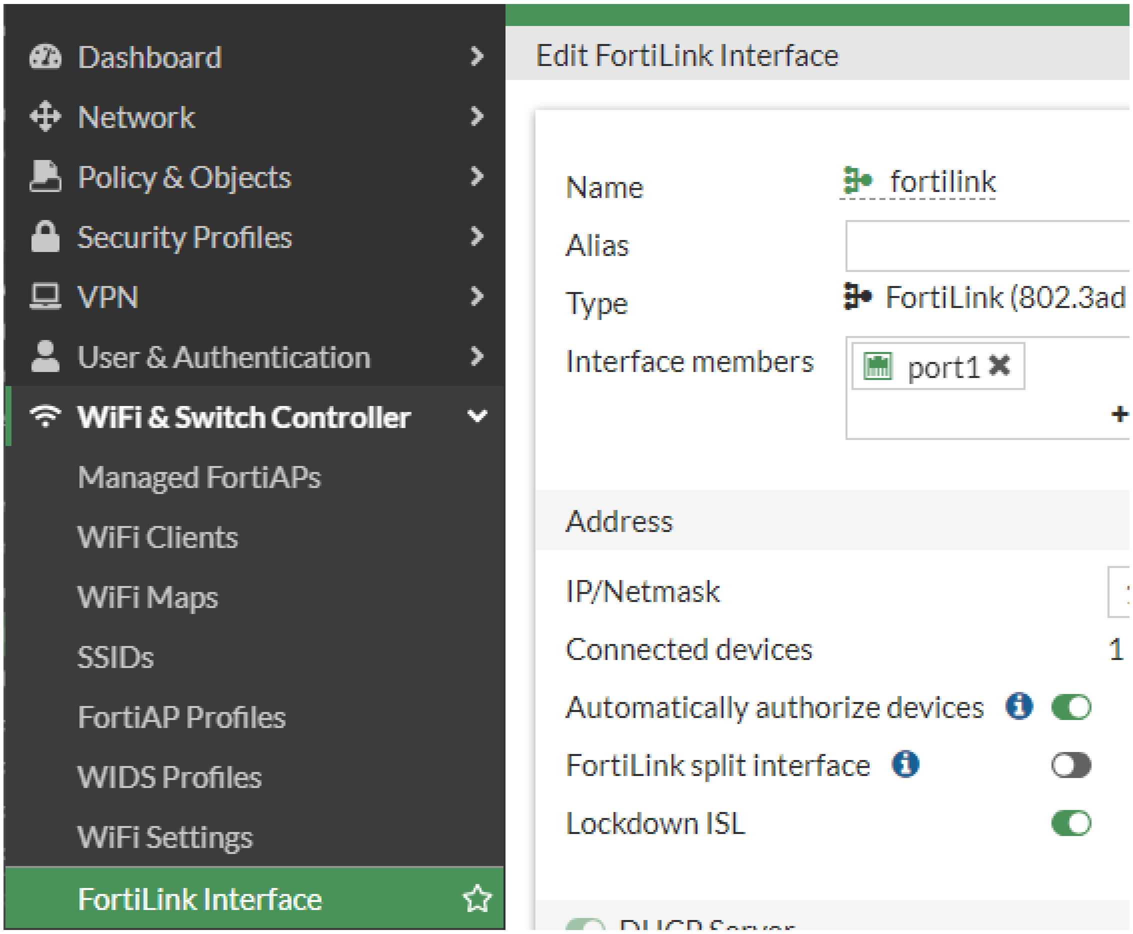
In some cases, you might want to manually create an ISL trunk, for example, for FortiLink mode over a point-to-point layer-2 network or for FortiLink mode over a layer-3 network. You can also enable or disable automatic VLAN configuration on the manually created (static) ISL trunk. The static ISL feature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

To manually create an ISL trunk in the CLI:

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

Locking down the ISL trunk in the GUI (when there is a single FortiLink interface):

1. Go to *WiFi & Switch Controller > FortiLink Interface*.
2. Enable *Lockdown ISL*.



Name: fortilink

Alias:

Type: FortiLink (802.3ad

Interface members: port1 ✖

IP/Netmask:

Connected devices: 1

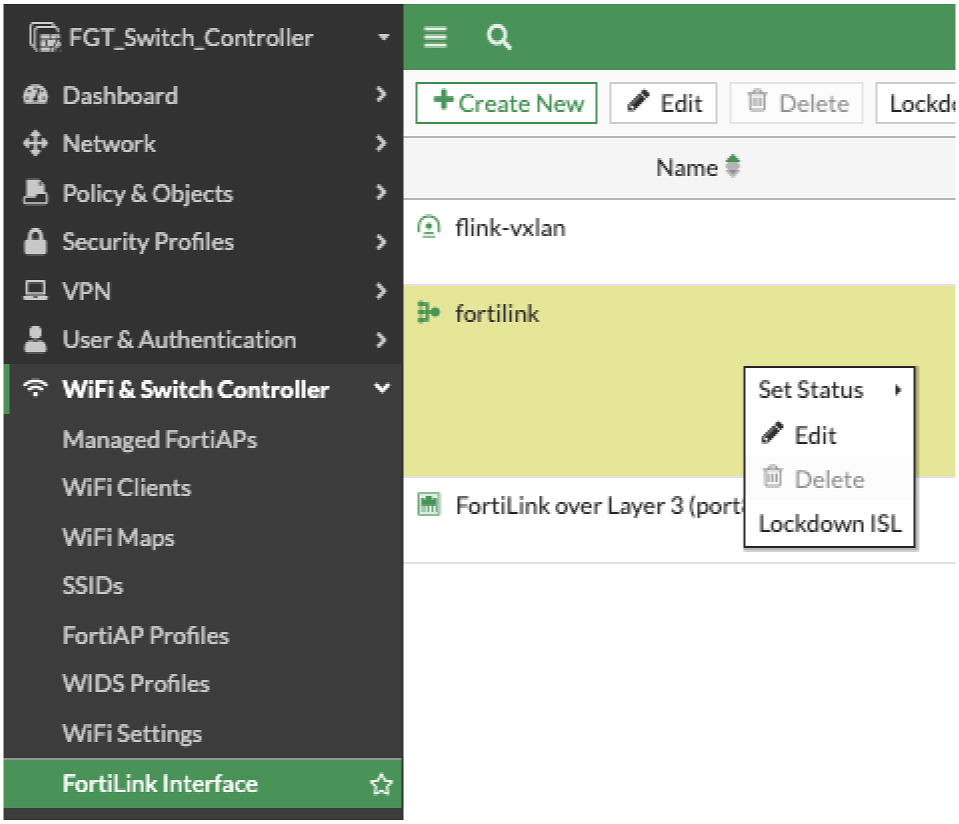
Automatically authorize devices ●

FortiLink split interface ○

Lockdown ISL ●

Locking down the ISL trunk in the GUI (when there are two or more FortiLink interfaces):

1. Go to *WiFi & Switch Controller > FortiLink Interface*.
2. Right-click the FortiLink interface in the *Name* column.
3. Click *Lockdown ISL*.



Locking down ISLs and ICLs is one of the recommendations in the Security Rating report (*Security Fabric > Security Rating*).

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 on page 34
- VLAN interface templates for FortiSwitch units on page 34

- Preventing automatically created VLANs on page 37
- Automatic provisioning of FortiSwitch firmware upon authorization on page 38

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

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>
   set nac-segment <template>
end
```

VLAN template	Description	Default IP address
default-vlan <template>	Default VLAN assigned to all switch ports upon discovery.	Not applicable
quarantine <template>	VLAN for quarantined traffic.	10.255.11.1/24
rspan <template>	VLAN for RSPAN/ERSPAN mirrored traffic.	10.255.12.1/24
voice <template>	VLAN dedicated for voice devices.	Not applicable
video <template>	VLAN dedicated for video devices.	Not applicable
nac <template>	VLAN for NAC onboarding devices.	Not applicable
nac-segment <template>	VLAN for the NAC segment primary interface.	10.255.13.1/24

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 `10.255.0.0/16`.

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 unit 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
```

Preventing automatically created VLANs

When a FortiSwitch unit is discovered, the switch controller automatically creates VLANs for quarantined traffic, RSPAN and ERSPAN mirrored traffic, voice devices, video devices, and NAC onboarding devices. You can use the CLI to prevent the switch controller from automatically creating VLANs.

When you disable the automatic creation of VLANs, only the default VLAN is created. All VLANs are hidden, except for the default VLAN. Features that use unassigned VLANs do not work unless you manually configure them.

This feature applies only to new FortiLink configurations that use FortiOS 7.6.3 and later. By default, the automatic creation of VLANs is enabled.

To prevent the switch controller from automatically creating VLANs:

```
config switch-controller initial-config vlans
   set optional-vlans disable
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 on page 41
- Preparing the FortiSwitch unit on page 41

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 on page 42
- Using the FortiSwitch serial number for automatic name resolution on page 42
- Changing the admin password on the FortiGate for all managed FortiSwitch units on page 43
- Disabling the FortiSwitch console port login on page 44
- Using automatic network detection and configuration on page 44
- Limiting the number of parallel processes for FortiSwitch configuration on page 45
- Configuring access to management and internal interfaces on page 45
- Enabling FortiLink VLAN optimization on page 46

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
```

Starting in FortiOS 7.6.1, empty passwords for the FortiSwitch admin account are no longer allowed. If a switch has no admin password set when it is authorized, the FortiGate device will generate an admin password for the FortiSwitch unit. FortiSwitch units that already have an admin password configured will remain unaffected.

To log in to the FortiSwitch CLI or GUI, you can configure the switch profile (under the `config switch-controller switch-profile` command) with an admin password on the FortiGate device, which is the Fortinet-recommended FortiLink setup.

A new command has been introduced to retain the password of the managed switch during deauthorization or to reset the managed switch to factory default settings during deauthorization. This command helps to clear the previously FortiGate-set random password on the managed switch when it is deauthorized.

To reset the switch to factory default settings when the switch is deauthorized:

```
config switch-controller global
   set switch-on-deauth factory-reset
end
```

To retain the password for the FortiSwitch admin account when the switch is deauthorized:

```
config switch-controller global
```

```
   set switch-on-deauth no-op
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, ICI, or FortiLink interface:

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

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

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

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

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

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

VLAN optimization is enabled by default.

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

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

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

VLAN pruning

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

To enable VLAN pruning in FortiOS:

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

To disable VLAN pruning in FortiOS:

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

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

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

For example:

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

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

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

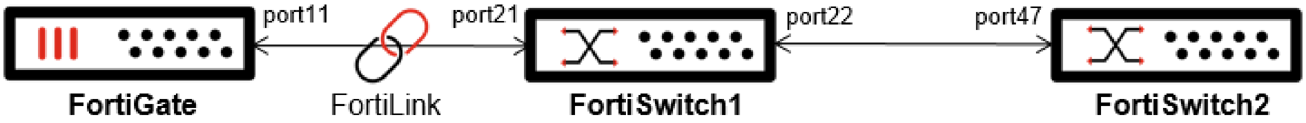
```
diagnose switch vlan-pruning protocol-packet stats [<interface_name>]
```

For example:

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

Configuration example

In the following example, a FortiGate device manages two FortiSwitch units.



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

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

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

```
end

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

2. Enable VLAN pruning on the FortiGate device.

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

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

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

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

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 358.

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.

Improving the FortiLink connection

Starting in FortiOS 7.4.0, there are two CLI commands under `config switch-controller system` that you can use to improve the FortiLink connection:

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

FortiLink with HTTPS

Starting in FortiOS 7.4.2 with FortiSwitchOS 7.4.2, you can use FortiLink with HTTPS to manage FortiSwitch units. Using FortiLink with HTTPS simplifies the management process and improves the user experience and efficiency.

The FortiGate device supports using both the CAPWAP protocol and HTTPS at the same time. Each FortiSwitch unit supports using the CAPWAP protocol or HTTPS; you cannot use both protocols to manage the same FortiSwitch unit.

FortiLink with HTTPS uses the same technology as FortiLAN Cloud to operate over both layer 2 and layer 3.

When you are using FortiLink with HTTPS to manage FortiSwitch units, the same FortiLink features are supported as when you are using FortiLink with the CAPWAP protocol.

Using FortiSwitchOS 7.4.7, 7.6.2, or later, you can specify the source IP address (IPv4) in a FortiSwitch unit for layer-3 FortiLink with HTTPS tunnel mode (in-band management and out-of-band management). This feature requires FortiSwitchOS 7.4.7, 7.6.2, or later but supports all versions of FortiOS. The `source-ip` value must match the switch interface IP address. In addition, this feature supports layer-3 FortiLink only. For example, configure the following commands in the FortiSwitchOS CLI:

```
config system flan-cloud
   set interval 3
   set name "10.105.20.254"
   set port 443
   set service-type fortilink-https
   set source-ip 3.4.5.6 // the source IP address is a loopback interface
   set status enable
end

config system interface
   edit "mgmt"
      set allowaccess ping https ssh
      set type physical
      set snmp-index 31
   next
   edit "internal"
      set mode dhcp
      set allowaccess ping https ssh
      set type physical
      set snmp-index 30
      set defaultgw enable
   next
   edit "loop-back"
      set ip 3.4.5.6 255.255.255.255 // source IP address
      set type loopback
      set snmp-index 32
   next
end
```

To use FortiLink with HTTPS:

1. On the FortiSwitch unit, enable the FortiLink HTTPS management mode (CAPWAP remains enabled):
```
config switch-controller global
   set mgmt-mode https
end
```
2. On the FortiSwitch unit, set the FortiLAN Cloud service to FortiLink with HTTPS, enter the FortiLink IPv4 address, and enable the status.
```
config system flan-cloud
   set service-type fortilink-https
   set name <FortiLink_IPv4_addresss>
   set status enable
end
```
3. On the FortiGate device, authorize the FortiSwitch unit if it has not already been authorized:
```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set fsw-wan1-admin enable
   next
end
```

4. On the FortiGate device, check that the tunnel has been established to allow FortiLink with HTTPS:
   `execute switch-controller get-conn-status`
   For example:

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

FortiLink interface : port11
SWITCH-ID         VERSION           STATUS         FLAG   ADDRESS        JOIN-TIME
 SERIAL
S524DN4K16000116  v7.4.0 (0796)     Authorized/Up   2T   10.255.1.2      Mon Dec 18 15:41:34
2023    S524DN4K16000116
S248EPTF18001384  v7.4.1 (787)      Authorized/Up   2    10.255.1.5      Mon Dec 18 15:41:43
2023    S248EPTF18001384
S248EPTF18001827  N/A               Discovered/Down 2                    N/A
      S248EPTF18001827
S124EN5918003682  N/A               Discovered/Down 2                    N/A
      S124EN5918003682

       Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=config sync error,
2=L2, 3=L3, V=VXLAN, T=tunnel, X=External
       Managed-Switches: 4 (UP: 2 DOWN: 2 MAX: 72)
```

5. On the FortiSwitch unit, check that FortiLAN Cloud has established the FortiLink connection:
   `S224DF3X15000367 # get system flan-cloud-mgr connection-info`
   For example:

```
S524DN4K16000116 # get system flan-cloud-mgr connection-info

Service Name:            : FortiLink
User Account-ID          : 0
SSL verify Code          : ok
Access Service           : IP= 10.255.1.1, Port= 443, Connected on: 2023-12-18 15:41:33
Bootstrap Service        : hostname= , Port= 0

State-Machine            : State= FLAN_MGR_STATE_READY, Event= EV_READY_SSL_SESSION_ESTD

SSL Local End-Point      : Interface: internal,  IP: 10.255.1.2
SSL Tunnel Uptime        : Days: 0  Hours: 0 Mins: 2 [Connected @2023-12-18 15:41:33]
SSL Tunnel stats         : restart-count= 279, Restart Reason= Boot-Strap fails to setup SSL to
Cloud

Stats:
========
Switch  Keep Alive  Tx/Reply := 3 / 1
Manager Keep Alive  Rx/Error := 2 / 0

Socks   Req Rx/Last Stream-ID  := 1193 / 5
Reset   Req Rx/last Stream-ID  := 137 / 276
Goaway  Req Rx  := 0
Unknown Req Rx  := 0

Syslog FD/Tx/Err  := 10 / 62 / 0
```

```
FortiLink details
=======================
stream_id : 5
online state_id : 7
localSock fd : 11
stpTelSock fd : 12
dhcpTelSock fd : 13
igmpsTelSock fd : 14
macSock fd : 15
cmfSock fd : 16
FortiGate - no response counter : 0
FortiGate - [Last no response time @1969-12-31 16:00:00]
online TX counter : 6
online RX_ACK counter : 6
online RX_NACK counter : 0
topology req : 8
topology resp : 4
system telemetry req : 8
system telemetry resp : 3
interface telemetry req : 2
interface telemetry resp : 2
mac telemetry req : 0
mac telemetry resp : 0
dot1x user req : 0
dot1x user resp : 0
lldp nbr req : 0
lldp nbr resp : 0
mac cache req : 0
mac cache resp : 0
trunk state req : 21
trunk state resp : 7
port state req : 4
port state resp : 2
poe status req : 0
poe status resp : 0

Used SOCKS stream-id:
=======================
SID       SockFd    Proxy-Ports            State         Description


__________________________________________________________________
1         0         UNKNOWN:0<-->0         DATA         BOOTSTRAP
3         0         UDP:9514<-->0          DATA         SYSLOG DATA
5         0         UNKNOWN:0<-->0         DATA         FORTILINK
```

To log in from the FortiGate device to a switch managed by FortiLink with HTTPS:

```
execute switch-controller ssh <FortiSwitch_user_name> <FortiSwitch_serial_number>
```

For example:

```
execute switch-controller ssh admin S524DF4K15000024
```

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.

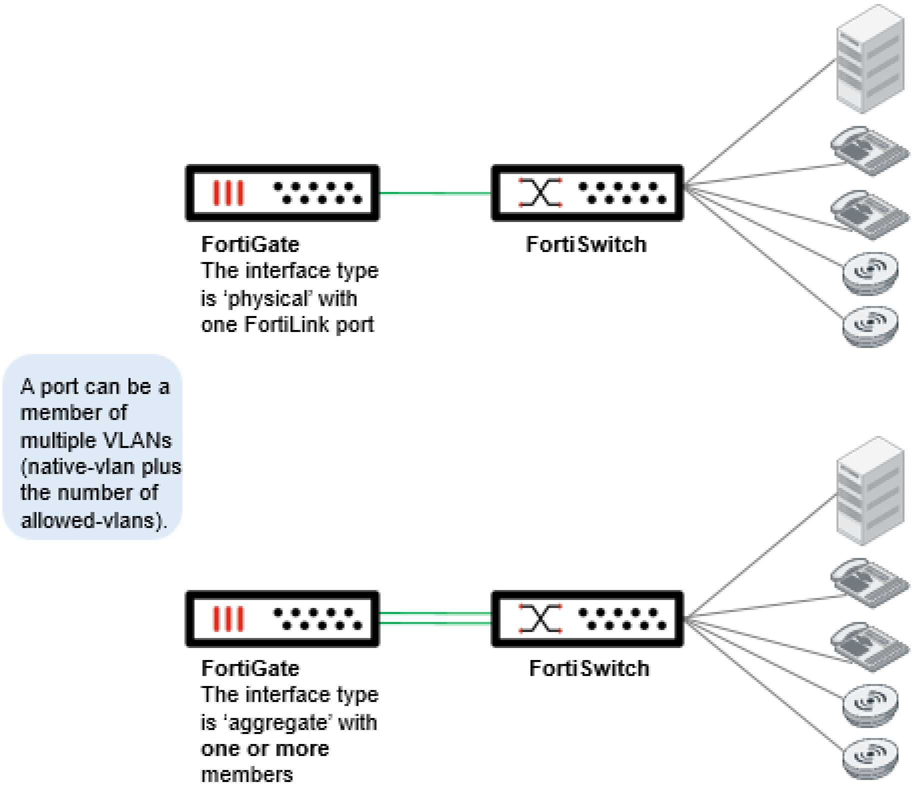
For any of the topologies:

- 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 page 55
- Single FortiGate unit managing a stack of several FortiSwitch units on page 56
- HA-mode FortiGate units managing a single FortiSwitch unit on page 57
- HA-mode FortiGate units managing a stack of several FortiSwitch units on page 58
- HA-mode FortiGate units managing a FortiSwitch two-tier topology on page 59
- Single FortiGate unit managing multiple FortiSwitch units (using a hardware or software switch interface) on page 60
- HA-mode FortiGate units using hardware-switch interfaces and STP on page 61
- FortiLink over a point-to-point layer-2 network on page 62
- FortiLink mode over a layer-3 network on page 63
- Managing FortiSwitch units on VXLAN interfaces on page 69
- Switch redundancy with MCLAG on page 75

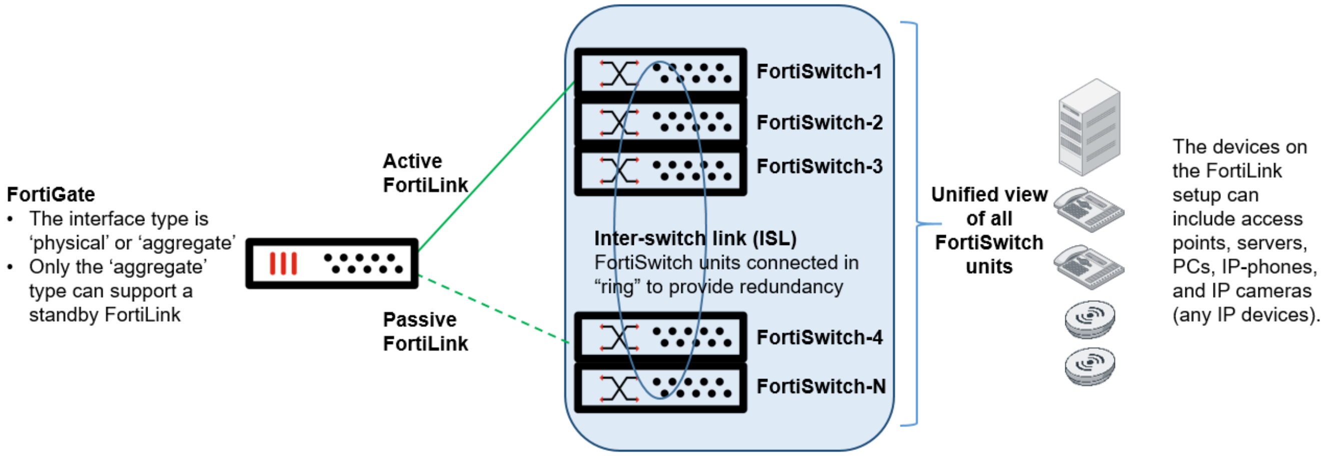
Single FortiGate managing a single FortiSwitch unit


FortiGate
The interface type is 'physical' with one FortiLink port
FortiSwitch
A port can be a member of multiple VLANs (native-vlan plus the number of allowed-vlans).
FortiGate
The interface type is 'aggregate' with one or more members
FortiSwitch

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.

For the aggregate interface, you must disable the split interface on the FortiGate unit.

Single FortiGate unit managing a stack of several FortiSwitch units


FortiGate
• The interface type is 'physical' or 'aggregate'
• Only the 'aggregate' type can support a standby FortiLink
Active FortiLink
Passive FortiLink
FortiSwitch-1
FortiSwitch-2
FortiSwitch-3
Inter-switch link (ISL)
FortiSwitch units connected in "ring" to provide redundancy
FortiSwitch-4
FortiSwitch-N
Unified view of all FortiSwitch units
The devices on the FortiLink setup can include access points, servers, PCs, IP-phones, and IP cameras (any IP devices).

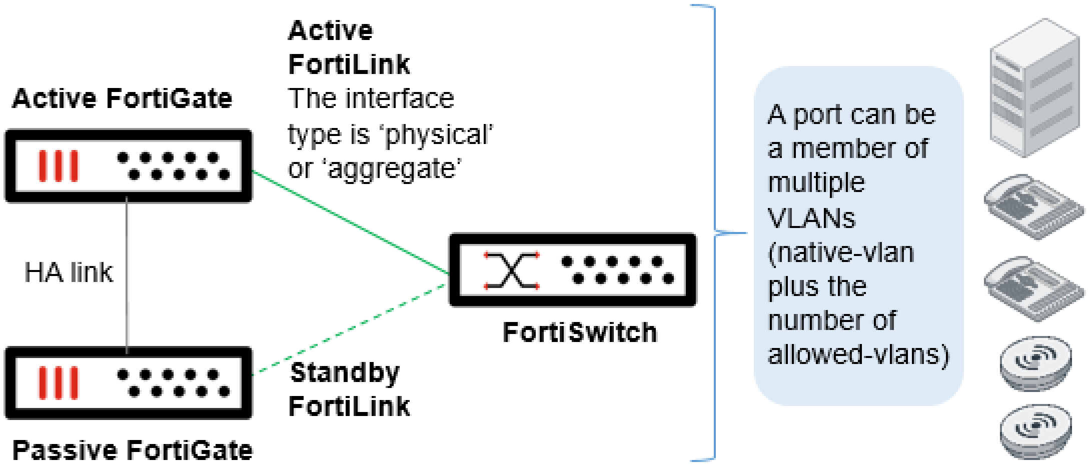
The FortiGate unit connects directly to one FortiSwitch unit using a physical or aggregate interface. The remaining FortiSwitch units connect in a ring using inter-switch links (that is, ISL).

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:

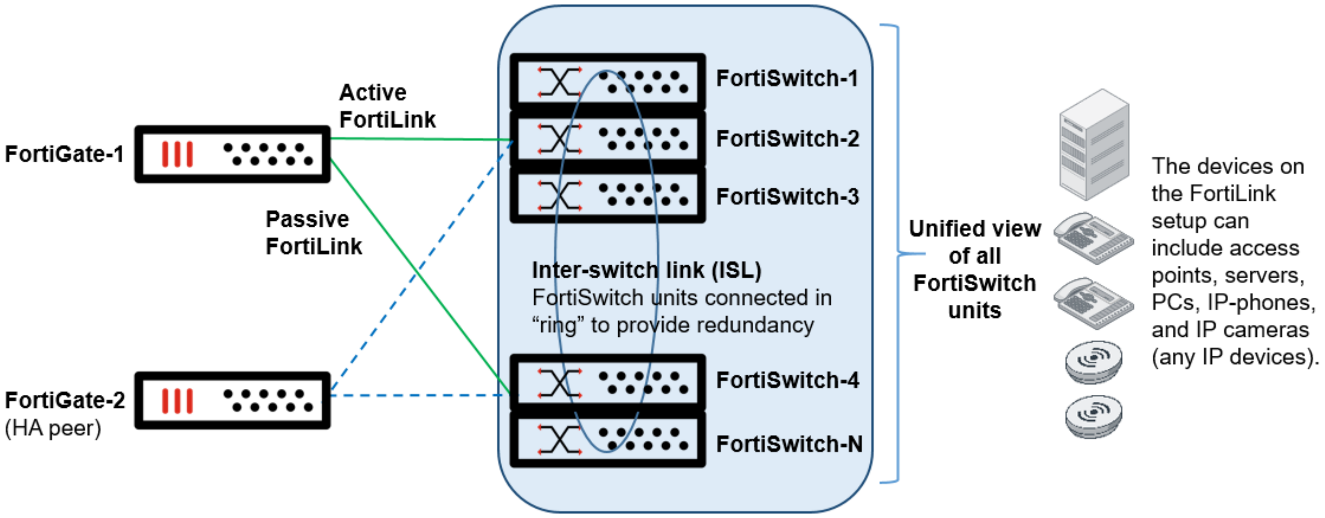
- When you are using the aggregate interface on the FortiGate unit for the FortiLink interface and you create a FortiLink split interface (with the `set fortilink-split-interface enable` command) , the LACP mode of the FortiLink aggregate interface must be set to active (with the `set lacp-mode active` command). See Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 85 for details.
- Do not create loops or rings with the FortiGate unit in the path.

HA-mode FortiGate units managing a single FortiSwitch unit


Active FortiGate
Active FortiLink
The interface type is 'physical' or 'aggregate'
HA link
FortiSwitch
Standby FortiLink
Passive FortiGate
A port can be a member of multiple VLANs (native-vlan plus the number of allowed-vlans)

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.

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

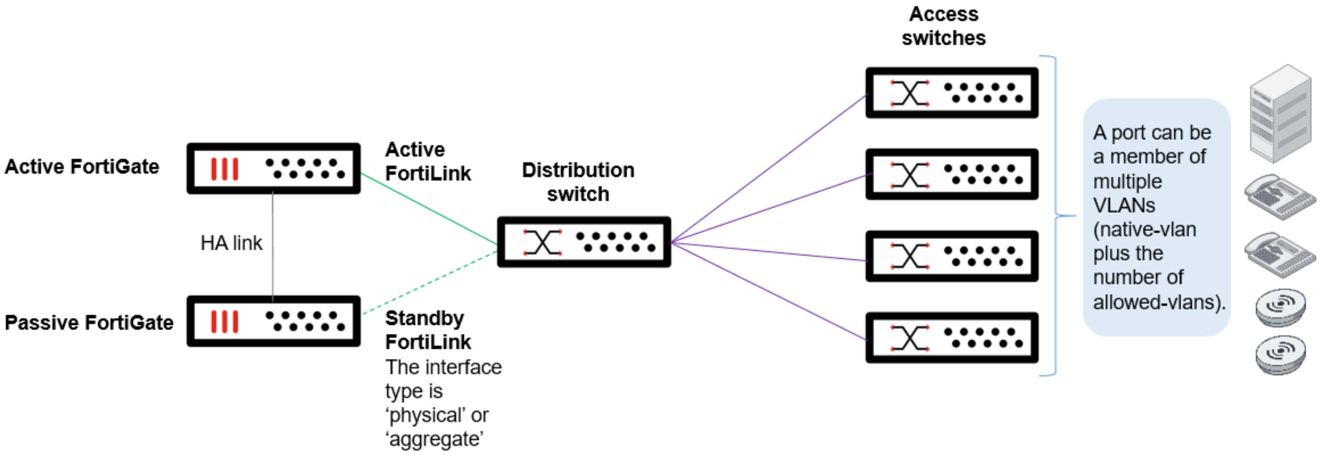

Active
FortiLink
FortiGate-1
Passive
FortiLink
FortiGate-2
(HA peer)
FortiSwitch-1
FortiSwitch-2
FortiSwitch-3
Inter-switch link (ISL)
FortiSwitch units connected in "ring" to provide redundancy
FortiSwitch-4
FortiSwitch-N
Unified view of all FortiSwitch units
The devices on the FortiLink setup can include access points, servers, PCs, IP-phones, and IP cameras (any IP devices).

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). The FortiLink split interface can be disabled later if you enable an MCLAG. See Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 85.

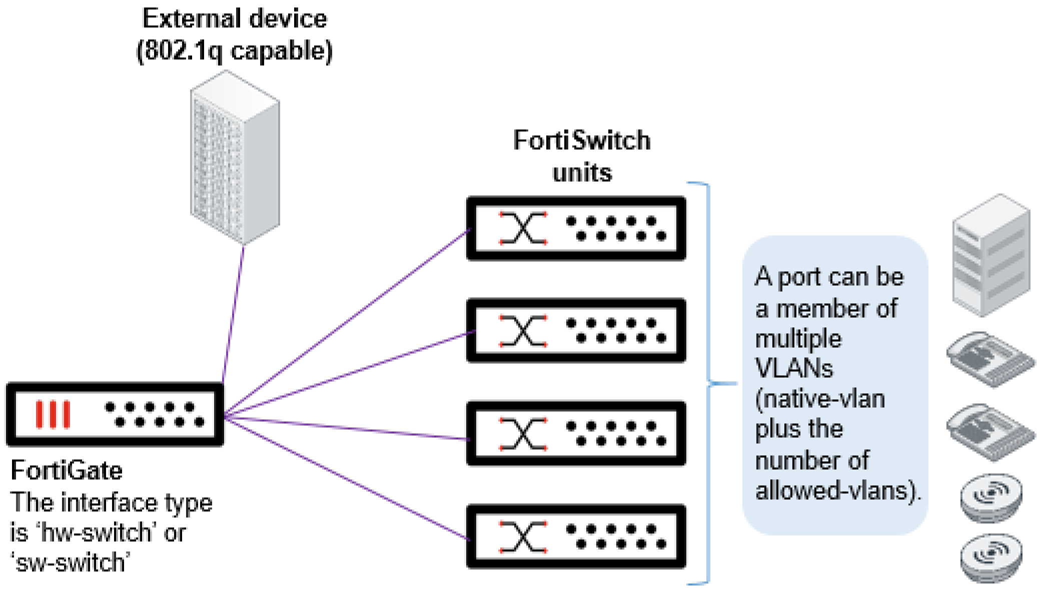
When you are using the aggregate interface on the FortiGate unit for the FortiLink interface and if you are not using MCLAG on the FortiSwitch units, the FortiLink split interface needs to be enabled (with the `set fortilink-split-interface enable` command) and the LACP mode of the FortiLink aggregate interface must be set to active (with the `set lacp-mode active` command).

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


Access switches
Active FortiGate
Active FortiLink
Distribution switch
HA link
Passive FortiGate
Standby FortiLink
The interface type is ‘physical’ or ‘aggregate’
A port can be a member of multiple VLANs (native-vlan plus the number of allowed-vlans).

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.

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


External device
(802.1q capable)
FortiSwitch
units
A port can be a member of multiple VLANs (native-vlan plus the number of allowed-vlans).
FortiGate
The interface type is 'hw-switch' or 'sw-switch'

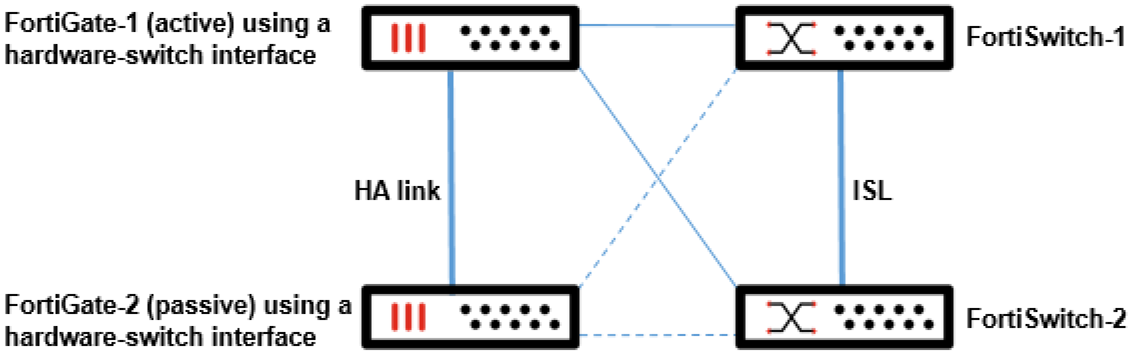
The FortiGate unit connects directly to each FortiSwitch unit. Each of these FortiLink ports is added to the logical hardware-switch or software-switch interface on the FortiGate unit.

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


FortiGate-1 (active) using a hardware-switch interface
FortiSwitch-1
HA link
ISL
FortiGate-2 (passive) using a hardware-switch interface
FortiSwitch-2

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.

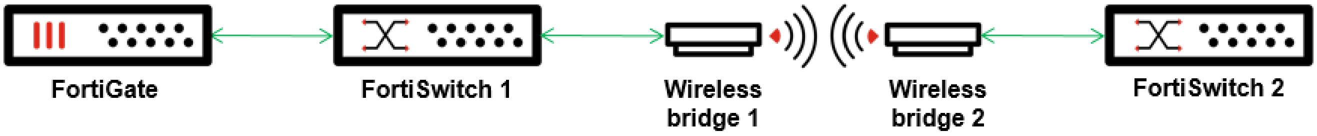
For this network topology to function, use the following commands on each FortiLink hardware-switch interface:

```
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). The LLDP destination MAC address is changed to the broadcast MAC address to bypass middle layer-2 devices. For example:

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-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.

Using FortiSwitchOS 7.4.7, 7.6.2, or later, you can specify the source IP address (IPv4 and IPv6) in a FortiSwitch unit for layer-3 FortiLink with CAPWAP tunnel mode (in-band management and out-of-band management). This feature requires FortiSwitchOS 7.4.7, 7.6.2, or later but supports all versions of FortiOS. The `source-ip` value must match the switch interface IP address. For example, configure the following commands in the FortiSwitchOS CLI:

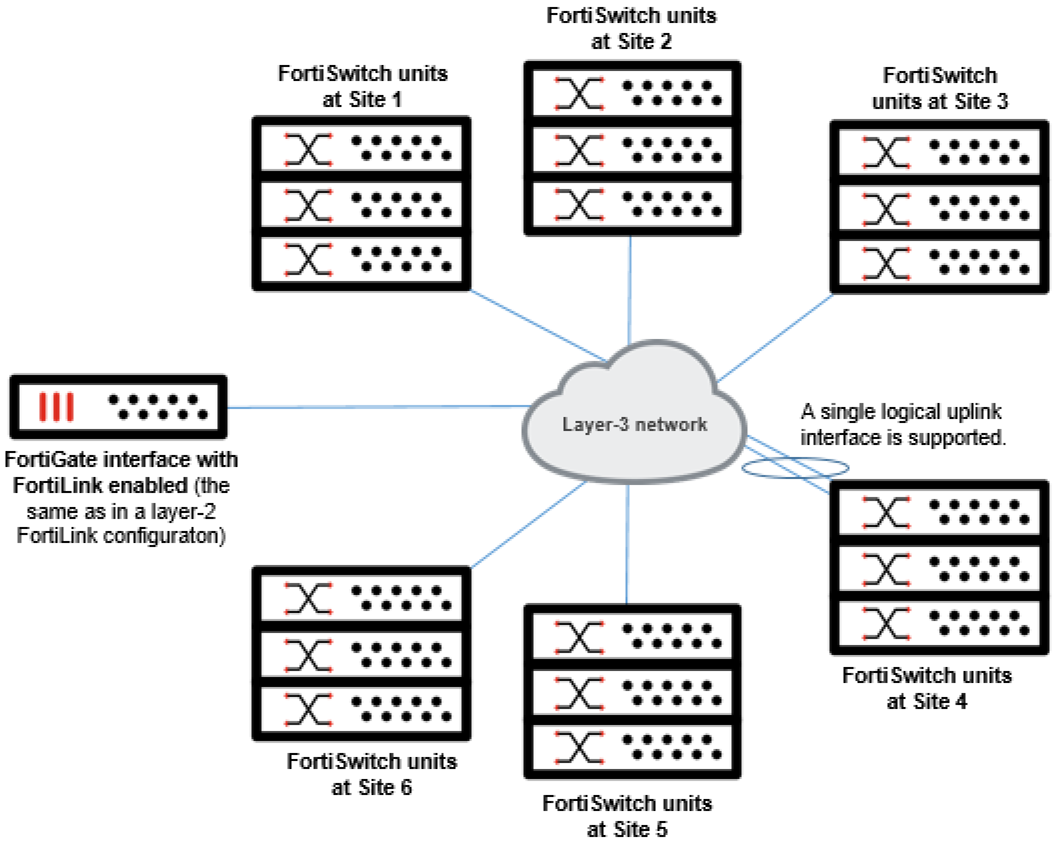
```
config switch-controller global
   set ac-discovery-type static
   set source-ip 3.4.5.6
   config ac-list
      edit 1
         set ipv4-address 1.1.1.1
      next
   end
end
```

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


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

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

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

1. Reset the FortiSwitch to factory default settings with the `execute factoryreset` command.
2. 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.
   NOTE: Starting in FortiOS 7.4.1 with FortiSwitchOS 7.4.1, when using FortiLink mode over a layer-3 network and DHCP discovery with DHCP option 138, the top FortiSwitch unit (with the _FlinkDhcpDisc_ trunk) will now automatically have a Spanning Tree Protocol (STP) priority of 24576, instead of an STP priority of 32768.

   #### To use DHCP discovery:

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

```
end
```

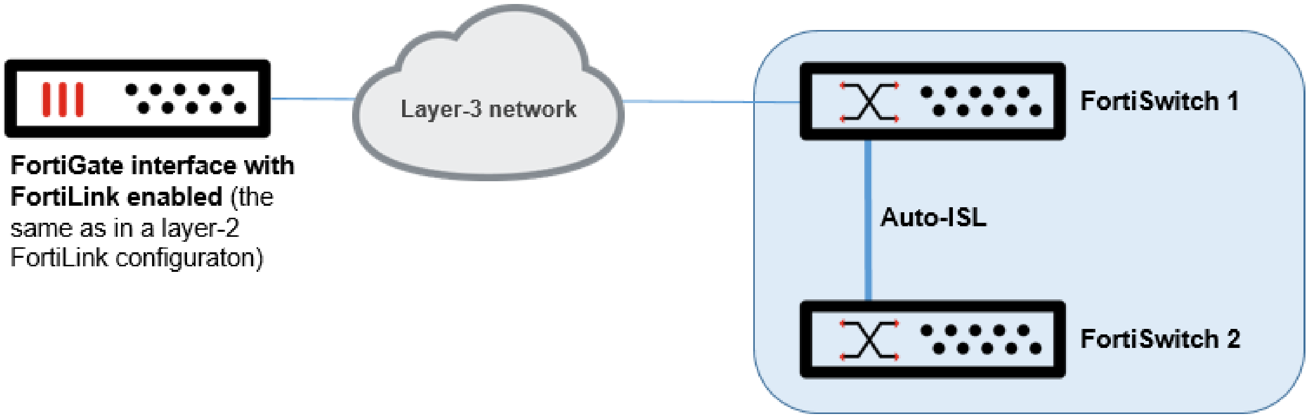
To use static discovery:

```
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}
      set members <switch_ports>
   next
end
```

NOTE:

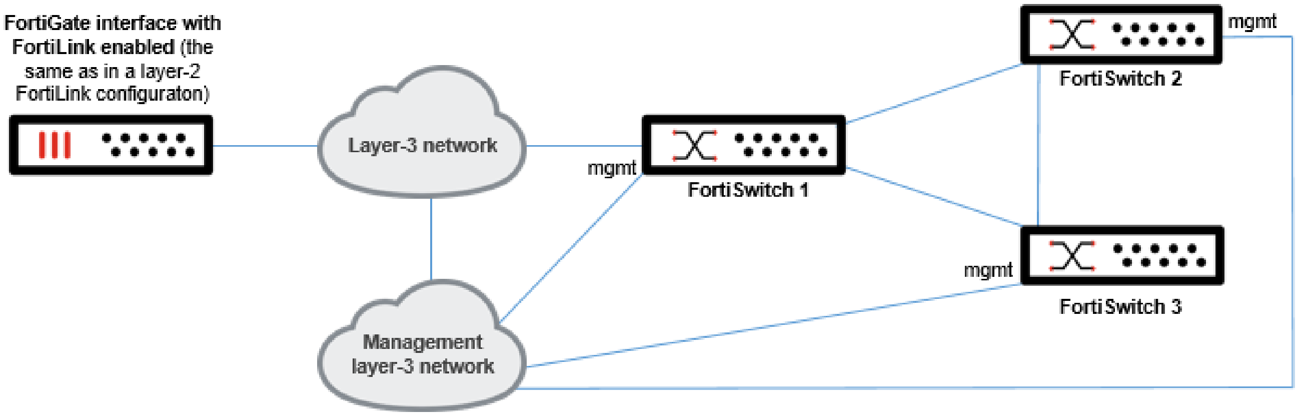
- Make certain that each FortiSwitch unit can successfully ping the FortiGate unit.
- The NTP server must be configured on the FortiSwitch unit either manually or provided by DHCP. The NTP server must be reachable from the FortiSwitch unit.
- In addition to the two layer-3 discovery modes (DHCP and static),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


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

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


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

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

Other topologies

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

If you have two FortiSwitch units separately connected to two different intermediary routers or switches 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:

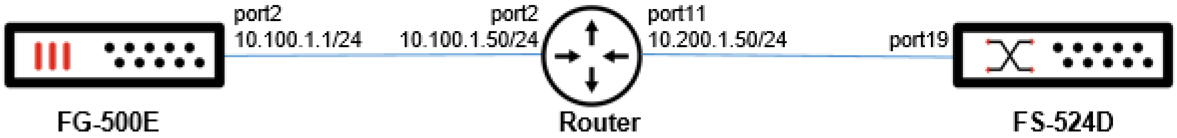
- FortiSwitch NAC is not supported.
- No layer-2 data path component, such as VLANs, can span across layer 3 between the FortiGate unit and the FortiSwitch unit.
- All FortiSwitch units within an FortiSwitch island must be connected to the same FortiGate unit.

- 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
```

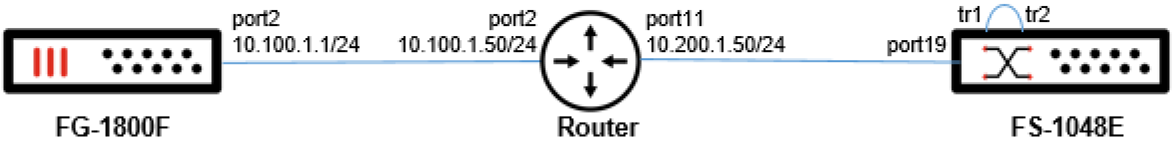
4. Configure a static route.

```
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
    ```

Verifying VXLAN management

Starting in FortiOS 7.4.0 with FortiSwitchOS 7.4.0, you can use the `execute switch-controller get-conn-status` command to show when the managed FortiSwitch unit is controlled by VXLAN.

In the following example, the V flag indicates that the managed FortiSwitch unit is controlled by VXLAN:

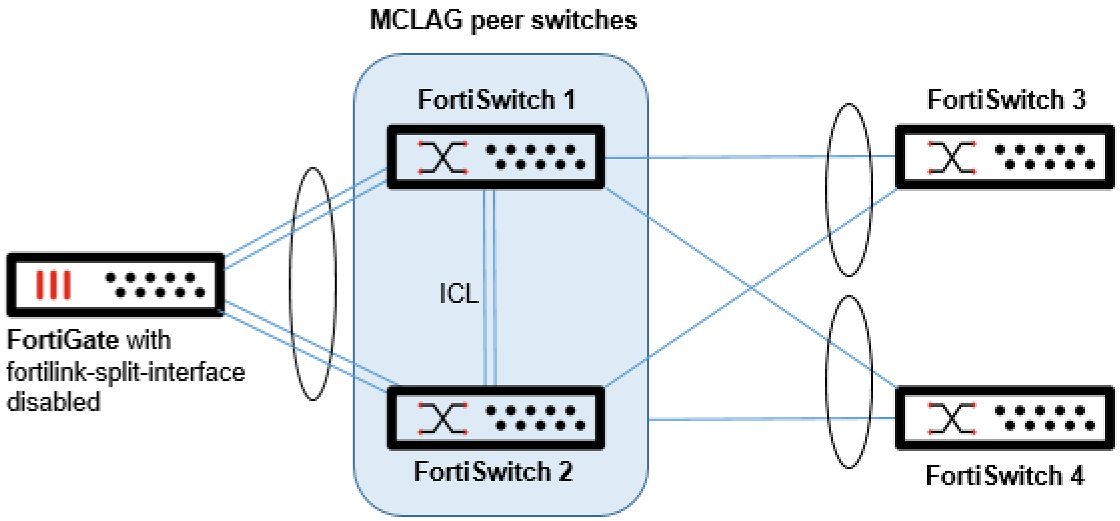
```
FGVMULTM22004064 # execute switch-controller get-conn-status
Managed-devices in current vdom root:

FortiLink interface : vx100
SWITCH-ID VERSION STATUS FLAG ADDRESS JOIN-TIME SERIAL
S108DV3A17000071 v7.2.0 (5029) Authorized/Up V 1.2.3.4 Wed Mar 29 17:23:24 2023 S108DV3A17000071



 Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=config sync error, 3=L3,
V=VXLAN
 Managed-Switches: 1 (UP: 1 DOWN: 0 MAX: 300)
```

Switch redundancy with MCLAG

The following network topologies provide switch redundancy with MCLAG:

- Standalone FortiGate unit with dual-homed FortiSwitch access on page 76
- HA-mode FortiGate units with dual-homed FortiSwitch access on page 77
- HA-mode one-tier MCLAG on page 78
- FortiLink with an HA cluster of four FortiGate units on page 79
- HA-mode FortiGate units in different sites on page 81
- Isolated LAN/WAN with multiple FortiLink interfaces on page 82
- Three-tier FortiLink MCLAG configuration on page 83
- Dual-homed servers connected to a pair of FortiSwitch units using an MCLAG on page 84

Standalone FortiGate unit with dual-homed FortiSwitch access



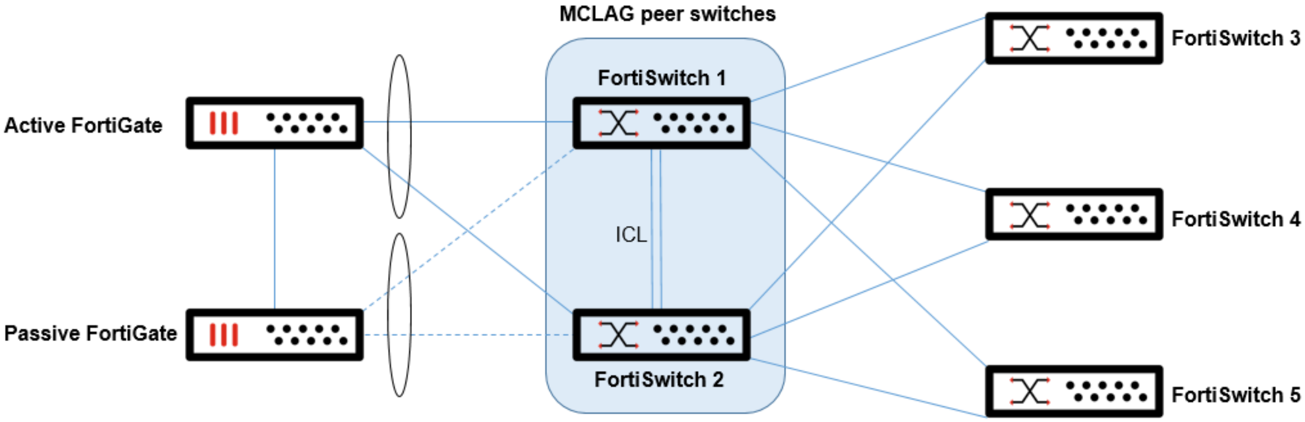
This network topology provides high port density with two tiers of FortiSwitch units.

See Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 85.

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).

See the requirements for using MCLAG topologies in MCLAG requirements on page 85.

HA-mode FortiGate units with dual-homed FortiSwitch access



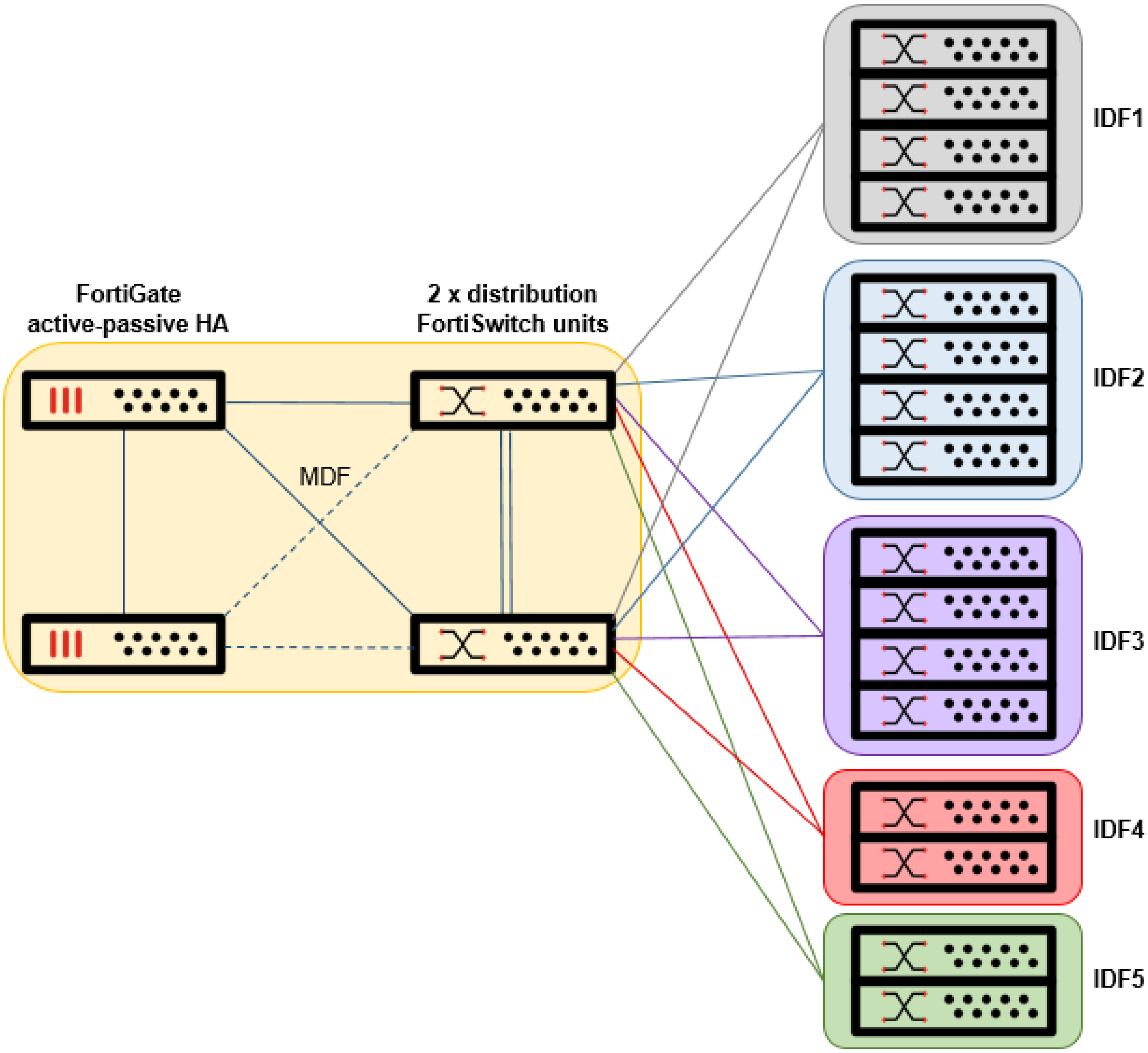
In an HA active-passive cluster, only one FortiGate is active at a time. If the active FortiGate unit fails, the backup FortiGate unit becomes active.

See Transitioning from a FortiLink split interface to a FortiLink MCLAG on page 85.

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).

See the requirements for using MCLAG topologies in MCLAG requirements on page 85.

HA-mode one-tier MCLAG

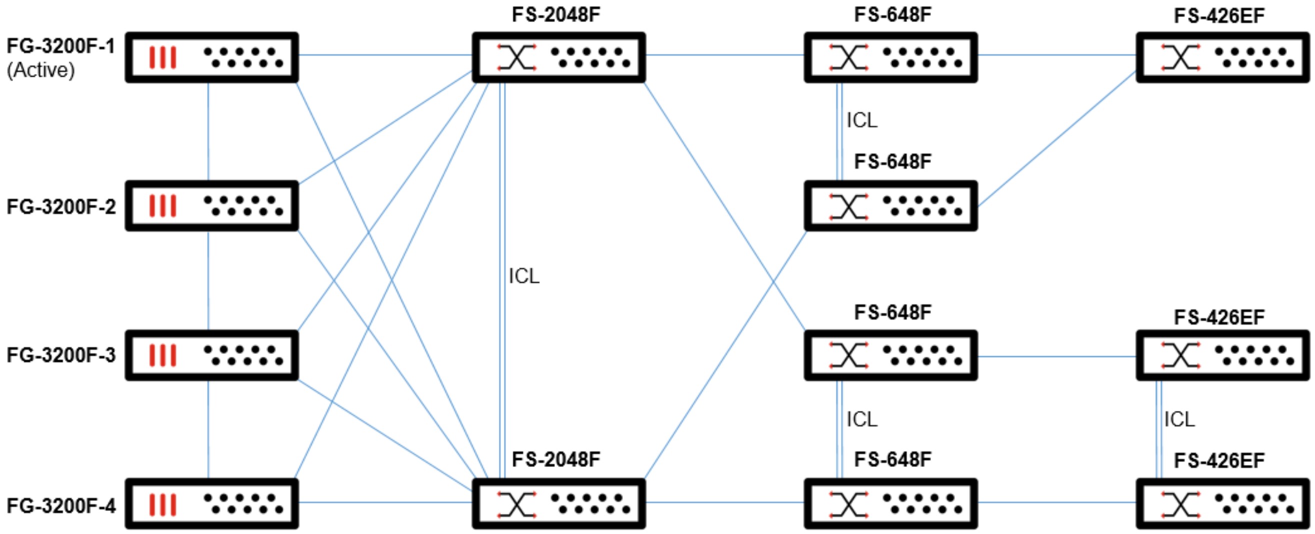


HA-mode FortiGate units connect to redundant distribution FortiSwitch units. Access FortiSwitch units are arranged in a stack in each IDF, connected to both distribution switches.

See the requirements for using MCLAG topologies in MCLAG requirements on page 85.

FortiLink with an HA cluster of four FortiGate units

The following network topology uses four FortiGate units; each is a FG-3200F model and is running FortiOS 6.4.0 build 1533. The FortiSwitch models are FS-2048F, FS-648F, and FS-426EF; they are running FortiSwitchOS 6.2.0 build 0202.



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.

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.

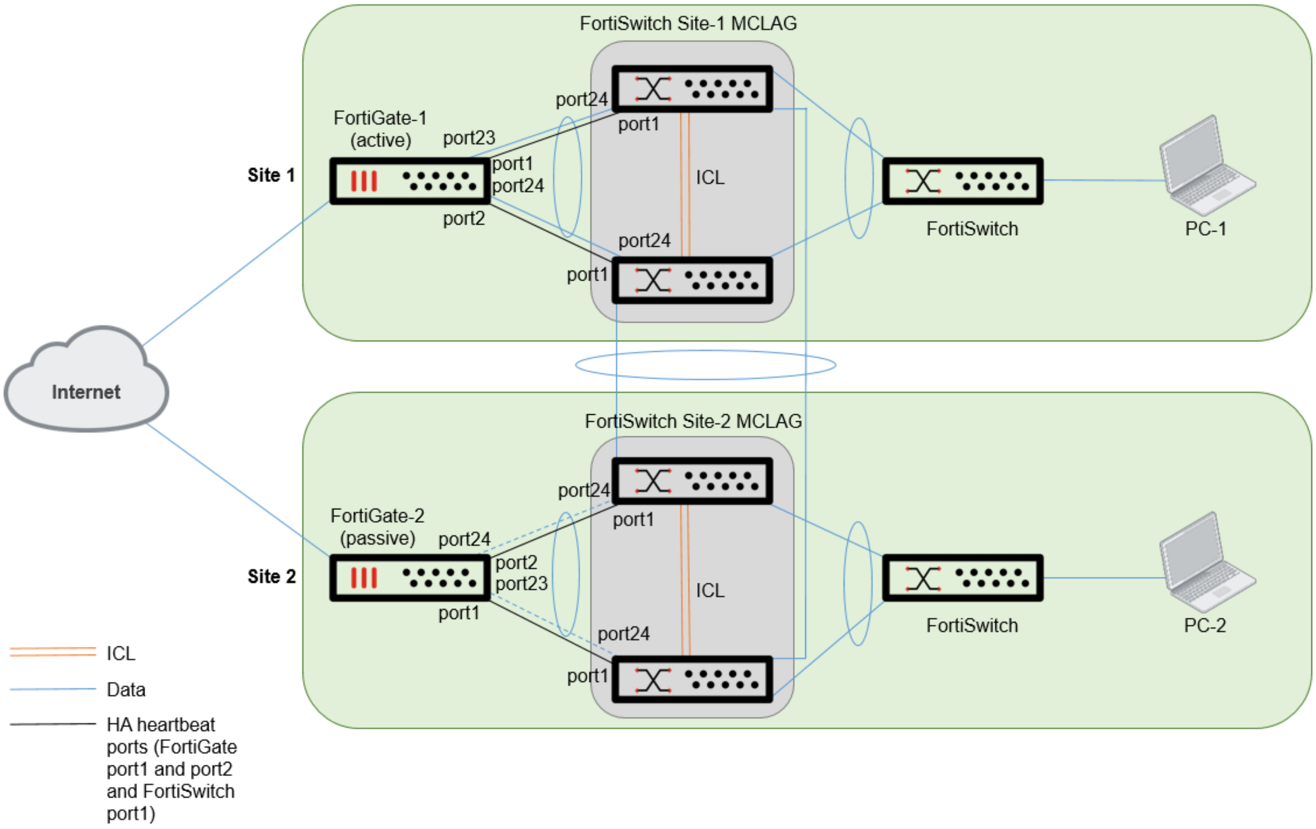
However, active-active FGCP HA results in diminishing performance returns as you add units to the cluster, so the additional performance achieved by adding the third cluster unit might not be worth the cost.

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.

See the requirements for using MCLAG topologies in MCLAG requirements on page 85.

HA-mode FortiGate units in different sites



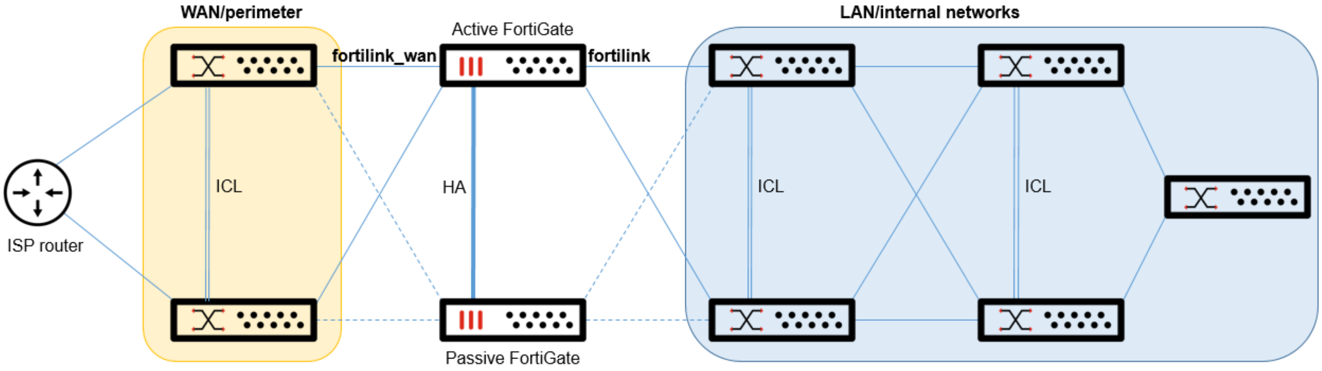
There are two sites in this topology, each with a FortiGate unit connected to the WAN/Internet. The two sites share the FortiGate units in active-passive HA mode. The FortiGate units use the FortiSwitch units in FortiLink mode as the heartbeat connections because of limited physical connections between 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 88.

See the requirements for using MCLAG topologies in MCLAG requirements on page 85.

