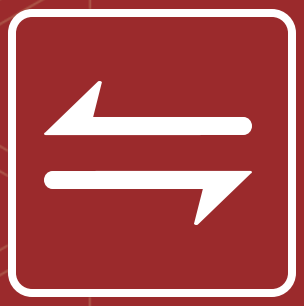


FORTINET
High Performance Network Security

FortiSwitch Devices Managed by FortiOS 5.6

FORTIOS
5.6
VERSION

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Wednesday, April 26, 2017

FortiSwitch Devices Managed by FortiOS 5.6

TABLE OF CONTENTS

Change Log

Date	Change Description
April 26, 2017	Fixes and improvements to the information in What's New for managed FortiSwitches in FortiOS 5.6 with FortiSwitch 3.5.4 (and later releases) on page 9.
April 24, 2017	Initial document release (FortiOS 5.6.0 and FortiSwitch 3.5.4)

Introduction

The maximum number of supported FortiSwitches depends on the FortiGate model:

FortiGate Model Range	Number of FortiSwitches Supported
Up to FortiGate-98 and FortiGate-VM01	8
FortiGate-100 to 280 and FortiGate-VM02	24
FortiGate-300 to 5*xx*	48
FortiGate-600 to 900 and FortiGate-VM04	64
FortiGate-1000 and up	128
FortiGate-3*xxx* and up, and FortiGate-VM08 and up	256

Supported Models

The following table shows the FortiSwitch models that support Fortilink mode when paired with the corresponding FortiGate models and the listed minimum software releases.

FortiGate and FortiWiFi Models	Earliest FortiOS	FortiSwitch Models
FGT-90D	5.2.2	FS-224D-POE
FGT-60D FGT-100D, 140D, 140D-POE, 140D-T1 FGT-200D, 240D, 280D, 280D-POE FGT-600C FGT-800C FGT-1000C, 1200D, 1500D FGT-3700D, FGT-3700DX	5.2.3	FSR-112D-POE FS-108D-POE FS-124D (POE) FS-224D-POE and FPOE
	5.4.0	All FortiSwitch D-series models. FortiSwitchOS 3.3.x or 3.4.0 is recommended.

FortiGate and FortiWiFi Models	Earliest FortiOS	FortiSwitch Models
FGT and FWF-30D, 30D-POE, 30E FGT and FWF-50E, 51E FGR-60D FGT-70D, 70D-POE FGT-80D FGR-90D FGT and FWF-92D FGT-94D-POE, 98D-POE FGT-300D FGT-400D FGT-500D FGT-600D FGT-900D FGT-1000D FGT-3000D, 3100D, 3200D, 3240C, 3600C, 3810D, 3815D FGT_VM, VM64, VM64-AWS, VM64-AWSONDEMAND, VM64-HV, VM64-KVM, VM-VMX, VM64-XEN	5.4.1	All FortiSwitch D-series models. FortiSwitchOS 3.4.2 or later is required for all managed switches.
FGT and FWF- 60E, 61E FGT-100E, 101E	5.4.2	All FortiSwitch D-series models. FortiSwitch 3.4.2 or later is required for all managed switches.
FGT-80E, 80E-POE, 81E, 81E-POE FGT-100EF	5.4.3	All FortiSwitch D-series models. FortiSwitch 3.4.2 or later is required for all managed switches.
FGT-90E, 91E FGT-200E, 201E FGT-2000E, 2500E	5.6.0	All FortiSwitch D-series models. FortiSwitch 3.5.4 or later is required for all managed switches.

What's New for managed FortiSwitches in FortiOS 5.6 with FortiSwitch 3.5.4 (and later releases)

This section describes new managed FortiSwitch features in FortiOS 5.6 with FortiSwitch 3.5.4:

Aggregating FortiSwitches into groups (397950)

In larger networks, the number of switches can be large. Different models and device purposes might exist. Furthermore, the topology might have "built-in" redundancy. Use the following command to create a FortiSwitch group allowing you to perform an operation on the entire group instead of one switch at a time.

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

Pre-authentication and Replacements of FortiSwitches (298533)

FortiSwitch configuration templates allow you to replace a FortiSwitch and have the configuration of the original FortSwitch installed on the replacement.

Use the `execute replace-device fortiswitch <sn-old> <sn-new>` to transfer the configuration for the FortiSwitch with serial number `<sn-old>` to the replacement FortiSwitch with serial number `<sn-new>`.

LLDP MED on Managed FortiSwitches (372288)

FortiOS 5.6 supports configuring Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP MED) for managed FortiSwitches. Additionally, you can use FortiGate CLI commands display the information collected by LLDP on the FortiSwitch.

You can use the following command 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
```

Enhanced 802.1x including FortiSwitch port security policy framework (389102)

New FortiSwitch port security features include:

- Dynamic VLAN Assignment
- “guest” and “auth-fail” VLAN
- Mac Address Bypass (MAB)
- Multiple host support on single physical port

Global Settings Applied across the Network

```
config switch-controller 802.1x-settings
   set reauth-period < int >
   set max-reauth-attempt < int >
   set link-down-auth < *set-unauth | no-action >
end
```

Local Switch Overrides

```
config switch-controller managed-switch
   edit < switch >
      config 802.1x-settings
         set local-override {disable | enable}
         set reauth-period <int>
         set max-reauth-attempt <int>
         set link-down-auth {set-unauth | no-action}
      end
   next
end
```

Policy Definitions (802.1x, and captive-portal)

```
config switch-controller security-policy 802.1x
   edit 8021X-policy-default
      set user-group <user.group>
      set mac-auth-bypas {disable | enable}
      set guest-vlan {disable | enable}
      set guest-vlanid <vlan-id>
      set guest-auth-delay <int>
      set auth-fail-vlan  {disable | enable}
      set auth-fail-vlanid <vlan-id>
      radius-timeout-overwrite {disable | enable}
   end
end


config switch-controller security-policy captive-portal
   edit captive-portal-default
      set vlan <vlan-id>
```

```
      config users
         edit 1
            set user-group <usergroup>
            set vlanid <vlan-id>
         next
      end
   end
end
```

Port Settings

```
config switch-controller managed-switch
   edit <managed-switch>
      config ports
         edit <port>
            set port-security-policy {802.1x-policy | captive-portal-policy}
         next
      end
   next
end
```

Firmware upgrade management and compatible version information (385171)

You can view the current firmware version of a FortiSwitch and upgrade the FortiSwitch to a new firmware version by going to **WiFi & Switch Controller > Managed FortiSwitch** and editing one of the FortiSwitches. Under **Firmware** you can see the current firmware version and select **Update** to update it.

Changed Managed-Switch Display Format for 'dynamic-capability' (387239)

FortiOS 5.6.0 displays capability flags as strings such as: dynamic-capability, igmp-snooping, dhcp-snooping, and so on. For example:

```
config switch-controller managed-switch
edit S124DP3X15000315
get
switch-id : S124DP3X15000315
name :
description :
fsw-wan1-peer : port9
fsw-wan1-admin : enable
fsw-wan2-peer :
fsw-wan2-admin : discovered
directly-connected : 0
connected : 1
version : 1
pre-provisioned : 0
dynamic-capability : igmp-snooping,dhcp-snooping
switch-device-tag :
dynamically-discovered: 1
```

Connecting to a managed switch CLI from the FortiGate GUI (378119)

To connect to a FortiSwitch CLI, go to **WiFi & Switch Controller > Managed FortiSwitch**, right click on the FortiSwitch to connect to and select **Connect to CLI**. You can also open the FortiGate CLI console and use the `execute telnet <ip>` command, where `<ip>` is the management IP address of the FortiSwitch.

Firmware upgrade of stacked or tiered switches (355050)

From your FortiGate CLI, you can upgrade the firmware of all of the managed FortiSwitches of the same model using a single `execute` command. The command includes the name of a firmware image file and all of the managed FortiSwitches compatible with that firmware image file are upgraded. For example:

```
execute switch-controller stage-swtp-image ALL <firmware-image-file>
```

You can also use the following new command to restart all of the managed FortiSwitches after a 2 minute delay.

```
execute switch-controller restart-swtp-delayed ALL
```

More information displayed by the execute switch-controller get-conn-status command (388751)

The `get-conn-status` command now displays more information for each managed switch including the ID of each switch, the version of the firmware running on the switch, the status of the switch, the IP address for managing the switch, and its join time.

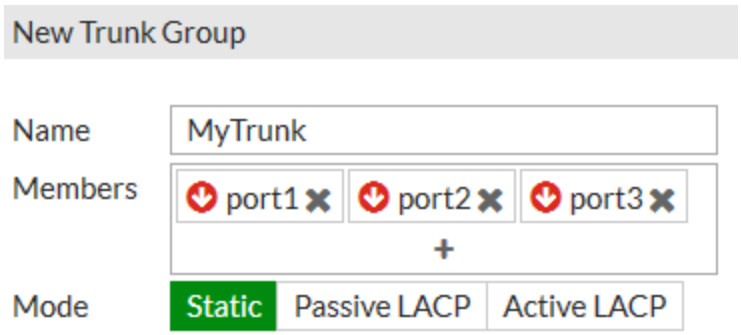
```
execute switch-controller get-conn-status
Managed-devices in current vdom root:

STACK-NAME: FortiSwitch-Stack-port3
SWITCH-ID        VERSION  STATUS          ADDRESS     JOIN-TIME NAME
FS108D3W16001177 v3.4     Authorized/Down 169.254.1.2 N/A       My-Switch
```

User-port Link Aggregation Groups available on the GUI (378470)

The GUI now supports the ability to configure user port LAGs on managed FortiSwitches.

To create a Link Aggregation Group for FortiSwitch user ports:

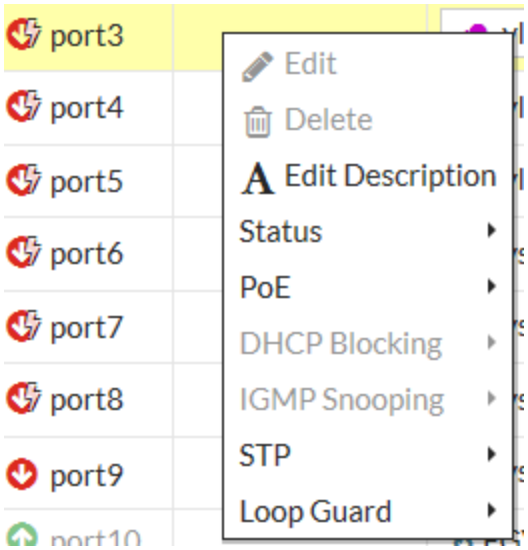
1. Go to **WiFi & Switch Controller > FortiSwitch Ports**.
2. Click **Create New > Trunk**.
3. In the New Trunk Group page enter a **Name** for the trunk group.
4. Select two or more physical ports to add to the trunk group.
5. Select the **Mode**: Static, Passive LACP, or Active LACP.
6. Click OK.



DHCP blocking, STP and Loop Guard on Managed FortiSwitch ports on the GUI (375860)

The managed FortiSwitch GUI now supports the ability to enable/disable DHCP blocking, STP and Loopguard for FortiSwitch user ports.

Go to **WiFi & Switch Controller > FortiSwitch Ports**. For any port you can select DHCP Blocking, STP, or Loop Guard. STP is enabled on all ports by default. Loop guard is disabled by default on all ports.



New Switch Profiles (387398)

Switch profiles allow specific settings to be applied to all authorized FortiSwitches. The default switch profile is automatically bound to every switch discovered by the FortiGate. You can create additional profiles as needed.

Within a switch profile, you can control the behavior of the FortiSwitch's admin account.You can add a password to a profile or create a new profile and bind that profile to any switch. The password provided in the profile is configured on the FortiSwitch to the default admin administrator account.

Miscellanous configuration option changes

- On a switch port, the default value of `dhcp-snooping` (also called DHCP-blocking) is changed from `trusted` in FortiOS 5.4 to `untrusted` in FortiOS 5.6.

- On a switch port, the default value of STP `edge-port` is changed from `disabled` in FortiOS 5.4 to `enabled` in FortiOS 5.6.0.
- Default value of `fortilink-split-port` is changed from `disable` in FortiOS 5.4.1/5.4.2 to `enable` in FortiOS 5.4.3 onward. This command applies to FortiGate aggregate interfaces.

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

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, and you have administrative access to the FortiSwitch web-based manager and CLI.
- You have installed a FortiGate unit on your network and have administrative access to the FortiGate web-based manager and CLI.

How this Guide is Organized

This guide contains the following sections:

- Connecting FortiLink Ports - information about connecting FortiSwitch ports to FortiGate ports.
- FortiLink Configuration Using the FortiGate GUI
- FortiLink Configuration Using FortiGate CLI
- Configuring Fortilink for FortiGate HA - how to configure Fortilink for FortiGate units in HA mode.
- Network Topologies for Managed FortiSwitch - describes configuration for various stacking topologies
- Optional Setup Tasks - describes other set up tasks.
- FortiSwitch features configuration - describes configuring managed FortiSwitch features including VLANs
- FortiSwitch Port Features - configure Ports and POE from the FortiGate unit.
- FortiSwitch port security policy - describes setting up FortiSwitch security policies
- Additional Capabilities - describes extra FortiSwitch features
- Troubleshooting - describes techniques for troubleshooting common problems.
- Scenarios - contains practical examples of how to use managed FortiSwitch units in a network.

Connecting FortiLink Ports

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

For all FortiGate models, you can connect up to 16 FortiSwitches to one FortiGate unit.

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).

In FortiSwitchOS 3.4.2 and later releases, you can deploy managed FortiSwitches in a stacked topology. See the Network Topologies for Managed FortiSwitch chapter for additional information about the supported topologies.

1. Enable the Switch Controller on FortiGate

Prior to connecting the FortiSwitch and FortiGate units, ensure that the Switch Controller feature is enabled on the FortiGate with the FortiGate web-based manager or CLI to enable the Switch Controller. Depending on the FortiGate model and software release, this feature may be enabled by default.

Using the FortiGate GUI

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

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

Using the FortiGate CLI

Use the following command to enable the Switch Controller.

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

2. Connect the FortiSwitch and FortiGate

FortiSwitchOS 3.3.0 and later, provide flexibility for FortiLink:

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

Auto-discovery of the FortiSwitch Ports

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

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

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

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

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

The table below lists the default auto-discovery ports for each switch model:

FortiSwitch Model	Default Auto-FortiLink ports
FS-108D	ports 9 and 10
FSR-112D	ports 9, 10, 11 and 12
FS-124D, FS-124D-POE	ports 23, 24, 25 and 26
FS-224D-POE	ports 21, 22, 23 and 24
FS-224D-FPOE	ports 25, 26, 27 and 28
FS-248D-POE	ports 49, 50, 51, and 52
FS-248D-FPOE	ports 49, 50, 51, and 52
FS-424D, FS-424D-POE, FS-424D-FPOE	ports 25 and 26
FS-448D, FS-448D-POE, FS-448D-FPOE	ports 49, 50, 51, and 52
FS-524D, FS-524D-FPOE	ports 25, 26, 27, 28, 29 and 30
FS-548D, FS-548D-FPOE	ports 49, 50, 51, 52, 53 and 54
FS-1024D, FS-1048D, FS-3032D	all ports

Choosing the FortiGate Ports

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

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

FortiLink Configuration Using the FortiGate GUI

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

You can configure FortiLink using the FortiGate GUI or CLI. We recommend using the former as the CLI steps 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 zero configuration steps on the FortiSwitch, and with a few simple configuration steps on the FortiGate.

Summary of the Steps

1. On the FortiGate, configure the FortLink port or create a logical FortLink interface.
2. Authorize the managed FortiSwitch.

Configure FortiLink as a Single Link

Configure the FortiLink port on the FortiGate using the following steps:

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

Configure FortiLink as a Logical Interface

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

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

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

1. Go to **Network> Interfaces**.
2. (Optional) If the FortiLink physical ports are currently included in the internal interface, edit it and remove the desired ports from the Physical Interface Members.
3. Select **Create New > Interface**.
4. Enter a name for the interface (11 characters maximum).
5. Set the **Type** to **802.3ad Aggregate, Hardware Switch**, or **Software Switch**.

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

FortiLink Split-Interface

You can create a FortiLink Split-Interface, which connects a FortiLink aggregate interface from one FortiGate to two FortiSwitches.

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

You must enable the Split-Interface option on the FortiLink aggregate interface. Using the FortiGate CLI:

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

Authorizing the FortiSwitch

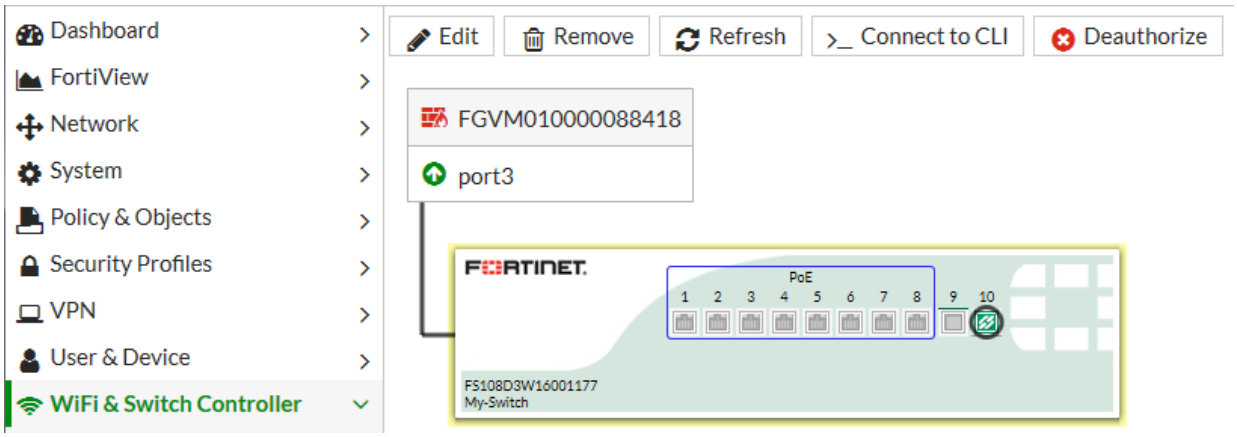
If you configured the FortiLink interface to manually authorize the FortiSwitch as a managed-switch, perform the following steps:

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.

Managed FortiSwitch Display

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

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 though and find more infomration about the status of the switch. The link to the FortiSwitch may 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 should make sure the firmware runnng on the FortiSwitch is compatible with the firmware running on the FortiGate.

From the Managed FortSwitch page you can edit any of the managed FortiSwitches, remove a FortiSwitch from the configuration, refresh the display, connect to the CLI of a FortiSwitch or deathorize a FortiSwitch.

Edit a Managed FortiSwitch

To edit a managed FortiSwitch:

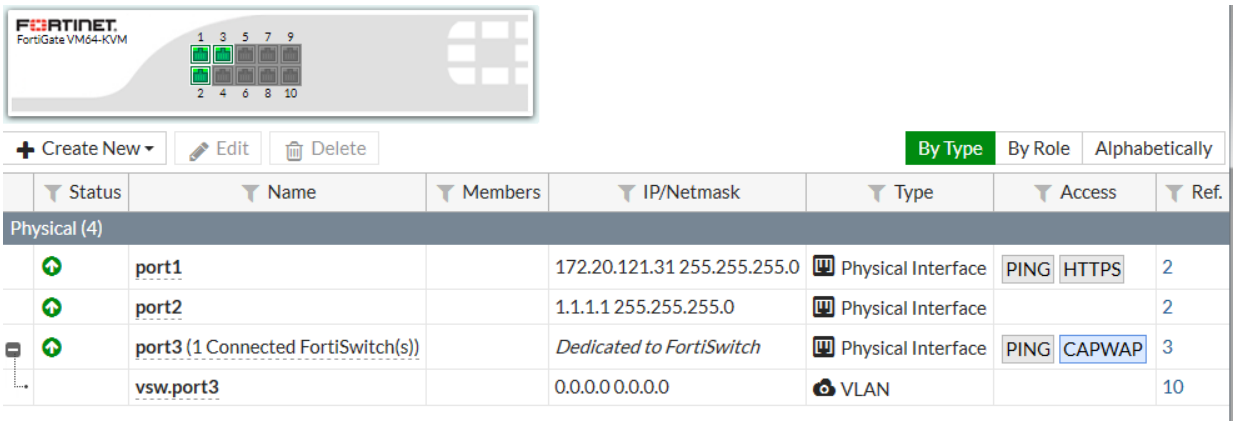
1. Go to **WiFi & Switch Controller > Managed FortiSwitch**.
2. Click on the FortiSwitch to and click **Edit**, right-click on a FortiSwitch and select **Edit**, or double-click on a FortiSwitch.

From the **Edit Managed FortiSwitch** form, you can:

- Change the **Name** and **Description** of the FortiSwitch.
- Vierw the **Status** of the FortiSwitch.
- **Restart** the FortiSwitch.
- **Authorize**d or deathorize the FortiSwitch.
- **Update** the firmware running on the switch.

Network Interface Display

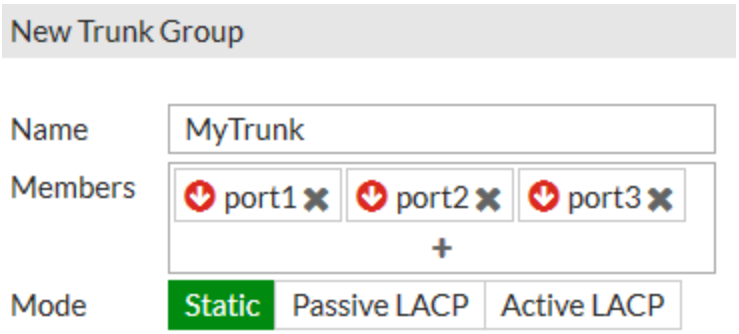
On the **Network > Interfaces** page you can see the FortiGate interface connected to the FortiSwitch. The GUI indicates **Dedicated to FortiSwitch** in the IP/Netmask field.



Add Link Aggregation Groups (Trunks)

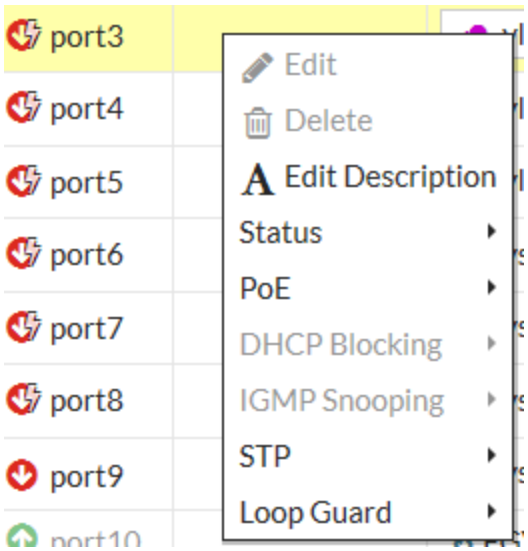
To create a Link Aggregation Group for FortiSwitch user ports:

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



Configure DHCP blocking, STP and Loop Guard on Managed FortiSwitch ports

Go to to **WiFi & Switch Controller > FortiSwitch Ports**. For any port you can select DHCP Blocking, STP, or Loop Guard. STP is enabled on all ports by default. Loop guard is disabled by default on all ports.


port3
port4
port5
port6
port7
port8
port9
port10
Edit
Delete
Edit Description
Status
PoE
DHCP Blocking
IGMP Snooping
STP
Loop Guard

FortiLink Configuration Using FortiGate CLI

This section describes how to configure FortiLink using the FortiGate CLI. We recommend using the FortiGate GUI, because the CLI steps 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 zero configuration steps on the FortiSwitch, and with a few simple configuration steps on the FortiGate.

Summary of the Steps

1. Remove the port(s) from the LAN interface.
2. Configure the FortLink port or create a logical FortLink interface.
3. Configure NTP.
4. Authorize the managed FortiSwitch.
5. Configure DHPC.

Configure FortiLink as a Single Link

Configure the FortiLink port on the FortiGate, and authorize the FortiSwitch as a managed switch.

In the following steps, port1 is configured as the FortiLink port.

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

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

2. Configure port 1 as the FortiLink interface:

```
config system interface
   edit port1
      set vdom root
      set ip 169.254.3.1 255.255.255.0
      set allowaccess capwap ping
      set type physical
      set snmp-index 1
      set auto-auth-extension-device enable
      set fortilink enable
   end
end
```

3. Configure an NTP server on port 1:

```
config system ntp
```

```
    set server-mode enable
    set interface port1
end
```

4. Authorize the FortiSwitch unit as a managed switch.

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

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

5. Configure a DHCP server on port 1.

```
config system dhcp server
    edit 0
        set ntp-service local
        set default-gateway 169.254.3.1
        set netmask 255.255.255.0
        set interface port1
        config ip-range
            edit 0
                set start-ip 169.254.3.2
                set end-ip 169.254.3.254
            end
        set vci-match enable
        set vci-string FortiAP FortiSwitch FortiExtender
    end
end
```

Configure FortiLink as a Logical Interface

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

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

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

In the following steps, port4 and port5 are configured as a FortiLink LAG.

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

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

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

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

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

3. Configure an NTP server on the LAG interface.

