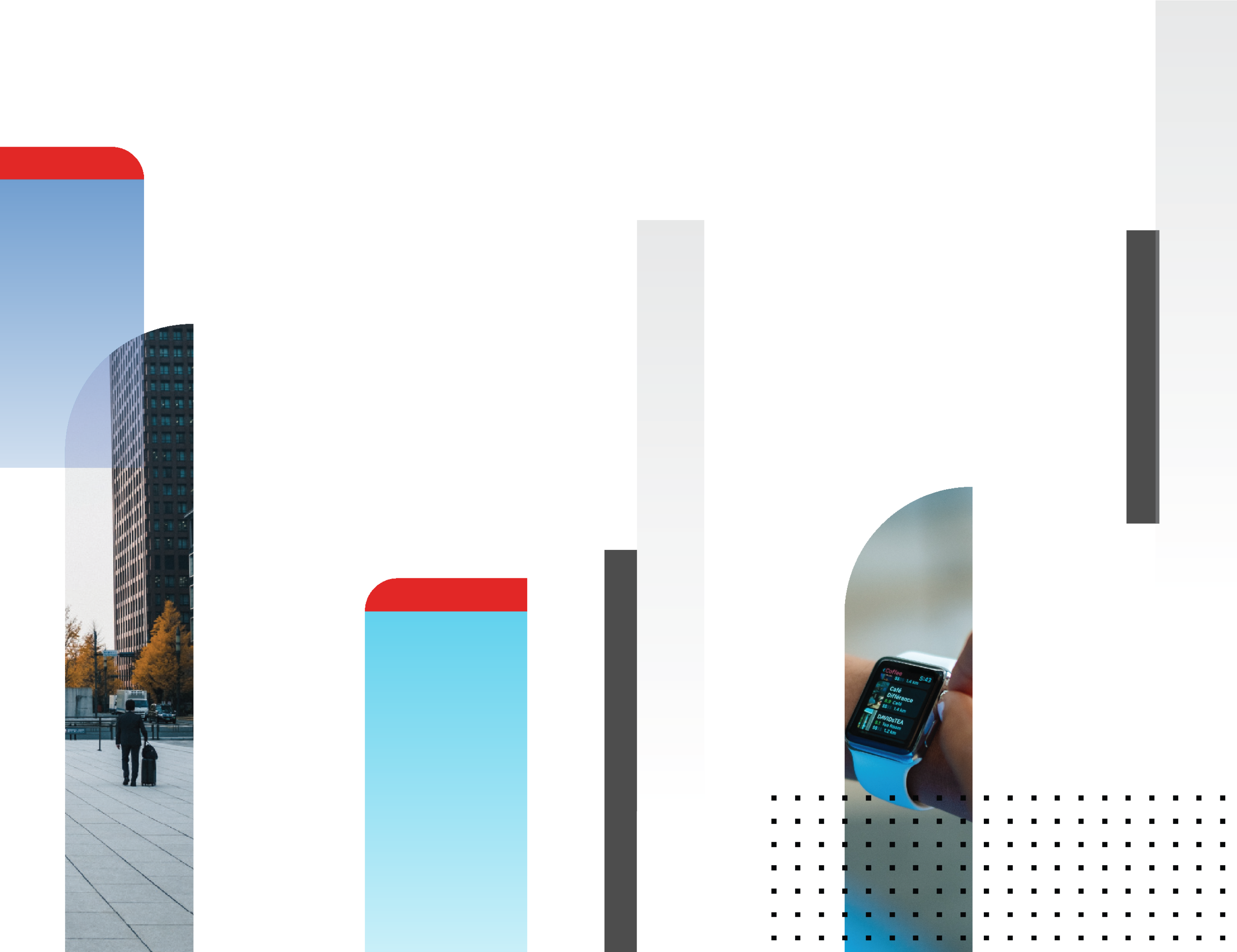
LAN Edge Deployment Guide

FortiGate, FortiSwitch, and FortiAP



April 13, 2023
FortiGate, FortiSwitch, and FortiAP LAN Edge Deployment Guide
11-644-762174-20230413

TABLE OF CONTENTS

Change log

Date	Change Description
February 7, 2022	Initial release
April 13, 2023	Updated step 4d of the “Configure the FortiLink interface” section.

Introduction

Executive summary

One of the great strengths of the Fortinet LAN Edge Solution is the tight integration of everything with FortiLink. With FortiLink, FortiSwitch units and FortiAP units are extensions of the FortiGate device. The entire network can be treated as a single unit with a single management system, and security can be applied consistently everywhere—in other words, *Security-Driven Networking*.

LAN edge equipment leverages Security-Driven Networking to extend the Fortinet Security Fabric throughout the LAN, converging security and network access into an integrated platform. This convergence increases security while reducing complexity, lowering cost, and improving performance at the LAN edge.

Security-driven networking is compelling and simplifies the network overall, but the integrated whole can be confusing. Everything you want and need in your network is in the FortiGate device, and all that integration that makes it so powerful can make it hard to decide where to start. With great power may come great confusion.

Security designs are generally specific to the deployment, but they can also be developed and improved over time. Indeed, that is generally the recommended approach. This deployment guide is focused on the network skeleton and the default firewall policies so that the baseline network can be up and running as quickly as possible.

Intended audience

This guide is intended for an audience who is interested in deploying Fortinet’s secure LAN Edge Solution in a new environment or replacing their equipment in an existing environment. Readers are expected to have a firm understanding of networking, wireless and security concepts. Interested audiences may include the following:

- Network, wireless, and security architects
- Network, wireless, and security engineers

About this guide

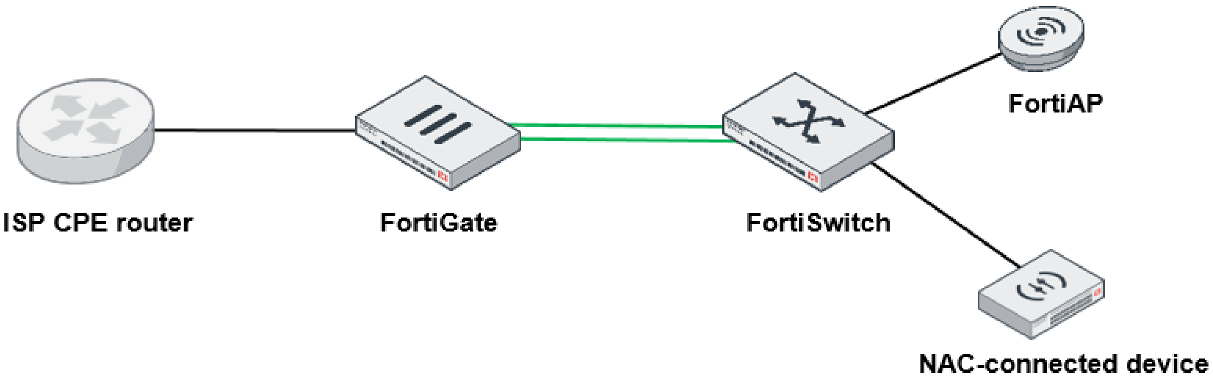
The deployment guide serves the purpose of going through the design and deployment steps involved in deploying a specific architecture. Readers should first evaluate their environment to determine whether the architecture and design outlined in this guide is suitable for them. It is advisable to review the Reference Architecture Guide(s) if readers are still in the process of selecting the right architecture.

This deployment guide presents one of possibly many ways to deploy the solution. It may also omit specific steps where readers must make design decisions to further configure their devices. It is recommended that readers also review supplementary material found in product admin guides, example guides, cookbooks, release notes and other documents where appropriate.

Design overview

Use case and topology

The following figure shows the topology:



- The focus is on getting the basic network up and running, leaving details for later.
- The ISP access router/modem has been deployed.
  - It will serve as a DHCP address to your FortiGate WAN link.
  - The physical WAN connection is Ethernet.
- The deployment will consist of the following:
  - 1 FortiGate device
  - 1 FortiSwitch unit
  - One or more FortiAP units
  - All necessary Ethernet cabling is available or already deployed/patched.
- A laptop or other management station with an Ethernet port is available.

Design concept and considerations

The topology presented in this deployment guide is a baseline network to deploy a secure LAN edge as quickly as possible. The solution can be scaled out to accommodate more users on a site by adding additional FortiSwitch units, FortiAP units, and using a higher model FortiGate device. Redundancy can be improved by adding an additional FortiGate device into an HA cluster, provisioning a full-mesh switch network, and using aggregate links for connections.

SD-WAN can also be configured in this setup to provide redundancy and intelligent traffic steering over multiple underlays. Finally, in multi-site deployments, the sites can be standardized into SD-branches and quickly provisioned with a FortiManager unit and other orchestration tools.

In summary, the basic design in this deployment guide offers many possibilities to extend, optimize, and scale your solution. Once you have understood the steps and concepts in this guide, also consider other guides listed in Appendix B: Documentation references on page 30 for further reading.

Deployment overview

Review the deployment plan before starting the configuration.

Deployment plan

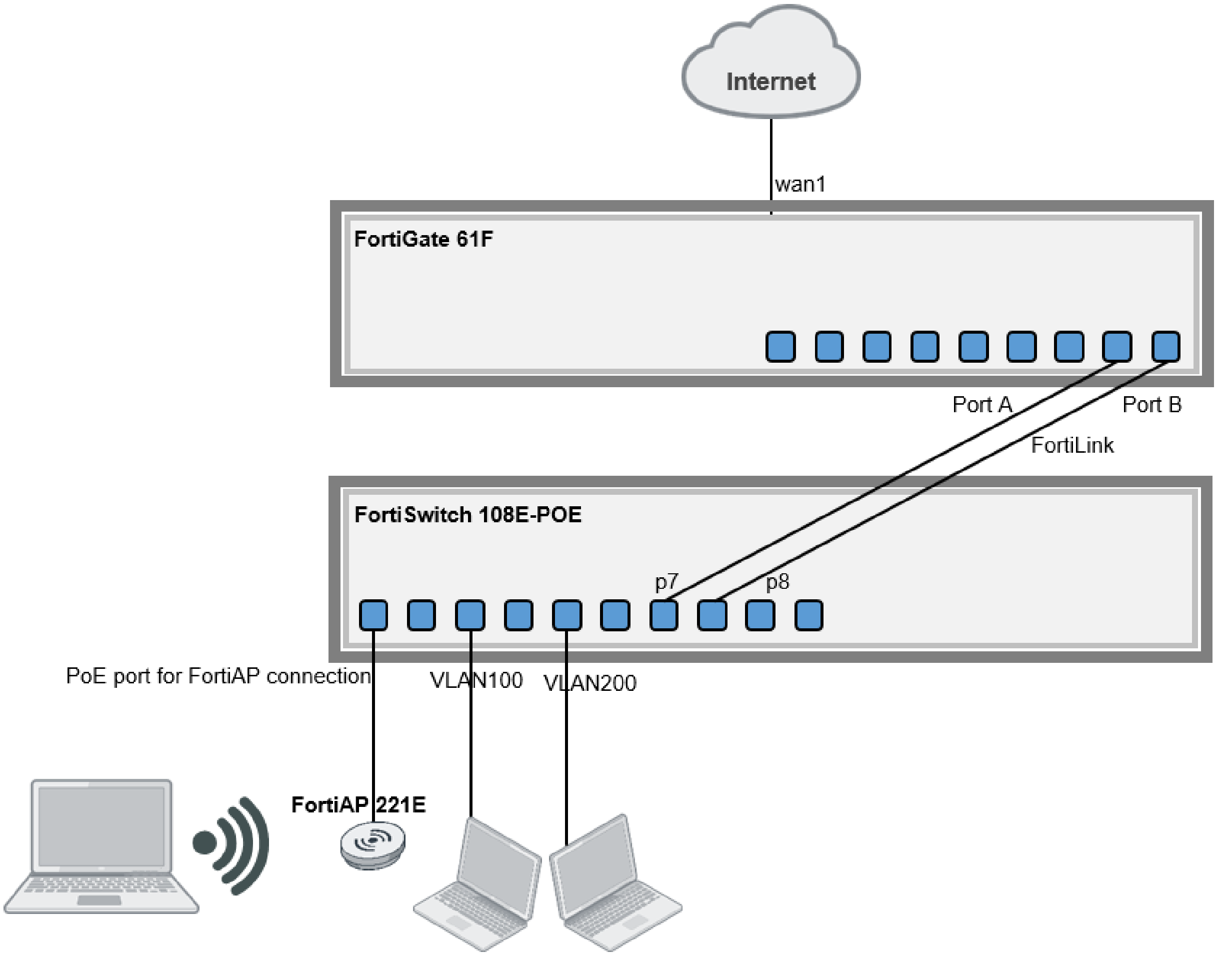
This deployment will configure a FortiGate device, a FortiSwitch unit, and a FortiAP unit from factory default settings to provide wired and wireless outbound access for internal users. Other than the physical connections, the majority of the steps are completed on the FortiGate device.