Isolated LAN/WAN with multiple FortiLink interfaces



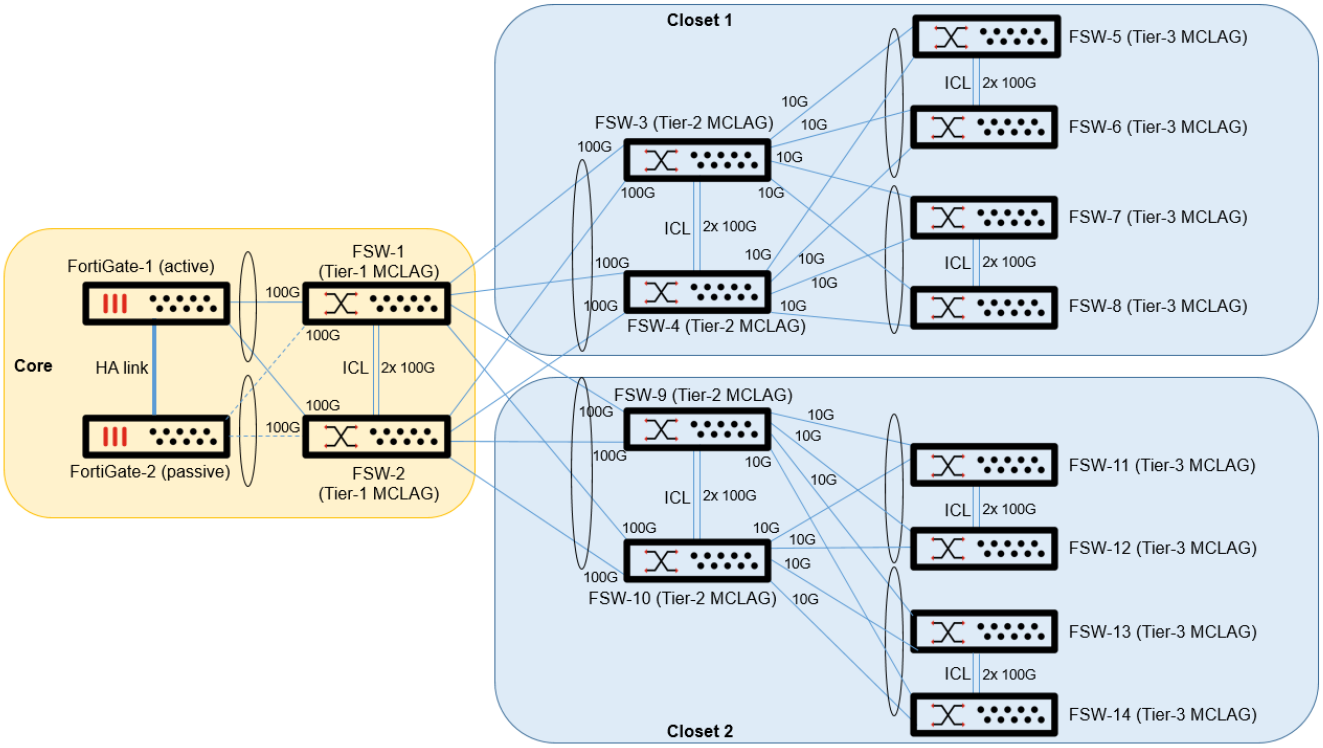
This topology makes use of two FortiLink interfaces to provide a dedicated switching layer for each part of the network, LAN and WAN. Each FortiLink interface is independent with its own FortiSwitch VLANs, providing two separate FortiLink stacks.

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.

See the requirements for using MCLAG topologies in MCLAG requirements on page 85.

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.

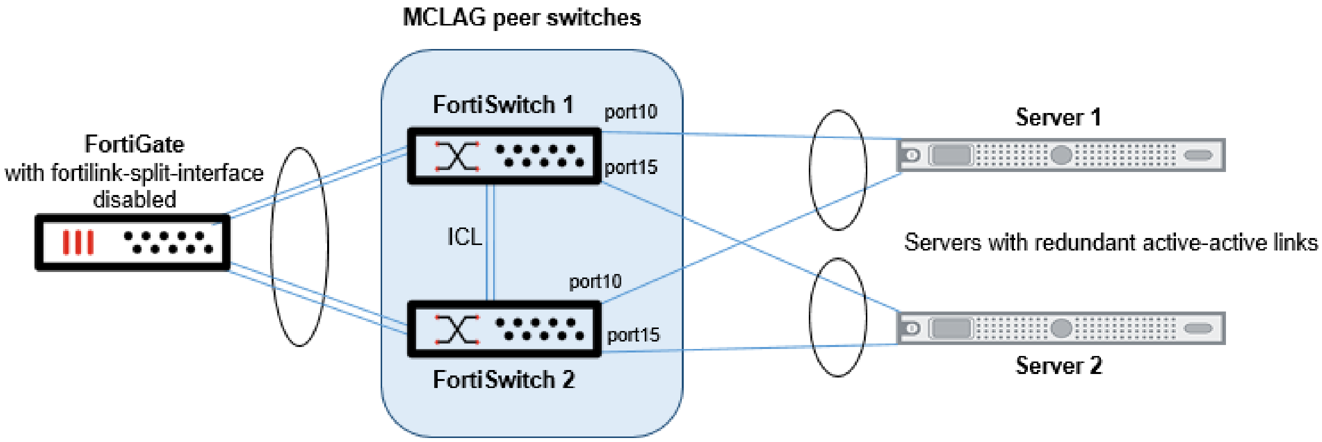
For the procedure, see Deploying MCLAG topologies on page 88.

See the requirements for using MCLAG topologies in MCLAG requirements on page 85.

An MCLAG peer switch could have a single link to only one of its two upper tier switches, but Fortinet recommends at least one link to each of its two upper tier switches. This configuration is known as *fully meshed connections between tiers* and is recommended for the following reasons:

- It provides link and switch redundancy for the topology.
- It allows the FortiGate device’s security rating feature to detect when there are possible tier-2 and tier-3 MCLAGs that can be formed, which will optimize your network.

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 88.

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

See the requirements for using MCLAG topologies in MCLAG requirements on page 85.

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

- Use at least two links for ICL redundancy.
- Connect to both MCLAG peer units when connecting devices to an MCLAG peer group, using the 802.3ad aggregate interface.
- There is a maximum of two FortiSwitch units per MCLAG. Both peer switches should be of the same hardware model and same software version. Mismatched configurations might work but are unsupported.
- 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.

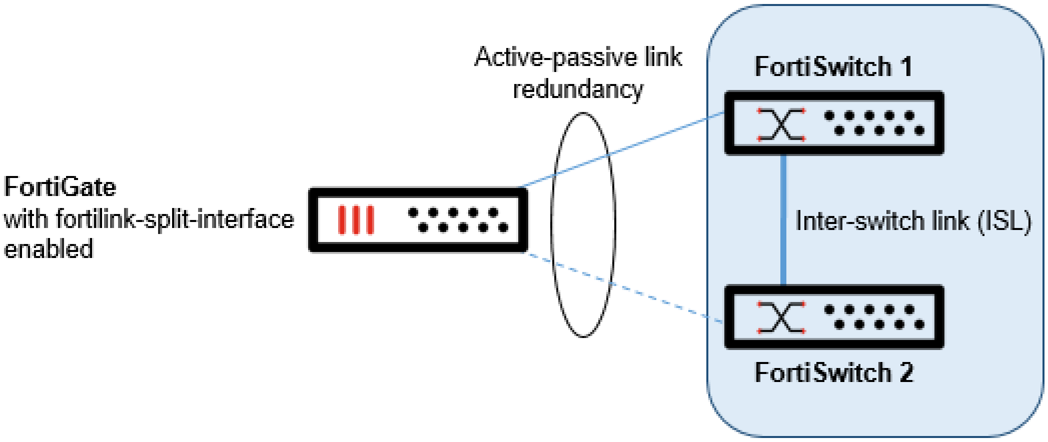
NOTE: If you are going to use IGMP snooping with an MCLAG topology:

- 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.

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.


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

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:

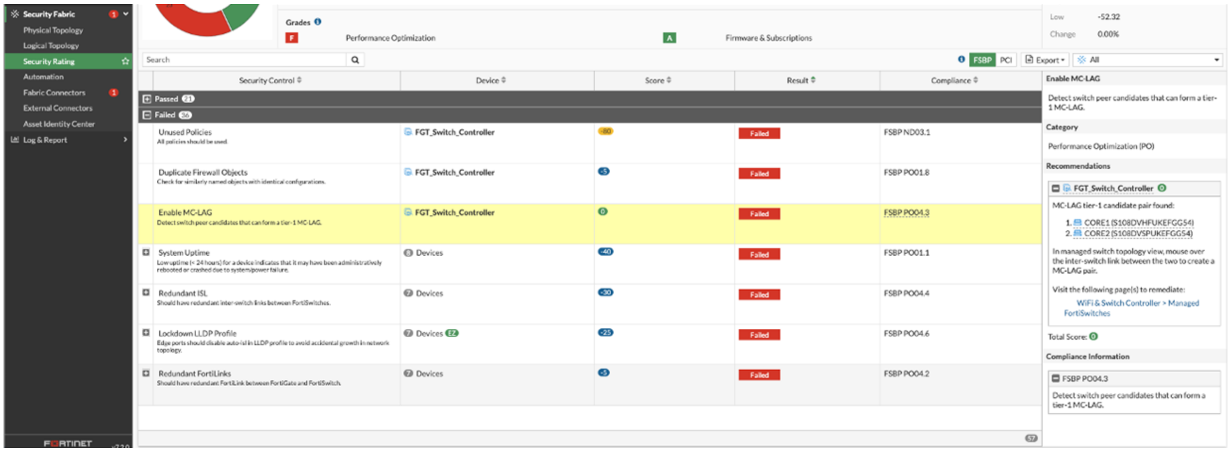
- On the global switch level, `mclag-igmpsnooping-aware` must be enabled. It is enabled by default.
- The `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *disabled* on the ISL and FortiLink trunks; but the `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports`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

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.



Low -52.32
Change 0.00%

	Security Control	Device	Score	Result	Compliance
⊞	Passed 21				
⊟	Failed 36				
	Unused Policies All policies should be used.	FGT_Switch_Controller	-80	Failed	FSBP ND03.1
	Duplicate Firewall Objects Check for similarly named objects with identical configurations.	FGT_Switch_Controller	-5	Failed	FSBP PO01.8
	Enable MC-LAG Detect switch peer candidates that can form a tier-1 MC-LAG.	FGT_Switch_Controller	0	Failed	FSBP PO04.3
⊞	System Uptime Low uptime (< 24 hours) for a device indicates that it may have been administratively rebooted or crashed due to system/power failure.	8 Devices	-40	Failed	FSBP PO01.1
⊞	Redundant ISL Should have redundant inter-switch links between FortiSwitches.	7 Devices	-30	Failed	FSBP PO04.4
⊞	Lockdown LLDP Profile Edge ports should disable auto-isl in LLDP profile to avoid accidental growth in network topology.	7 Devices E2	-25	Failed	FSBP PO04.6
⊞	Redundant FortiLinks Should have redundant FortiLink between FortiGate and FortiSwitch.	7 Devices	-5	Failed	FSBP PO04.2

Enable MC-LAG

Detect switch peer candidates that can form a tier-1 MC-LAG.

Category

Performance Optimization (PO)

Recommendations

FGT_Switch_Controller 0

MC-LAG tier-1 candidate pair found:

1. CORE1 (S108DVHFUKEFGG54)
2. CORE2 (S108DVSPUKEFGG54)

In managed switch topology view, mouse over the inter-switch link between the two to create a MC-LAG pair.

Visit the following page(s) to remediate:

WiFi & Switch Controller > Managed FortiSwitches

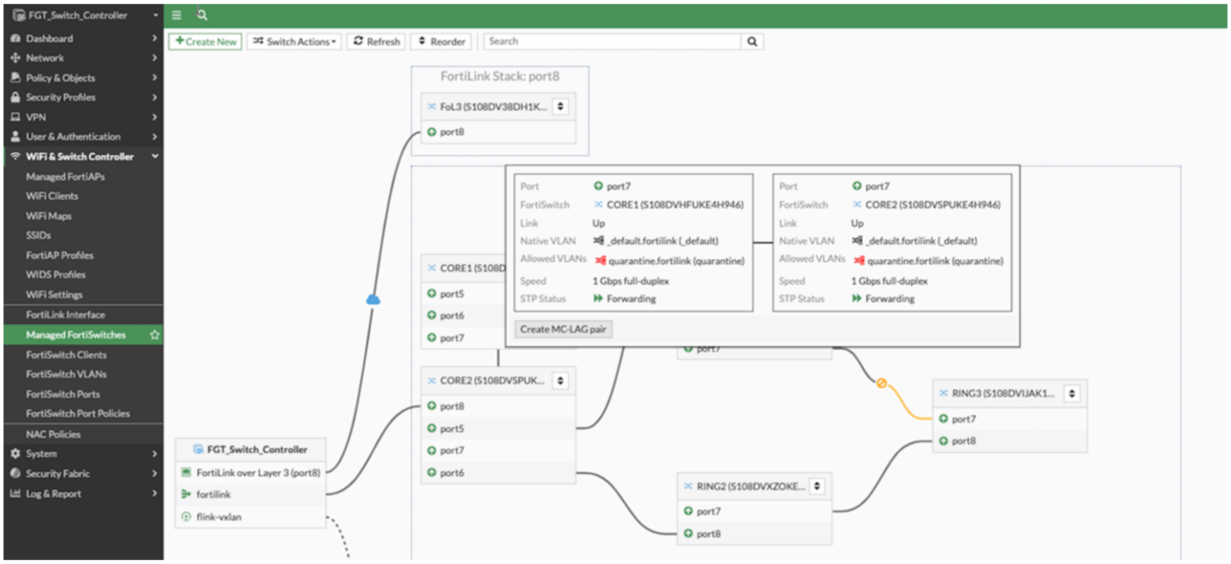
Total Score: 0

Compliance Information

FSBP PO04.3

Detect switch peer candidates that can form a tier-1 MC-LAG.

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.



Port	port7
FortiSwitch	CORE1 (S108DVHFUKE4H946)
Link	Up
Native VLAN	_default.fortilink (_default)
Allowed VLANs	quarantine.fortilink (quarantine)
Speed	1 Gbps full-duplex
STP Status	Forwarding

Port	port7
FortiSwitch	CORE2 (S108DVSPUKE4H946)
Link	Up
Native VLAN	_default.fortilink (_default)
Allowed VLANs	quarantine.fortilink (quarantine)
Speed	1 Gbps full-duplex
STP Status	Forwarding

Create MC-LAG pair

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
```

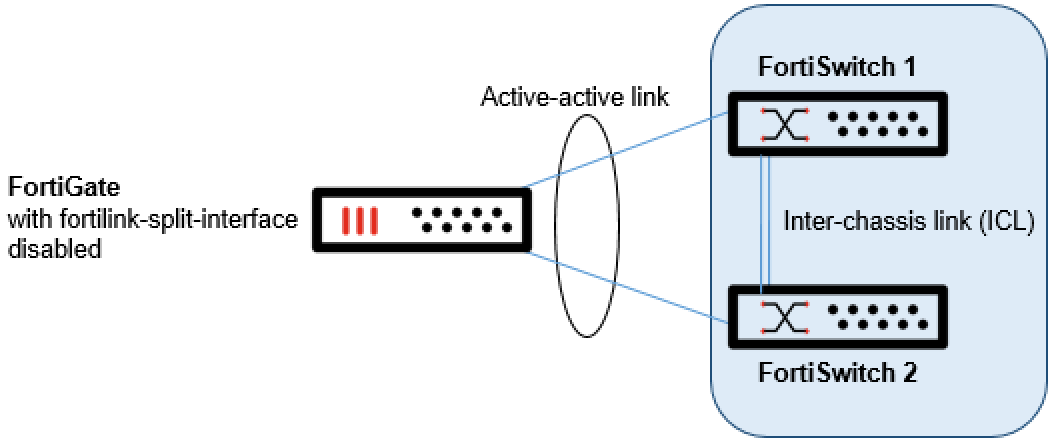
3. From the FortiGate unit, enable the LACP active mode if not already set:

```
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>
```



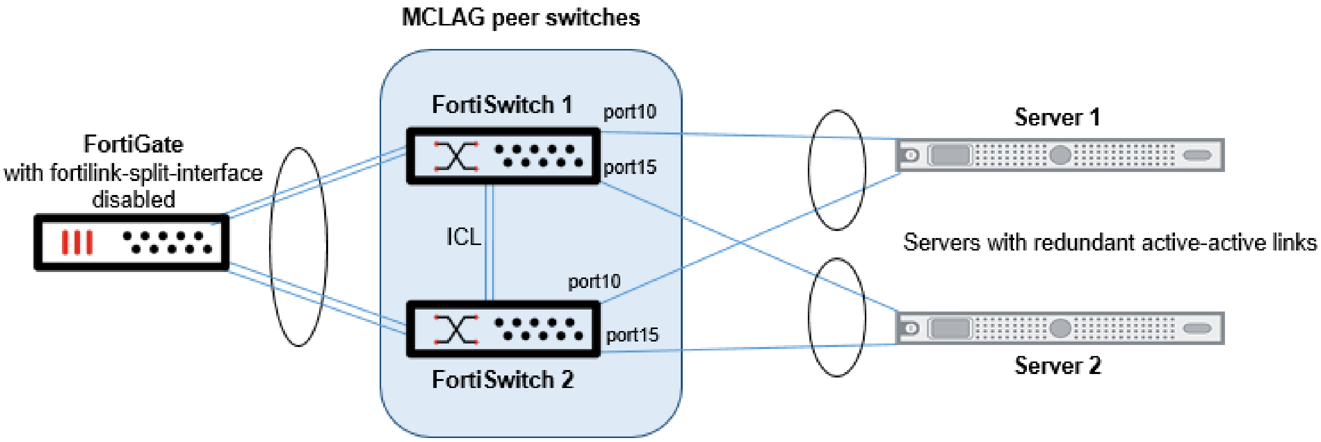
If you disable the MCLAG ICL, you need to enable the `fortilink-split-interface`.

Deploying MCLAG topologies

This section covers the following topics:

- Dual-homed servers connected to a pair of FortiSwitch units using an MCLAG on page 89
- Multi-tiered MCLAG with HA-mode FortiGate units on page 90
- HA-mode FortiGate units in different sites on page 93
- Interconnecting FortiLink fabrics on page 96

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 85. 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.

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

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

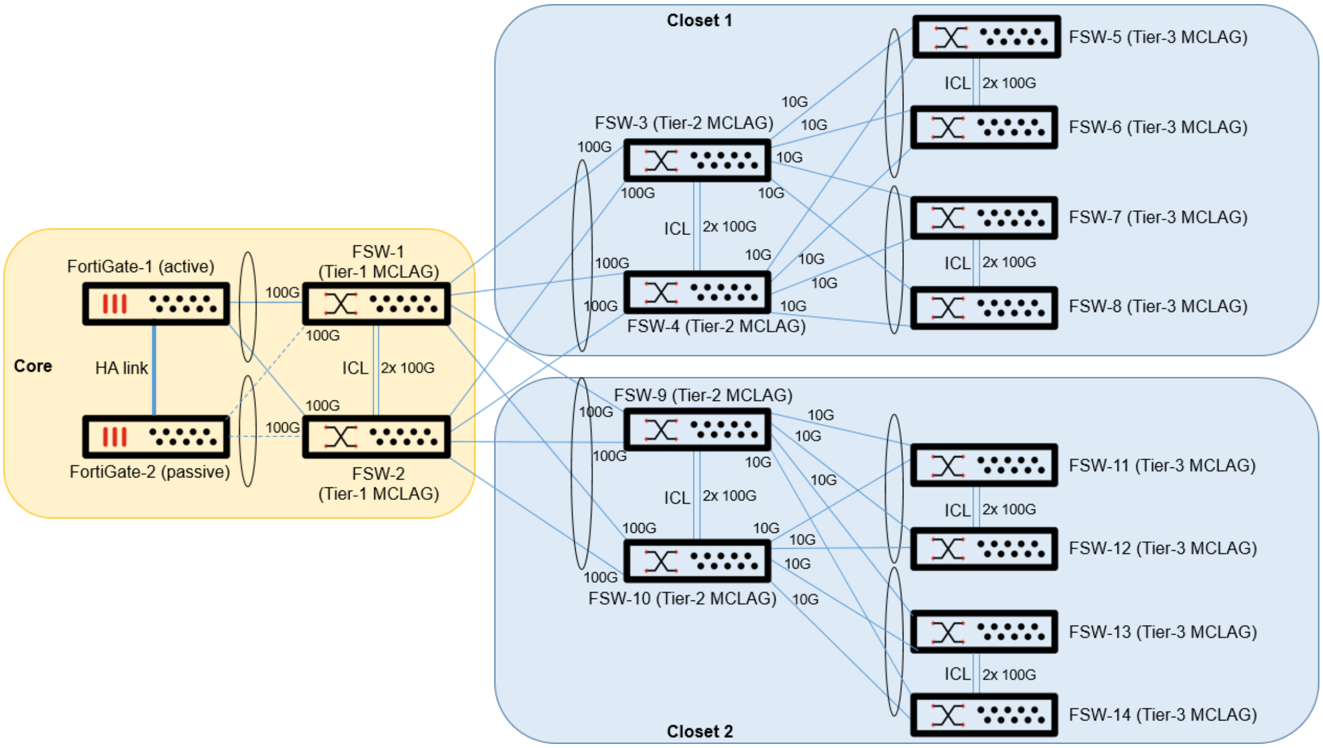
Step 2: For each server, configure a trunk with MCLAG enabled. For server 1, select port10 on FortiSwitch 1 and FortiSwitch 2. For server 2, select port15 on FortiSwitch 1 and FortiSwitch 2.

For details, refer to MCLAG trunks on page 116.

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.

An MCLAG peer switch could have a single link to only one of its two upper tier switches, but Fortinet recommends at least one link to each of its two upper tier switches. This configuration is known as *fully meshed connections between tiers* and is recommended for the following reasons:

- It provides link and switch redundancy for the topology.
- It allows the FortiGate device’s security rating feature to detect when there are possible tier-2 and tier-3 MCLAGs that can be formed, which will optimize your network.

NOTE:

- Before FortiOS 6.2.0, when using HA-mode FortiGate units to manage FortiSwitch units, the HA mode must be active-passive. Starting in FortiOS 6.2.0, the FortiGate HA mode can be either active-passive or active-active.
- In this topology, you must use the `auto-isl-port-group` setting as described in the following configuration example. This setting instructs the switches to group ports from MCLAG peers together into one MCLAG when the inter-switch link (ISL) is formed.
- The `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:

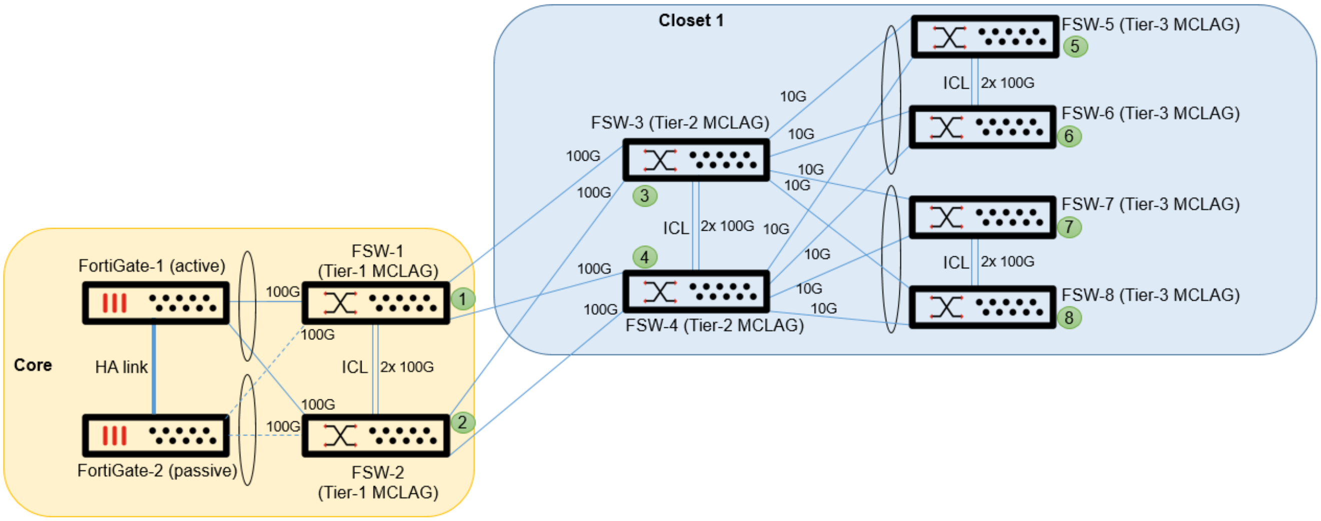
- On the global switch level, `mclag-igmpsnooping-aware` must be enabled. It is enabled by default.
- The `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports` settings must be *disabled* on the ISL and FortiLink trunks; but the `mcast-snooping-flood-traffic` and `igmp-snooping-flood-reports`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

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 85.

Tier-2 and Tier-3 MCLAGs



1. Connect *only* the tier-2 MCLAG FSW-3 and FSW-4 to FSW-1 and FSW-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 FSW-3 and FSW-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. On each of the tier-1 MCLAG switches, add an `auto-isl-port-group` for each tier-2 MCLAG peer group:

```
config switch auto-isl-port-group
   edit tier2-closet-1
      set members port1 port2
   next
   edit tier2-closet-2 // (not in the diagram)
      set members port3 port4
   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 358.

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

4. Wire the tier-3 MCLAG FSW-5, FSW-6, FSW-7, and FSW-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-groups` for the tier-3 MCLAG switches on both tier-2 MCLAG switches (FSW-3 and FSW-4):

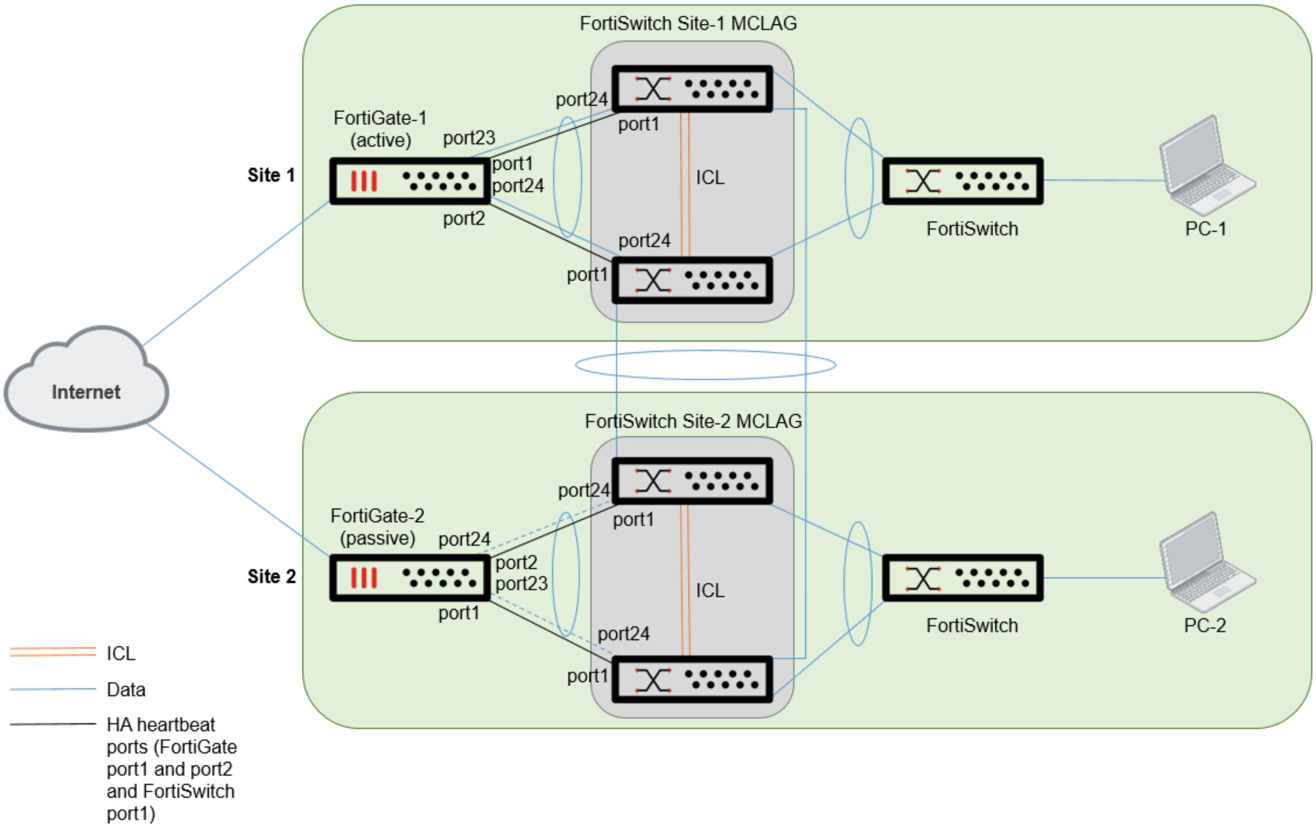
```
config switch auto-isl-port-group
   edit tier-2-closet-<1>-downlink-trunk-A
      set member <port_name>
   next
   edit tier-2-closet-<1>-downlink-trunk-B
      set member <port_name>
   next
end
```

   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 358.
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 FSW-5 and FSW-6 and FSW-7 and FSW-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 88.

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 22.
   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 85.
   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.

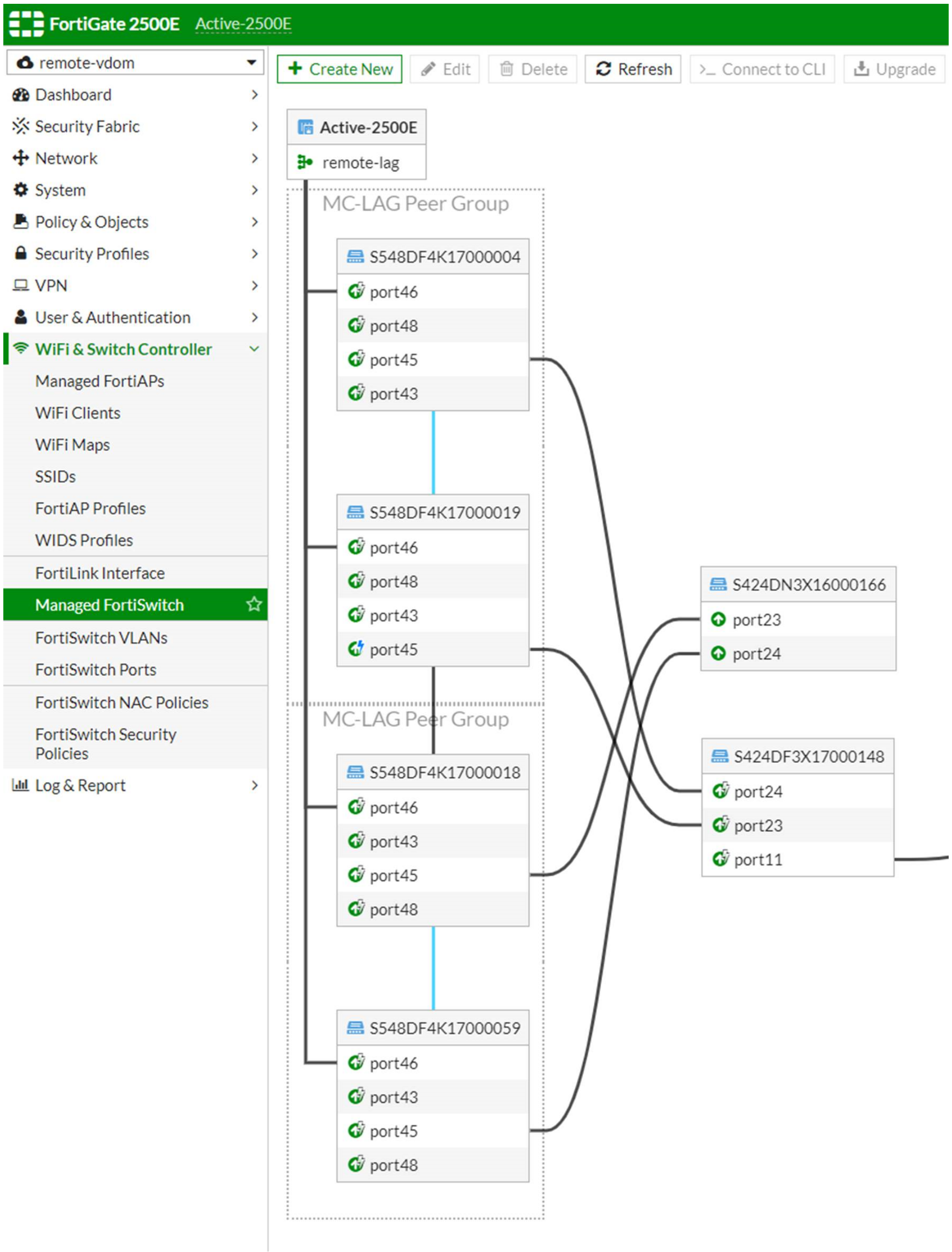
   In this example, you need to assign port1 of core-switch1 to vlan998 and connect port1 of the active FortiGate unit to port1 of core-switch1. Then you need to assign port1 of core-switch2 to vlan999 and connect port2 of the active FortiGate unit to port1 of core-switch2.

```
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
```

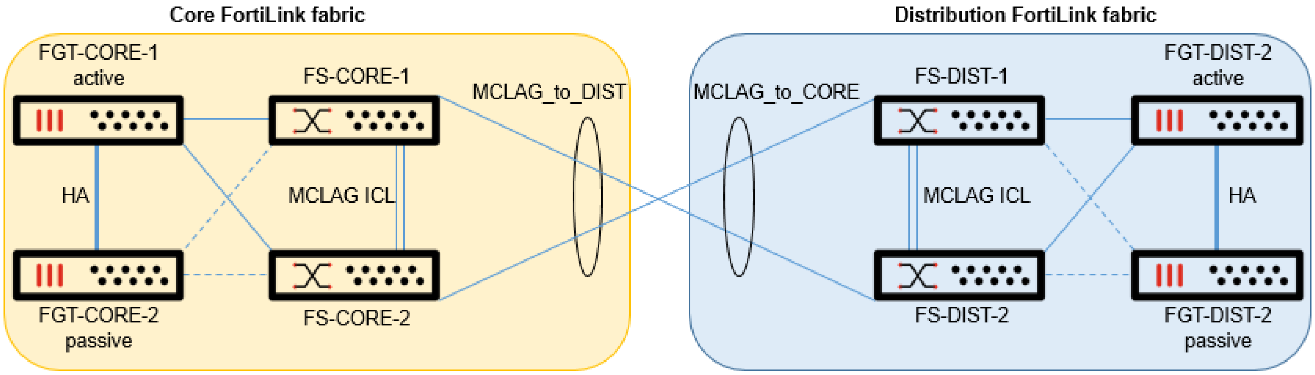
f. Make sure all FortiLinks are up.

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 88.
   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 88.
   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 85.
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 109.
4. Create the MCLAG trunk for the interconnection. See Adding 802.3ad link aggregation groups (trunks) on page 115.
5. Assign matching native VLANs and allowed VLANs to the MCLAG trunk. See Configuring ports using the GUI on page 109.
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
```

Upgrading MCLAG topologies

The following recommended procedure will minimize downtime when upgrading MCLAG (the expected impact is within 5 seconds).

1. If MCLAG split-brain protection is enabled, disable it in both switches in the MCLAG peer group.
2. In the FortiSwitchOS CLI, use the `diagnose switch mclag icl` command to find out which switch has the lower MAC address. .

```
3032E-1 # diagnose switch mclag icl
_FlInK1_ICL0_
       icl-ports            1-2
       egress-block-ports   3-5,31.1,32.1,17.3,17.4,31.2,32.2,32.3,32.4
       interface-mac        84:39:8f:13:96:4d   <-- local switch MAC address
       local-serial-number  FS3E32T422000275
       peer-mac             84:39:8f:13:99:59   <-- peer switch MAC address
       peer-serial-number   FS3E32T422000281
       Local uptime         0 days 23h:55m: 0s
       Peer uptime          0 days 23h:55m: 0s
       MCLAG-STP-mac        84:39:8f:13:96:4c
       keepalive interval   1
       keepalive timeout    60
       dormant candidate    Peer
       split-brain          Disabled
```

3. Stage the image in both switches using the `execute stage image` CLI command).
4. Restart the switch with the lower MAC address.

In the preceding example, the local switch has the lower MAC address, so the local switch should be restarted first.

5. Wait for the switch to restart and check that all links come up (the LACP trunks could be in a down state).
6. Restart the other switch.
7. After MCLAG comes up, enable split-brain protection if it was enabled before the upgrade.

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. 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. You can specify native, allowed, and untagged VLANs.

Native VLAN

You can configure a native VLAN for each port. The native VLAN is like a default VLAN for untagged incoming frames. Outgoing frames for the native VLAN are sent as untagged frames.

The native VLAN is assigned to any untagged frame arriving at an ingress port.

At an egress port, if the frame tag matches the native VLAN, the frame is sent out without the VLAN header.

Allowed VLAN list

The allowed VLAN list for each port specifies the VLAN tag values for which the port can transmit or receive frames.

For a tagged frame arriving at an ingress port, the tag value must match a VLAN on the allowed VLAN list or the native VLAN.

At an egress port, the frame tag must match the native VLAN or a VLAN on the allowed VLAN list.

Untagged VLAN list

The untagged VLAN list on a port specifies the VLAN tag values for which the port will transmit frames without the VLAN tag. Any VLAN in the untagged VLAN list must also be a member of the allowed VLAN list.

The untagged VLAN list applies only to egress traffic on a port.

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.

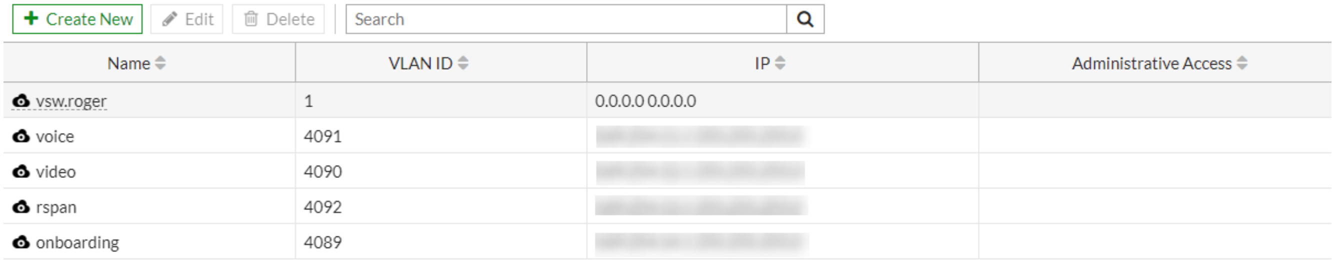
```
 config switch-controller managed-switch
   edit <Switch ID>
      config ports
         edit <port name>
            set vlan <vlan name>
            set allowed-vlans <vlan name>
            or
            set allowed-vlans-all enable
         next
      end
   end
```

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.



Name	VLAN ID	IP	Administrative Access
vsw.roger	1	0.0.0.0 0.0.0.0	
voice	4091	[redacted]	
video	4090	[redacted]	
rspan	4092	[redacted]	
onboarding	4089	[redacted]	

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 inter-VLAN routing offload

Inter-VLAN routing offload requires an advanced features license. For more information, refer to Adding a license.

Starting in FortOS 7.4.1 with FortiSwitchOS 7.4.1, managed FortiSwitch units can perform inter-VLAN routing. The FortiGate device can program the FortiSwitch unit to do the layer-3 routing of trusted traffic between specific VLANs. In this case, the traffic flows are trusted by the user and do not need to be inspected by the FortiGate device.

Inter-VLAN routing offload is applied to the supported FortiSwitch model located closest to FortiGate device in the topology. Refer to the FortiLink Compatibility table to find which FortiSwitchOS models support this feature.

You can use an MCLAG with inter-VLAN routing.

To configure inter-VLAN routing offload:

1. Configure both VLANs for routing offload.
2. Configure the switches for routing offload.

Configure both VLANs for routing offload

By default, `switch-controller-offload` and `switch-controller-offload-gw` are disabled.

The `switch-controller-offload-ip` option is available only when `switch-controller-offload` is enabled.

The `set allowaccess ping` command is configured automatically if it is not already specified.

Enable `switch-controller-offload-gw` on a single VLAN interface. The clients can use the offload IP addresses (configured in the `set switch-controller-offload-ip` command) as the default gateway, which is executed on the FortiSwitch unit. If you are using a DHCP server on the offloaded FortiSwitch VLANs, adjust the DHCP gateway address to match the `switch-controller-offload-ip` address.

```
config system interface
   edit <VLAN_name>
      set ip <IP_address_netmask>
      set switch-controller-offload {enable | disable}
      set switch-controller-offload-ip <IP_address>
      set switch-controller-offload-gw {enable | disable}
   next
end
```

Configure the switches for routing offload

By default, `route-offload` and `route-offload-mclag` are disabled.

When you have an MCLAG configured, you need to enable `route-offload-mclag` and configure `config route-offload`.

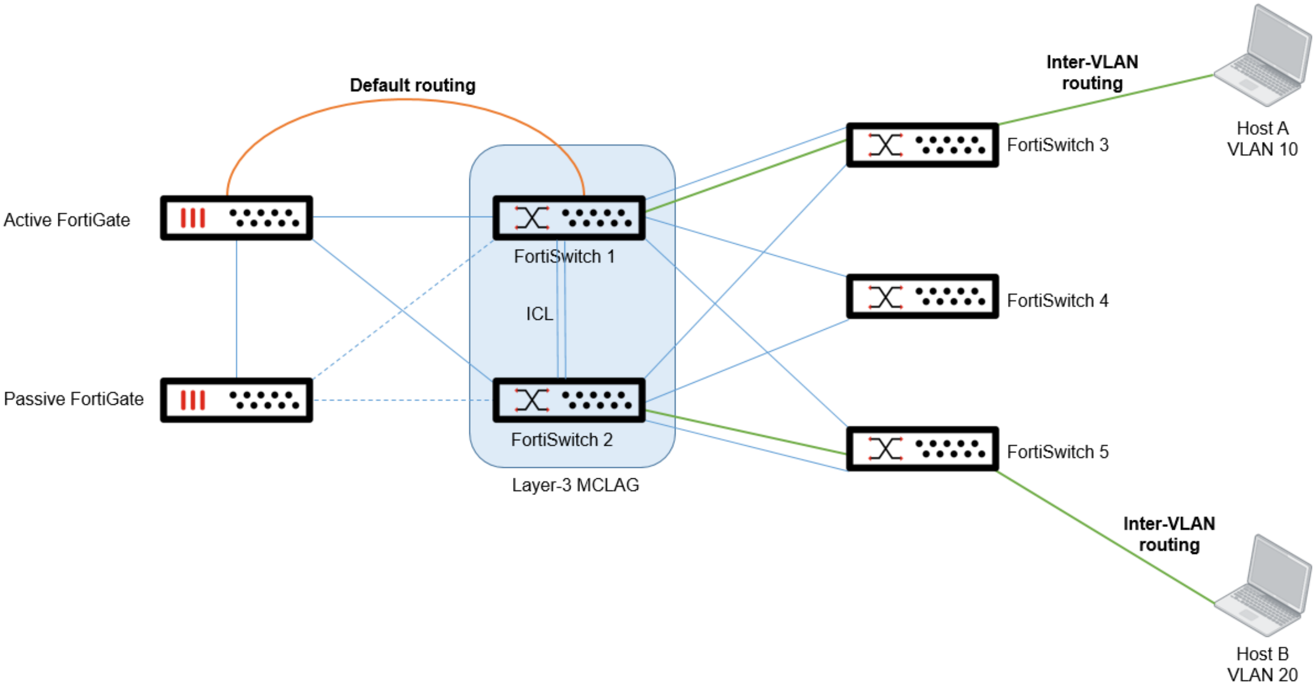
The `config route-offload` commands are available only when `route-offload-mclag` is enabled.

Use `router-ip` to specify the router IP address for VRRP.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      set route-offload {enable | disable}
      set route-offload-mclag {enable | disable}
      config route-offload
         edit <VLAN_name_1>
            set router-ip <IP_address_1>
         next
         edit <VLAN_name_2>
            set router-ip <IP_address_2>
         next
      end
   next
end
```

Configuration example

The following example shows how the default routing between Host A and Host B uses the active FortiGate device in HA mode. When inter-VLAN routing is enabled, VLAN10 on Host A routes through FortiSwitch 3, FortiSwitch 1, FortiSwitch 2, and FortiSwitch 5 to VLAN 20 on Host B.



1. Configure both VLANs for routing offloading

```
config system interface
   edit "vlan.10"
      set ip 192.168.10.1/24
      set switch-controller-offload enable
      set switch-controller-offload-ip 192.168.10.2
      set switch-controller-offload-gw enable
   next
   edit "vlan.20"
   set ip 192.168.20.1/24
```

```
      set switch-controller-offload enable
      set switch-controller-offload-ip 192.168.20.2
   next
end
```

2. Configure FortiSwitch 1 to route to Host A and Host B. Because this example uses MCLAG, you need to enable `route-offload-mclag` and configure `config route-offload`.

```
config switch-controller managed-switch
   edit ST1E24TF21000347
      set route-offload enable
      set route-offload-mclag enable
      config route-offload
         edit "vlan.10"
            set router-ip 192.168.10.3
         next
         edit "vlan.20"
            set router-ip 192.168.20.3
         next
      end
   next
end
```

3. Configure FortiSwitch 2 to route to route to Host A and Host B. Because this example uses MCLAG, you need to enable `route-offload-mclag` and configure `config route-offload`.

```
config switch-controller managed-switch
   edit ST1E24TF21000408
      set route-offload enable
      set route-offload-mclag enable
      config route-offload
         edit "vlan.10"
            set router-ip 192.168.10.4
         next
         edit "vlan.20"
            set router-ip 192.168.20.4
         next
      end
   next
end
```

When inter-VLAN routing is enabled on a VLAN, the FortiGate device configures the following on a FortiSwitch unit:

- A switch virtual interface (SVI) for each FortiSwitch VLAN, configured with the `switch-controller-offload-ip` address.
- A default route in `vrf1`:
  - with the gateway set to the IP address on the FortiGate device of the VLAN with `switch-controller-offload-gw` enabled
  - with `set gw-l2-switch` enabled to forward packets to the FortiGate device without modifying the VLAN and source MAC address

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
```

Starting in FortiOS 7.6.5, the FSR-108F, FSR-112F-POE, and FSR-216F-POE models support auto-negotiation in SGMII mode.

To configure auto-negotiation in SGMII mode:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set description <text>
            set speed sgmii-auto
            set status {down | 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 on page 112
- Enabling PoE pre-standard detection on page 113
- Configuring PoE port settings on page 113
- Resetting the PoE port on page 114
- Displaying general PoE status on page 114

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: FS-548D-FPOE, FS-524D-FPOE, FS-224D-POE, FS-124E-POE, FS-124E-FPOE, 148F-POE, and 148F-FPOE. 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.

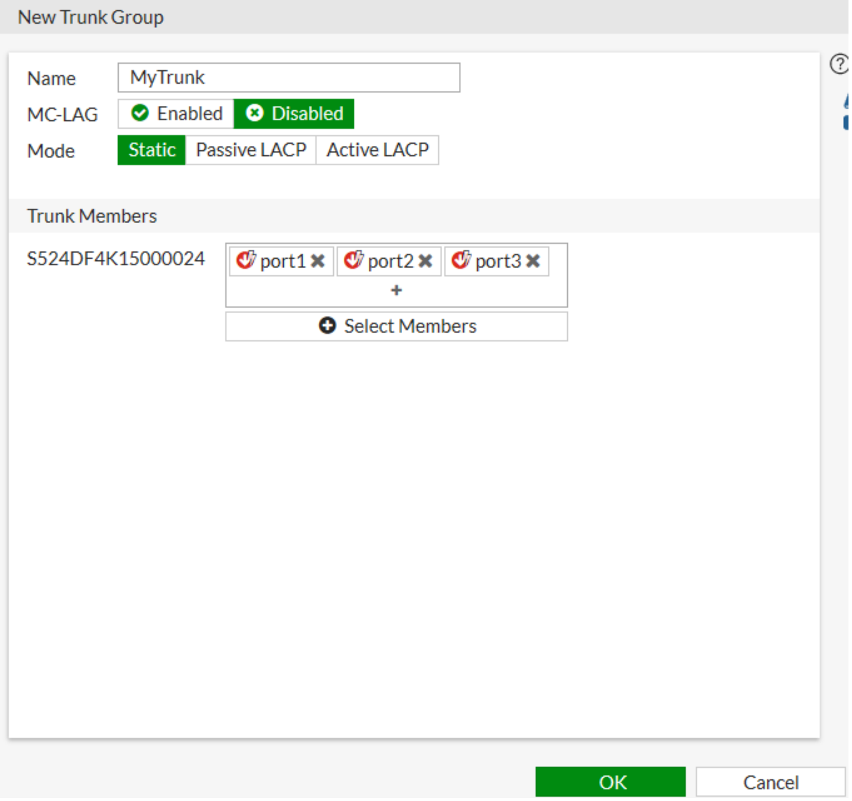
If multiple aggregators exist, one and only one of the aggregators is used by the trunk.

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 85.
    - Make sure to select ports from switches that are part of the same MCLAG peer group.
7. Select *OK*.



New Trunk Group

Name: MyTrunk

MC-LAG: ○ Enabled ● Disabled

Mode: ● Static ○ Passive LACP ○ Active LACP

Trunk Members

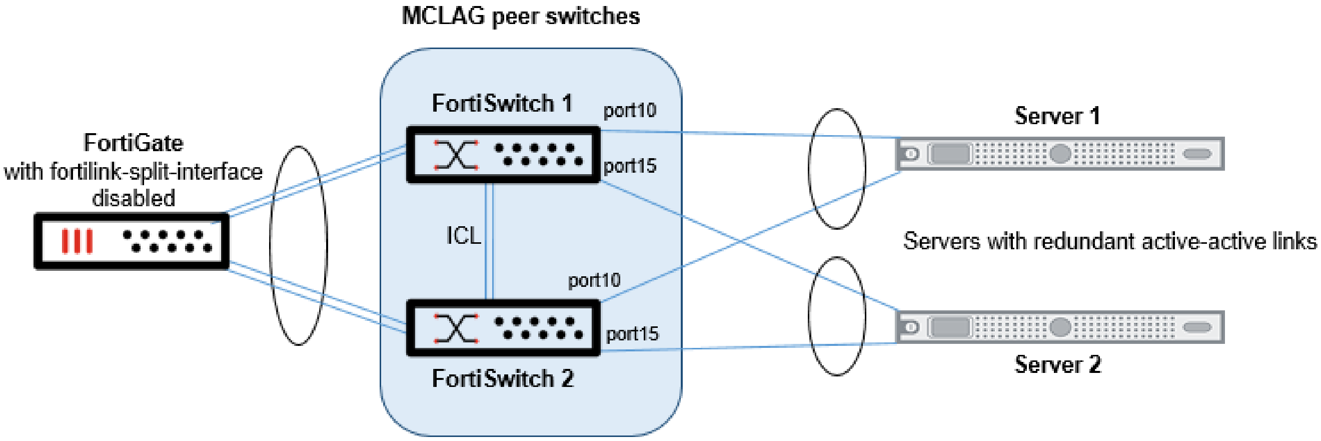
S524DF4K15000024: port1 ✖ port2 ✖ port3 ✖

Using 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 85). 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
mode {static | lacp-passive | lacp-active}	Set the LACP mode. • Set to `static` for static aggregation. In this mode, no control messages are sent, and received control messages are ignored. • Set to `lacp-passive` to passively use LACP to negotiate 802.3ad aggregation. • Set to `lacp-active` to actively use LACP to negotiate 802.3ad aggregation.	lacp-active
members "<port>,<port>"	Set the aggregated LAG bundle interfaces.	No default
mclag enable	Enable or disable the MCLAG.	disable

LACP fallback mode

Starting in FortiOS 7.4.4, LACP fallback mode is supported in the CLI. LACP fallback mode allows a selected port to stay up so that a device not running LACP can still connect to the network. LACP fallback mode is useful if you have a preboot execution environment (PXE) and need to download an image from the network before running LACP in active mode.

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

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

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

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

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

To configure LACP fallback mode:

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

For example:

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

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

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

FortiLink mode supports the FortiSwitch split-port configuration:

- Configuring split ports on a previously discovered FortiSwitch unit on page 120
- Configuring split ports with a new FortiSwitch unit on page 120
- Configuring forward error correction on switch ports on page 121
- Configuring a split port on the FortiSwitch unit on page 122

After you make a change to the `phy-mode` configuration, you must restart the switch. Restarting the switch is necessary to update the port list.

Notes

- Split ports are not configured for pre-configured FortiSwitch units.
- Splitting ports is supported on the following FortiSwitch models:
  - 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.
  - FS-524D and FS-524D-FPOE—Ports 29 and 30 are splittable as 4 x 10G.
  - FS-548D and FS-548D-FPOE—Ports 53 and 54 are splittable as 4 x 10G.
  - FS-1024E—Ports 25 and 26 have a maximum speed of 100G; each port can be split into four subports of 25G or 10G.
  - FS-T1024E and FS-T1024F-FPOE—Ports 25 and 26 have a maximum speed of 100G; each port can be split into four subports of 25G or 10G.
  - FS-1048E—In the 4 x 100G configuration, ports 49, 50, 51, and 52 are splittable as 4 x 25G, 4 x 10G, 4 x 1G, or 2 x 50G.
  - FS-1048E—In the 4 x 4 x 25G configuration, ports 49, 50, 51, and 52 are splittable as 4 x 4 x 25G or 2 x 50G. All four ports can be split.
  - FS-1048E—In the 6 x 40G configuration, ports 49, 50, 51, 52, 53, 54 are splittable as 4 x 10G or 4 x 1G.

  Use the `set port-configuration ?` command to check which ports are supported for each model.
- Starting in FortiSwitchOS 7.6.0, FortiSwitchOS supports 128 ports in software plus the internal and mgmt interfaces (for a total of 130 ports), which allows for more ports to be split. Previously, the maximum number of ports supported in software was 64.
- 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.
- 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).

Configuring split ports on a previously discovered FortiSwitch unit

Using FortiLink mode over a layer-3 network requires both FortiOS 7.2.x (and later) and FortiSwitchOS 7.2.x (and later).

Before FortiOS 7.2.0:

1. On the FortiSwitch unit, configure the split ports. See Configuring a split port on the FortiSwitch unit on page 122.
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 FortiOS 7.2.0:

1. On the FortiSwitch unit, configure the split ports. See Configuring a split port on the FortiSwitch unit on page 122.
2. Restart the FortiSwitch unit.

Configuring split ports with a new FortiSwitch unit

Using FortiLink mode over a layer-3 network requires both FortiOS 7.2.x (and later) and FortiSwitchOS 7.2.x (and later).

Before FortiOS 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 122.
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 FortiOS 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 122.
4. Restart the FortiSwitch unit.

Configuring forward error correction on switch ports

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

Starting in FortiOS 7.4.2, when a FortiSwitch unit is capable of FEC, the default setting for `fec-state` is `detect-by-module`, which automatically detects whether FEC is supported by the module.

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

`fec-capable {0 | 1}`	Set whether the port is FEC capable. • `0`: The port is not FEC capable. • `1`: The port is FEC capable.
`fec-state {cl74 | cl91 | detect-by-module | disabled}`	Set the FEC state: • `c174`: Enable Clause 74 FC-FEC. This option is only available for on FS-1048E, FS-3032E, FS-1024E, and FS-T1024E ports that have been split to 4x25G. • `c191`: Enable Clause 91 RS-FEC. This option is only available for on FS-1048E and FS-3032E ports that have been split to 4x100G. • `detect-by-module`: Automatically detect whether FEC is supported by the module. • `disabled`: Disable FEC on the port.

In this example, a 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.
- 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.
- 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.
  NOTE: For the FS-T1024E and FS-1024E models, the auto-module selects the correct speed for the subports. If you insert a 100G QSFP28 module, the subports are automatically changed to 4x25G. If you insert a 40G QSFP+ module, the subports are automatically changed to 4x10G.
- 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 524D is configured with port29 set to 4x10G:

```
config switch phy-mode
   set port29-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 auto
      next
      edit "port2"
         set lldp-profile "default-auto-isl"
         set speed auto
      next
      .
      .
      .
      edit "port29.1"
         set lldp-profile "default-auto-isl"
         set speed auto-module
      next
      edit "port29.2"
         set lldp-profile "default-auto-isl"
         set speed auto-module
      next
      edit "port29.3"
         set lldp-profile "default-auto-isl"
         set speed auto-module
      next
      edit "port29.4"
         set lldp-profile "default-auto-isl"
         set speed auto-module
      next
      edit "port30"
         set lldp-profile "default-auto-isl"
         set speed auto-module
      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 on page 124
- FortiSwitch VLANs from different VDOMs sharing the same FortiSwitch ports on page 126
- VLAN stacking (QinQ) on page 127

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
```

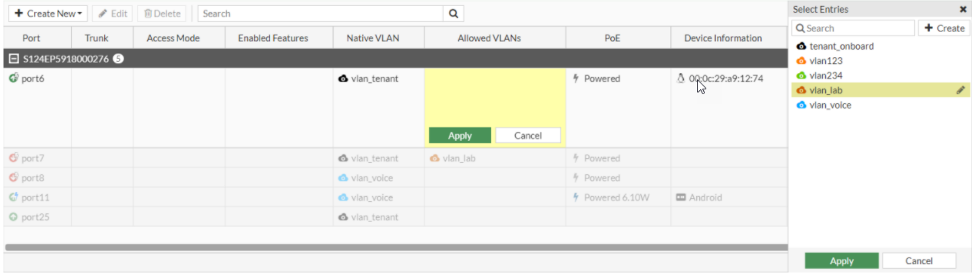
NOTE: Shared ports do not support the DHCP-snooping feature.

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 global level, go to *Network > Interfaces* and click *Create New* to create the VLANs and then assign them to their respective VDOMs.
2. In the GUI, go to *WiFi & Switch Controller > FortiSwitch Ports*.
3. Select a port and click *Edit*.
4. Assign the VLAN to the FortiSwitch port.
   The assigned VLANs are displayed in the GUI (*WiFi & Switch Controller > FortiSwitch Ports*) in the root VDOM.



Port	Trunk	Access Mode	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information
S124EP5918000276 5							
port6				vlan_tenant		Powered	00:0c:29:a9:12:74
port7				vlan_tenant	vlan_lab	Powered	
port8				vlan_voice		Powered	
port11				vlan_voice		Powered 6.10W	Android
port25				vlan_tenant			

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

VLAN stacking (QinQ)

The FortiOS switch controller now supports QinQ. With QinQ, each client of a managed security service provider (MSSP) can have a unique customer VLAN with a self-managed 4k VLAN range in its own virtual domain. QinQ allows better segregation and control over network traffic.

QinQ allows you to have multiple VLAN headers in an Ethernet frame. The value of the EtherType field specifies where the VLAN header is placed in the Ethernet frame.

Use the VLAN TPID profile to specify the value of the EtherType field. The FortiSwitch unit supports a maximum of four VLAN TPID profiles, including the default (0x8100). Use the default (0x8100) VLAN TPID profile to reach layer 3. The default VLAN TPID profile (0x8100) cannot be deleted or changed.

To see which FortiSwitch models support this feature, refer to the FortiSwitch feature matrix.

The following features are not supported with QinQ:

- DHCP relay
- DHCP snooping
- IGMP snooping
- IP source guard
- PVLAN
- STP

Settings under `config QinQ` are for customer VLANs (C-VLANs). Other settings such as `set allowed-vlans`, `set native-vlan`, and `set vlan-tpid` are for service-provider VLANs (S-VLANs).

To configure QinQ with the switch controller:

1. Using the FortiOS CLI, create a separate VDOM for each customer.
2. Using the FortiOS CLI, create VLANs for the service provider and each customer and assign the VLANs to the appropriate VDOM.
3. Using the FortiOS CLI, configure QinQ for the managed switch port that will be used by the customer's VLANs.

Create a VDOM for each customer

Use the FortiOS CLI to configure a separate VDOM for each customer. For example:

```
config vdom
   edit root
   next
   edit vdom1
   next
end
```

Create VLANs for each customer

Use the FortiOS CLI to create VLANs for each customer and assign the VLANs to the appropriate VDOM.

The S-VLAN must be configured on the same VDOM where the FortiLink interface is; for example, if the FortiLink interface is on the root VDOM, all S-VLANs must be defined in the root VDOM.

In the following example, three VLANs are created and then assigned to the same VDOM:

```
config system interface
   edit "c1.svlan999"
      set vdom "root"
      set device-identification enable
      set role lan
      set snmp-index 52
      set interface "fortilink"
      set vlanid 999
   next
end

config system interface
   edit "c1.cvlan10"
      set vdom "root"
      set ip 15.1.1.1 255.255.255.0
      set allowaccess ping
      set device-identification enable
      set role lan
      set snmp-index 53
      set interface "c1.svlan999"
      set vlanid 10
   next
end

config system interface
   edit "c1.cvlan20"
      set vdom "root"
      set ip 16.1.1.1. 255.255.255.0
      set allowaccess ping
      set device-identification enable
      set role lan
      set snmp-index 54
      set interface "c1.svlan999"
      set vlanid 20
   next
end
```

In the following example, three VLANs are created and then assigned to the `root` or `vdom1` VDOM:

```
config system interface
   edit "909824.1"
      set vdom "vdom1"
      set interface "fortilink"
      set vlanid 3000
   next
end

config system interface
   edit "1.vlan1"
      set vdom "root"
      set interface "909824.1"
      set vlanid 1
   next
end

config system interface
   edit "1.vlan2"
      set vdom "root"
      set interface "909824.1"
      set vlanid 2
   next
end
```

Configure QinQ with the switch controller

Use the FortiOS CLI to configure QinQ for the managed switch port that will be used by the customer's VLANs. In the following example, QinQ is enabled on port10 of the managed switch:

```
config switch-controller managed-switch
   edit "S248EPTF18001384"
      config ports
         edit "port10"
            set qnq "909824.1"
            set vlan "1.vlan1"
            set allowed-vlans "1.vlan2"
         next
      end
   next
end
```

If you enable the `set allowed-vlans-all` command when QinQ is enabled, all C-VLANs in that VDOM that have the same parent interface as the `set qnq` VLAN are pushed. In the following example, all C-VLANs in the root VDOM with `svlan100` as the parent interface are pushed:

```
config switch-controller managed-switch
   edit S548DN5018000532
      config ports
         edit "port16"
            set vlan "cv_sv_50"
            set allowed-vlans-all enable
            set export-to "root"
            set mac-addr 70:4c:a5:a5:9d:59
            set qnq "svlan100"
         next
      end
   next
end
```

Configuration example

In this example, there are two customers. Customer `c1` is assigned a customer tag of 3000 and VLANs 1-4094. Customer `c2` is assigned a customer tag of 3001 and VLANs 1-4094.

1. Use the FortiOS CLI to create separate VDOMs for the two customers, `c1` and `c2`.

```
config vdom
   edit root
   next
   edit c1
   next
   edit c2
   next
end
```

2. Use the FortiOS CLI to create VLANs for each customer and assign the VLANs to the appropriate VDOM. In this example, you create three VLANs for customer `c1` and three VLANs for customer `c2`.

```
config system interface
   edit "fortilink"
      set fortilink enable
   next
   edit "customer.c1"
      set vdom "root"
      set interface "fortilink"
      set vlanid 3000
   next
   edit "customer.c2"
      set vdom "root"
      set interface "fortilink"
      set vlanid 3001
   next
   edit "c1.vlan1"
      set vdom "c1"
      set interface "customer.c1"
      set vlanid 1
   next
   edit "c1.vlan10"
      set vdom "c1"
      set interface "customer.c1"
      set vlanid 10
   next
   edit "c1.vlan20"
      set vdom "c1"
      set interface "customer.c1"
      set vlanid 20
   next
   edit "c2.vlan1"
      set vdom "c2"
      set interface "customer.c2"
      set vlanid 1
   next
   edit "c2.vlan10"
```

```
         set vdom "c2"
         set interface "customer.c2"
         set vlanid 10
      next
         edit "c2.vlan20"
         set vdom "c2"
         set interface "customer.c2"
         set vlanid 20
      next
   end
```

3. Use the FortiOS CLI to configure QinQ for the managed switch port (`port8`) that will be used by the VLANs (1, 10, and 20) for customer `c1`.