```
config system ntp
   set server-mode enable
   set interface flink1
end
```

4. Authorize the FortiSwitch unit as a managed switch.

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

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

5. Configure a DHCP server on port 1.

```
config system dhcp server
   edit 0
      set ntp-service local
      set default-gateway 169.254.254.1
      set netmask 255.255.255.252
      set interface flink1
      config ip-range
         edit 1
            set start-ip 169.254.254.2
            set end-ip 169.254.254.2
         end
      set vci-match enable
      set vci-string FortiAP FortiSwitch FortiExtender
   end
end
```

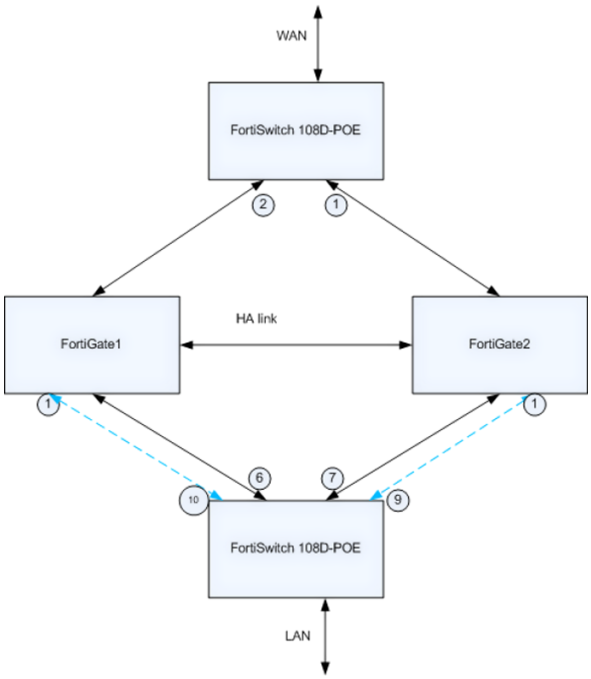
Configuring FortiLink for FortiGate HA

A FortiGate operating in HA mode can use FortiLink to FortiSwitches running FortiSwitchOS 3.3.0 or later release. To use FortiLink mode with a pair of FortiGate units in a high-availability cluster, you must connect FortiLink from the switch to both of the FortiGate units.

Be aware of the following:

1. No console port or direct management is required on the FortiSwitch.
2. All the actions described here can be performed from FortiCloud if needed.
3. All FortiSwitch internal state and counters are visible in FortiLink managed mode.

Example Topology



The LAN and WAN links connect to distinct FortiSwitch ports. The FortiSwitch with FortiLink to both units connects to the FortiGate units (active and standby). If the standby FortiGate (for example, FGT2) becomes active, this is transparent to the LAN and WAN ports. FortiLink is automatically established to FGT2, and the active traffic path becomes LAN <-> FGT2<-> WAN.

Note the following points:

1. LAN and WAN links can connect to separate FortiSwitches, as shown in the figure. You can also connect them to the same FortiSwitch (and use VLANs to separate the LAN and WAN traffic).
2. Connect the FortiLinks from any two FortiSwitch ports to FGT1 port X and FGT2 port X, where the FortiGate port numbers must match (port1 in the above topology diagram).

3. For a Logical FortiLink interface with two ports, connect FortiLinks from two additional FortiSwitch ports to FGT1 port Y and FGT2 port Y, where the FortiGate port numbers must match.

Adding a Second FortiGate to Existing Single FortiGate

Connect an additional FortiLink from the FortiSwitch to the new FortiGate, and configure HA on both of the FortiGate units.

Configuration Steps

Configuration consists of the following major steps:

1. Configure “auto-discovery-fortilink enable” on the FortiSwitch ports that you will connect to FGT2. This step is not required if the port is auto-fortilink by default.
2. Add cable connections from FGT2 to the directly-connected FortiSwitches (exact duplicate of FGT1 to the FortiSwitches).
3. Connect HA cables between FGT1 and FGT2.
4. At FGT1: configure FortiGate High Availability using the GUI. For additional information, refer to the High Availability chapter in the FortiOS Handbook.
5. At FGT2: Configure FortiGate High Availability using the CLI from the console port. The following parameters must be identical to FGT1:
   - HA-mode
   - Priority
   - Group Name and Password
6. At this point, the FGT1 synchronizes with FGT2.
7. After several minutes, verify the configuration at FGT2 using the following commands:

```
get ha status
get system ha status
```

Adding the First Switch to Existing HA FortiGates (single FortiLinks)

Connect one FortiSwitch port to each of the FortiGate units. On FGT1, follow the same FortiLink configuration steps as for the non-HA configuration. FGT1 synchronizes the configuration with FGT2.

Configuration Steps

1. Configure two FortiSwitch ports as “auto-discovery-fortilink enable”. This step is not required for any port is auto-fortilink by default.
2. Connect one port to FGT1 and the other port to FGT2.
   - The FGT1 and FGT2 port numbers must be identical (e.g., FortiSwitch port21 and port22 connect to FGT1 port4 and FGT2 port4).
3. At FGT1, perform the steps to configure FortiLink (as described in FortiLink Configuration Using the FortiGate GUI):

a. Configure a port to be the FortiLink port.
b. Authorize the FortiSwitch.

4. At FGT2, run the command "get switch-controller managed-switch" to verify that the FGT1 configuration was synchronized successfully.

Adding the First Switch to Existing FGT HA setup (Logical Fortilink Interface)

In this configuration, we connect two FortiSwitch ports to each FortiGate unit. Enter the configuration commands on FGT1 (same commands as for the non-HA configuration). The HA feature synchronizes the configuration to FGT2.

Configuration Steps

1. Configure four FortiSwitch ports as “auto-discovery-fortilink enable” (bypass this ste-p if a port is auto-fortilink by default).
2. Connect two ports to FGT1 and the other ports to FGT2:
 - the FGT1 and FGT2 port numbers must match (e.g., FortiSwitch port21 and port22 connect to FGT1 port4 and port5 and FortiSwitch port23 and port24 connect to FGT2 port4 and port5).
3. At FGT1, configure the Fortilink interface (see FortiLink Configuration Using the FortiGate GUI):
   a. Create the FortiLink logical interface and add the physical ports as members.
   b. Authorize the FortiSwitch.
4. At FGT2, run the **get switch-controller managed-switch** command to verify that the FGT1 configuration was synchronized successfully.

(Optional) Test the HA Capability

Warning: This is a *destructive test* that simulates a FortiGate failure. You should conduct this test only in a lab or test network, not in a production network:

1. Disconnect power from FGT1 to simulate failure.
2. From the FGT2 UI:
 Check **Wifi and Switch Controller** > **Managed FortiSwitch**.
3. FortiSwitch is now visible from the management interface on FGT2.

Network Topologies for Managed FortiSwitch

The FortiGate requires only one active FortiLink to manage all of the subtending FortiSwitches (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 may also configure a standby FortiLink.

For any of the topologies, note the following:

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

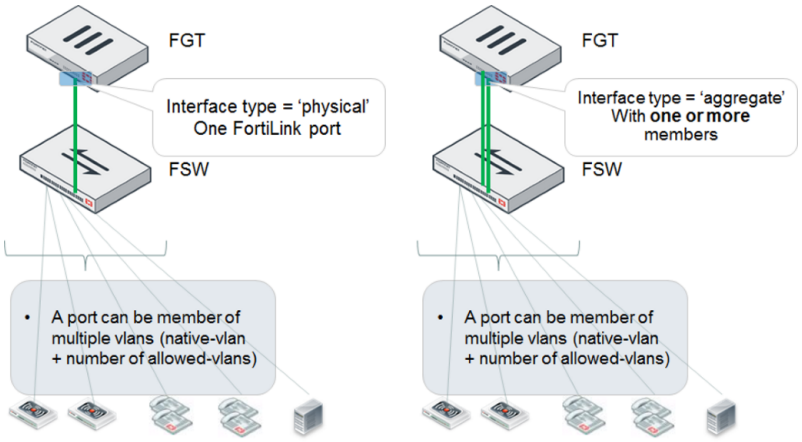
Supported Topologies

Fortinet recommends the following topologies for managed FortiSwitches:

- Single FortiGate managing a single FortiSwitch
- Single FortiGate managing a stack of several FortiSwitches
- HA-mode FortiGate managing a single FortiSwitch
- HA-mode FortiGate managing a stack of several FortiSwitches
- HA-mode FortiGate managing a FortiSwitch two-tier topology
- Single FortiGate managing multiple FortiSwitches (using hardware or software switch interface)
- Enterprise/Office Closet Topology
- Aggregated FortiSwitches

Single FortiGate managing a single FortiSwitch

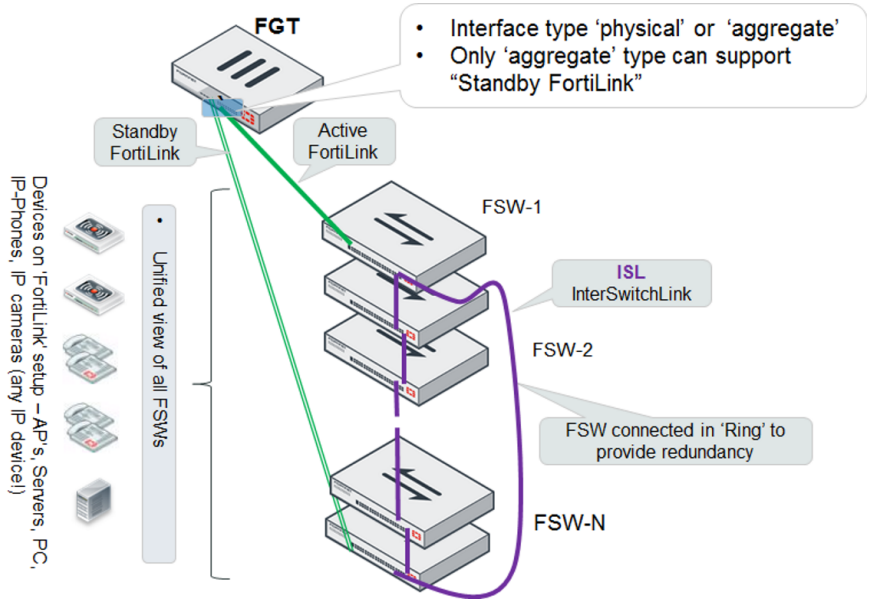
On the FortiGate, the FortiLink interface is configured as physical or aggregate. The 802.3ad aggregate interface type provides a logical grouping of one or more physical interfaces.



Single FortiGate managing a stack of several FortiSwitches

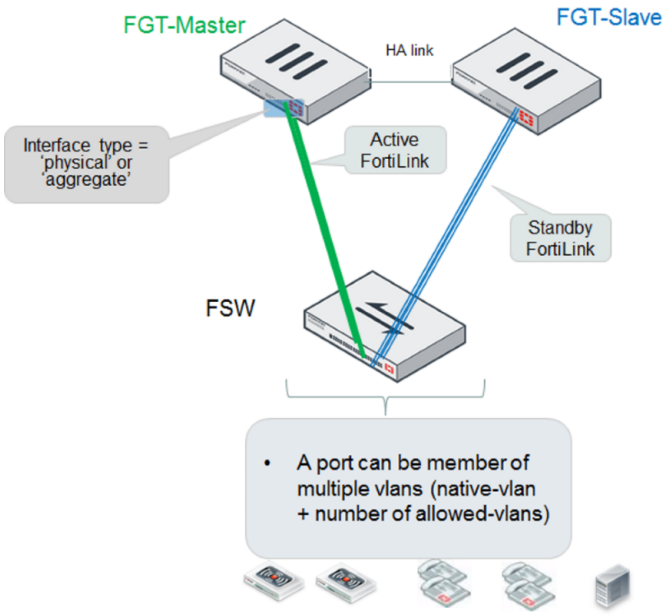
The FortiGate connects directly to one FortiSwitch device using a physical or aggregate interface. The remaining FortiSwitches connect in a ring using inter-switch links (i.e., ISL).

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



HA-mode FortiGate managing a single FortiSwitch

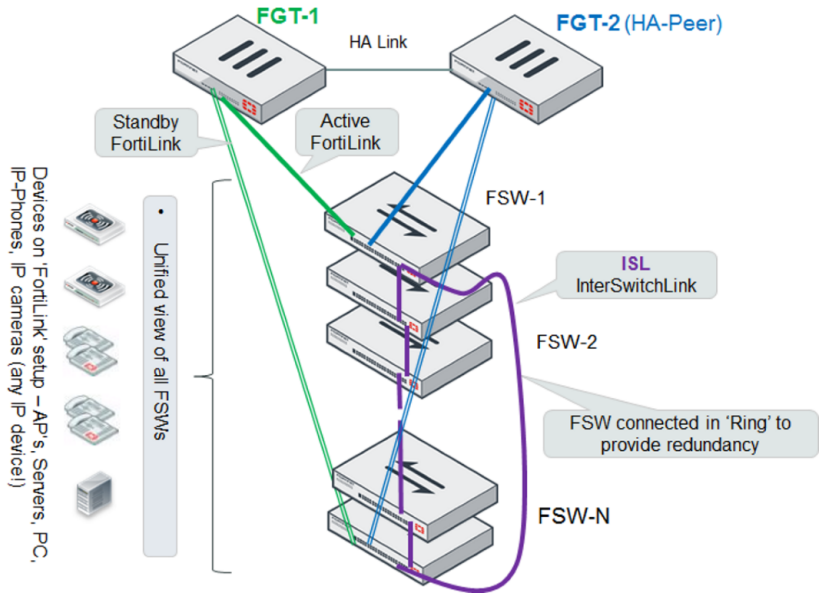
The master and slave FortiGate units both connect a FortiLink to the FortiSwitch. The FortiLink port(s) and interface type must match on the two FortiGate units.



HA-mode FortiGate managing a stack of several FortiSwitches

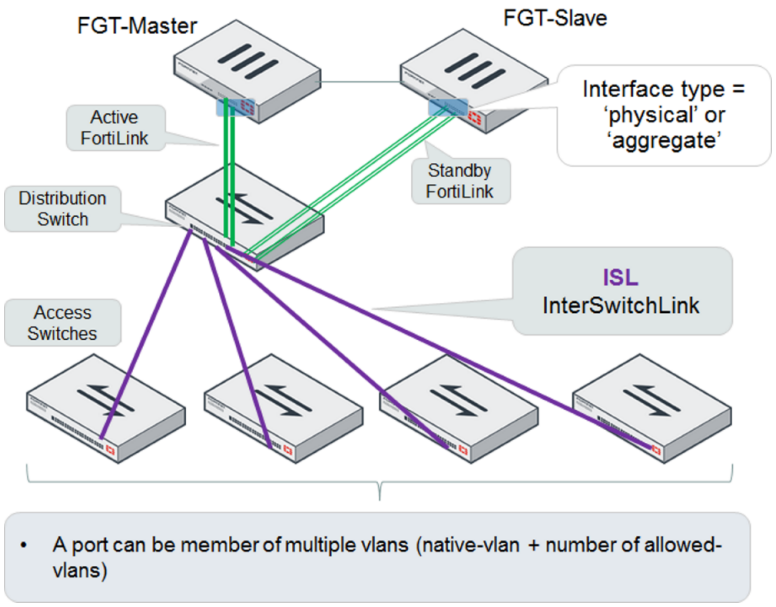
The master and slave FortiGate units both connect a FortiLink to the first FortiSwitch, and (optionally) to the last FortiSwitch. The FortiLink ports and interface type must match on the two FortiGate units.

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



HA-mode FortiGate managing a FortiSwitch two-tier topology

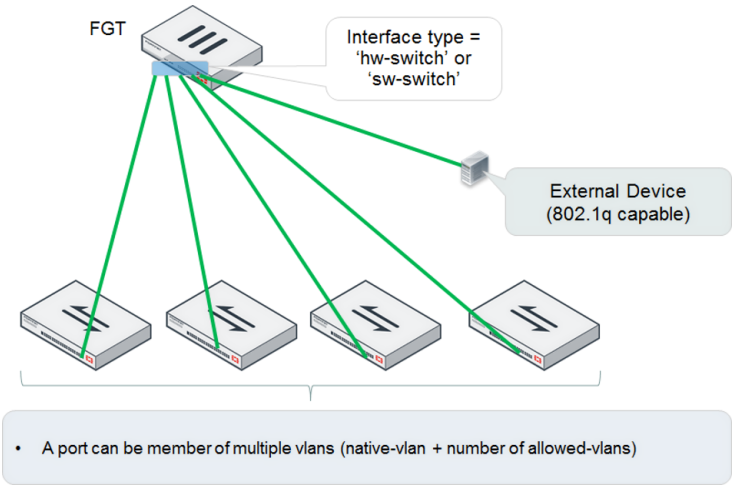
The distribution FortiSwitch connects to the master and slave FortiGate units. The FortiLink port(s) and interface type must match on the two FortiGate units.



Single FortiGate managing multiple FortiSwitches (using hardware or software switch interface)

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

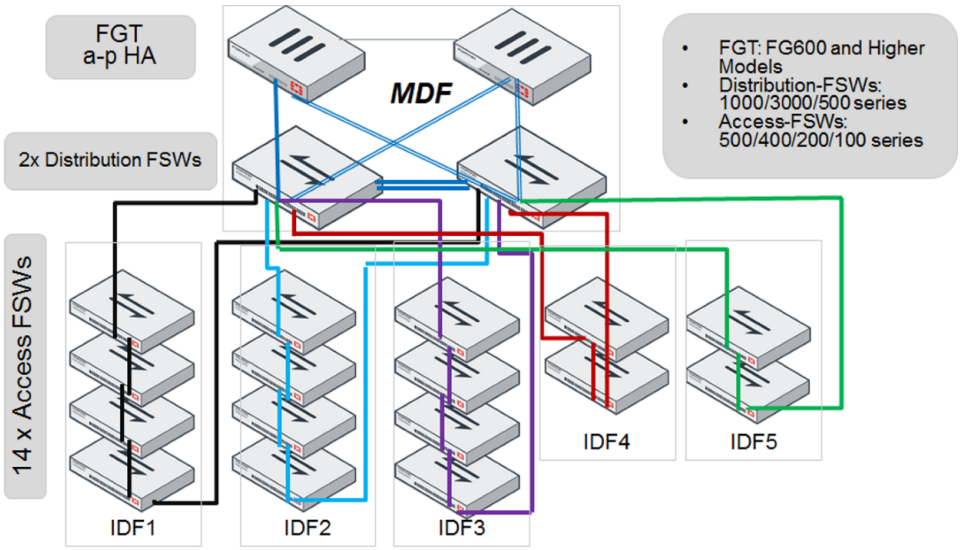
Optionally, you can connect other devices to the FortiGate logical interface. These devices, which must support IEEE 802.1q VLAN tagging, will have Layer 2 connectivity with the FortiSwitch ports.



Enterprise/Office Closet Topology

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

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



Grouping FortiSwitches

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

