FORTINET®

High Performance Network Security

ADMINISTRATION GUIDE

Managing a FortiSwitch unit with a FortiGate

for FortiOS 5.2 and FortiSwitchOS 3.x

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

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

FORTINET®

Thursday, October 15, 2015

Managing a FortiSwitch unit with a FortiGate

for FortiOS 5.2 and FortiSwitchOS 3.x

TABLE OF CONTENTS

Change Log

Date	Change Description
April 20, 2015	Initial document release (FortiOS 5.2.1 and FortiSwitchOS 3.0.1)
June 11, 2015	Updated the list of supported FortiSwitch models. Included tables to list the FortiLink ports for each switch model and gateway model.
July 9, 2015	Updates for FortiOS 5.2.3
July 17, 2015	Correction in setup section. FortiLink enhancements in FortiSwitch 3.3.0 are only available when the FortiGate uses FortiOS 5.4
July 22, 2015	Correction in setup section: Last port on FS-224D-FPOE is port 28
Sept 18, 2015	Corrections to supported FortiGate list on page 6: each of the listed FortiSwitches supports the "FGT-Models1" list of FortiGate models.
Oct 8, 2015	Corrrections to setting up FortiLink from the FortiGate GUI.
Oct 15, 2015	Corrected the Firewall User Identity policy CLI syntax in scenarios 1 and 3

Introduction

This document describes how to use FortiGate to remotely manage FortiSwitch units, which is also known as using a FortiSwitch in FortiLink mode. FortiLink defines the management interface and the remote management protocol between the FortiGate and FortiSwitch.

FortiGate supports remote management for up to 16 FortiSwitches.

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.

FortiSwitch	FortiGate	Earliest FortiSwitchOS	Earliest FortiOS
FS-224D-POE	FGT-90D(Wifi/poe) + FGT-Models1	3.0.0	5.2.2
FS-108D-POE	FGT-60D(all) + FGT-Models1	3.0.1	5.2.3
FSR-112D-POE	FGR-90D + FGT-Models1	3.0.1	5.2.3
FS-124D	FGT-90D + FGT-60D + FGT-Models1	3.0.1	5.2.3
FS-124D-POE	FGT-90D + FGT-60D + FGT-Models1	3.0.1	5.2.3
FS-224D-FPOE	FGT-90D + FGT-60D + FGT-Models1	3.0.1	5.2.3

FortiGate models 1 includes the following: 100D/200D/240D/140D(POE, T1),280D(POE)/600C/800C/1000C

Before You Begin

Before you set up remote management of your FortiSwitch unit, certain assumptions have been made in the writing of this manual:

- 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:

Getting Started - describes how to configure the FortiGate for remote management of the FortiSwitch units.

VLAN Configuration - configure VLANs from the FortiGate unit.

Port Configuration - configure Ports from the FortiGate unit.

Scenarios - contains practical examples of how to use the FortiGate unit to manage a network of FortiSwitches.

Getting Started

This chapter describes how to configure the FortiGate to provide remote management for FortiSwitch units.

The FortiGate requires a one-time configuration task to enable the Switch Controller on the FortiGate.

Adding a new managed FortiSwitch is very simple. You connect a cable from a port on the FortiGate to the designated FortiLink port on the FortiSwitch. Using the FortiGate GUI, you then set two simple configuration settings. No configuration changes are required on the FortiSwitch (one change is required in FortiSwitchOS releases prior to 3.3.0).

Optionally, you can also configure remote management access directly to the FortiSwitch.

Enable the Switch Controller on FortiGate

Prior to configuring the first managed FortiSwitch, you must enable the Switch Controller on the FortiGate unit. If the main left menu already contains the **WiFi & Switch Controller** entry, you can skip this step.

Using the FortiGate web-based manager

1. Go to **System > Config > Features**.
2. Set the **WiFi & Switch Controller** feature to **on**.
3. Select **Apply**.

The menu now includes the **WiFi & Switch Controller** entry.