```
config switch-controller managed-switch
   edit "S108DV3A17000077"
      config ports
         edit "port8"
            set qnq "customer.c1"
            set vlan "c1.vlan1"
            set allowed-vlans "c1.vlan10" "c1.vlan20"
         next
      end
   next
end
```

4. Use the FortiOS CLI to configure QinQ for the managed switch port (`port9`) that will be used by the VLANs (1, 10, and 20) for customer `c2`

```
config switch-controller managed-switch
   edit "S548DF5018000776"
      config ports
         edit "port9"
            set qnq "customer.c2"
            set vlan "c2.vlan1"
            set allowed-vlans "c2.vlan10" "c2.vlan20"
         next
      end
   next
end
```

Configuring switching features

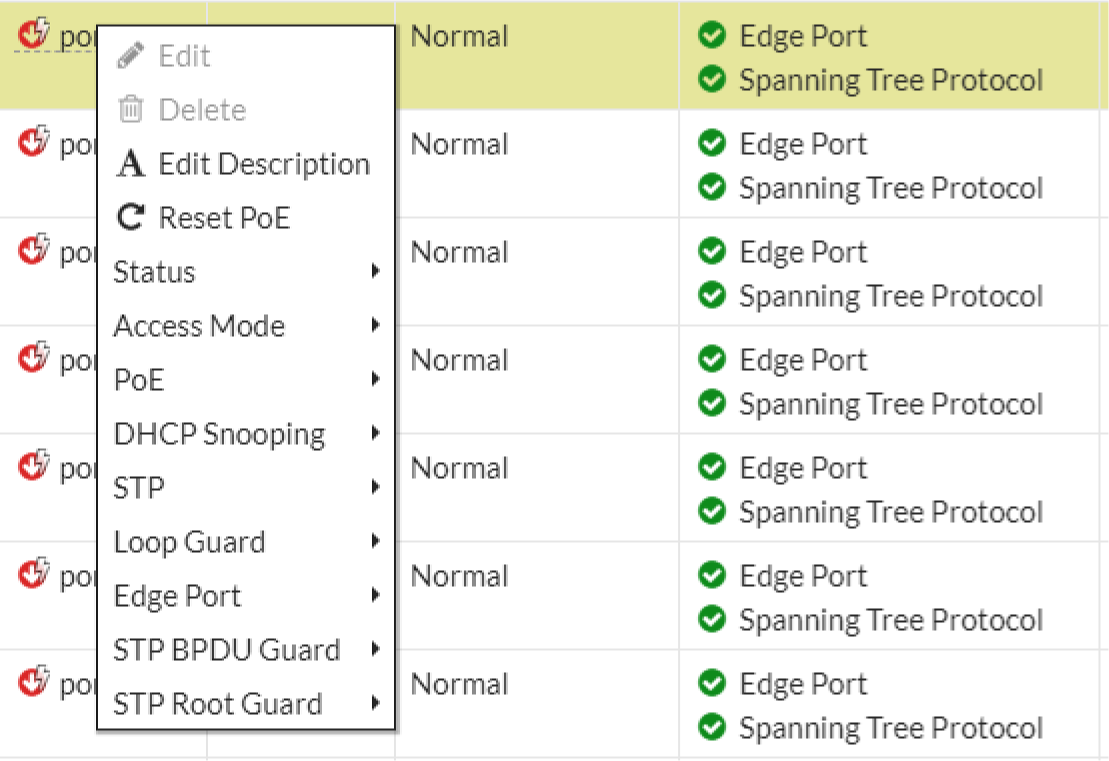
This section covers the following features:

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.

⚠ Changing the `auto-stp-priority` setting causes FortiLink to go down temporarily.

This section covers the following topics:

- Configuring STP on FortiSwitch ports on page 136
- Configuring STP root guard on page 138
- Configuring STP BPDU guard on page 138
- Configuring interoperation with per-VLAN RSTP on page 140

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
```

Refer to the FortiSwitchOS feature matrix to see how many VLANs are 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 on page 141
- Controlling how long learned MAC addresses are saved on page 142
- Logging violations of the MAC address learning limit on page 142
- Persistent (sticky) MAC addresses on page 143
- Logging changes to MAC addresses on page 144

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.

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

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
```

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 on managed FortiSwitch units. By default, each learned MAC address is aged out after 300 seconds. After this amount of time, the inactive MAC address is deleted from the FortiSwitch hardware. The value ranges from 10 to 1000,000 seconds. Set the value to 0 to disable MAC address aging.

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

For example:

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

Logging violations of the MAC address learning limit

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

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

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.

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

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 (1-10,000,000 packets per seconds with a default is 500; set to 0 to drop all packets) 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.

You can configure storm control globally or for all ports on a specific switch. To configure storm control for a specific FortiSwitch unit, enable `local-override`, and the settings in the storm-control policy (if one has been configured) are used for that switch.

Starting in FortiOS 7.6.4, you can configure the maximum burst size allowed by storm control. Select the burst size level from 1 to 4 with the highest number for the highest maximum burst size allowed. By default, the burst size level is set to 0, and the switch uses the default burst size. The maximum number of packets or bytes allowed for the burst-size level depends on the switch model.

- 1—1,024 packets or bytes
- 2—64 packets or bytes
- 3—4 packets or bytes
- 4—maximum burst size

The burst-size level cannot be controlled on a port level for the FS-124E, FS-124E-POE, and FS-124E-FPOE models. Are there any additional models that should be listed?

To configure storm control globally for all switch ports (both FortiLink ports and non-FortiLink ports):

```
config switch-controller storm-control
   set rate <1-10000000 or 0 to drop all packets>
   set burst-size-level {1 | 2 | 3 | 4}
   set unknown-unicast {enable | disable}
   set unknown-multicast {enable | disable}
   set broadcast {enable | disable}
end
```

For example:

```
config switch-controller storm-control
   set rate 500
   set burst-size-level 2
   set unknown-unicast disable
   set unknown-multicast disable
   set broadcast disable
end
```

To configure storm control for a specific managed switch:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config storm-control
         set local-override {enable | disable}
         set rate <1-10000000 or 0 to drop all packets>
         set burst-size-level {0 | 1 | 2 | 3 | 4}
         set unknown-unicast {enable | disable}
         set unknown-multicast {enable | disable}
         set broadcast {enable | disable}
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "FS1E48T422005162"
      config storm-control
         set local-override enable
         set rate 500
         set burst-size-level 1
         set unknown-unicast disable
         set unknown-multicast disable
         set broadcast disable
      end
   next
end
```

To configure a storm-control policy:

```
 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 burst-size-level {0 | 1 | 2 | 3 | 4}
      set unknown-unicast {enable | disable}
      set unknown-multicast {enable | disable}
      set broadcast {enable | disable}
   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 burst-size-level 4
      set unknown-unicast enable
      set unknown-multicast enable
      set broadcast enable
   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. For more information about IGMP snooping on the FortiSwitch unit, refer to IGMP snooping.

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 on page 146
- Configuring IGMP-snooping settings on a switch on page 147
- Configuring the IGMP-snooping proxy on page 147
- Configuring the IGMP-snooping querier on page 148

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.

- 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.
- Multicast addresses with a destination of 239.x.x.x will flood within the VLAN. This issue affects the FS-110G-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-124G, FS-124G-FPOE, FS-148F, FS-148F-POE, and FS-148F-FPOE models.

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

For more information about using PTP on FortiSwitch units, see Precision Time Protocol.

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

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

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

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

   By default, the PTP status is enabled.

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

To configure a PTP profile:

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

For example:

```
config system ptp profile
   edit newPTPprofile
      set description "New PTP profile"
      set mode transparent-p2p
      set ptp-profile C37.238-2017
      set transport l2-mcast
      set domain 1
      set pdelay-req-interval 2sec
   next
end
```

To configure the PTP settings:

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

For example:

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

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

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

For example:

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

To apply your custom PTP policy to a port:

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

For example:

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

Layer-3 switch configuration

Starting in FortiOS 7.6.4, FortiOS supports configuring the following features on layer-3 managed switches:

- Switched virtual interfaces (SVIs). See Switch virtual interfaces on page 152.
- Routed virtual interfaces (RVIs). See Routed VLAN interfaces on page 153.
- Static IPv4 routing. See Static IPv4 routing on page 156.
- Virtual routing and forwarding (VRF). See Virtual routing and forwarding on page 157.
- DHCP servers. See Configuring a DHCP server on page 160.

Switch virtual interfaces

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

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

To create an SVI:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config system-interface
         edit <interface_name>
            set switch-id <FortiSwitch_serial_number>
            set mode {static | dhcp}
            set ip <IPv4_address_netmask>
            set status {disable | enable}
            set allowaccess {ping | https | http | ssh | snmp | telnet | radius-acct}
            set vlan <string>
            set type vlan
            set vrf <VRF_name>
         next
      end
   next
end
```

Option	Description	Default
switch-id <FortiSwitch_serial_number>	Required. The FortiSwitch serial number here should match the one in `edit <FortiSwitch_serial_number>`.	No default

Option	Description	Default
mode {static | dhcp}	Configure the connection mode for the interface: • `static`—Configure a static IP address for the interface. • `dhcp`—Configure the interface to receive its IP address from an external DHCP server.	static
ip <IPv4_address_ netmask>	Required. Enter the interface IP address and netmask. You can set the IP and netmask, but they are not displayed. The IP address cannot be on the same subnet as any other interface.	0.0.0.0 0.0.0.0
status {disable | enable}	Enable or disable the interface. If the interface is disabled, it does not accept or send packets. If you disable a physical interface, associated virtual interfaces such as VLAN interfaces will also stop.	enable
allowaccess {ping | https | http | ssh | snmp | telnet | radius-acct}	Enter the types of management access permitted on this interface. Separate each type with a space. To add or remove an option from the list, retype the complete list as required.	No default
vlan <string>	Required. Enter the name of the VLAN. Type `?` to see a list of interfaces.	No default
type vlan	Enter the type of interface. Use the default value of `vlan` for an SVI.	vlan
vrf <string>	Assign the specified virtual routing and forwarding (VRF) instance to this SVI.	No default

For example:

```
config switch-controller managed-switch
   edit "FS2F48TV23000017"
      config system-interface
         edit "svi1"
         set switch-id "FS2F48TV23000017"
         set mode static
         set ip 0.0.0.0 0.0.0.0
         set status enable
         unset allowaccess
         set vlan ''
         set type vlan
         set vrf ''
      next
      end
   next
end
```

Routed VLAN interfaces

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

RVIs support ECMP, VRF, multiple IP addresses, IPv4 addresses, IPv6 addresses, BFD, VRRP, DHCP server, DHCP relay, RIP, OSPF, ISIS, BGP, and PIM.

Layer-2 protocols and most switch interface features are disabled on RVIs. When RVI is enabled, the following features are not available:

- 802.1X port mode
- 802.1X MAC-based security mode
- User-based (802.1X) VLAN assignment
- 802.1X enhancements, including MAB
- MAB reauthentication
- open-auth mode
- Support of the RADIUS accounting server
- Support of RADIUS CoA and disconnect messages
- EAP pass-through
- Network device detection
- DHCP snooping
- DHCP blocking
- Dynamic ARP inspection
- Access VLANs
- VLAN tag by ACL
- IGMP snooping
- IGMP proxy
- IGMP querier
- Per-port maximum for learned MACs
- MAC learning limit
- Learning limit violation log
- set mac-violation-timer
- Sticky MAC
- Total MAC entries
- MSTP
- STP root guard
- STP BPDU guard
- 'forced-untagged' or 'force-tagged' setting on switch interfaces
- Private VLANs
- Multi-stage load balancing
- MAC/IP/protocol-based VLAN assignment
- Virtual wire
- Loop guard
- VLAN stacking (QinQ)
- VLAN mapping
- MCLAG
- STP support in MCLAGs
- IGMP snooping support in MCLAG

- Edge port
- Host quarantine on switch port

When you configure a trunk interface as an RVI, you must configure a static MAC address to avoid a disruption of adjacency when adding or removing a group of ports.

To configure an RVI:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config system-interface
         edit <interface_name>
            set switch-id <FortiSwitch_serial_number>
            set mode {static | dhcp}
            set ip <IPv4_address_netmask>
            set status {disable | enable}
            set allowaccess {ping | https | http | ssh | snmp | telnet | radius-acct}
            set vlan <VLAN_name>
            set type physical
            set vrf <VRF_name>
         next
      end
   next
end
```

Option	Description	Default
switch-id <FortiSwitch_serial_number>	Required. The FortiSwitch serial number here should match the one in `edit <FortiSwitch_serial_number>`.	No default
mode {static | dhcp}	Configure the connection mode for the interface: • `static`—Configure a static IP address for the interface. • `dhcp`—Configure the interface to receive its IP address from an external DHCP server.	static
ip <IPv4_address_netmask>	Required. Enter the interface IP address and netmask. You can set the IP and netmask, but they are not displayed. The IP address cannot be on the same subnet as any other interface.	0.0.0.0 0.0.0.0
status {disable | enable}	Enable or disable the interface. If the interface is disabled, it does not accept or send packets. If you disable a physical interface, associated virtual interfaces such as VLAN interfaces will also stop.	enable
allowaccess {ping | https | http | ssh | snmp | telnet | radius-acct}	Enter the types of management access permitted on this interface. Separate each type with a space. To add or remove an option from the list, retype the complete list as required.	No default
vlan <string>	Required. Enter the name of the VLAN. Type `?` to see a list of interfaces.	No default
type physical	Enter the type of interface. You need to select `physical` for an RVI.	vlan

Option	Description	Default
vrf <string>	Assign the specified virtual routing and forwarding (VRF) instance to this RVI.	No default

For example:

```
config switch-controller managed-switch
   edit S524DN4K16000116
      config system-interface
         edit "rvi22"
            set switch-id "S524DN4K16000116"
            set ip 10.2.2.2 255.255.255.0
            set allowaccess ping
            set type physical
            set interface "port19"
         next
      end
   next
end
```

Static IPv4 routing

Static routing uses manually configured routes.

To configure a static IPv4 route:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config router-static
         edit <id>
            set switch-id <FortiSwitch_serial_number>
            set blackhole {disable | enable}
            set comment <string>
            set device <string>
            set distance <1-255>
            set dst <IP_address_netmask>
            set dynamic-gateway {disable | enable}
            set gateway <IPv4_address>
            set status {disable | enable}
            set vrf <string>
         next
      end
   next
end
```

Option	Description	Default
switch-id <FortiSwitch_serial_number>	Required. The FortiSwitch serial number here should match the one in `edit <FortiSwitch_serial_number>`.	No default

Option	Description	Default
blackhole {disable | enable}	Enable or disable dropping all packets that match this route.	disable
comment <string>	Optional. Enter a descriptive comment.	No default
device <string>	Enter the name of the interface through which to route traffic. Type ? to see a list of interfaces.	No default
distance <1-255>	Enter the administrative distance for the route.	10
dst <IP_address_ netmask>	Enter the destination IPv4 address and network mask for this route. You can enter 0.0.0.0/0 to create a new static default route.	0.0.0.0 0.0.0.0
dynamic-gateway {disable | enable}	When enabled, the route gateway IP is obtained using DHCP running on the provided route's device interface.	disable
gateway <IPv4_ address>	Required. When enabled, the route gateway IP is obtained using DHCP running on the provided route's device interface.	0.0.0.0
status {disable | enable}	Enable this setting for the route to be added to the routing table.	enable
vrf <string>	Assign the specified virtual routing and forwarding (VRF) instance to this static route. After the static route is created, the VRF instance cannot be changed or unset.	No default

For example:

```
config switch-controller managed-switch
   edit S524DN4K16000116
      config router-static
         edit 1
            set switch-id "S524DN4K16000116"
            set device "rvi22"
            set dst 10.5.5.6 255.255.255.255
            set gateway 10.2.2.1
         next
      end
   next
end
```

Virtual routing and forwarding

You must have an advanced features license to use virtual routing and forwarding.

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

Use the following steps to configure VRF:

1. Create a VRF instance.

   You create a VRF instance by assigning a name and an identifier.

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

2. Assign the VRF instance to an SVI or RVI.

   You assign the VRF instance to an SVI or RVI when you create the SVI or RVI. After the SVI or RVI is created, the VRF instance cannot be changed or unset. You can assign the same VRF instance to more than one SVI or RVI. The VRF instance cannot be assigned to an internal SVI or RVI.

3. Assign the VRF instance to a static route.

   You assign the VRF instance to an IPv4 static route when you create the static route. After the static route is created, the VRF instance cannot be changed or unset. You can assign the same VRF instance to more than one static route.

To create a VRF instance:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config router-vrf
         edit <VRF entry name>
            set switch-id <FortiSwitch_serial_number>
            set vrfid <1-1023>
         next
      end
   next
end
```

Option	Description	Default
switch-id <FortiSwitch_ serial_number>	Required. The FortiSwitch serial number here should match the one in `edit <FortiSwitch_serial_number>`.	No default
vrfid <1-1023>	Required. Set the VRF identifier. You cannot use 252, 253, 254, or 255. After the VRF instance is created, the VRF ID cannot be changed.	0

For example:

```
config switch-controller managed-switch
   edit "S524DN4K16000116"
      config router-vrf
         edit "20"
            set switch-id "S524DN4K16000116"
            set vrfid 20
         next
      end
   next
end
```

To assign the VRF instance to an SVI:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config system-interface
         edit <interface_name>
            set switch-id <FortiSwitch_serial_number>
            set mode {static | dhcp}
            set ip <IPv4_address_netmask>
            set status {disable | enable}
            set allowaccess {ping | https | http | ssh | snmp | telnet | radius-acct}
            set vlan <string>
            set type vlan
            set vrf <VRF_name>
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S524DN4K16000116"
      config system-interface
         edit "svi20"
            set switch-id "S524DN4K16000116"
            set ip 10.2.2.2 255.255.255.0
            set vlan "vlan20"
            set type vlan
            set vrf "20"
         next
      end
   next
end
```

To assign the VRF instance to an RVI:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config system-interface
         edit <interface_name>
            set switch-id <FortiSwitch_serial_number>
            set mode {static | dhcp}
            set ip <IPv4_address_netmask>
            set status {disable | enable}
            set allowaccess {ping | https | http | ssh | snmp | telnet | radius-acct}
            set vlan <VLAN_name>
            set type physical
            set vrf <VRF_name>
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S524DN4K16000116"
      config system-interface
```

```
            edit "rvi22"
               set switch-id "S524DN4K16000116"
               set ip 10.2.2.2 255.255.255.0
               set allowaccess ping
               set type physical
               set interface "port19"
               set vrf "20"
            next
         end
      next
   end
```

To assign the VRF instance to a static route:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config router-static
         edit <id>
            set switch-id <FortiSwitch_serial_number>
            set blackhole {disable | enable}
            set comment <string>
            set device <string>
            set distance <1-255>
            set dst <IP_address_netmask>
            set dynamic-gateway {disable | enable}
            set gateway <IPv4_address>
            set status {disable | enable}
            set vrf <string>
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "S524DN4K16000116"
      config router-static
         edit 1
            set switch-id "S524DN4K16000116"
            set device "svi20"
            set dst 10.5.5.6 255.255.255.255
            set gateway 10.2.2.1
            set vrf "20"
         next
      end
   next
end
```

Configuring a DHCP server

A DHCP server provides an address, from a defined address range, to a client on the network that requests it.

You can configure one or more DHCP servers on any managed FortiSwitch interface. A DHCP server dynamically assigns IP addresses to hosts on the network connected to the interface. The host computers must be configured to obtain their IP addresses using DHCP.

To see which models support this feature, refer to the FortiSwitch feature matrix.

The following table lists the maximum number of clients for the supported FortiSwitch models:

FortiSwitch models	Maximum number of clients
FS-1xx	250
FS-2xx	500
FS-4xx	15,000
FS-5xx	20,000
FS-1048D	30,000
FS-1048E, FS-3032E	50,000

To configure a DHCP server:

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config system-dhcp-server
         edit <id>
            set switch-id <FortiSwitch_serial_number>
            set lease-time <300-8640000>
            set dns-service {local | default | specify}
            set dns-server1 <IPv4_address>
            set dns-server2 <IPv4_address>
            set dns-server3 <IPv4_address>
            set ntp-service {local | default | specify}
            set ntp-server1 <IPv4_address>
            set ntp-server2 <IPv4_address>
            set ntp-server3 <IPv4_address>
            set default-gateway <IPv4_address>
            set netmask <IPv4_address>
            set interface <interface_name>
            config ip-range
               edit <id>
                  set start-ip <IPv4_address>
                  set end-ip <IPv4_address>.
               end
            config options
               edit <id>
                  set code <0-255>
                  set type {hex | string | ip | fqdn>
                  set value <string>
               end
            next
         end
```

```
    next
end
```

Option	Description	Default
switch-id <FortiSwitch_serial_number>	Required.The FortiSwitch serial number here should match the one in `edit <FortiSwitch_serial_number>`.	No default
lease-time <300-8640000>	Enter the lease time in seconds. The lease time determines the length of time an IP address remains assigned to a client. After the lease expires, the address is released for allocation to the next client that requests an IP address. Set this option to 0 for an unlimited lease time. The default lease time is seven days.	604800
dns-service {local | default | specify}	Select how DNS servers are assigned to DHCP clients: • `local`—Use the IP address of the DHCP server interface for the client's DNS server IP address. • `default`—The clients are assigned to the FortiSwitch unit's configured DNS servers. • `specify`—Enter the IPv4 address for up to three DNS servers.	specify
dns-server1 <IPv4_address>	Enter the IP address for DNS server 1.	0.0.0.0
dns-server2 <IPv4_address>	Enter the IP address for DNS server 2.	0.0.0.0
dns-server3 <IPv4_address>	Enter the IP address for DNS server 3.	0.0.0.0
ntp-service {local | default | specify}	Select how Network Time Protocol (NTP) servers are assigned to DHCP clients: • `local`—Use the IP address of the DHCP server interface for the client's NTP server IP address. • `default`—The clients are assigned to the FortiSwitch unit's configured NTP servers. • `specify`—Enter the IPv4 address for up to three NTP servers.	specify
ntp-server1 <IPv4_address>	Enter the IP address for NTP server 1.	0.0.0.0
ntp-server2 <IPv4_address>	Enter the IP address for NTP server 2.	0.0.0.0
ntp-server3 <IPv4_address>	Enter the IP address for NTP server 3.	0.0.0.0
default-gateway <IPv4_address>	Enter the IP address for the default gateway assigned by the DHCP server.	0.0.0.0
netmask <IPv4_address>	Required. Enter the netmask for the addresses that the DHCP server assigns.	0.0.0.0
interface <interface_name>	Required. Enter the name of the interface. The DHCP server can assign IP configurations to clients connected to this interface.	No default

Option	Description	Default
start-ip <IPv4_ address>	Required. Enter the start of the DHCP IP address range.	0.0.0.0
end-ip <IPv4_ address>	Required. Enter the end of the DHCP IP address range.	0.0.0.0
code <0-255>	Required. Select the DHCP option code.	0
type {hex | string | ip | fqdn>	Select the format of the DHCP option: hexadecimal, string, IP address, or fully qualified domain name.	hex
value <string>	Enter the DHCP option value.	No default

For example:

```
config switch-controller managed-switch
   edit "S524DN4K16000116"
      config system-dhcp-server
         edit 1
            set switch-id "S524DN4K16000116"
            set ntp-service default
            set default-gateway 10.2.2.3
            set netmask 255.255.255.0
            set interface "rvi22"
            config ip-range
               edit 1
                  set start-ip 10.2.2.10
                  set end-ip 10.2.2.50
               next
            end
            set dns-server1 10.8.8.8
         next
      end
   next
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
```

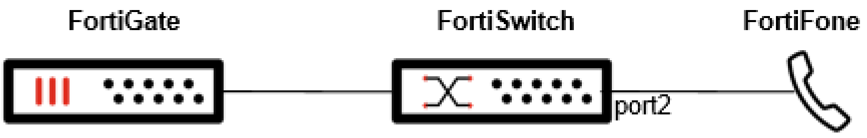
You can display a list of detected devices from the *Device Inventory* menu in the GUI. To list the detected devices in the CLI, enter the following command:

```
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.



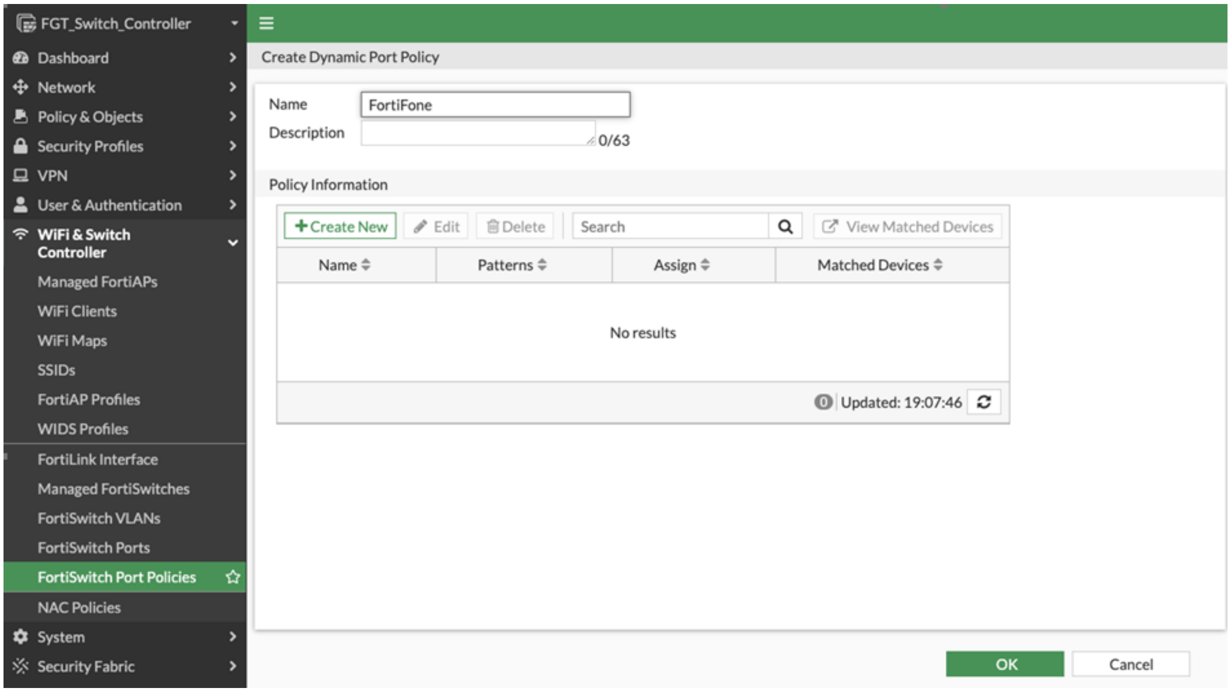
The following is a summary of the procedure:

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`.



Create Dynamic Port Policy

Name: FortiFone

Description: 0/63

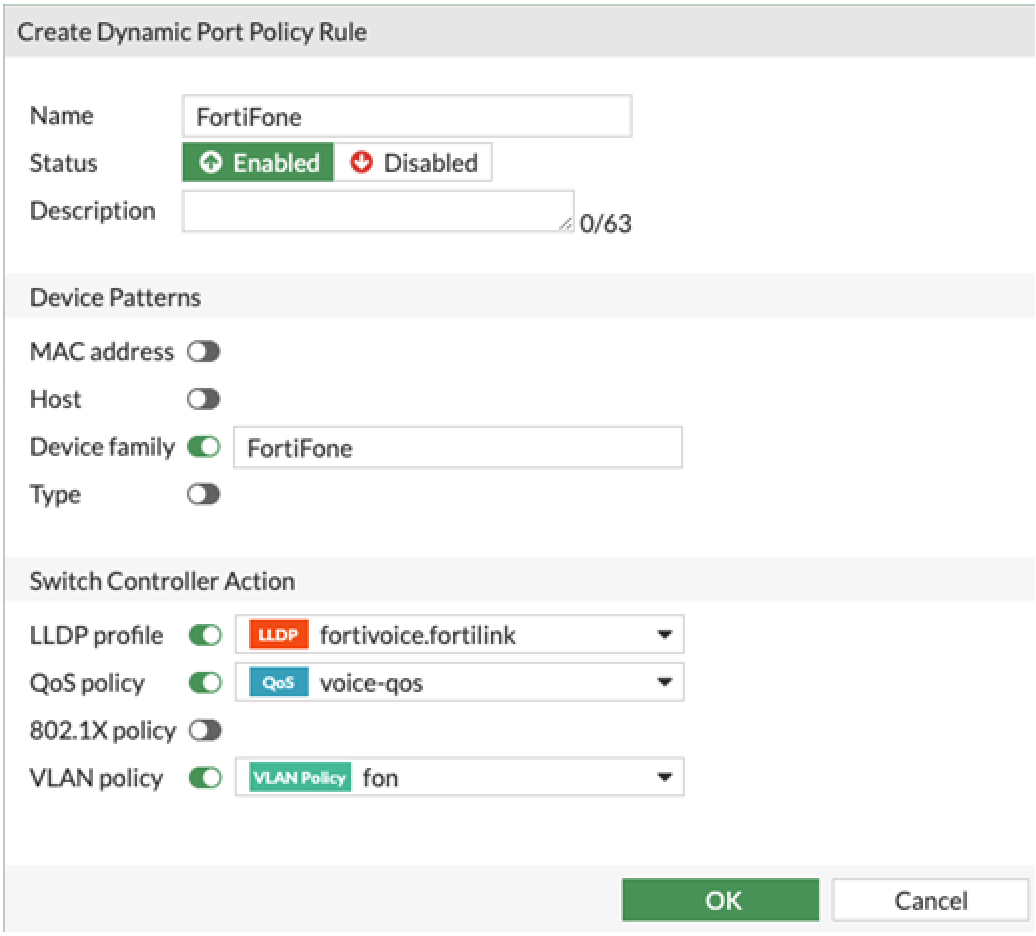
Policy Information

Name	Patterns	Assign	Matched Devices
No results			

Updated: 19:07:46

   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.



Create Dynamic Port Policy Rule

Name: FortiFone

Status: Enabled | Disabled

Description: 0/63

Device Patterns

MAC address: off

Host: off

Device family: on — FortiFone

Type: off

Switch Controller Action

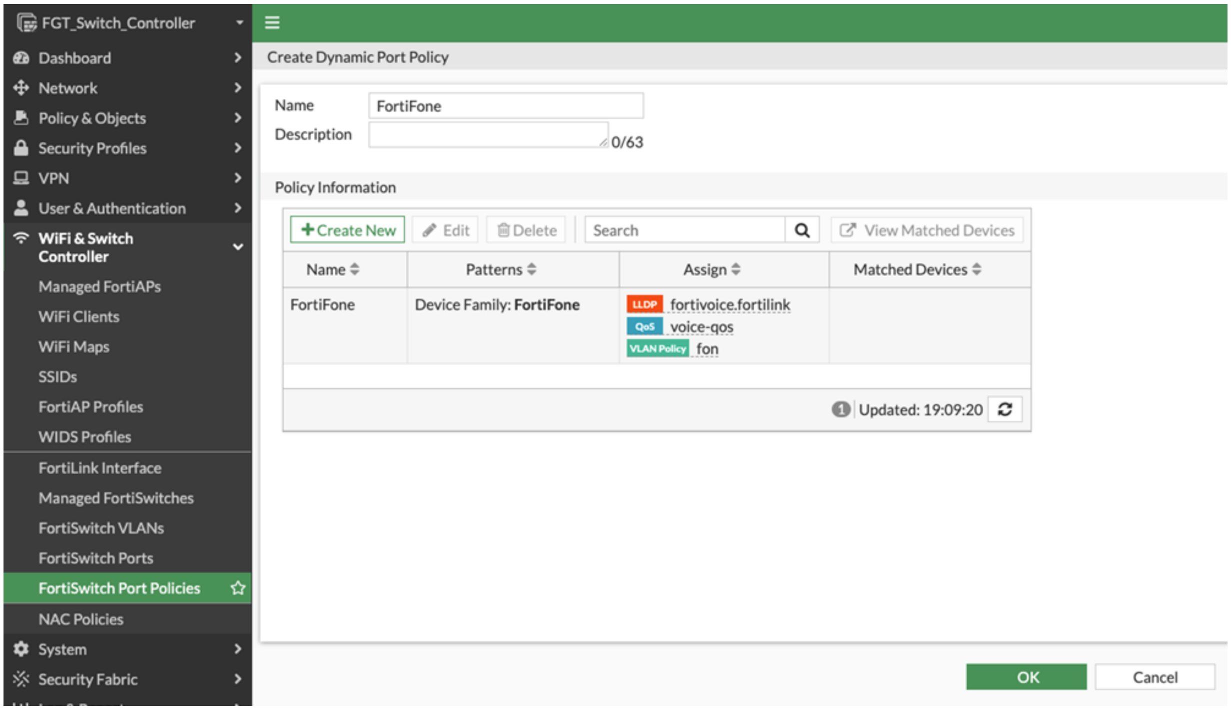
LLDP profile: on — LLDP fortivoice.fortilink

QoS policy: on — QoS voice-qos

802.1X policy: off

VLAN policy: on — VLAN Policy fon

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



Create Dynamic Port Policy

Name FortiFone

Description 0/63

Policy Information

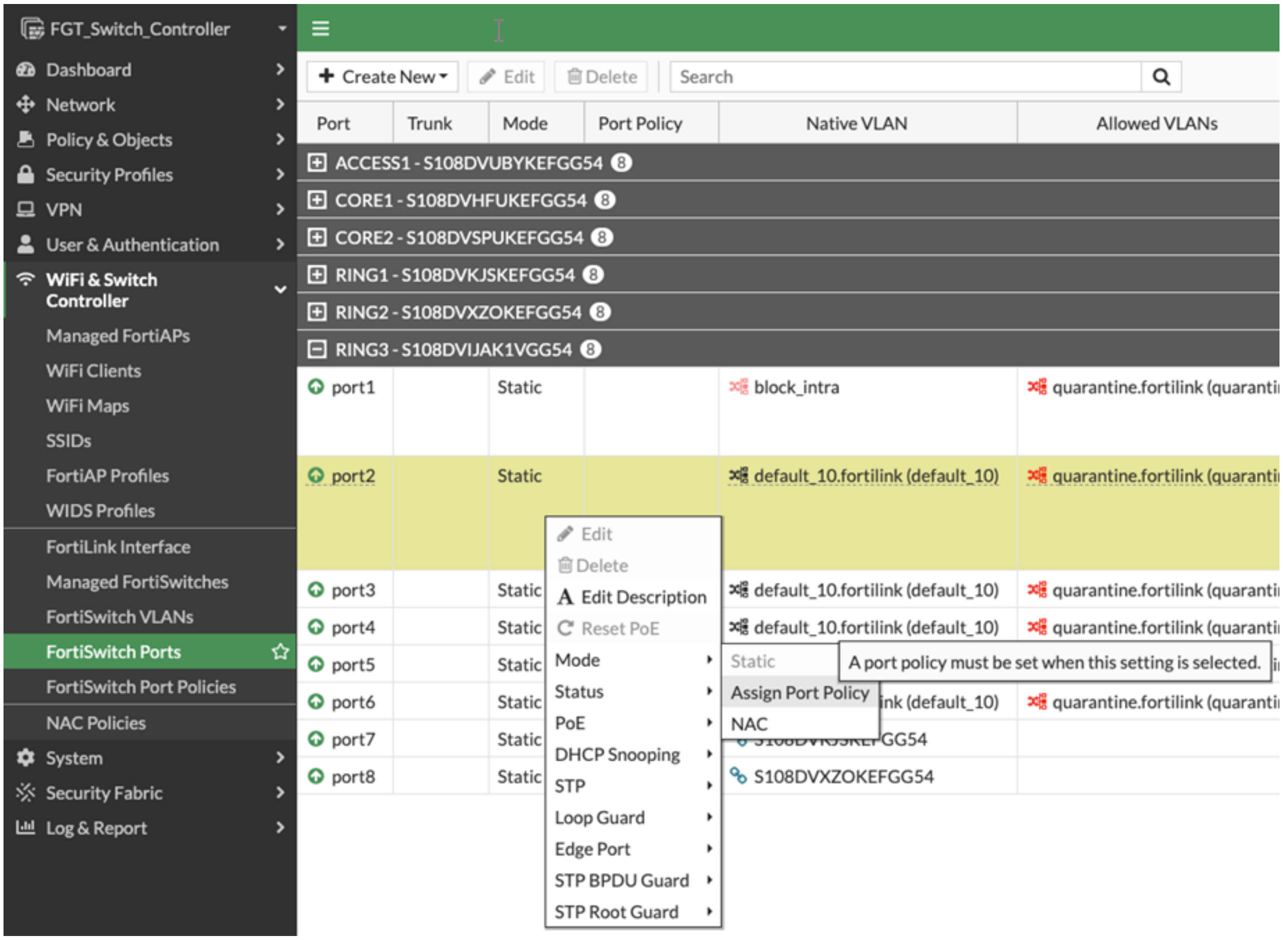
Name	Patterns	Assign	Matched Devices
FortiFone	Device Family: **FortiFone**	LLDP fortivoice.fortilink QoS voice-qos VLAN Policy fon	

1 Updated: 19:09:20

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

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

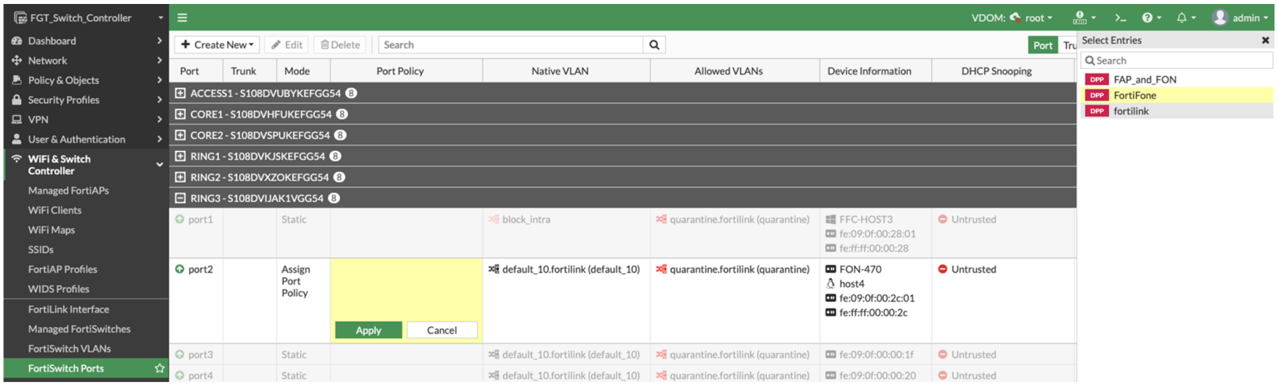
3. Right-click *port2* and select *Mode > Assign Port Policy*.



A port policy must be set when this setting is selected.

Port	Trunk	Mode	Port Policy	Native VLAN	Allowed VLANs
ACCESS1 - S108DVUBYKEFGG54 8					
CORE1 - S108DVHFUKEFGG54 8					
CORE2 - S108DVSPUKEFGG54 8					
RING1 - S108DVKJSKEFGG54 8					
RING2 - S108DVXZOKEFGG54 8					
RING3 - S108DVIJAK1VGG54 8					
port1		Static		block_intra	quarantine.fortilink (quaranti
port2		Static		default_10.fortilink (default_10)	quarantine.fortilink (quaranti
port3		Static		default_10.fortilink (default_10)	quarantine.fortilink (quaranti
port4		Static		default_10.fortilink (default_10)	quarantine.fortilink (quaranti
port5		Static			
port6		Static		ink (default_10)	quarantine.fortilink (quaranti
port7		Static		GG54	
port8		Static		S108DVXZOKEFGG54	

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



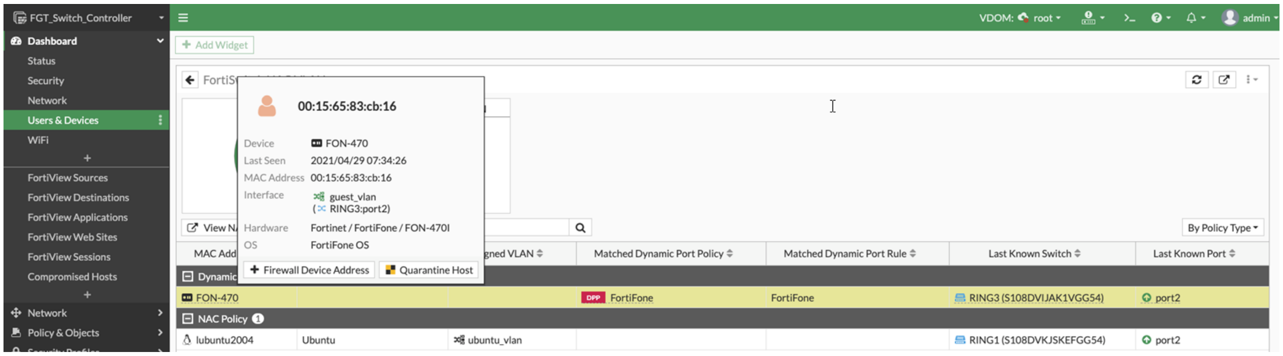
Port	Trunk	Mode	Port Policy	Native VLAN	Allowed VLANs	Device Information	DHCP Snooping
ACCESS1 - S108DVUBYKEFGG54 8							
CORE1 - S108DVHFUKEFGG54 8							
CORE2 - S108DVSPUKEFGG54 8							
RING1 - S108DVKJSKEFGG54 8							
RING2 - S108DVXZOKEFGG54 8							
RING3 - S108DVIJAK1VGG54 8							
port1		Static		block_intra	quarantine.fortilink (quarantine)	FFC-HOST3 fe:09:0f:00:28:01 fe:ff:ff:00:00:28	Untrusted
port2		Assign Port Policy		default_10.fortilink (default_10)	quarantine.fortilink (quarantine)	FON-470 host4 fe:09:0f:00:2c:01 fe:ff:ff:00:00:2c	Untrusted
port3		Static		default_10.fortilink (default_10)	quarantine.fortilink (quarantine)	fe:09:0f:00:00:1f	Untrusted
port4		Static		default_10.fortilink (default_10)	quarantine.fortilink (quarantine)	fe:09:0f:00:00:20	Untrusted

Select Entries

- DPP FAP_and_FON
- DPP FortiFone
- DPP fortilink

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.



00:15:65:83:cb:16

Device: FON-470
Last Seen: 2021/04/29 07:34:26
MAC Address: 00:15:65:83:cb:16
Interface: guest_vlan (RING3:port2)
Hardware: Fortinet / FortiFone / FON-470I
OS: FortiFone OS

MAC Add		gned VLAN	Matched Dynamic Port Policy	Matched Dynamic Port Rule	Last Known Switch	Last Known Port
Dynamic						
FON-470			DPP FortiFone	FortiFone	RING3 (S108DVIJAK1VGG54)	port2
NAC Policy 1						
lubuntu2004	Ubuntu	ubuntu_vlan			RING1 (S108DVKJSKEFGG54)	port2

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
```

The managed-switch ports matched to the dynamic port policy interface-tag category are displayed under the `managed-switch port` CLI command.

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:

- Creating LLDP asset tags for each managed FortiSwitch on page 175
- Adding media endpoint discovery (MED) to an LLDP configuration on page 175
- Displaying LLDP information on page 176
- Configuring the LLDP settings on page 176

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	

Variable	Description
{address-civic | coordinates | elin-number}	Select which Media Endpoint Discovery (MED) location type-length-value (TLV) category to edit.
status {enable | disable}	Enable or disable whether this TLV is transmitted.
sys-location-id <string>	If you enabled the status, you can enter the location service identifier. The maximum length is 63 characters.
config-tlvs	
<TLV_name>	Enter the name of a custom TLV entry.
oui <hexadecimal_number>	Ener the organizationally unique identifier (OUI), a 3-byte hexadecimal number, for this TLV.
subtype <0-255>	Enter the organizationally defined subtype.
information-string <0-507>	Enter the organizationally defined information string in hexadecimal bytes.

To configure LLDP settings in FortiOS:

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

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

To configure dynamic detection of LLDP neighbor devices in FortiSwitchOS:

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

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:

FortiLink secure fabric

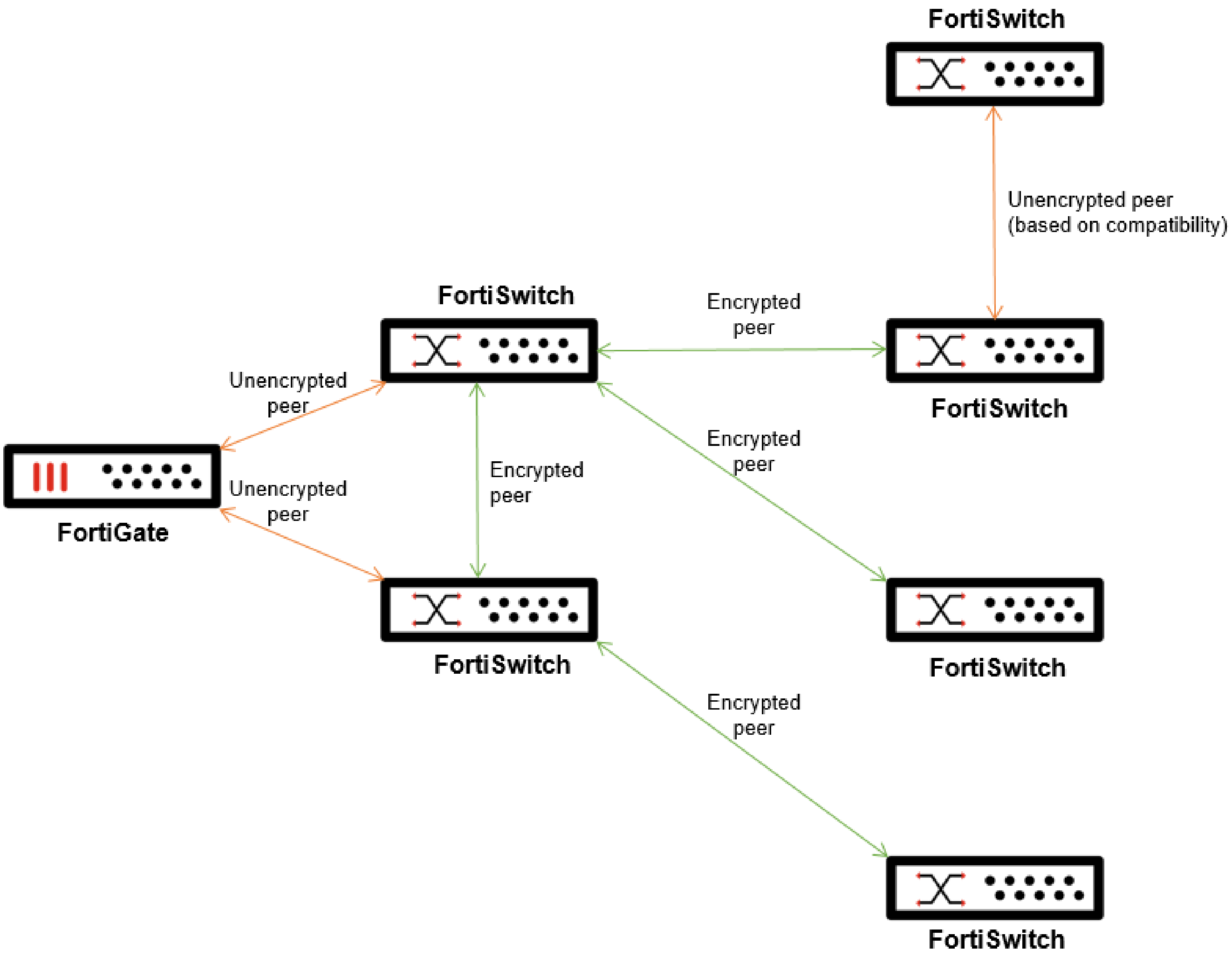
The FortiLink secure fabric provides authentication and encryption to all fabric links, wherever possible, making your Security Fabric more secure.

By default, authentication and encryption are disabled on the Security Fabric. After you specify the authentication mode and encryption mode for the FortiLink secure fabric in the LLDP profile:

1. FortiOS authenticates the connected LLDP neighbors.
2. FortiOS forms an authenticated secure inter-switch link (ISL) trunk.
3. Ports that are members of the authenticated secure ISL trunk are encrypted with Media Access Control security (MACsec) (IEEE 802.1AE-2018).
4. After the peer authentication (and MACsec encryption, if enabled) is complete, FortiOS configures the user VLANs.
5. If FortiOS detects a new FortiSwitch unit in the Security Fabric, one of the FortiSwitch peers validates whether the new switch has a Fortinet factory SSL certificate chain. If the new FortiSwitch unit has a valid certificate, it becomes a FortiSwitch peer in the FortiLink secure fabric.

- When `set static-isl` is enabled, authentication and encryption are not supported.
- When you are using the FortiLink secure fabric, locking down the Security Fabric topology from the *Security Fabric > Security Rating* page is not supported.
- When you are using the FortiLink secure fabric, the `diagnose switch-controller switch-recommendation fabric-lockdown-enable` command is not supported.

The following figure shows the FortiLink secure fabric. The links between the FortiGate device and the managed FortiSwitch units are always unencrypted. The green links between FortiSwitch peers are encrypted ISLs. The orange links between FortiSwitch peers are unencrypted ISLs.



Authentication modes

By default, there is no authentication. You can select one of three authentication modes:

- *Legacy*—This mode is the default. There is no authentication.
- *Relax*—If authentication succeeds, FortiOS forms a secure ISL trunk. If authentication fails, FortiOS forms a restricted ISL trunk.

  A restricted ISL trunk is the same as a regular ISL trunk, but FortiOS does not add any user VLANs. The restricted ISL trunk allows limited access so that users can authenticate unauthenticated switches. Use a restricted ISL trunk for a new FortiSwitch unit that was just added to the Security Fabric or a FortiSwitch unit that does not support authentication or encryption.
- *Strict*—If authentication succeeds, FortiOS forms a secure ISL trunk. If authentication fails, no ISL trunk is formed.

Encryption modes

By default, there is no encryption. You must select the `strict` or `relax` authentication mode before you can select the `mixed` or `must` encryption mode.

- *None*—There is no encryption, and FortiOS does not enable MACsec on the ISL trunk members.
- *Mixed*—FortiOS enables MACsec on the ISL trunk ports that support MACsec; the ISL trunk members act as encrypted links. FortiOS disables MACsec on the ISL members that do not support MACsec; these ISL trunk members act as unencrypted links.
- *Must*—FortiOS enables MACsec on all ISL trunk members. If the port supports MACsec, the port acts as an encrypted link. If the port does not support MACsec, the port is removed from the ISL trunk, but the port still functions as a user port.

Configuring the FortiLink secure fabric

To configure the FortiLink secure fabric:

1. Configure the LLDP profile.
2. Assign the LLDP profile to a FortiSwitch physical port.

To configure the LLDP profile:

```
config switch-controller lldp-profile
   edit {LLDP_profile_name | default-auto-isl | default-auto-mclag-icl}
      set auto-isl-auth {legacy | relax | strict}
      set auto-isl-auth-user <string>
      set auto-isl-auth-identity <string>
      set auto-isl-auth-reauth <10-3600>
      set auto-isl-auth-encrypt {none | mixed | must}
      set auto-isl-auth-macsec-profile default-macsec-auto-isl
   next
end
```

Option	Description	Default
{LLDP_profile_name | default-auto-isl | default-auto-mclag-icl}	Select one of the two default LLDP profiles (`default-auto-isl` or `default-auto-mclag-icl`) or create your own LLDP profile.	No default
auto-isl-auth {legacy | relax | strict}	Select the authentication mode.	legacy
auto-isl-auth-user <string>	Select the user certificate, such as `Fortinet_Factory`. This option is available when `auto-isl-auth` is set to `relax` or `strict`.	No default
auto-isl-auth-identity <string>	Enter the identity, such as `fortilink`. This option is available when `auto-isl-auth` is set to `relax` or `strict`.	No default

Option	Description	Default
auto-isl-auth-reauth <10-3600>	Enter the reauthentication period in minutes. This option is available when `auto-isl-auth` is set to `relax` or `strict`.	3600
auto-isl-auth-encrypt {none | mixed | must}	Select the encryption mode. This option is available when `auto-isl-auth` is set to `strict` or `relax`.	none
auto-isl-auth-macsec-profile <string>	Use the `default-macsec-auto-isl` profile. This option is available when `auto-isl-auth-encrypt` is set to `mixed` or `must`.	default-macsec-auto-isl

Configuration example

```
config switch-controller lldp-profile
   edit customLLDPprofile
      set auto-isl-auth relax
      set auto-isl-auth-user Fortinet_Factory
      set auto-isl-auth-identity fortilink
      set auto-isl-auth-encrypt mixed
      set auto-isl-auth-macsec-profile default-macsec-auto-isl
   next
end

config switch-controller managed-switch
   edit S524DF4K15000024
      config ports
         edit port49
            set lldp-profile customLLDPprofile
         next
      end
   next
end
```

Viewing the FortiLink secure fabric

To get information from the FortiGate device about which FortiSwitch units ports are authenticated, secured, or restricted:

```
execute switch-controller get-physical-conn {dot | standard} <FortiLink_interface>
```

To get the FortiLink authentication status for the port from the FortiSwitch unit:

```
diagnose switch fortilink-auth status <port_name>
```

To get the FortiLink authentication traffic statistics for the port from the FortiSwitch unit:

```
diagnose switch fortilink-auth statistics <port_name>
```

To delete the FortiLink authentication traffic statistics for the port from the FortiSwitch unit:

```
execute fortilink-auth clearstat physical-port <port_name>
```

To reauthenticate FortiLink secure fabric peers from the specified port from the FortiSwitch unit:

```
execute fortilink-auth reauth physical-port <port_name>
```

To reset the authentication for the FortiLink secure fabric from the FortiSwitch unit on the specified port:

```
execute fortilink-auth reset physical-port <port_name>
```

To display statistics and status of the FortiLink secure fabric for the port from the FortiSwitch unit:

```
get switch lldp auto-isl-status <port_name>
```

To display the status of the FortiLink secure fabric for the trunk from the FortiSwitch unit:

```
get switch trunk
```

Requirements and limitations

- FortiOS 7.4.1 or later and FortiSwitchOS 7.4.1 or later are required.
- FortiLink mode over a layer-2 network and FortiLink mode over a layer-3 network are supported.
- VXLAN is not supported.
- When a new FortiSwitch unit is added to the fabric, it must have a Fortinet factory SSL certificate before it is allowed to become an authenticated peer within the FortiLink secure fabric.
- When a new FortiSwitch unit is added to the FortiLink secure fabric with the `strict` authentication mode, the restricted ISL trunk is not formed. You must configure the FortiSwitch unit manually (under the `config switch lldp-profile` command).
- You need to manually import a custom certificate on the managed FortiSwitch units first; then you can specify the custom certificate on the FortiLink secure fabric with the `set auto-isl-auth-user` command under `config switch-controller lldp-profile`. After that, you can configure the custom certificate on the running Security Fabric.

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.

NAC settings are enabled automatically on the `fortilink` interface when the first FortiSwitch unit is discovered. If no FortiSwitch unit has been discovered yet or the NAC configuration has been deleted from the `fortilink` interface, you need to configure the FortiSwitch NAC settings before defining a NAC policy. See Configuring the FortiSwitch NAC settings on page 184.

Summary of the procedure

1. Define a FortiSwitch NAC VLAN. See Defining a FortiSwitch NAC VLAN on page 183.
2. Configure the FortiSwitch NAC settings. See Configuring the FortiSwitch NAC settings on page 184.
3. Create a FortiSwitch NAC policy. See Defining a FortiSwitch NAC policy on page 188.
4. View the devices that match the NAC policy. See Viewing the devices that match the NAC policy on page 203.
5. View device statistics. See Viewing device statistics on page 204.

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*, click *Create New*, and change the following settings:

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

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

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.fortilink (onboarding)` NAC VLAN.
3. Click *Edit*.
4. Make your changes.
5. Click *OK* to save your changes.

Configuring the FortiSwitch NAC settings

NAC settings are enabled automatically on the `fortilink` interface when the first FortiSwitch unit is discovered. If no FortiSwitch unit has been discovered yet or the NAC configuration has been deleted from the `fortilink` interface, you need to configure the FortiSwitch NAC settings before defining a NAC policy. See Configuring the FortiSwitch NAC settings on page 184.

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 1 to 1,440 minutes.

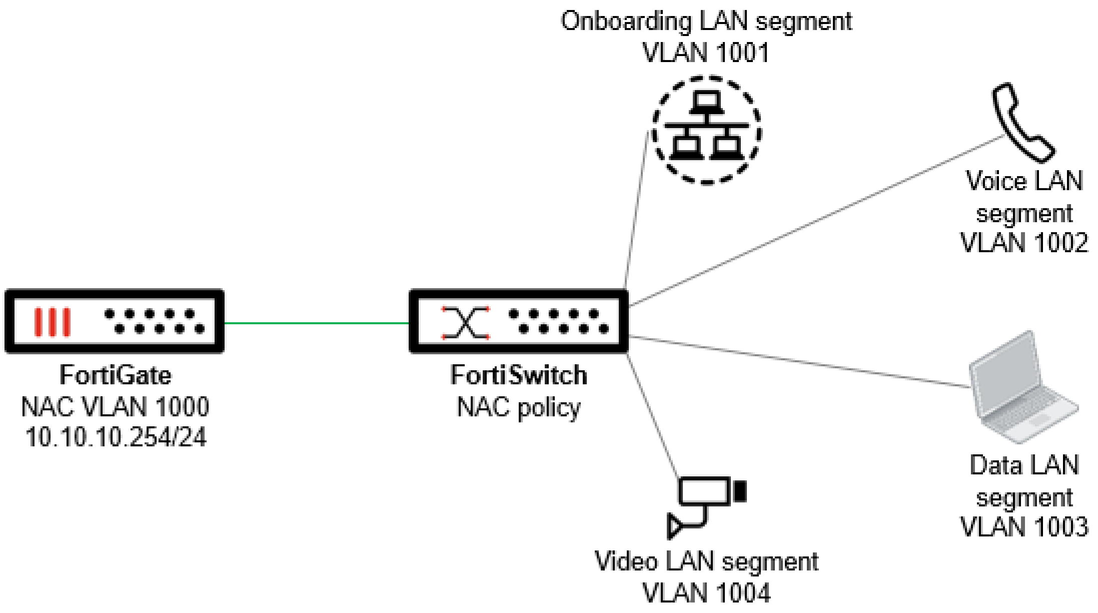
When NAC devices are discovered, they are assigned to the NAC onboarding VLAN. You can specify the default `onboarding` VLAN or specify another existing VLAN. By default, there is no NAC onboarding VLAN assigned.

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-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-148E, FS-148E-POE, and FSR-216F-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 five types of NAC policies:

- *Device*—The NAC policy matches devices with the specified MAC address, hardware vendor, device family, type, operating system, and user. See Creating a device policy on page 189. Visit the following location to see a list of values for hardware vendor, type, device family, and operating system: https://filestore.fortinet.com/product-downloads/fortilink/HTFO_list.json
- *User*—The NAC policy matches devices belonging to the specified user group. See Creating a user policy on page 192.
- *EMS tag*—The NAC policy matches devices with the specified FortiClient EMS tag. See Creating an EMS-tag policy on page 194.
- *FortiVoice tag*—The NAC policy matches the specified FortiVoice tag. See Creating a FortiVoice-tag policy on page 196.
- *Vulnerability*—The NAC policy matches devices with the specified severity level, which indicates how vulnerable an IoT device is. See Creating a vulnerability policy on page 200.

NAC policies are matched in the order that they are listed in the configuration. You can change the order of the policies in the GUI and CLI.

To change the priority of NAC policies in the GUI, go to *WiFi & Switch Controller > NAC Policies* and drag the NAC policy above or below other NAC policies.

To change the priority of NAC policies in the CLI, enter the following commands:

```
config user nac-policy
   move <NAC_policy_name> {after | before} <NAC_policy_name>
end
```

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 202.

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 184.

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.

Starting in FortiOS 7.4.0 with FortiSwitchOS 7.4.0, you can use NAC to identify Internet of Things (IoT) and Operational Technology (OT) devices that need to be patched and isolate these devices in a separate VLAN segment. You can specify how severe the IoT and OT vulnerabilities must be for the devices to be isolated

This feature requires that the FortiGate device has a valid Attack Surface Security Rating service license. You can check whether the FortiGate device has the Attack Surface Security Rating service license (FGSA) in the FortiOS CLI with the `diagnose test update info` command. You can also check the *Attack Surface Security Rating* field on the *System > FortiGuard* page.

Starting in FortiOS 7.4.4, the NAC policy will match a dynamic MAC address group of all FortiFones registered with a FortiVoice unit.

Starting in FortiOS 7.4.4, you can use the CLI to control how long matched devices are kept for NAC policies. In previous releases, matched devices were deleted when the connection-ID table entry was deleted, the port link status went down, the device was inactive, or the switch was offline.

To control how long matched devices are kept:

1. Change the `set match-type` setting from `dynamic` to `override`.
2. Select the number of days to keep matched devices with the `set match-period` command. By default, `match-period` is set to 0, and the matched devices are kept forever or until a user-configured event occurs in the CLI or the FortiGate device is restarted. You can change the value to 1 to 120 days to keep matched devices.

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.

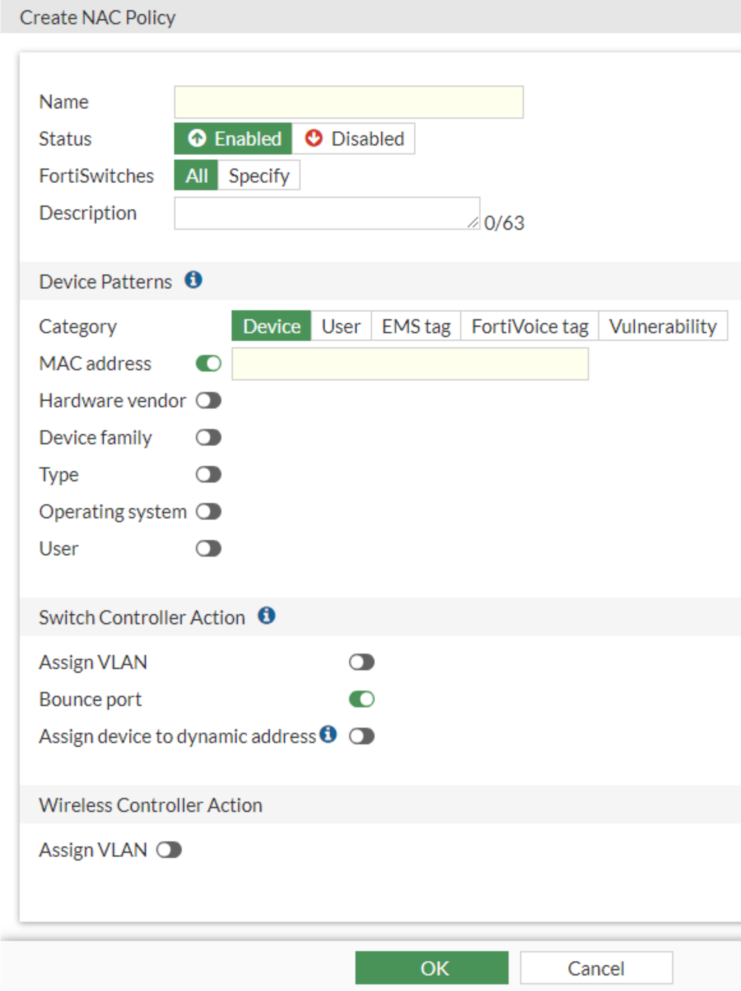
Starting in FortiOS 7.6.3, when you create a device NAC policy in the FortiOS GUI, FortiOS suggests values when you select the hardware vendor, device family, type, operating system, and host to match. For example, if you want the NAC policy to match a device family, FortiOS suggests *FortiSwitch*, *FortiGate*, *FortiAP*, *FortiFone*, *FortiCam*, *FortiRecorder*, *FortiManager*, *FortiAnalyzer*, *Mac*, *iPhone*, *Galaxy*, *Virtual Machine*, and *Printer*.

To identify devices to add to a device policy:

- Use the `diagnose user device list` command to see devices connected to your FortiGate device.
- Use the FortiGuard IoT Detection service 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*.



Create NAC Policy

Name

Status [✓ Enabled] Disabled

FortiSwitches [✓ All] Specify

Description 0/63

Device Patterns

Category [✓ Device] User EMS tag FortiVoice tag Vulnerability

MAC address ●

Hardware vendor ○

Device family ○

Type ○

Operating system ○

User ○

Switch Controller Action

Assign VLAN ○

Bounce port ●

Assign device to dynamic address ○

Wireless Controller Action

Assign VLAN ○

3. In the *Name* field, enter a name for the NAC policy.
   You can enter a number as the NAC policy name, although names are string values.
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. Click *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 hos <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>
      set match-type {dynamic | override}
      set match-period <0-120>
   end
```

For example:

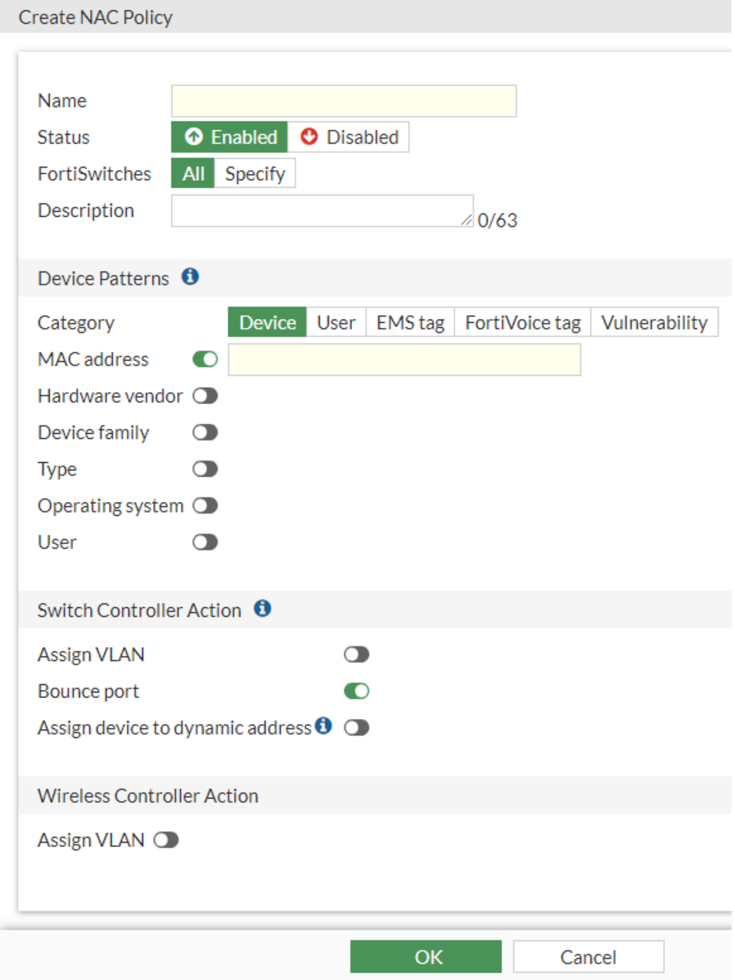
```
config user nac-policy
   edit "OFFICE_VM"
      set hw-vendor "VMware"
      set switch-fortilink "fortilink"
      set switch-mac-policy "OFFICE_VM"
      set firewall-address "office_vm_device"
   next
end
```

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 to create a user policy:

1. Go to *WiFi & Switch Controller > NAC Policies*.
2. Click *Create New*.



3. In the *Name* field, enter a name for the NAC policy.
   You can enter a number as the NAC policy name, although names are string values.
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. Click *OK* to create the new NAC policy.

