

DEPLOYMENT GUIDE

Fortinet Verified Design for LAN Edge Initial Deployment

For Network Engineers Deploying Basic Fortinet LAN Edge Solution in a Single Office

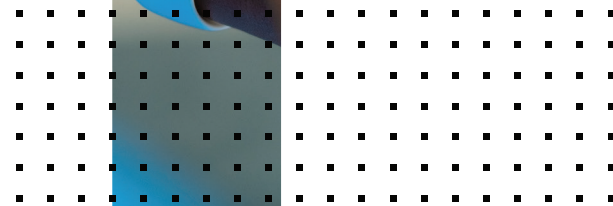


Table of Contents

- Introduction 3
- Deployment Assumptions 3
- Steps To Follow 4
- Create and Assign VLANs in the Switch Controller 11
- Configuration Is Complete 21



Introduction

One of the great strengths of Fortinet LAN Edge and other solutions is the tight integration of everything via FortiLink. With FortiLink, FortiSwitches and FortiAPs are extensions of the FortiGate. 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, this is Security-Driven Networking.

Fortinet 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.

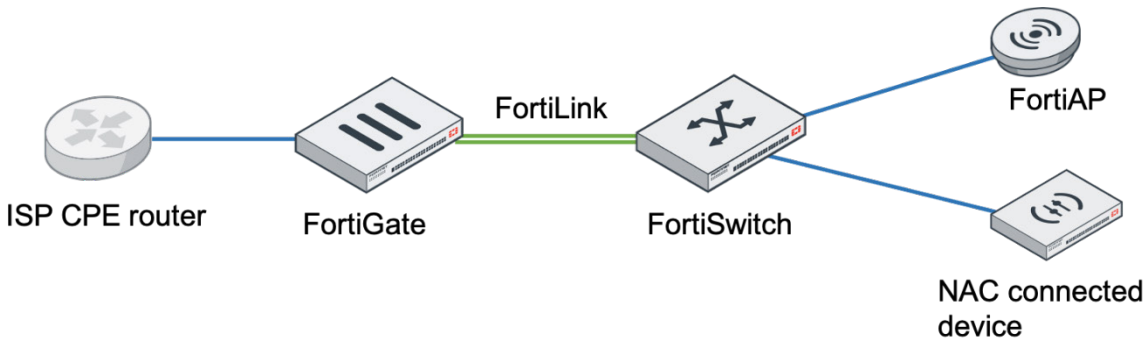


Figure 1: Fortinet LAN Edge equipment.

Security-Driven Networking is compelling and simplifies the network overall, but the integrated whole can be confusing. Everything needed in a network is in the FortiGate, and with all that integration that makes it so powerful, it can be hard to decide where to start.

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 document 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.

Deployment Assumptions

- 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 the FortiGate WAN link.
 - The physical WAN connection is Ethernet.
- The deployment will consist of:
 - One FortiGate
 - One FortiSwitch
 - One or more FortiAPs
- All necessary Ethernet cabling is available or already deployed/patched.
- This guide is written using FortiOS 7.0. There may be some differences if running a different version of FortiOS.
- A laptop or other management station with an Ethernet port is available.

Steps To Follow

- Bring up a FortiGate and connect to an ISP.
- Configure FortiLink and add a switch.
- Add one or more FortiAPs.
- Configure a typical SSID.
- Configure FortiOS NAC on the switch.