Using the FortiGate CLI

Use the following command to enable the Switch Controller and set the reserved subnetwork for the controller:

```
config system global
   set switch-controller enable
   set switch-controller-reserved-network 169.254.254.0 255.255.255.0
end
```

Adding a Managed FortiSwitch with FortiGate GUI

The procedure to add a new managed FortiSwitch consists of the following simple steps using the FortiGate GUI:

Note: For FortiSwitchOS releases prior to 3.3.0, you must Set the FortiSwitch to remote management mode prior to starting step 1

1. Connect a cable from the designated FortiSwitch port to an unused port on the FortiGate. For example, use port 24 on the FS-224D-POE switch. Refer to FortiLink Port for each FortiSwitch Model for additional information.
2. Go to **System > Network > Interfaces** and edit an internal port on the FortiGate.
3. Set **Addressing mode** to **Dedicate to Extension Device**.
4. Select **OK**.
5. Go to **WiFi & Switch Controller > Managed Devices > Managed FortiSwitch**.
   The new FortiSwitch should now be displayed in the table.
6. Right-click on the FortiSwitch and select **Authorize**.

After a delay (while FortiGate processes the request), an icon with a green checkmark appears in the Status column. For smaller FortiSwitch models, such as FS-108D-POE, the delay may be up to 3 minutes.

Set the FortiSwitch to remote management mode

Use the FortiSwitch web-based manager or the CLI to set remote management mode.

Note: This configuration step is not required in FortiSwitchOS release 3.3.0 or later releases.

Using the FortiSwitch web-based manager

1. Go to **System > Dashboard > Status** and locate the **System Information** widget.
2. Beside **Operation Mode**, select **Change**.
3. Change **Management Mode** to **FortiGate Remote Management**.
4. Select **OK**.
5. A warning will appear, asking if you wish to continue. Select **OK**.

Using the FortiSwitch CLI

Use the following command to change the FortiSwitch management mode:

```
config system global
   set switch-mgmt-mode fortilink
end
```

The FortiSwitch unit is now ready to be connected to the FortiGate unit.

FortiLink Port for each FortiSwitch Model

Each FortiSwitch model provides one designated port for the FortiLink connection. The table below lists the FortiLink port for each model:

FortiSwitch Model	Port for FortiLink connection
FS-28C	WAN port 1
FS-324B-POE	Management Port
FS-448B (10G only)	WAN port (uplink 1)
FS-348B	Last port (port 48)
For all D-series switches, use the last (highest number) port for FortiLink. For example:	
FS-108D-POE	Last port (port 10)
FSR-112D-POE	Last port (port 12)
FS-124D	Last port (port 26). May require an SFP module. See note below the table.
FS-224D-POE	Last port (port 24)
FS-224D-FPOE	Last port (port 28). May require an SFP module. See note below the table.

Note: FortiSwitch 3.3.1 and later releases support the use of an RJ-45 port for FortiLink.
Please contact Fortinet Customer Support for additional information.

FortiLink Ports for Each FortiGate Model

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

The following table shows the ports for each model of FortiGate that can be FortiLink-dedicated.

FortiGate Model	Ports for FortiLink connection
FGT-90D, FGT-90D-POE FWF-90D, FWF-90D-POE	port1 - port14
FGT-60D, FGT-60D-POE FWF-60D, FWF-60D-POE	port1 - port7
FGT-100D	port1 - port16
FGT-140D , 140D-POE, 140D-POE-T1	port1 - port36
FGT-200D	port1 - port16
FGT-240D	port1 - port40
FGT-280D, FGT-280D-POE	port1 - port84
FGT-600C	port3 - port22
FGT-800C	port3 - port24
FGT-1000C	port3 - port14, port23 - port24

Adding a Managed FortiSwitch with FortiGate CLI

We recommend that you add a new managed FortiSwitch using the FortiGate GUI. However, the following steps show how to add a new managed FortiSwitch using the FortiGate CLI. In these steps, the FortiGate 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 the interface for port 1.

```
config system interface
   edit port1
      set ip 172.20.120.10 255.255.255.0
      set allowaccess capwap
      set vlanforward 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 above command.
   ```

5. Configure a DHCP server on port 1.

   ```
   config system dhcp server
      edit 0
         set netmask 255.255.255.252
         set interface port1
         config ip-range
            edit 0
               set start-ip 169.254.254.2
               set end-ip 169.254.254.50
            end
         set vci-match enable
         set vci-string FortiSwitch
         set ntp-service local
      end
   end
   ```

Configuring FortiSwitch Remote 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.