The general deployment steps are as follows:

1. Bring up a FortiGate device and connect to an ISP.
2. Configure FortiLink and authorize a FortiSwitch unit.
3. Create and assign VLANs in the switch controller.
4. Set up NAC and create NAC policies.
5. Add one or more FortiAP units.

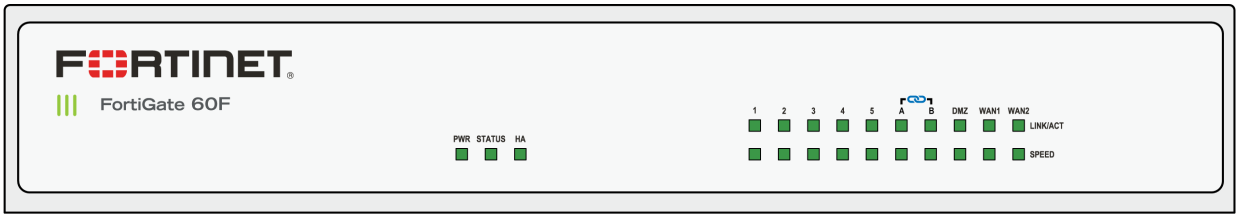
Deployment procedures

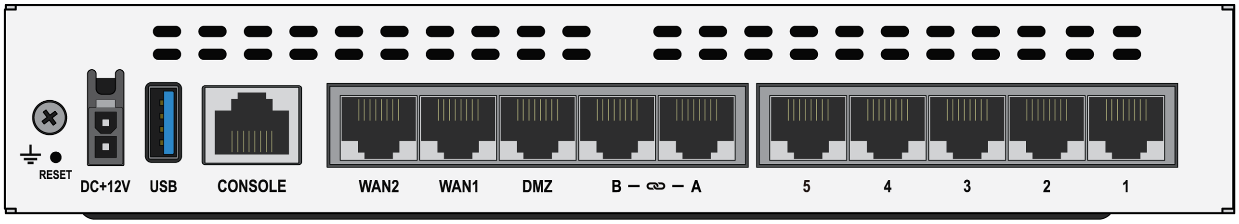
The following deployment steps provision a FortiGate device, a FortiSwitch unit, and a FortiAP unit in the following topology:



Step 1: Bring up the FortiGate device

The following figures show the faceplate and back of the FortiGate 60F, which are similar to the FortiGate 61F:





On larger models, DMZ, HA, and MGMT ports might also be available.

When a FortiGate device is fresh out of the box, depending on the model, there are an array of physical ports labeled according to their default configuration. To a large extent, these ports can be reconfigured, with some hardware-dependent exceptions, to serve any purpose. However, in this case, as is best in most cases, you can use the preconfigured and labeled defaults. Make a special note if you have ports labeled 'A' and 'B'. If so, these are preconfigured for FortiLink and will be connected to the FortiSwitch unit.

The following table lists some of the default settings on an out-of-the-box FortiGate device.

Setting	Value
Management IP address and login credentials	
Management IP	192.168.1.99/24
User name	admin
Password	<blank> The FortiGate device prompts for a new password at the first login.
Ports and interfaces	
MGMT port address range (if it exists)	192.168.1.0/24, with the FortiGate device as the default gateway
LAN port only	If there is no MGMT port, the LAN port address range is 192.168.1.0/24.
MGMT and LAN port	If there is an MGMT port, the LAN ports default to a different subnet.
WAN1	DHCP client (will request an IP address from the ISP)

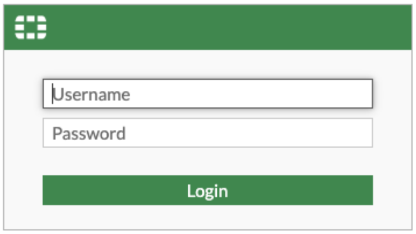
Setting	Value
LAN ports labeled ‘A’ and ‘B’	Preconfigured for FortiLink
Firewall policies	
LAN → WAN	A firewall policy allows outgoing traffic from LAN ports but does not allow incoming traffic from the Internet/uplink (WAN1).
	If MGMT is a separate port, it will *not* have default Internet access.

See FortiGate Best Practices for tips on securing your administrative access.

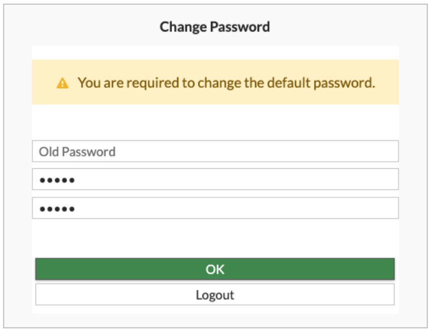
Power on the FortiGate device and log in

1. Plug in the FortiGate device and power it on.
2. Plug the ISP uplink into the FortiGate WAN1 port.
3. Connect a management station to the MGMT (or LAN port 1) port using the Ethernet cable.

   The management station should get an IP address from the FortiGate device. If it does not, configure the management station to 192.168.1.110/255.255.255.0 with a gateway of 192.168.1.99.
4. Open a web browser and connect to 192.168.1.99.
5. At the login page, enter the user name `admin`, leave the password blank, and press `Enter`.



6. You will be prompted for a new password. Choose anything that fits your password policy. Leave the *Old Password* field blank.


Change Password

You are required to change the default password.

7. The first boot sequence setup continues with a FortiGate setup screen. This document skips these details.

   A station that is Ethernet-connected to a FortiGate LAN port can now access the Internet through the FortiGate firewall.

Step 2: Configure FortiLink and authorize the FortiSwitch unit

FortiLink allows a FortiSwitch unit to be fully managed from the FortiGate device as if it was simply part of the FortiGate device. VLAN tags are provisioned automatically, and there is no need to configure trunks—the FortiGate device and FortiSwitch unit act as a unified device.

Remove the ports in the LAN hardware switch interface

On FortiGate models where there are no dedicated FortiLink ports like port A and port B, you need to remove two of the LAN ports from the LAN interface to be used in the FortiLink interface.

By default, LAN ports are grouped together into the LAN hardware switch interface. These ports are connected with an internal hardware switch controller and are part of the same broadcast domain.

The following steps show the configurations on a FortiGate 61F:

1. Go to *Network* > *Interfaces* and double-click on *LAN*.
2. In the *Interface Members* field, remove two physical ports by clicking on the ‘X’s.

   A common practice is to use the two highest-numbered ports, but you can remove any two ports.
3. Click *OK*.
4. On the *Network* > *Interfaces* page, the two ports are now removed from the LAN interface, and these interfaces are listed under the Physical Interface grouping.

Configure the FortiLink interface

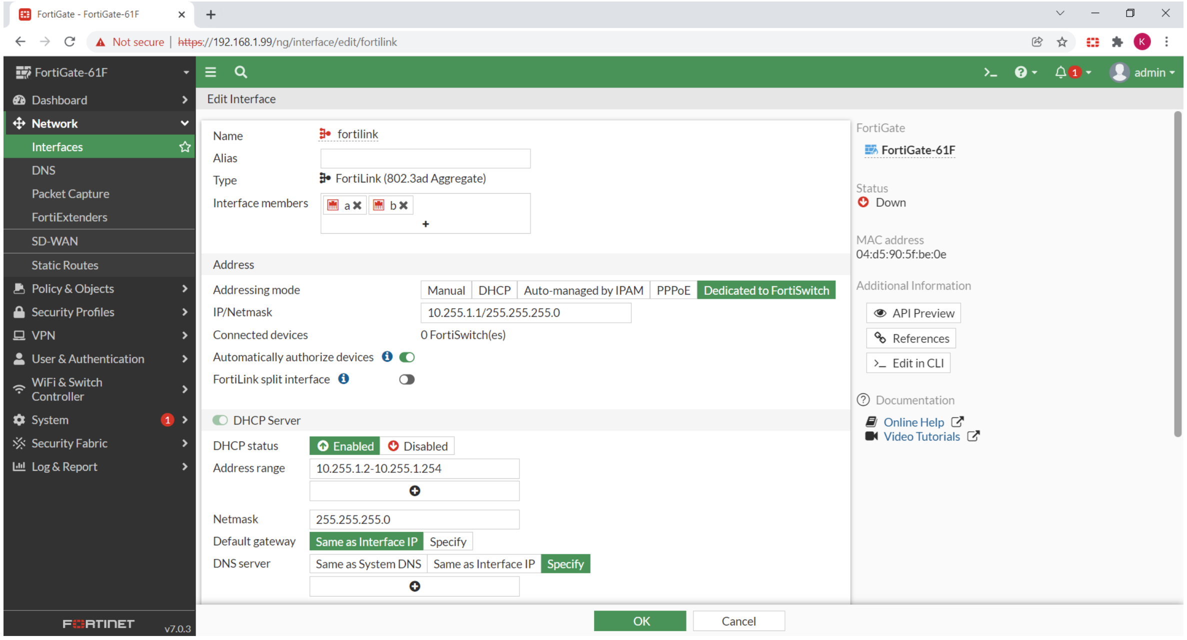
FortiLink connects switches (and access points) directly to the FortiGate device so that the network acts as a single device.

1. Go to *Network* > *Interfaces*.
2. Double-click on *FortiLink*.
3. Check if there are interface members listed at the top.
   - If there are already two members, FortiLink is ready to connect to a switch. The two members are likely the ports labeled ‘A’ and ‘B’ if they exist on your physical FortiGate device.
   - If there are no interface members, select the two LAN ports that were removed in Remove the ports in the LAN hardware switch interface on page 12.
4. Check the FortiLink settings.
   a. In the *Address* section, leave the addressing mode at the default setting, *Dedicated to FortiSwitch*.
   b. In the *Address* section, ensure that *Automatically authorize devices* is enabled.

      Devices can be manually admitted one at a time later if you prefer.
   c. In the *Address* section, disable *FortiLink split interface*.

      The split interface is used when more than one switch is connected directly to a FortiGate device.
   d. Make certain that the DHCP server is enabled.

      Connected FortiSwitch units will receive an IP address in this range.



Name: fortilink
Alias:
Type: FortiLink (802.3ad Aggregate)
Interface members: a, b

Address
Addressing mode: Manual | DHCP | Auto-managed by IPAM | PPPoE | Dedicated to FortiSwitch (selected)
IP/Netmask: 10.255.1.1/255.255.255.0
Connected devices: 0 FortiSwitch(es)
Automatically authorize devices: enabled
FortiLink split interface: disabled

DHCP Server
DHCP status: Enabled (selected) | Disabled
Address range: 10.255.1.2-10.255.1.254
Netmask: 255.255.255.0
Default gateway: Same as Interface IP (selected) | Specify
DNS server: Same as System DNS | Same as Interface IP | Specify (selected)

FortiGate: FortiGate-61F
Status: Down
MAC address: 04:d5:90:5f:be:0e
Additional Information

5. Click *OK*.

Make the switch controller and WiFi controller visible in the GUI

Ensure that the switch controller is visible in the GUI by changing the feature visibility.