Bring up the FortiGate

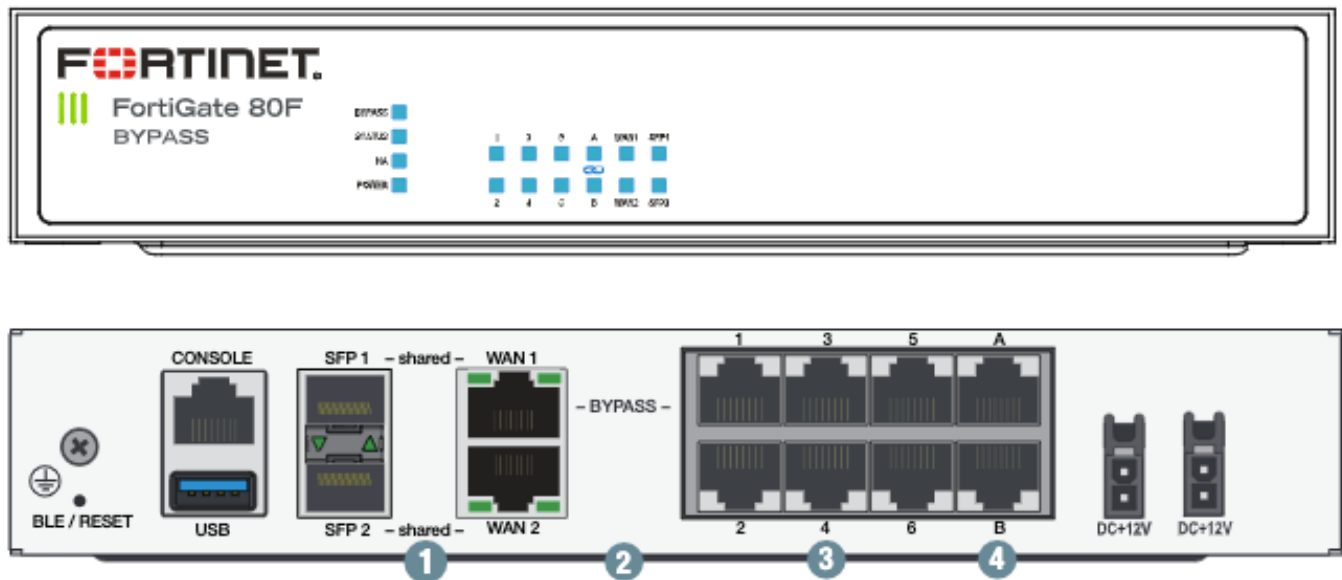


Figure 2: FortiGate ports. On larger models, DMZ, HA, and MGMT ports may also be available.

When a FortiGate is fresh out of the box, depending on the model, there is 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, we will 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.

Default settings on an out-of-the-box FortiGate include:

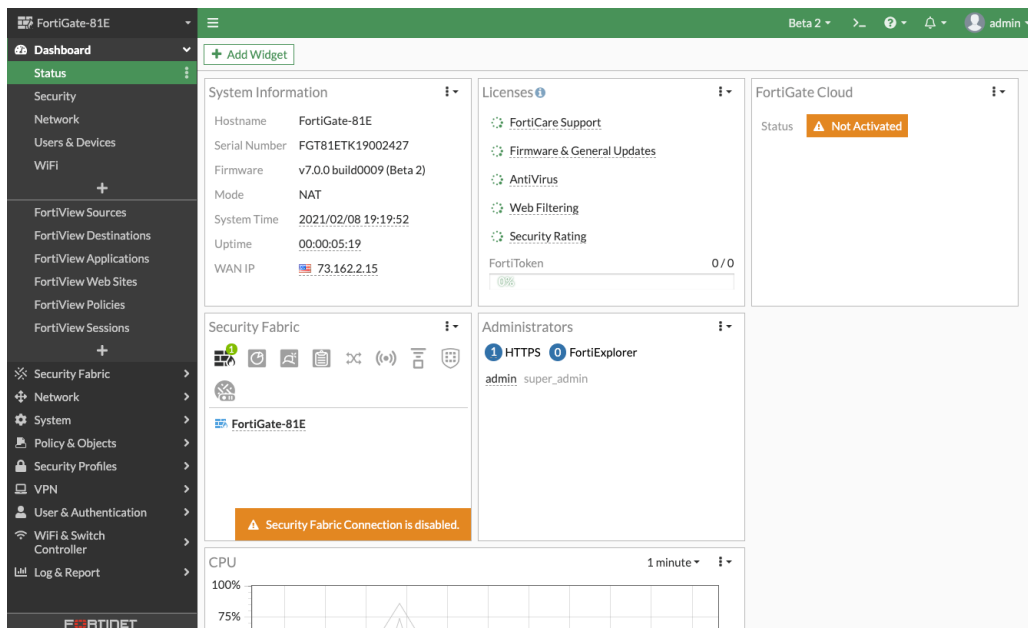
- Management IP address and login credentials
 - 192.168.1.99
 - User: admin
 - Password: <blank>
 - The FortiGate will prompt for a new password at the first login.