From 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
```

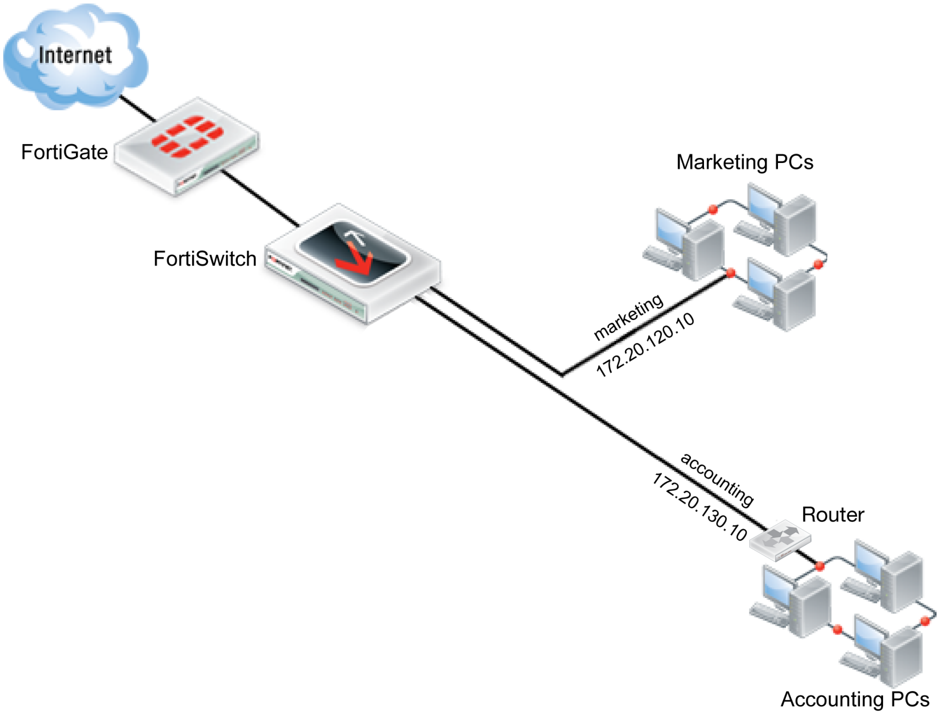
In the following example, the FortiSwitch management port is connected to a router with IP address 192.168.0.10:

```
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
```

VLAN Configuration

Using Virtual Local Area Networks (VLANs) allows you to get the most out of using your FortiSwitch unit by using ID tags to logically separate a LAN into smaller broadcast domains. A single LAN can contain many unique VLANs, which allows different policies to be created for different types of users and segments traffic so that it is only sent to and from the intended VLAN.

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.



Now that your FortiSwitch unit is managed by your FortiGate unit, a VLAN can be configured on the FortiSwitch, using the FortiGate.

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

Setting up a VLAN requires:

- Creating the VLAN.
- Assigning ports on the FortiSwitch unit to the VLAN.

Creating VLANs

Using the web-based manager

Creating the VLAN

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

Name	marketing
Color	🟥
IP/Network Mask	172.20.120.10/255.255.255.0

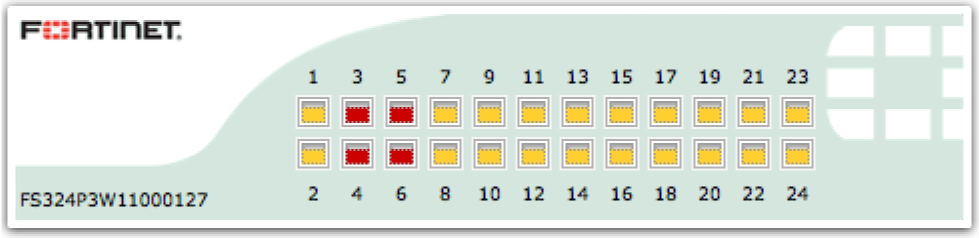
1. Enable **DHCP Server.** Set the IP range to 172.20.120.11-172.20.120.254.
2. Select **OK**.

The entry **marketing** is now shown on the list of **Virtual Switches**. A **marketing** interface has also been added, which can be seen by going to **System > Network > Interfaces**.

Assigning FortiSwitch Ports to the VLAN

1. Go to **WiFi & Switch Controller** > **Managed Devices** > **Managed FortiSwitch**
2. Highlight the FortiSwitch unit and select **Edit Managed FortiSwitch**.
3. Click and drag a box around ports 3-6 to select them.
4. Select **marketing** from the **Assign to** list.

Ports 3-6 on the FortiSwitch have now been assigned to the marketing VLAN and will appear in red.



Using the CLI

1. Create the marketing VLAN.