```
config switch-controller switch-group
   edit <name>
      set description <string>
```

```
        set members <serial-number> <serial-number> ...
        end
    end
```

Grouping FortiSwitches 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 FortiSwitches in a group named `my-sw-group`:

```
execute switch-controller restart-swtp my-switch-group
```

Stacking Configuration

The configuration steps for stacking include:

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

1. Configure the Active FortiLink

Configure the FortiLink interface (as described in the FortiLink Configuration section).

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

2. Configure the Standby FortiLink

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

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

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

3. Connect the FortiSwitches

Refer to the topology diagrams to see how to connect the FortiSwitches.

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

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

Disable Stacking

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

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

Firmware upgrade of stacked or tiered FortiSwitches

You can upgrade the firmware of all of your managed FortiSwitches in groups. For example, you can use the following command to update the firmware of all of the FortiSwitches in a stack

```
execute switch-controller stage-swtp-image ALL <firmware-image-file>
```

Use the following command to restart all of the managed FortiSwitches after a 2 minute delay.

```
execute switch-controller restart-swtp-delayed ALL
```

Optional Setup Tasks

This section describes the following tasks:

- Configuring FortiSwitch Management Port
- Converting to FortiSwitch Standalone Mode

Configuring FortiSwitch Management Port

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

Using the Web Administration GUI

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

Using the FortiSwitch CLI

Enter the following commands:

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

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

```
config router static
   edit 1
      set device mgmt
      set gateway 192.168.0.10
      set dst 192.168.0.0 255.255.0.0
   end
end
```

Converting to FortiSwitch Standalone Mode

If a FortiSwitch is operating in managed mode, do the following to convert it to standalone mode.

1. From the switch CLI:

```
config system global
   set mgmt-mode local
end
```

NOTE: FortiSwitch will reboot when you issue the **set mgmt-mode local** command.

2. From the FortiGate, use the web-based manager or CLI to perform the following commands before the switch reboot completes:

Using the Web-based manager

a. Navigate to **WiFi & Switch Controller**> **Managed FortiSwitch**.

b. Right-click on the switch and select **De-authorize**.

Using the CLI

```
config switch-controller managed-switch
   edit <switch-id>
      set fsw-wan1-admin disable
   end
end
```

FortiSwitch features configuration

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

VLAN Configuration

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.)

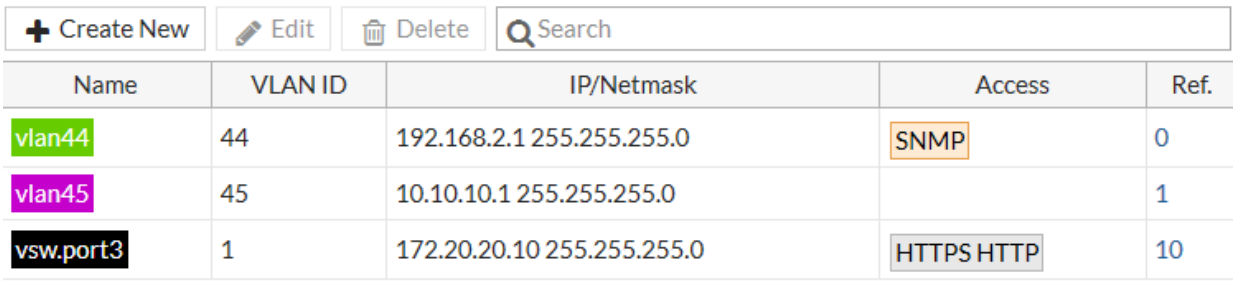
From the FortiGate, you can centrally configure and manage VLANs for the managed FortiSwitches.

In FortiSwitchOS 3.3.0 and later releases, the FortiSwitch supports untagged and tagged frames in Fortilink mode. The switch supports up to 1023 user-defined VLANs. You can assign a VLAN number (ranging from 1-4095) to each of the VLANs.

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

FortiSwitch VLANs Display

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



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

Creating VLANs

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

Using the Web Administration GUI

Creating the VLAN

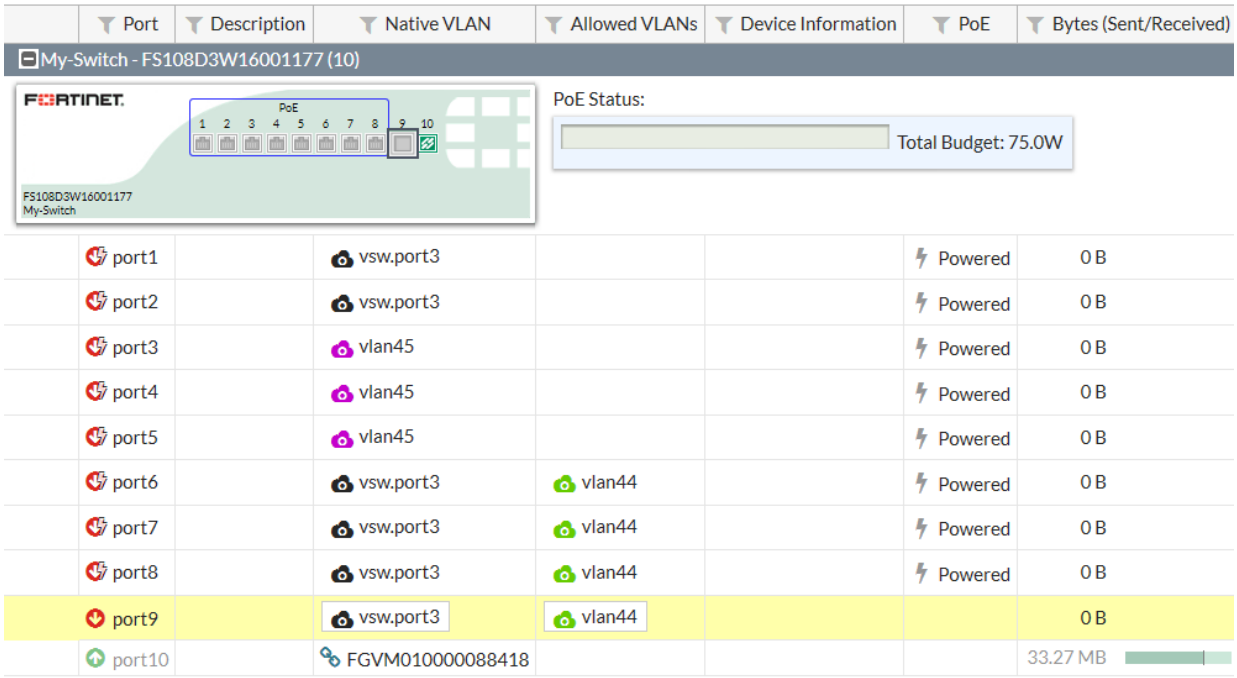
1. Go to **WiFi & Switch Controller > FortiSwitch VLANs**, select **Create New**, and change the following settings:

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

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

Assigning FortiSwitch Ports to the VLAN

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



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
```

Configure MAC Aging Interval

Use the following command to configure the MAC aging interval. The range is 10 to 1,000,000 seconds. After this amount of time, an inactive MAC is aged out.