- DHCP server is enabled on MGMT port (if it exists).
 - Addresses will be 192.168.1.0/24, with FortiGate as the default GW.
 - If there is no MGMT port, LAN port one will match the above.
 - If there is an MGMT port, the LAN ports will default to a different subnet.
- WAN 1 - DHCP client (will request an IP from the ISP).
- A firewall policy is allowing outgoing traffic from LAN ports but not allowing incoming traffic from the internet/uplink (WAN1).
 - If MGMT is a separate port, then it will NOT have default internet access.
- If the FortiGate has ports labeled A and B, these are preconfigured for FortiLink.

Power on and the first login

- Plug in the FortiGate and power it on.
 - Depending on the model, it may have a power switch, or it may just respond when plugged in. Give it a moment to boot. Let the lights settle down.
- Plug the ISP uplink into the FortiGate WAN1 port.
- Connect a management station (i.e., administrator laptop) to the MGMT port (or LAN port 1) via Ethernet cable (or LAN port 1).
 - The management station should get an IP address from the FortiGate.
 - If it does not, configure the management station to 192.168.1.110/255.255.255.0, GW 192.168.1.99.
 - When there is an existing Wi-Fi network, it's recommended to leave out the gateway setting to use Wi-Fi to access the internet while configuring the FortiGate.
- Open a web browser and connect to 192.168.1.99.
 - There will probably be a certificate error, as FortiGate uses a self-signed certificate rather than one from a Certificate Authority the browser already trusts. Proceed anyway.
 - If Chrome does not proceed, in the browser window (not the address bar), type: "thisisunsafe" (it will not be visible). Proceed.
- At the login page, enter username admin and leave the password blank. Hit enter.
- When prompted for a new password, choose anything that fits the password policy. Leave the old password blank.
 - The original login page appears, but now admin and the new password will work.
- The first boot sequence setup continues with a FortiGate setup screen.
 - These configurations can be done now or later. This document will skip these details. Click later to skip until later, or follow through now.
 - There may also be a what's new video, which can be watched now or later.
- A station Ethernet-connected to a FortiGate LAN port should now be able to access the internet through the FortiGate firewall. In the next section, the network interface settings will be confirmed and the basics of FortiGate network configuration will be covered.





Basic FortiGate navigation and confirmation of network setup

Note - no configuration changes will be needed in this section.

This section primarily goes over what is already configured by default to serve as a basic introduction to FortiGate networking. Depending on the FortiGate model, the most likely place to require some configuration changes is FortiLink.

FortiGate navigation

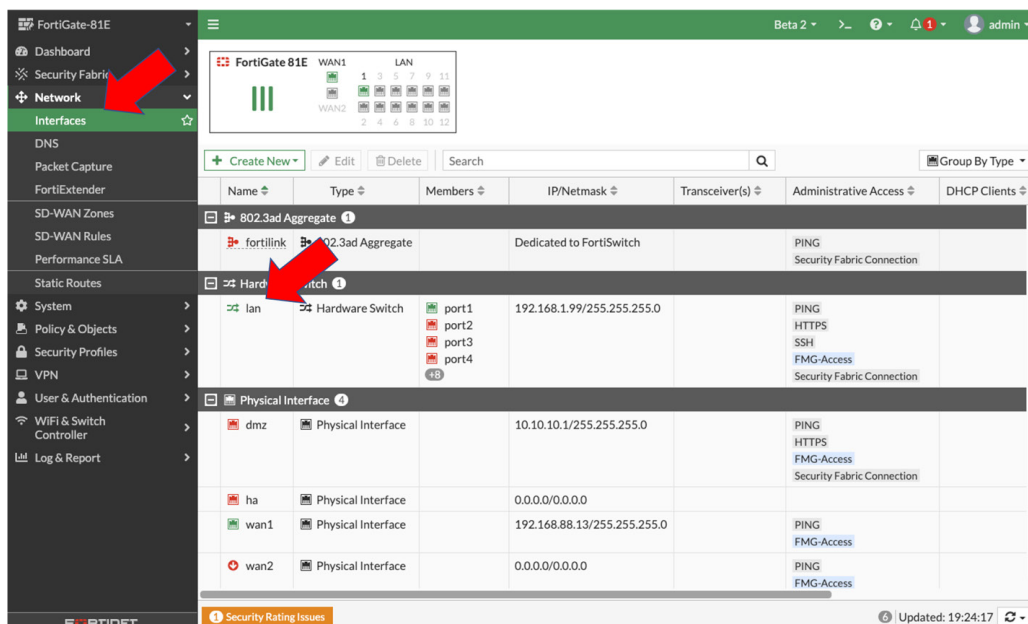
Connect and log in to the FortiGate via a web browser as described above.