1. Go to *System* > *Feature Visibility*.
2. Under *Core Features*, enable *Switch Controller* if it is not already enabled.
3. Under *Core Features*, enable *WiFi Controller* if it is not already enabled.

Connect the FortiLink ports to the switch ports

1. Unpack the FortiSwitch unit and deploy it.
2. Turn on the FortiSwitch unit.
3. Connect the FortiSwitch unit to the FortiGate device using two Ethernet connections. Use the two designated FortiLink ports of the FortiGate device to connect to the last two ports on the FortiSwitch unit.

   It will take a few minutes for the switch to become visible and configurable in the FortiGate device.

Explore the switch controller

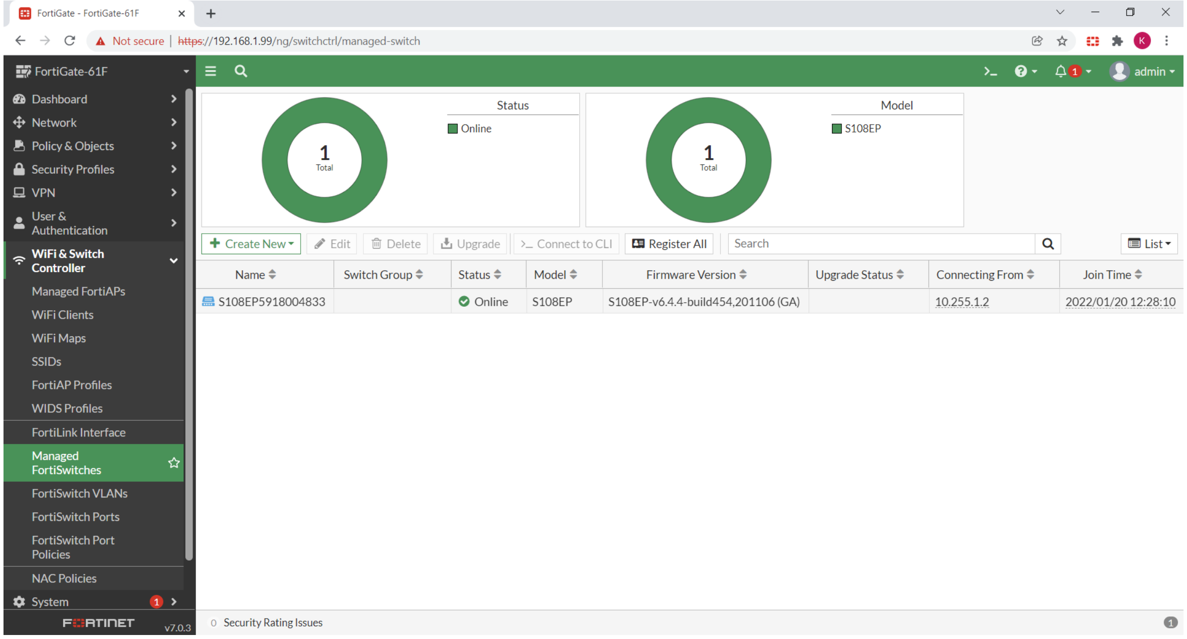
Go to *WiFi & Switch Controller* > *FortiLink Interface*.

This is the same FortiLink interface that you configured earlier, but there are some additional options here such as FortiOS network address control (NAC).

Check the switch authorization and topology

1. Go to *WiFi & Switch Controller* > *Managed FortiSwitch*.
2. Check that the FortiSwitch unit is visible, connected to the FortiGate device, and authorized.

   If the FortiSwitch unit has not been automatically authorized, click on the icon and authorize the switch.

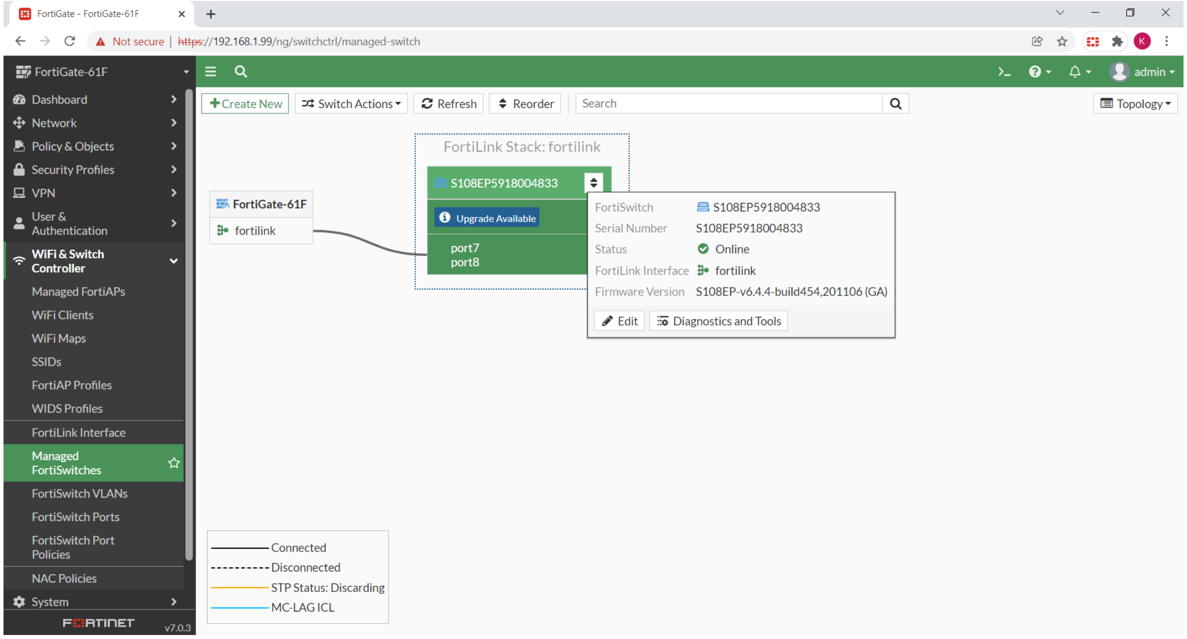


Name	Switch Group	Status	Model	Firmware Version	Upgrade Status	Connecting From	Join Time
S108EP5918004833		✓ Online	S108EP	S108EP-v6.4.4-build454,201106 (GA)		10.255.1.2	2022/01/20 12:28:10

3. To get a topology view, use the dropdown menu in the upper right corner to change *List* to *Topology*.

   The Topology view shows the logical connection between the FortiGate device and the connected FortiSwitch unit.
4. Hover over the switch icon to see the context menu with several options.
5. The following figure shows that the FortiSwitch unit is now connected, authorized, and ready to be

configured.



FortiSwitch S108EP5918004833
Serial Number S108EP5918004833
Status Online
FortiLink Interface fortilink
Firmware Version S108EP-v6.4.4-build454,201106 (GA)

Step 3: Create and assign VLANs in the switch controller

Create FortiSwitch VLANs

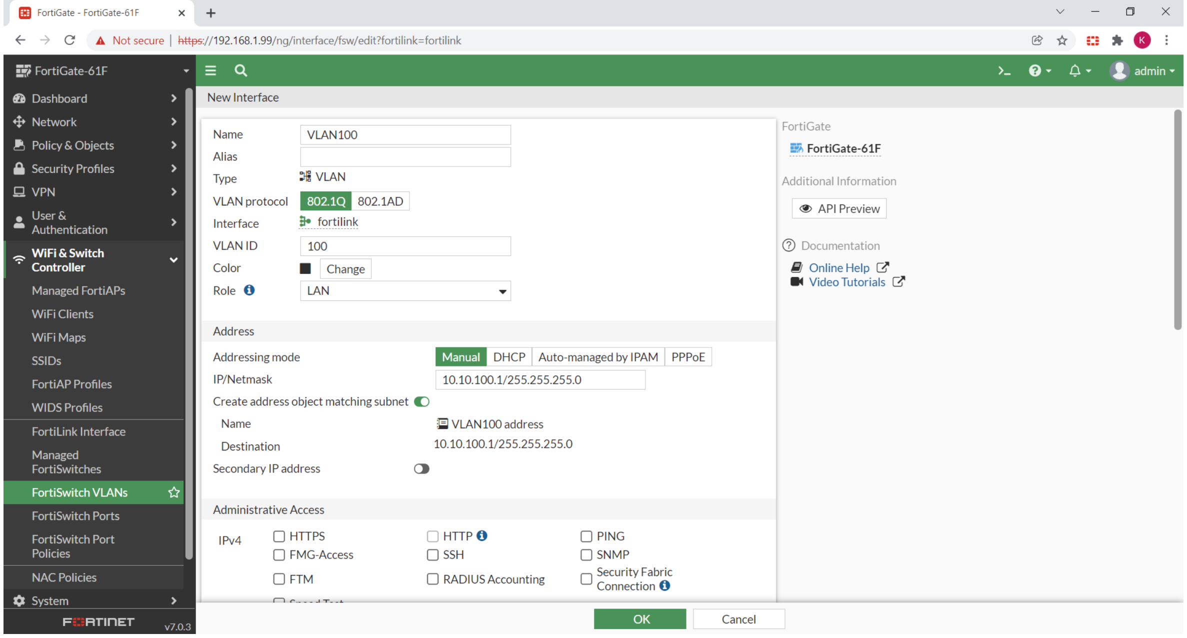
There are several predefined VLANs for NAC purposes, which allow devices connected to the FortiSwitch unit to be assigned a default VLAN automatically. This is covered in a later section. For now, you can create two example VLANs.

Up to this point, the recommended configuration has been virtually identical to this guide. At this point, you might want your specific deployment to deviate from this guide due to a preferred IP address scheme and the number of VLANs needed, and if inter-VLAN routing is needed. The following configuration is for two internal VLANs, both with Internet access and routing between them allowed.

1. Go to *WiFi & Switch Controller > FortiSwitch VLANs*.
2. Click *Create New*.
3. Assign a VLAN name. For example, enter `VLAN100`.
4. By default, *Type* is set to *VLAN*, and *Interface* is set to *fortilink*.
5. Assign a number between 2 and 4,094 not already in use for the VLAN ID. For example, enter `100`.

   The default configuration uses 4089-4093 for the predefined VLANs.
6. Select a color if you want to.
7. From the *Role* dropdown list, select *LAN*.
8. For the addressing mode, click *Manual*.
9. In the *IP/Netmask* field, enter an IP address and netmask. For example, enter `10.10.100.1/255.255.255.0`.
10. Enable *Create address object matching subnet* if it is not already enabled.

This setting will be useful in policies later.