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

Enable Multiple FortiLink interfaces

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

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

Configure IGMP settings

Use the following command to configure the global IGMP settings.

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

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

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

Configure LLDP Profiles

Use the following command to configure LLDP profiles.

```
config switch-controller lldp-profile
   edit <profile number>
```

```
        set 802.1-tlvs port-vlan-id
        set 802.3-tlvs max-frame-size
        set auto-isl {enable | disable}
        set auto-isl-hello-timer <1-30>
        set auto-isl-port-group <0-9>
        set auto-isl-receive-timeout <3-90>
        set med-tlvs (inventory-management | network-policy)
    end
```

Configure LLDP Settings

Use the following command to configure LLDP settings.

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

Variable	Description
status	Enable or disable
tx-hold	Number of tx-intervals before the local LLDP data expires. Therefore, the packet TTL (in seconds) is **tx-hold** times **tx-interval**. The range for tx-hold is 1 to 16, and the default value is 4.
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.

Create LLDP asset tags for each managed FortiSwitch

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

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

Adding Media Endpoint Discovery (MED) to and LLDP configuration

You can use the following command to add Media Endpoint Discovery (MED) featues to an LLDP profile.

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

Display LLDP information

You can use the following commands to display LLDP information:

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

Configure the MAC sync interval

Use the following command to configure the global xx settings.

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 STP settings

Use the following CLI commands for global STP configuration. This configuration applies to all managed FortiSwitches:

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

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

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

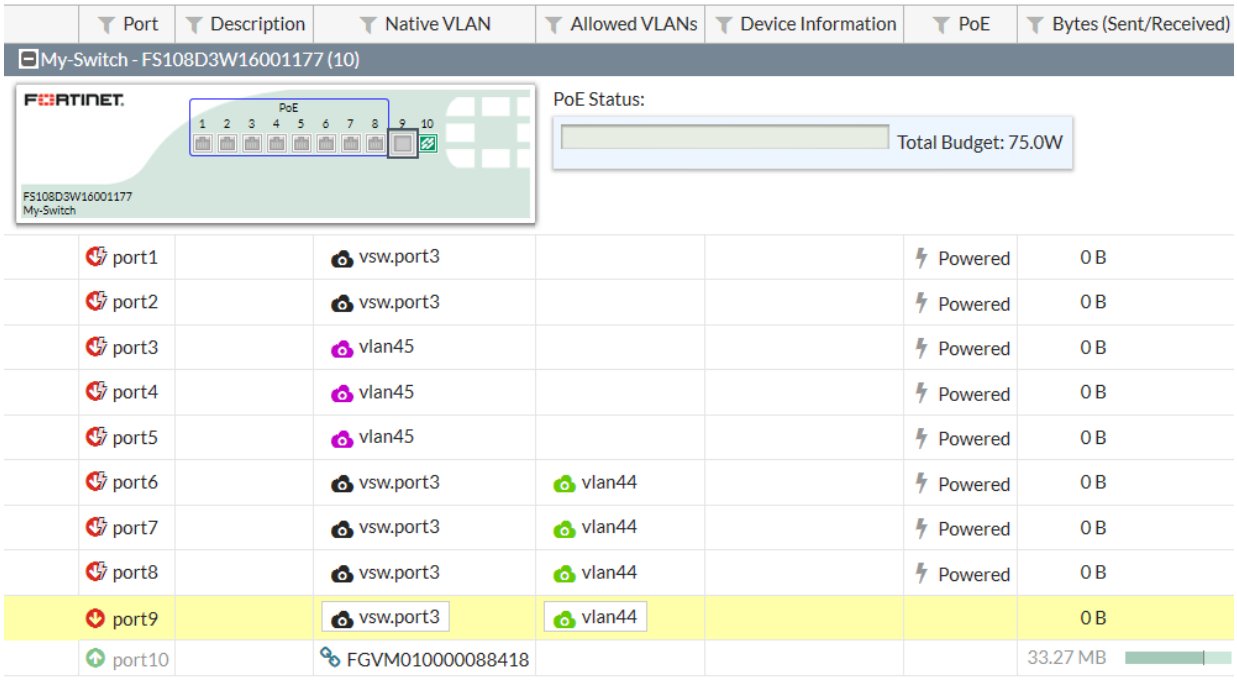
FortiSwitch Port Features

You can configure the FortiSwitch port feature settings from the FortiGate using the FortiSwitch CLI or Web Administration GUI.

FortiSwitch Ports Display

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

The following figure shows the display for a FortiSwitch 108D-POE:

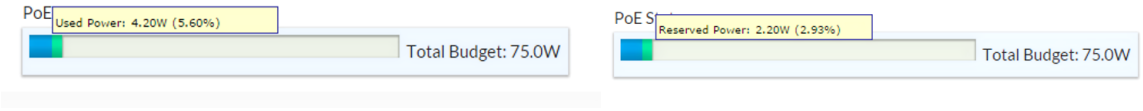


The switch faceplate displays:

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

POE Status displays the total power budget, and the actual power currently allocated.

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



Each entry in the port list displays the following information:

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

Configuring Ports Using the GUI

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

- Set the native VLAN and add more VLANs
- Edit the description of the port
- Enable or disable the port
- Enable or disable PoE for the port
- Enable or disable DHCP blocking (if supported by the port)
- Enable or disable IGMP snooping (if supported by the port)
- Enable or disable STP (if supported by the port)
- Enable or disable loop Guard (if supported by the port)

Configuring Ports Using the FortiGate CLI

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

- Set port speed and administration status
- Configure VLAN on the port (see VLAN Configuration)
- DHCP trust setting
- Enable or disable PoE
- Enable STP on FortiSwitch ports
- LLDP settings
- IGMP settings

Configuring Port Speed and Admin Status

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

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

```
edit <switch>
   config ports
      edit <port>
         set description <text>
         set speed <speed>
         set status {down | up}
```

Configuring DHCP Snooping

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

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set dhcp-snooping {trusted | untrusted}
```

Configuring PoE

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

Enable PoE on the Port

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set poe-status {enable | disable}
```

Reset the PoE port

The following command resets PoE on the port

```
execute switch-controller poe-reset <fortiswitch-id> <port>
```

Display general PoE status

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

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

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

Configuring STP

Starting with FortiSwitch Release 3.4.2, STP is enabled by default for the non-FortiLink ports on the managed FortiSwitches. Use the following commands to enable or disable STP on FortiSwitch ports:

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set stp-state (enabled | disabled)
```

Configuring loop-guard

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

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set loop-guard {enabled | disabled}
```

Configuring LLDP

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

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit <port name>
            set lldp-status (rx-only | tx-only | tx-rx | disable)
            set lldp-profile <profile name>
```

Configuring IGMP

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

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

FortiSwitch port security policy

The features captured here are valuable in end-point authorization and access-control within a retail/enterprise LAN environment. In a Fortilink setup we need the ability to configure these capabilities from the FortiGate while endpoints are connected to switch ports.

End-devices fall into two supported categories: one that supports 8021.x client and one that does not.

Prior to Managed Release 5.6.0, we supported only the following configuration per VLAN:

- Captive Portal
- 802.1x

With Managed Release 5.6.0, we enhance the port security offerings as follows:

- Move 802.1 x control from VLAN to port
  - In the older model, only one VLAN could be assigned to one port. With both tagged and untagged VLAN allowed in 5.4.x this is no longer suitable and will be migrated to the switch port.
  - Automatic customer config migration must be supported.
- Support for client-less devices via mac-auth-bypass (MAB)
  - For devices that are incapable of supporting EAPoL/EAP, FSW will conduct the authentication on behalf of the device. A maximum of three concurrent MAB devices per port exists.
- Multiple secured endpoints on single port
  - Enforce per mac-address based enforcement
- Dynamic VLAN assignment
  - RADIUS assigned VLANs
- Guest VLAN configuration
  - With authentication timeout
- Additional timers and modes
  - Re-auth period
  - Max re-auth attempts
  - Link Down to un-auth

Using the FortiSwitch CLI

NOTE: In the following "*" indicates Default.

Global Settings Applied across the Network

```
config switch-controller 802.1x-settings
   set reauth-period < int >
   set max-reauth-attempt < int >
   set link-down-auth < *set-unauth | no-action >
end
```

Local Switch Overrides

```
config switch-controller managed-switch
   edit < switch >
      config 802.1x-settings
         set local-override [ enable | *disable ]
         set reauth-period < int >                  // visable if override enabled
         set max-reauth-attempt < int >             // visable if override enabled
         set link-down-auth < *set-unauth | no-action >   // visable if override enabled
      end
   next
end
```

Policy Definitions (802.1x,captive-portal,and dynamic-discovery)

```
config switch-controller security-policy 802.1x
   edit < policy.name >  // limited to 1 policy
      set user-group <user.group>
      set mac-auth-bypas [ enable | *disable ]
      set guest-vlan [ enable | *disable ]
      set guest-vlanid <vlan-id>
      set guest-auth-delay < int >
      set auth-fail-vlan  [ enable | *disable ]
      set auth-fail-vlanid [ vlan-id ]
      radius-timeout-overwrite [ enable | *disable ]
   end
end


config switch-controller security-policy captive-portal
   edit < policy.name >
      set vlan < vlan.id >
      config users
         edit <1..x>
            set user-group <user.group>
            set vlanid < vlan >
         next
      end
   end
end


config switch-controller security-policy dynamic-discovery
   edit < policy.name >  // limited to 1 policy
      set identification-timeout <int>
      set discovery-vlan <vlan.id>
      set quarantine-vlan <vlan.id>
      edit <entry>
         set user-group <group.id>
         set device-group <group.id>
         set vlanid <vlan>
      next
   end
end
// user-group or device-group must be set, but one can be empy.
// vlanid is always required
```

Port Settings

```
config switch-controller managed-switch
   edit <managed-switch>
      config ports
         edit <port>
            set port-security-policy < 802.1x-policy | captive-portal-policy | dynamic-
                device >
         next
      end
   next
end
```

Additional Capabilities

Execute Custom FortiSwitch Commands

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

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

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

Create a command

Use the following syntax to create a command file:

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

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

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

Execute a command

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

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

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

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

Firmware upgrade management and compatible version information

You can view the current firmware version of a FortiSwitch and upgrade the FortiSwitch to a new firmware version.

Using the FortiGate web interface

To view the FortiSwitch firmware version:

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

To update the FortiSwitch firmware version:

4. Click **Update** to open the **Update Firmware panel**.
5. Click **Select File**. In the file chooser, click the image file and click **Open**.
6. Click **Upload and Reboot** to install the new image and reboot the FortiSwitch.

Using the CLI command interface

Use the following command to display the latest version:

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

Use the following command to download the image:

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

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

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

diagnose fdsm fortisw-download 03004000FIMG0900904002

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

FortiSwitch Log export

You can enable/disable the managed FortiSwitches to export their syslogs to the FortiGate. The setting is global, and the default setting is disabled.

To allow a level of filtering, FortiGate sets the user field to "fortiswitch-syslog" for each entry.

CLI Command Syntax:

```
config switch-controller switch-log
   set status (enable | disable)
   set severity [ emergency | alert | critical | error | warning | notification |
       *information | debug ]
end
```

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

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

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

FortiSwitch Per-Port Device Visibility

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

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

```
diagnose switch-controller dump mac-hosts_switch-ports
```

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

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

Configuring a Link Aggregation Group (LAG)

You can configure a Link Aggregation Group (LAG) for non-fortilink ports on a FortiSwitch. You cannot configure ports from different FortiSwitches in one LAG.

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

Configuring Storm Control

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

When the data rate exceeds the configured threshold, storm control drops excess traffic. You can configure the types of traffic to drop: broadcast, unknown unicast, or multicast.

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

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

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

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

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

Display Port Statistics

Port stats will be accessed via FSW REST Monitor API.

Configuring DHCP Snooping

Configure FortiSwitch trusted or un-trusted DHCP snooping interface.