- MGMT or LAN1, 192.168.1.99/admin/<blank/password>

In the FortiGate GUI, using the left-hand menu ribbon, navigate to:

- Network → Interfaces

The predefined interfaces are here. This is where VLANs can be defined, assigned to ports, etc.

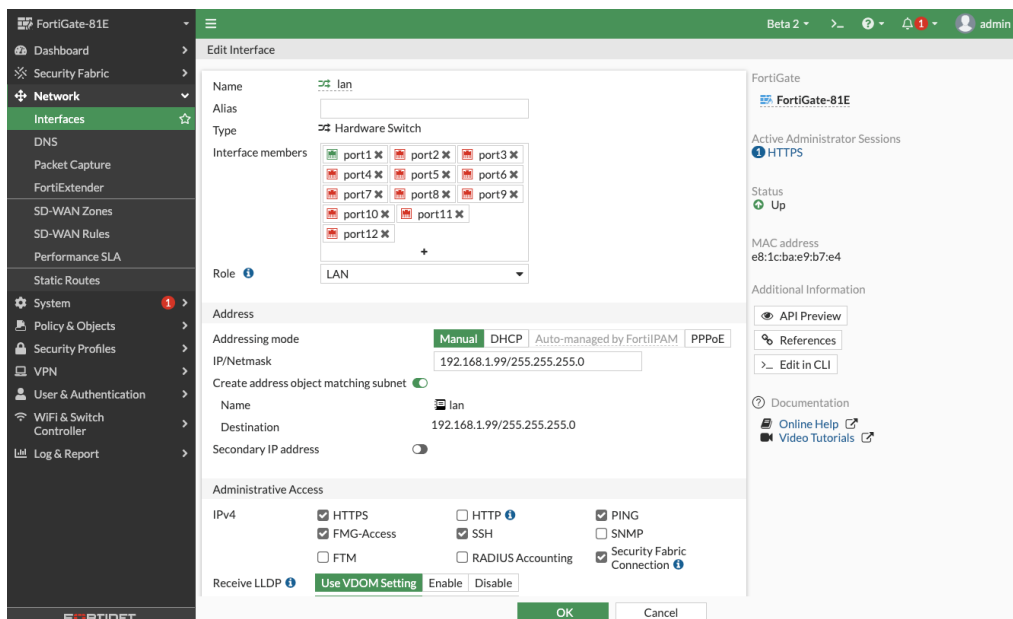


LAN preconfigured defaults

- In the Name column, find and double-click on LAN.
- Scroll through the Edit Interface screen to gain familiarity.
 - Interface members/ports can be added and removed.
 - Address mode is set to manual.
 - The address will depend on whether there is an MGMT interface.
 - It can be changed, but that is not necessary.
 - The DHCP server is enabled.
 - When done, click cancel.

WAN preconfigured defaults

- Back in the interfaces screen, find and double-click on WAN1.
 - WAN one should be green, as the port is active.
 - Address mode should be DHCP, with a status connected.
 - DHCP server is not available because the role is set to WAN.
 - When done, click cancel.