Using the CLI to create a user policy:

```
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>
      set match-type {dynamic | override}
      set match-period <0-120>
   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. On the FortiGate device, create a firewall policy to allow FortiClient endpoints to always reach FortiClient EMS before and after matching the FortiLink NAC policy.
2. In FortiClient EMS, group FortiClient Fabric Agent endpoints with an EMS tag.
3. In FortiClient EMS, share these endpoint groups with a FortiGate unit over the EMS connector.
4. 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
   ```

5. In FortiOS, verify the EMS certificate. For example:

   ```
   execute fctems verify EMS_Server
   ```

6. In FortiOS, check that the FortiGate unit and FortiClient are connected:

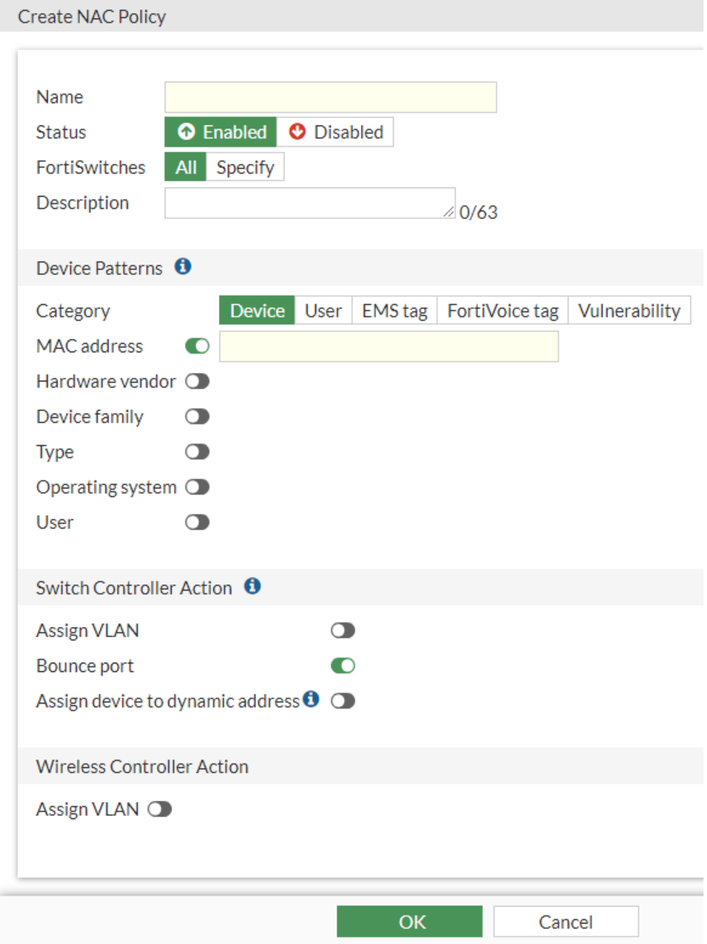
   ```
   diagnose user device get <FortiClient_MAC_address>
   ```

7. 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. Click *Create New*.



Create NAC Policy

Name

Status: [✓ Enabled] Disabled

FortiSwitches: [✓ All] Specify

Description 0/63

Device Patterns

Category: [✓ Device] User EMS tag FortiVoice tag Vulnerability

MAC address ●

Hardware vendor ○

Device family ○

Type ○

Operating system ○

User ○

Switch Controller Action

Assign VLAN ○

Bounce port ●

Assign device to dynamic address ○

Wireless Controller Action

Assign VLAN ○

3. In the *Name* field, enter a name for the NAC policy.
   You can enter a number as the NAC policy name, although names are string values.
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. Click *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>
      set match-type {dynamic | override}
      set match-period <0-120>
   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 FortiVoice-tag policy

A FortiVoice-tag policy matches devices with a specified FortiVoice tag and then assigns a specific VLAN to those devices. The FortiVoice tag identifies a dynamic MAC address group of all FortiFones registered with a FortiVoice unit.

The required FortiVoice version for this feature is 7.0.1 or higher. FortiOS must be 7.4.4 or higher.

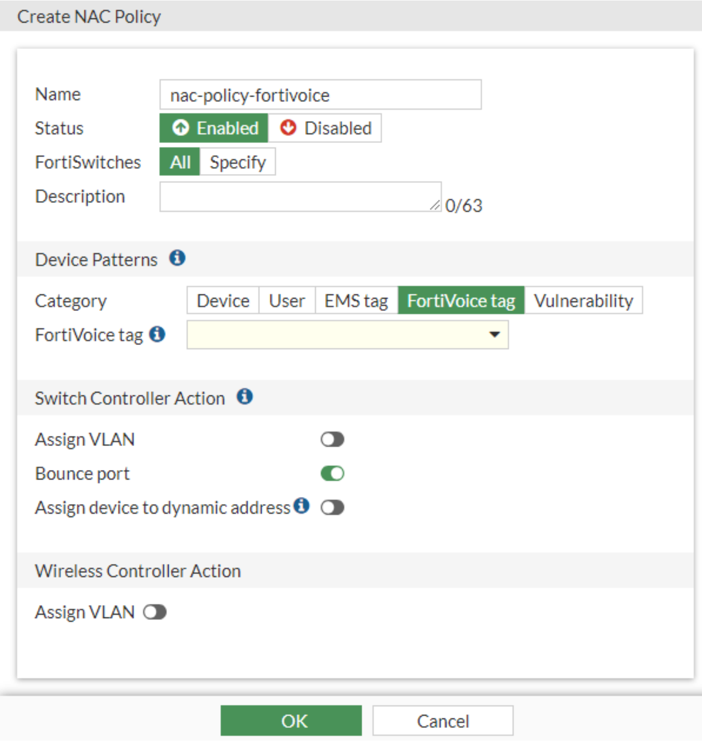
Before creating an FortiVoice-tag policy:

1. On the FortiGate device, create a firewall policy to allow FortiFones to always reach FortiVoice before and after matching the FortiLink NAC policy.
2. Connect the FortiFones to the managed-switch ports and enable NAC on the ports.
3. Connect FortiVoice to the FortiGate device on a different subnet.
4. Ensure that the FortiFones get connected and registered to FortiVoice on the onboarding VLAN.
   The FortiVoice connector pushes the FortiVoice tags to the FortiGate device, along with the registered FortiFone MAC/IP address.
5. In FortiOS, verify which FortiFone MAC/IP address is added to the dynamic firewall list when it gets registered with FortiVoice:
   `diagnose firewall dynamic list`
6. Configure the `fortivoice-tag` NAC policy, which helps NAC to move the FortiFone to the data VLAN.

Using the GUI to create a FortiVoice-tag policy:

1. Go to *WiFi & Switch Controller > NAC Policies*.
2. Click *Create New*.
3. In the *Name* field, enter a name for the NAC policy.
   You can enter a number as the NAC policy name, although names are string values.
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 *FortiVoice tag* for the category.
   NOTE: The object type of the FortiVoice tag must be MAC.



Create NAC Policy

Name: nac-policy-fortivoice
Status: [✓ Enabled] Disabled
FortiSwitches: [✓ All] Specify
Description: 0/63

Device Patterns

Category: Device User EMS tag [✓ FortiVoice tag] Vulnerability
FortiVoice tag:

Switch Controller Action

Assign VLAN: off
Bounce port: on
Assign device to dynamic address: off

Wireless Controller Action

Assign VLAN: off

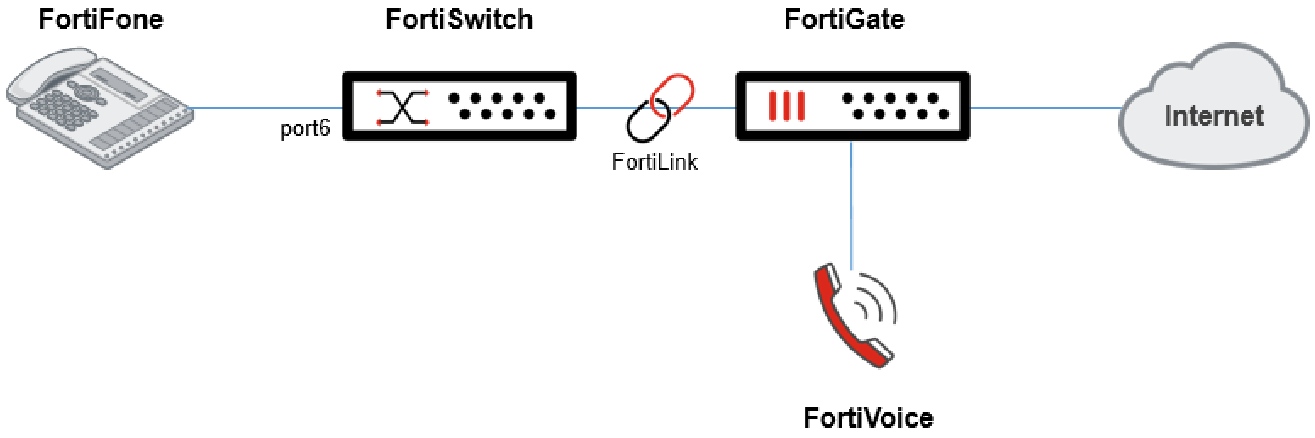
7. Select which FortiVoice tag that devices must be assigned.
8. If you want to assign a specific VLAN to a device assigned to the specified FortiVoice tag, select *Assign VLAN* and enter the VLAN identifier.
9. Click *OK* to create the new NAC policy.

Using the CLI to create a FortiVoice-tag policy:

```
config user nac-policy
   edit <policy_name>
      set description <description_of_policy>
      set category fortivoice-tag
      set status enable
      set fortivoice-tag <string>
      set switch-fortilink <FortiLink_interface>
      set switch-group <list_of_FortiSwitch_groups>
      set switch-mac-policy <switch_mac_policy>
      set firewall-address <firewall_address_name>
      set ssid-policy <policy_name>
      set match-type {dynamic | override}
      set match-period <0-120>
   next
end
```

Configuration example

The NAC policy on the FortiGate matches the dynamic FortiVoice-tag MAC address. The MAC address is connected to a FortiSwitch port (port6). After the MAC address is matched, port6 is moved to vlan12, where traffic is controlled for registered FortiFones.

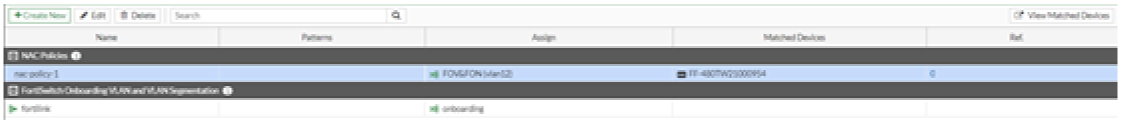


To configure this example in the GUI:

1. Configure the FortiVoice-tag NAC policy.
   a. Go to *WiFi & Switch Controller > NAC Policies* and click *Create New*.
   b. In the *Name* field, enter `nac-policy-fortivoice`.
   c. Select *FortiVoice tag* for the category.
   d. Enter `MAC_FortiVoice_Registered_Phones` in the *FortiVoice tag* field.
   e. Use the CLI to configure the NAC policy to match the FortiVoice tag.
   f. Enable *Assign VLAN* and select *vlan12*.
   g. Configure the other settings as needed.
   h. Click *OK*.
2. Enable NAC on port6:
   a. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
   b. Right-click port6 and set the *Mode* to *NAC*.
3. Configure a firewall policy to control the outbound internet access for FortiFones (vlan12 to wan1).
   a. Go to *Policy & Objects > Firewall Policy* and click *Create New*.
   b. In the *Name* field, enter a name for the policy.
   c. From the *Incoming Interface* dropdown list, select *vlan12*.
   d. From the *Outgoing Interface* dropdown list, select *wan1*.
   e. In the *Source* field, click +, select *all* from the *Select Entries* pane, and click *Close*.
   f. In the *Destination* field, click +, select *all* from the *Select Entries* pane, and click *Close*.
   g. In the *Schedule* dropdown list, select *always*.
   h. For the *Action* field, click *ACCEPT*.
   i. Configure the other settings as needed.

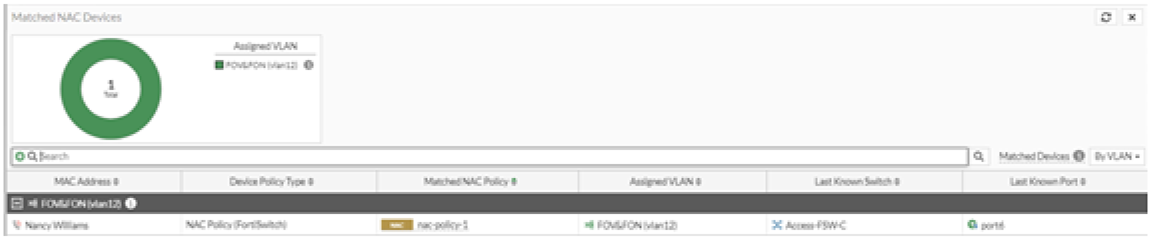
   j. Click *OK*

4. Generate traffic from the FortiFone.
5. After the NAC policy is matched, go to *WiFi & Switch Controller > NAC Policies* to view the device matched to the policy.



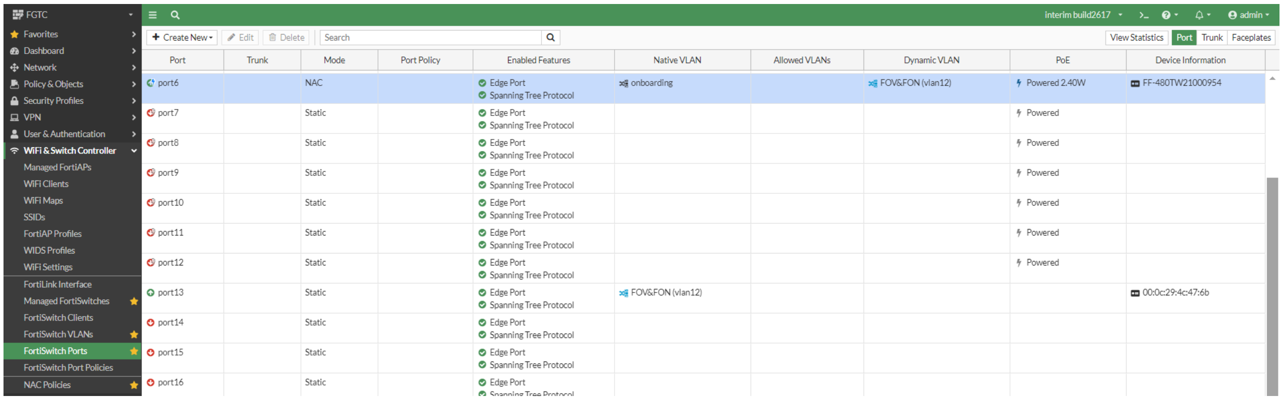
Name	Patterns	Assign	Matched Devices	Ref.
NAC Policies				
nac-policy-1		FOV&FON (vlan12)	FF-480TW21000954	0
FortiSwitch Onboarding VLAN and VLAN Segmentation				
fortilink		onboarding		

   The FortiFone is also shown on *Dashboard > Assets & Identities* in the *Matched NAC Devices* widget.



MAC Address	Device Policy Type	Matched NAC Policy	Assigned VLAN	Last Known Switch	Last Known Port
FOV&FON (vlan12)					
Nancy Williams	NAC Policy (FortiSwitch)	NAC nac-policy-1	FOV&FON (vlan12)	Access-FSW-C	port6

6. Go to *WiFi & Switch Controller > FortiSwitch Ports* and locate the port that the FortiFone is connected to.



Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	Dynamic VLAN	PoE	Device Information
port6		NAC		Edge Port Spanning Tree Protocol	onboarding		FOV&FON (vlan12)	Powered 2.40W	FF-480TW21000954
port7		Static		Edge Port Spanning Tree Protocol				Powered	
port8		Static		Edge Port Spanning Tree Protocol				Powered	
port9		Static		Edge Port Spanning Tree Protocol				Powered	
port10		Static		Edge Port Spanning Tree Protocol				Powered	
port11		Static		Edge Port Spanning Tree Protocol				Powered	
port12		Static		Edge Port Spanning Tree Protocol				Powered	
port13		Static		Edge Port Spanning Tree Protocol	FOV&FON (vlan12)				00:0c:29:4c:47:6b
port14		Static		Edge Port Spanning Tree Protocol					
port15		Static		Edge Port Spanning Tree Protocol					
port16		Static		Edge Port Spanning Tree Protocol					

   The port has been dynamically assigned vlan12.

To configure this example in the CLI:

1. Configure the FortiVoice-tag NAC policy.

```
config user nac-policy
   edit "nac-policy-fortivoice"
      set category fortivoice-tag
      set fortivoice-tag "MAC_FortiVoice_Registered_Phones"
      set switch-fortilink "fortilink"
      set switch-mac-policy "mac-policy-1"
   next
end
```

2. Configure the VLAN in the MAC policy.

```
config switch-controller mac-policy
   edit "mac-policy-1"
      set fortilink "fortilink"
      set vlan "vlan12"
   next
end
```

3. Enable NAC on the FortiSwitch port connected to the FortiFone.

```
config switch-controller managed-switch
   edit "Access-FortiSwitch-1”
      config ports
         edit "port6"
            set access-mode nac
         next
      end
   next
end
```

4. Configure the firewall policy.

```
config firewall policy
   edit 1
      set name "fortivoice_policy"
      set srcintf "vlan12"
      set dstintf "wan1"
      set action accept
      set srcaddr "all"
      set dstaddr "all"
      set schedule "always"
      set service "ALL"
      set logtraffic all
      set nat enable
   next
end
```

Creating a vulnerability policy

To use a vulnerability policy requires to following:

- A valid Attack Surface Security Rating service license to download the IoT signature package.
- Enable device detection on the LAN interface used by the IoT devices.
  - In the GUI, go to *Network > Interfaces*, edit a LAN interface, enable *Device detection*, and click *OK*.
  - In the CLI, enter:

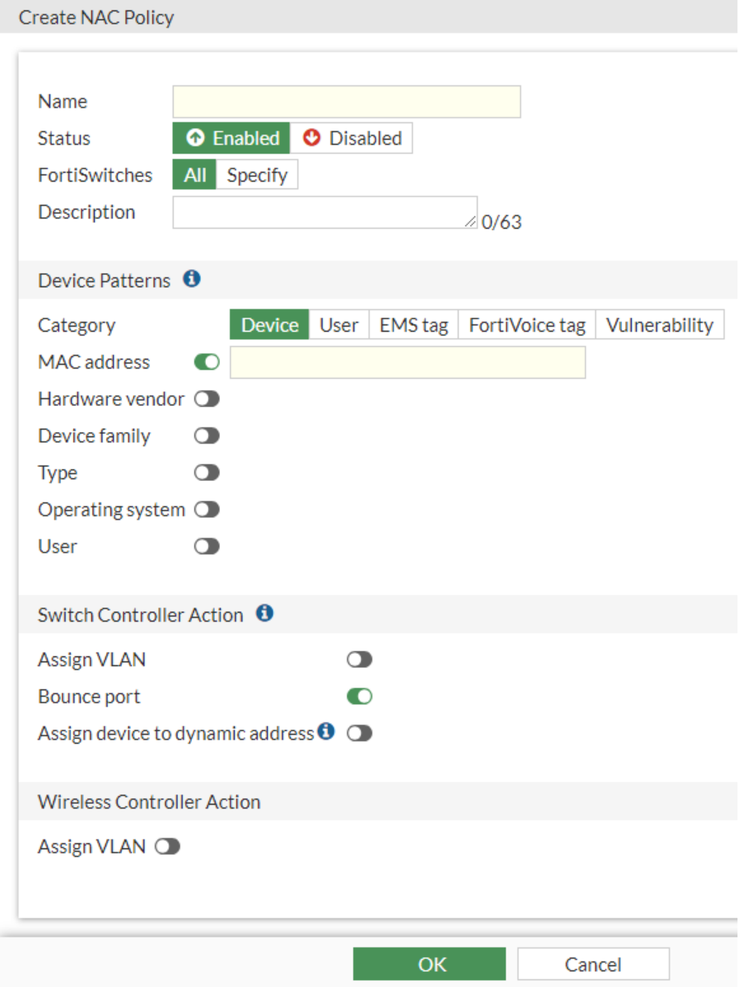
    ```
    config system interface
       edit <name>
          set device-identification enable
       next
    end
    ```
- Configure a firewall policy with an application control sensor.

The NAC policy matches IoT devices with the specified severity levels, which indicate how vulnerable an IOT device is. The following severity levels are available:

- Critical (4)
- High (3)
- Medium (2)
- Low (1)
- Information (0)

Using the GUI to create a vulnerability policy:

1. Go to *WiFi & Switch Controller > NAC Policies*.
2. Click *Create New*.



Create NAC Policy

Name

Status: Enabled [selected] | Disabled

FortiSwitches: All [selected] | Specify

Description 0/63

Device Patterns

Category: Device [selected] | User | EMS tag | FortiVoice tag | Vulnerability

MAC address ●

Hardware vendor ○

Device family ○

Type ○

Operating system ○

User ○

Switch Controller Action

Assign VLAN ○

Bounce port ●

Assign device to dynamic address ○

Wireless Controller Action

Assign VLAN ○

3. In the *Name* field, enter a name for the NAC policy.
   You can enter a number as the NAC policy name, although names are string values.
4. Make certain that the status is set to *Enabled*.
5. For the *FortiSwitches* buttons, click *Specify* to select which FortiSwitch groups to apply the NAC policy to or click *All*.
6. In the *Description* field, enter a description of the vulnerability policy.
7. Select *Vulnerability* for the category.
8. For the *Match* buttons, click *Specify* and + to select one or more severity levels to match or select *Severity is at least* and + to specify the lowest level of severity and above to match.
9. If you want to assign a specific VLAN to the device that matches the specified criteria, select *Assign VLAN* and enter the VLAN identifier.
10. 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*.
11. 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.
12. Click *OK* to create the new NAC policy.

Using the CLI to create a vulnerability policy:

```
config user nac-policy
   edit <policy_name>
      set description <description_of_policy>
      set category vulnerability
      set severity {0 | 1 | 2 | 3 | 4}
      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>
      set match-type {dynamic | override}
      set match-period <0-120>
   next
end
```

For example:

```
config user nac-policy
   edit nac_policy_1
      set category vulnerability
      set severity 3 4
      set switch-fortilink fortilink1
   next
end
```

Creating a MAC policy

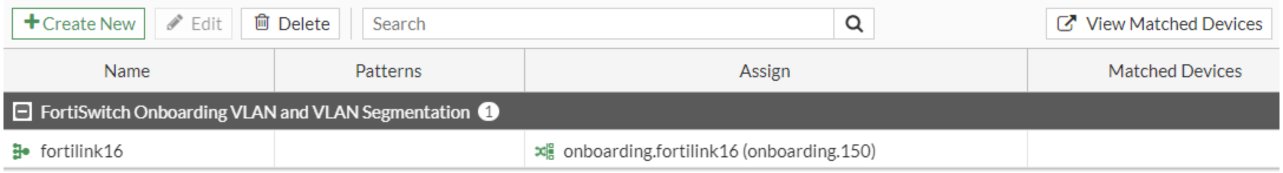
You can apply a MAC policy to the devices that were matched by the NAC policy. You can specify which VLAN is applied, select which traffic policy is used, and enable or disable packet count.

```
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:

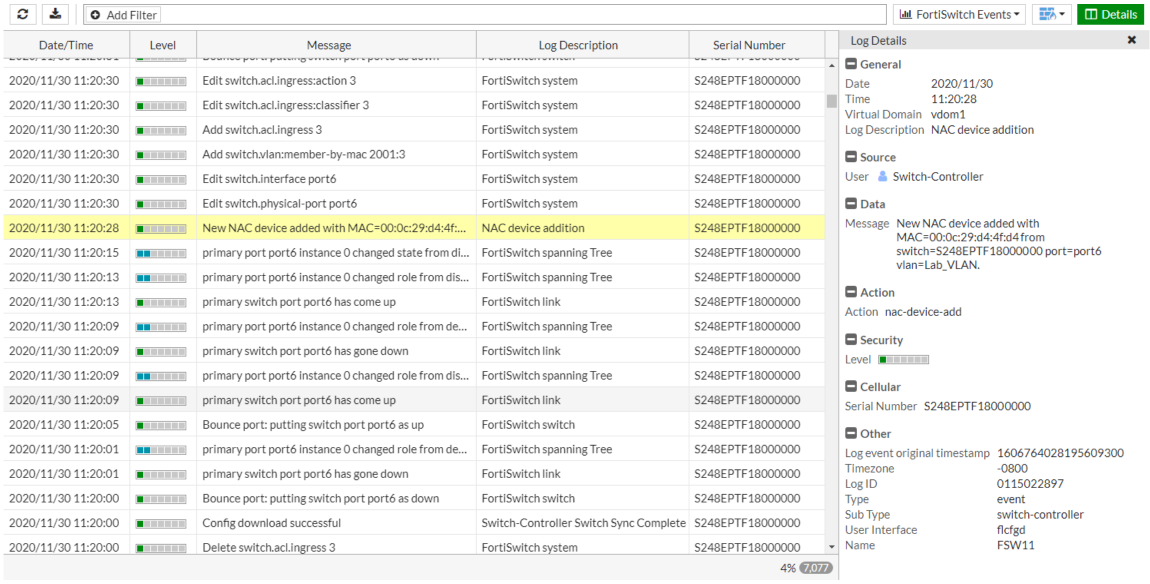
1. Go to *WiFi & Switch Controller > NAC Policies*.



Name	Patterns	Assign	Matched Devices
FortiSwitch Onboarding VLAN and VLAN Segmentation 1			
fortilink16		onboarding.fortilink16 (onboarding.150)	

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.



Date/Time	Level	Message	Log Description	Serial Number
2020/11/30 11:20:30	■□□□□□□	Edit switch.acl.ingress:action 3	FortiSwitch system	S248EPTF18000000
2020/11/30 11:20:30	■□□□□□□	Edit switch.acl.ingress:classifier 3	FortiSwitch system	S248EPTF18000000
2020/11/30 11:20:30	■□□□□□□	Add switch.acl.ingress 3	FortiSwitch system	S248EPTF18000000
2020/11/30 11:20:30	■□□□□□□	Add switch.vlan:member-by-mac 2001:3	FortiSwitch system	S248EPTF18000000
2020/11/30 11:20:30	■□□□□□□	Edit switch.interface port6	FortiSwitch system	S248EPTF18000000
2020/11/30 11:20:30	■□□□□□□	Edit switch.physical-port port6	FortiSwitch system	S248EPTF18000000
2020/11/30 11:20:28	■□□□□□□	New NAC device added with MAC=00:0c:29:d4:4f:...	NAC device addition	S248EPTF18000000
2020/11/30 11:20:15	■■□□□□□	primary port port6 instance 0 changed state from di...	FortiSwitch spanning Tree	S248EPTF18000000
2020/11/30 11:20:13	■■□□□□□	primary port port6 instance 0 changed role from dis...	FortiSwitch spanning Tree	S248EPTF18000000
2020/11/30 11:20:13	■□□□□□□	primary switch port port6 has come up	FortiSwitch link	S248EPTF18000000
2020/11/30 11:20:09	■■□□□□□	primary port port6 instance 0 changed role from de...	FortiSwitch spanning Tree	S248EPTF18000000
2020/11/30 11:20:09	■□□□□□□	primary switch port port6 has gone down	FortiSwitch link	S248EPTF18000000
2020/11/30 11:20:09	■■□□□□□	primary port port6 instance 0 changed role from dis...	FortiSwitch spanning Tree	S248EPTF18000000
2020/11/30 11:20:09	■□□□□□□	primary switch port port6 has come up	FortiSwitch link	S248EPTF18000000
2020/11/30 11:20:05	■□□□□□□	Bounce port: putting switch port port6 as up	FortiSwitch switch	S248EPTF18000000
2020/11/30 11:20:01	■■□□□□□	primary port port6 instance 0 changed role from de...	FortiSwitch spanning Tree	S248EPTF18000000
2020/11/30 11:20:01	■□□□□□□	primary switch port port6 has gone down	FortiSwitch link	S248EPTF18000000
2020/11/30 11:20:00	■□□□□□□	Bounce port: putting switch port port6 as down	FortiSwitch switch	S248EPTF18000000
2020/11/30 11:20:00	■□□□□□□	Config download successful	Switch-Controller Switch Sync Complete	S248EPTF18000000
2020/11/30 11:20:00	■□□□□□□	Delete switch.acl.ingress 3	FortiSwitch system	S248EPTF18000000

4% 7,077

General

Date 2020/11/30
Time 11:20:28
Virtual Domain vdom1
Log Description NAC device addition

Source

User Switch-Controller

Data

Message New NAC device added with MAC=00:0c:29:d4:4f:d4 from switch=S248EPTF18000000 port=port6 vlan=Lab_VLAN.

Action

Action nac-device-add

Security

Level ■□□□□□□

Cellular

Serial Number S248EPTF18000000

Other

Log event original timestamp	1606764028195609300
Timezone	-0800
Log ID	0115022897
Type	event
Sub Type	switch-controller
User Interface	flcfgd
Name	FSW11

Using the CLI:

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

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

For example:

```
FortiGate-3000F # diagnose switch-controller  mac-device nac  known
Vdom: root
MAC                 LAST-KNOWN-SWITCH  LAST-KNOWN-PORT    MATCHED-NAC-POLICY MAC-POLICY-ACTION
LAST-SEEN(sec) OVERRIDE(min)  FSW-ID COMMENTS
0c:82:b9:ae:00:00  S548DF4K15000008   port5              ems                ems               0
           -              2      auto detected @ 2024-08-16 00:12:39
70:4c:a5:24:4c:12  S548DF4K15000008   port15             ap                 ap                0
           -              3      auto detected @ 2024-08-16 00:12:51

Matched Devices in the vdom:2 (All-vdom:2 Max:14400)
```

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

```
diagnose switch-controller mac-device nac onboarding
```

For example:

```
FortiGate-3000F # diagnose switch-controller  mac-device nac  onboarding
Vdom: root
MAC                     LAST-SEEN       TYPE    LOCATION
00:1b:21:68:e2:2c       173             SW      S548DF4K15000008  port5
00:a8:59:f5:b8:54       0               SW      S548DF4K15000008  port9
c6:95:ae:ce:ec:03       0               SW      S548DF4K15000008  port5
e8:1c:ba:63:38:a0       0               SW      S548DF4K15000008  port10
```

To view the NAC clients:

```
diagnose switch-controller mac-device cache
```

For example:

```
FortiGate-3000F # diagnose switch-controller  mac-device cache
Vdom: root
VFID     SWITCH             MAC-ADDRESS        VLAN CREATION(secs ago)  LAST-SEEN(secs ago)
INTERFACE
0        S548DF4K15000008   0c:82:b9:ae:00:00  103  34840               0                    port5

0        S548DF4K15000008   70:4c:a5:24:4c:12  104  34888               0
port15
0        S548DF4K15000008   00:1b:21:68:e2:2c  4089 608                 160                  port5

0        S548DF4K15000008   00:a8:59:f5:b8:54  4089 34926               0                    port9

0        S548DF4K15000008   c6:95:ae:ce:ec:03  4089 446                 0                    port5

0        S548DF4K15000008   e8:1c:ba:63:38:a0  4089 34926               0
port10
```

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-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-1024E, FS-T1024E, FS-1048E, and FS-3032E.
- Accuracy is not guaranteed.

To display device statistics:

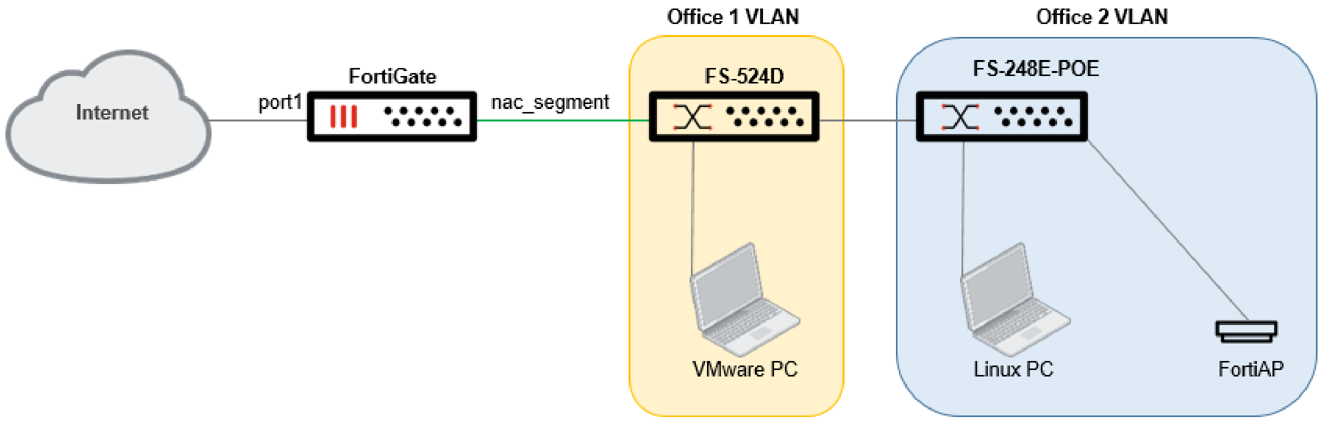
1. Enable NAC.
```
config user nac-policy
   edit <NAC_policy_name>
      set status enable
   next
end
```
2. Enable packet counting in the MAC policy. By default, packet counting is disabled.
```
config switch-controller mac-policy
   edit <MAC_policy_name>
      set count enable
   next
end
```
3. 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.

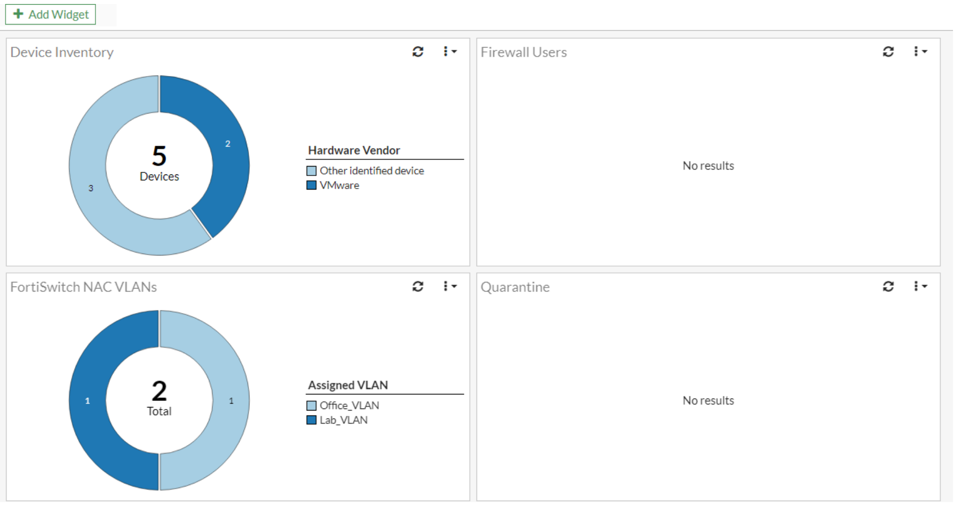
```
config switch-controller managed-switch
   edit "S524DN4K16000116"
      config ports
         edit "port7"
            set vlan "onboarding"
            set allowed-vlans "quarantine" "nac_segment"
            set untagged-vlans "quarantine" "nac_segment"
            set access-mode nac
         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

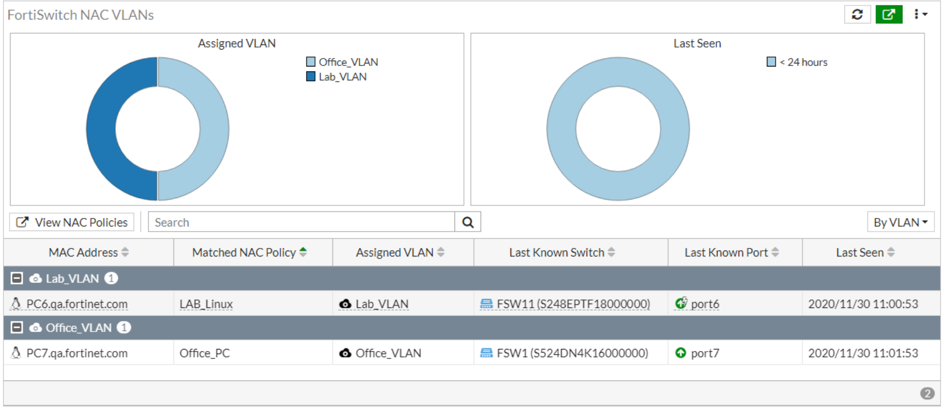
The widget shows a pie chart of the assigned FortiSwitch NAC VLANs. When expanded to the full screen, the widget shows a full list of devices grouped by VLAN, NAC policy, or last seen.

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*.



MAC Address	Matched NAC Policy	Assigned VLAN	Last Known Switch	Last Known Port	Last Seen
Lab_VLAN 1					
PC6.qa.fortinet.com	LAB_Linux	Lab_VLAN	FSW11 (S248EPTF18000000)	port6	2020/11/30 11:00:53
Office_VLAN 1					
PC7.qa.fortinet.com	Office_PC	Office_VLAN	FSW1 (S524DN4K16000000)	port7	2020/11/30 11:01:53

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.

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 IoT Detection service 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 212
2. Set the FortiLink policy settings to the FortiLink interface on page 212
3. Create the FortiLink policy settings on page 212
4. Create the dynamic port policy rule on page 213
5. Set how often the dynamic port policy engine runs on page 216

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

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, from the top to the bottom of the list. 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 change the order of the dynamic port policy rules in the CLI:

```
config switch-controller dynamic-port-policy
   edit <dynamic_port_policy_name>
      config policy
         move <DPP_policy_name> {after | before} <DPP_policy_name>
       end
   next
end
```

Starting in FortiOS 7.4.4, you can use the CLI to control how long matched devices are kept for dynamic port policies. In previous releases, matched devices were deleted when the connection-ID table entry was deleted, the port link status went down, the device was inactive, or the switch was offline.

To control how long matched devices are kept:

1. Change the `set match-type` setting from `dynamic` to `override`.
2. Select the number of days to keep matched devices with the `set match-period` command. By default, `match-period` is set to 0, and the matched devices are kept forever or until a user-configured event occurs in the CLI or

the FortiGate device is restarted. You can change the value to 1 to 120 days to keep matched devices.

Starting in FortiOS 7.4.4, devices matched by dynamic port policies are now matched according to the priority, instead of using First Come, First Serve (FCFS) matching.

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}
            set match-type {dynamic | override}
            set match-period <0-120>
         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 Extensible Authentication Protocol (EAP). 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.

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 device.

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 untagged VLAN for users after the authentication server timeout period expires.

Starting in FortiOS 7.4.4, you can specify a tagged VLAN for users to be assigned to when the authentication server is unavailable. This feature is available with 802.1x MAC-based authentication. It is compatible with both EAP and MAB.

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

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

This section covers the following topics:

- Number of devices supported per port for 802.1X MAC-based authentication on page 217
- Configuring the 802.1X settings for a virtual domain on page 217

- Overriding the virtual domain settings on page 218
- Specifying how RADIUS request attributes are formatted on page 219
- Dynamically and manually assigning the NAS-IP-Address attribute on page 220
- Dynamic VLAN assignment on page 221
- Dynamic access control lists on page 223
- Defining an 802.1X security policy on page 227
- Applying an 802.1X security policy to a FortiSwitch port on page 230
- Using NAC with 802.1X authentication on page 230
- Changing the priority of MAB and EAP 802.1X authentication on page 231
- Testing 802.1X authentication with monitor mode on page 236
- Clearing authorized sessions on page 237
- RADIUS accounting support on page 237
- RADIUS change of authorization (CoA) support on page 238
- 802.1X authentication deployment example on page 240
- Detailed deployment notes on page 242

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
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:

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

Option	Description	Default
`link-down-auth {set-unauth | no-action}`	If a link is down, this command determines the authentication state. Choosing `set-unauth` sets the interface to unauthenticated when a link is down, and reauthentication is needed. Choosing `no-action` means that the interface does not need to be reauthenticated when a link is down.	set-unauth
`reauth-period <integer>`	This command sets how often reauthentication is needed. The range is 1-1440 minutes. Setting the value to 0 minutes disables reauthentication. **NOTE:** Setting the `reauth-period` to 0 is supported only in the CLI. The RADIUS dynamic session timeout and CoA session timeout do not support setting the Session Timeout to 0. 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 <FortiSwitch_serial_number>
      config 802-1X-settings
         set local-override {enable | *disable}
            set reauth-period <integer>                  // visible if override enabled
            set max-reauth-attempt <integer>             // visible if override enabled
            set link-down-auth {*set-unauth | no-action}   // visible if override enabled
            set mab-reauth {enable | disable}             // visible if override enabled
         end
      next
   end
```

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

Specifying how RADIUS request attributes are formatted

Starting in FortiOS 7.4.2 with FortiSwitchOS 7.4.1, you can specify how the following RADIUS request attributes are formatted when they are sent to the RADIUS server:

- User-Name

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

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

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

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

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

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

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

To specify how RADIUS request attributes are formatted:

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

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

Dynamically and manually assigning the NAS-IP-Address attribute

Starting in FortiOS 7.4.2, you can dynamically assign a different NAS-IP-Address attribute to the managed switches when authenticating users with a RADIUS server. When this feature is enabled, the NAS-IP-Address attribute is based on the FortiLink IP address when the IP address is IPv4.

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

Note:

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

To dynamically assign a different NAS-IP-Address attribute on the FortiGate device to all managed switches:

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

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

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

For example:

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

```
end
```

Dynamic VLAN assignment

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

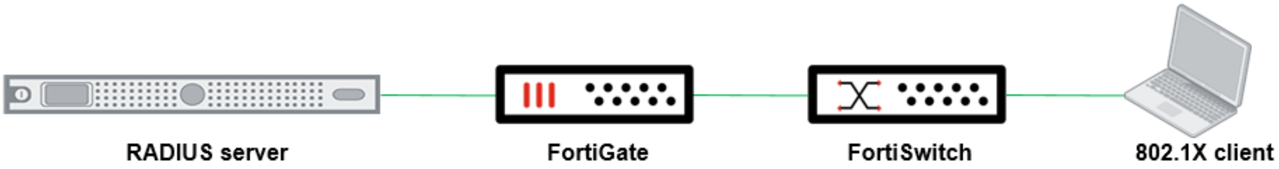
Starting in FortiOS 6.2, when the FortiSwitch unit receives a VLAN assignment from RADIUS, it determines if the data is an integer or string representation. If the representation is an integer, the FortiSwitch unit assigns the VLAN. If the representation is a string, the 802.1X agent will search each VLAN's description field for all VLANs (names defined by the FortiOS VLAN name). If found, the 802.1X agent will make the assignment.

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

Starting in FortiOS 7.4.1, the FortiOS switch controller also supports the synchronization of the FortiGate system interface description to the switch VLAN description (up to the first 63 characters of FortiSwitch VLAN description field in FortiOS). This allows a more flexible use of the Tunnel-Private-Group-Id RADIUS attribute. To use the maximum length of 63 characters, set the `vlan-identity` command to `description` (under `config switch-controller global`).

Configuration examples

To configure dynamic VLAN name assignment:



1. Configure a RADIUS server. In this example, the Tunnel-Private-Group-Id is set to the VLAN name, instead of the VLAN identifier.
   - Set Tunnel-Type to "VLAN".
   - Set Tunnel-Medium-Type to "IEEE-802".
   - Set Tunnel-Private-Group-Id to "my.vlan.10".
2. Configure the FortiGate device:
```
config system interface
   edit "my.vlan.10"
      set vdom "root"
      set ip 1.1.1.254 255.255.255.0
      set allowaccess ping
      set interface "my.fortlink"
      set vlanid 10
   next
end
```
3. Check the FortiSwitch unit. The VLAN name is stored in the value for the `set description` command.
```
# show switch vlan
config switch vlan
   edit 10
```

```
        set description "my.vlan.10"
    next
end
```

To synchronize the FortiGate system interface description to the switch VLAN description:

FortiGate
FortiSwitch

1. Configure the FortiSwitch VLAN on the FortiGate device:

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

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

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

Setting the priority for dynamic or egress VLAN assignment

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

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

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

VLAN ID	VLAN name
4	`testVLAN`

VLAN ID	VLAN name
5	testVLAN
6	testVLAN

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

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

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

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

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

For example:

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

Dynamic access control lists

Starting in FortiOS 7.4.4, you can use RADIUS attributes to configure dynamic access control lists (DACLs) on the 802.1x ports of managed switches. DACLs are configured on a switch or saved on a RADIUS server. You can use

DACLs to control traffic per user session or per port for switch ports directly connected to user clients. DACLs apply to hardware only when 802.1x authentication is successful.

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

DACLs are disabled by default. After you enable DACL in an 802.1X security policy, you must apply the 802.1X security policy to a managed FortiSwitch port. See Applying an 802.1X security policy to a FortiSwitch port on page 230.

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

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

Two RADIUS attributes are supported:

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

The following is the Filter-Id format:

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

For example:

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

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

The following is the NAS-Filter-Rule format:

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

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

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

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

For example:

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

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

- You can use 8 port ranges (source or destination ports) on the FS-148E, FS-148E-POE, and FS-148E-FPOE models.
- You can use 16 port ranges (source or destination ports) on the FS-108F, FS-108F-POE, FS-108F-FPOE, FS-124E, FS-124E-POE, FS-124E-FPOE, FS-124F, FS-124F-POE, FS-124F-FPOE, FS-148F, FS-148F-POE, and FS-148F-FPOE models.
- You can use up to 32 port ranges (source or destination ports) on the FS-1024E, FS-T1024E, FS-T1024F-FPOE, FS-1048E, FS-3032E, FS-424E, FS-424E-POE, FS-424E-FPOE, FS-M426E-FPOE, FS-224D-FPOE, FS-248D, FS-224E, FS-224E-POE, FS-248E-POE, FS-248E-FPOE, FS-424E-Fiber, FS-448E, FS-448E-POE, FS-448E-FPOE, FS-524D, FS-524D-FPOE, FS-548D, and FS-548D-FPOE models.
- Port ranges must have the smaller port number as the first number in the range and the larger port number as the second number in the range. For example, you can specify a port range of `8-10` but not `10-8`.
- If you specify a layer-4 port or layer-4 port range (for example, `permit in TCP from any to any 100-200 cnt`) when defining the source or destination in a dynamic ACL entry, FortiSwitchOS discards any port configurations made after the layer-4 configuration.

To enable DACL:

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

For example:

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

To configure a value for NAS-Filter-Rule:

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

For example:

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

To use a custom command to configure Filter-Id:

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

For example:

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

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

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

For example:

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

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

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

For example:

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

Defining an 802.1X security policy

You can define multiple 802.1X security policies.

Using the 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-period <integer>
      set authserver-timeout-tagged {lldp-voice | static | disable}
      set authserver-timeout-tagged-vlanid <1-4094>
      set authserver-timeout-vlan {enable | disable}
      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. Use port-based authentication when the client is connected directly to a switch port and is capable of 802.1X authentication. Use MAC-based authentication when more than one device needs to be authenticated on the same switch port, and you need to authenticate based on the MAC address.

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

Applying an 802.1X security policy to a FortiSwitch port

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

Using the 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
```

Using NAC with 802.1X authentication

Starting in FortiOS 7.6.4, you can use both FortiSwitch NAC and 802.1X authentication on the same switch port. After a device is successfully authenticated with 802.1X authentication, the NAC user policy checks if the device is assigned to a specific user group. If the device matches the NAC user policy, it is assigned to a specific VLAN.

A new command, `set firewall-auth-user-hold-period`, allows you to specify how long 802.1X users are kept in the firewall authenticated MAC users table. The default period is 5 minutes. You can change the `firewall-auth-user-hold-period` to 5-1,440 minutes or set it to 0 to disable it.

To use NAC with 802.1 authentication, you must specify 802.1X MAC-based authentication. 802.1X port-based authentication is not supported.

The following are the prerequisites for this feature:

- The RADIUS server must return the Fortinet-Group-Name RADIUS attribute with the user group information.
- The FortiGate device must have a user group matching the Fortinet-Group-Name RADIUS attribute, and the RADIUS server can be added as a member to the user group.

To use NAC with 802.1X authentication:

1. Configure a NAC user policy. For example:
   ```
   config user nac-policy
      edit "auth.user"
   ```

```
      set category firewall-user
      set user-group "FortinetCustomGroup"
      set switch-fortilink "fortilink"
      set switch-mac-policy "auth.users.vlan"
   next
end
```

2. Configure an 802.1X MAC-based security policy. For example:

```
config switch-controller security-policy 802-1X
   edit "NAC-802-1X"
      set security-mode 802.1X-mac-based
      set user-group "radiususers"
      set open-auth enable
   next
end
```

3. Apply the NAC user policy and 802.1X security policy to the same port:

```
config switch-controller managed-switch
   edit S108DV3A17000075
      config ports
         edit port3
            set access-mode nac
            set port-security-policy <802.1x-policy>
         next
      end
   next
end
```

4. (Optional) Change how long 802.1X users are kept in the firewall authenticated MAC users table:

```
config switch-controller global
   set firewall-auth-user-hold-period <5-1440 minutes>
end
```

Changing the priority of MAB and EAP 802.1X authentication

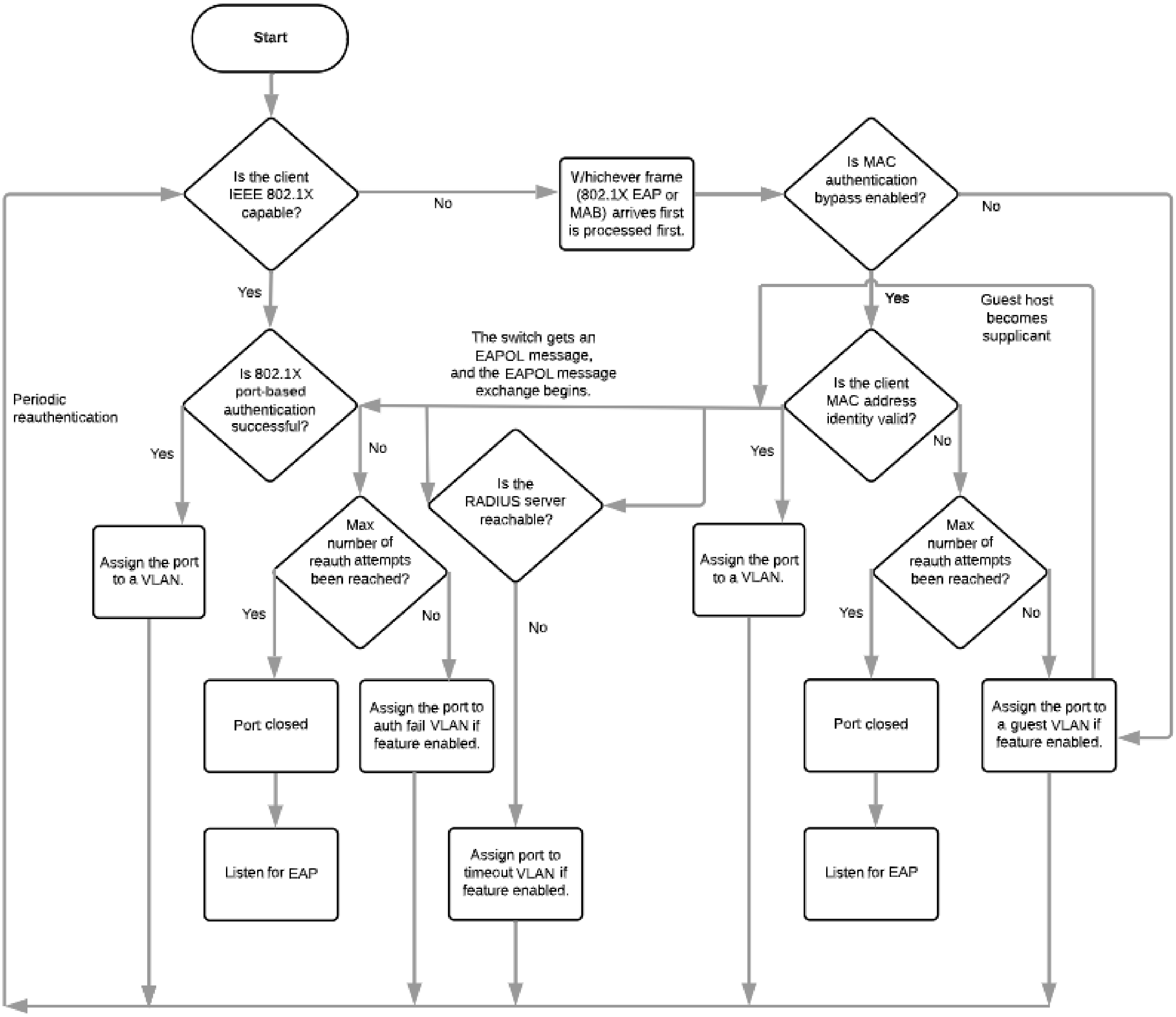
- 802.1X authentication and MAB authentication must be enabled before you can change the priority of MAB and EAP 802.1X authentication.
- This feature requires FortiSwitchOS 7.2.1 or later.
- This feature is supported by both 802.1X port-based authentication and 802.1X MAC-based authentication.

You can use the CLI to change the priority of MAB authentication and EAP 802.1X authentication to fit your specific network security requirements.

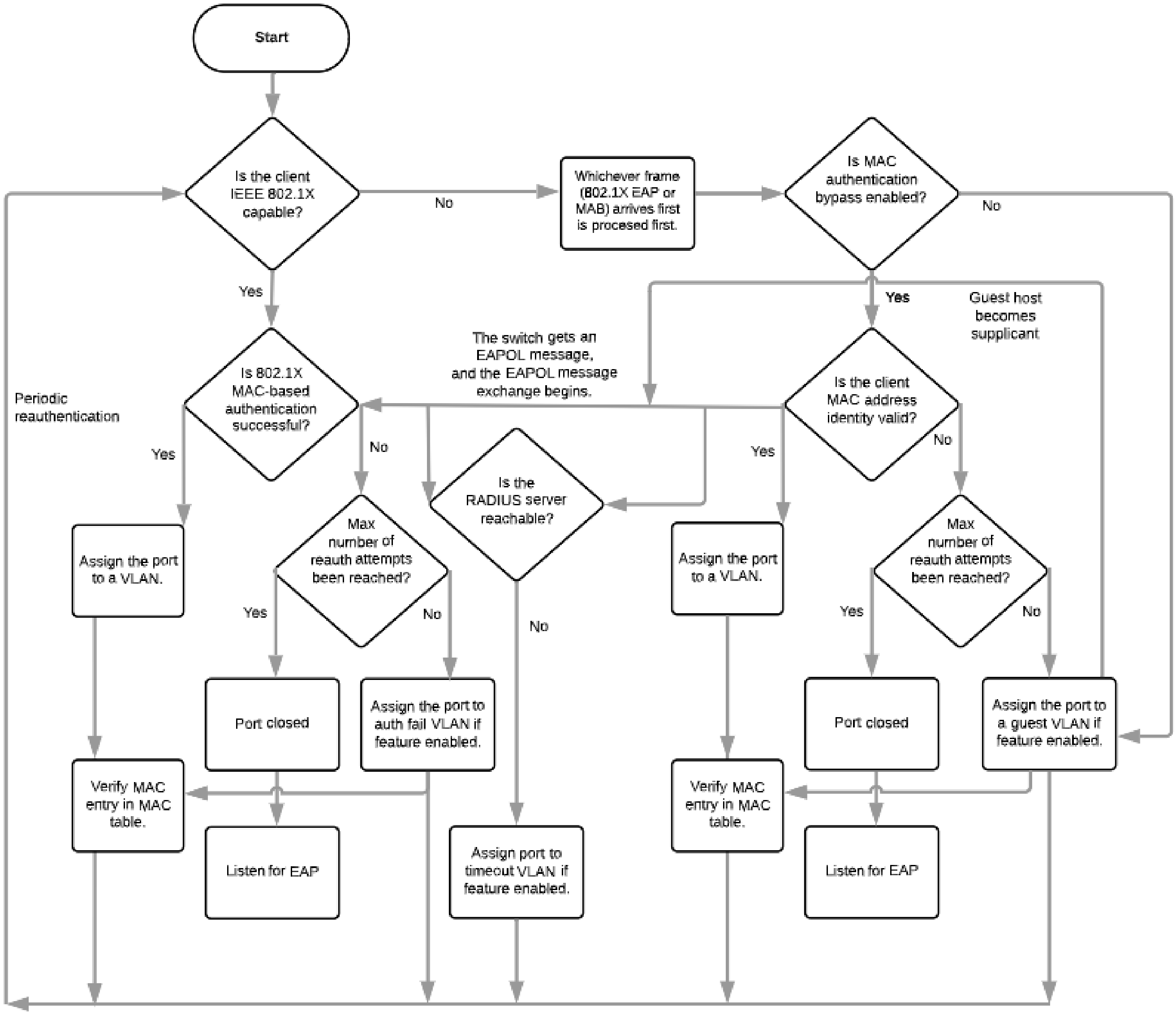
- Before FortiOS 7.6.0, the managed switch tried EAP 802.1X authentication and MAB authentication in the order that they were received with EAP 802.1X authentication having absolute priority. If authentication failed, users were assigned to the `auth-fail-vlanid` VLAN if it had been configured. There was no time delay. Starting inFortiOS 7.6.0, use the `set auth-priority legacy` command to keep this priority. After an upgrade, `auth-priority` is set to `legacy` by default.
- Starting in FortiOS 7.6.0, if you want the managed switch to try EAP 802.1X authentication first and then MAB authentication if EAP 802.1X fails, use the `set auth-priority dot1x-mab` command. If MAB authentication also fails, users are assigned to the `auth-fail-vlanid` VLAN if it is configured.

- Starting in FortiOS 7.6.0, if you want the managed switch to try MAB authentication first and then EAP 802.1X authentication if MAB authentication fails, use the `set auth-priority mab-dot1x` command. If EAP 802.1X authentication also fails, users are assigned to the `auth-fail-vlanid` VLAN if it is configured.
- Starting in FortiOS 7.6.0 with FortiSwitchOS 7.2.3, MAB-only authentication is supported. In this mode, the managed FortiSwitch unit performs MAB authentication without performing EAP authentication. EAP packets are not sent. To enable MAB-only authentication, set the `auth-order` command to `mab`.