```
config switch-controller managed-switch
   edit <switch-id>
      config ports
         edit port1
            set dhcp-snooping (trusted | untrusted)
         end
```

Troubleshooting

If the FortiGate does not establish the Fortilink connection with the switch, perform the following troubleshooting checks.

Troubleshooting FortiLink Issues

Check the FortiGate configuration

Using the FortiGate GUI, check the FortiLink interface configuration:

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

Using the FortiGate CLI, verify that you have configured the DHCP and NTP settings correctly with the following commands:

1. Verify that the NTP server is enabled, and that the Fortilink interface has been added to the list:

```
show system ntp
```

2. Ensure that the DHCP server on the Fortilink interface is configured correctly:

```
show system dhcp
```

Check the FortiSwitch configuration

Use the following FortiSwitch CLI commands to check the FortiSwitch configuration:

1. Verify that the switch system time matches the time on the FortiGate:

```
get system status
```

2. Verify that FortiGate has sent an IP address to the FortiSwitch (anticipate an IP address in the range 169.254.x.x):

```
get system interfaces
```

3. Verify that you can ping the FortiGate IP address:

```
exec ping x.x.x.x
```

Scenarios

This chapter contains practical examples of how to use the FortiSwitch unit to manage a network.

The scenarios are as follows:

- Scenario 1: Creating the marketing VLAN
- Scenario 2: Allowing access to specific users on the marketing VLAN
- Scenario 3: Adding a specific device to the marketing VLAN
- Scenario 3: Accessing the marketing VLAN remotely using an SSL VPN
- Scenario 4: Configuring the accounting VLAN using an SFP port
- Scenario 5: Connecting a VoIP phone to the FortiSwitch
- Scenario 6: Connecting a FortiAP unit to the FortiSwitch

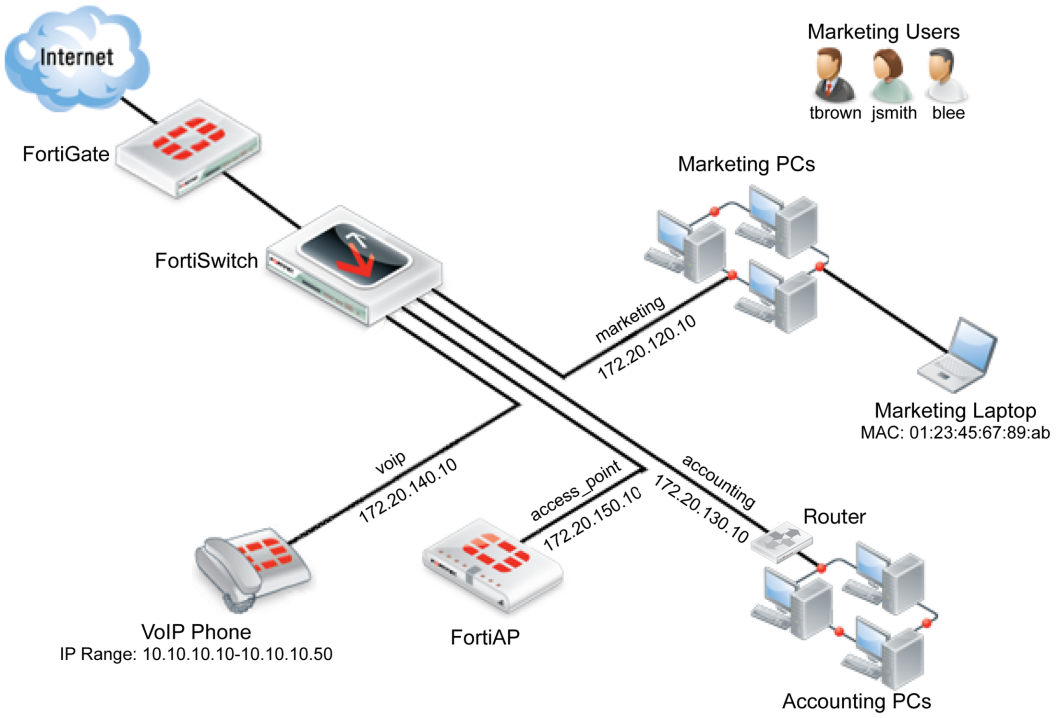
The Example Network

All the scenarios are interrelated and are used to manage an example network with the following attributes:

- The FortiSwitch unit used is a FortiSwitch-224D-POE, serial number FS224D3W14000370.
- The FortiSwitch unit's port 24 connects to port1 on the FortiGate unit.
- The LAN is divided into four distinct VLANs, configured as follows:

VLAN	IP	Device(s)	Port(s)	Policy ID(s)	GUI Color
marketing	172.20.120.10/255.255.255.0	marketing PCs, marketing laptop	3-6	2, 3	
accounting	172.20.130.10/255.255.255.0	accounting PCs	21	4	
voip	172.20.140.10/255.255.255.0	VoIP phone	10	5	
access_ point	172.20.150.10/255.255.255.0	FortiAP	1	6	

- Six devices directly connect to the FortiSwitch unit's ports using Ethernet cables: the 3 marketing PCs, the marketing laptop, the VoIP phone, and the FortiAP unit.
- The accounting VLAN connects to the FortiSwitch using an SFP port.
- Three marketing employees (Jane Smith, Tom Brown, Bob Lee) employ the marketing PCs to apply the marketing VLAN.
- The MAC address of the marketing laptop is 01:23:45:67:89:ab.
- The IP range for the VoIP phone is 10.10.10.10-10.10.10.50.
- The FortiAP unit is a FortiAP-11C, serial number FAP11C3X12000412.



Scenario 1: Creating the Marketing VLAN

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).

For example, if a company has one LAN which is to be used for both the marketing and the accounting department, this LAN can be segmented into two VLANs. This allows the traffic from each department to be isolated, so information packets sent to the marketing department are only sent on the marketing VLAN. It also allowed different policies to be created, so that security can be increased for the accounting department without also increasing it for the marketing department.

The following instructions will create a VLAN to be used by the marketing team for network and Internet access. The marketing team PCs will connect to ports 3-6 on the FortiSwitch.

Using the Web Administration GUI

Creating the VLAN

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

Interface Name	marketing
VLAN ID	Enter a number (1-4094)

Color	Choose a unique color for each VLAN, for ease of visual display.
IP/Network Mask	172.20.120.10/255.255.255.0

1. Enable **DHCP Server.** Set the IP range to 172.20.120.11-172.20.120.254.
2. Select **OK**.

The entry **marketing** is now shown on the list of **VLANs**. A **marketing** interface has also been added, which is visible by selecting **Network > Interfaces**.

Assigning FortiSwitch Ports to the VLAN

1. Go to **WiFi & Switch Controller**>**FortiSwitch Ports**.
2. Click the rows for ports 3-6 to select them.
3. Right-click and select **Assign VLANS**>**Native VLAN**. Select a VLAN from the list.
   Ports 3-6 on the FortiSwitch have now been assigned to the selected VLAN and will appear in red.

Using the CLI

1. Create the marketing VLAN.

```
config switch-controller vlan
   edit marketing
      set vlanid 4
      set color 32
end
```

2. Set the VLAN's IP address.

```
config system interface
   edit marketing
      set ip 172.20.120.14 255.255.255.0
end
```

3. Enable a DHCP Server.

```
config system dhcp server
   edit 1
      set default-gateway 172.20.120.10
      set dns-service default
      set interface marketing
         config ip-range
            set start-ip 172.20.120.11
            set end-ip 172.20.120.254
         end
      set netmask 255.255.255.0
end
```

4. Assign ports 3-6 to the VLAN.

```
config switch-controller managed-switch
   edit FS224D3W14000370
      config ports
         edit port3
            set vlan marketing
         next
         edit port4
```

```
            set vlan marketing
          next
          edit port5
            set vlan marketing
          next
          edit port6
            set vlan marketing
          next
        end
    end
```

Setting up a Security Policy for the VLAN

The following instructions configure a basic security policy for the marketing VLAN that will allow all traffic from the marketing VLAN to have access to the Internet.

Using the Web Administration GUI

1. Go to **Policy & Objects**>**IPv4 Policy**, select **Create New**, and change the following settings:

Incoming Interface	marketing
Source	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Enable
Fixed Port	
IP Pool Configuration	
Security Profiles	
Logging Options	Log all Sessions

2. Select **OK**.

With this security policy set, all computers connected to the marketing VLAN can now access the Internet.

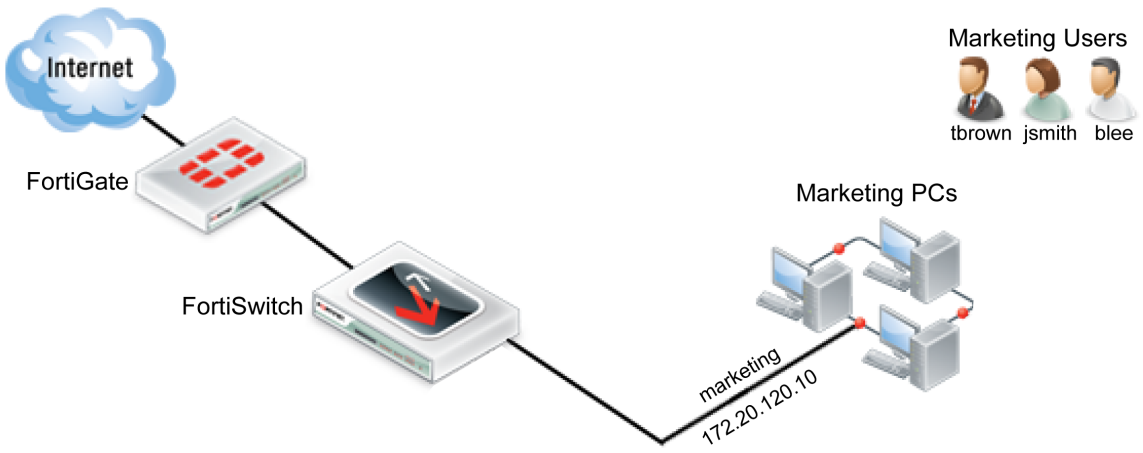
Using the CLI

Create a security policy for the marketing VLAN.

```
config security policy
   edit 2
      set srcintf marketing
      set dstintf wan1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
      set logtraffic all
      set nat enable
end
```

Scenario 2: Allowing Access to Specific Users on the Marketing VLAN

In Scenario 1, the policy for the marketing VLAN will be altered so that different users have different access. The firewall policy will be created so that all three marketing employees (Jane Smith, Tom Brown, Bob Lee) have user accounts. These accounts will be put into one of two groups: full-time and part-time. Full-time employees will always have network access, while part-time employees will only have access on Mondays, Wednesdays and Fridays. This policy will apply to each user when they use any of the PCs that connect to the marketing VLAN through ports 3, 4, 5 or 6 on the FortiSwitch.



Creating a policy to match scenario 1 requires:

- Creating users.
- Creating groups.
- Creating a schedule.
- Configuring the firewall policies.

Using the Web Administration GUI

Creating a User Group

1. Go to **User & Device**>**User Groups** and select **Create New**.
2. Name the user group **part-time**.
3. Set **Type** as **Firewall**.
4. Select **OK**.

The entry **part-time** will now appear on the user group list. Repeat these steps to create another user group, named **full-time**.

Creating a User

1. Go to **User & Device**>**User Definition**. Select **Create New**.
2. Use the **User Creation Wizard** to create a user. In part 1, select **Local User**.
3. In part 2, change the following settings:

User Name	blee
Password	password

4. In part 3, enter the email address blee@example.com.
5. In part 4, select **Enable** and **User Group**. Set **part-time** as the group.
6. Select **Done**.

The entry **blee** will now appear in the user list. Repeat these steps to create user accounts **tbrown** and **jsmith** and add both of these accounts to the **full-time group**.

Creating a Schedule

1. Go to **Policy & Objects**> **Schedules**. Select **Create New** and then select **Recurring**.
2. Change the following settings:

Name	part-time_schedule
Day of the Week	Monday, Wednesday, Friday

3. Select **OK**.

The entry **part-time schedule** will now appear on the schedules list.

Configuring the Firewall Policy

1. Go to **Policy & Objects**>**IPv4 Policy** and select the policy for the marketing VLAN. Select **Edit**.
2. Set the policy to use the following the following settings, allowing access for part-time employees:

Incoming Interface	marketing

Source Address	all
Source User(s)	part-time
Outgoing Interface	wan1
Destination Address	all
Schedule	part-time_schedule
Service	ALL
Action	ACCEPT
Enable NAT	Enable
Logging Options	Log all Sessions

3. Select **OK**.
4. Go to **Policy & Objects**>**IPv4 Policy** and create a new policy.
5. Change the following settings to set access for full-time employees:

Incoming Interface	marketing
Source Address	all
Source User(s)	full-time
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Enable
Logging Options	Log all Sessions

6. Select **OK**.

You have now finished creating the policies that matches scenario 1. These policies will apply to all three users when they use any of the PCs that connect to the marketing VLAN.

Using the CLI

1. Create the 3 users.