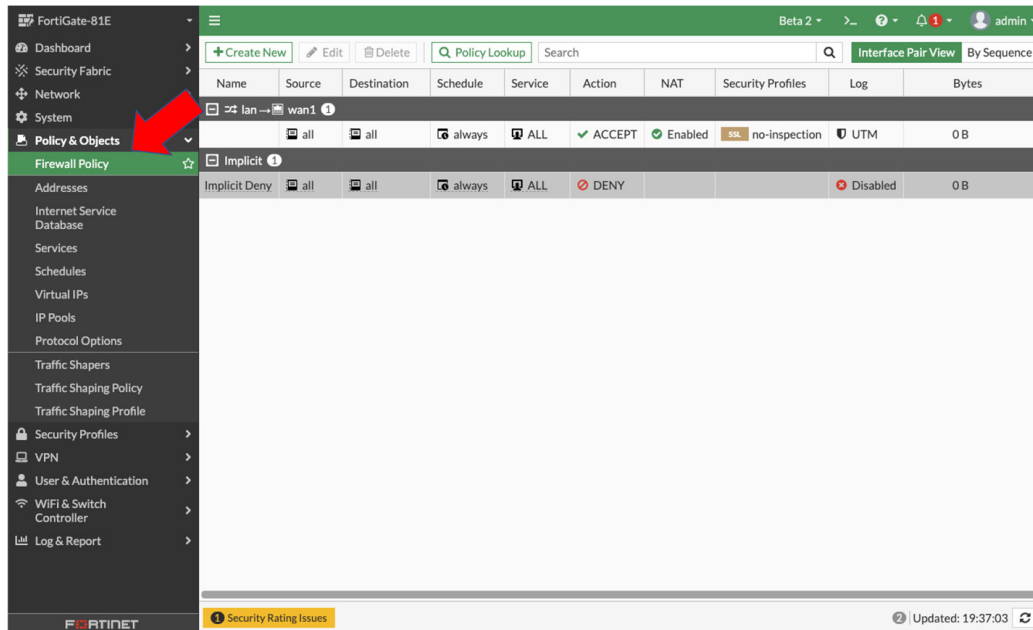


Firewall default policies

Firewall and other security policies can get complex, and this document is focused on the initial networking configuration. See other documentation at docs.fortinet.com.

Two rules are defined by default in the firewall policy. To view and confirm the policies:

- Navigate to Policy & Objects → Firewall Policy.
- The first default rule allows all traffic from the default LAN to go out of the WAN interface (to the internet).
- As is typical for a firewall rule base, the final rule denies all traffic not explicitly allowed above it.