```
config switch-controller vlan
   edit marketing
      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
      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-based manager

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

Incoming Interface	marketing
Source Address	all
Outgoing Interface	wan1

Destination Address	all
Schedule	always
Service	ALL
Action	ACCEPT
Enable NAT	Enable
Logging Options	Log all Sessions

2. Select **OK**.

With this security policy in place, 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
```

Port Configuration

You can configure the FortiSwitch port and POE settings from the FortiGate using CLI commands. Currently, these functions are not available in the FortiGate web-based manager.

The following port CLI commands are available:

- Set port speed.
- Set port admin status
- Configure vlan on the port

Port CLI commands

```
config switch-controller
   edit <switch>
      config ports
         edit <port>
            speed <speed>
            status {down | up}
            vlan <vlan_id>
```

Scenarios

This chapter contains practical examples of how to use the FortiSwitch unit to manage a network. The scenarios are as follows:

- Scenario 1: Allowing access to specific users on the marketing VLAN
- Scenario 2: 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

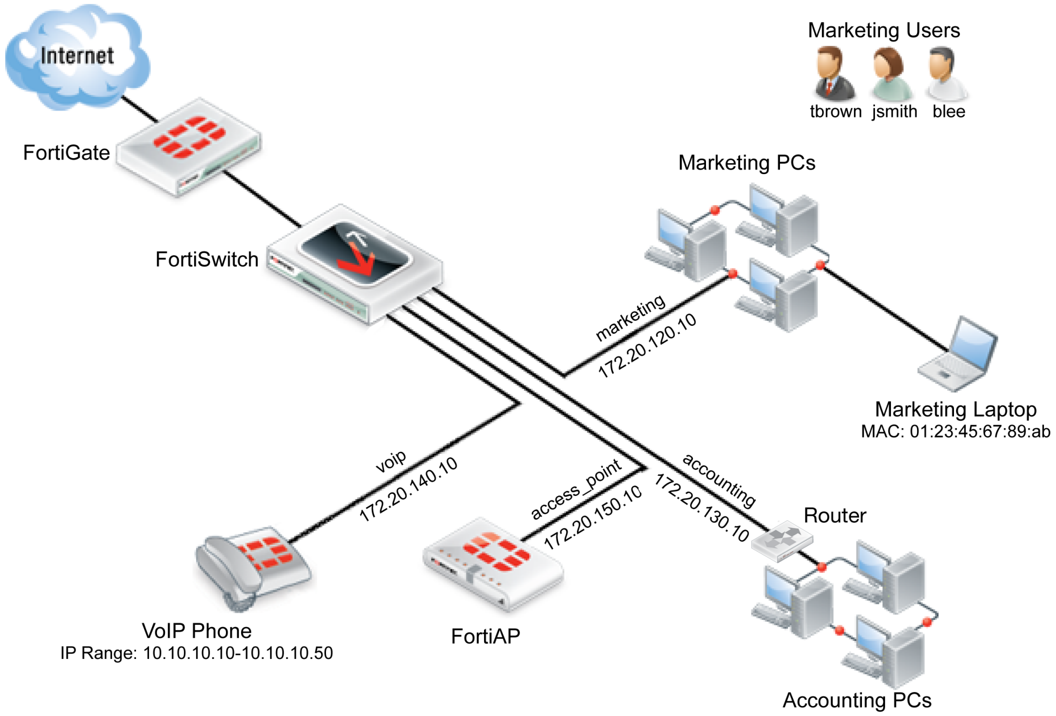
The Example Network

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:

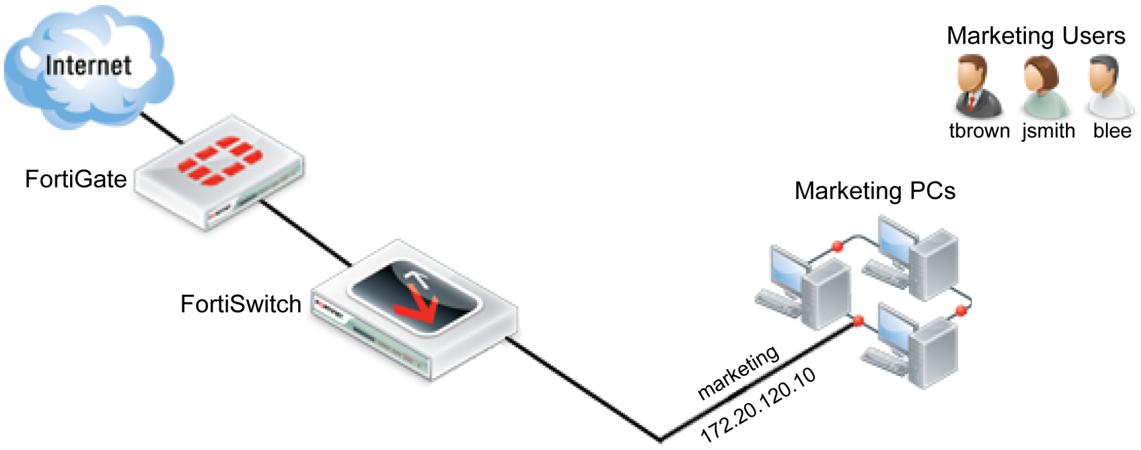
VLAN	IP	Device(s)	Port(s)	Policy ID(s)	GUI Color
marketing	172.20.120.10/255.255.255.0	marketing PCs, marketing laptop	3-6	2, 3	🟥
accounting	172.20.130.10/255.255.255.0	accounting PCs	21	4	🟦
voip	172.20.140.10/255.255.255.0	VoIP phone	10	5	🟩
access_ point	172.20.150.10/255.255.255.0	FortiAP	1	6	🟧

- There are six devices that connect directly 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.
- There are three marketing employees (Jane Smith, Tom Brown, Bob Lee) who will use the marketing VLAN using the marketing PCs.
- 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: Allowing access to specific users on the marketing VLAN

In Scenario 1, the policies for the marketing VLAN will be created 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-based manager

Creating a User Group

1. Go to **User & Device** > **User** > **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** > **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** > **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** > **Policy** > **IPv4** and select **Create New**.
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** > **Policy> IPv4** 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 match 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
```