New Interface

Name: VLAN100

Alias:

Type: VLAN

VLAN protocol: 802.1Q | 802.1AD

Interface: fortilink

VLAN ID: 100

Color: ■ Change

Role: LAN

Address

Addressing mode: Manual | DHCP | Auto-managed by IPAM | PPPoE

IP/Netmask: 10.10.100.1/255.255.255.0

Create address object matching subnet: ●

Name: VLAN100 address

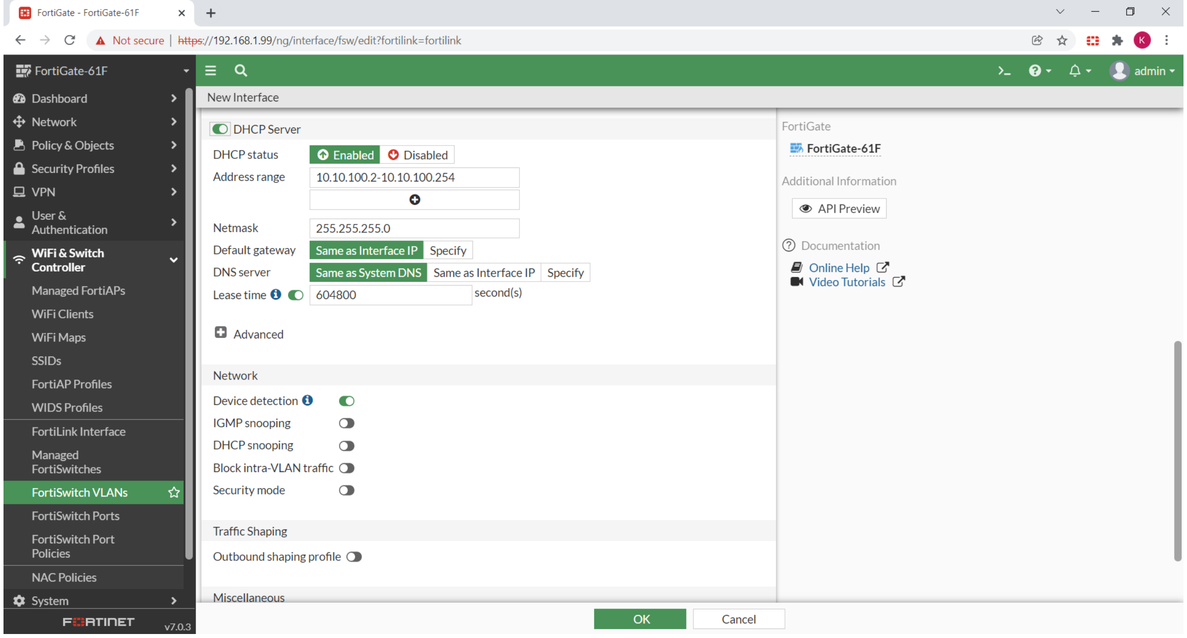
Destination: 10.10.100.1/255.255.255.0

Secondary IP address: ○

Administrative Access

IPv4: □ HTTPS □ HTTP □ PING □ FMG-Access □ SSH □ SNMP □ FTM □ RADIUS Accounting □ Security Fabric Connection

11. Enable *DHCP Server*.
12. Accept the default address range or adjust it for your environment.
13. Check that *Same as Interface IP* and *Same as System DNS* are enabled.



New Interface

● DHCP Server

DHCP status: Enabled | Disabled

Address range: 10.10.100.2-10.10.100.254

Netmask: 255.255.255.0

Default gateway: Same as Interface IP | Specify

DNS server: Same as System DNS | Same as Interface IP | Specify

Lease time ●: 604800 second(s)

Advanced

Network

Device detection: ●

IGMP snooping: ○

DHCP snooping: ○

Block intra-VLAN traffic: ○

Security mode: ○

Traffic Shaping

Outbound shaping profile: ○

Miscellaneous

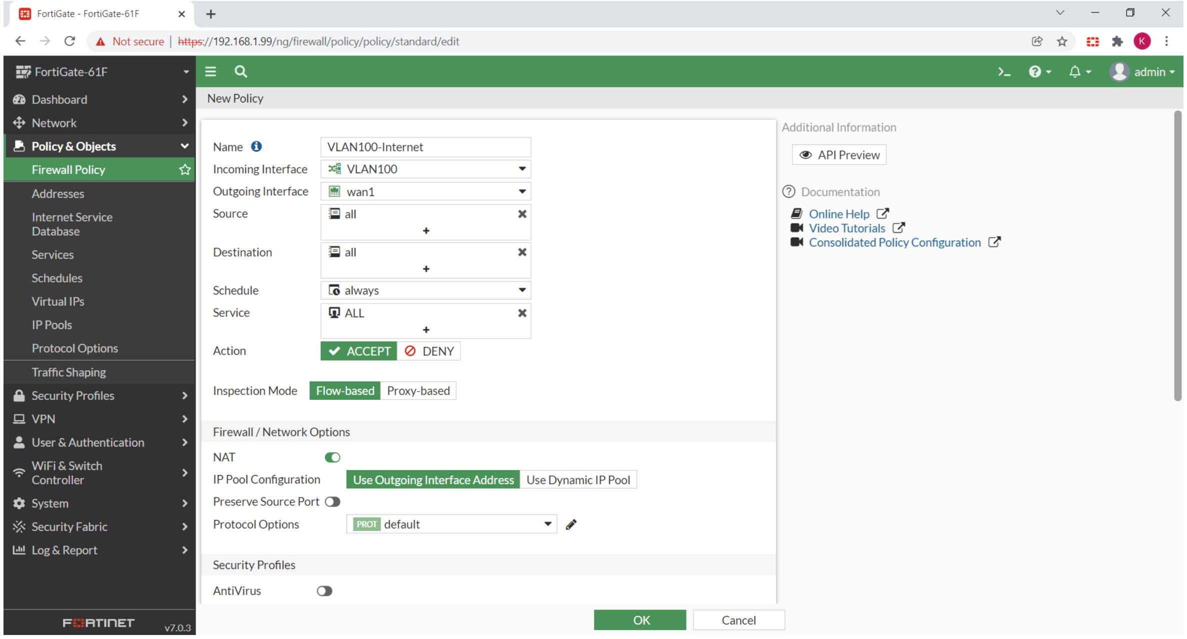
14. Click *OK*.
15. For the second VLAN, repeat the preceding procedure with a different interface address:
    a. Enter `VLAN200` for the VLAN name.
    b. Enter `200` for the VLAN ID.
    c. Enter `10.10.200.1/255.255.255.0` for the IP address and netmask.
    d. Configure other settings as needed.

16. Click *OK*.

Create firewall policies for Internet access

The Internet access policies will mirror the LAN internet policy described in Step 1: Bring up the FortiGate device on page 10.

1. Go to *Policy & Objects* > *Firewall Policy*.
2. Click *Create New*.
3. Configure the firewall policy according to your VLAN names.
   a. Enter a name for the Internet access policy for the first VLAN. For example, enter `VLAN100-Internet`.
   b. Select your first VLAN for the incoming interface. For example, select *VLAN100*.
   c. Select *WAN1* for the outgoing interface.
   d. Select *all* for the source.
   e. Select *all* for the destination.
   f. Select *always* for the schedule.
   g. Select *all* for the service.
   h. Click *ACCEPT* for the action.
4. Under *Firewall/Network Options*, make certain that *NAT* is enabled and *Use Outgoing Interface Address* is selected.



New Policy

Name: VLAN100-Internet
Incoming Interface: VLAN100
Outgoing Interface: wan1
Source: all
Destination: all
Schedule: always
Service: ALL
Action: ✓ ACCEPT | DENY
Inspection Mode: Flow-based | Proxy-based

Firewall / Network Options
NAT: ●
IP Pool Configuration: Use Outgoing Interface Address | Use Dynamic IP Pool
Preserve Source Port: ○
Protocol Options: PROT default

Security Profiles
AntiVirus: ○

5. Accept the rest of the default settings and then click *OK*.
6. Repeat steps 1-5 for your second VLAN.

Enable inter-VLAN routing (if needed)

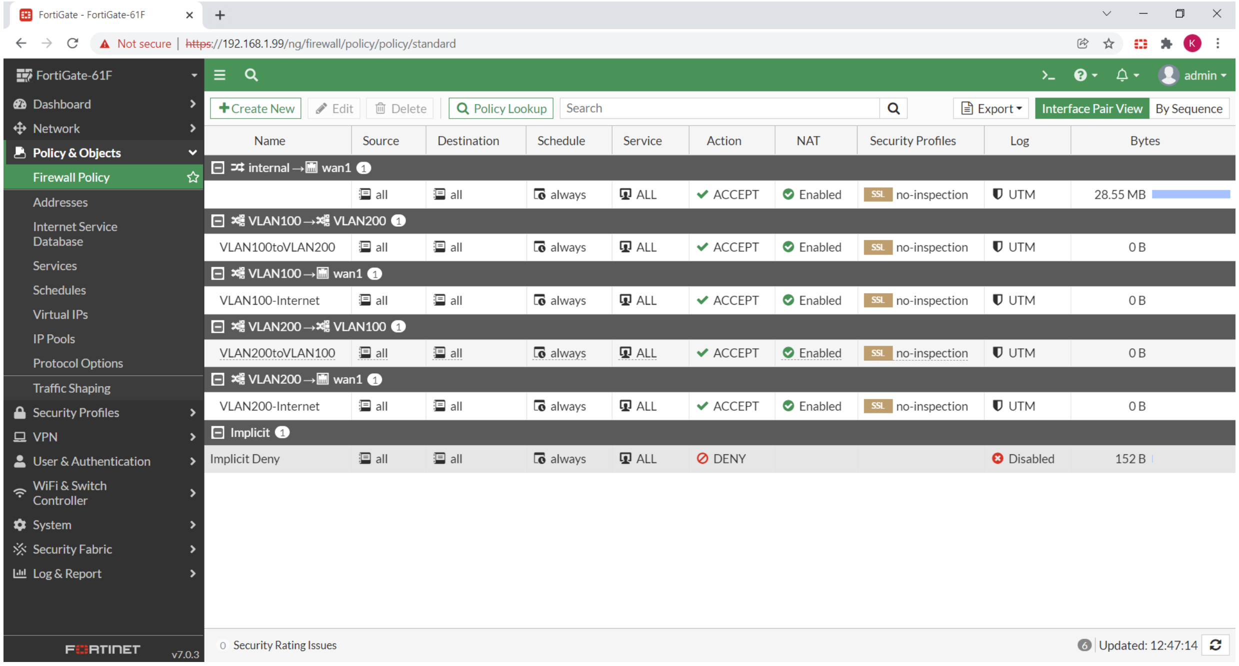
Both VLANs now have Internet access. If the VLANs need to reach each other, you need to configure two more policies for inter-VLAN routing. Repeat the steps in Create firewall policies for Internet access on page 17 but with changes to the incoming and outgoing interfaces.

For example, for the first inter-VLAN routing policy:

- Select *VLAN100* as the incoming interface.
- Select *VLAN200* as the outgoing interface.

For example, for the second inter-VLAN routing policy:

- Select *VLAN200* as the incoming interface.
- Select *VLAN100* as the outgoing interface.



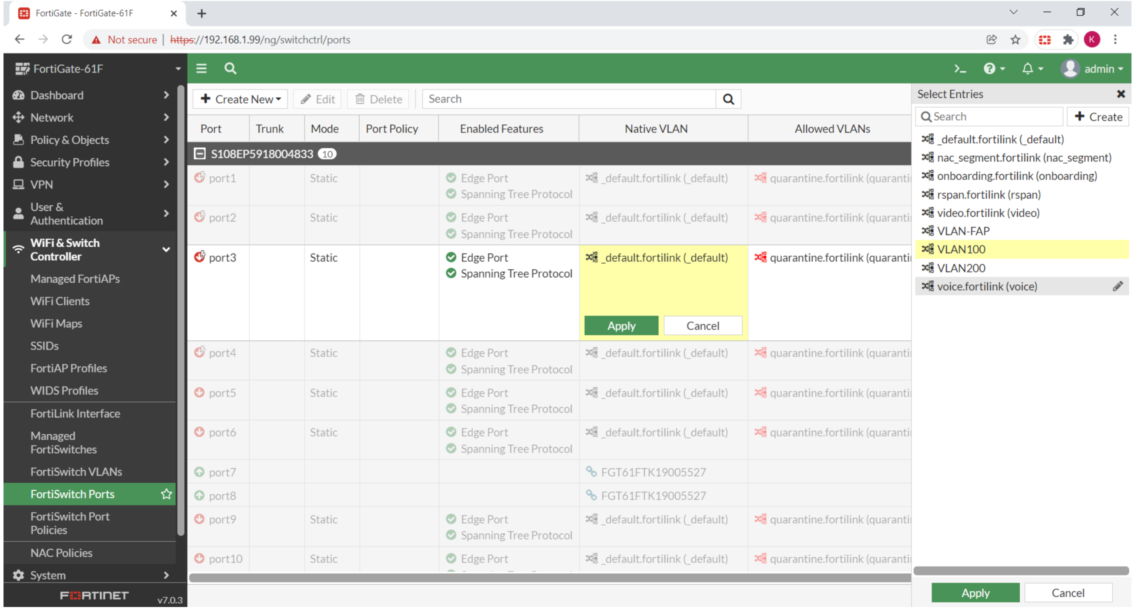
Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
internal → wan1 1									
	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	28.55 MB
VLAN100 → VLAN200 1									
VLAN100toVLAN200	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B
VLAN100 → wan1 1									
VLAN100-Internet	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B
VLAN200 → VLAN100 1									
VLAN200toVLAN100	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B
VLAN200 → wan1 1									
VLAN200-Internet	all	all	always	ALL	✓ ACCEPT	Enabled	SSL no-inspection	UTM	0 B
Implicit 1									
Implicit Deny	all	all	always	ALL	⊘ DENY			Disabled	152 B

Assign VLANs to switch ports

Now that the VLANs and policies are configured, you need to assign the VLANs to the switch ports. This method assigns VLANs statically to a port. The next section describes how to use NAC policies to assign VLANs.