Add a FortiSwitch with FortiLink

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

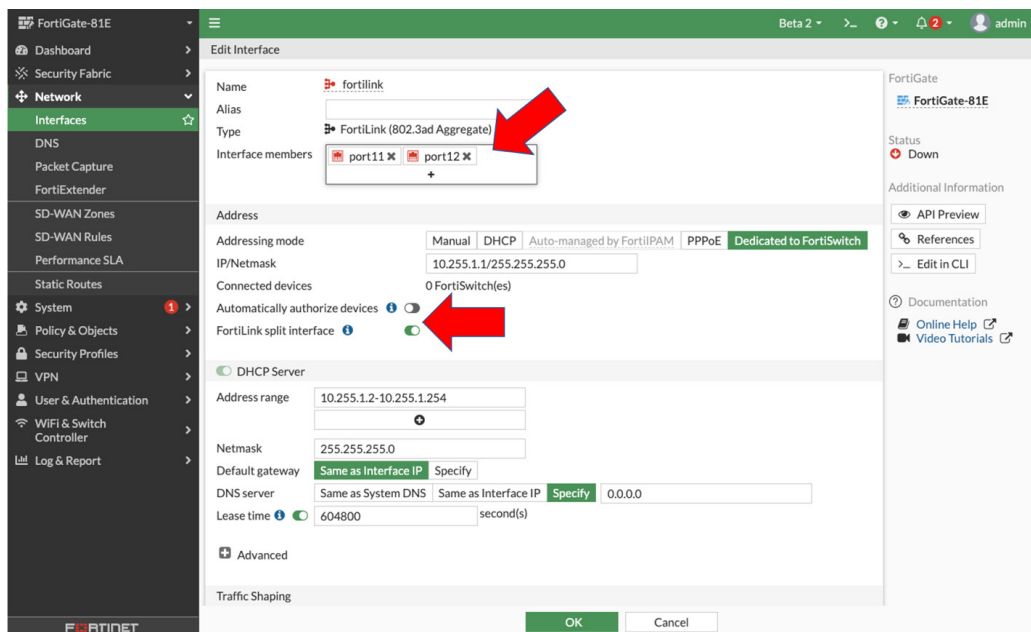
Adjust FortiLink defaults

Turn split interface off, enable automatic device authorization.

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

- From the left-side menu ribbon, navigate to Network → Interfaces.
- In the Interfaces screen, find and double-click on FortiLink.
- FortiLink settings:
 - Address mode defaults to Dedicated to FortiSwitch.
 - In the address section, ensure Automatically authorize devices is enabled with the associated toggle.
 - Devices can be manually admitted one at a time later.
 - At the bottom of the address section, FortiLink split interface needs to be disabled with the selection slider. The split interface is used in scenarios where more than one switch is connected directly to a FortiGate.
 - DHCP server is enabled.
- Notice the Interface members list at the top. Are there two members or no members?
 - If there are already two members, FortiLink is ready to connect to a switch. Note the two members (likely the ports labeled A and B if they exist on your physical FortiGate).
 - If there are no interface members, go on to the next section.
 - When done, click OK (to save slider change).





If the FortiLink had no member ports, two would be needed from the LAN interface members

- In the Interfaces screen, double-click on LAN.
- In the Interface members box, remove two physical ports by clicking on the x's.
 - A common practice is to use the two highest-numbered ports, but any two will do.
- Click OK at the bottom.
- Back in the Interfaces screen, double-click on FortiLink.
- In the Interface members box, add two physical ports by clicking on the + sign, then single-click on the appropriate ports from above.
- Click OK at the bottom.

Enable switch controller feature

FortiGate has so many features that many may not be visible in the GUI. Ensure the Switch Controller is visible in the GUI by checking Feature Visibility.

- In the left-hand navigation ribbon, go to System → Feature Visibility.
- In Core Features, check that the Switch controller toggle is on. If not, turn it on.
- In the Core Features section in the upper left, ensure that Switch Controller and WiFi Controller are both enabled.

Connect the FortiLink ports to the switch ports

- Unbox the FortiSwitch and deploy it, whether mounting it in a rack or otherwise.
- Power the FortiSwitch on.
- Connect the FortiSwitch to the FortiGate via two Ethernet connections. Use the two designated FortiLink ports of the FortiGate and the last two RJ-45 ports.
 - If you have populated the SFP ports on the switch and the FortiGate, use these instead.