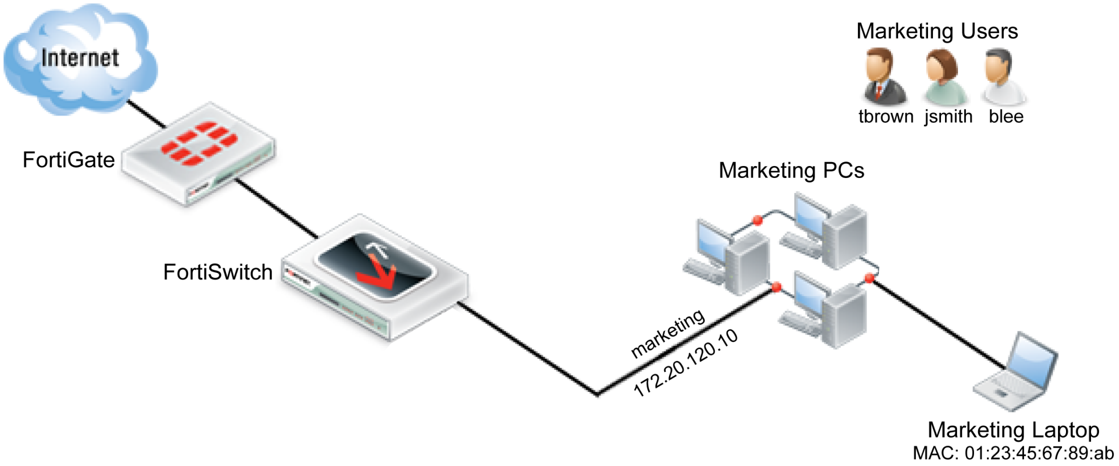
4. Create two firewall policies for the marketing VLAN, one for each user group:

```
config firewall policy
   edit 2
      set srcintf marketing
      set dstintf wan1
      set srcaddr all
      set dstaddr all
      set nat enable
      set action accept
      set schedule part-time_schedule
      set logtraffic all
      set groups part-time
      set service ALL
   next
   edit 3
      set srcintf marketing
      set dstintf wan1
      set srcaddr all
      set dstaddr all
      set nat enable
```

```
            set action accept
            set schedule always
            set logtraffic all
            set groups full-time
            set service ALL
        end
```