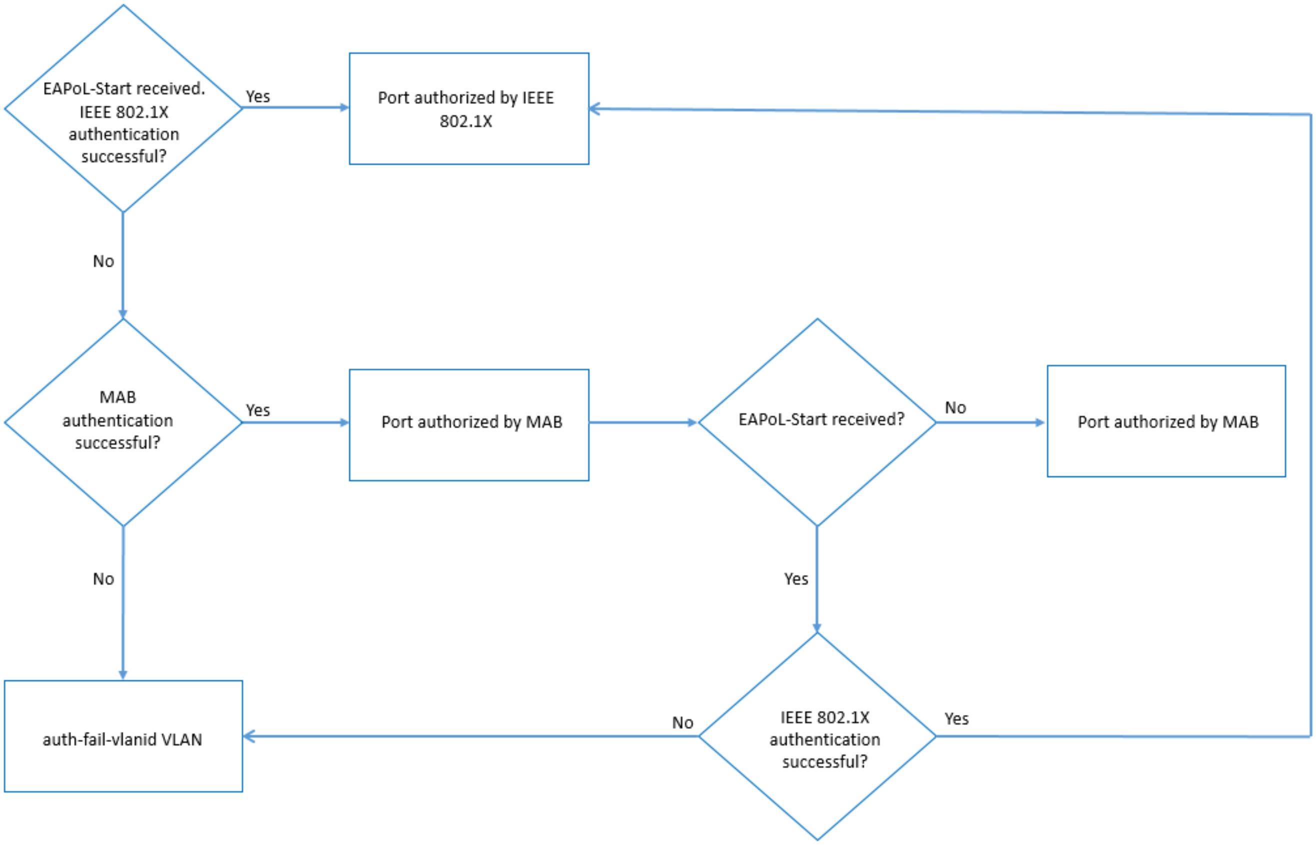
The following flowchart shows the FortiSwitch 802.1X port-based authentication with MAB enabled and with an authentication priority of `auth-priority legacy`:


Start
Is the client IEEE 802.1X capable?
No
Whichever frame (802.1X EAP or MAB) arrives first is processed first.
Is MAC authentication bypass enabled?
No
Yes
Yes
Guest host becomes supplicant
The switch gets an EAPOL message, and the EAPOL message exchange begins.
Periodic reauthentication
Is 802.1X port-based authentication successful?
Yes
No
Is the client MAC address identity valid?
Yes
No
Is the RADIUS server reachable?
Assign the port to a VLAN.
Max number of reauth attempts been reached?
Yes
No
No
Assign the port to a VLAN.
Max number of reauth attempts been reached?
Yes
No
Port closed
Assign the port to auth fail VLAN if feature enabled.
Port closed
Assign the port to a guest VLAN if feature enabled.
Listen for EAP
Assign port to timeout VLAN if feature enabled.
Listen for EAP

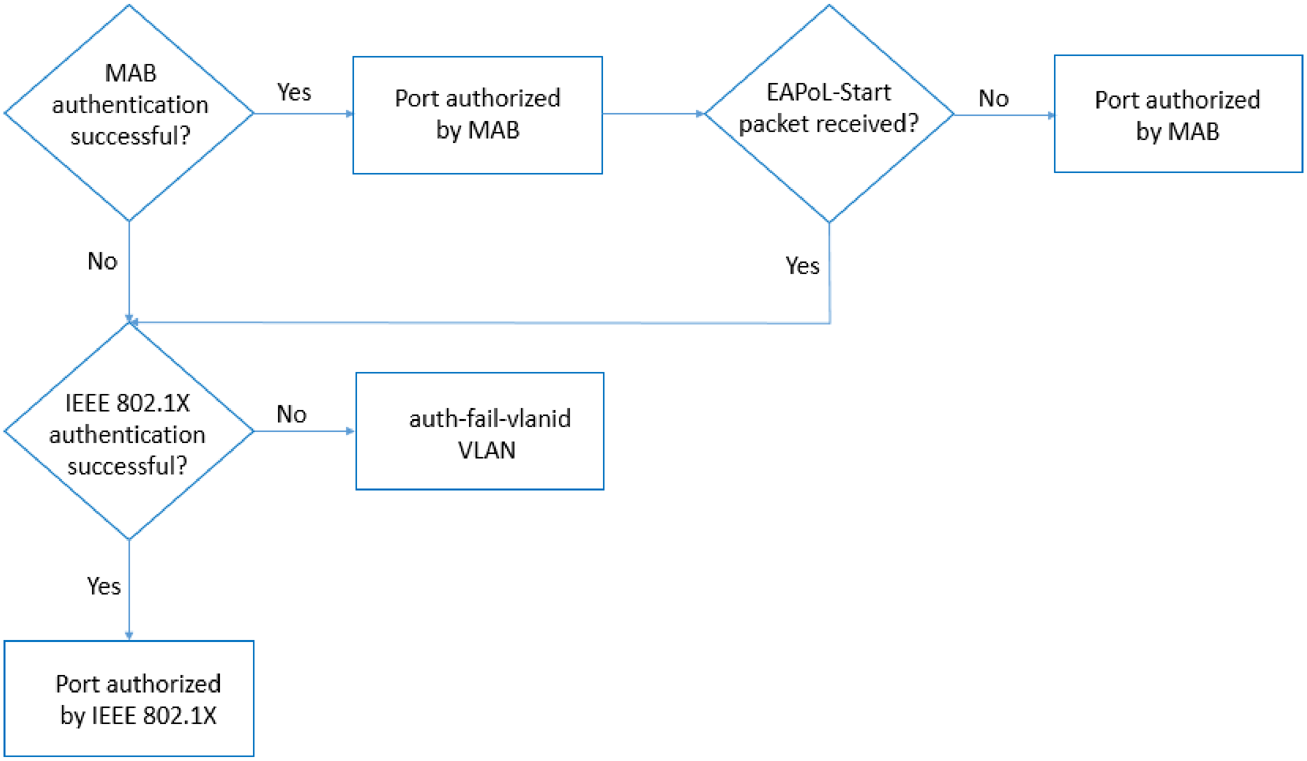
The following flowchart shows the FortiSwitch 802.1X MAC-based authentication with MAB enabled and with an authentication priority of `auth-priority legacy`:


Start
Is the client IEEE 802.1X capable?
No
Whichever frame (802.1X EAP or MAB) arrives first is procesed first.
Is MAC authentication bypass enabled?
No
Yes
Yes
Guest host becomes supplicant
The switch gets an EAPOL message, and the EAPOL message exchange begins.
Periodic reauthentication
Is 802.1X MAC-based authentication successful?
Yes
No
Is the RADIUS server reachable?
Is the client MAC address identity valid?
Yes
No
Assign the port to a VLAN.
Max number of reauth attempts been reached?
Yes
No
No
Assign the port to a VLAN.
Max number of reauth attempts been reached?
Yes
No
Port closed
Assign the port to auth fail VLAN if feature enabled.
Port closed
Assign the port to a guest VLAN if feature enabled.
Verify MAC entry in MAC table.
Listen for EAP
Assign port to timeout VLAN if feature enabled.
Verify MAC entry in MAC table.
Listen for EAP

In the following flowchart, the authentication priority is `dot1x-mab`. If both EAP 802.1X authentication and MAB authentication fail, the user is assigned to the `auth-fail-vlanid` VLAN. If an EAPoL-Start packet is received after MAB authentication, the switch changes to EAP 802.1X authentication.


EAPoL-Start received. IEEE 802.1X authentication successful?
Yes
Port authorized by IEEE 802.1X
No
MAB authentication successful?
Yes
Port authorized by MAB
EAPoL-Start received?
No
Port authorized by MAB
No
Yes
auth-fail-vlanid VLAN
No
IEEE 802.1X authentication successful?
Yes

In the following flowchart, the authentication priority is `mab-dot1x`. If MAB authentication fails, the switch attempts EAP 802.1X authentication. If an EAPoL-Start packet is received after MAB authentication, the switch attempts EAP 802.1X authentication without any time delay or processing impact.


MAB authentication successful?
Yes
Port authorized by MAB
EAPoL-Start packet received?
No
Port authorized by MAB
No
Yes
IEEE 802.1X authentication successful?
No
auth-fail-vlanid VLAN
Yes
Port authorized by IEEE 802.1X

To configure the priority of MAB and EAP 802.1X authentication for managed switches:

1. Enable 802.1X authentication and MAB authentication.

```
config switch-controller security-policy 802-1X
   edit <policy_name>
      set security-mode {802.1X | 802.1X-mac-based}
      set mac-auth-bypass enable
```

Variable	Description	Default
`security-mode 802.1X | 802.1X-mac-based}`	Set the security mode for the port. • `802.1X`—Use this setting for port-based authentication. • `802.1X-mac-based`—Use this setting for MAC-based authentication. If you change the security mode to `802.1X` or `802.1X-mac-based`, you must set the user group with the `set user-group` command.	`802.1X`

2. Specify the authentication order and priority.

```
      set auth-order mab
      set auth-priority {legacy | dot1x-mab | mab-dot1x}
```

Variable	Description
`auth-order mab`	This command is available only when the `set mac-auth-bypass` command is enabled. Use this command if you want to use the MAB-only authentication mode, where the FortiSwitch unit performs MAB authentication without performing EAP authentication. EAP packets are not sent.
`auth-priority {legacy | dot1x-mab | mab-dot1x}`	Select the priority of MAB authentication and EAP 802.1X authentication. • `legacy`—The switch tries EAP 802.1X authentication and MAB authentication in the order that they are received with EAP 802.1X authentication having absolute priority. If authentication fails, users are assigned to a guest VLAN if it has been configured. There is no time delay involved. This is the default value. • `dot1x-mab`—The switch tries EAP 802.1X authentication first and then MAB authentication if EAP 802.1X fails. If MAB authentication also fails, users are assigned to the `auth-fail-vlanid` VLAN if it is configured. • `mab-dot1x`—The switch tries MAB authentication first and then EAP 802.1X authentication if MAB authentication fails. If EAP 802.1X authentication also fails, users are assigned to the `auth-fail-vlanid` VLAN if it is configured. This command is available only when the `set mac-auth-bypass` command is enabled.

For example:

```
config switch-controller security-policy 802-1X
   edit "8021Xmabpolicy"
      set security-mode 802.1X
      set user-group "1X_RADIUS_GROUP"
      set mac-auth-bypass enable
      set auth-order mab-dot1x
      set auth-priority mab-dot1x
   next
end
```

Testing 802.1X authentication with monitor mode

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

To enable or disable monitor mode:

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

Clearing authorized sessions

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

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

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

For example:

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

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

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

For example:

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

RADIUS accounting support

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

Error Cause	Error Code	Description
		or Disconnect-Request message contains an attribute with an unsupported value.
Session Context Not Found	503	This error is a fatal error if the session context identified in the CoA-Request or Disconnect-Request message does not exist on the NAS.

Configuring CoA and disconnect messages

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

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

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

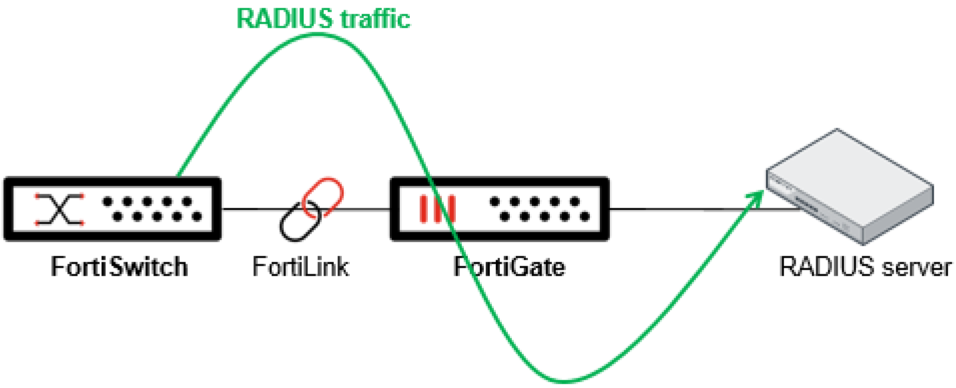
Variable	Description
server <server_name_IPv4>	Enter the domain name or IPv4 address for the RADIUS server. There is no default.

Example: RADIUS CoA

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

```
config switch-controller security-policy local-access
   edit default
      set internal-allowaccess ping https http ssh snmp telnet radius-acct
   next
end
config user radius
   edit "Radius-188-200"
      set radius-coa enable
      set radius-port 0
      set secret ENC
            +2NyBcp8JF3/OijWl/w5nOC++aDKQPWnlC8Ug2HKwn4RcmhqVYE+q07yI9eSDhtiIw63kR/oMBLGwFQoeZfOQWen
            gIlGTb+YQo/lYJn1V3Nwp9sdkcblfyayfc9gTeqe+mFltKl5IWNI7WRYiJC8sxaF9Iyr2/l4hpCiVUMiPOU6fSrj
      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

This feature requires FortiOS 7.4.0 or later and FortiSwitchOS 7.2.2 or later.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

For example:

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

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

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

For example:

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

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

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

For example:

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

Configuring dynamic ARP inspection (DAI)

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

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

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

```
config system interface
```

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

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

To check DAI statistics for a FortiSwitch unit:

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

To delete DAI statistics for a specific VLAN:

```
diagnose switch-controller switch-info arp-inspection stats-clear <VLAN_ID> <FortiSwitch_serial_
      number>
```

Monitoring ARP packets

Starting in FortiOS 7.4.4, you can monitor ARP packets for a specific VLAN on a DHCP-snooping trusted port of a managed switch and save the VLAN ID, MAC addresses, and IP addresses in the DHCP-snooping database. The static IP addresses can be used in RADIUS accounting.

To monitor ARP packets:

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

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

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

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

Configuring DHCP-snooping static entries

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

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

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

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

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

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

To create a static entry for DHCP snooping and DAI:

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

For example:

```
config switch-controller managed-switch
   edit S524DN4K16000116
      config dhcp-snooping-static-client
         edit DHCPclient
```

```
            set vlan 100
            set ip 192.168.101.1
            set mac 00:21:cc:d2:76:72
            set port port19
         next
      next
   end
```

Configuring IPv4 source guard

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

IPv4 source guard allows traffic from the following sources:

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

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

If you add more than 2,048 IP source guard entries from 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.

Refer to the FortiSwitchOS feature matrix to see which FortiSwitch models support this feature.

Configuring IPv4 source guard consists of the following steps:

1. Enabling IPv4 source guard on page 250
2. Creating static entries on page 251
3. Checking the IPv4 source-guard entries on page 252
4. (Optional) Checking the IPv4 source-guard violation log on page 252

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 132.

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>
```

Checking the IPv4 source-guard violation log

Starting in FortiOS 7.6.4, you can log events that violate the IPv4 source-guard settings. The IPv4 source-guard violation log contains a maximum of 128 entries with a maximum of 5 entries per port, even if more violations have occurred. The maximum values cannot be changed. The IP source-guard violation log applies to all FortiSwitch units in the virtual domain (VDOM).

After you enable the IPv4 source-guard violation log, you can specify how many seconds before source-guard violations are removed from the log. The range of values is 1-1,500 minutes. The default is 0, which disables the violation timer.

To enable the IPv4 source-guard violation log:

```
config switch-controller ip-source-guard-log
   set log-violations enable
   set violation-timer <0-1500>
end
```

To display all IPv4 source-guard violations on the FortiSwitch unit:

```
get switch ip-source-guard-violations all
```

For example:

```
          Timestamp |       Interface |              IP |              MAC
-----------------------------------------------------------------------
2025-06-02 17:19:36 |          port23 |         0.1.2.3 | 00:11:22:aa:bb:cc
```

You can also check the FortiSwitch event log to see the source-guard violations. For example:

```
2025-06-02 17:19:36 log_id=0103042201 tz=-0700 type=event subtype=system pri=notice vd=root
      user="srcguardd" msg="Source guard violation, interface=port23, mac=00:11:22:aa:bb:cc,
      ip=0.1.2.3"
```

Configuring an ACL

Starting in FortiOS 7.4.0 with FortiSwitchOS 7.4.0, you can use an access control list (ACL) to configure a policy for the ingress stage of the pipeline for incoming traffic. After creating an ACL group for the ingress policy, you apply the ACL group to a managed switch port.

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

To use an ACL:

1. Create an ACL ingress policy.
2. Create an ACL group and add the ingress policy to it.
3. Apply the ACL group to a managed switch port.
4. View the counters on page 255.

Create an ACL ingress policy

The ACL ingress policy includes the following key attributes:

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

The switch uses specialized TCAM memory to perform ACL matching.

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

To create an ACL ingress policy in the CLI:

```
config switch-controller acl ingress
   edit <policy_identifier>
      config action
         set count {enable | disable}
         set drop {enable | disable}
      end
      config classifier
         set dst-ip-prefix <IPv4_address> <netmask>
         set dst-mac <destination_MAC_address>
         set src-ip-prefix <IPv4_address> <netmask>
         set src-mac <source_MAC_address>
         set vlan <1-4094>
      end
   next
end
```

Create an ACL group

An ACL group contains one or more ACLs.

The ACL ingress policies are assigned to ACL group 3 in the managed FortiSwitch unit. If the managed FortiSwitch unit does not support ACL group 3, the user-configurable ACL is not supported. Refer to the FortiSwitchOS feature matrix to see which models support ACL with FortiLink.

To create an ACL group in the CLI:

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

For example:

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

Apply the ACL group to a managed switch port

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

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

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

For example:

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

View the counters

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

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

To view the counters in the CLI:

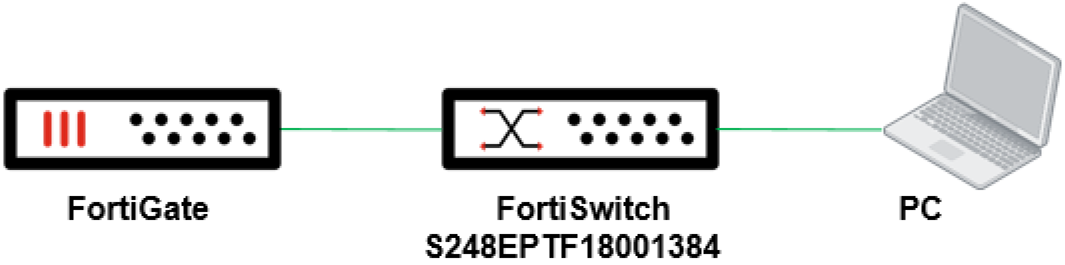
```
diagnose switch-controller switch-info acl-counters <FortiSwitch_serial_number>
```

For example:

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

Configuration example

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



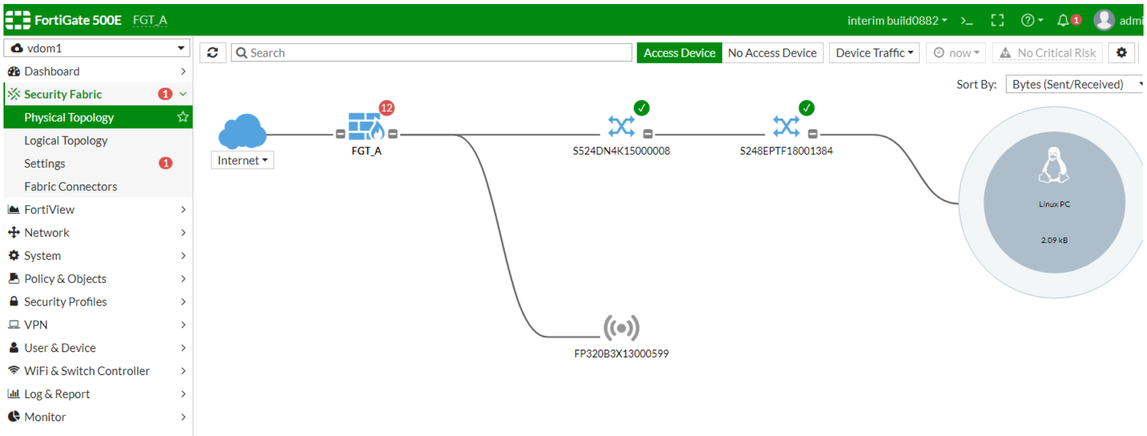
```
config switch-controller acl ingress
   edit 1
      config action
         set drop enable
      end
      config classifier
         set dst-ip-prefix 8.8.8.8 255.255.255.255
         set src-mac 00:0c:29:d4:4f:3c
      end
   next
end

config switch-controller acl group
   edit "group1"
      set ingress 1
   next
```

```
end

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

Showing Security Fabric information

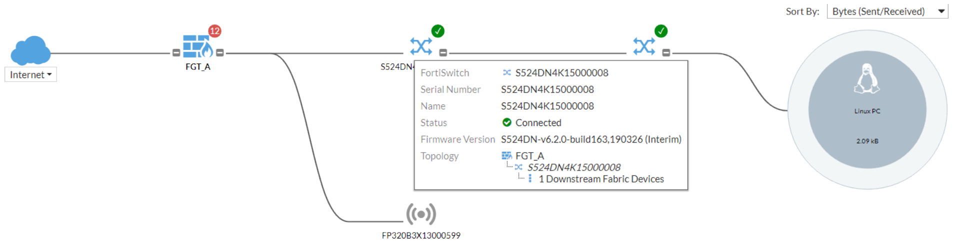
This example shows one of the key components in the concept of Security Fabric: FortiSwitch units in FortiLink. In the FortiGate GUI, you can see the whole picture of the Security Fabric working for your network security.

Sample topology

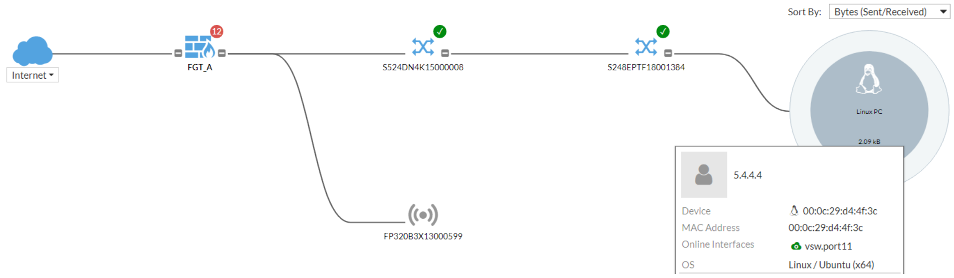


To show Security Fabric information:

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.



FortiSwitch S524DN4K15000008
Serial Number S524DN4K15000008
Name S524DN4K15000008
Status Connected
Firmware Version S524DN-v6.2.0-build163,190326 (Interim)
Topology FGT_A
└ *S524DN4K15000008*
└ 1 Downstream Fabric Devices



5.4.4.4
Device 00:0c:29:d4:4f:3c
MAC Address 00:0c:29:d4:4f:3c
Online Interfaces vsw.port11
OS Linux / Ubuntu (x64)

Blocking intra-VLAN traffic

If you are blocking intra-VLAN traffic on a FortiGate device for a packet with ingress and egress on the same interface, you must disable the `set allow-traffic-redirect` command before blocking intra-VLAN traffic. For example:

```
config system global
   set allow-traffic-redirect disable
end
```

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.

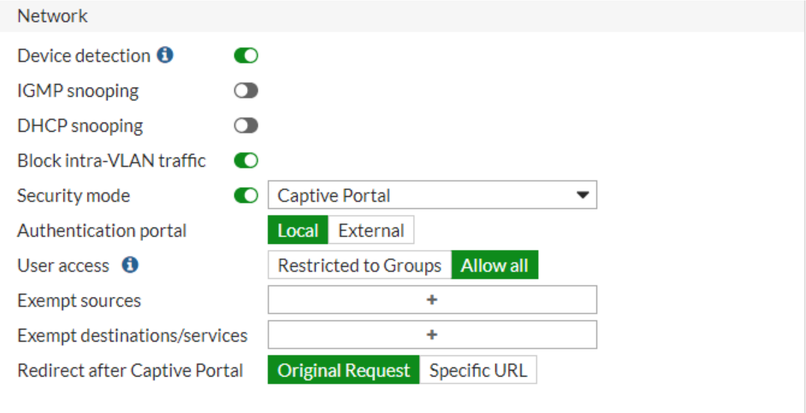
Use `enable` to allow traffic only to and from the FortiGate and to block FortiSwitch port-to-port traffic on the specified VLAN. Use `disable` to allow normal traffic on the specified VLAN.

Starting in FortiOS 7.4.1 with FortiSwitchOS 7.4.1, you can allow or block intra-VLAN traffic on the managed FortiSwitch units when the connection to the FortiGate device is lost.

To block intra-VLAN traffic 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*.



Network

Device detection	●
IGMP snooping	○
DHCP snooping	○
Block intra-VLAN traffic	●
Security mode	● Captive Portal
Authentication portal	[✓ Local] External
User access	Restricted to Groups [✓ Allow all]
Exempt sources	+
Exempt destinations/services	+
Redirect after Captive Portal	[✓ Original Request] Specific URL

To block intra-VLAN traffic 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
```

Starting in FortiOS 7.4.2, you can create a maximum number of 256 proxy-arp entries. For each proxy-arp entry, the IP range can be up to 1,024 IP addresses. Therefore, the maximum number of addresses that can be covered per VDOM is 256 x 1,024 IP addresses.

To allow or block intra-VLAN traffic when the connection to the FortiGate device is lost:

```
config switch-controller fortilink-settings
   edit "<FortiLink_interface>"
      set access-vlan-mode { legacy | fail-open | fail-close}
   next
end
```

Option	Description
legacy	This is the default, which is backward compatible with 7.4.1 and earlier.
fail-open	When the connection to the FortiGate device is lost, intra-VLAN traffic on the managed FortiSwitch units is allowed.
fail-close	When the connection to the FortiGate device is lost, intra-VLAN traffic on the managed FortiSwitch units is blocked.

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 on page 259
- Using quarantine with DHCP on page 263
- Using quarantine with 802.1x MAC-based authentication on page 263
- Viewing quarantine entries on page 265
- Releasing MAC addresses from quarantine on page 267

Quarantining MAC addresses

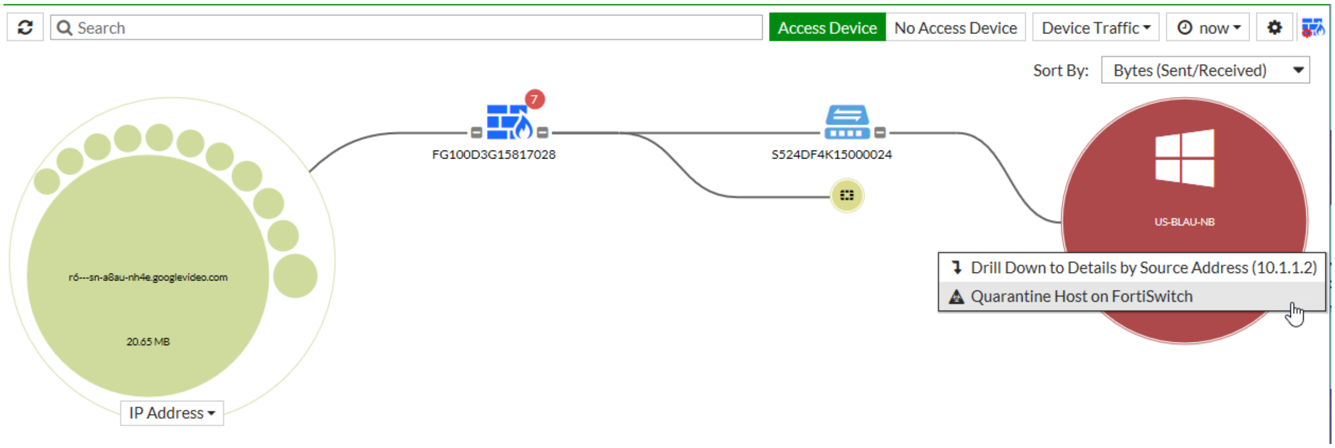
You can use the FortiGate GUI or CLI to quarantine a MAC address.

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.
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:

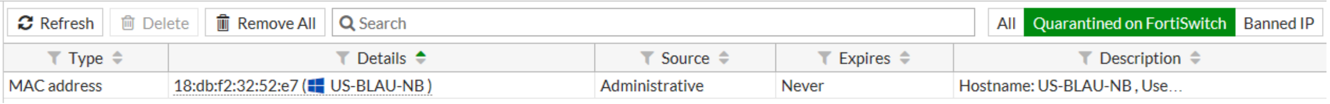
```
S448DF3X16000118 # diagnose switch vlan assignment mac list
00:05:65:ad:15:03 VLAN: 4093 Installed: yes
Source: 802.1X-MAC-Radius
Description: port17

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.



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

Using the FortiGate CLI

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

```
show user quarantine
```

For example:

```
show user quarantine

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

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
```

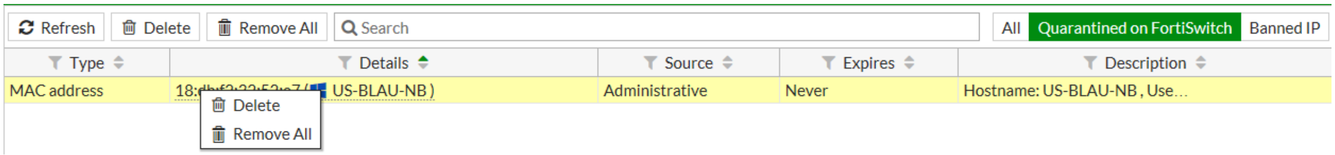
For example:

```
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.



Type	Details	Source	Expires	Description
MAC address	18:db:f2:22:52:a7 (US-BLAU-NB)	Administrative	Never	Hostname: US-BLAU-NB , Use...

Using the FortiGate CLI

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

To delete a single quarantined MAC address:

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

To delete all MAC addresses in a quarantine entry:

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

To disable the quarantine feature:

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

Certificates

To use a certificate with FortiLink:

1. Upload the CA certificate to the FortiGate device. For example:
   - `# execute vpn certificate ca import auto <CA_server> [identifier] [source_ip] [fingerprint]`
   - `# execute vpn certificate ca import bundle <filename> <tftp_IP>`
   - `# execute vpn certificate ca import tftp <filename> <server_address>`
   - `# execute vpn certificate ems_ca import tftp <filename> <server_address>`
2. Set the tunnel mode on the FortiGate device:
   ```
   config switch-controller system
      set tunnel-mode {compatible | moderate | strict}
   end
   ```

Variable	Description
compatible	This is the least restrictive setting. It supports the lowest level of security and provides the highest compatibility between all FortiSwitch and FortiGate devices. Third-party certificates are permitted. This setting is the default.
moderate	This setting provides a moderate level of security. Use this setting when you need peer verification but not host verification. Third-party certificates are permitted.
strict	This setting provides the highest level of security. If it is enabled, the FortiGate device follows the same security mode requirements as in the FIPS/CC mode.

Optimizing the FortiSwitch network

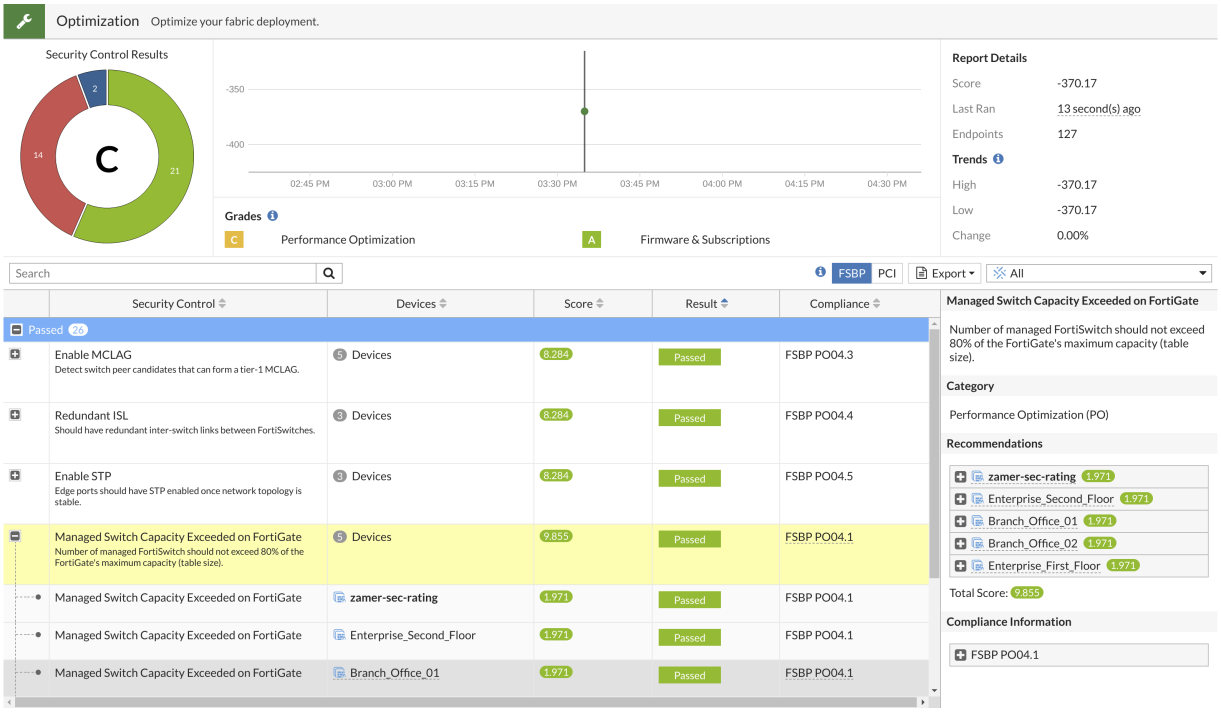
Starting in FortiOS 6.4.2 with FortiSwitchOS 6.4.2, you can check your FortiSwitch network and get recommendations on how to optimize it. If you agree with the configuration recommendations, you can accept them, and they are automatically applied. The following tests have been added:

- Managed Switch Capacity Exceeded on FortiGate

  This test checks for the number of FortiSwitch units managed by the downstream FortiGate devices that have exceeded 80% of the limit. The score is calculated individually and then averaged out. If the number of connected FortiSwitch units is equal or greater than the maximum limit, then the result is a fail.

  You can upgrade to higher capacity FortiGate devices or add more FortiGate devices to the Security Fabric so the FortiSwitch units can be split between multiple FortiGate devices.

  In the following example, the downstream FortiGate device passed.



Optimization Optimize your fabric deployment.

Report Details

Score	-370.17
Last Ran	13 second(s) ago
Endpoints	127

Trends

High	-370.17
Low	-370.17
Change	0.00%

Grades

C Performance Optimization

A Firmware & Subscriptions

Search | FSBP | PCI | Export | All

Security Control	Devices	Score	Result	Compliance
Passed 26				
Enable MCLAG Detect switch peer candidates that can form a tier-1 MCLAG.	5 Devices	8.284	Passed	FSBP PO04.3
Redundant ISL Should have redundant inter-switch links between FortiSwitches.	3 Devices	8.284	Passed	FSBP PO04.4
Enable STP Edge ports should have STP enabled once network topology is stable.	3 Devices	8.284	Passed	FSBP PO04.5
Managed Switch Capacity Exceeded on FortiGate Number of managed FortiSwitch should not exceed 80% of the FortiGate's maximum capacity (table size).	5 Devices	9.855	Passed	FSBP PO04.1
Managed Switch Capacity Exceeded on FortiGate	zamer-sec-rating	1.971	Passed	FSBP PO04.1
Managed Switch Capacity Exceeded on FortiGate	Enterprise_Second_Floor	1.971	Passed	FSBP PO04.1
Managed Switch Capacity Exceeded on FortiGate	Branch_Office_01	1.971	Passed	FSBP PO04.1

Managed Switch Capacity Exceeded on FortiGate

Number of managed FortiSwitch should not exceed 80% of the FortiGate's maximum capacity (table size).

Category

Performance Optimization (PO)

Recommendations

zamer-sec-rating	1.971
Enterprise_Second_Floor	1.971
Branch_Office_01	1.971
Branch_Office_02	1.971
Enterprise_First_Floor	1.971

Total Score: 9.855

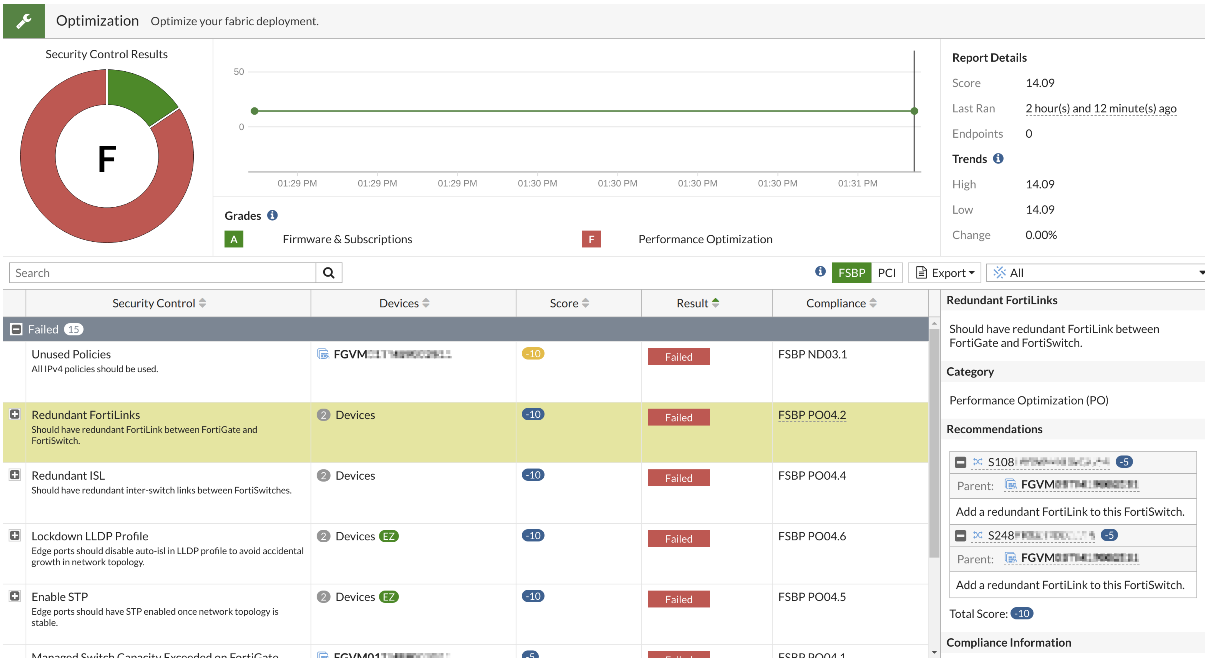
Compliance Information

FSBP PO04.1

- Redundant FortiLinks

  This test checks for redundant FortiLinks between the FortiGate device and the FortiSwitch unit. There are multiple ports dedicated to FortiLink on FortiSwitch units directly connected to FortiGate devices. FortiSwitch units that are not directly connected to the FortiGate device are exempt from this test. If there are no redundant FortiLinks, then the result is a fail.

  In the following example, the FortiGate device failed. The *Recommendations* section lists which FortiSwitch units require redundant FortiLinks.



Optimization Optimize your fabric deployment.

Security Control Results

F

Grades

A Firmware & Subscriptions

F Performance Optimization

Report Details

Score	14.09
Last Ran	2 hour(s) and 12 minute(s) ago
Endpoints	0
Trends	
High	14.09
Low	14.09
Change	0.00%

Search | FSBP | PCI | Export | All

	Security Control	Devices	Score	Result	Compliance
	Failed 15				
	Unused Policies All IPv4 policies should be used.	FGVM[redacted]	-10	Failed	FSBP ND03.1
⊞	Redundant FortiLinks Should have redundant FortiLink between FortiGate and FortiSwitch.	2 Devices	-10	Failed	FSBP PO04.2
⊞	Redundant ISL Should have redundant inter-switch links between FortiSwitches.	2 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.	2 Devices EZ	-10	Failed	FSBP PO04.6
⊞	Enable STP Edge ports should have STP enabled once network topology is stable.	2 Devices EZ	-10	Failed	FSBP PO04.5
	Managed Switch Capacity Exceeded on FortiGate	FGVM01[redacted]	-5	Failed	FSBP PO04.1

Redundant FortiLinks

Should have redundant FortiLink between FortiGate and FortiSwitch.

Category

Performance Optimization (PO)

Recommendations

⊟ S108[redacted] -5

Parent: FGVM[redacted]

Add a redundant FortiLink to this FortiSwitch.

⊟ S248[redacted] -5

Parent: FGVM[redacted]

Add a redundant FortiLink to this FortiSwitch.

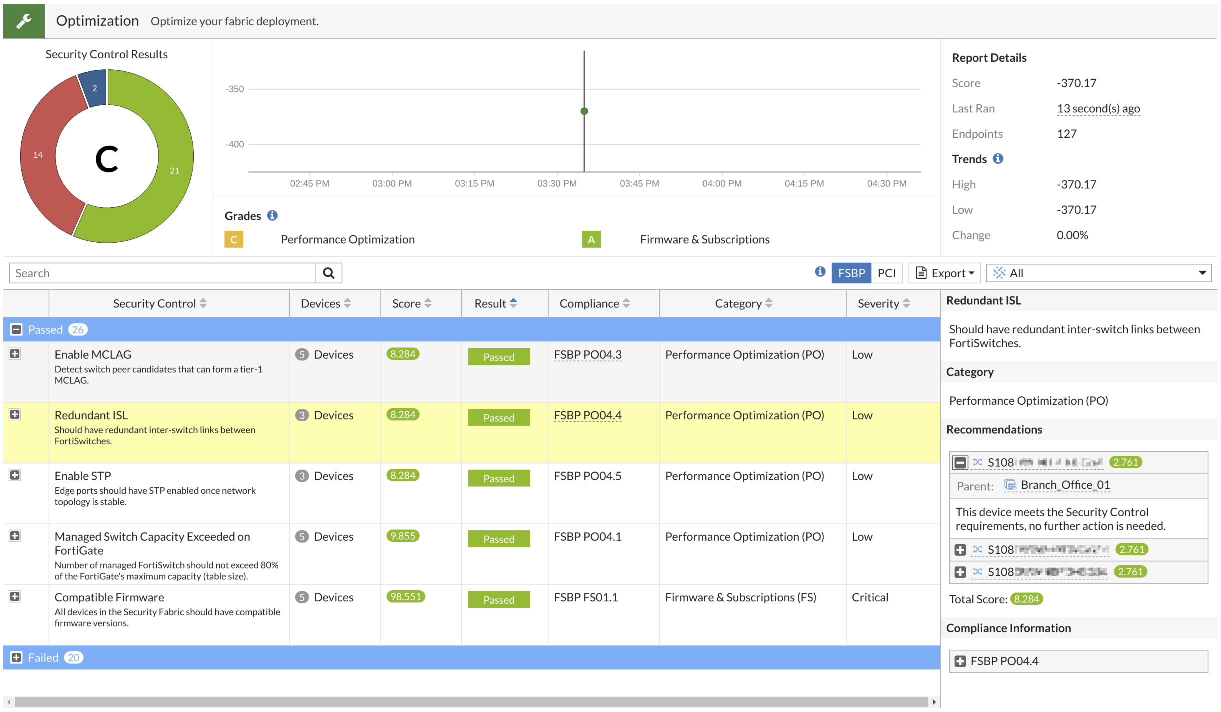
Total Score: -10

Compliance Information

- Redundant ISL

  For FortiSwitch units with inter-switch links (ISLs), this test checks for two redundant links. If there is only one link, then the result is a fail. The *Recommendations* section lists which devices require an additional link. FortiSwitch units with inter-chassis links (ICLs) are exempt from the test.

  In the following example, the devices passed.



Optimization Optimize your fabric deployment.

Security Control Results

C

Grades

C Performance Optimization

A Firmware & Subscriptions

Report Details

Score	-370.17
Last Ran	13 second(s) ago
Endpoints	127
Trends	
High	-370.17
Low	-370.17
Change	0.00%

Search | FSBP | PCI | Export | All

	Security Control	Devices	Score	Result	Compliance	Category	Severity
	Passed 26						
⊞	Enable MCLAG Detect switch peer candidates that can form a tier-1 MCLAG.	5 Devices	8.284	Passed	FSBP PO04.3	Performance Optimization (PO)	Low
⊞	Redundant ISL Should have redundant inter-switch links between FortiSwitches.	3 Devices	8.284	Passed	FSBP PO04.4	Performance Optimization (PO)	Low
⊞	Enable STP Edge ports should have STP enabled once network topology is stable.	3 Devices	8.284	Passed	FSBP PO04.5	Performance Optimization (PO)	Low
⊞	Managed Switch Capacity Exceeded on FortiGate Number of managed FortiSwitch should not exceed 80% of the FortiGate's maximum capacity (table size).	5 Devices	9.855	Passed	FSBP PO04.1	Performance Optimization (PO)	Low
⊞	Compatible Firmware All devices in the Security Fabric should have compatible firmware versions.	5 Devices	98.551	Passed	FSBP FS01.1	Firmware & Subscriptions (FS)	Critical
	Failed 20						

Redundant ISL

Should have redundant inter-switch links between FortiSwitches.

Category

Performance Optimization (PO)

Recommendations

⊟ S108[redacted] 2.761

Parent: Branch_Office_01

This device meets the Security Control requirements, no further action is needed.

⊞ S108[redacted] 2.761

⊞ S108[redacted] 2.761

Total Score: 8.284

Compliance Information

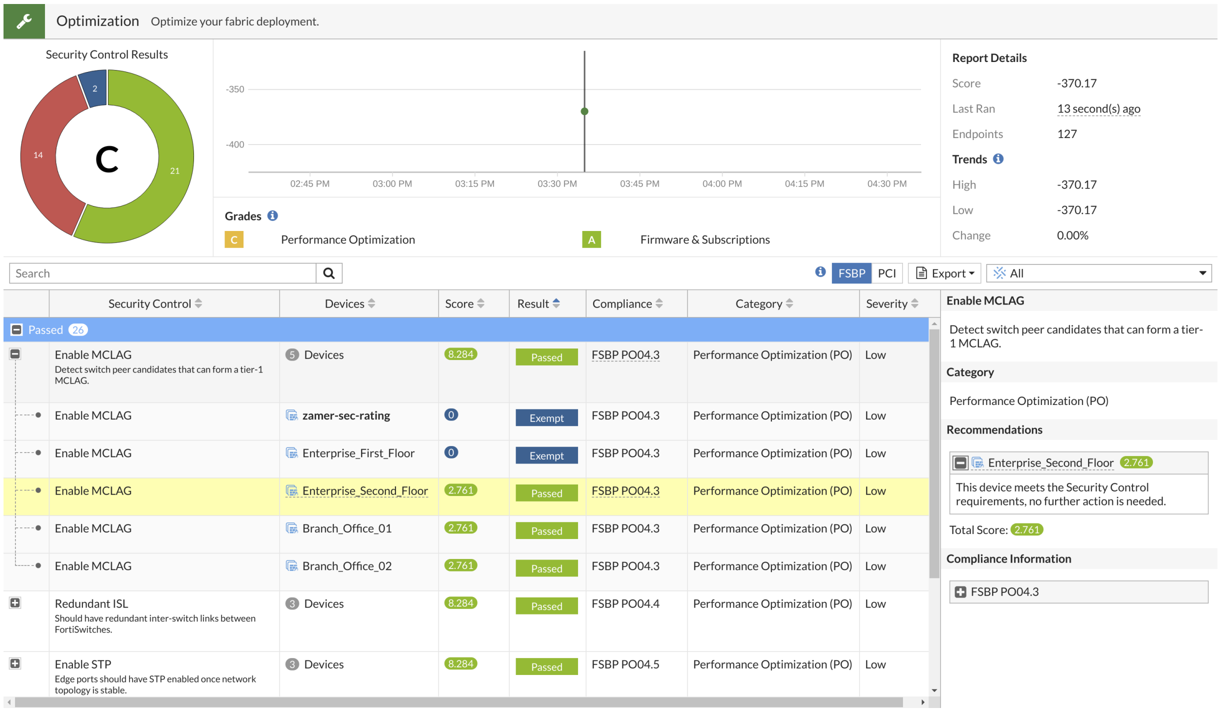
⊞ FSBP PO04.4

- Enable MCLAG

  This test checks for candidate FortiSwitch units that can form a tier-1 MCLAG. To do this, the FortiSwitch units must be connected to each other and directly connected to the FortiGate device. The FortiSwitch unit must support

MCLAG. If an MCLAG already exists, this check is skipped.

In the following example, three devices passed the test and two devices were exempt.



Report Details

Score	-370.17
Last Ran	13 second(s) ago
Endpoints	127
Trends	
High	-370.17
Low	-370.17
Change	0.00%

Grade	
C	Performance Optimization
A	Firmware & Subscriptions

	Security Control	Devices	Score	Result	Compliance	Category	Severity
Passed 26							
⊟	Enable MCLAG Detect switch peer candidates that can form a tier-1 MCLAG.	5 Devices	8.284	Passed	FSBP PO04.3	Performance Optimization (PO)	Low
	Enable MCLAG	**zamer-sec-rating**	0	Exempt	FSBP PO04.3	Performance Optimization (PO)	Low
	Enable MCLAG	Enterprise_First_Floor	0	Exempt	FSBP PO04.3	Performance Optimization (PO)	Low
	Enable MCLAG	Enterprise_Second_Floor	2.761	Passed	FSBP PO04.3	Performance Optimization (PO)	Low
	Enable MCLAG	Branch_Office_01	2.761	Passed	FSBP PO04.3	Performance Optimization (PO)	Low
	Enable MCLAG	Branch_Office_02	2.761	Passed	FSBP PO04.3	Performance Optimization (PO)	Low
⊞	Redundant ISL Should have redundant inter-switch links between FortiSwitches.	3 Devices	8.284	Passed	FSBP PO04.4	Performance Optimization (PO)	Low
⊞	Enable STP Edge ports should have STP enabled once network topology is stable.	3 Devices	8.284	Passed	FSBP PO04.5	Performance Optimization (PO)	Low

Enable MCLAG

Detect switch peer candidates that can form a tier-1 MCLAG.

Category

Performance Optimization (PO)

Recommendations

⊟ Enterprise_Second_Floor 2.761

This device meets the Security Control requirements, no further action is needed.

Total Score: 2.761

Compliance Information

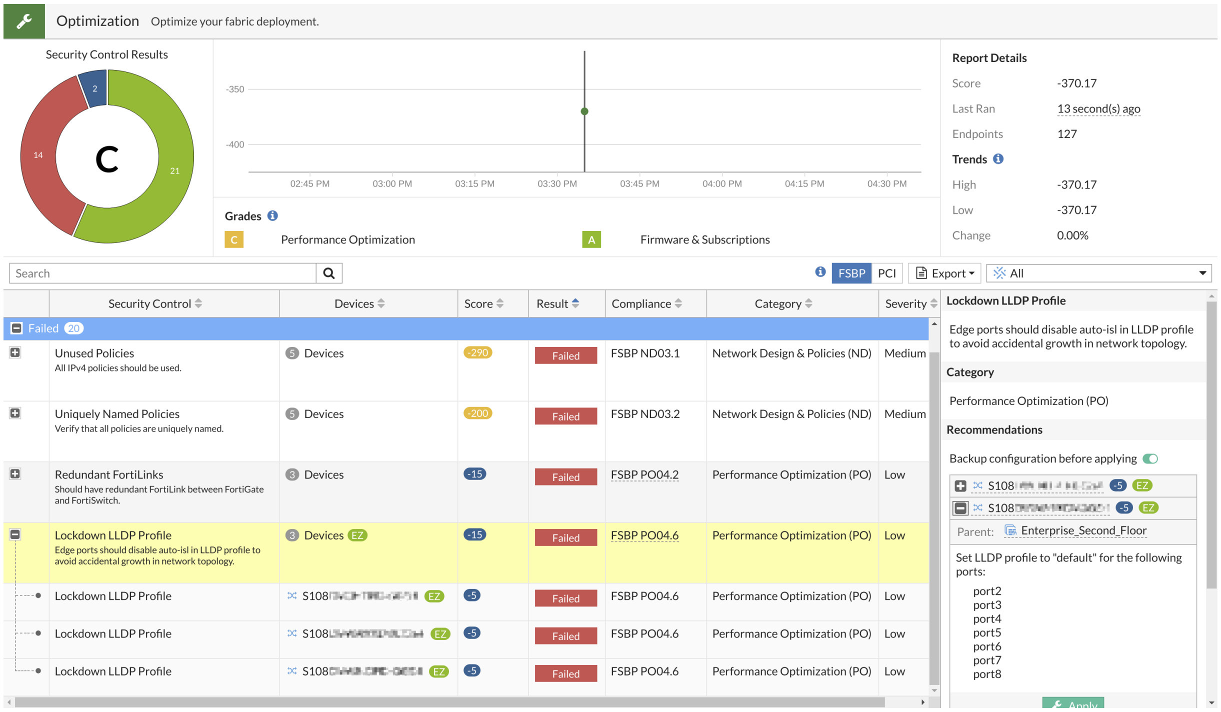
⊞ FSBP PO04.3

- Lockdown LLDP Profile

  This test ensures that there are no accidental changes to the topology. For edge ports (not FortiLink or ISL), FortiOS suggests using the default LLDP profile. The test verifies the following:

  - Looks for an edge port that has an auto-ISL LLDP profile
  - Checks if the edge port BPDU guard is disabled
  - Check if the FortiGate DHCP server and switches do not have a DHCP key

  In the following example, the devices failed. The *EZ* (Easy Apply) symbol appears, and port configurations to optimize the Security Fabric can be applied in the *Recommendations* section.



Optimization Optimize your fabric deployment.

Security Control Results

Grades

C Performance Optimization

A Firmware & Subscriptions

Report Details	
Score	-370.17
Last Ran	13 second(s) ago
Endpoints	127
Trends	
High	-370.17
Low	-370.17
Change	0.00%

Search | FSBP | PCI | Export | All

	Security Control	Devices	Score	Result	Compliance	Category	Severity
Failed 20							
⊞	Unused Policies All IPv4 policies should be used.	5 Devices	-290	Failed	FSBP ND03.1	Network Design & Policies (ND)	Medium
⊞	Uniquely Named Policies Verify that all policies are uniquely named.	5 Devices	-200	Failed	FSBP ND03.2	Network Design & Policies (ND)	Medium
⊞	Redundant FortiLinks Should have redundant FortiLink between FortiGate and FortiSwitch.	3 Devices	-15	Failed	FSBP PO04.2	Performance Optimization (PO)	Low
⊟	Lockdown LLDP Profile Edge ports should disable auto-isl in LLDP profile to avoid accidental growth in network topology.	3 Devices EZ	-15	Failed	FSBP PO04.6	Performance Optimization (PO)	Low
	Lockdown LLDP Profile	S108[redacted] EZ	-5	Failed	FSBP PO04.6	Performance Optimization (PO)	Low
	Lockdown LLDP Profile	S108[redacted] EZ	-5	Failed	FSBP PO04.6	Performance Optimization (PO)	Low
	Lockdown LLDP Profile	S108[redacted] EZ	-5	Failed	FSBP PO04.6	Performance Optimization (PO)	Low

Lockdown LLDP Profile

Edge ports should disable auto-isl in LLDP profile to avoid accidental growth in network topology.

Category

Performance Optimization (PO)

Recommendations

Backup configuration before applying

⊞ S108[redacted] -5 EZ

⊟ S108[redacted] -5 EZ

Parent: Enterprise_Second_Floor

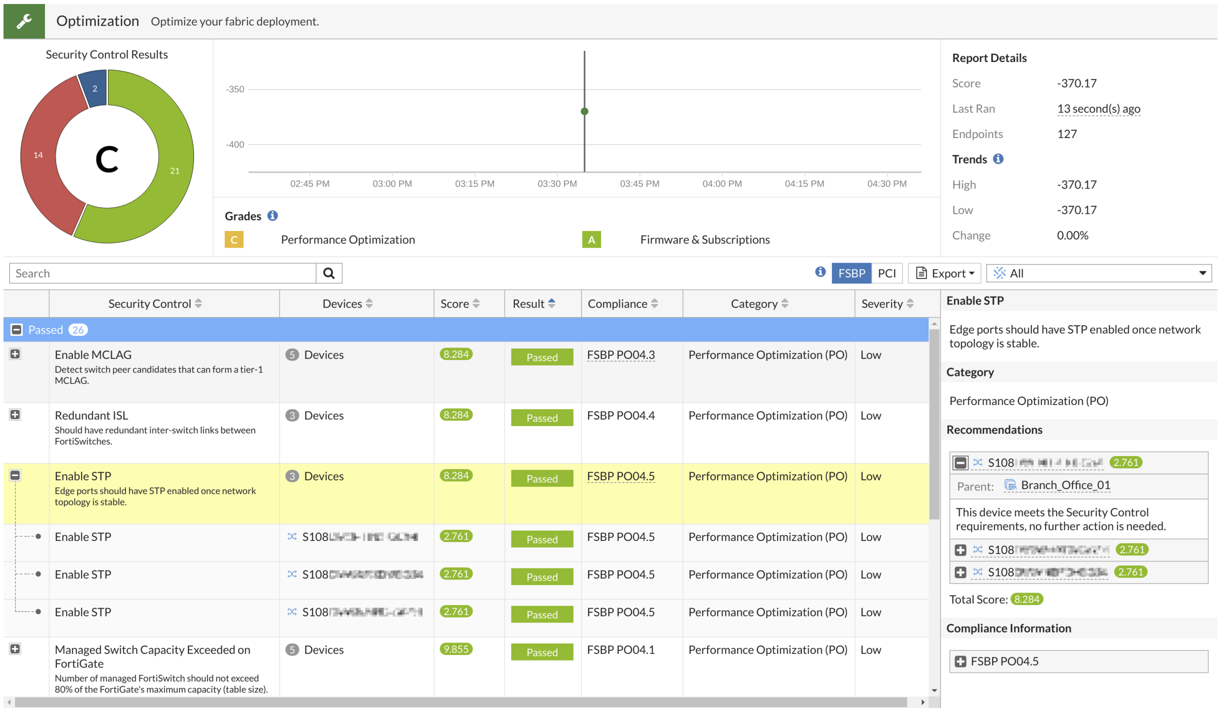
Set LLDP profile to "default" for the following ports:

port2
port3
port4
port5
port6
port7
port8

Apply

- Enable STP

  This test checks if STP is enabled on edge ports. After the network topology is stable, edge ports should have STP enabled to optimize the Security Fabric. In the following example, the devices passed.



Optimization Optimize your fabric deployment.

Security Control Results

Grades

C Performance Optimization

A Firmware & Subscriptions

Report Details	
Score	-370.17
Last Ran	13 second(s) ago
Endpoints	127
Trends	
High	-370.17
Low	-370.17
Change	0.00%

Search | FSBP | PCI | Export | All

	Security Control	Devices	Score	Result	Compliance	Category	Severity
Passed 26							
⊞	Enable MCLAG Detect switch peer candidates that can form a tier-1 MCLAG.	5 Devices	8.284	Passed	FSBP PO04.3	Performance Optimization (PO)	Low
⊞	Redundant ISL Should have redundant inter-switch links between FortiSwitches.	3 Devices	8.284	Passed	FSBP PO04.4	Performance Optimization (PO)	Low
⊟	Enable STP Edge ports should have STP enabled once network topology is stable.	3 Devices	8.284	Passed	FSBP PO04.5	Performance Optimization (PO)	Low
	Enable STP	S108[redacted]	2.761	Passed	FSBP PO04.5	Performance Optimization (PO)	Low
	Enable STP	S108[redacted]	2.761	Passed	FSBP PO04.5	Performance Optimization (PO)	Low
	Enable STP	S108[redacted]	2.761	Passed	FSBP PO04.5	Performance Optimization (PO)	Low
⊞	Managed Switch Capacity Exceeded on FortiGate Number of managed FortiSwitch should not exceed 80% of the FortiGate's maximum capacity (table size).	5 Devices	9.855	Passed	FSBP PO04.1	Performance Optimization (PO)	Low

Enable STP

Edge ports should have STP enabled once network topology is stable.

Category

Performance Optimization (PO)

Recommendations

⊟ S108[redacted] 2.761

Parent: Branch_Office_01

This device meets the Security Control requirements, no further action is needed.

⊞ S108[redacted] 2.761

⊞ S108[redacted] 2.761

Total Score: 8.284

Compliance Information

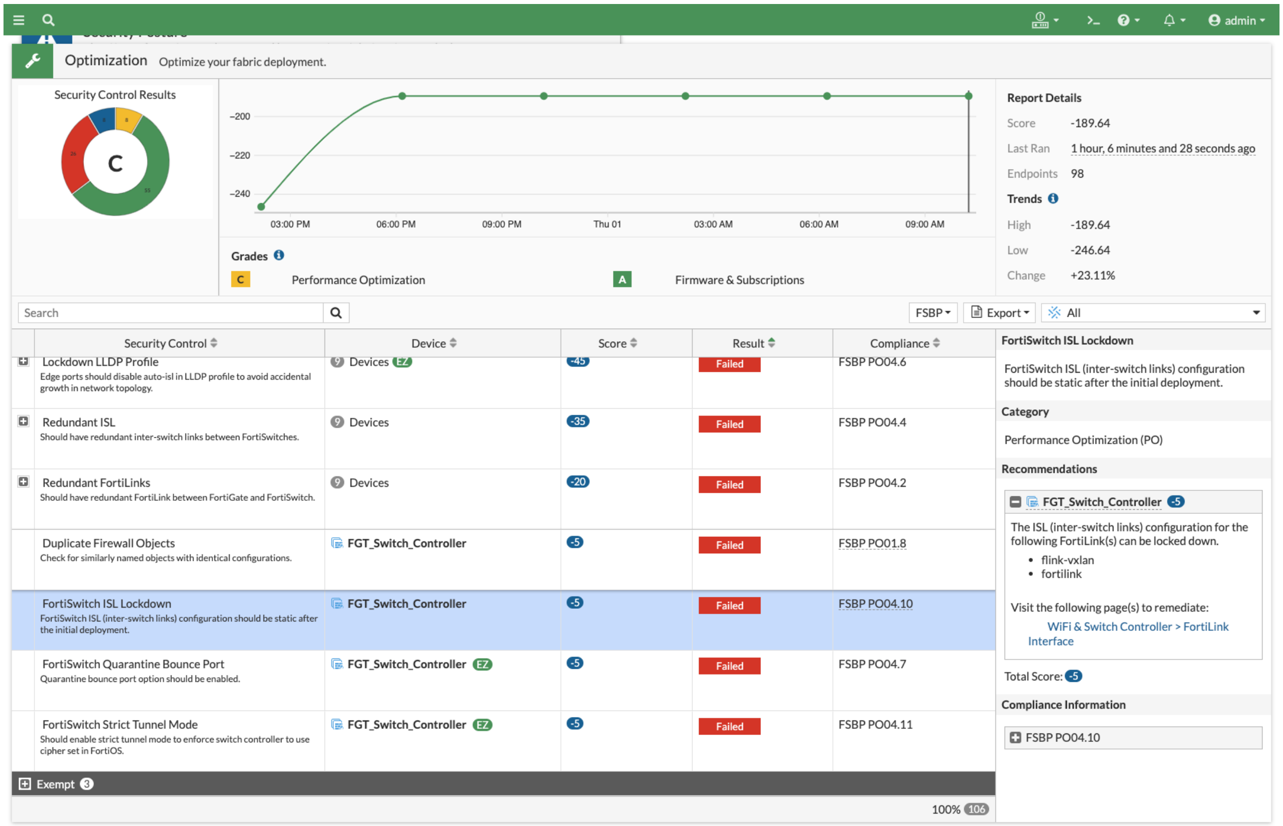
⊞ FSBP PO04.5

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 port 8 of an FS-108F 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.
- FortiOS checks if the ISLs and inter-chassis links (ICLs) are static to increase stability during events such as cable disconnections or power outages. If any ISLs or ICLs are not static, FortiOS recommends locking down the Security Fabric topology to prevent the automatically created ISLs and ICLs from being accidentally deleted.

  In the following figure, two ISL configurations need to be locked down.



Optimization Optimize your fabric deployment.

Report Details

Score	-189.64
Last Ran	1 hour, 6 minutes and 28 seconds ago
Endpoints	98

Trends

High	-189.64
Low	-246.64
Change	+23.11%

Grades

C Performance Optimization

A Firmware & Subscriptions

Search FSBP Export All

Security Control	Device	Score	Result	Compliance
Lockdown LLDP Profile Edge ports should disable auto-isl in LLDP profile to avoid accidental growth in network topology.	9 Devices EZ	-45	Failed	FSBP PO04.6
Redundant ISL Should have redundant inter-switch links between FortiSwitches.	9 Devices	-35	Failed	FSBP PO04.4
Redundant FortiLinks Should have redundant FortiLink between FortiGate and FortiSwitch.	9 Devices	-20	Failed	FSBP PO04.2
Duplicate Firewall Objects Check for similarly named objects with identical configurations.	FGT_Switch_Controller	-5	Failed	FSBP PO01.8
FortiSwitch ISL Lockdown FortiSwitch ISL (inter-switch links) configuration should be static after the initial deployment.	FGT_Switch_Controller	-5	Failed	FSBP PO04.10
FortiSwitch Quarantine Bounce Port Quarantine bounce port option should be enabled.	FGT_Switch_Controller EZ	-5	Failed	FSBP PO04.7
FortiSwitch Strict Tunnel Mode Should enable strict tunnel mode to enforce switch controller to use cipher set in FortiOS.	FGT_Switch_Controller EZ	-5	Failed	FSBP PO04.11

Exempt 3

100% 106

FortiSwitch ISL Lockdown

FortiSwitch ISL (inter-switch links) configuration should be static after the initial deployment.