1. Go to *WiFi & Switch Controller > FortiSwitch Ports*.
2. Notice that the FortiLink ports show the FortiGate device itself in the native VLAN column. You do not need to configure a trunk port.
3. To change the VLAN assigned to any port, hover over the current native VLAN of that port, and a pencil icon is displayed.

4. Click the pencil icon to edit the port.
   a. In the *Select Entries* pane, select the VLAN to assign to this port.



Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs
S108EP5918004833 10						
port1		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quaranti
port2		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quaranti
port3		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default) Apply Cancel	quarantine.fortilink (quaranti
port4		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quaranti
port5		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quaranti
port6		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quaranti
port7					FGT61FTK19005527	
port8					FGT61FTK19005527	
port9		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quaranti
port10		Static		Edge Port	_default.fortilink (_default)	quarantine.fortilink (quaranti

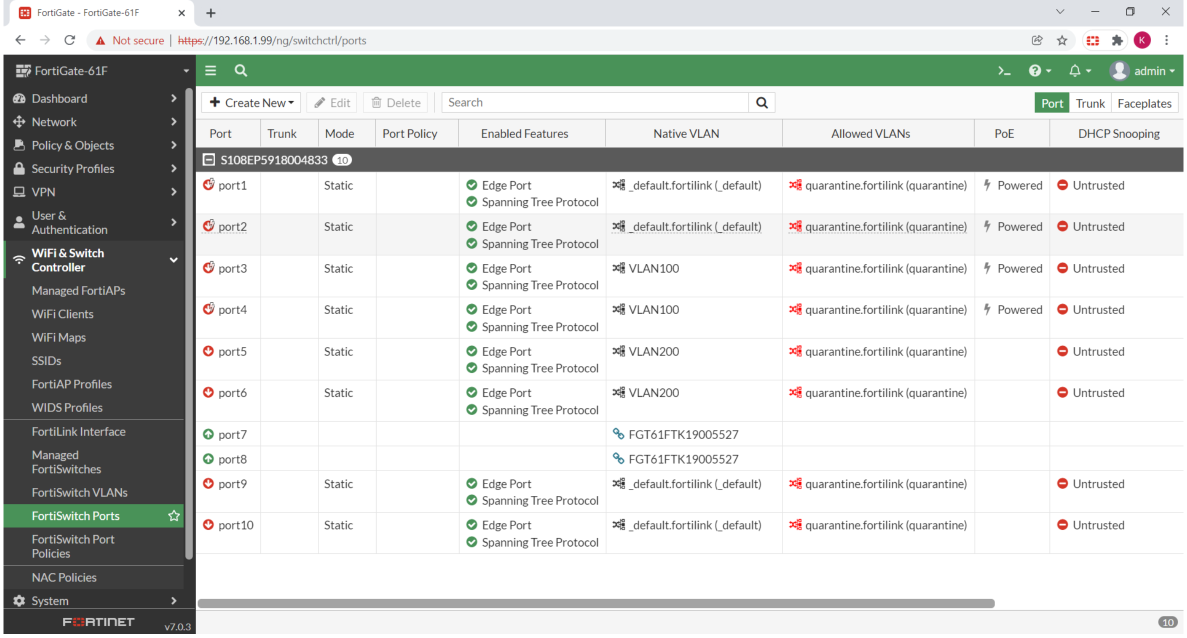
Select Entries

Search | Create

- _default.fortilink (_default)
- nac_segment.fortilink (nac_segment)
- onboarding.fortilink (onboarding)
- rspan.fortilink (rspan)
- video.fortilink (video)
- VLAN-FAP
- VLAN100
- VLAN200
- voice.fortilink (voice)

Apply | Cancel

   b. If that VLAN has not been defined yet, click *Create* to create a new VLAN.
   c. Click *Apply* to save the change.
5. Assign other ports to static VLANs as needed.



Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	PoE	DHCP Snooping
S108EP5918004833 10								
port1		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	Untrusted
port2		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	Untrusted
port3		Static		Edge Port Spanning Tree Protocol	VLAN100	quarantine.fortilink (quarantine)	Powered	Untrusted
port4		Static		Edge Port Spanning Tree Protocol	VLAN100	quarantine.fortilink (quarantine)	Powered	Untrusted
port5		Static		Edge Port Spanning Tree Protocol	VLAN200	quarantine.fortilink (quarantine)		Untrusted
port6		Static		Edge Port Spanning Tree Protocol	VLAN200	quarantine.fortilink (quarantine)		Untrusted
port7					FGT61FTK19005527			
port8					FGT61FTK19005527			
port9		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)		Untrusted
port10		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)		Untrusted

Step 4: Set up NAC and create NAC policies

NAC identifies a device by some criteria, such as the operating system and hardware vendor, and then assigns it to a policy-defined VLAN.

By default, there is an onboarding VLAN for NAC onboarding devices. For NAC, the onboarding VLAN is treated differently than other VLANs. When a device connects to a switch port in NAC mode, the device goes the following process:

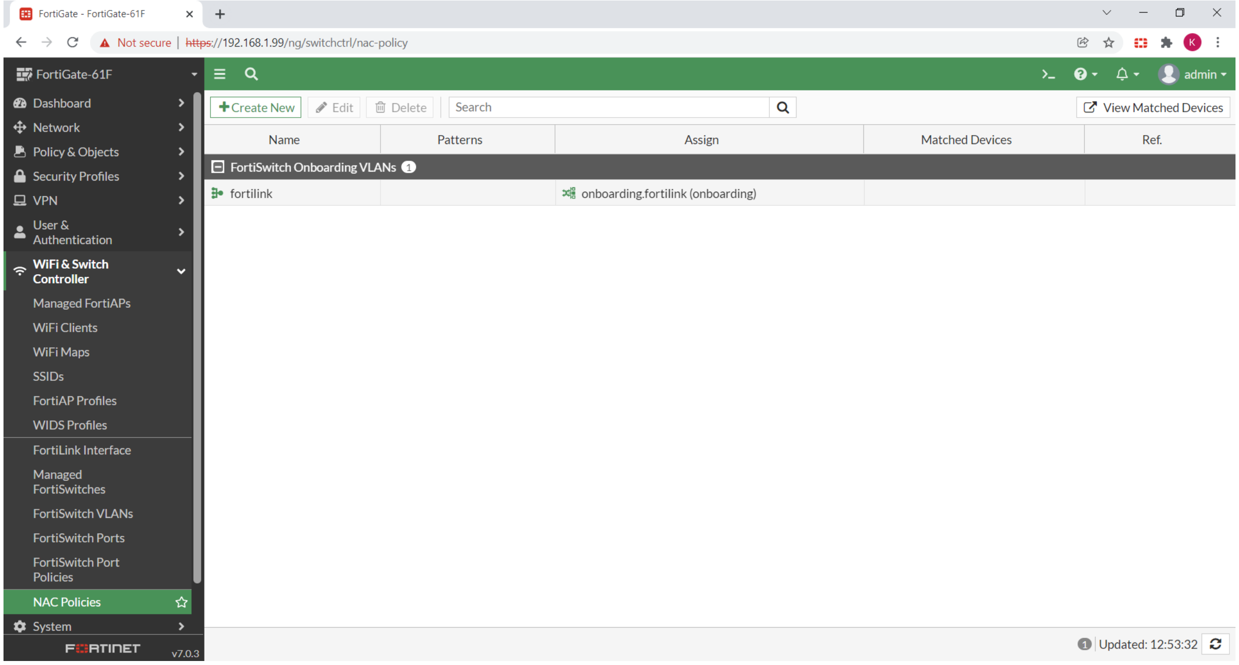
1. The device gets a DHCP address on the onboarding VLAN.
2. The device gets categorized by a NAC policy.
3. The device gets a new DHCP address on the assigned VLAN.

If the device does not match any category, the device remains in the onboarding VLAN. Therefore, consider applying stricter restrictions on the policy to allow traffic for the onboarding VLAN.

By default, there are other default defined VLANs that you can use for your NAC policies. You can also add additional VLANs for your NAC policy.

Change the onboarding VLAN

By default, FortiGate NAC policies place onboarding devices into the onboarding VLAN. To change this behavior, you can edit the VLAN from *NAC Policies* > *FortiSwitch VLANs* and edit the FortiLink interface.



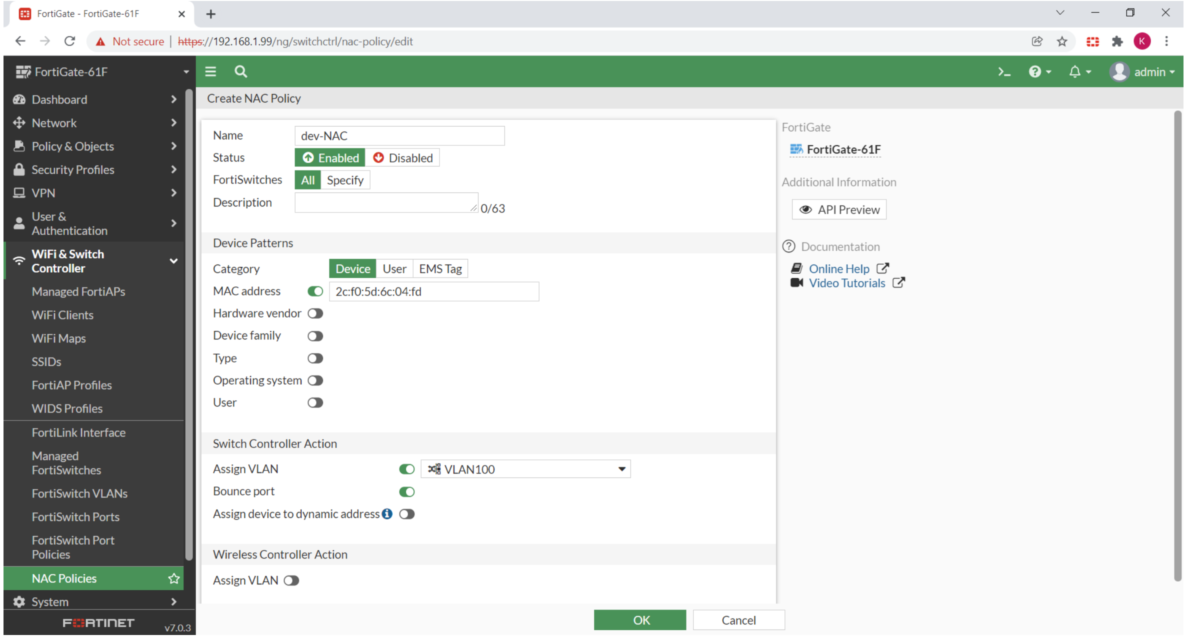
Name	Patterns	Assign	Matched Devices	Ref.
FortiSwitch Onboarding VLANs 1				
fortilink		onboarding.fortilink (onboarding)		

Set up NAC policies on the FortiSwitch unit

You can define additional rules to assign devices into VLANs based on device patterns, user information, or EMS tags.