Scenario 2: 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-based manager

Assigning a Reserve IP to the Laptop

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

Category	Address
Name	marketing_laptop
Type	Subnet
Subnet/IP Range	172.20.120.254
Interface	marketing

Configuring a Firewall Policy

1. Go to **Policy & Objects > Policy > IPv4** 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 4
      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 4 before 2
end
```

Scenario 3: Accessing the marketing VLAN remotely using an SSL VPN

In Scenario 3, 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 3 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-based manager

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
```

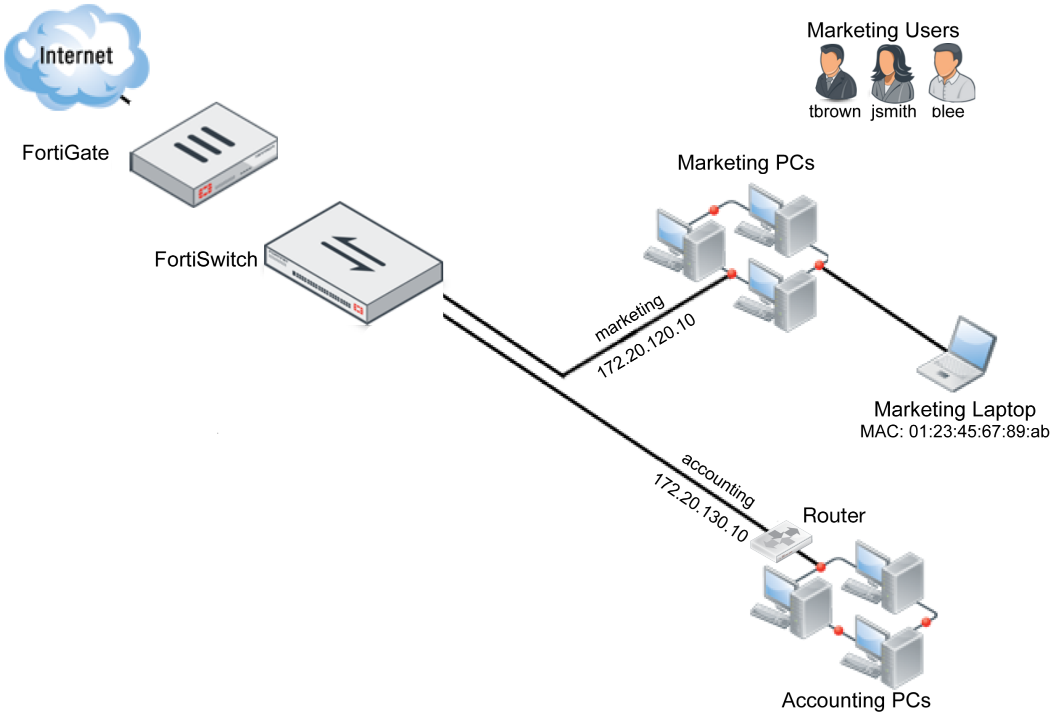
4. Create a firewall policy to allow remote access to the marketing VLAN.