Category

Performance Optimization (PO)

Recommendations

FGT_Switch_Controller -5

The ISL (inter-switch links) configuration for the following FortiLink(s) can be locked down.

- flink-vxlan
- fortilink

Visit the following page(s) to remediate:

WiFi & Switch Controller > FortiLink Interface

Total Score: -5

Compliance Information

FSBP PO04.10

- When a multichassis link-aggregation group (MCLAG) is recommended between two FortiSwitch units, there is a *Create MCLAG button* available under *WiFi & Switch Controller > Managed FortiSwitches* in the *Topology* view.

In FortiOS 7.4.0 with FortiSwitchOS 7.4.0, more tests have been added to the FortiSwitch recommendations to help optimize your network:

- Check if the switch port where a quarantined device was last seen has bouncing enabled.
- Check if the Basic Input/Output System (BIOS) on the FortiSwitch unit needs to be upgraded before FortiSwitchOS can be upgraded.
- 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.

In FortiOS 7.4.1 with FortiSwitchOS 7.4.1, more tests have been added to the FortiSwitch recommendations to help optimize your network:

- When a connected tier-1 MCLAG peer group is detected and FortiOS detects a possible tier-2 MCLAG pair of switches, FortiOS recommends forming a tier-2 MCLAG.

  After you accept the recommendation, the `set lldp-profile default-auto-mclag-icl` command is configured on the two switches with the recommended interchassis link (ICL) ports, and the `config switch auto-`

`isl-port-group` command is configured on the parent MCLAG peer group.

- When a connected tier-2 MCLAG peer group is detected and FortiOS detects a possible tier-3 MCLAG pair of switches, FortiOS recommends forming a tier-3 MCLAG.

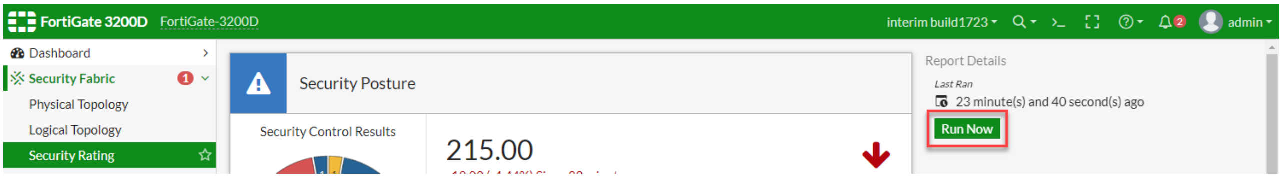
  After you accept the recommendation, the `set lldp-profile default-auto-mclag-icl` command is configured on the two switches with the recommended ICL ports, and the `config switch auto-isl-port-group` command is configured on the parent MCLAG peer group.

NOTE: For detection to be successful, there must be fully meshed connection (each tier-2 FortiSwitcch unit must have a connection to each tier-1 FortiSwitch unit; each tier-3 FortiSwitch unit must have a connection to each tier-2 FortiSwitch unit.

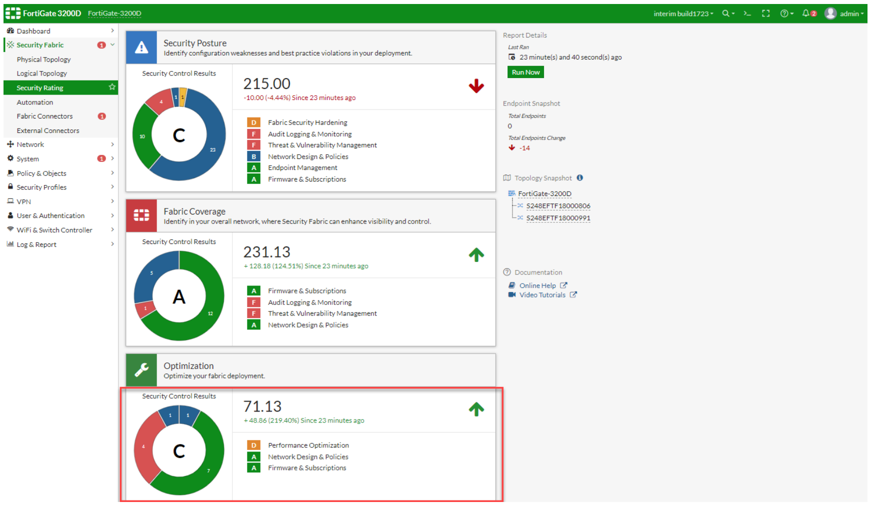
NOTE: The Security Rating feature is available only when VDOMs are disabled.

To optimize your FortiSwitch network:

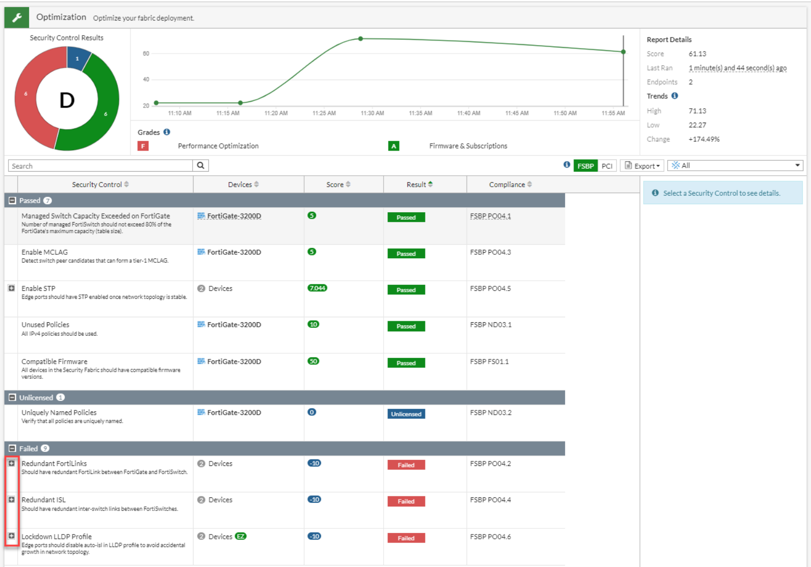
1. Go to *Security Fabric > Security Rating*.
2. Select *Run Now* (under *Report Details* in the right pane) to generate the Security Rating report.



3. Select the *Optimization* section.


FortiGate 3200D
FortiGate-3200D
interim build1723
admin
Dashboard
Security Fabric
Physical Topology
Logical Topology
Security Rating
Automation
Fabric Connectors
External Connectors
Network
System
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
Log & Report
Security Posture
Identify configuration weaknesses and best practice violations in your deployment.
Security Control Results
C
215.00
-10.00 (-4.44%) Since 23 minutes ago
D Fabric Security Hardening
F Audit Logging & Monitoring
F Threat & Vulnerability Management
B Network Design & Policies
A Endpoint Management
A Firmware & Subscriptions
Fabric Coverage
Identify in your overall network, where Security Fabric can enhance visibility and control.
Security Control Results
A
231.13
+ 128.18 (124.51%) Since 23 minutes ago
A Firmware & Subscriptions
F Audit Logging & Monitoring
F Threat & Vulnerability Management
A Network Design & Policies
Optimization
Optimize your fabric deployment.
Security Control Results
C
71.13
+ 48.86 (219.40%) Since 23 minutes ago
D Performance Optimization
A Network Design & Policies
A Firmware & Subscriptions
Report Details
Last Ran
23 minute(s) and 40 second(s) ago
Run Now
Endpoint Snapshot
Total Endpoints
0
Total Endpoints Change
-14
Topology Snapshot
FortiGate-3200D
S248EFTF18000806
S248EFTF18000991
Documentation
Online Help
Video Tutorials

4. Under *Failed*, select + next to each item to see more details in the right pane.



Optimize your fabric deployment.

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

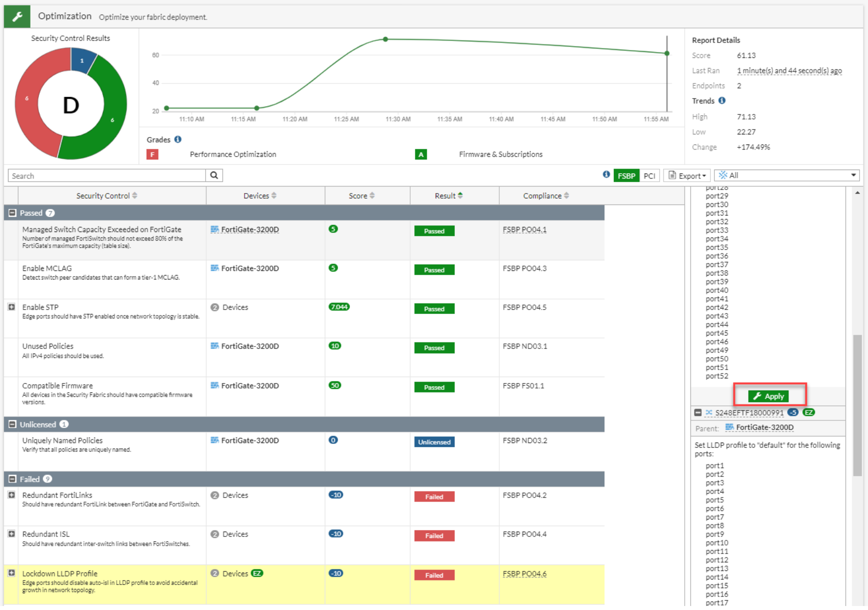
F Performance Optimization

A Firmware & Subscriptions

Security Control	Devices	Score	Result	Compliance
Passed 7				
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.	2 Devices	7.044	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	50	Passed	FSBP FS01.1
Unlicensed 1				
Uniquely Named Policies Verify that all policies are uniquely named.	FortiGate-3200D	0	Unlicensed	FSBP ND03.2
Failed 9				
Redundant FortiLinks Should have redundant FortiLink between FortiGate and FortiSwitch.	2 Devices	-10	Failed	FSBP PO04.2
Redundant ISL Should have redundant inter-switch links between FortiSwitches.	2 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.	2 Devices EZ	-10	Failed	FSBP PO04.6

Select a Security Control to see details.

5. If you agree with a suggestion in the *Recommendations* section, select *Apply* for the change to be made.



Optimize your fabric deployment.

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

Security Control	Devices	Score	Result	Compliance
Passed 7				
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.	2 Devices	7.044	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	50	Passed	FSBP FS01.1
Unlicensed 1				
Uniquely Named Policies Verify that all policies are uniquely named.	FortiGate-3200D	0	Unlicensed	FSBP ND03.2
Failed 9				
Redundant FortiLinks Should have redundant FortiLink between FortiGate and FortiSwitch.	2 Devices	-10	Failed	FSBP PO04.2
Redundant ISL Should have redundant inter-switch links between FortiSwitches.	2 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.	2 Devices EZ	-10	Failed	FSBP PO04.6

```
port28
port29
port30
port31
port32
port33
port34
port35
port36
port37
port38
port39
port40
port41
port42
port43
port44
port45
port46
port49
port50
port51
port52
```

S248EFTF18000991 -5 EZ

Parent: FortiGate-3200D

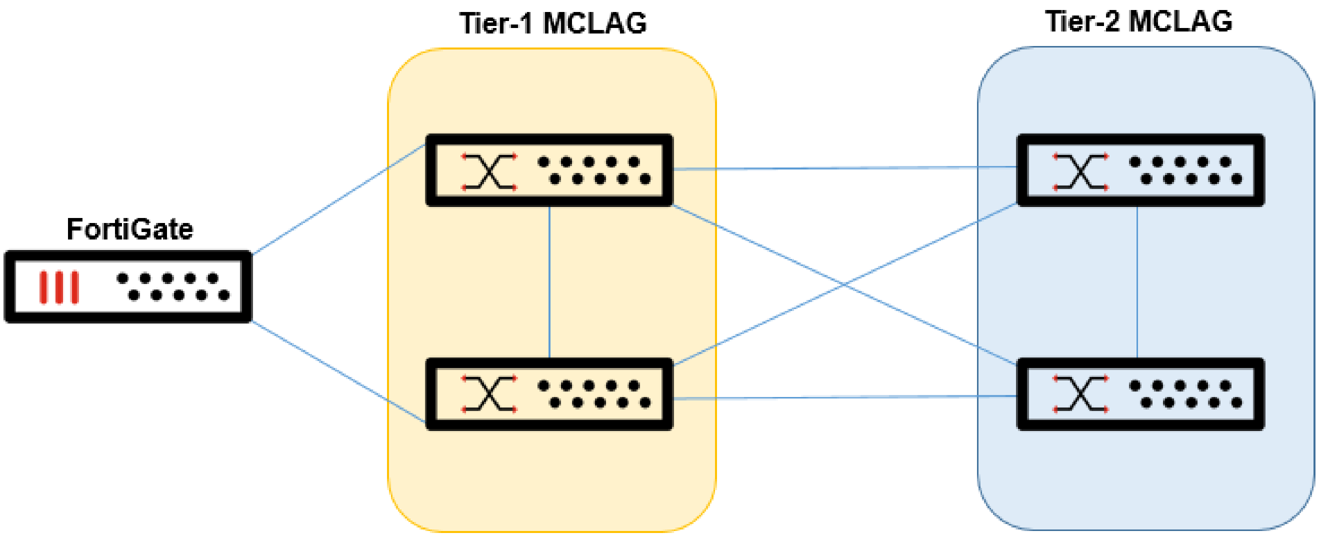
Set LLDP profile to "default" for the following ports:

```
port1
port2
port3
port4
port5
port6
port7
port8
port9
port10
port11
port12
port13
port14
port15
port16
port17
```

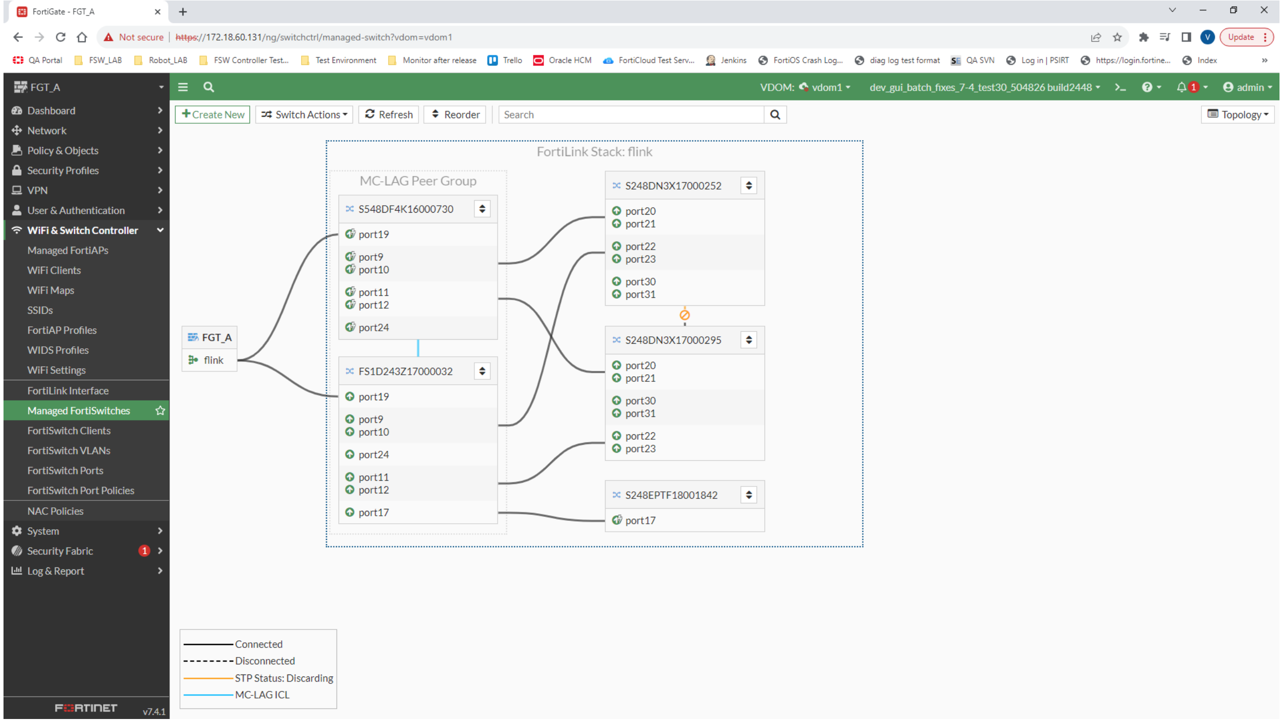
After accepting a recommended change to the network, you must go to *Security Fabric > Security Rating* and click *Run Now* again after the network change is made to update the recommendations based on the new network topology.

Example

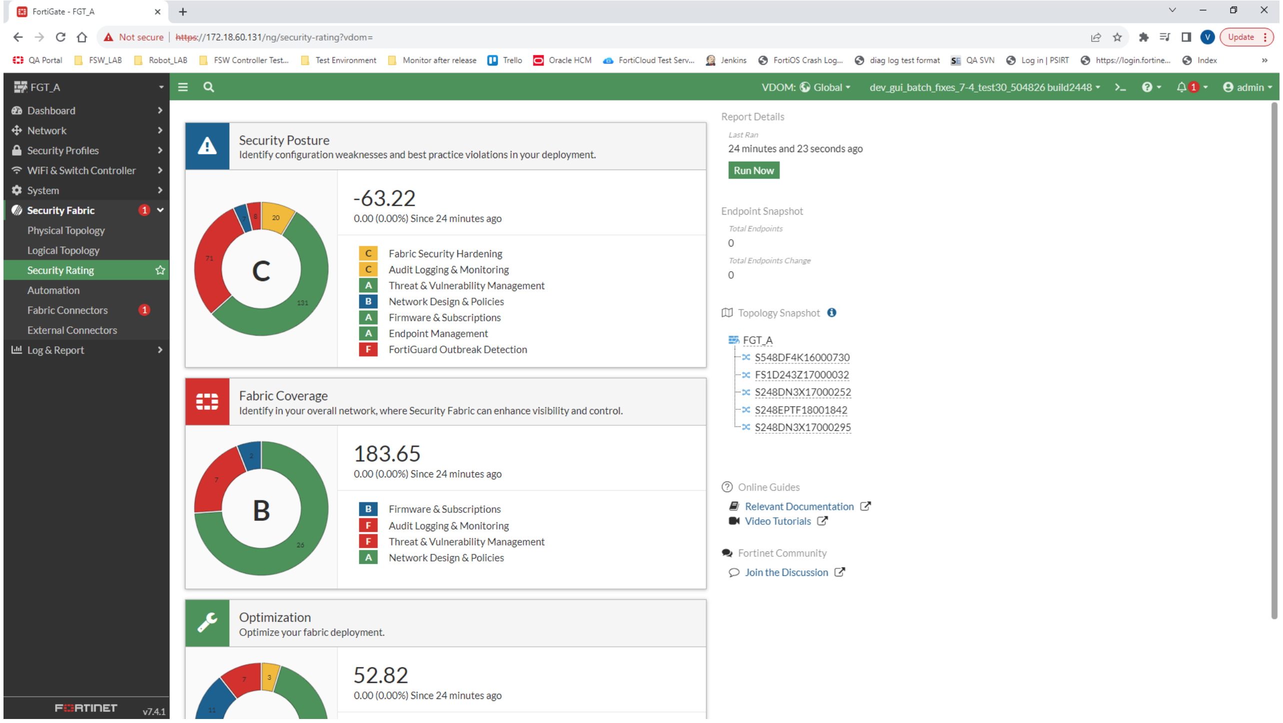
In this example, a FortiGate device manages four FortiSwitch units. Two of the switches already form an MCLAG, and the user wants a second MCLAG tier for redundancy.



1. In the FortiOS GUI, go to *WiFi & Switch Controller > Managed FortiSwitches* and verify that the two tier-2 FortiSwitch units are the same model so that they can form an MCLAG.



2. Go to *Security Fabric > Security Rating* and click *Run Now*.



Security Posture
Identify configuration weaknesses and best practice violations in your deployment.

C

-63.22
0.00 (0.00%) Since 24 minutes ago

C	Fabric Security Hardening
C	Audit Logging & Monitoring
A	Threat & Vulnerability Management
B	Network Design & Policies
A	Firmware & Subscriptions
A	Endpoint Management
F	FortiGuard Outbreak Detection

Fabric Coverage
Identify in your overall network, where Security Fabric can enhance visibility and control.

B

183.65
0.00 (0.00%) Since 24 minutes ago

B	Firmware & Subscriptions
F	Audit Logging & Monitoring
F	Threat & Vulnerability Management
A	Network Design & Policies

Optimization
Optimize your fabric deployment.

52.82
0.00 (0.00%) Since 24 minutes ago

Report Details
Last Ran
24 minutes and 23 seconds ago
Run Now

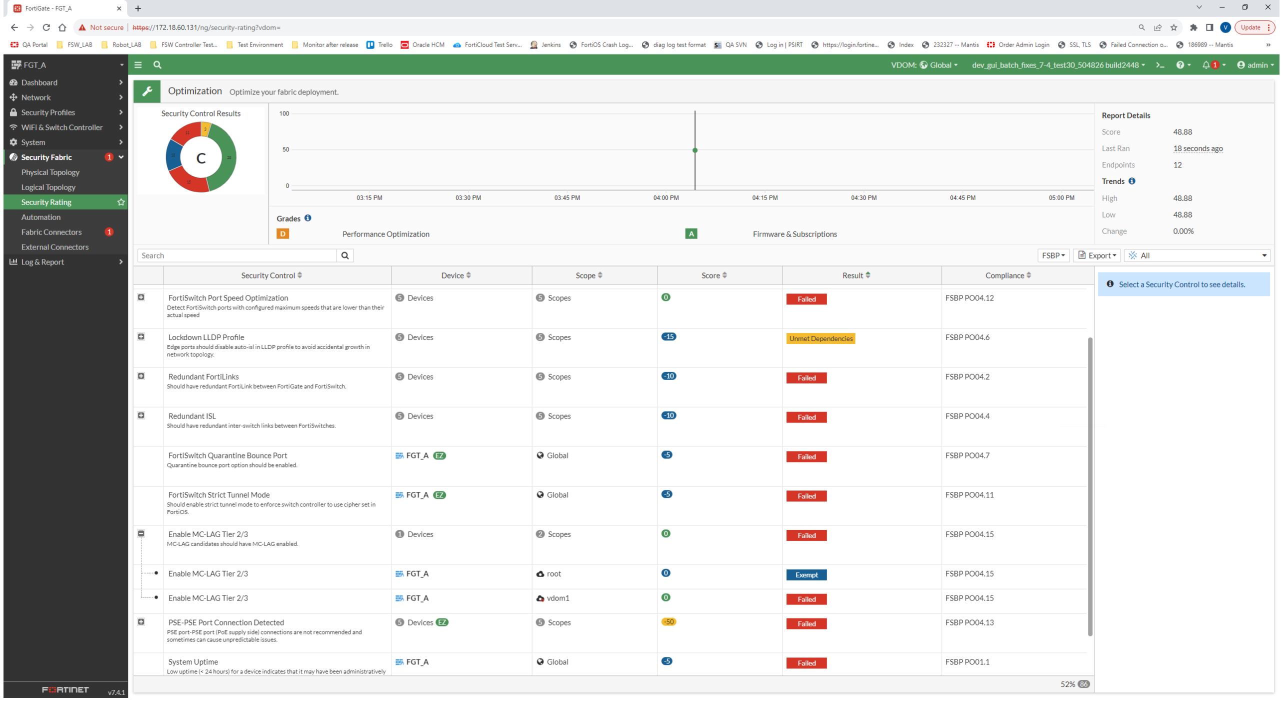
Endpoint Snapshot
Total Endpoints
0
Total Endpoints Change
0

Topology Snapshot
FGT_A
S548DF4K16000730
FS1D243Z17000032
S248DN3X17000252
S248EPTF18001842
S248DN3X17000295

Online Guides
Relevant Documentation
Video Tutorials

Fortinet Community
Join the Discussion

3. After the security rating report has run, expand the *Optimization* results to see *Enable MC-LAG Tier 2/3*.



Optimization Optimize your fabric deployment.

Grades
D Performance Optimization
A Firmware & Subscriptions

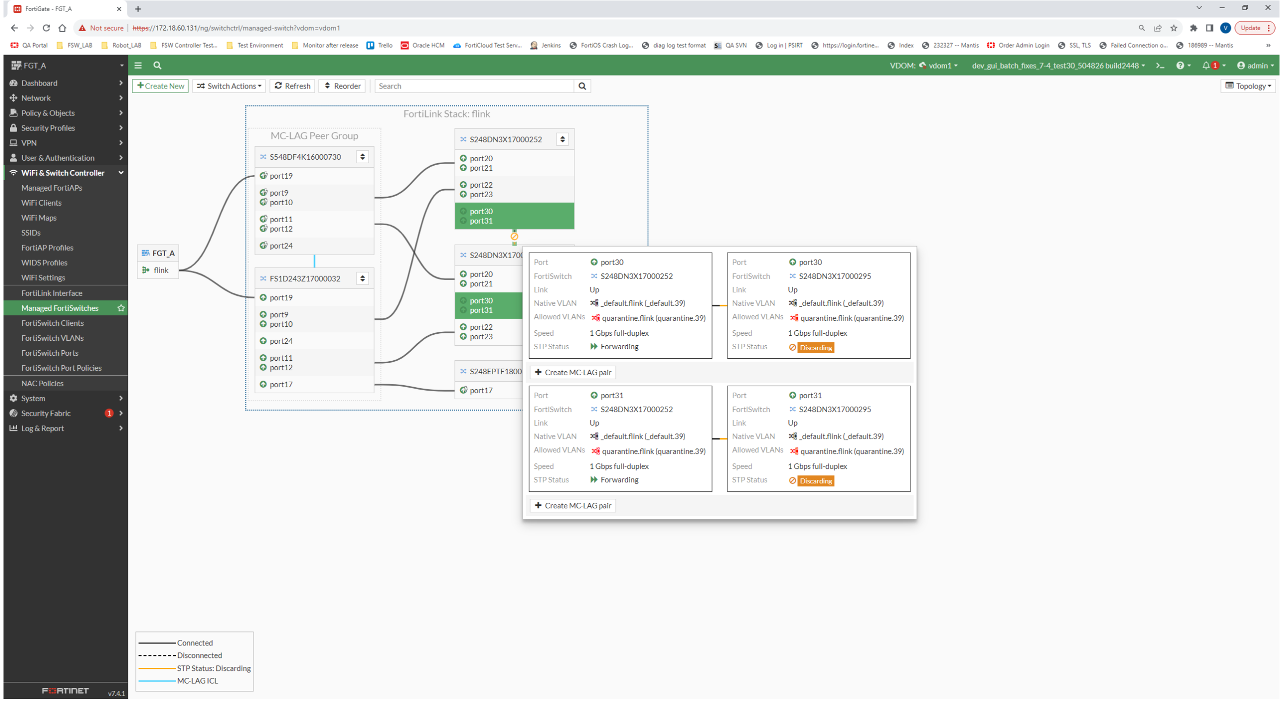
Report Details

Score	48.88
Last Ran	18 seconds ago
Endpoints	12
Trends	
High	48.88
Low	48.88
Change	0.00%

Select a Security Control to see details.

Security Control	Device	Scope	Score	Result	Compliance
FortiSwitch Port Speed Optimization Detect FortiSwitch ports with configured maximum speeds that are lower than their actual speed	5 Devices	5 Scopes	0	Failed	FSBP PO04.12
Lockdown LLDP Profile Edge ports should disable auto-isl in LLDP profile to avoid accidental growth in network topology.	5 Devices	5 Scopes	-15	Unmet Dependencies	FSBP PO04.6
Redundant FortiLinks Should have redundant FortiLink between FortiGate and FortiSwitch.	5 Devices	5 Scopes	-10	Failed	FSBP PO04.2
Redundant ISL Should have redundant inter-switch links between FortiSwitches.	5 Devices	5 Scopes	-10	Failed	FSBP PO04.4
FortiSwitch Quarantine Bounce Port Quarantine bounce port option should be enabled.	FGT_A EZ	Global	-5	Failed	FSBP PO04.7
FortiSwitch Strict Tunnel Mode Should enable strict tunnel mode to enforce switch controller to use cipher set in FortiOS.	FGT_A EZ	Global	-5	Failed	FSBP PO04.11
Enable MC-LAG Tier 2/3 MC-LAG candidates should have MC-LAG enabled.	1 Devices	2 Scopes	0	Failed	FSBP PO04.15
Enable MC-LAG Tier 2/3	FGT_A	root	0	Exempt	FSBP PO04.15
Enable MC-LAG Tier 2/3	FGT_A	vdom1	0	Failed	FSBP PO04.15
PSE-PSE Port Connection Detected PSE port-PSE port (PoE supply side) connections are not recommended and sometimes can cause unpredictable issues.	5 Devices EZ	5 Scopes	-50	Failed	FSBP PO04.13
System Uptime Low uptime (< 24 hours) for a device indicates that it may have been administratively	FGT_A	Global	-5	Failed	FSBP PO01.1

4. Go to *WiFi & Switch Controller > Managed FortiSwitches* and hover over the link connecting the two tier-2 FortiSwitch units. Click *Create MC-LAG pair*.



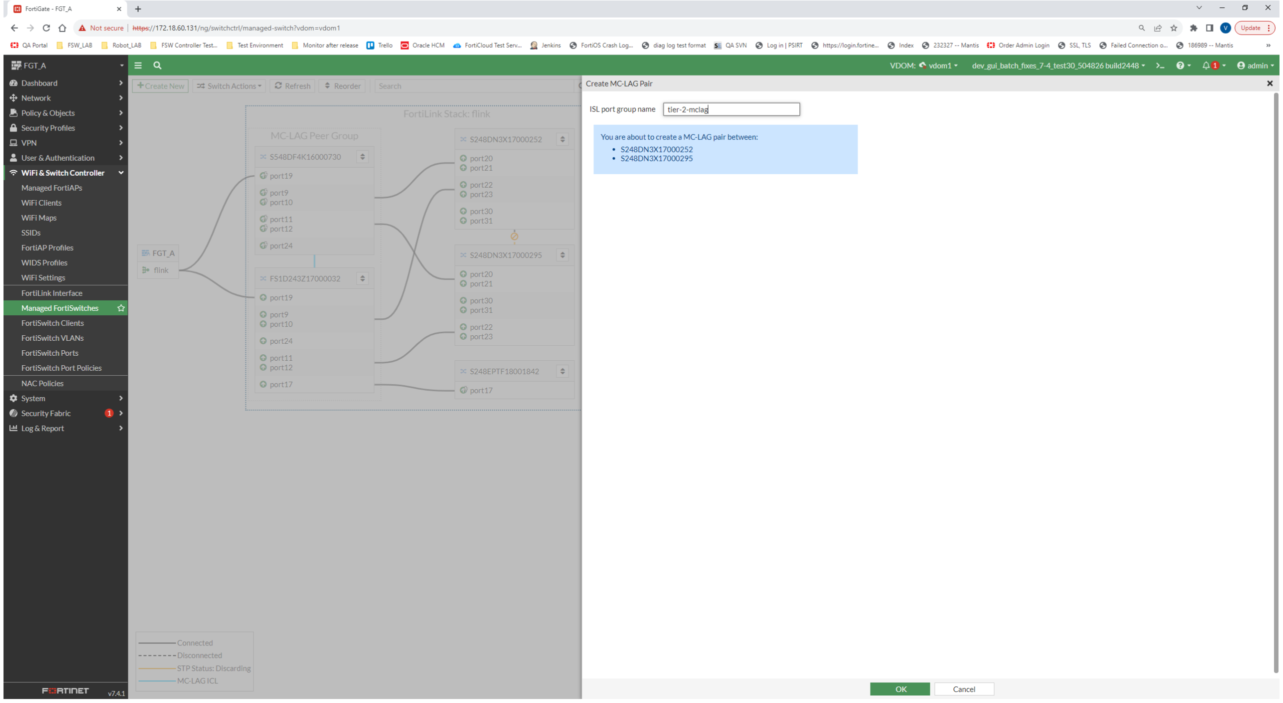
Port	port30	Port	port30
FortiSwitch	S248DN3X17000252	FortiSwitch	S248DN3X17000295
Link	Up	Link	Up
Native VLAN	_default.flink (_default.39)	Native VLAN	_default.flink (_default.39)
Allowed VLANs	quarantine.flink (quarantine.39)	Allowed VLANs	quarantine.flink (quarantine.39)
Speed	1 Gbps full-duplex	Speed	1 Gbps full-duplex
STP Status	Forwarding	STP Status	Discarding

+ Create MC-LAG pair

Port	port31	Port	port31
FortiSwitch	S248DN3X17000252	FortiSwitch	S248DN3X17000295
Link	Up	Link	Up
Native VLAN	_default.flink (_default.39)	Native VLAN	_default.flink (_default.39)
Allowed VLANs	quarantine.flink (quarantine.39)	Allowed VLANs	quarantine.flink (quarantine.39)
Speed	1 Gbps full-duplex	Speed	1 Gbps full-duplex
STP Status	Forwarding	STP Status	Discarding

+ Create MC-LAG pair

5. In the *Create MC-LAG Pair* panel, enter the ISL port group name.



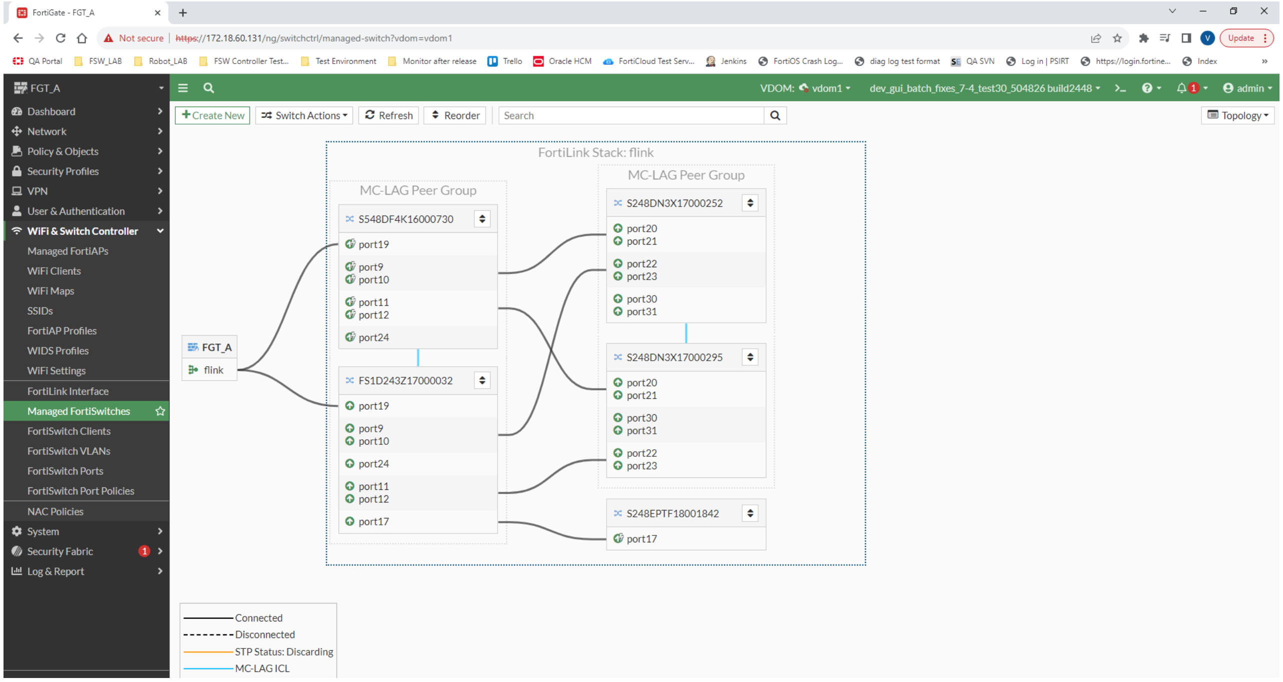
Create MC-LAG Pair

ISL port group name: tier-2-mclag

You are about to create a MC-LAG pair between:

- S248DN3X17000252
- S248DN3X17000295

6. The *Managed FortiSwitches* page shows that the MCLAG is formed for the tier-2 managed FortiSwitch units.


FortiGate - FGT_A
Not secure
https://172.18.60.131/ng/switchctrl/managed-switch?vdom=vdom1
FGT_A
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
Managed FortiAPs
WiFi Clients
WiFi Maps
SSIDs
FortiAP Profiles
WIDS Profiles
WiFi Settings
FortiLink Interface
Managed FortiSwitches
FortiSwitch Clients
FortiSwitch VLANs
FortiSwitch Ports
FortiSwitch Port Policies
NAC Policies
System
Security Fabric
Log & Report
VDOM: vdom1
dev_gui_batch_fixes_7-4_test30_504826 build2448
admin
Create New
Switch Actions
Refresh
Reorder
Search
Topology
FortiLink Stack: flink
MC-LAG Peer Group
S548DF4K16000730
port19
port9
port10
port11
port12
port24
FS1D243Z17000032
port19
port9
port10
port24
port11
port12
port17
MC-LAG Peer Group
S248DN3X17000252
port20
port21
port22
port23
port30
port31
S248DN3X17000295
port20
port21
port30
port31
port22
port23
S248EPTF18001842
port17
FGT_A
flink
Connected
Disconnected
STP Status: Discarding
MC-LAG ICL

Configuring QoS with managed FortiSwitch units

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

- The FortiGate unit does not support QoS for hard or soft switch ports.
- The FS-1xxE and FS-1xxF models support a single QoS map. If there is more than one QoS map, the first configured map is used.

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>
```

For QoS commands to be successfully executed, the feature must be supported by the FortiSwitch unit. Refer to the FortiSwitch feature matrix for details about the features supported by each FortiSwitch model.

Configuring a voice QoS policy

The FortiOS switch controller offers a predefined QoS policy for Voice-over-IP, based on the common best practices in the VoIP industry. The following is the mapping of DSCP and CoS values:

Application	DSCP value	CoS value	Queue
VoIP Data	DSCP 46	CoS 5	Queue 1
VoIP Control	DSCP 24,26	CoS 3	Queue 2
Routing Protocol	DSCP 48	CoS 6	Queue 2
STP BPDU	DSCP 56	CoS 7	Queue 2
Real-Time Video	DSCP 34 DSCP others DSCP others	CoS 3 CoS 2 CoS 0,1	Queue 3 Queue 3 Queue 4

The egress policy is based on the following requirements:

Application	Bandwidth requirement
VoIP Data	Up to 100% bandwidth
VoIP Control, Routing Protocol, and STP BPDU	Up to 10% bandwidth
Real-Time Video	Up to 60% bandwidth
Other applications	Up to 20% bandwidth

To assign the QoS policy to the FortiSwitch ports, go to *WiFi & Switch Controller > FortiSwitch Ports*.

The following is the default 802.1p map for the voice QoS policy:

```
config switch-controller qos dot1p-map
   edit "voice-dot1p"
      set priority-0 queue-4
      set priority-1 queue-4
      set priority-2 queue-3
      set priority-3 queue-2
      set priority-4 queue-3
      set priority-5 queue-1
      set priority-6 queue-2
      set priority-7 queue-2
   next
end
```

The following is the default DSCP map for the voice QoS policy:

```
config switch-controller qos ip-dscp-map
   edit "voice-dscp"
      config map
         edit "1"
            set cos-queue 1
            set value 46
         next
         edit "2"
            set cos-queue 2
            set value 24,26,48,56
         next
         edit "5"
            set cos-queue 3
            set value 34
         next
      end
   next
end
```

The following is the default egress policy for the voice QoS policy:

```
config switch-controller qos queue-policy
   edit "voice-egress"
      set schedule weighted
      set rate-by kbps
      config cos-queue
         edit "queue-0"
         next
         edit "queue-1"
            set weight 0
         next
```

```
            edit "queue-2"
               set weight 6
            next
            edit "queue-3"
               set weight 37
            next
            edit "queue-4"
               set weight 12
            next
            edit "queue-5"
            next
            edit "queue-6"
            next
            edit "queue-7"
            next
         end
      next
   end
```

The following is the default voice QoS policy:

```
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
```

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 one RSPAN session or one ERSPAN session.

In RSPAN mode, traffic is encapsulated in VLAN 4092 and sent toward the FortiGate device, where it can be captured using packet capture. The FortiSwitch unit assigns the uplink port and the dst port. The switching functionality is enabled on the dst interface when mirroring.

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 is the device acting as an ERSPAN collector. The collector must be reachable by the FortiSwitch unit using IPv4 ICMP ping (**NOTE:** A firewall policy might be required on the FortiGate device.). If the collector IP address is not specified, the traffic is not mirrored.

ERSPAN cannot be used with SPAN or RSPAN.

When you are using RSPAN or ERSPAN, the switch controller automatically configures a policer to limit the traffic. For example:

```
config switch-controller traffic-policy
   edit "sniffer"
      set description "Rate control for sniffer mirrored traffic"
      set guaranteed-bandwidth 50000
      set guaranteed-burst 8192
      set maximum-burst 163840
      set cos-queue 0
   next
end

config system interface
   edit "rspan"
      set switch-controller-traffic-policy "sniffer"
   next
end
```

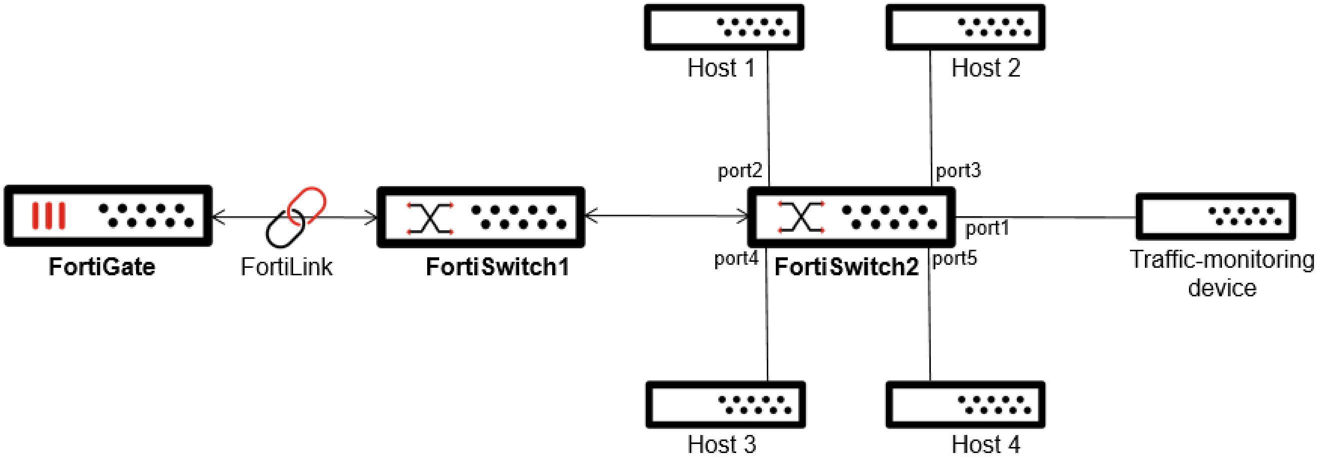
Refer to the FortiSwitchOS feature matrix to see which FortiSwitch models support the policer.

FortiSwitch port-based mirroring

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
```

In the following example, the ingress traffic from port2 and port3 and the egress traffic from port4 and port5 are mirrored to port1, where the traffic-monitoring device is connected.



```
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 disable FortiSwitch port mirroring:

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

FortiSwitch RSPAN

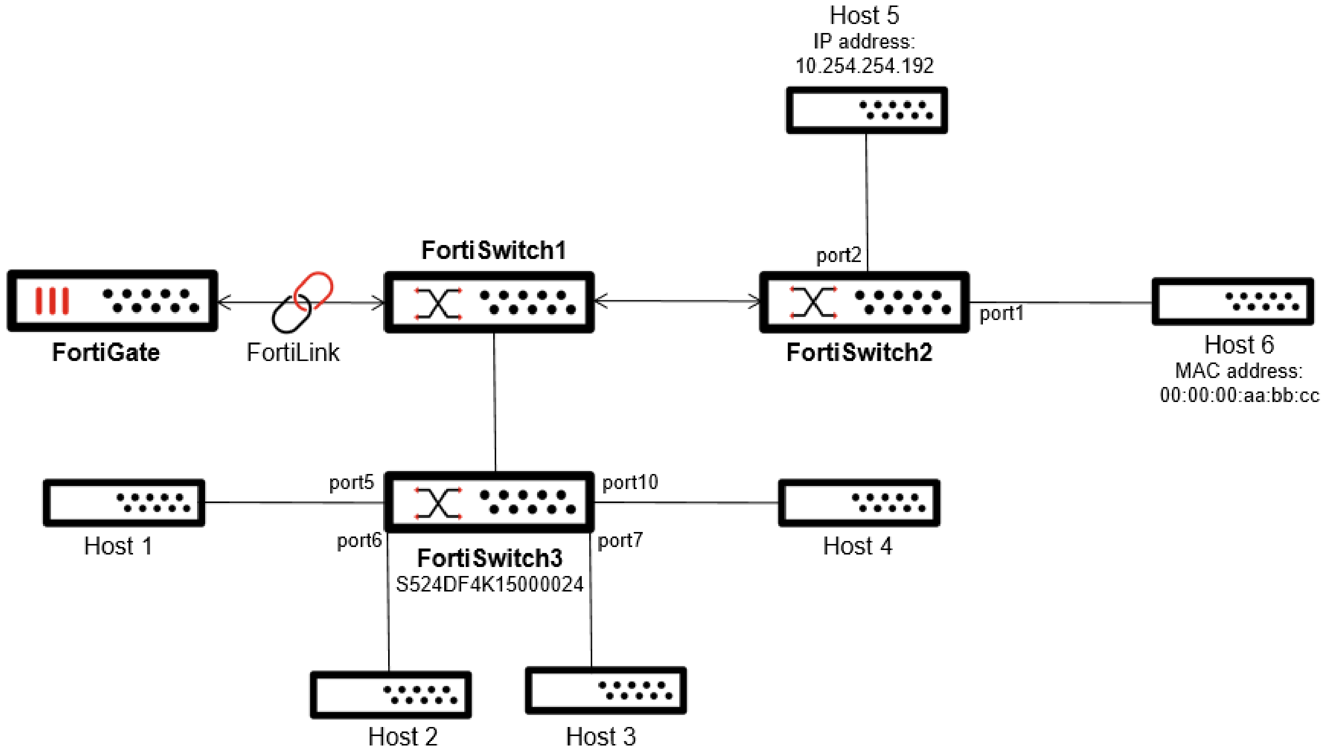
To configure FortiSwitch RSPAN:

```
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
```

In the following example, traffic matching any of the `target-mac`, `target-ip`, and `target-port` parameters is captured.

To monitor the traffic on a FortiGate device, go to *Network > Diagnostics > Packet Capture* and capture the traffic on the “rspan” VLAN. The traffic can also be downloaded as a PCAP file. For more details, see Using the packet capture tool.



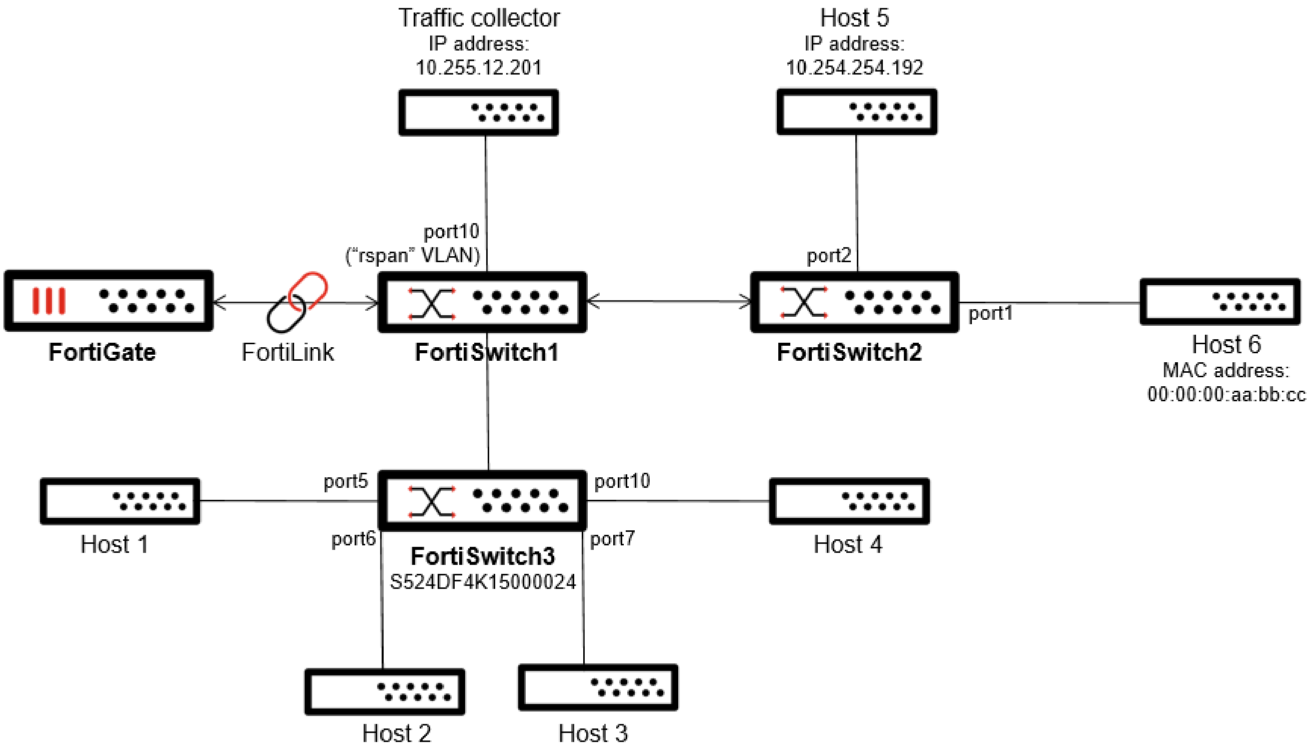
```
config switch-controller traffic-sniffer
   set mode rspan
   config target-mac
      edit 00:00:00:aa:bb:cc
         set description MACtarget1
      end
   config target-ip
      edit 10.254.254.192
         set description IPtarget1
      end
   config target-port
      edit S524DF4K15000024
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

FortiSwitch ERSPAN

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 from this MAC address
         set description <string>
      end
   config target-ip
      edit <xxx.xxx.xxx.xxx> // mirror traffic sent from 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 10.255.12.201
   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
```

Configuring the FortiOS one-arm sniffer

Starting in FortiOS 7.4.1 with FortiSwitchOS 7.4.1, you can use the FortiOS one-arm sniffer to configure a VLAN interface on a managed FortiSwitch unit as an intrusion detection system (IDS). Traffic sent to the interface is examined for matches to the configured security profile. The matches are logged, and the unmatched sniffed traffic is not forwarded to the FortiGate device. Sniffing only reports on attacks; it does not deny or influence traffic.

Traffic scanned on the FortiOS one-arm sniffer interface is processed by the CPU. The FortiOS one-arm sniffer might cause higher CPU usage and perform at a lower level than traditional inline scanning.

The absence of high CPU usage does not indicate the absence of packet loss. Packet loss might occur due to the capacity of the TAP devices hitting maximum traffic volume during mirroring or, on the FortiGate device, when the kernel buffer size is exceeded and it is unable to handle bursts of traffic.

To configure the FortiOS one-arm sniffer in the CLI:

1. Specify the managed switch port to use to mirror traffic in RSPAN or ERSPAN mode on page 293.

2. Enable the FortiOS one-arm sniffer on the VLAN interface that will mirror traffic on page 294.

3. Configure the FortiOS one-arm sniffer in a firewall policy on page 294.

4. Generate traffic on the client.

5. Review the logs for the sniffer policy on page 295.

1. Specify the managed switch port to use to mirror traffic in RSPAN or ERSPAN mode

You can mirror traffic in RSPAN or ERSPAN mode on a layer-2 VLAN. Specify which ingress port you want to use for a mirroring source.

```
config switch-controller traffic-sniffer
   set mode {rspan | erspan-auto}
   config target-port
      edit <FortiSwitch_serial_number>
         set in-ports <port_name>
      next
```

```
    end
end
```

For example:

```
config switch-controller traffic-sniffer
   set mode rspan
   config target-port
      edit S524DF4K15000024
         set in-ports port6
      next
   end
end
```

2. Enable the FortiOS one-arm sniffer on the VLAN interface that will mirror traffic

After you enable `ips-sniffer-mode`, `switch-controller-access-vlan` and `switch-controller-rspan-mode` are enabled by default, and `switch-controller-traffic-policy` is set to `sniffer` by default.

```
config system interface
   edit <interface_name>
      set ips-sniffer-mode enable
      set switch-controller-access-vlan enable
      set switch-controller-traffic-policy sniffer
      set switch-controller-rspan-mode enable
   next
end
```

For example:

```
config system interface
   edit rspan
      set ips-sniffer-mode enable
      set switch-controller-access-vlan enable
      set switch-controller-traffic-policy sniffer
      set switch-controller-rspan-mode enable
   next
end
```

3. Configure the FortiOS one-arm sniffer in a firewall policy

Specify the same interface that you used in step 2. Enable the security profiles that you want to use and specify the `sniffer-profile` profile for each security profile. By default, all security profiles are disabled.

```
config firewall sniffer
   edit <sniffer_ID>
      set logtraffic {all | utm}
      set interface <interface_name>
      set av-profile-status {enable | disable}
      set av-profile "sniffer-profile"
      set webfilter-profile-status {enable | disable}
      set webfilter-profile "sniffer-profile"
      set application-list-status {enable | disable}
      set application-list "sniffer-profile"
      set ips-sensor-status {enable | disable}
      set ips-sensor "sniffer-profile"
      set file-filter-profile-status {enable | disable}
      set file-filter-profile "sniffer-profile"
   next
end
```

For example:

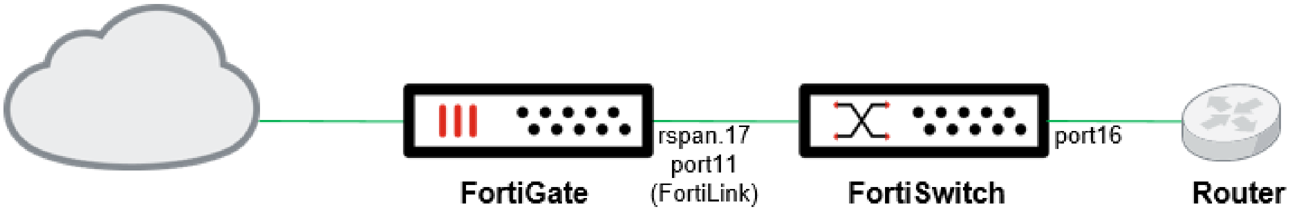
```
config firewall sniffer
   edit 50
      set logtraffic all
      set interface rspan
      set av-profile-status enable
      set av-profile sniffer-profile
      set webfilter-profile-status enable
      set webfilter-profile sniffer-profile
      set application-list-status enable
      set application-list sniffer-profile
      set ips-sensor-status enable
      set ips-sensor sniffer-profile
      set file-filter-profile-status enable
      set file-filter-profile sniffer-profile
   next
end
```

5. Review the logs for the sniffer policy

```
execute log display
```

Configuration example

The following example shows how a managed FortiSwitch unit mirrors traffic from a client and then sends the traffic to the FortiGate device for analysis. In this example, enable the FortiOS one-arm sniffer in the FortiOS CLI and then use the FortiOS GUI for the rest of the example.

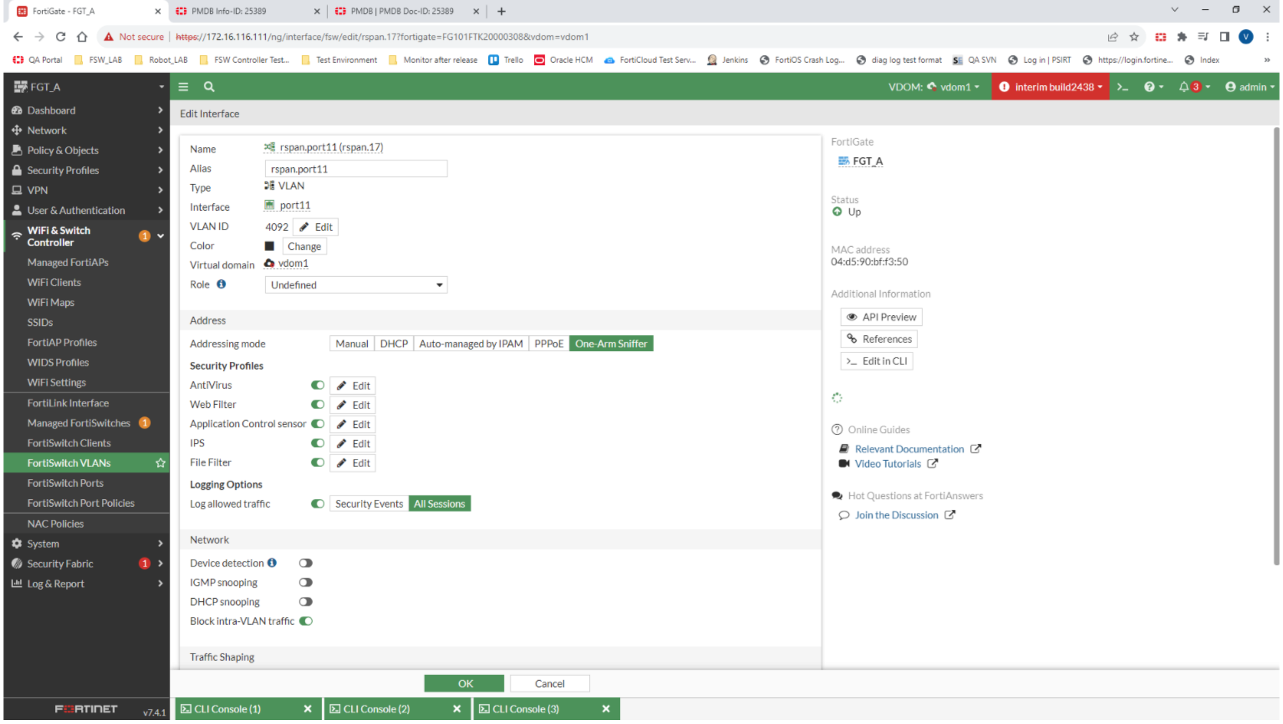


1. Enable the FortiOS one-arm sniffer.

```
config system interface
   edit "rspan.17"
      set ips-sniffer-mode enable
      set vdom root
      set interface port11
      set vlanid 4092
```

```
    next
end
```

2. Go to *Network > Interfaces*.
3. Select *rspan.17* (under *port11*) and click *Edit*.
4. Enable the security profiles that you want to use.



Edit Interface

Name rspan.port11 (rspan.17)
Alias rspan.port11
Type VLAN
Interface port11
VLAN ID 4092 Edit
Color ■ Change
Virtual domain vdom1
Role Undefined

Address

Addressing mode: Manual | DHCP | Auto-managed by IPAM | PPPoE | [✓ One-Arm Sniffer]

Security Profiles

AntiVirus ● Edit
Web Filter ● Edit
Application Control sensor ● Edit
IPS ● Edit
File Filter ● Edit

Logging Options

Log allowed traffic ● Security Events [✓ All Sessions]

Network

Device detection ○
IGMP snooping ○
DHCP snooping ○
Block intra-VLAN traffic ●

Traffic Shaping

OK Cancel

FortiGate
FGT_A

Status
Up

MAC address
04:d5:90:bf:f3:50

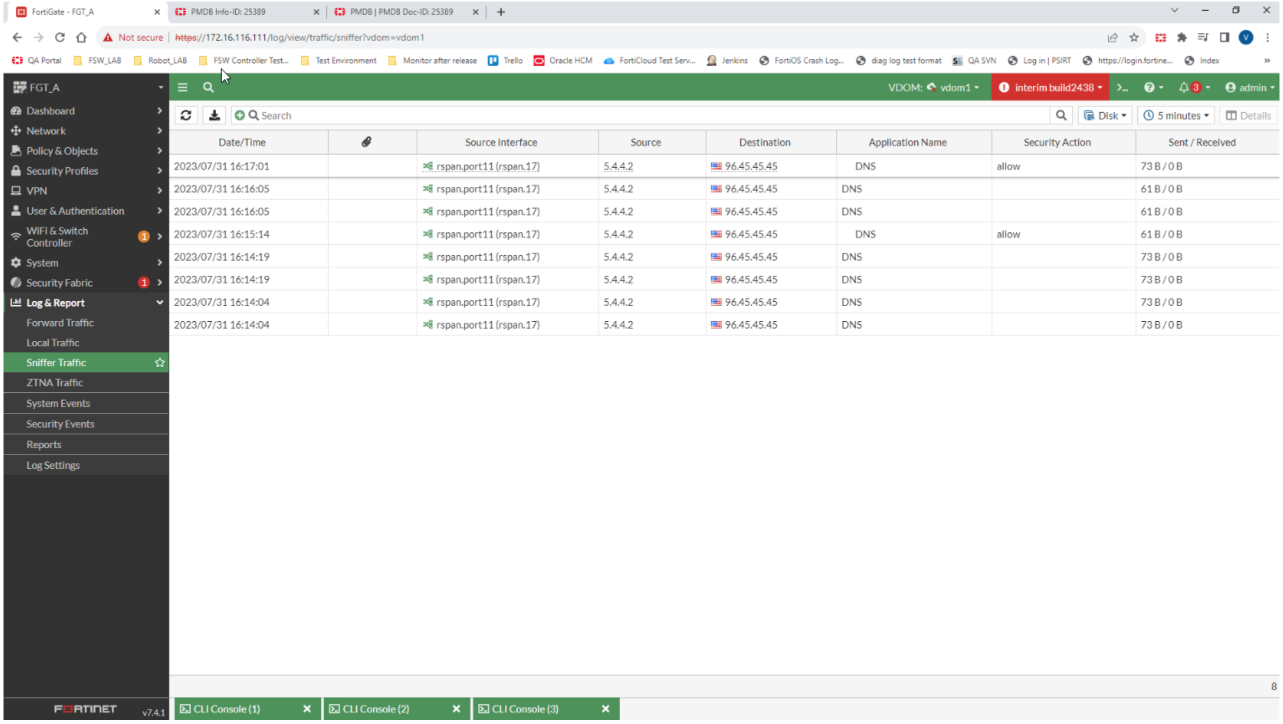
Additional Information
API Preview
References
Edit in CLI

Online Guides
Relevant Documentation
Video Tutorials

Hot Questions at FortiAnswers
Join the Discussion

5. Click *OK*.
6. Generate traffic on the client.
7. Go to *Log & Report > Sniffer Traffic*.

   The logs generated from the mirrored traffic are listed.



Date/Time		Source Interface	Source	Destination	Application Name	Security Action	Sent / Received
2023/07/31 16:17:01		rspan.port11 (rspan.17)	5.4.4.2	96.45.45.45	DNS	allow	73 B / 0 B
2023/07/31 16:16:05		rspan.port11 (rspan.17)	5.4.4.2	96.45.45.45	DNS		61 B / 0 B
2023/07/31 16:16:05		rspan.port11 (rspan.17)	5.4.4.2	96.45.45.45	DNS		61 B / 0 B
2023/07/31 16:15:14		rspan.port11 (rspan.17)	5.4.4.2	96.45.45.45	DNS	allow	61 B / 0 B
2023/07/31 16:14:19		rspan.port11 (rspan.17)	5.4.4.2	96.45.45.45	DNS		73 B / 0 B
2023/07/31 16:14:19		rspan.port11 (rspan.17)	5.4.4.2	96.45.45.45	DNS		73 B / 0 B
2023/07/31 16:14:04		rspan.port11 (rspan.17)	5.4.4.2	96.45.45.45	DNS		73 B / 0 B
2023/07/31 16:14:04		rspan.port11 (rspan.17)	5.4.4.2	96.45.45.45	DNS		73 B / 0 B

In the FortiOS CLI, use the `execute log display` command to view the logs:

```
784 logs found.
10 logs returned.
1: date=2023-07-31 time=16:28:13 eventtime=1690846092971957519 tz="-0700" logid="0004000017"
      type="traffic" subtype="sniffer" level="notice" vd="vdom1" srcip=5.4.4.2 srcport=51293
      srcintf="rspan.17" srcintfrole="undefined" dstip=96.45.45.45 dstport=53 dstintf="rspan.17"
      dstintfrole="undefined" srccountry="Germany" dstcountry="United States" sessionid=784
      proto=17 action="accept" policyid=1 policytype="sniffer" service="DNS" trandisp="snat"
      transip=0.0.0.0 transport=0 duration=180 sentbyte=70 rcvdbyte=0 sentpkt=1 rcvdpkt=0
      appid=16195 app="DNS" appcat="Network.Service" apprisk="elevated" utmaction="allow"
      countapp=1 sentdelta=70 rcvddelta=0 mastersrcmac="00:0c:29:38:2a:c6"
      srcmac="00:0c:29:38:2a:c6" srcserver=0 masterdstmac="04:d5:90:bf:f3:50"
      dstmac="04:d5:90:bf:f3:50" dstserver=0
2: date=2023-07-31 time=16:27:39 eventtime=1690846059062169260 tz="-0700" logid="0004000017"
      type="traffic" subtype="sniffer" level="notice" vd="vdom1" srcip=5.4.4.2 srcport=37800
      srcintf="rspan.17" srcintfrole="undefined" dstip=96.45.45.45 dstport=53 dstintf="rspan.17"
      dstintfrole="undefined" srccountry="Germany" dstcountry="United States" sessionid=782
      proto=17 action="accept" policyid=1 policytype="sniffer" service="DNS" trandisp="snat"
      transip=0.0.0.0 transport=0 duration=180 sentbyte=70 rcvdbyte=0 sentpkt=1 rcvdpkt=0
      appid=16195 app="DNS" appcat="Network.Service" apprisk="elevated" utmaction="allow"
      countapp=1 sentdelta=70 rcvddelta=0 mastersrcmac="00:0c:29:38:2a:c6"
      srcmac="00:0c:29:38:2a:c6" srcserver=0 masterdstmac="04:d5:90:bf:f3:50"
      dstmac="04:d5:90:bf:f3:50" dstserver=0 utmref=0-6524
3: date=2023-07-31 time=16:27:39 eventtime=1690846059062027560 tz="-0700" logid="0004000017"
      type="traffic" subtype="sniffer" level="notice" vd="vdom1" srcip=5.4.4.2 srcport=52702
      srcintf="rspan.17" srcintfrole="undefined" dstip=96.45.45.45 dstport=53 dstintf="rspan.17"
      dstintfrole="undefined" srccountry="Germany" dstcountry="United States" sessionid=780
      proto=17 action="accept" policyid=1 policytype="sniffer" service="DNS" trandisp="snat"
      transip=0.0.0.0 transport=0 duration=180 sentbyte=61 rcvdbyte=0 sentpkt=1 rcvdpkt=0
      appid=16195 app="DNS" appcat="Network.Service" apprisk="elevated" utmaction="allow"
      countapp=1 sentdelta=61 rcvddelta=0 mastersrcmac="00:0c:29:38:2a:c6"
      srcmac="00:0c:29:38:2a:c6" srcserver=0 masterdstmac="04:d5:90:bf:f3:50"
      dstmac="04:d5:90:bf:f3:50" dstserver=0 utmref=0-6510
```

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 on page 298
- Configuring SNMP locally on page 300
- Sending SNMP traps for MAC address changes on page 302
- SNMP OIDs on page 303

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
```

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 system snmp user
   edit <SNMP_user_configuration>
      set notify-hosts <IPv4_address>
      set notify-hosts6 <IPv6_address>
   next
end

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
```

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
```

Sending SNMP traps for MAC address changes

Starting in FortiOS 7.6.0, you can configure an SNMP trap so that you receive a message when a layer-2 MAC address has been added to, moved from or to, or deleted from a managed FortiSwitch port. This SNMP trap allows network administrators to monitor MAC address changes in real time, which strengthens overall network security.