1. Go to *WiFi & Switch Controller* > *NAC Policies*.
2. Click *Create New* to created a FortiSwitch NAC policy.
   a. Enter `dev-NAC` for the name of the NAC policy.
   b. Click *Enabled* for the status.

c. Click *Device* for the category.
d. Enable *MAC address* and then enter a device MAC address using the `00:00:00:00:00:00` format.
e. You can enable multiple criteria.
f. Under *Switch Controller Action*, enable *Assign VLAN* and then select a previously configured VLAN from the dropdown list.



Create NAC Policy

Name: dev-NAC
Status: Enabled | Disabled
FortiSwitches: All | Specify
Description: 0/63

Device Patterns

Category: Device | User | EMS Tag
MAC address: 2c:f0:5d:6c:04:fd
Hardware vendor
Device family
Type
Operating system
User

Switch Controller Action

Assign VLAN: VLAN100
Bounce port
Assign device to dynamic address

Wireless Controller Action

Assign VLAN

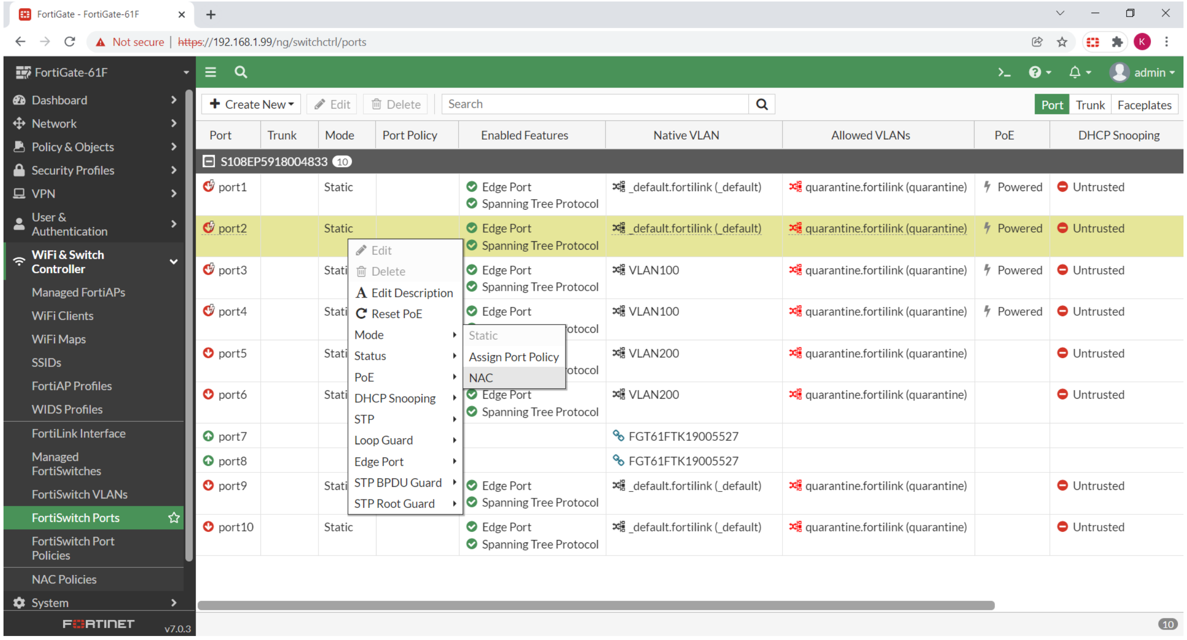
OK | Cancel

3. Click *OK* to save the NAC policy
4. Create other NAC policies to assign devices to different VLANs.

Assign ports to use a NAC policy

So far, you have statically assigned ports to a VLAN. However, for ports that require different access or security levels based on the device connected, they can be configured to use NAC policies.

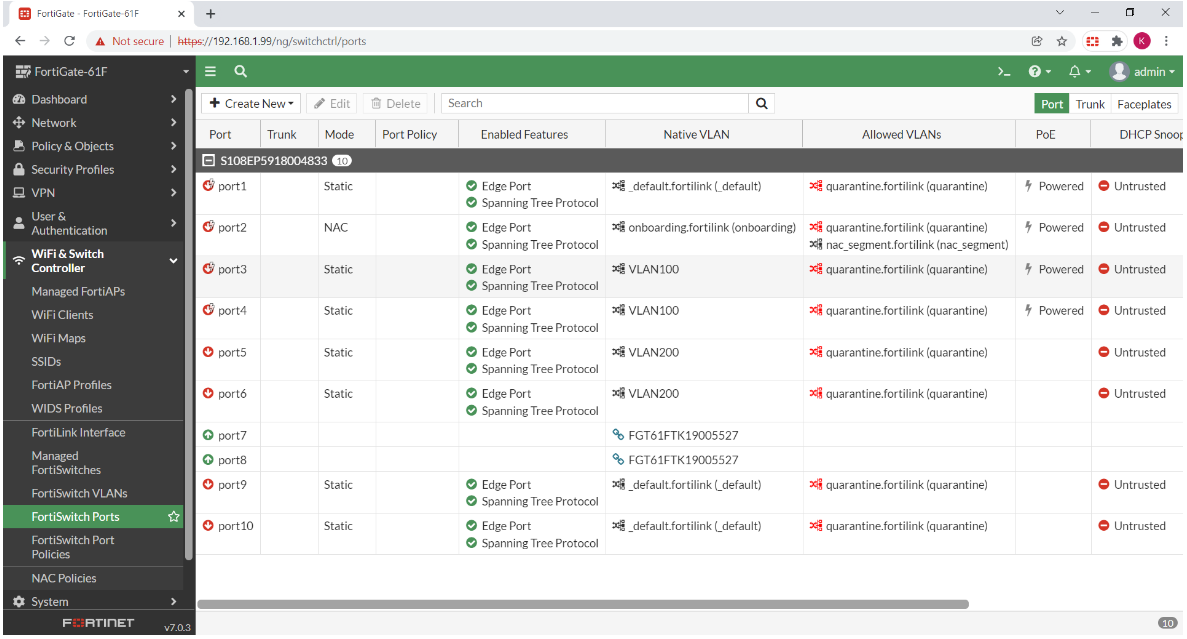
1. Go to *WiFi & Switch Controller* > *FortiSwitch Ports*.
2. Select the ports that need to be changed to NAC mode.
3. Right-click and select *Mode* > *NAC*.



S108EP5918004833 10

Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	PoE	DHCP Snooping
port1		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	Untrusted
port2		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	Untrusted
port3		Stati		Edge Port Spanning Tree Protocol	VLAN100	quarantine.fortilink (quarantine)	Powered	Untrusted
port4		Stati		Edge Port otocol	VLAN100	quarantine.fortilink (quarantine)	Powered	Untrusted
port5		Stati		otocol	VLAN200	quarantine.fortilink (quarantine)		Untrusted
port6		Stati		Edge Port Spanning Tree Protocol	VLAN200	quarantine.fortilink (quarantine)		Untrusted
port7					FGT61FTK19005527			
port8					FGT61FTK19005527			
port9		Stati		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)		Untrusted
port10		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)		Untrusted

4. After applying the NAC mode, refresh the page in a few seconds. The *Native VLAN* value will be updated.



S108EP5918004833 10

Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	PoE	DHCP Snoop
port1		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)	Powered	Untrusted
port2		NAC		Edge Port Spanning Tree Protocol	onboarding.fortilink (onboarding)	quarantine.fortilink (quarantine) nac_segment.fortilink (nac_segment)	Powered	Untrusted
port3		Static		Edge Port Spanning Tree Protocol	VLAN100	quarantine.fortilink (quarantine)	Powered	Untrusted
port4		Static		Edge Port Spanning Tree Protocol	VLAN100	quarantine.fortilink (quarantine)	Powered	Untrusted
port5		Static		Edge Port Spanning Tree Protocol	VLAN200	quarantine.fortilink (quarantine)		Untrusted
port6		Static		Edge Port Spanning Tree Protocol	VLAN200	quarantine.fortilink (quarantine)		Untrusted
port7					FGT61FTK19005527			
port8					FGT61FTK19005527			
port9		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)		Untrusted
port10		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)		Untrusted

FortiSwitch configuration complete

Your FortiSwitch configuration is now complete. Connecting devices to ports in static mode allows traffic to pass through the firewall policy assigned to those VLANs. Connecting devices to the NAC-mode port places the device in the VLAN based on the NAC policy that matches.

Step 5: Deploy WiFi

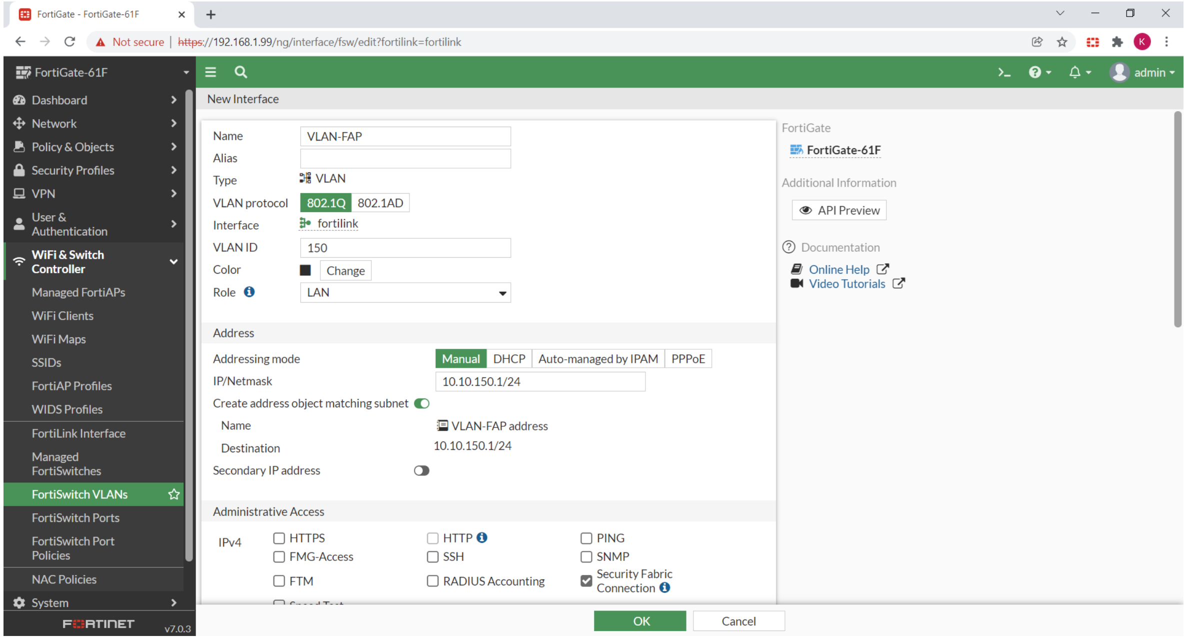
This deployment guide does not cover the details of installing access points (APs); see the FortiAP Quick Start Guides. However, here are some of the best practices to follow:

- Access points with integrated/internal antennas are intended for ceiling mounts. If wall mounting is necessary, use an external antenna access point with the appropriate antenna.
  - All antennas have a directional element. Omnidirectional antennas propagate the signal in a donut pattern (a torus) and have the strongest signal at the level of the access point. They work fine for 10-20-foot ceilings. Down-pointed directional antennas might be better for higher ceilings. High-gain omnidirectional antennas are a poor choice for high ceilings because they flatten the donut into a pancake, raising signal strength at the ceiling level.
  - Wall-mounted access points must have external antennas so that the signal can be directed properly. Omnidirectional antennas (the standard “rubber ducks”) need to be vertically aligned.
- Be sure you have the correct power over Ethernet (PoE) level to power the access points available from the switch and that the total PoE budget is sufficient for the total number of access points.
- Note the MAC address and/or a serial number of the access points and their locations. These notes will help with later documentation.
- When running cable for access points, leave plenty of extra cable at the AP end to allow the access point to be moved to adjust coverage. Sometimes a few feet (meters) can eliminate an unanticipated dead spot.