```
config user local
   edit blee
      set type password
      set passwd password
   next
```

```
   edit tbrown
      set type password
      set passwd password
   next
   edit jsmith
      set type password
      set passwd password
end
```

2. Create the 2 user groups and add the users to them.

```
config user group
   edit part-time
      set group-type firewall
      set member blee
next
   edit full-time
      set group-type firewall
      set member tbrown jsmith
end
```

3. Create the schedule for part-time employees.

```
config firewall schedule recurring
   edit part-time_schedule
      set day monday wednesday friday
end
```

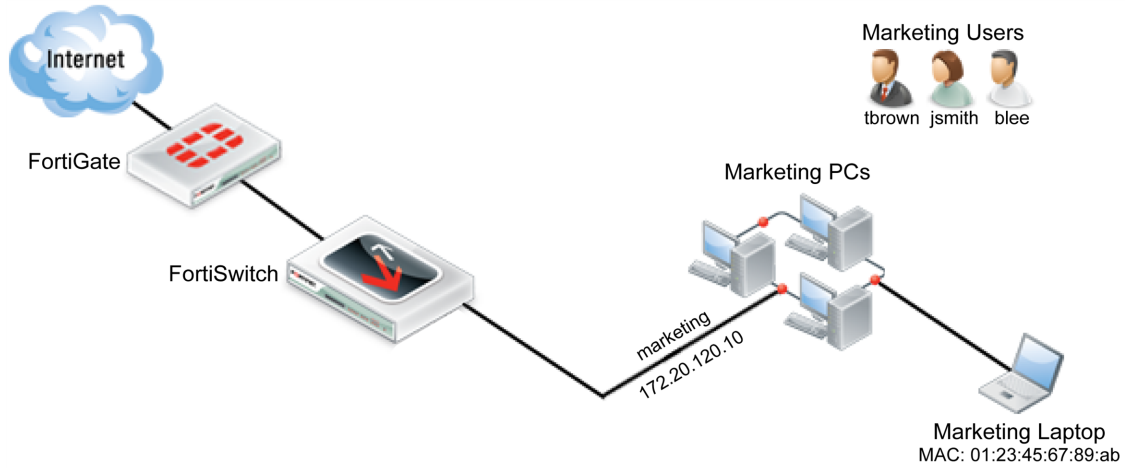
4. Add user authentication to the firewall policy for the marketing VLAN.

```
config firewall policy
   edit 2
      set identity-based enable
         config identity-based-policy
            edit 1
               set schedule part-time_schedule
               set logtraffic all
               set groups part-time
               set dstaddr all
               set service ALL
            next
            edit 2
               set schedule always
               set logtraffic all
               set groups full-time
               set dstaddr all
               set service ALL
         end
end
```

Scenario 3: Adding a specific device to the marketing VLAN

In Scenario 2, a new policy will be created for the marketing VLAN that will be used by the marketing laptop. This policy will affect the marketing laptop that is used periodically for tasks such as boardroom presentations or for guests, tasks for which the laptop requires Internet access. The laptop will access the Internet by connecting to

the marketing VLAN through ports 3, 4, 5 or 6 on the FortiSwitch. Adding a new policy for the laptop will allow it to connect without requiring user authentication and will also limit the scope of the device's access.



Creating a policy to match scenario 2 requires:

- Assigning a reserve IP to the laptop.
- Creating a firewall address for the reserve IP.
- Creating a firewall policy that uses the reserve IP.

Using the Web Administration GUI

Assigning a Reserve IP to the Laptop

1. Go to **Network>Interfaces** and select **marketing**.
2. Under **DHCP Server**, expand the **Advanced** options.
3. In the **MAC Address Access Control List** and select **Create New**.
4. Change the following settings:

MAC	01:23:45:67:89:ab
IP	172.20.120.254
Action	Reserve IP

Creating a Firewall Address for the Reserve IP

1. Go to **Policy & Objects>Addresses** and select **Create New**.
2. Change the following settings:

Category	Address
Name	marketing_laptop

Type	IP/Netmask
Subnet/IP Range	172.20.120.254
Interface	marketing

Configuring a Firewall Policy

1. Go to **Policy & Objects>IPv4 Policy** and select **Create New**.
2. Change the following settings:

Incoming Interface	marketing
Source Address	marketing_laptop
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	HTTP HTTPS DNS
Action	ACCEPT
Enable NAT	Enabled
Logging Options	Log all Sessions

3. Select **OK.**
4. In the policy list, select the column on the far left for the new policy (usually **Seq #)** and drag the policy above the previous policy for the marketing VLAN. This will ensure that the laptop will be identified through this policy.

You have now finished creating a policy that matches scenario 2. This policy will apply to anyone who uses the laptop to connect to the **marketing** VLAN using an Ethernet cable.

Using the CLI

1. Assign a reserve IP to the laptop.

```
config system dhcp server
   edit 2
      config reserved-address
         edit 1
            set action reserved
            set ip 172.20.120.254
            set mac 01:23:45:67:89:ab
      end
end
```

2. Create a firewall address for the reserve IP.

```
config firewall address
   edit marketing_laptop
      set subnet 172.20.120.254
end
```

3. Create a firewall policy for the marketing VLAN that uses the reserve IP.

```
config firewall policy
   edit 3
      set srcintf marketing
      set dstintf wan1
      set srcaddr marketing_laptop
      set dstaddr all
      set action accept
      set schedule always
      set service HTTP HTTPS DNS
      set logtraffic all
      set nat enable
end
```

4. Place the new firewall policy at the top of the policy list.

```
config firewall policy
   move 2 after 3
end
```

Scenario 3: Accessing the Marketing VLAN Remotely using an SSL VPN

In Scenario 4, a policy is created to allow remote access to the marketing VLAN, using a virtual private network (VPN) tunnel. This policy will allow marketing employee Tom Brown to connect to the marketing VLAN remotely from his home. The default IP Pool, **SSLVPN_TUNNEL_ADDR1**, will be used to configure the SSL VPN web portal. The computer Tom Brown is using to access the network remotely has a dynamic IP address and will be using the FortiClient application to auto connect to the VPN tunnel. To maintain security, split tunneling will be disabled. This policy will be used whenever Tom Brown accesses the marketing VLAN remotely.

Creating a policy to match scenario 2 requires:

- Creating a user group.
- Creating a firewall address for the marketing VLAN.
- Creating an SSL VPN portal.
- Creating a SSL VPN firewall policy for the marketing VLAN.

Using the Web Administration GUI

Creating a User Group

1. Go to **User & Device** > **User**>**User Groups** and select **Create New**.
2. Name the Group **remote access**.
3. Set **Type** as **Firewall**.
4. Highlight **tbrown** on the **Available Users** list.
5. Select the right-pointing arrow to move **tbrown** to the **Members** list.
6. Select **OK**.

The entry **remote access** will now appear on the **Group** list, with **tbrown** listed under **Members**.

Creating a Firewall Address for the marketing VLAN

1. Go to **Policy & Objects**>**Objects**>**Addresses** and select **Create New**. Change the following settings:

Address Name	marketing VLAN
Type	Subnet
Subnet/IP Range	172.20.120.14/255.255.255.0
Interface	marketing

2. Select **OK**.

Creating an SSL VPN Portal

1. Go to **VPN**>**SSL**>**Portals** and select **Create New**. Change the following settings:

Name	marketing-remote
Enable Tunnel Mode	Enable
Enable Split Tunneling	Disable
IP Pools	SSLVPN_TUNNEL_ADDR1
Enable Web Mode	Enable

2. Select **Apply**.

Creating a Firewall Policy

1. Go to **Policy & Objects**>**Policy>IPv4** and select **Create New.**
2. Change the following settings to allow Tom Brown to access the marketing VLAN:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	marketing_laptop
Outgoing Interface	marketing
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Enabled
Logging Options	Log all Sessions

3. Select **OK**.
4. Go to **Policy & Objects**>**Policy>IPv4** and create a second policy.
5. Change the following settings to allow Tom Brown to access the Internet through the FortiGate:

Incoming Interface	ssl.root (sslvpn tunnel interface)
Source Address	marketing_laptop
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	HTTP HTTPS DNS
Action	ACCEPT
Enable NAT	Enabled
Logging Options	Log all Sessions

6. Select **OK**.

The FortiClient SSL VPN tunnel client will also need to be configured, in order for the Tom Brown to connect to the SSL VPN tunnel.

You have now finished creating a policy that matches scenario 4. This policy will be used whenever Tom Brown accesses the marketing VLAN remotely.

Using the CLI

1. Create the user group for remote users.

```
config user group
   edit remote-access
      set group-type firewall
      set member tbrown
end
```

2. Create a firewall address for the marketing VLAN.

```
config firewall address
   edit marketing_VLAN
      set associated-interface marketing
      set subnet 172.20.120.14 255.255.255.0
end
```

3. Create the SSL VPN web portal.

```
config vpn ssl web portal
   edit marketing-remote
      set allow-access web ftp ssh
      config widget
         edit 1
```

```
            set type tunnel
            set split-tunneling disable
            set ip-pools SSLVPN_TUNNEL_ADDR1
            set auto-connect enable
        end
end
```

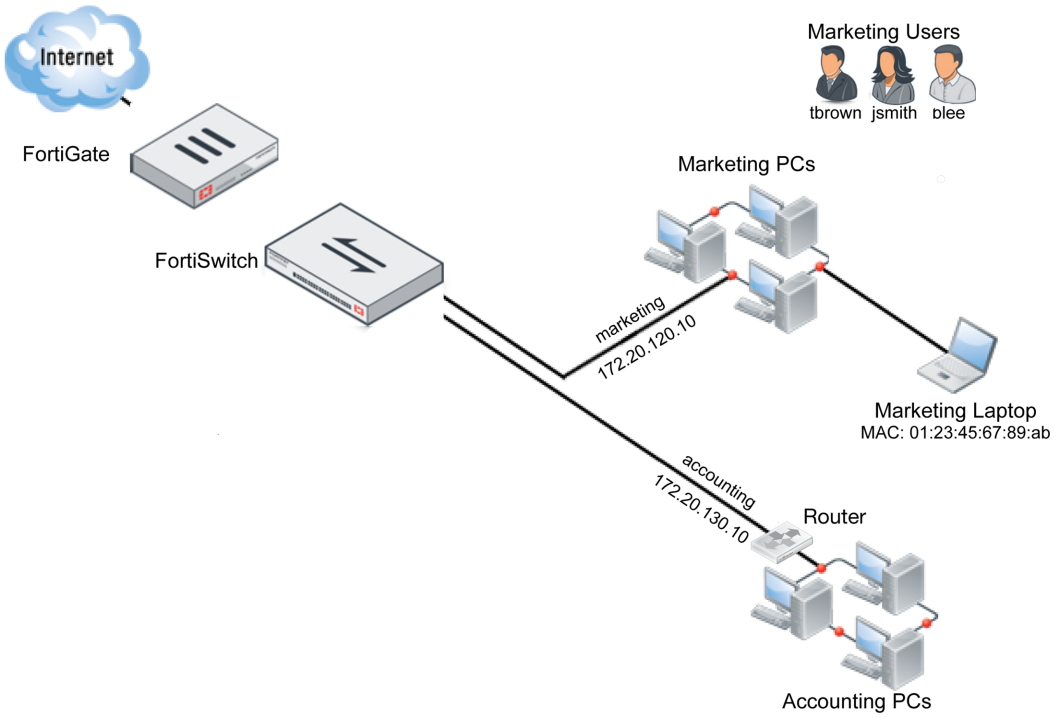
4. Create a firewall policy to allow remote access to the marketing VLAN.