This SNMP trap applies only to dynamic MAC addresses learned on the managed FortiSwitch port. MAC events can be lost by the hardware or software.

To send SNMP traps for MAC address changes:

1. Enable the SNMP trap for MAC address changes in a specific SNMP community.

   By default, this SNMP trap is disabled.

   ```
   config switch-controller snmp-community
      edit <SNMP_community_identifier>
         set name <SNMP_community_name>
         set events l2mac
      next
   end
   ```

   For example:

   ```
   config switch-controller snmp-community
      edit 1
         set name newsnmpcommunity
         set events l2mac
      next
   end
   ```

2. If the managed switch's port has `set access-mode static`, enable the logging of dynamic MAC address events for this interface. If the managed switch's port has `set access-mode dynamic` or `set access-mode nac`, the `set log-mac-event` command is hidden. By default, dynamic MAC address events are not logged. Enabling the logging for an interface reports when a dynamic MAC address is learned, moved, or deleted.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set log-mac-event enable
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit S548DF5018000776
      config ports
         edit port10
            set log-mac-event enable
         next
      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 unit 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 unit 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 unit 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.

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 packet-sampler {disabled | enabled}
            set packet-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 packet-sampler enabled
            set packet-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.

To use flow tracking and export:

1. Enabling packet sampling on page 306
2. Configuring flow tracking on page 306
3. Viewing the flow-export data on page 308

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.

Enabling packet sampling

To use flow export, you must first enable packet sampling for each switch port and trunk. You can specify the packet sampling rate and the sampling direction. The default packet sampling rate is 512 packets per second, and the default sampling direction is `both`, which monitors transmitted traffic and received traffic.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set packet-sampler enabled
            set packet-sample-rate <0-99999>
            set sample-direction {tx | rx | both}
         next
      end
   next
end
```

For example:

```
config switch-controller managed-switch
   edit "mdf1-1"
      config ports
         edit "port1"
            set packet-sampler enabled
            set packet-sample-rate 512
            set sample-direction both
         next
      end
   next
end
```

Configuring flow tracking

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.

Viewing the flow-export data

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
```

Using the FortiView Internal Hubs monitor

Starting in FortiOS 7.2.4 with FortiSwitchOS 7.2.3, you can use the *FortiView Internal Hubs* monitor in FortiOS to monitor the connections between devices in private networks, as specified in RFC 1918 (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16). The *FortiView Internal Hubs* monitor reports 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.

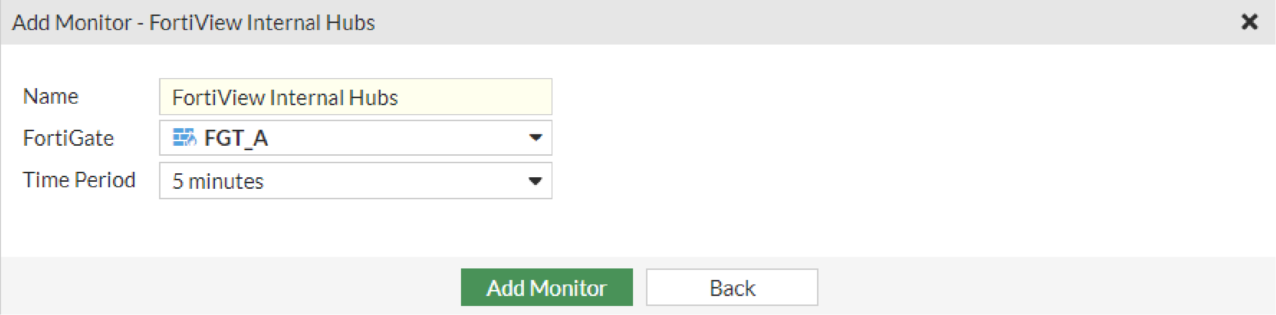
To enable the *FortiView Internal Hubs* monitor on a managed FortiSwitch unit:

```
config system interface
   edit <FortiLink_interface>
      set ip <IP_address_and_netmask>
      set switch-controller-netflow-collect enable
   next
end

config switch-controller flow-tracking
   config collectors
      edit <name>
         set ip <FortiLink_interface_IPv4_address>
      next
   end
end
```

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.

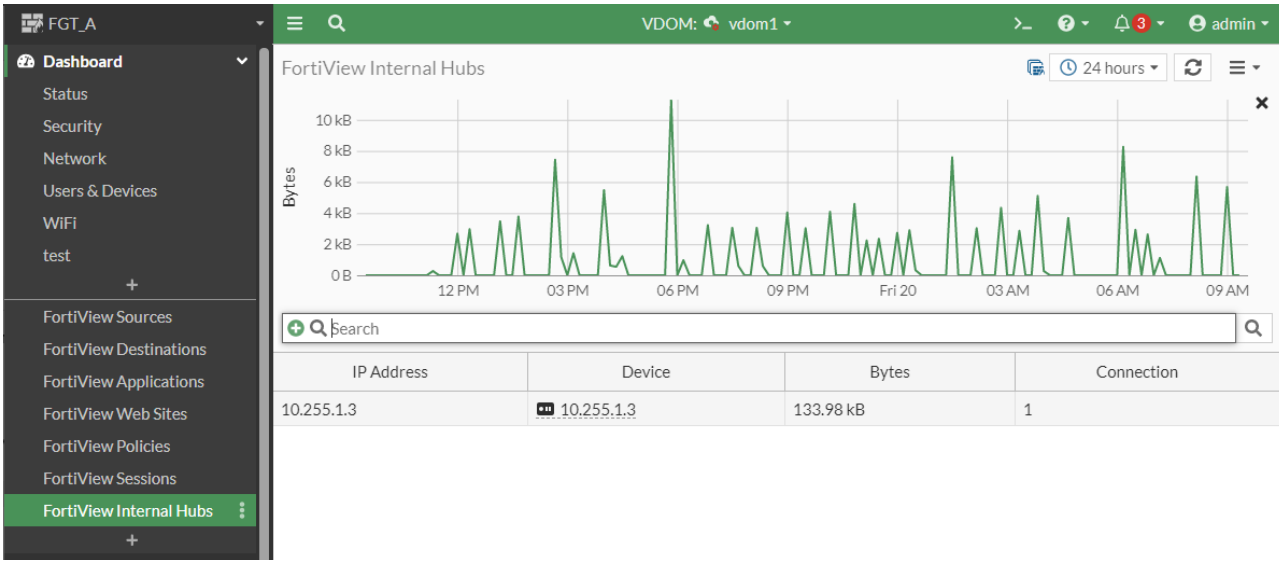
4. From the *Time Period* dropdown list, select how long to monitor (5 minutes, 1 hour, or 24 hours).



Add Monitor - FortiView Internal Hubs

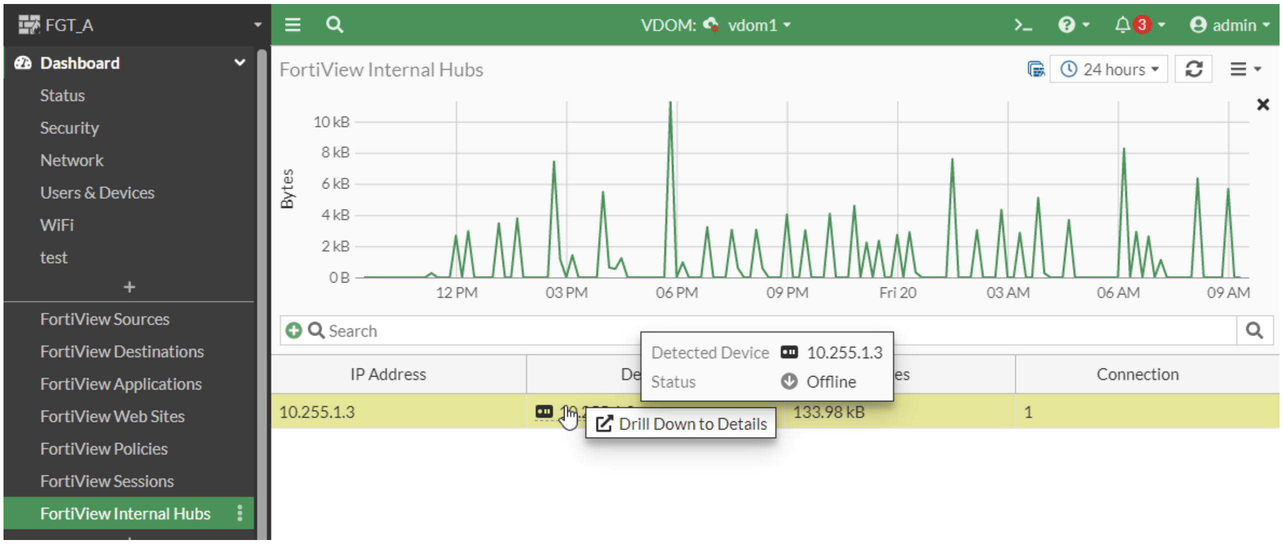
Name	FortiView Internal Hubs
FortiGate	FGT_A
Time Period	5 minutes

5. Click *Add Monitor*.
6. Under *Dashboard*, select *FortiView Internal Hubs* to display the *FortiView Internal Hubs* page.



IP Address	Device	Bytes	Connection
10.255.1.3	10.255.1.3	133.98 kB	1

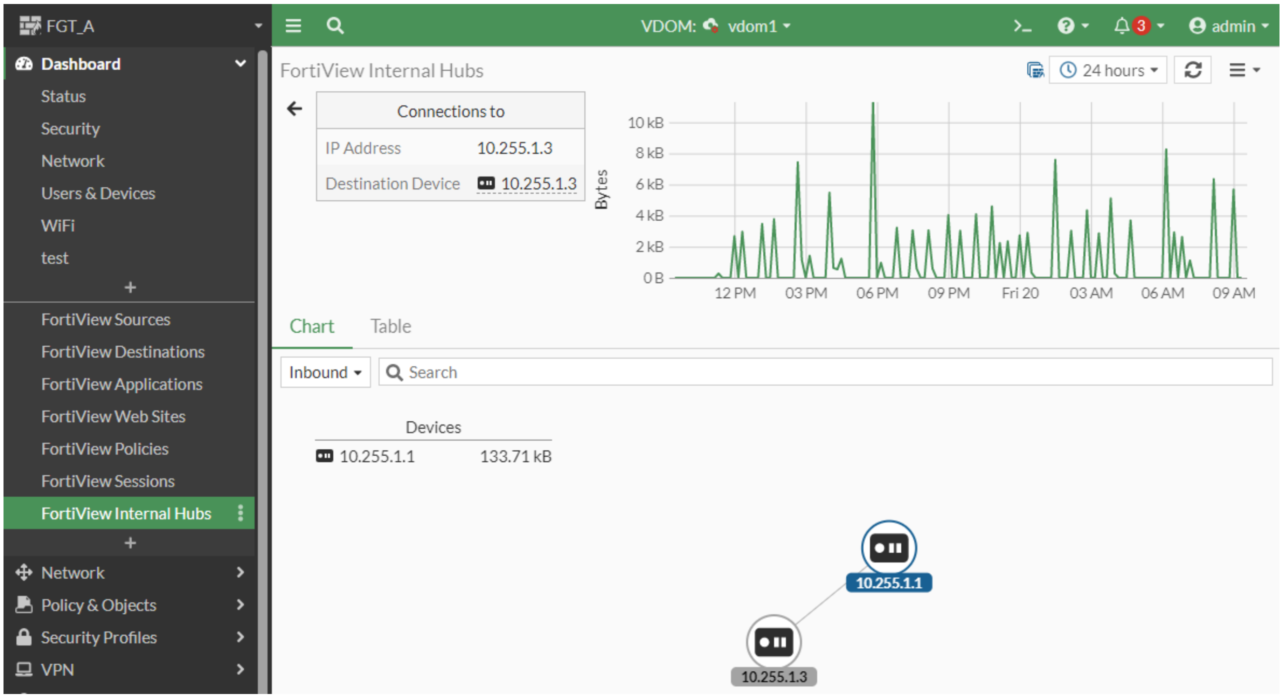
7. Right-click on one of the devices and select *Drill Down to Details*.



Detected Device 10.255.1.3
Status Offline

IP Address	De	es	Connection
10.255.1.3	10.2	133.98 kB	1

8. You can select the *Chart* or *Table* tab to change how the details are displayed.



Connections to	
IP Address	10.255.1.3
Destination Device	10.255.1.3

Devices	
10.255.1.1	133.71 kB

Configuring flow control and ingress pause metering

Flow control allows you to configure a port to send or receive a “pause frame” (that is, a special packet that signals a source to stop sending flows for a specific time interval because the buffer is full). By default, flow control is disabled on all ports.

```
config switch-controller managed-switch
   edit <FortiSwitch_serial_number>
      config ports
         edit <port_name>
            set flow-control {both | rx | tx | disable}
         next
      end
   end
```

Parameters enable flow control to do the following:

- rx—receive pause control frames
- tx—transmit pause control frames
- both—transmit and receive pause control frames

If you enable flow control to transmit pause control frames or to transmit and receive pause control frames, you can also use ingress pause metering to limit the input bandwidth of an ingress port. Because ingress pause metering stops the traffic temporarily instead of dropping it, ingress pause metering can provide better performance than policing when the port is connected to a server or end station. To use ingress pause metering, you need to set the ingress metering rate in kilobits and set the percentage of the threshold for resuming traffic on the ingress port.

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

```
      config ports
         edit <port_name>
            set flow-control {tx | both}
            set pause-meter <128–2147483647; set to 0 to disable>
            set pause-meter-resume {25% | 50% | 75%}
         next
      end
   end
```

For example:

```
config switch-controller managed-switch
   edit S424ENTF19000007
      config ports
         edit port29
            set flow-control tx
            set pause-meter 900
            set pause-meter-resume 50%
         next
      end
   end
```

Operation and maintenance

This section covers the following topics:

Defining names for managed switches

Starting in FortiOS 7.4.0, you can use names for managed FortiSwitch units in switch-controller CLI commands. The user-defined name is also used in the FortiOS GUI and logs. The FortiSwitch unit’s serial number is saved in a read-only field.

Follow these rules for defining a managed FortiSwitch name:

- The name can be a maximum of 16 characters in length. Starting in FortiOS 7.6.4, the name can be a maximum of 35 characters in length.
- Use numbers (0-9), letters (a-z and A-Z), dashes, and underscores for the managed FortiSwitch name.

When you upgrade to FortiOS 7.4.0 and later, the FortiSwitch unit’s serial number is used as the managed FortiSwitch name if a managed FortiSwitch name has not been defined. If you downgrade from FortiOS 7.4.0 to an earlier version, the managed FortiSwitch name is changed to the FortiSwitch unit’s serial number.

Using the GUI

1. Go to *WiFi & Switch Controller > Managed FortiSwitches*.
2. Select an unauthorized FortiSwitch unit and then click *Edit*.
3. In the *Name* field, enter a name for the managed FortiSwitch unit.
4. Click *OK* to save the new name.

Using the CLI

```
config switch-controller managed-switch
   rename <FortiSwitch_serial_number> to <managed_FortiSwitch_name>
end
```

For example:

```
config switch-controller managed-switch
   rename S124EN5918003682 to Canada-branch2-finance-team1
end
```

Other CLI changes

In FortiOS 7.4.0, the following CLI changes were made:

- When you pre-configure a managed switch, you must use the `set sn` command under `config switch-controller managed-switch` to store the FortiSwitch serial number. For example:
  ```
  config switch-controller managed-switch
     edit switch1
        set sn S524DNTV21000212
        set fsw-wan1-peer fortilink
        set fsw-wan1-admin enable
     next
  end
  ```
- The `execute switch-controller get-sync-status switch-id <managed_FortiSwitch_name>` command uses the user-defined switch name, and the `execute switch-controller get-sync-status serial <FortiSwitch_serial_number>` command uses the FortiSwitch serial number. For example:
  - `execute switch-controller get-sync-status serial S524DN4K16000116`
  - `execute switch-controller get-sync-status switch-id Racktray-127`
- There is a new `set isl-peer-device-sn` command under `config switch-controller managed-switch` to store the serial number of the ISL peer device. For example:
  ```
  config switch-controller managed-switch
     edit Distribution
        config ports
           edit port2
              set isl-local-trunk-name isltrunk1
              set isl-peer-port-name port23
              set isl-peer-device-name islpeerswitch
              set isl-peer-device-sn S124EN5918003682
           next
        end
     next
  end
  ```

- The following switch-controller CLI commands now use the user-defined FortiSwitch name:
  - `diagnose switch-controller trigger config-sync <managed_FortiSwitch_name>`
  - `execute switch-controller get-conn-status`
  - `execute switch-controller get-physical-conn standard <port_name>`
  - `execute switch-controller get-sync-status all`
  - `execute switch-controller get-upgrade-status`

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 <FortiSwitch_name>
      set sn <PREFIX****nnnnnn>
      ...
   next
end
```

For example:

```
config switch-controller managed-switch
   edit template1
      set sn "S248EP****000000"
      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
```

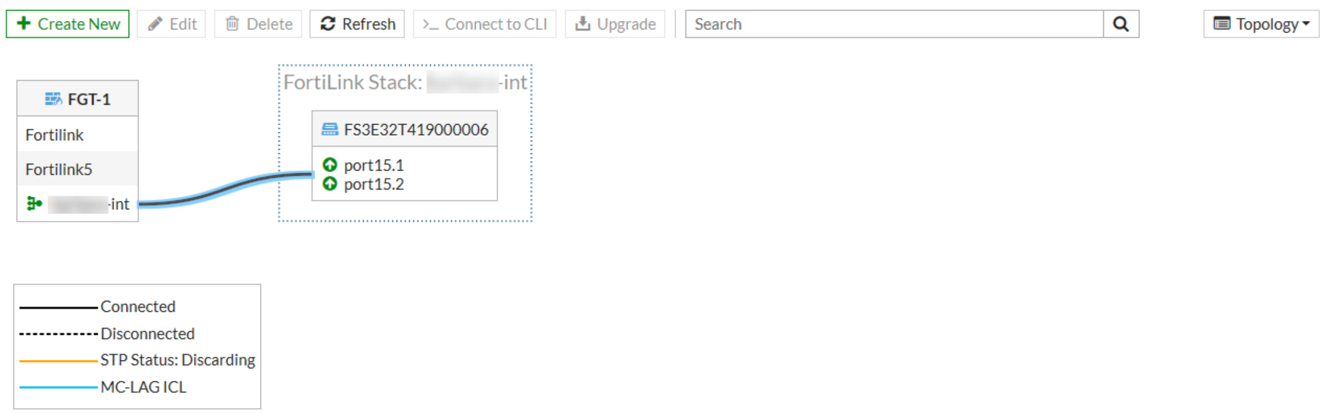
For example:

```
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.



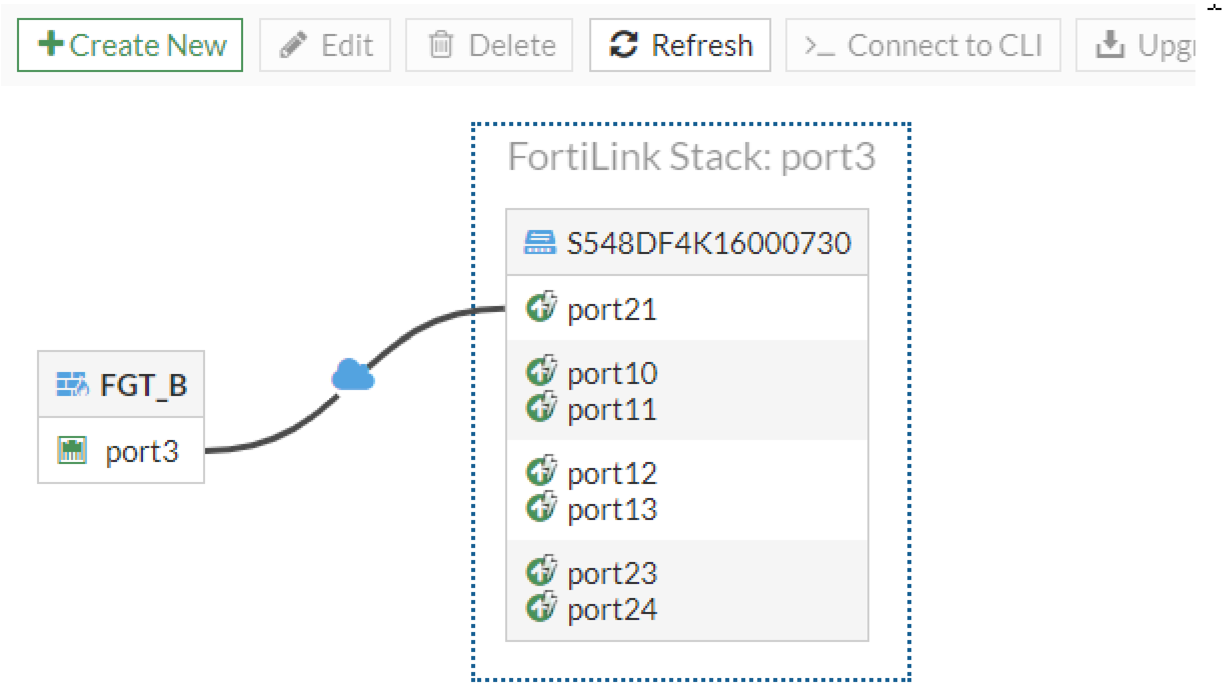
If the link has gone down for some reason, the line will be dashed, and a broken link icon will appear. You can still edit the FortiSwitch unit though and find more information about the status of the switch. The link to the FortiSwitch unit might be down for a number of reasons; for example, a problem 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.

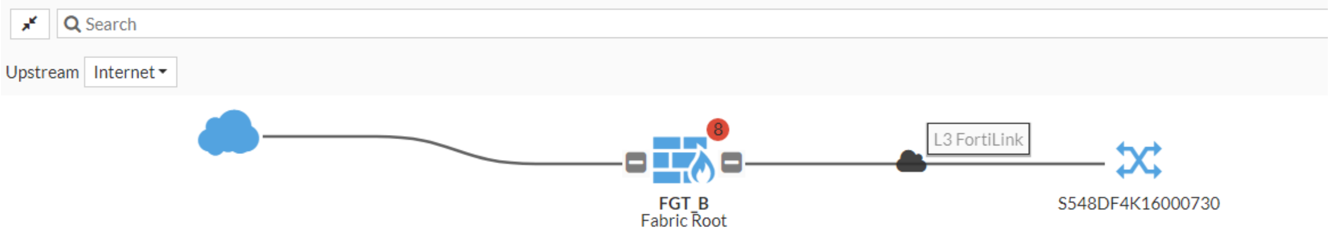
Cloud icon indicates that the FortiSwitch unit is managed over layer 3

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.



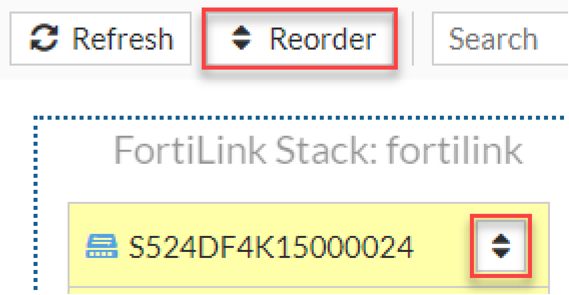
Re-ordering FortiSwitch units in the Topology view

Starting in FortiOS 7.0.1, you can change the order in which FortiSwitch units are displayed in the Topology view.

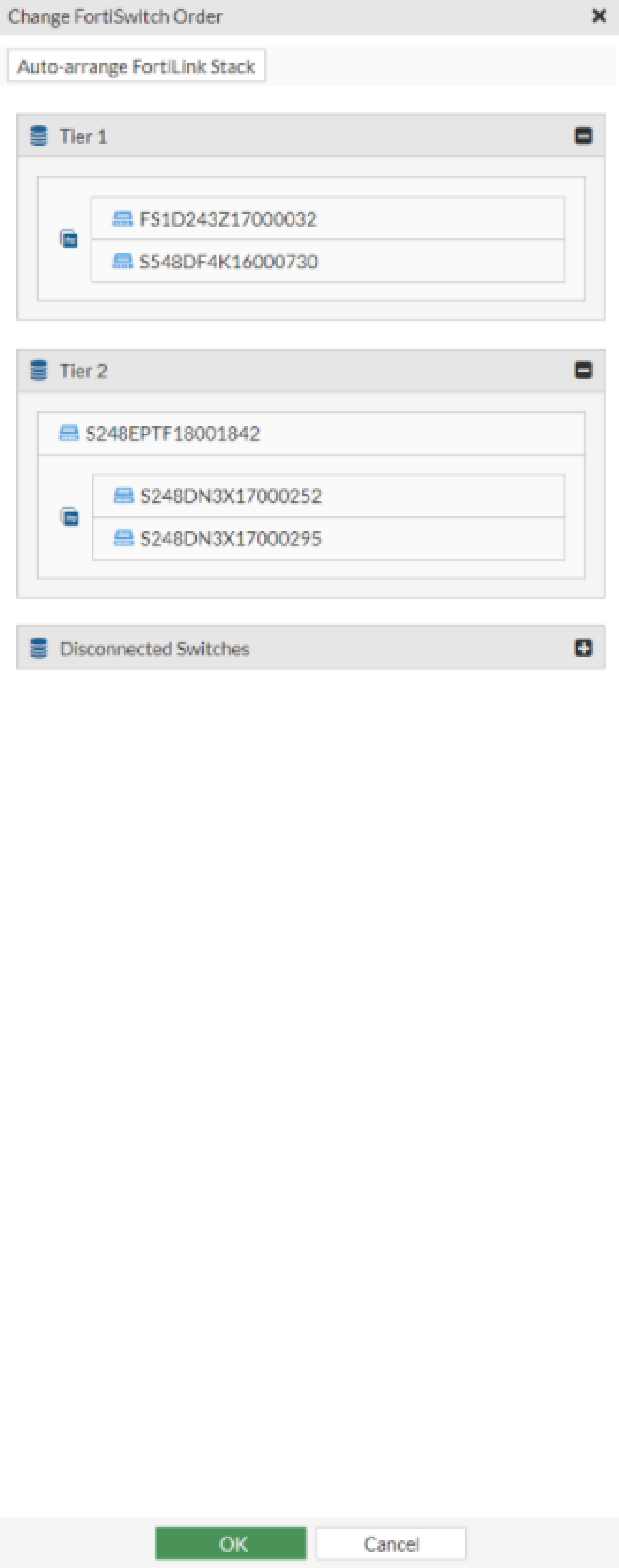
To rearrange the FortiSwitch units in the GUI:

1. Go to *WiFi & Switch Controller > Managed FortiSwitches*.
2. In the *View* dropdown list, select *Topology.*

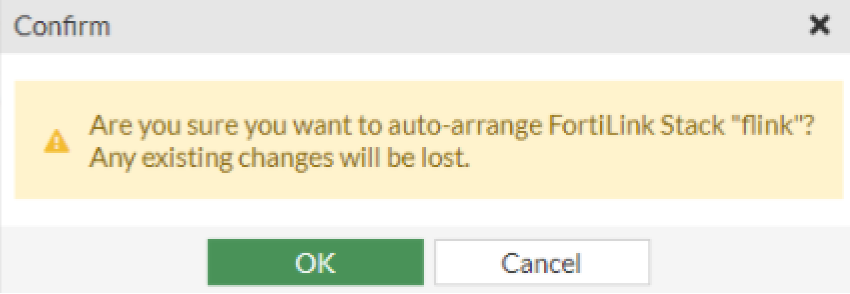
3. Click *Reorder* or the double-arrow button next to the FortiSwitch serial number.



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.



Confirm

Are you sure you want to auto-arrange FortiLink Stack "flink"? Any existing changes will be lost.

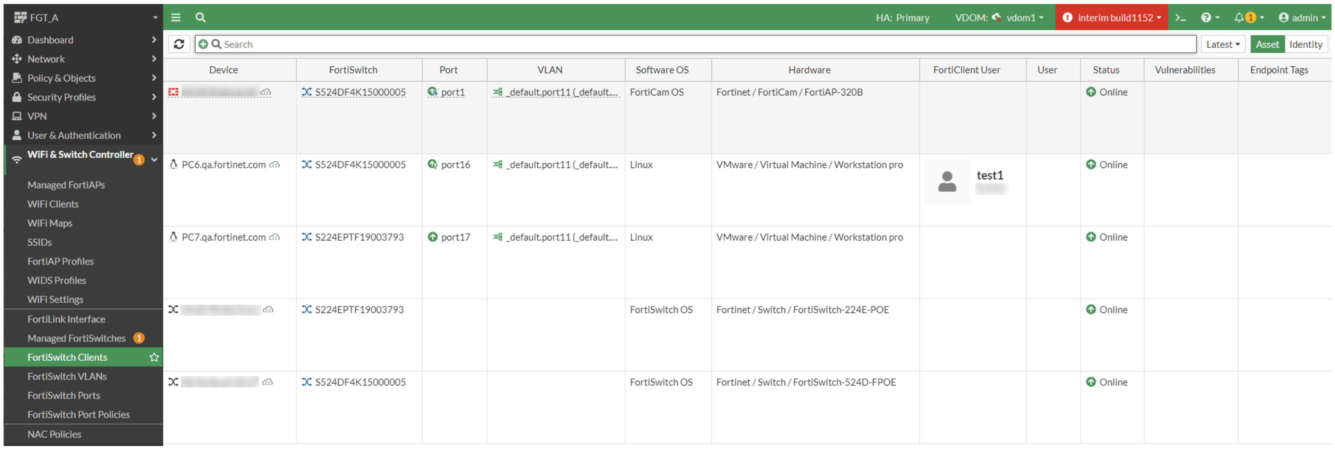
To rearrange the FortiSwitch units in the FortiOS CLI:

```
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.

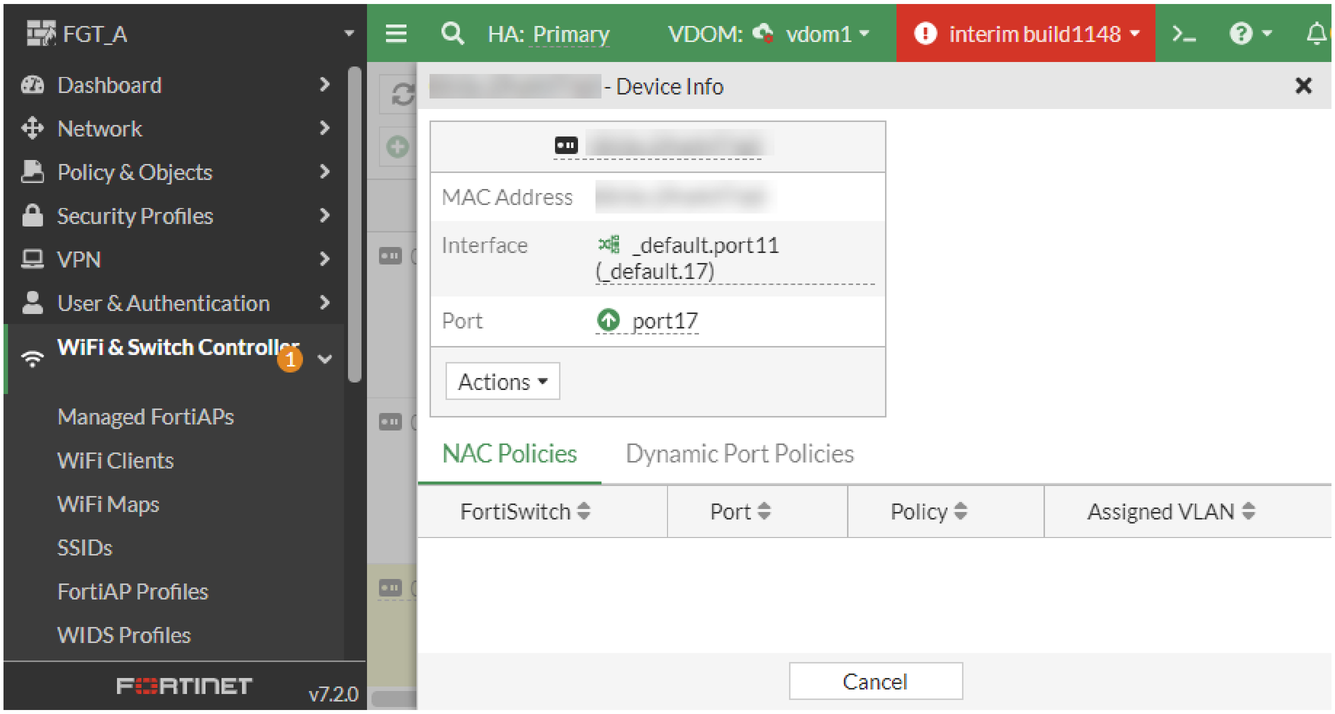
FortiSwitch clients

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.



Device	FortiSwitch	Port	VLAN	Software OS	Hardware	FortiClient User	User	Status	Vulnerabilities	Endpoint Tags
[redacted]	S524DF4K15000005	port1	_default.port11 (_default....	FortiCam OS	Fortinet / FortiCam / FortiAP-320B			Online		
PC6.qa.fortinet.com	S524DF4K15000005	port16	_default.port11 (_default....	Linux	VMware / Virtual Machine / Workstation pro	test1 [redacted]		Online		
PC7.qa.fortinet.com	S224EPTF19003793	port17	_default.port11 (_default....	Linux	VMware / Virtual Machine / Workstation pro			Online		
[redacted]	S224EPTF19003793			FortiSwitch OS	Fortinet / Switch / FortiSwitch-224E-POE			Online		
[redacted]	S524DF4K15000005			FortiSwitch OS	Fortinet / Switch / FortiSwitch-524D-FPOE			Online		

Double-click a row to display the *Device Info* pane.



[redacted] - Device Info

[redacted]

MAC Address	[redacted]
Interface	_default.port11 (_default.17)
Port	port17

NAC Policies | Dynamic Port Policies

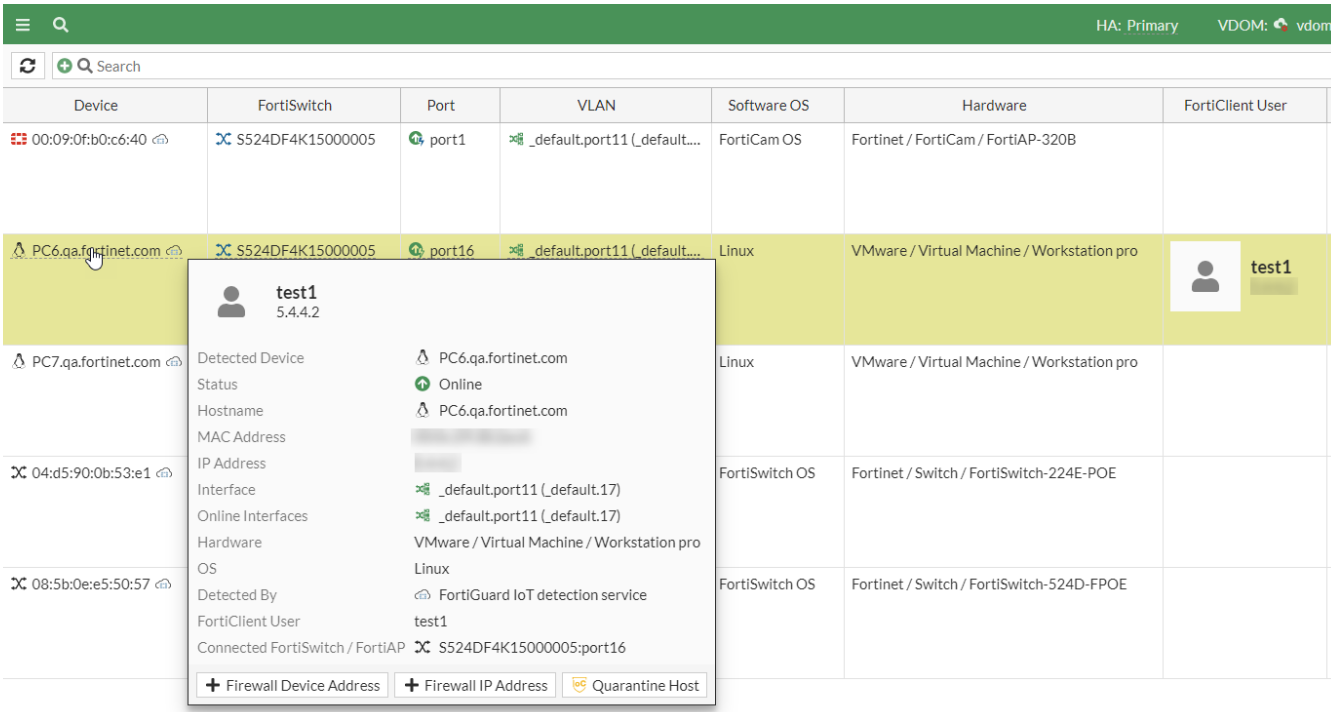
FortiSwitch	Port	Policy	Assigned VLAN

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.



Device	FortiSwitch	Port	VLAN	Software OS	Hardware	FortiClient User
00:09:0f:b0:c6:40	S524DF4K15000005	port1	_default.port11 (_default....	FortiCam OS	Fortinet / FortiCam / FortiAP-320B	
PC6.qa.fortinet.com	S524DF4K15000005	port16	_default.port11 (_default....	Linux	VMware / Virtual Machine / Workstation pro	test1
PC7.qa.fortinet.com				Linux	VMware / Virtual Machine / Workstation pro	
04:d5:90:0b:53:e1				FortiSwitch OS	Fortinet / Switch / FortiSwitch-224E-POE	
08:5b:0e:e5:50:57				FortiSwitch OS	Fortinet / Switch / FortiSwitch-524D-FPOE	

test1
5.4.4.2

Detected Device	PC6.qa.fortinet.com
Status	Online
Hostname	PC6.qa.fortinet.com
MAC Address	[redacted]
IP Address	[redacted]
Interface	_default.port11 (_default.17)
Online Interfaces	_default.port11 (_default.17)
Hardware	VMware / Virtual Machine / Workstation pro
OS	Linux
Detected By	FortiGuard IoT detection service
FortiClient User	test1
Connected FortiSwitch / FortiAP	S524DF4K15000005:port16

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:

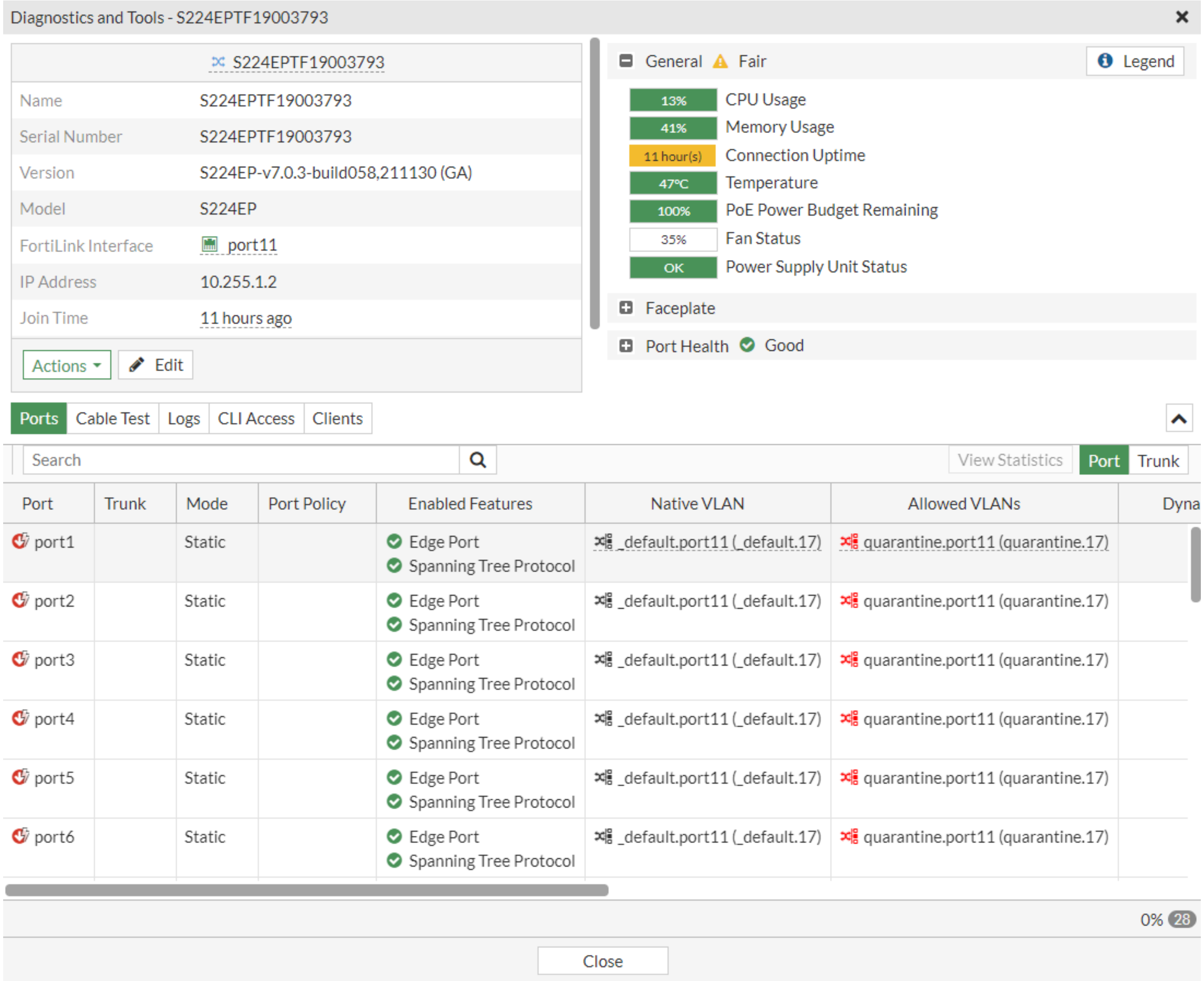
1. Click *Firewall IP Address*.
2. In the *Name* field, enter a name for the firewall IP address.
3. Click *Change* if you want a different color for the icon on the GUI.
4. In the *IP/Netmask* field, change the value as needed.
5. From the *Interface* dropdown list, select an interface.
6. Enable or 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.



Diagnostics and Tools - S224EPTF19003793

	S224EPTF19003793
Name	S224EPTF19003793
Serial Number	S224EPTF19003793
Version	S224EP-v7.0.3-build058,211130 (GA)
Model	S224EP
FortiLink Interface	port11
IP Address	10.255.1.2
Join Time	11 hours ago

General Fair

13%	CPU Usage
41%	Memory Usage
11 hour(s)	Connection Uptime
47°C	Temperature
100%	PoE Power Budget Remaining
35%	Fan Status
OK	Power Supply Unit Status

Faceplate

Port Health Good

Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	Dyna
port1		Static		✓ Edge Port ✓ Spanning Tree Protocol	_default.port11 (_default.17)	quarantine.port11 (quarantine.17)	
port2		Static		✓ Edge Port ✓ Spanning Tree Protocol	_default.port11 (_default.17)	quarantine.port11 (quarantine.17)	
port3		Static		✓ Edge Port ✓ Spanning Tree Protocol	_default.port11 (_default.17)	quarantine.port11 (quarantine.17)	
port4		Static		✓ Edge Port ✓ Spanning Tree Protocol	_default.port11 (_default.17)	quarantine.port11 (quarantine.17)	
port5		Static		✓ Edge Port ✓ Spanning Tree Protocol	_default.port11 (_default.17)	quarantine.port11 (quarantine.17)	
port6		Static		✓ Edge Port ✓ Spanning Tree Protocol	_default.port11 (_default.17)	quarantine.port11 (quarantine.17)	

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 327.
- 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 327.
- 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*.

For the 5xx switches, LED Blink flashes only the SFP port LEDs, instead of all the port LEDs.

Running the cable test

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-124E, 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.

Checking the system and fan status

Starting in FortiOS 7.6.3, there are CLI commands to check the system status and the fan status.

To check the system status:

```
diagnose switch-controller switch-info status
```

For example:

```
diagnose switch-controller switch-info status
Vdom: root
Managed Switch : FS2F48TV23000017     0
Version: FortiSwitch-2048F v7.6.2,build1066,250212 (Interim)
Model Variant: FortiSwitch-2048F-F2B
Airflow: Front to Back(F2B)
Serial-Number: FS2F48TV23000017
Firmware Signature: invalid
Boot: Warmboot
BIOS version: 04000006
System Part-Number: P28505-01
Burn in MAC: 84:39:8f:ba:55:44
Hostname: FS2F48TV23000017
Security mode: none
Security level: low
Distribution: International
Branch point: 1066
FortiSwitch x86-64: Yes
System time: Tue Mar  4 13:44:09 2025
Private Data Encryption : Disabled

Managed Switch : FS1D483Z14000068     0
Version: FortiSwitch-1048D v7.0.11,build0137,241121 (GA)
Serial-Number: FS1D483Z14000068
Boot: Coldboot
BIOS version: 04000013
System Part-Number: P15415-02
Burn in MAC: 08:5b:0e:5b:84:fa
Hostname: FS1D483Z14000068
Distribution: International (r)
Branch point: 137
```

```
System time: Tue Mar  4 13:44:10 2025

Managed Switch : FS2F48TV23000021     0
```

To check the fan status:

`diagnose switch-controller switch-info fan [<FortiSwitch_serial_number>]`

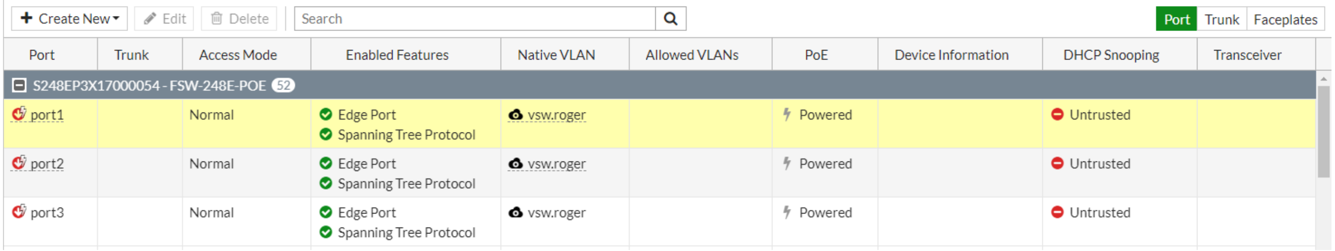
For example:

```
diagnose switch-controller switch-info fan
Vdom: root
Managed Switch : FS2F48TV23000017     0

Airflow: Front to Back(F2B)

Module          Status
___________________________________

FAN1-1          Good(40.4 %)
FAN1-2          Good(42.6 %)
FAN2-1          Good(40.0 %)
FAN2-2          Good(42.1 %)
FAN3-1          Good(40.4 %)
FAN3-2          Good(42.1 %)
FAN4-1          Good(40.0 %)
FAN4-2          Good(43.6 %)
FAN5-1          Good(40.0 %)
FAN5-2          Good(42.6 %)
FAN6-1          Good(41.3 %)
FAN6-2          Good(43.6 %)

Managed Switch : FS1D483Z14000068     0

Module          Status
___________________________________
FAN0            Tray0 OK (Insert)(62.1 %)
FAN1            Tray0 OK (Insert)(62.1 %)
FAN0            Tray1 OK (Insert)(62.1 %)
FAN1            Tray1 OK (Insert)(62.1 %)

Managed Switch : FS2F48TV23000021     0
```

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:



Port	Trunk	Access Mode	Enabled Features	Native VLAN	Allowed VLANs	PoE	Device Information	DHCP Snooping	Transceiver
S248EP3X17000054 - FSW-248E-POE 52									
port1		Normal	✓ Edge Port ✓ Spanning Tree Protocol	vsw.roger		Powered		Untrusted	
port2		Normal	✓ Edge Port ✓ Spanning Tree Protocol	vsw.roger		Powered		Untrusted	
port3		Normal	✓ Edge Port ✓ Spanning Tree Protocol	vsw.roger		Powered		Untrusted	

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:

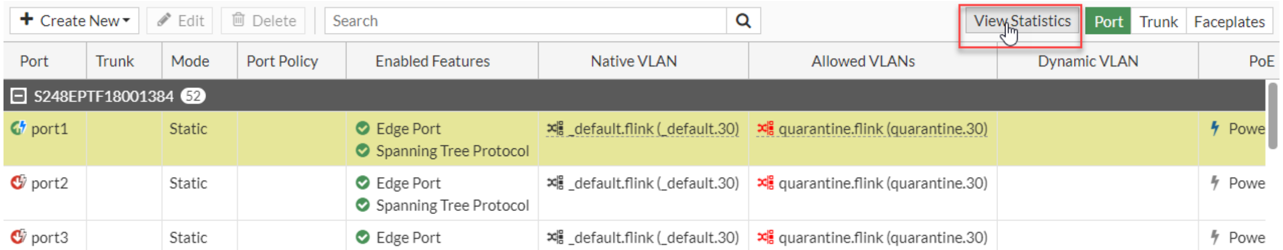
```
diagnose switch-controller mac-cache show <switch-id>
```

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.

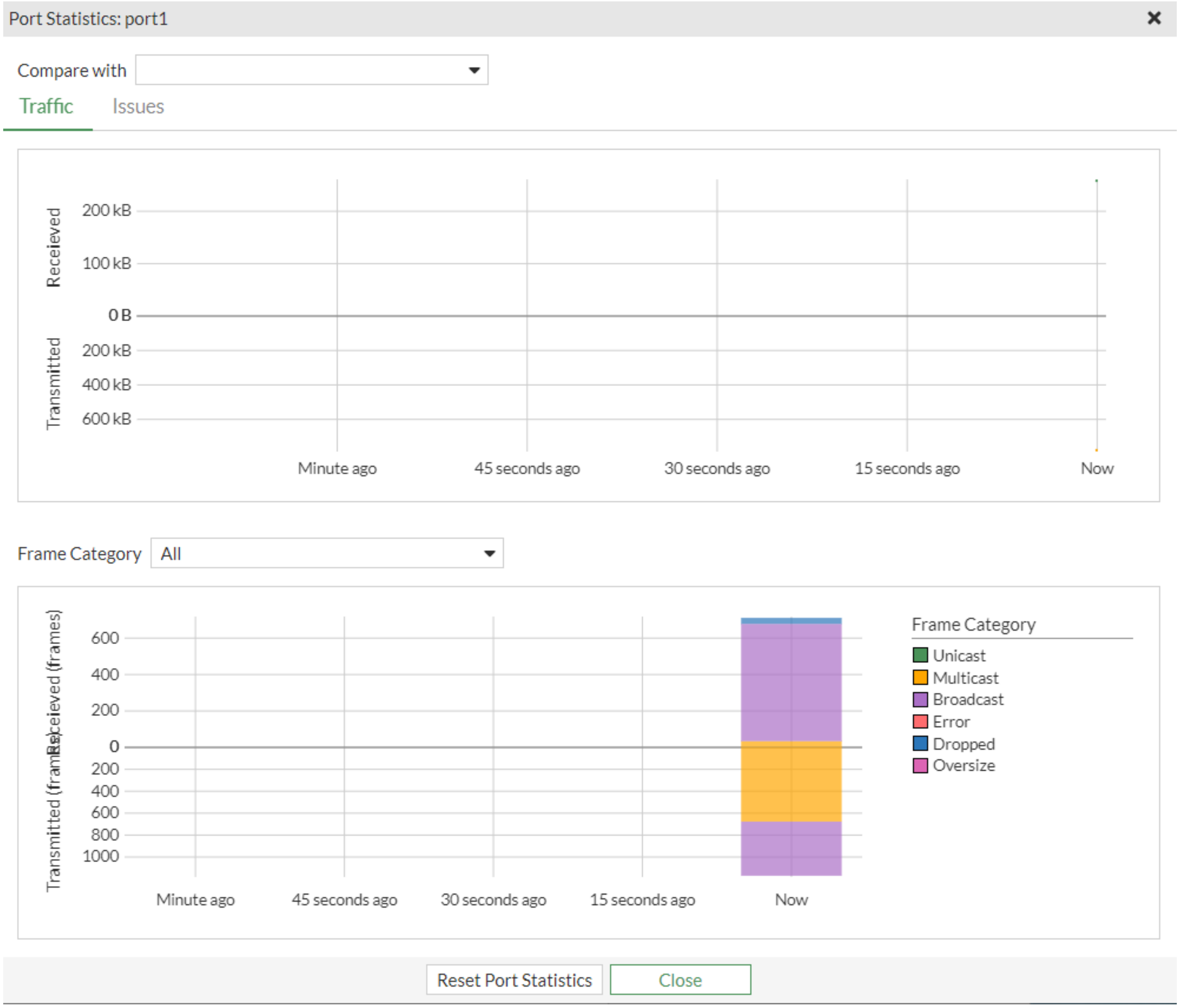
To display port statistics using the GUI:

1. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
2. Select a port.
3. Click *View Statistics*.



Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	Dynamic VLAN	PoE
S248EPTF18001384 52								
port1		Static		Edge Port Spanning Tree Protocol	_default.flink (_default.30)	quarantine.flink (quarantine.30)		Powe
port2		Static		Edge Port Spanning Tree Protocol	_default.flink (_default.30)	quarantine.flink (quarantine.30)		Powe
port3		Static		Edge Port	_default.flink (_default.30)	quarantine.flink (quarantine.30)		Powe

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>
```

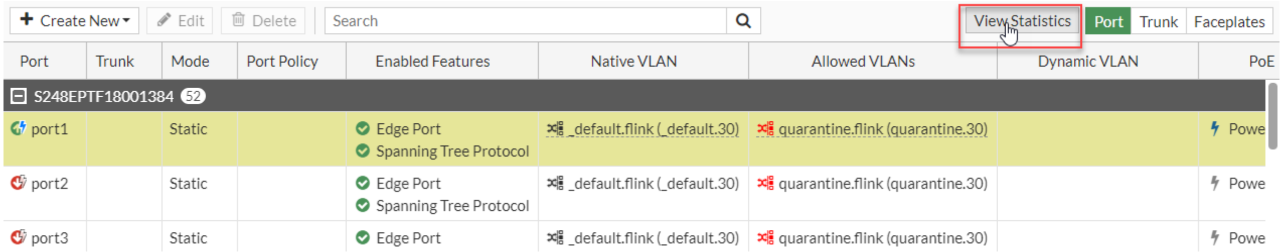
For example:

```
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
```

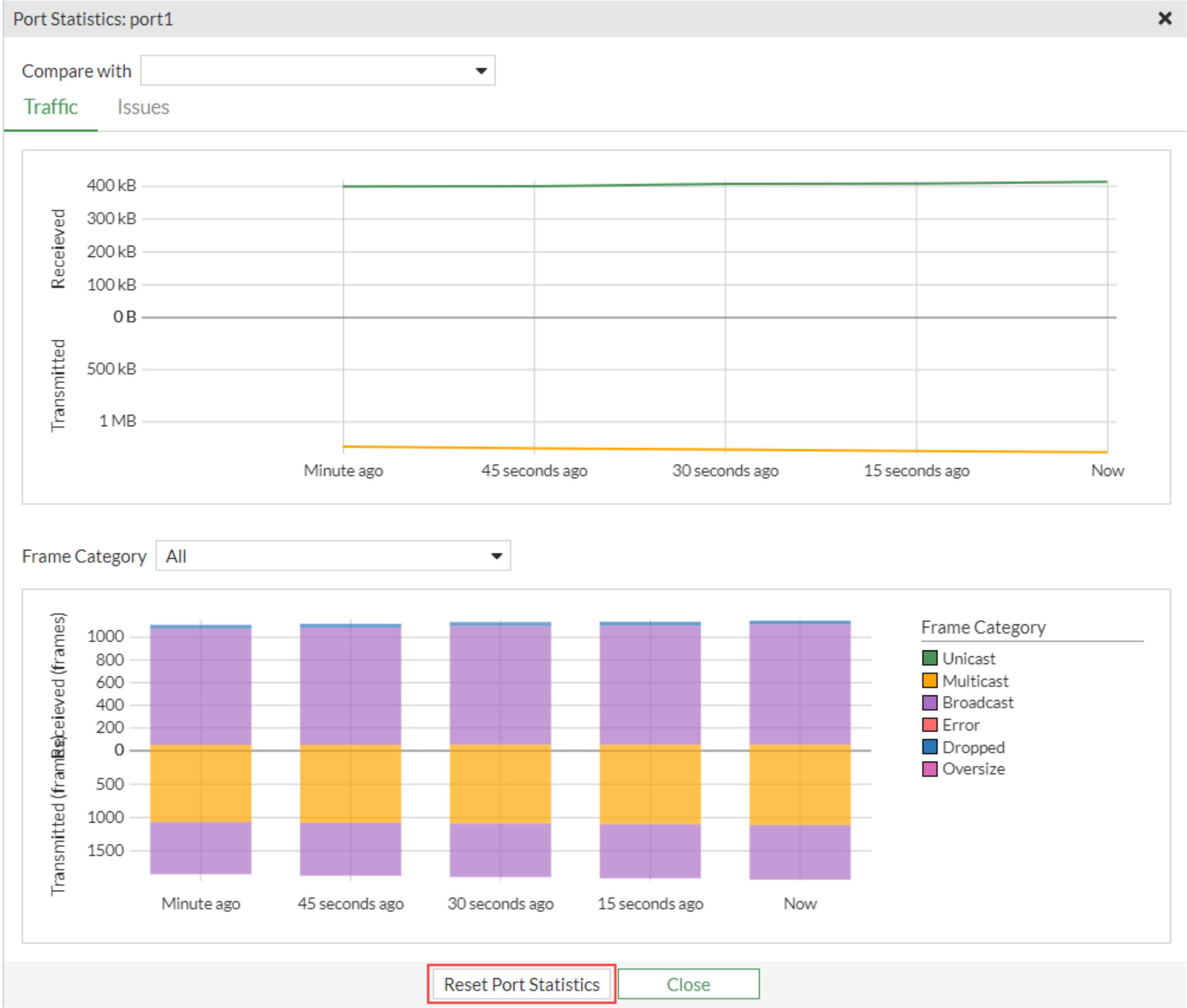
To reset the port statistics counters using the GUI:

1. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
2. Select a port.
3. Click *View Statistics*.



Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	Dynamic VLAN	PoE
S248EPTF18001384 52								
port1		Static		✓ Edge Port ✓ Spanning Tree Protocol	_default.flink (_default.30)	quarantine.flink (quarantine.30)		Powe
port2		Static		✓ Edge Port ✓ Spanning Tree Protocol	_default.flink (_default.30)	quarantine.flink (quarantine.30)		Powe
port3		Static		✓ Edge Port	_default.flink (_default.30)	quarantine.flink (quarantine.30)		Powe

4. Click *Reset Port Statistics*.



Port Statistics: port1

Compare with

Frame Category: All

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:

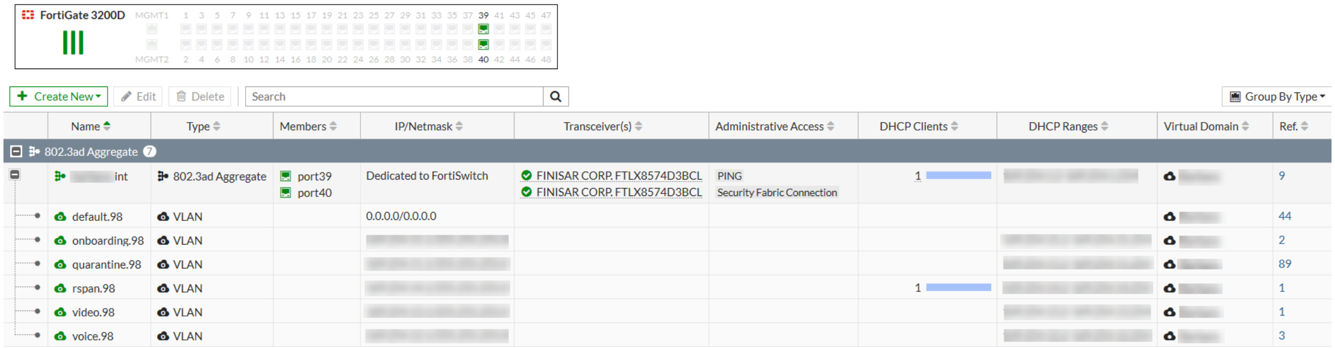
```
execute switch-controller dsl reset <FortiSwitch_serial_number> <port_name>
```

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.