Add an AP VLAN

Prepare an AP VLAN by going to *WiFi & Switch Controller* > *FortiSwitch VLANs* and creating a VLAN (see Create FortiSwitch VLANs on page 15) for AP management (control plane). This VLAN creates security isolation between the AP management (control channel) and user traffic (data channel).

1. Enter a name for the VLAN.
2. Assign a VLAN ID.
3. Select *Manual* for the addressing mode and assign a VLAN/gateway IP address.
4. Under *Administrative Access*, click *Security Fabric Connection*. Add other access types as needed.



New Interface

Name: VLAN-FAP
Alias:
Type: VLAN
VLAN protocol: 802.1Q | 802.1AD
Interface: fortilink
VLAN ID: 150
Color: Change
Role: LAN

Address

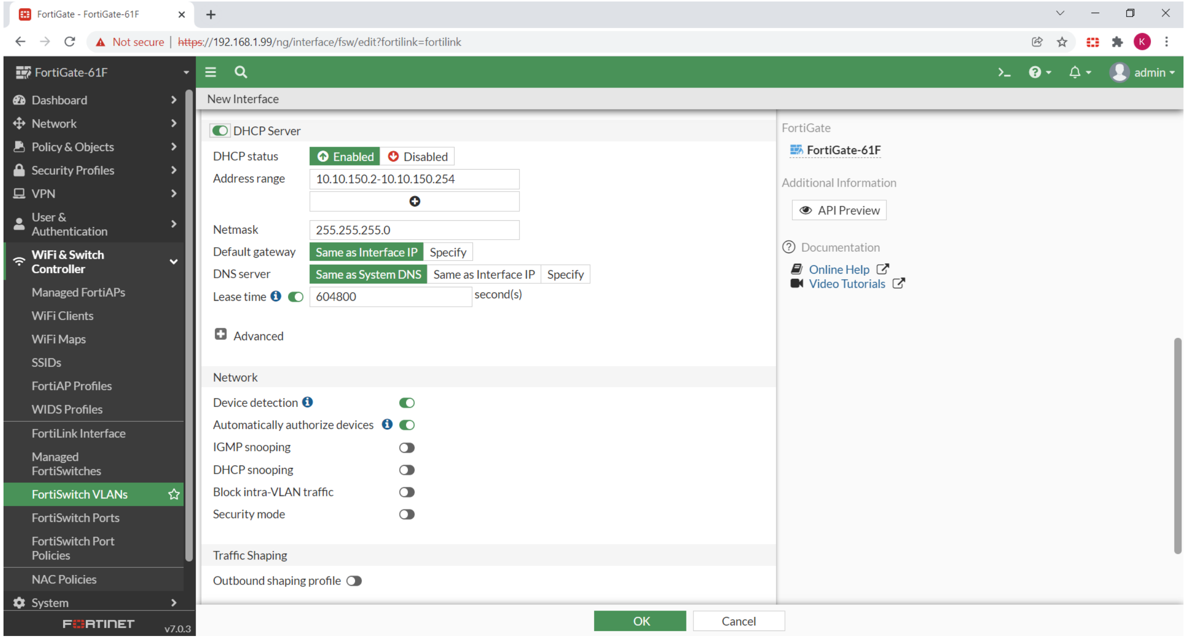
Addressing mode: Manual | DHCP | Auto-managed by IPAM | PPPoE
IP/Netmask: 10.10.150.1/24
Create address object matching subnet: enabled
Name: VLAN-FAP address
Destination: 10.10.150.1/24
Secondary IP address: disabled

Administrative Access

IPv4: ☐ HTTPS ☐ HTTP ☐ PING ☐ FMG-Access ☐ SSH ☐ SNMP ☐ FTM ☐ RADIUS Accounting ☑ Security Fabric Connection

5. Enable *DHCP server* and enter the IP address range.
6. Under *Network*, enable *Device detection*.
7. Enable *Automatically authorize devices*.

   Even in a high-security environment, it is usually best to enable this option until the initial deployment is done. Then disable it to lock down the network.



New Interface

DHCP Server: enabled
DHCP status: Enabled | Disabled
Address range: 10.10.150.2-10.10.150.254
Netmask: 255.255.255.0
Default gateway: Same as Interface IP | Specify
DNS server: Same as System DNS | Same as Interface IP | Specify
Lease time: 604800 second(s)
Advanced

Network

Device detection: enabled
Automatically authorize devices: enabled
IGMP snooping: disabled
DHCP snooping: disabled
Block intra-VLAN traffic: disabled
Security mode: disabled

Traffic Shaping

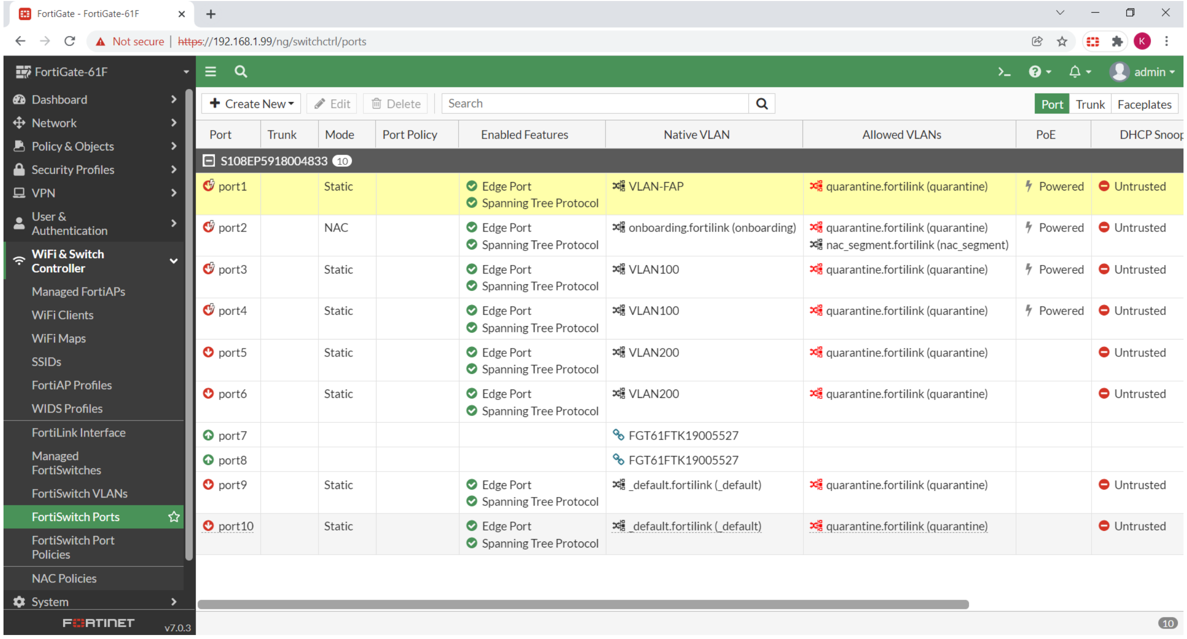
Outbound shaping profile: disabled

8. Click *OK*.

Assign the AP VLAN to AP ports on the FortiSwitch unit

Any FortiAP units connected to the FortiSwitch ports that are assigned as the AP VLAN will automatically connect to the FortiGate device, get an IP address, and be authorized by the FortiGate device. To simplify the deployment, a FortiAP unit can connect to a FortiSwitch PoE port for power. Otherwise, an external power source is needed.

1. Go to *WiFi & Switch Controller > FortiSwitch Ports.*
2. Select a PoE-capable port if possible and change the native VLAN to the AP VLAN.



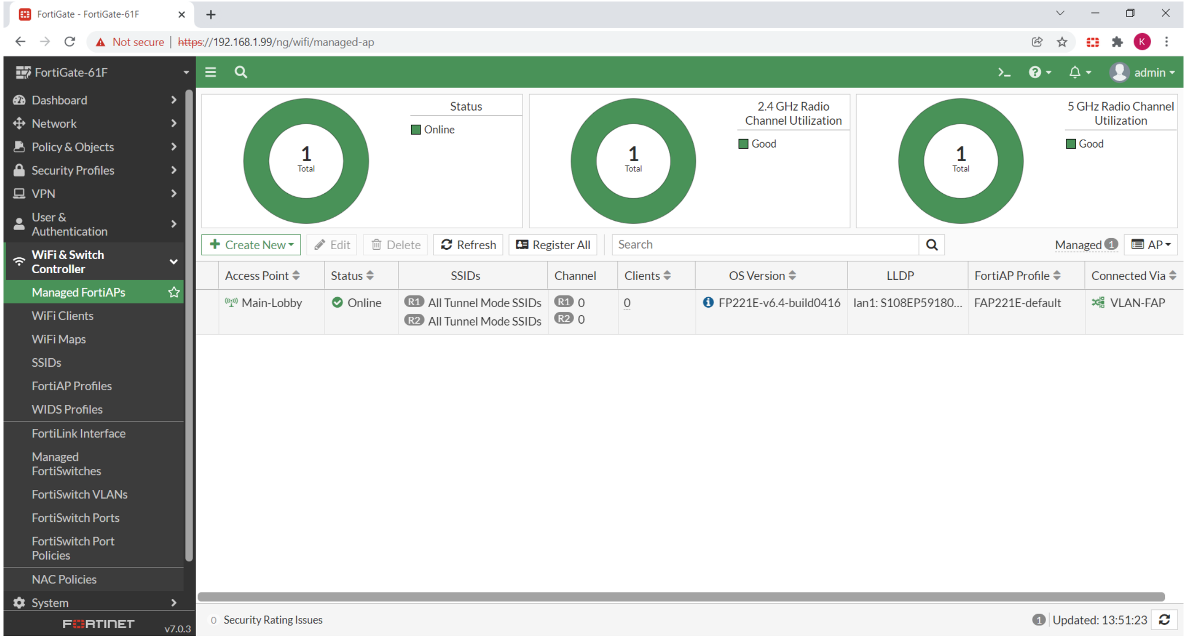
S108EP5918004833 10

Port	Trunk	Mode	Port Policy	Enabled Features	Native VLAN	Allowed VLANs	PoE	DHCP Snoop
port1		Static		Edge Port Spanning Tree Protocol	VLAN-FAP	quarantine.fortilink (quarantine)	Powered	Untrusted
port2		NAC		Edge Port Spanning Tree Protocol	onboarding.fortilink (onboarding)	quarantine.fortilink (quarantine) nac_segment.fortilink (nac_segment)	Powered	Untrusted
port3		Static		Edge Port Spanning Tree Protocol	VLAN100	quarantine.fortilink (quarantine)	Powered	Untrusted
port4		Static		Edge Port Spanning Tree Protocol	VLAN100	quarantine.fortilink (quarantine)	Powered	Untrusted
port5		Static		Edge Port Spanning Tree Protocol	VLAN200	quarantine.fortilink (quarantine)		Untrusted
port6		Static		Edge Port Spanning Tree Protocol	VLAN200	quarantine.fortilink (quarantine)		Untrusted
port7					FGT61FTK19005527			
port8					FGT61FTK19005527			
port9		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)		Untrusted
port10		Static		Edge Port Spanning Tree Protocol	_default.fortilink (_default)	quarantine.fortilink (quarantine)		Untrusted

10

3. Connect the access points with Ethernet cables to the correct ports on the PoE-capable FortiSwitch unit and give them a few minutes to start and become authorized.

   You can check the progress by going to *Security Fabric > Physical Topology* or in *WiFi & Switch Controller > Managed FortiAPs*.
4. Go to *WiFi & Switch Controller > Managed FortiAPs*.
5. If necessary, change the view in the dropdown list from *Group* to *AP*.