```
config firewall policy
   edit 3
      set srcintf wan1
      set dstintf marketing
      set dstaddr marketing_VLAN
      set action ssl-vpn
      set identity-based-policy
      config identity-based-policy
         set schedule always
         set groups remote_access
         set users tbrown
         set sslvpn-portal marketing-remote
      end
end
```

Scenario 4: Configuring the Accounting VLAN using an SFP Port

The SFP ports should only be used to connect UL-listed optical transceiver products, rated Laser Class 1.33V DC.

In Scenario 4, a second VLAN will be created on the FortiSwitch, to be used for the accounting department. This VLAN will connect to the FortiSwitch unit using a copper SFP receiver that has been installed in the FortiSwitch. Due to the sensitive nature of information within the accounting network, the firewall policy that controls traffic to this network uses the default profile for all security features.



Creating an interface to match scenario 4 requires:

- Creating and assigning a VLAN.
- Configuring a firewall policy.

SFP ports are only available on certain FortiSwitch models. SFP ports are also shared with Ethernet ports and so when an SFP port is used, the Ethernet port with the same number cannot be.

Using the Web Administration GUI

Creating and Assigning the VLAN

1. Go to **WiFi & Switch Controller**>**Switch Network**>**Virtual Switch** and select **Create New**. Change the following settings:

Name	accounting
Color	
IP/Network Mask	172.20.130.15/255.255.255.0

2. Select **OK**.
3. Go to **WiFi & Switch Controller**>**Managed Devices**>**Managed FortiSwitch** and assign FortiSwitch **port 21** to **accounting**.

Configuring the Firewall Policy

1. Go to **Policy & Objects**>**Policy>IPv4**, select **Create New**, and change the following settings:

Incoming Interface	accounting
Source Address	all
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Enabled
Logging Options	Log all Sessions

2. Enable the following Security Profiles and set them to use the **default** profile: **AntiVirus**, **Web Filter**, **Application Control**, **IPS**, **Email Filter**, **DLP Sensor**, and **SSL/SSH Inspection**.
3. Select **OK**.

You have now finished creating a policy that matches scenario 5. This policy will be used for all traffic on the accounting VLAN.

Using the CLI

1. Create the accounting VLAN.

```
config switch-controller vlan
   edit accounting
      set color 32
end
```

2. Set the VLAN's IP address.

```
config system interface
   edit marketing
      set ip 172.20.130.15 255.255.255.0
end
```

3. Assign the accounting VLAN to port 21.

```
config switch-controller managed-switch
   edit FS224D3W14000370
      config ports
         edit port21
            set vlan accounting
      end
end
```

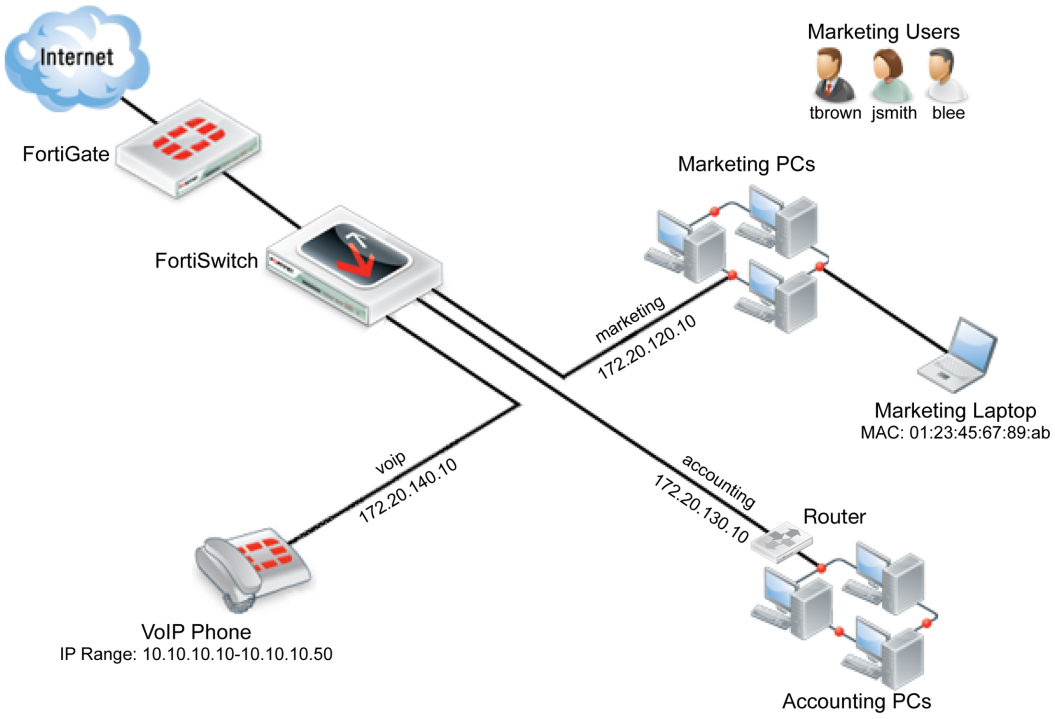
4. Create a firewall policy for the accounting VLAN that uses the default security profiles.

```
config firewall policy
   edit 4
```

```
        set srcintf accounting
        set dstintf wan1
        set srcaddr all
        set dstaddr all
        set action accept
        set schedule always
        set service ALL
        set logtraffic all
        set nat enable
        set av-profile default
        set webfilter-profile default
        set spamfilter-profile default
        set dlp-sensor default
        set ips-sensor default
        set application-list default
        set profile-protocol-options default
        set deep-inspection-options default
end
```

Scenario 5: Connecting a VoIP Phone to the FortiSwitch

In Scenario 5, an interface will be configured to use a Voice over IP (VoIP) phone. This VoIP phone will be assigned the IP range 10.10.10.10-10.10.10.50 and connect to the FortiSwitch unit through port 10 using an Ethernet cable. The FortiGate unit's default VoIP profile will be used.



Creating an interface to match scenario 5 requires:

- Creating and assigning a VLAN.
- Creating a firewall address for the VoIP phone.

- Configuring a firewall policy.

Using the Web Administration GUI

Creating and Assigning the VLAN

1. Go to **WiFi & Switch Controller**>**Switch Network**>**Virtual Switch** and select **Create New**. Change the following settings:

Name	voip
Color	
IP/Network Mask	172.20.140.16/255.255.255.0

2. Select **OK**.
3. Go to **WiFi & Switch Controller**>**Managed Devices**>**Managed FortiSwitch** and assign FortiSwitch **port10** to **voip**.

Creating a Firewall Address

1. Go to **Policy & Objects**>**Objects**>**Addresses** and select **Create New**. Change the following settings:

Category	Address
Name	voip
Color	
Type	IP Range
Subnet/IP Range	10.10.10.10-10.10.10.50
Interface	voip

2. Select **OK**.

Create a Firewall Policy

1. Go to **Policy & Objects>Policy>IPv4** and select **Create New**. Change the following settings:

Incoming Interface	voip
Source Address	voip_phone
Outgoing Interface	wan1
Destination Address	all
Schedule	always

Service	SIP
Action	ACCEPT
Enable NAT	Enabled
Logging Options	Log all Sessions

2. Go to **Policy & Objects**>**Policy>IPv4** and select **Create New**. Change the following settings:
3. Enable the **VoIP** Security Profile and set it to **default**.

You have now finished creating a policy that matches scenario 6.

Using the CLI

1. Create the voip VLAN.

```
config switch-controller vlan
   edit voip
      set color 25
end
```

2. Set the VLAN's IP address.

```
config system interface
   edit marketing
      set ip 172.20.140.16 255.255.255.0
end
```

3. Assign the voip VLAN to port 10.

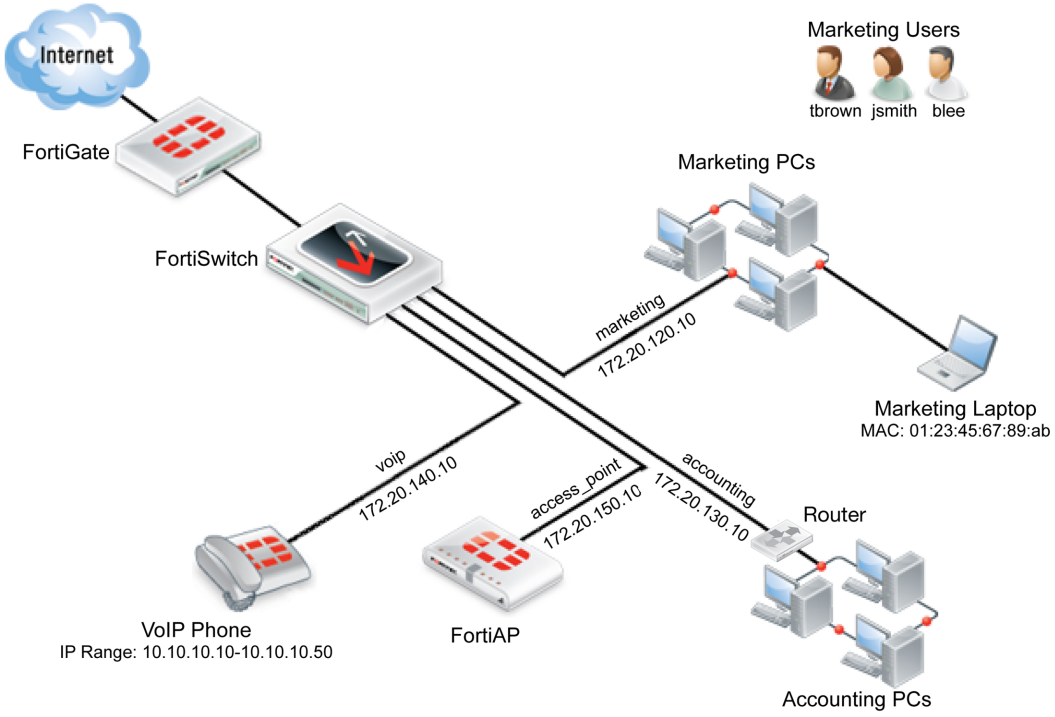
```
config switch-controller managed-switch
   edit FS224D3W14000370
      config ports
         edit port10
            set vlan voip
      end
end
```

4. Configure the firewall policy.

```
config firewall policy
   edit 5
      set srcintf voip
      set dstintf wan1
      set srcaddr voip_phone
      set dstaddr all
      set action accept
      set schedule always
      set service SIP
      set logtraffic all
      set nat enable
      set voip-profile default
end
```

Scenario 6: Connecting a FortiAP unit to the FortiSwitch

In Scenario 6, an interface will be configured to use a FortiAP unit that will provide wireless Internet access.



Creating an interface to match scenario 6 requires:

- Creating and assigning a VLAN.
- Authorizing the FortiAP unit.
- Creating an SSID.
- Creating a firewall address.
- Configuring a firewall policy.

The WiFi network provided by the access point will use the marketing schedule and allow HTTP and HTTPS traffic.

Using the Web Administration GUI

Creating and Assigning the VLAN

1. Go to **WiFi & Switch Controller**>**Switch Network**>**Virtual Switch** and select **Create New**. Change the following settings:

Name	access_point
Color	

IP/Network Mask	172.20.150.17/255.255.255.0
DHCP Server	Enable

2. Select **OK**.
3. Go to **WiFi & Switch Controller**>**Managed Devices**>**Managed FortiSwitch** and assign FortiSwitch **port1** to **access_point**.

Authorizing the FortiAP unit

1. Go to **WiFi & Switch Controller>Managed Devices > Managed FortiAPs**.
2. Right-click on the FortiAP unit and select **Authorize**.

A icon with a checkmark now appears in the Status column.

Creating an SSID

1. Go to **WiFi & Switch Controller>WiFi Network>SSIDs** and select **Create New**.
2. Change the following settings:

Name	WLAN
Type	WiFi SSID
Traffic Mode	Tunnel to Wireless Controller
IP/Network Mask	172.20.150.17/255.255.255.0
DHCP Server	Enabled
SSID	wireless
Pre-shared Key	password

3. Select **OK**.

Create a Firewall Policy

1. Go to **Policy & Objects**>**Policy>IPv4** and select **Create New**.
2. Change the following settings:

Incoming Interface	access_point
Outgoing Interface	wan1
Destination Address	all
Schedule	always
Service	HTTP HTTPS DNS
Action	ACCEPT

Enable NAT	Enabled
Logging Options	Log all Sessions

3. Select **OK**.
4. Go to **WiFi & Switch Controller>Managed Devices>Managed FortiAPs**. The Status icon now appears in green, showing that the FortiSwitch unit is online.

You have now finished creating a policy that matches scenario 7.

Using the CLI

1. Create the access_point VLAN.

```
config switch-controller vlan
   edit access_point
      set color 7
end
```

2. Assign the access_point VLAN to port 1.

```
config switch-controller managed-switch
   edit FS224D3W14000370
      config ports
         edit port1
            set vlan access_point
      end
end
```

3. Set the interface IP and enable CAPWAP.

```
config system interface
   edit access_point
      set ip 172.20.150.17
      set allowaccess capwap
end
```

4. Enable the FortiAP unit.

```
config wireless-controller wtp
   edit FAP11C3X13000412
      set admin enable
end
```

5. Create an SSID for the FortiAP unit.

```
config wireless-controller vap
   edit WLAN
      set ssid wireless
      set passphrase password
end
```

6. Configure the firewall policy.

```
config firewall policy
   edit 6
      set srcintf access_point
      set dstintf wan1
      set srcaddr all
      set dstaddr all
```

```
        set action accept
        set schedule always
        set service HTTP HTTPS DNS
        set logtraffic all
        set nat enable
    end
```

FORTINET

High Performance Network Security