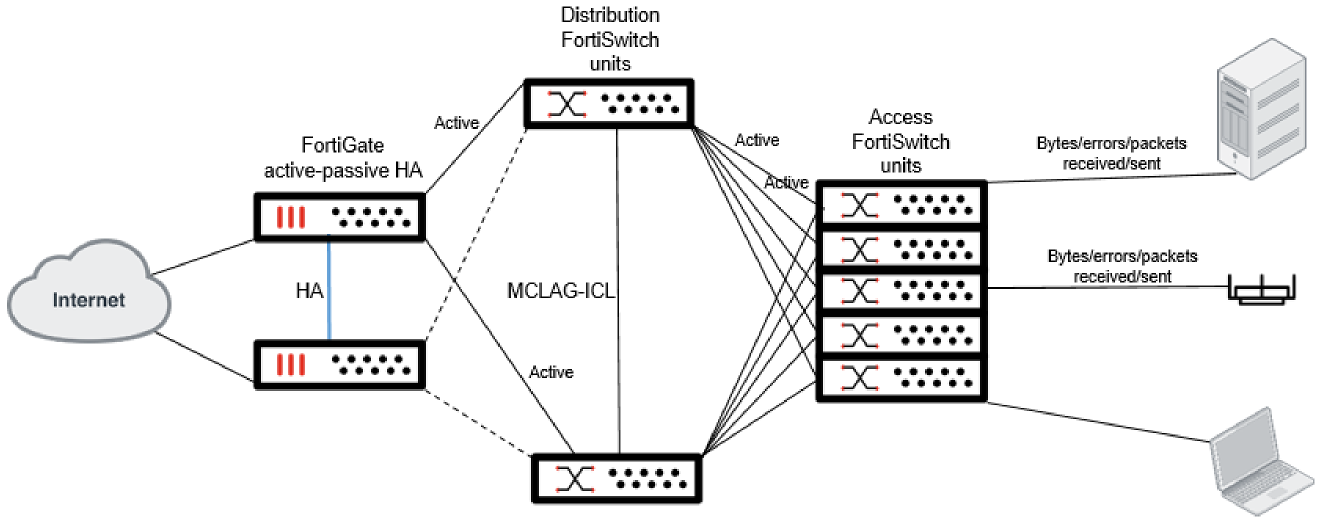


Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges	Virtual Domain	Ref.
802.3ad Aggregate 7									
[redacted]int	802.3ad Aggregate	port39 port40	Dedicated to FortiSwitch	✓ FINISAR CORP. FTLX8574D3BCL ✓ FINISAR CORP. FTLX8574D3BCL	PING Security Fabric Connection	1	[redacted]	[redacted]	9
default.98	VLAN		0.0.0.0/0.0.0.0					[redacted]	44
onboarding.98	VLAN		[redacted]				[redacted]	[redacted]	2
quarantine.98	VLAN		[redacted]				[redacted]	[redacted]	89
rspan.98	VLAN		[redacted]			1	[redacted]	[redacted]	1
video.98	VLAN		[redacted]				[redacted]	[redacted]	1
voice.98	VLAN		[redacted]				[redacted]	[redacted]	3

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


Distribution FortiSwitch units
Active
FortiGate active-passive HA
Active
Access FortiSwitch units
Active
Bytes/errors/packets received/sent
Bytes/errors/packets received/sent
Internet
HA
MCLAG-ICL
Active

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.

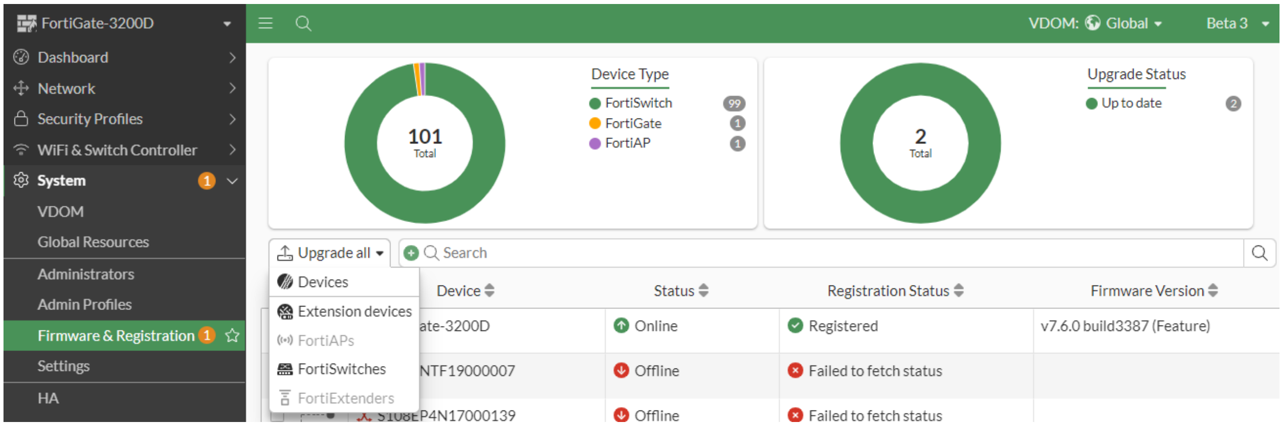
Using the FortiGate GUI

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 all FortiSwitch units at the same time:

1. Go to *System* > *Firmware & Registration*.
2. Click *Upgrade all* > *FortiSwitches*.



Device	Status	Registration Status	Firmware Version
ate-3200D	Online	Registered	v7.6.0 build3387 (Feature)
NTF19000007	Offline	Failed to fetch status	
S108EP4N17000139	Offline	Failed to fetch status	

3. Select *Recommended* if you want to upgrade using FortiGuard or *File Upload* to use a downloaded firmware file.
4. Complete the steps as needed.
   You can monitor the upgrade progress using the tray on the bottom-right corner of the GUI.

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

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

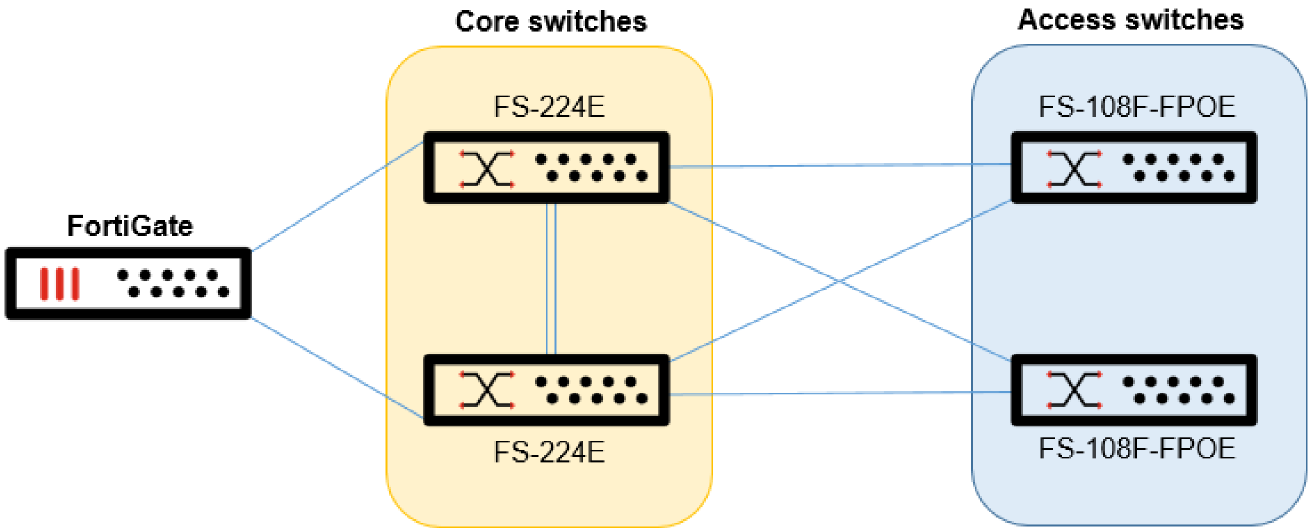
From your FortiGate CLI, you can upgrade the firmware of all of the managed FortiSwitch units of the same model using a single `execute` command. The command includes the name of a firmware image file and all of the managed FortiSwitch units compatible with that firmware image file are upgraded. For 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-108F-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
S108FF5918003577   v6.2.1 (176)      Authorized/Up   -    10.105.22.6     Thu Oct 24 10:47:27
2019    -
S108FP5918008265   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_108F_POE-v6-
build0194-FORTINET.out 10.105.16.15

Downloading file FSW_108F_POE-v6-build0194-FORTINET.out from tftp server 10.105.16.15...
##################
Image checking ...
Image MD5 calculating ...
Image Saving S108FP-IMG.swtp ...
Successful!

File Syncing...

FGT81ETK19001274 # execute switch-controller switch-software upload tftp FSW_108F_FPOE-v6-
build0194-FORTINET.out 10.105.16.15

Downloading file FSW_108F_FPOE-v6-build0194-FORTINET.out from tftp server 10.105.16.15...
##################
Image checking ...
Image MD5 calculating ...
Image Saving S108FF-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
S108FF-IMG.swtp        19574769       S108FF-v6.2-build194     Thu Oct 24 13:03:51 2019
S108FP-IMG.swtp        19583362       S108FP-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 S108FF-IMG.swtp
Staged Image Version S108FF-v6.2-build194
Image staging operation is started for FortiSwitch S108FF5918003577 ...

FGT81ETK19001274 # execute switch-controller switch-software stage all S108FP-IMG.swtp
Staged Image Version S108FP-v6.2-build194
Image staging operation is started for FortiSwitch S108FP5918008265 ...
```

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)
S108FP5918008265  S108FP-v6.2.1-build176,190620 (GA)             (18/0/0)   S108FP-v6.2-
build176        (Staging)
S108FF5918003577  S108FF-v6.2.1-build176,190620 (GA)             (25/0/0)   S108FF-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)
S108FP5918008265  S108FP-v6.2.1-build176,190620 (GA)             (0/100/100)   S108FP-v6.2-
build194     (Idle)
S108FF5918003577  S108FF-v6.2.1-build176,190620 (GA)             (0/100/100)   S108FF-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 S108FP5918008265 ...
Delayed restart operation is requested for FortiSwitch S108FF5918003577 ...
```

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 S108FP5918008265 ...
Delayed restart operation is requested for FortiSwitch S108FF5918003577 ...

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
S108FP5918008265                        Prepping for delayed restart triggered ... please wait
for switch to reboot in a moment
S108FF5918003577                        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
S108FF5918003577  v6.2.1 ()         Authorized/Down D   0.0.0.0         N/A               -
S108FP5918008265  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-
```

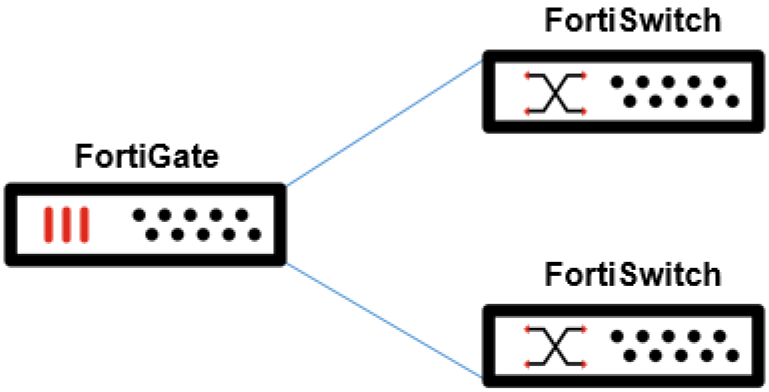
```
build194     (Idle)
S224ENTF18001432  S224EN-v6.2.2-build194,191018 (GA)             (0/100/100)   S224EN-v6.2-
build194     (Idle)
S108FP5918008265  S108FP-v6.2.2-build194,191018 (GA)             (0/100/100)   S108FP-v6.2-
build194     (Idle)
S108FF5918003577  S108FF-v6.2.2-build194,191018 (GA)             (0/100/100)   S108FF-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
S108FF5918003577  v6.2.2 (194)      Authorized/Up   -   10.105.22.6     Thu Oct 24 13:22:27
2019    -
S108FP5918008265  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
```

Configuring automatic federated firmware updates

When the automatic firmware updates setting is enabled, in addition to an automatic federated upgrade being performed on the FortiGate device, automatic federated upgrades are now performed on managed FortiSwitch units, starting in FortiOS 7.4.1. The federated upgrades of these LAN edge devices adhere to the FortiOS-FortiSwitch compatibility matrix information maintained on the FortiGuard Distribution Network (FDN).

Configuration example



In this example, automatic firmware updates are enabled on a FortiGate device that is running FortiOS 7.4.1. Two FortiSwitch units with older firmware are upgraded after the federated update.

To configure automatic federated firmware updates:

```
config system fortiguard
       set auto-firmware-upgrade enable
       set auto-firmware-upgrade-day tuesday
       set auto-firmware-upgrade-delay 0
       set auto-firmware-upgrade-start-hour 11
       set auto-firmware-upgrade-end-hour 12
end
```

The auto-upgrade time is scheduled on Tuesday, between 11:00 a.m. and 12:00 p.m.

You can also use the `execute federated-upgrade` commands:

Option	Description
cancel	Cancel the current federated upgrade.
initialize	Set up a federated upgrade.
quick-fortigate-upgrade	Set up a federated upgrade for all FortiGate devices.
quick-full-upgrade	Set up a federated upgrade for all devices.
restart	Restart the current federated upgrade.
status	Display the status of the current federated upgrade.

To verify that the federated update occurs:

1. Verify that the update is scheduled:

```
FGT_A (global) # diagnose test application forticldd 13
Scheduled push image upgrade: no
Scheduled Config Restore: no
Scheduled Script Restore: no
Automatic image upgrade: Enabled.
       Next upgrade check scheduled at (local time) Tue Sep  5 11:06:58 2023
```

2. Verify if there are managed FortiSwitch that can be upgraded:

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

FortiLink interface : flink
SWITCH-ID         VERSION           STATUS         FLAG   ADDRESS              JOIN-TIME
     SERIAL
FS1D243Z17000032  v7.2.5 (453)      Authorized/Up   2   169.254.1.4     Tue Sep  5 10:16:26
2023    FS1D243Z17000032
S548DF4K16000730  v7.0.7 (096)      Authorized/Up   2   169.254.1.5     Tue Sep  5 10:16:51
2023    S548DF4K16000730

       Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=config sync error,
3=L3, V=VXLAN
       Managed-Switches: 2 (UP: 2 DOWN: 0 MAX: 72)
```

3. Verify the compatibility matrix:

```
FGT_A (global) # diagnose test application forticldd 16
Last update: 3 secs ago

FS1D24: 7.4.0 b767 07004000FIMG0900304000 (FGT Version 7.4.1 b0)
```

4. Wait for the FortiGate device to perform the federated update.
5. After the federated update is complete, verify that the managed FortiSwitch units were upgraded to the latest version:

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

FortiLink interface : flink
SWITCH-ID         VERSION           STATUS         FLAG   ADDRESS              JOIN-TIME
     SERIAL
FS1D243Z17000032  v7.4.0 (767)      Authorized/Up   2   169.254.1.2     Tue Sep  5 11:22:44
2023    FS1D243Z17000032
S548DF4K16000730  v7.4.0 (767)      Authorized/Up   2   169.254.1.5     Tue Sep  5 11:23:37
2023    S548DF4K16000730

       Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=config sync error,
3=L3, V=VXLAN
       Managed-Switches: 2 (UP: 2 DOWN: 0 MAX: 72)
```

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:

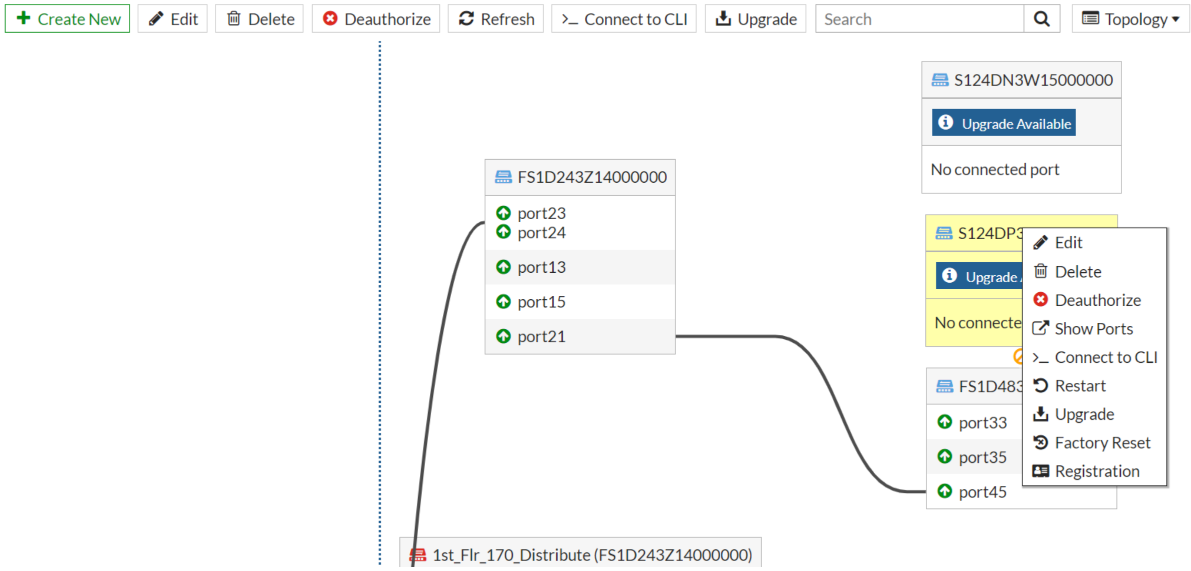
```
config switch-controller switch-profile
   edit {default | FortiSwitch_profile_name}
      set revision-backup-on-upgrade enable
   next
end
```

Registering FortiSwitch to FortiCloud

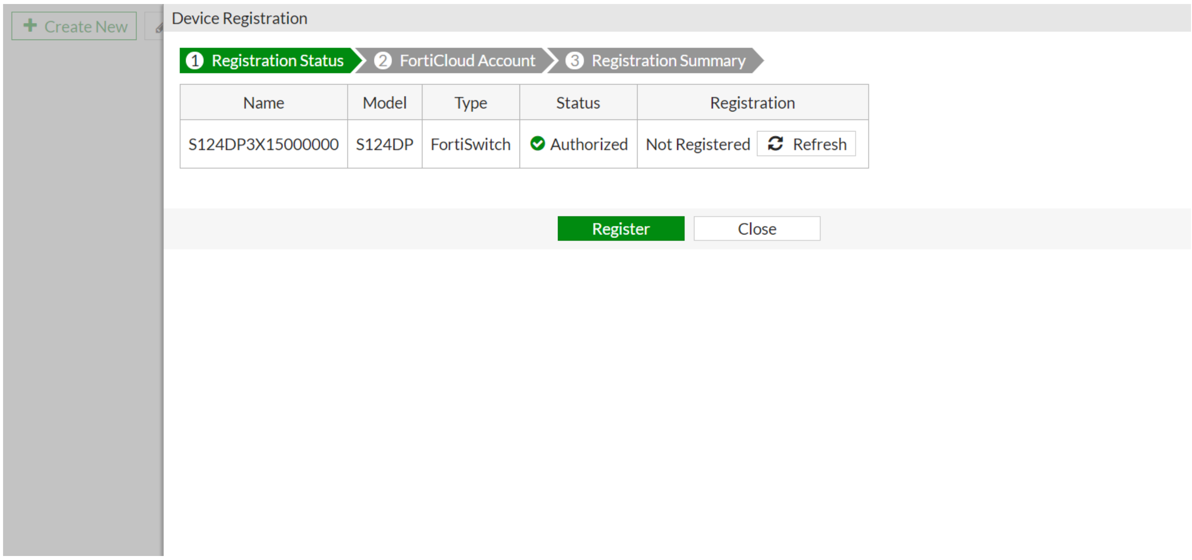
After authorizing a FortiSwitch, administrators can register the FortiSwitch to FortiCloud directly from the FortiOS GUI.

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*.

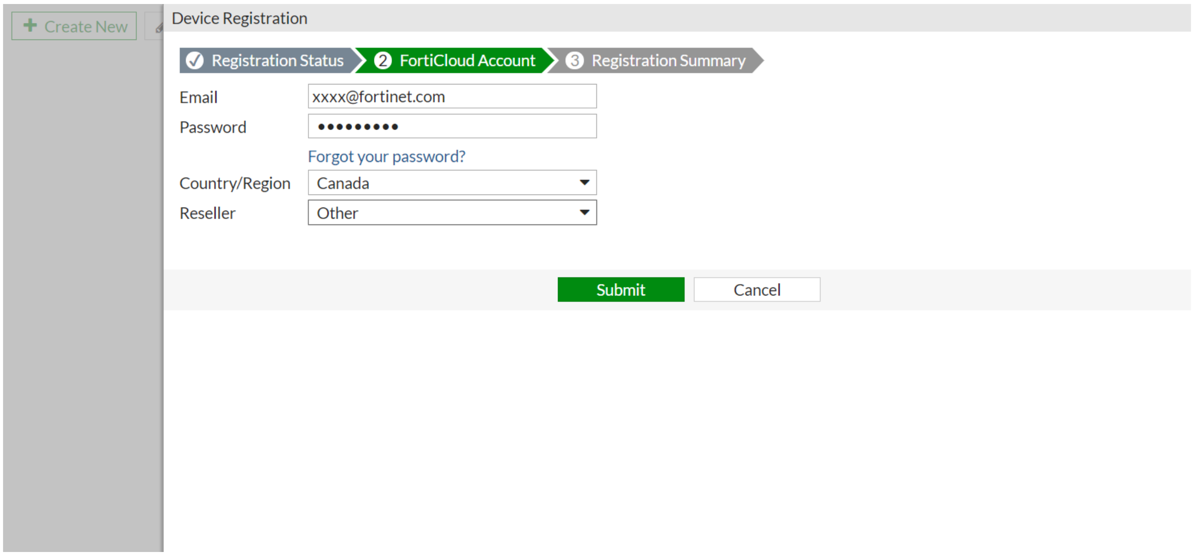


3. Complete the device registration wizard:
   a. Click *Register* to proceed.



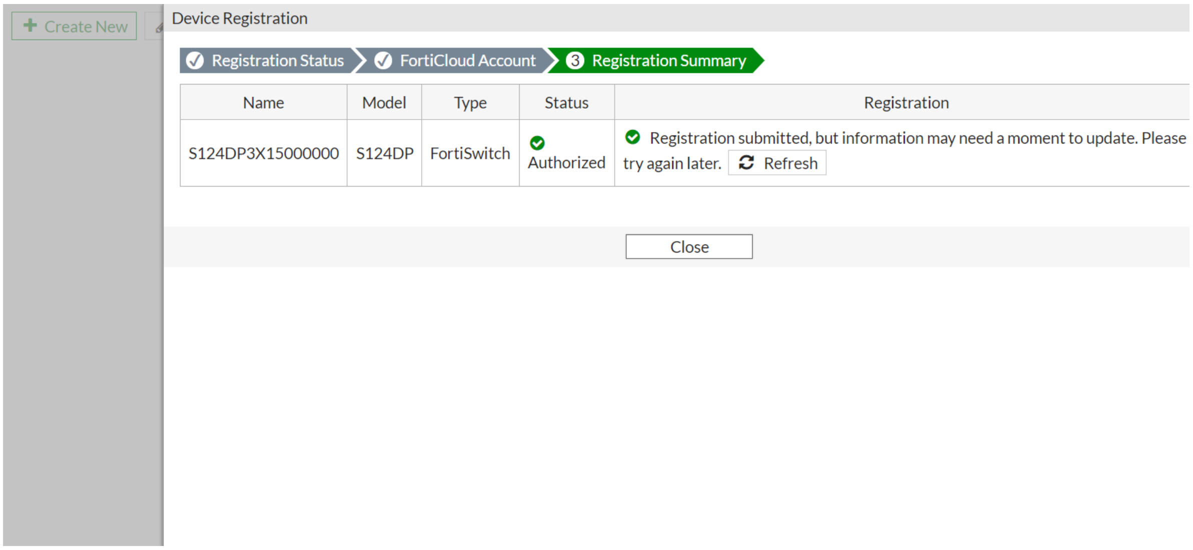
Name	Model	Type	Status	Registration
S124DP3X15000000	S124DP	FortiSwitch	✓ Authorized	Not Registered Refresh

b. Enter the FortiCloud account information and click *Submit*.



Email	xxxx@fortinet.com
Password	•••••••••
	Forgot your password?
Country/Region	Canada
Reseller	Other

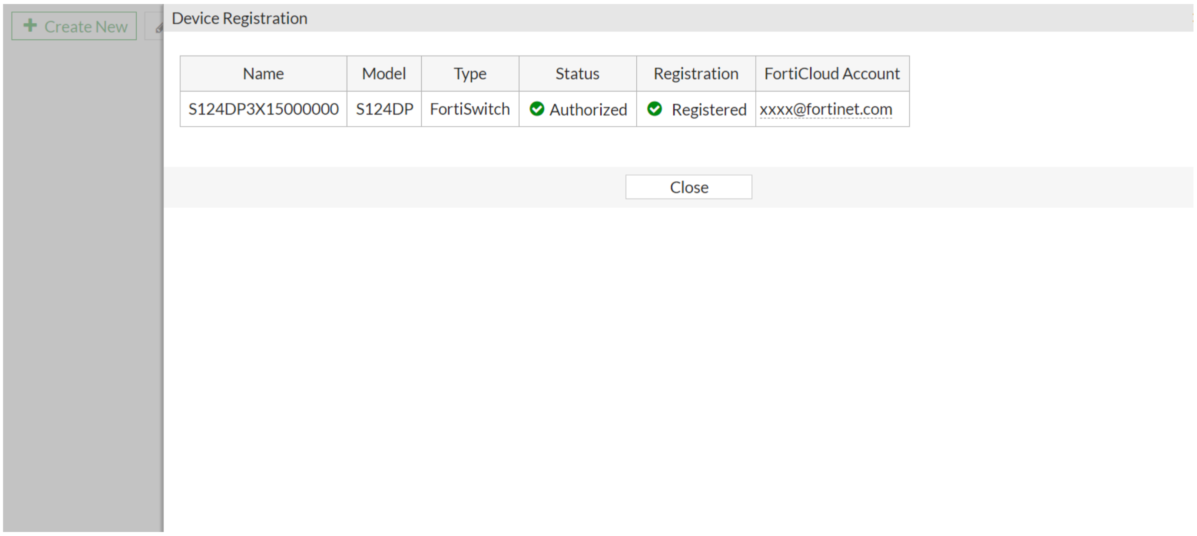
The registration information is submitted to FortiCare, and FortiOS attempts to collect the registration status from FortiGuard. Since FortiGuard and FortiCare synchronize periodically, the registration status may not update immediately (it may take up to a few hours).



Name	Model	Type	Status	Registration
S124DP3X15000000	S124DP	FortiSwitch	✓ Authorized	✓ Registration submitted, but information may need a moment to update. Please try again later. Refresh

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.



Device Registration

Name	Model	Type	Status	Registration	FortiCloud Account
S124DP3X15000000	S124DP	FortiSwitch	✓ Authorized	✓ Registered	xxxx@fortinet.com

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.
- 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.

To replace a managed FortiSwitch unit when split ports are not enabled:

1. Remove the failed FortiSwitch unit from the network.
2. Deauthorize the failed switch:
```
config switch-controller managed-switch
   edit <failed_FortiSwitch_serial_number>
      set fsw-wan1-admin disable
   end
```
3. If the replacement switch is not new, reset the replacement FortiSwitch unit to factory default settings with the `execute factoryreset` command.
4. Without connecting to the existing network, 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 339.
5. On the FortiGate device, use the `execute replace-device fortiswitch <failed_FortiSwitch_serial_number> <replacement_FortiSwitch_serial_number>` command to change the replacement switch name to match the failed switch name.
6. Authorize the replacement switch:
```
config switch-controller managed-switch
   edit <replacement_FortiSwitch_serial_number>
      set fsw-wan1-admin enable
   end
```
7. Connect the replacement switch to the network.

To replace a managed FortiSwitch unit when split ports are enabled:

1. Remove the failed FortiSwitch unit from the network.
2. Deauthorize the failed switch:
```
config switch-controller managed-switch
   edit <failed_FortiSwitch_serial_number>
      set fsw-wan1-admin disable
   end
```
3. If the replacement switch is not new, reset the replacement FortiSwitch unit to factory default settings with the `execute factoryreset` command.
4. Without connecting to the existing network, 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 339.
5. Log in to the replacement switch and use the `config switch phy-mode` commands to configure the split ports with the same configuration that was on the failed switch.
6. On the FortiGate device, use the `execute replace-device fortiswitch <failed_FortiSwitch_serial_number> <replacement_FortiSwitch_serial_number>` command to change the replacement switch name to match the failed switch name.
7. Authorize the replacement switch:
```
config switch-controller managed-switch
   edit <replacement_FortiSwitch_serial_number>
      set fsw-wan1-admin enable
   end
```

8. Connect the replacement switch to the network.

To replace a managed FortiSwitch unit of an MCLAG pair:

1. Remove the failed FortiSwitch unit from the network.
2. Deauthorize the failed switch:
   ```
   config switch-controller managed-switch
      edit <failed_FortiSwitch_serial_number>
         set fsw-wan1-admin disable
      end
   ```
3. If the replacement switch is not new, reset the replacement FortiSwitch unit to factory default settings with the `execute factoryreset` command.
4. Without connecting to the existing network, 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 339.
5. On the FortiGate device, use the `execute replace-device fortiswitch <failed_FortiSwitch_serial_number> <replacement_FortiSwitch_serial_number>` command to change the replacement switch name to match the failed switch name.
6. Authorize the replacement switch:
   ```
   config switch-controller managed-switch
      edit <replacement_FortiSwitch_serial_number>
         set fsw-wan1-admin enable
      end
   ```
7. Connect the ICL physical port(s) of the replacement MCLAG switch to the peer switch's ICL ports. An ISL trunk with the peer's name is formed on the replacement switch. Wait until the replacement switch's FortiLink is up.
   - On the FortiGate device, if the failed switch had `set lldp-profile default-auto-mclag-icl` configured in the ICL ports of the switch, the replaced switch will not have these settings configured to begin with. Use the console or SSH to the replacement switch and manually configure `set mclag-icl enable` in the ISL trunk with the peer switch's name. Then wait for the replaced switch to form FortiLink with the FortiGate device, and all configurations, including `set lldp-profile default-auto-mclag-icl`, are pushed to the replacement switch. After this is done, from the console or SSH to the replaced switch, delete the automatically formed ICL trunk, which then triggers the automatic formation of the FlInK1_ICL0_ trunk.
   - On the FortiGate device, if the failed switch did not have "`set lldp-profile default-auto-mclag-icl`" configured in the ICL ports of the switch, the replacement switch will not have the setting as well. SSH to the replacement switch, manually configure "`set mclag-icl enable`" in the ISL trunk with the peer switch's name. Then wait for the replaced switch to form FortiLink with the FortiGate device, and all configurations are pushed to the replacement switch. After this is done, SSH to the peer switch to delete the ICL trunk (with the failed switch's name) and configure "`set mclag-icl enable`" after a new ISL trunk with the replacement switch's name forms automatically.
8. Use the `diagnose switch mclag icl` command to make sure that there are no errors and that the ICL trunk is up.
9. Check the neighbor peer switch to see if it has `auto-isl-port-group` configured. If it does, you need to configure the replacement switch with the same `auto-isl-port-group` name.
10. Connect the rest of the ports to the replacement switch.
11. Execute the `diagnose switch mlcag peer-consistency-check` command to make sure there are no MCLAG or ICL errors.

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 on page 358
- Executing a custom script once on page 358
- Binding a custom script to a managed switch on page 358

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.

Appendix A: Configuring the Media Redundancy Protocol

A ring of Ethernet switches can use the Media Redundancy Protocol (MRP) to overcome a failure faster than with STP. An MRP network consists of a ring of switches with one manager switch; the rest of the switches are clients. The switches in the ring must use physical ports to form the ring or a single port configured as a static trunk. The MRP ring ports are disabled in STP.

If a ring has more than one switch that can be manager, MRP selects the switch with the highest priority (numerically lower number) as the manager. If a ring has more than one switch that can be manager and the switches have the same priority, MRP selects the switch with the lowest MAC address as the manager. Each node of the MRP network must be configured as an automanager (manager switch) or a client. The MRP automanager and client switches must have matching parameters, such as MRP VLAN and domain identifier, for the MRP ring to function properly.

MRP sends three types of frames through the ring ports:

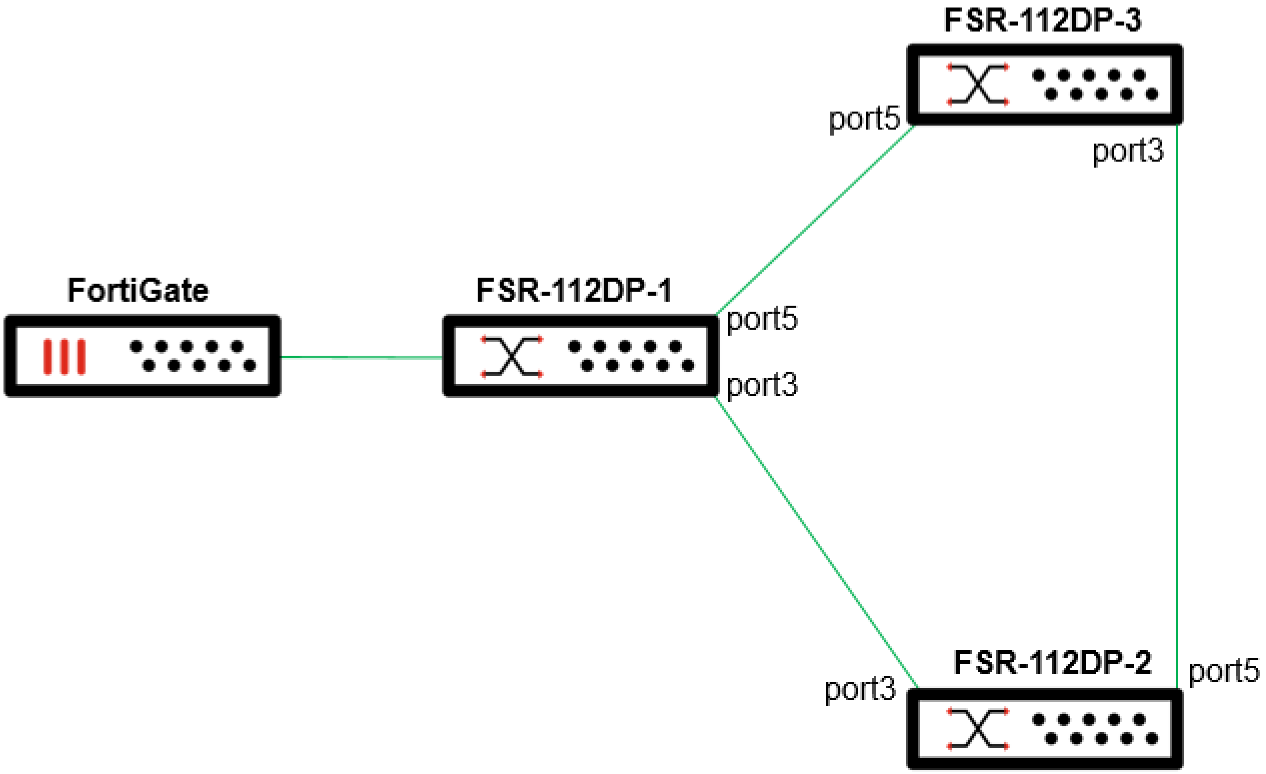
- MRP_Test frames detect a failure or recovery of a ring port link.
- MRP_LinkChange frames indicate a failure or recovery of a ring port link.
- MRP_TopologyChange frames indicate that the MRP network topology has changed.

Starting in FortiSwitchOS 7.6.0, the FortiSwitch unit supports the following:

- Two MRP rings
- Ring-check mode
- The media redundancy interconnection manager (MIM) is not supported.
- The media redundancy interconnection client (MIC) is not supported.
- Fortinet recommends configuring no more than two automanagers in a ring.

Refer to the FortiSwitchOS feature matrix to see which FortiSwitch models support MRP.

To configure MRP in FortiLink mode:



NOTE: The FortiSwitch units must be first configured in standalone mode without being connected to any FortiGate devices.

1. Enable auto-network using a management VLAN of 4094.

   By default, auto-network is enabled in FortiSwitchOS 7.2.0 and later.

   For example:

   ```
   config switch auto-network
      set mgmt-vlan 4094
   end
   ```

2. Let the ISL trunks automatically form between the FortiSwitch units. For example:

   ```
   config switch trunk
      edit "2DP4F16000319-0"
         set auto-isl 1
         set static-isl disable
         set members "port3"
      next
      edit "2DP4F14000094-0"
         set auto-isl 1
         set static-isl disable
         set members "port5"
      next
   end
   ```

3. Change the ISL trunks to `static-isl` trunks. For example:

   ```
   config switch trunk
      edit "2DP4F16000319-0"
         set auto-isl 1
   ```

```
      set static-isl enable
      set members "port3"
   next
   edit "2DP4F14000094-0"
      set auto-isl 1
      set static-isl enable
      set members "port5"
   next
end
```

4. Configure the MRP settings with VLAN 4094. Use the physical ports of the `static-isl` trunk members as MRP ring ports. For example:

```
config switch mrp settings
   set status enable
   set vlan-id 4094
   set ring-port1 "port3"
   set ring-port2 "port5"
end
```

5. Connect the link to the FortiGate device and authorize the FortiSwitch units.

Appendix B: Configuring HSR and PRP with FortiLink

Starting in FortiSwitchOS 7.2.4, High-Availability Seamless Redundancy (HSR) and Parallel Redundancy Protocol (PRP) are supported.

Refer to the FortiSwitchOS feature matrix to see which FortiSwitch models support HSR and PRP.

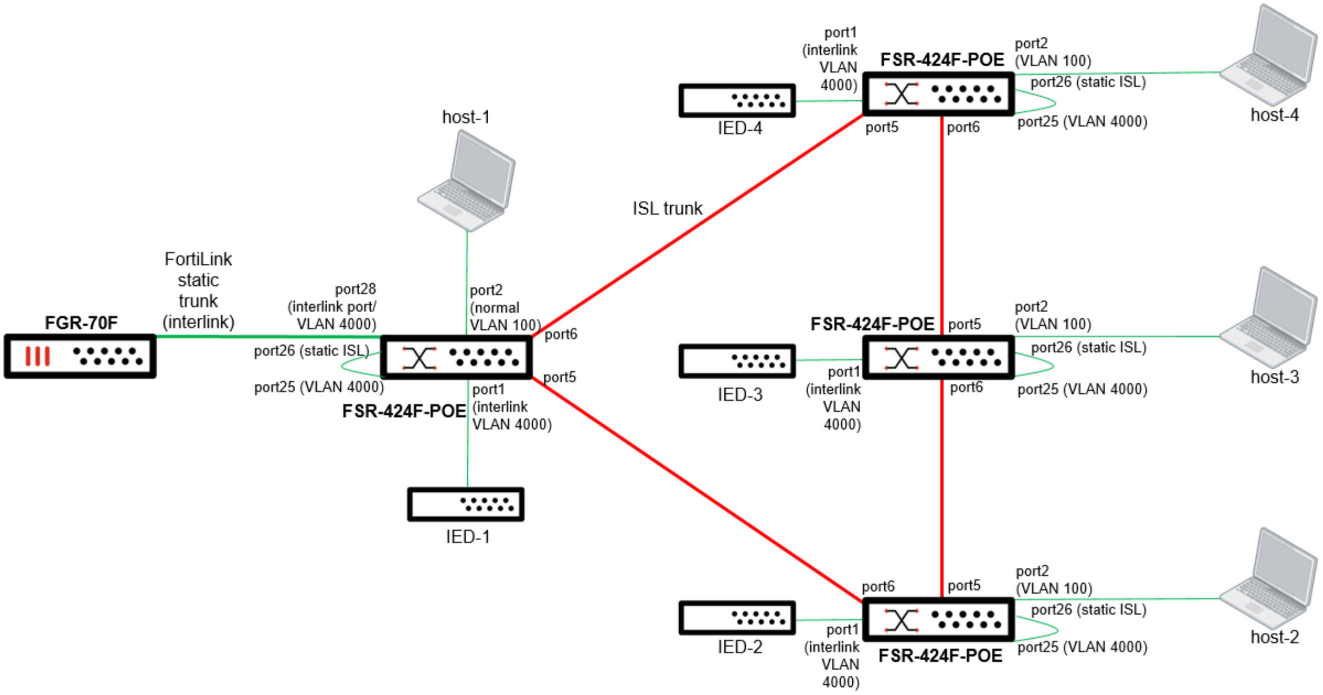
This section covers the following topics:

- Configuring HSR with FortiLink on page 363
- Configuring HSR and PRP with FortiLink on page 369
- Limitations for HSR and PRP with FortiLink on page 377

Configuring HSR with FortiLink

HSR is defined in the international standard IEC 62439-3-2016 clause 5. HSR provides seamless communication with fault tolerance by duplicating every unicast frame sent in HSR networks. Although HSR can be used in different topologies such as ring, bus, and mesh, the most commonly used topology is a single ring topology. This document focuses on the HSR ring topology. A simple HSR network consists of doubly attached bridging nodes, each having two ring ports, interconnected by full-duplex links. The simplest HSR topology contains two switches with two links between them; the ports connected to these two links serve as the HSR ring ports.

The following figure shows HSR being used with FortiLink.



You need to first configure HSR and the static-isl trunks on the physical loopbacks on the FortiSwitch units before authorizing and managing them on the FortiGate device.

In the preceding figure, the HSR ring ports (port5-port6) belong to the hsr-internal-vlan 4000. The hsr-internal-vlan cannot be same as the FortiLink management VLAN 4094 because the loopback static-isl trunk cannot have the native VLAN 4094 configured if the hsr-internal-vlan is set to 4094.

The switch management VLAN 4094 uses port26 for output with the native VLAN set to 4094 in all switches (port26 is the static ISL trunk with a native VLAN of 4094, which allows other normal data VLANs except for hsr-internal-vlan 4000). The native control packets in VLAN 4094 are sent to the port25 interlink port (VLAN 4000) through the physical loopback connection. Therefore, the native control packets go through the HSR ring to reach the tier-1 switch.

In the tier-1 switch, the native control packets are forwarded from the HSR ring to port28 (the interlink port of the FortiLink trunk) and then to the FortiLink interface. Therefore, the FortiGate device can manage all switches.

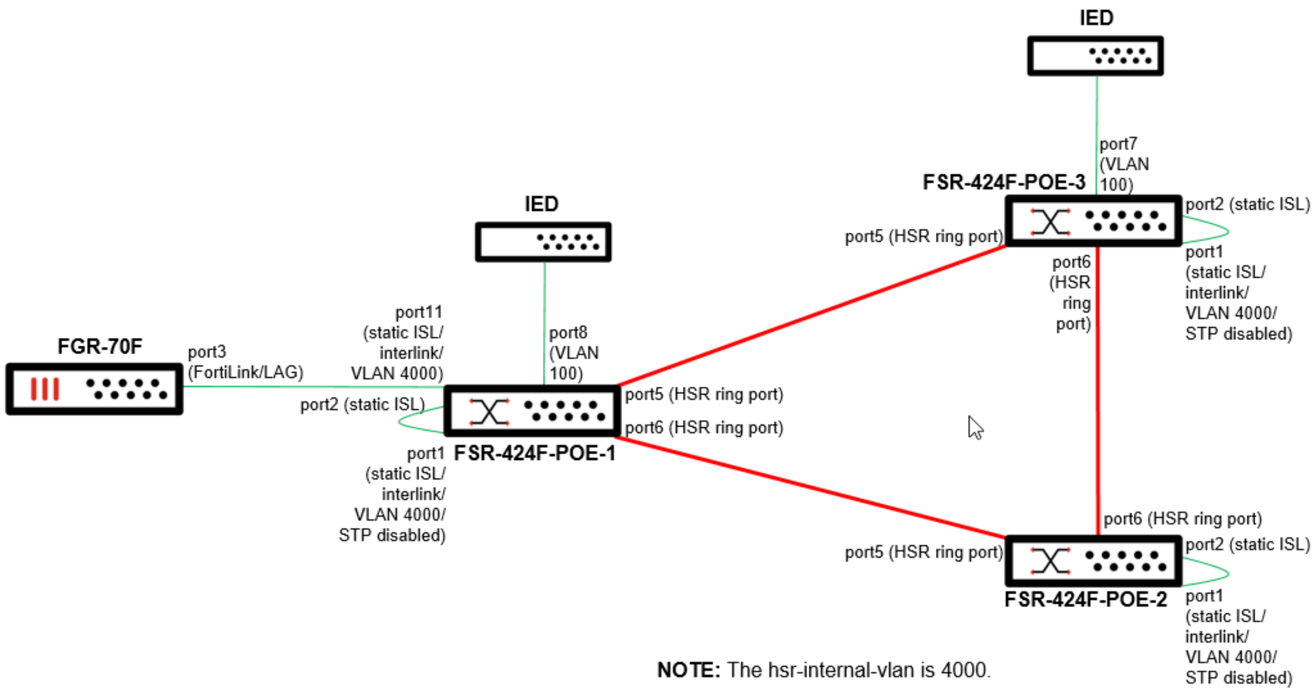
NOTE: The switch control plane (VLAN 4094) and intelligent electronic device (IED) data plane (hsr-internal-vlan 4000) are in same layer-2 broadcast domain.

All IED hosts in the VLAN 4000 go out of port28 (FortiLink trunk) of the tier-1 switch with native packets. The FortiLink interface in the FortiGate device receives these packets from all IED hosts. Therefore, the traffic of all IED hosts are in the FortiLink management VLAN on the FortiGate device (the management VLAN is 4094).

NOTE: The data traffic in VLAN 4000 will use the FortiLink interface as a gateway.

FortiLink can manage other normal data VLANs as usual.

Configuration example



NOTE: The hsr-internal-vlan is 4000.

To configure FGR-70F:

```
config system interface
   edit "fortilink"
      set vdom "root"
      set fortilink enable
      set ip 10.255.1.1 255.255.255.0
      set allowaccess ping fabric
      set type aggregate
      set member "port3"
      set lldp-reception enable
      set lldp-transmission enable
      set lacp-mode static
   next
end
```

To configure FSR-424F-POE-1:

```
config switch hsr ring
   edit 1
      set status enable
      set ring-port-pair port5-port6
      set hsr-internal-vlan 4000
   next
end

config switch trunk
   edit "HSR1" // automatically created
      set mode prp-hsr
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port5" "port6"
   next
   edit "trunk11"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port11"
   next
   edit "trunk1"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port1"
   next
   edit "trunk2"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port2"
   next
end

config switch interface
   edit "trunk11"
      set native-vlan 4000
      set dhcp-snooping trusted
      set edge-port disabled
   next
end

config switch interface
   edit "trunk1"
      set native-vlan 4000
      set dhcp-snooping trusted
      set stp-state disabled
      set edge-port disabled
   next
end

config switch interface
   edit "trunk2"
      set native-vlan 4094
      set allowed-vlans 1-3999,4001-4094
      set dhcp-snooping trusted
      set edge-port disabled
   next
end

config switch interface
   edit "HSR1" // automatically created
      set native-vlan 4000
      set dhcp-snooping trusted
      set stp-state disabled
      set edge-port disabled
   next
```

```
end
```

To configure FSR-424F-POE-2:

```
config switch hsr ring
   edit 1
      set status enable
      set ring-port-pair port5-port6
      set hsr-internal-vlan 4000
   next
end

config switch trunk
   edit "trunk1"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port1"
   next
   edit "trunk2"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port2"
   next
   edit "HSR1" // automatically created
      set mode prp-hsr
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port5" "port6"
   next
end

config switch interface
   edit "trunk1"
      set native-vlan 4000
      set dhcp-snooping trusted
      set stp-state disabled
      set edge-port disabled
      set snmp-index 49
   next
end

config switch interface
   edit "trunk2"
      set native-vlan 4094
      set allowed-vlans 1-3999,4001-4094
      set dhcp-snooping trusted
      set edge-port disabled
   next
end

config switch interface
   edit "HSR1" // automatically created
      set native-vlan 4000
      set dhcp-snooping trusted
      set stp-state disabled
      set edge-port disabled
   next
end
```

To configure FSR-424F-POE-3:

```
config switch hsr ring
   edit 1
      set status enable
      set ring-port-pair port5-port6
      set hsr-internal-vlan 4000
   next
end

config switch trunk
   edit "trunk1"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port1"
   next
   edit "trunk2"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port2"
   next
   edit "HSR1" // automatically created
      set mode prp-hsr
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port5" "port6"
   next
end

config switch interface
   edit "trunk1"
      set native-vlan 4000
      set dhcp-snooping trusted
      set stp-state disabled
      set edge-port disabled
   next
end

config switch interface
   edit "trunk2"
      set native-vlan 4094
      set allowed-vlans 1-3999,4001-4094
      set dhcp-snooping trusted
      set edge-port disabled
   next
end

config switch interface
   edit "HSR1" // automatically created
      set native-vlan 4000
      set dhcp-snooping trusted
```

```
        set stp-state disabled
        set edge-port disabled
    next
end
```

Configuring HSR and PRP with FortiLink

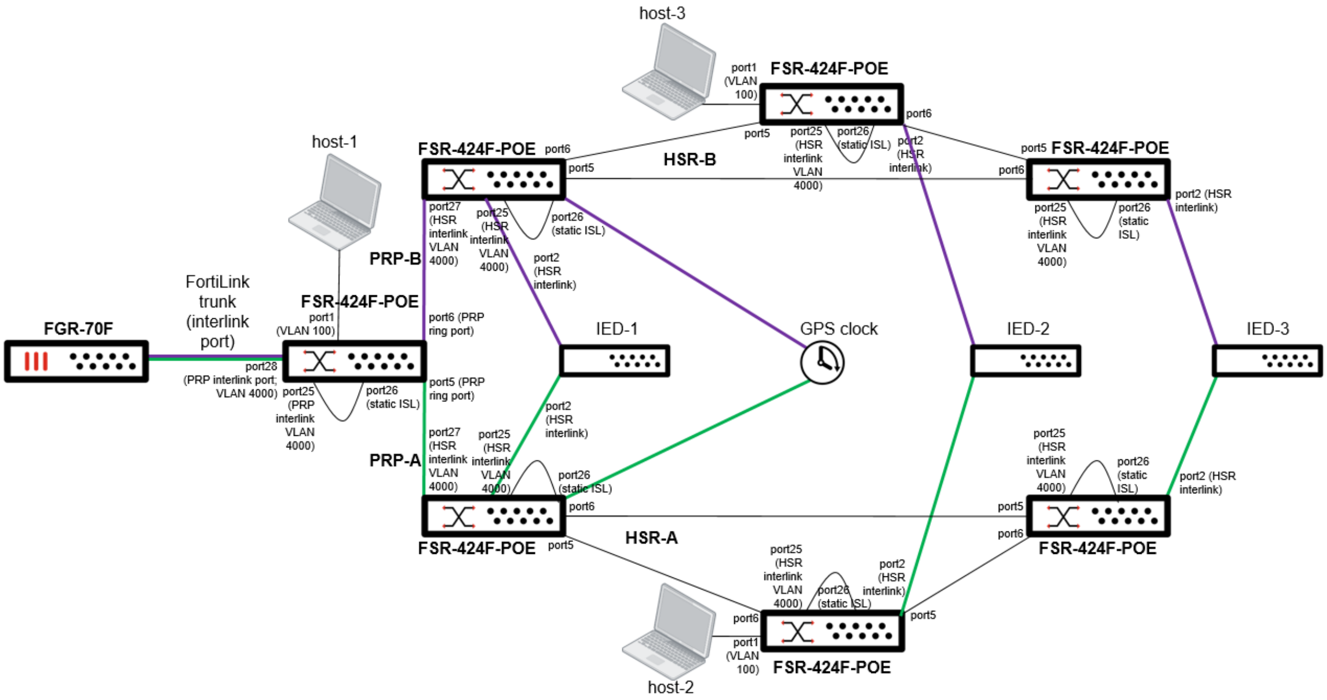
The PRP is defined in the international standard IEC 62439-3-2016 clause 4. PRP provides seamless communication with fault tolerance by duplicating every unicast frame sent in PRP networks. You can use PRP in different topologies such as ring, bus, or meshed.

A doubly attached node with PRP (DANP) is attached to two independent local area networks (LANs) with similar topologies, named LAN_A and LAN_B, which operate in parallel. A source DANP sends the same frame over both LANs, and a destination DANP receives it from both LANs within a certain time, consumes the first frame, and discards the duplicate. If a LAN fails, a DANP destination continues to operate with the frames from the other LAN.

Uncritical nodes, such as laptops or printers, are usually attached to just one LAN as single attached nodes (SANs). SANs that need to communicate with each other must be on the same LAN. If a critical node without PRP capability needs to communicate with all other nodes, it can be attached to a redundancy box (RedBox). The RedBox allows the single interface node to be attached to both networks and communicate with all other nodes. Because a node behind a RedBox appears to be a doubly attached node (DAN) to the other nodes, it is called a virtual DAN (VDAN). The RedBox itself is a DANP and acts as a proxy on behalf of its VDANs. Because both LAN A and LAB B must be independent, any connections among DANs and RedBoxes are not allowed.

The simplest PRP topology configuration is two switches with two links between them; the ports connected to these two links serve as PRP channel ports. PRP channel ports are always a pair of an odd-numbered switch port and an even-numbered switch port. The pair of switch ports are hard coded, for example, port1-port2, port3-port4,...port27-port28.

The following figure shows HSR and PRP being used with FortiLink.

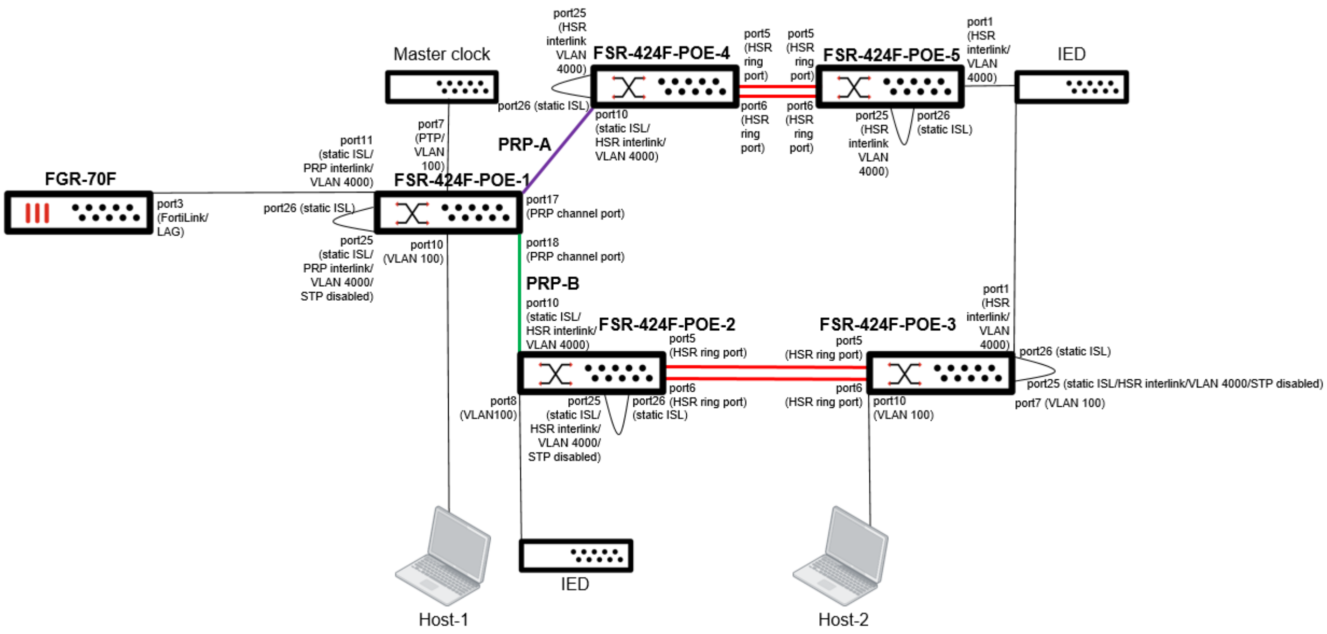


You need to first configure HSR and PRP and the static-isl trunks on the physical loopbacks on the FortiSwitch units before authorizing and managing them on the FortiGate device.

NOTE:

- The IEDs and the GPS clock are PRP cable stations. The hosts are normal hosts without PRP support.
- All hosts receive packets with the PRP trailer, so the host applications need to ignore the PRP trailer in the packets to make the applications work.

Configuration example


Master clock
port25 (HSR interlink VLAN 4000)
FSR-424F-POE-4
port5 (HSR ring port)
port5 (HSR ring port)
FSR-424F-POE-5
port1 (HSR interlink/ VLAN 4000)
IED
port26 (static ISL)
port10 (static ISL/ HSR interlink/ VLAN 4000)
port6 (HSR ring port)
port6 (HSR ring port)
port25 (HSR interlink VLAN 4000)
port26 (static ISL)
port11 (static ISL/ PRP interlink/ VLAN 4000)
port7 (PTP/ VLAN 100)
PRP-A
FGR-70F
FSR-424F-POE-1
port3 (FortiLink/ LAG)
port26 (static ISL)
port17 (PRP channel port)
port25 (static ISL/ PRP interlink/ VLAN 4000/ STP disabled)
port10 (VLAN 100)
port18 (PRP channel port)
PRP-B
port10 (static ISL/ HSR interlink/ VLAN 4000)
FSR-424F-POE-2
port5 (HSR ring port)
FSR-424F-POE-3
port5 (HSR ring port)
port1 (HSR interlink/ VLAN 4000)
port26 (static ISL)
port25 (static ISL/HSR interlink/VLAN 4000/STP disabled)
port7 (VLAN 100)
port6
port8 (VLAN100)
port25 (static ISL/ HSR interlink/ VLAN 4000/ STP disabled)
port26 (static ISL)
(HSR ring port)
port6 (HSR ring port)
port10 (VLAN 100)
IED
Host-1
Host-2

NOTE: The prp-internal-vlan and hsr-internal-vlan are 4000.

To configure FSR-424F-POE-1:

```
config switch prp channel
   edit 1
      set status enable
      set channel-port-pair port17-port18
      set prp-internal-vlan 4000
   next
end

config switch trunk
   edit "trunk11"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port11"
   next
   edit "trunk1"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port25"
   next
   edit "trunk2"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port26"
   next
   edit "PRP1"
      set mode prp-hsr
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port17" "port18"
   next
end

config switch interface
   edit "trunk11"
      set native-vlan 4000
      set dhcp-snooping trusted
      set edge-port disabled
   next
end

config switch interface
   edit "trunk1"
      set native-vlan 4000
      set dhcp-snooping trusted
      set stp-state disabled
      set edge-port disabled
   next
end

config switch interface
   edit "trunk2"
      set native-vlan 4094
      set allowed-vlans 1-3999,4001-4094
      set dhcp-snooping trusted
      set edge-port disabled
   next
end

config switch interface
   edit "PRP1"
      set native-vlan 4000
      set stp-state disabled
      set snmp-index 50
   next
end
```

To configure FSR-424F-POE-2:

```
config switch hsr ring
   edit 1
      set status enable
      set ring-port-pair port5-port6
      set hsr-internal-vlan 4000
   next
end

config switch trunk
   edit "trunk1"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port25"
   next
   edit "trunk2"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port26"
   next
   edit "trunk10"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port10"
   next
   edit "HSR1"
      set mode prp-hsr
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port5" "port6"
   next
end

config switch interface
   edit "trunk1"
      set native-vlan 4000
      set dhcp-snooping trusted
      set stp-state disabled
      set edge-port disabled
   next
end

config switch interface
   edit "trunk2"
      set native-vlan 4094
      set allowed-vlans 1-3999,4001-4094
      set dhcp-snooping trusted
      set edge-port disabled
   next
end

config switch interface
   edit "trunk10"
      set native-vlan 4000
      set dhcp-snooping trusted
      set edge-port disabled
   next
end

config switch interface
   edit "HSR1"
      set native-vlan 4000
      set dhcp-snooping trusted
      set stp-state disabled
      set edge-port disabled
   next
end
```

To configure FSR-424F-POE-3:

```
config switch hsr ring
   edit 1
      set status enable
      set ring-port-pair port5-port6
      set hsr-internal-vlan 4000
   next
end

config switch trunk
   edit "trunk1"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port25"
   next
   edit "trunk2"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port26"
   next
   edit "HSR1"
      set mode prp-hsr
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port5" "port6"
   next
end

config switch interface
   edit "trunk1"
      set native-vlan 4000
      set dhcp-snooping trusted
      set stp-state disabled
      set edge-port disabled
   next
end

config switch interface
   edit "trunk2"
      set native-vlan 4094
      set allowed-vlans 1-3999,4001-4094
      set dhcp-snooping trusted
      set edge-port disabled
   next
end

config switch interface
   edit "HSR1"
      set native-vlan 4000
      set stp-state disabled
   next
end
```

To configure FSR-424F-POE-4:

```
config switch hsr ring
   edit 1
      set status enable
      set ring-port-pair port5-port6
      set hsr-internal-vlan 4000
   next
end

config switch trunk
   edit "trunk1"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port25"
   next
   edit "trunk2"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port26"
   next
   edit "trunk10"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port10"
   next
   edit "HSR1"
      set mode prp-hsr
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port5" "port6"
   next
end

config switch interface
   edit "trunk1"
      set native-vlan 4000
      set dhcp-snooping trusted
      set stp-state disabled
      set edge-port disabled
   next
end

config switch interface
   edit "trunk2"
      set native-vlan 4094
      set allowed-vlans 1-3999,4001-4094
      set dhcp-snooping trusted
      set edge-port disabled
   next
end

config switch interface
   edit "trunk10"
```

```
         set native-vlan 4000
         set dhcp-snooping trusted
         set edge-port disabled
      next
   end

   config switch interface
      edit "HSR1"
         set native-vlan 4000
         set dhcp-snooping trusted
         set stp-state disabled
         set edge-port disabled
      next
   end
```

To configure FSR-424F-POE-5:

```
config switch hsr ring
   edit 1
      set status enable
      set ring-port-pair port5-port6
      set hsr-internal-vlan 4000
   next
end

config switch trunk
   edit "trunk1"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port25"
   next
   edit "trunk2"
      set auto-isl 1
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port26"
   next
   edit "HSR1"
      set mode prp-hsr
      set static-isl enable
      set static-isl-auto-vlan disable
      set members "port5" "port6"
   next
end

config switch interface
   edit "trunk1"
      set native-vlan 4000
      set dhcp-snooping trusted
      set stp-state disabled
      set edge-port disabled
   next
end

config switch interface
   edit "trunk2"
```

```
      set native-vlan 4094
      set allowed-vlans 1-3999,4001-4094
      set dhcp-snooping trusted
      set edge-port disabled
   next
end

config switch interface
   edit "HSR1"
      set native-vlan 4000
      set stp-state disabled
   next
end
```

Limitations for HSR and PRP with FortiLink

- You have to configure the static-isl trunk on the loopback trunk and the interlink port connected to the loopback trunk, and you have to set `static-isl-auto-vlan` to `disable`.
- The HSR and PRP internal VLANs must be defined on the FortiGate device with the default options and without an IP address. This VLAN can be assigned as the native VLAN on those HSR and PRP interlink ports.

  In the following example, VLAN 4000 is the `hsr-internal-vlan` and `prp-internal-vlan`:

  a. Configure VLAN 4000 in the FortiGate system interface:

  ```
  config system interface
     edit "vlan4000"
        set vdom "root"
        set allowaccess ping https ssh http
        set device-identification enable
        set role lan
        set snmp-index 109
        set interface "fortilink1"
        set vlanid 4000
     next
  end
  ```

  b. Configure VLAN 4000 in the FortiGate switch controller:

  ```
  config switch-controller managed-switch
      edit SR24FPTF21000005
        config ports
           edit port8
              set vlan vlan4000
              unset allowed-vlans
              unset untagged-vlans
           end
        end
  ```

www.fortinet.com