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

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** and select **Create New**. 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
```

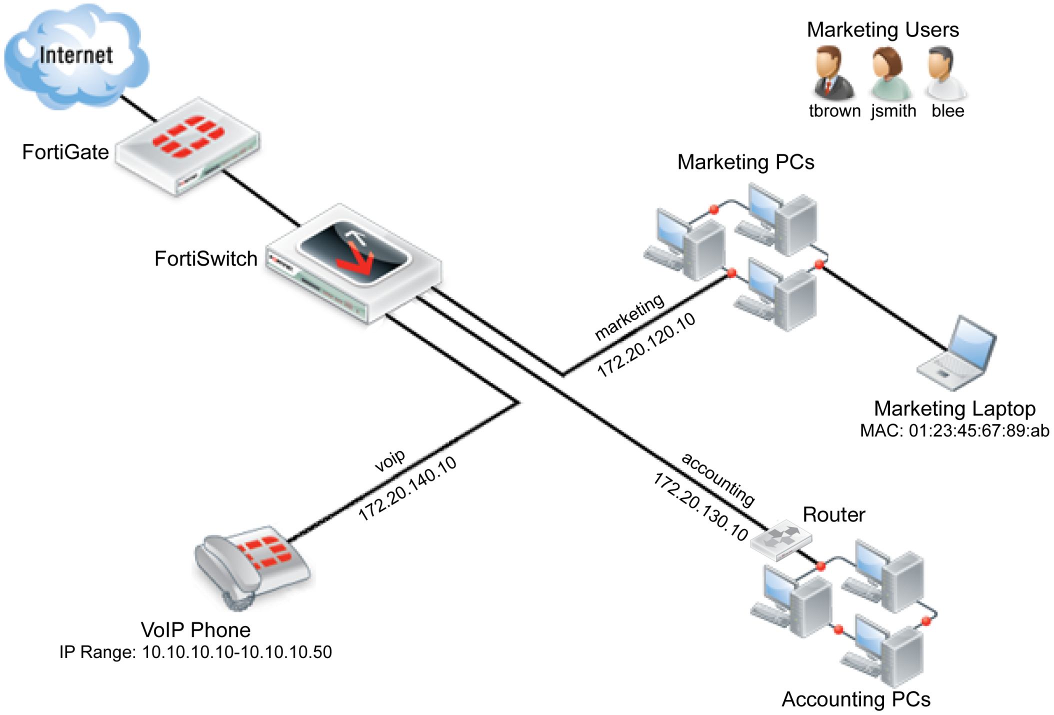
4. Create a firewall policy for the accounting VLAN that uses the default security profiles.

```
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-based manager

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.

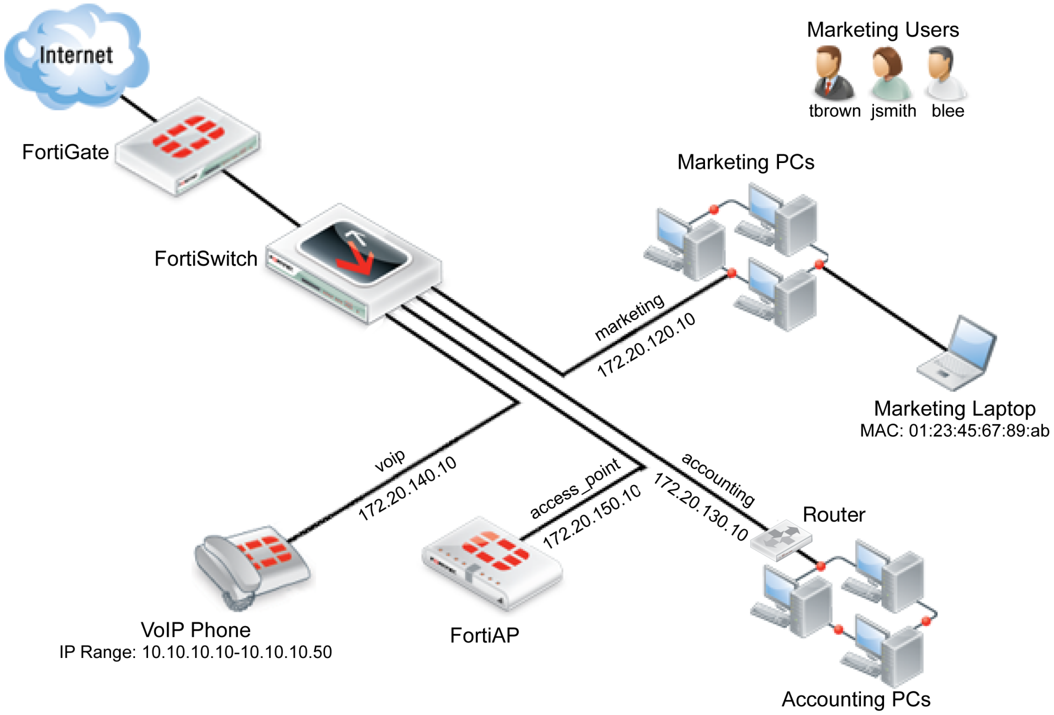
```
config switch-controller managed-switch
   edit FS224D3W14000370
      config ports
         edit port10
            set vlan voip
      end
end
```

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-based manager

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
```

High Performance Network Security

Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.