Access Point	Status	SSIDs	Channel	Clients	OS Version	LLDP	FortiAP Profile	Connected Via
Main-Lobby	Online	R1 All Tunnel Mode SSIDs R2 All Tunnel Mode SSIDs	R1 0 R2 0	0	FP221E-v6.4-build0416	lan1: S108EP59180...	FAP221E-default	VLAN-FAP

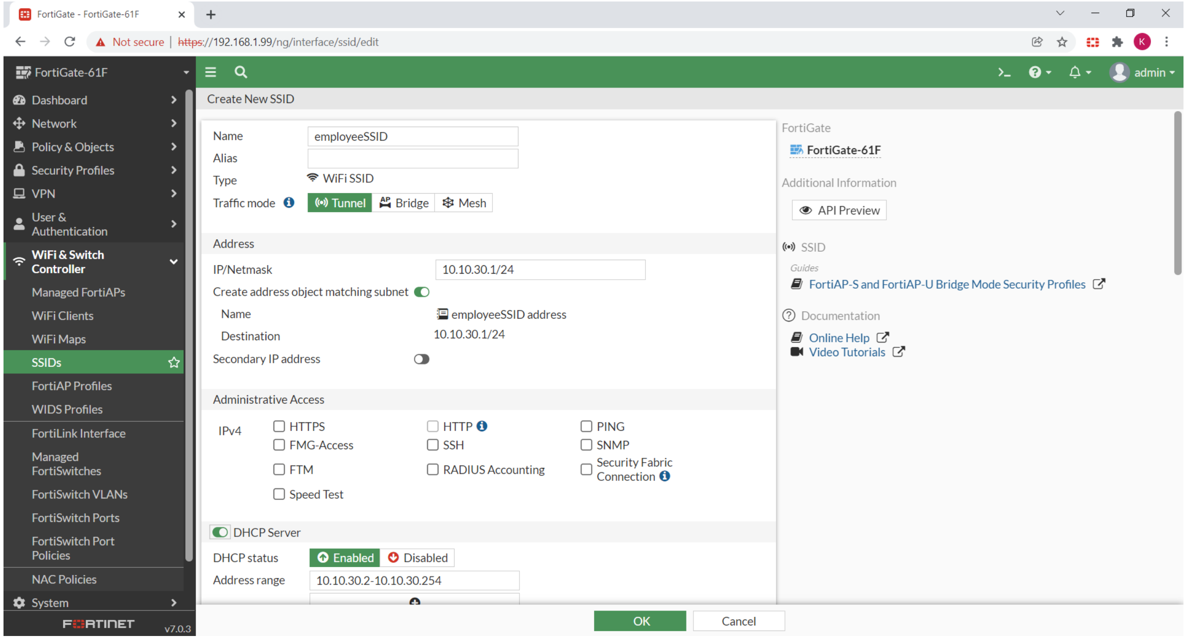
6. If necessary, access points that have not been automatically authorized can be authorized using the right-click menu or the *Edit* button.
7. Fortinet recommends using the edit function to rename the access points to something helpful, such as "Main-Lobby" or "breakroom."

Create SSIDs

1. Go to *WiFi & Switch Controller* > *SSIDs*.
2. Click *Create New* > *SSID*.
3. Enter a name for the SSID.

   This is an internal name and does not have to match an over-the-air SSID.
4. Make certain that *Tunnel* is selected for the traffic mode.

   In tunnel mode, WLANs are treated as interfaces in the FortiGate device and behave as a VLAN interface.
5. Assign an IP address (VLAN gateway) and set up the DHCP server.



Create New SSID

Name: employeeSSID
Alias:
Type: WiFi SSID
Traffic mode: Tunnel | Bridge | Mesh

Address
IP/Netmask: 10.10.30.1/24
Create address object matching subnet: ●
Name: employeeSSID address
Destination: 10.10.30.1/24
Secondary IP address: ○

Administrative Access
IPv4
□ HTTPS □ HTTP □ PING
□ FMG-Access □ SSH □ SNMP
□ FTM □ RADIUS Accounting □ Security Fabric Connection
□ Speed Test

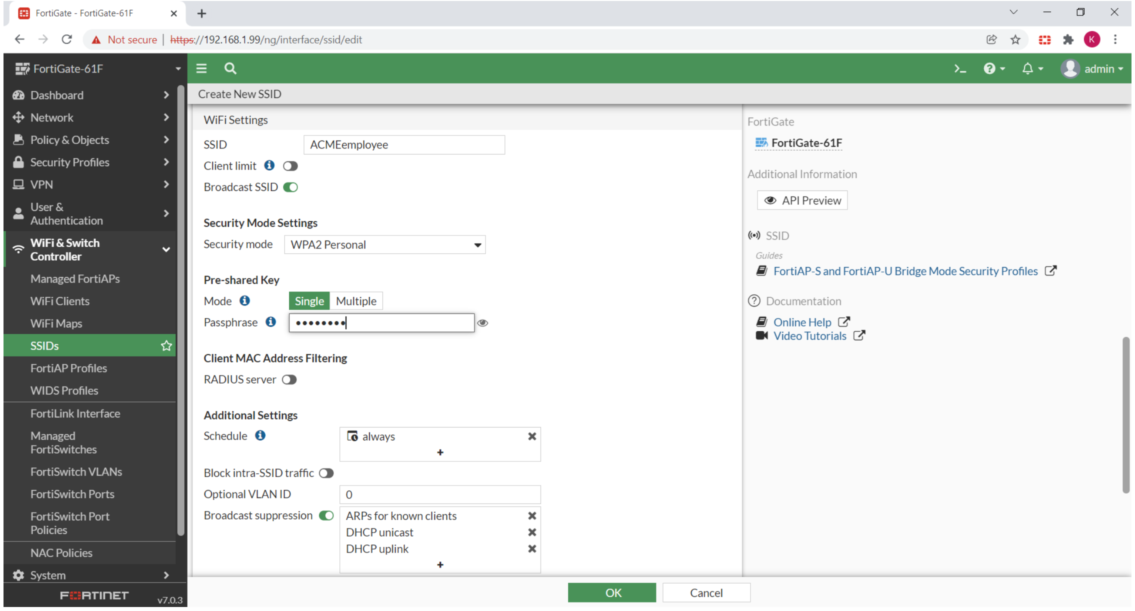
DHCP Server
DHCP status: Enabled | Disabled
Address range: 10.10.30.2-10.10.30.254

FortiGate
FortiGate-61F
Additional Information
API Preview
SSID
Guides
FortiAP-S and FortiAP-U Bridge Mode Security Profiles
Documentation
Online Help
Video Tutorials

6. Under *WiFi Settings*, configure the following:
   a. Enter the name of the SSID.

      This is the over-the-air name.
   b. Select *WPA3 SAE* or *WPA2 Personal* for the security mode.

      Ideally, as you refine your security policies, you will use one of the enterprise security modes. See the primary documentation for how to set up WPA2 Enterprise and WPA3 Enterprise with a RADIUS server.
   c. Enter a pre-shared key.



Create New SSID

WiFi Settings
SSID: ACMEmployee
Client limit: ○
Broadcast SSID: ●

Security Mode Settings
Security mode: WPA2 Personal

Pre-shared Key
Mode: Single | Multiple
Passphrase: ••••••••

Client MAC Address Filtering
RADIUS server: ○

Additional Settings
Schedule: always
Block intra-SSID traffic: ○
Optional VLAN ID: 0
Broadcast suppression: ● ARPs for known clients, DHCP unicast, DHCP uplink

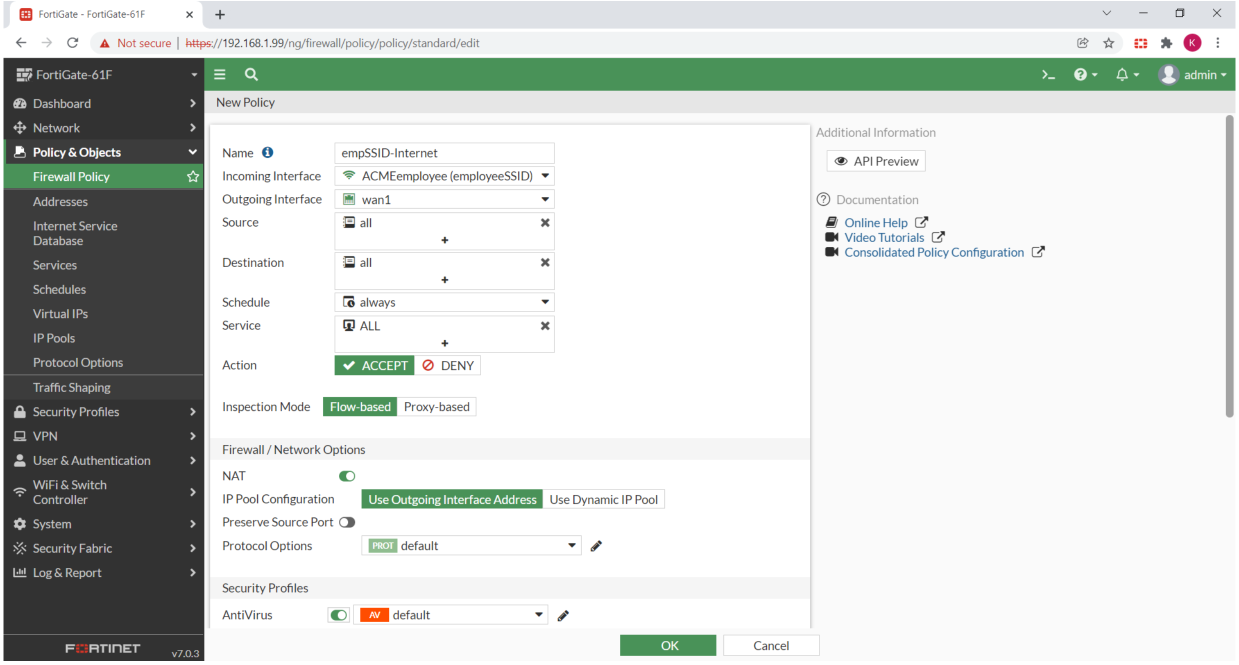
FortiGate
FortiGate-61F
Additional Information
API Preview
SSID
Guides
FortiAP-S and FortiAP-U Bridge Mode Security Profiles
Documentation
Online Help
Video Tutorials

   d. Click *OK*.

The SSIDs are deployed to the APs. More complex deployments involving groups of access points with different WLANs can be configured. See the primary documentation.

Configure the firewall policies

Firewall policies must be configured (see Create firewall policies for Internet access on page 17) to allow wireless access from the SSID. Here you can also define the profiles to use for scanning the traffic.



New Policy

Name: empSSID-Internet
Incoming Interface: ACMEemployee (employeeSSID)
Outgoing Interface: wan1
Source: all
Destination: all
Schedule: always
Service: ALL
Action: ✓ ACCEPT | DENY
Inspection Mode: [✓ Flow-based] Proxy-based

Firewall / Network Options

NAT: ● (on)
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port: ○ (off)
Protocol Options: PROT default

Security Profiles

AntiVirus: ● AV default

Deployment complete

The basic LAN edge network design is configured. The FortiGate device is a gateway to the Internet, a FortiSwitch unit is connected and communicating over a FortiLink, Wi-Fi is available, and an example NAC policy is configured.

You can refer to other Fortinet documentation to further secure, refine, optimize, and scale your solution.

Appendix A: Products used in this guide

The following product models and firmware were used in this guide. FortiSwitch 7.0 and FortiAP 7.0 can also be used for this deployment.

Product	Model	Firmware
FortiGate	FortiGate 61F	7.0.3
FortiSwitch	FortiSwitch 108E-POE	6.4.4
FortiAP	FortiAP 221E	6.4.4

Appendix B: Documentation references

For more information, use the following resources:

- Product administration guides
  - FortiGate Administration Guide
  - Managed FortiSwitch Administration Guide
  - FortiWiFi and FortiAP Configuration Guide
- Solution hub
  - Secure Access

FURTINET

www.fortinet.com