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

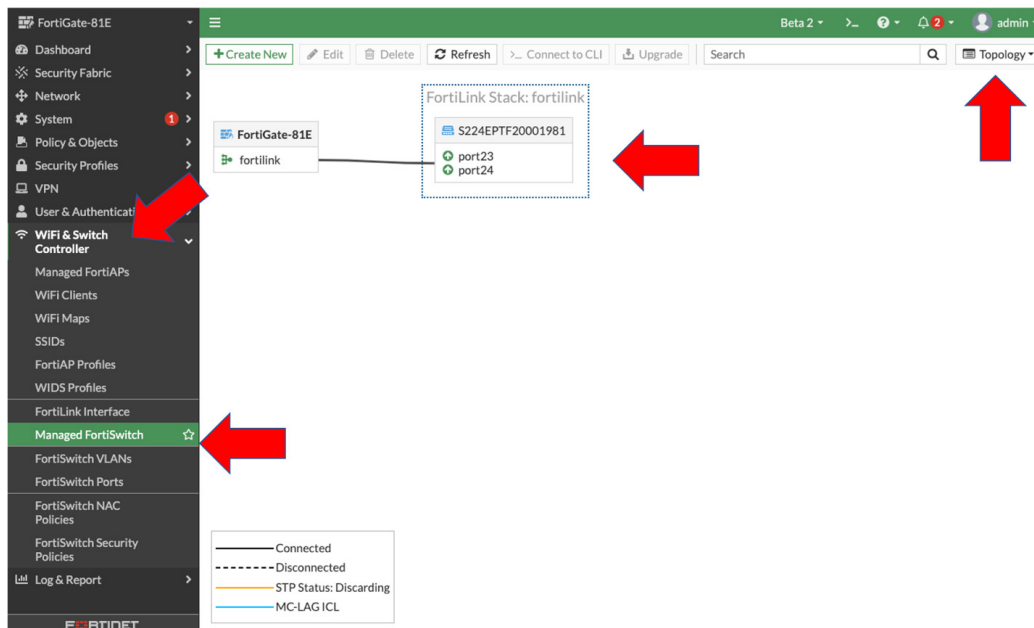


Explore the Switch Controller

- In the Navigation panel, expand WiFi & Switch Controller.
- Click on FortiLink Interface.
- This is the same FortiLink interface we configured earlier, but there are some additional options here. Specifically, this is where FortiOS NAC (network access control) is enabled. However, this will be covered later.

Managed FortiSwitch—topology and switch authorization

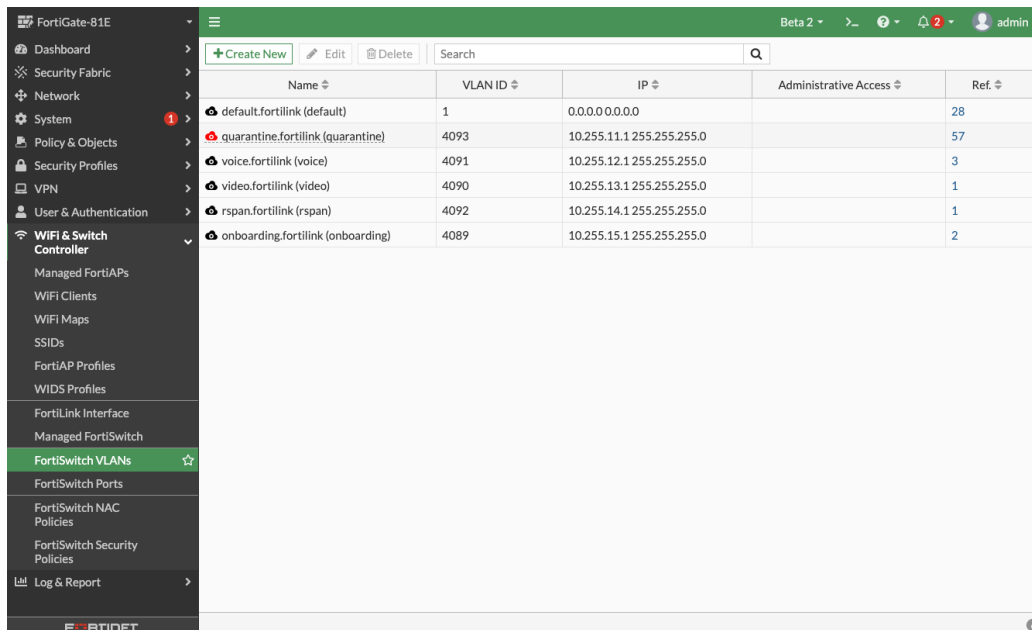
- In the navigation ribbon, click on WiFi & Switch Controller → Managed FortiSwitch.
- To get a topology view, use the upper right corner drop-down to switch to Topology View.
- The FortiSwitch should be visible, connected to the FortiGate.
 - If it has not been automatically authorized, click on the icon and authorize it.
- Hovering the mouse over the switch icon presents a context menu with several options.



Create and Assign VLANs in the Switch Controller

View FortiSwitch VLANs

- Navigate to WiFi & Switch Controller → FortiSwitch VLANs



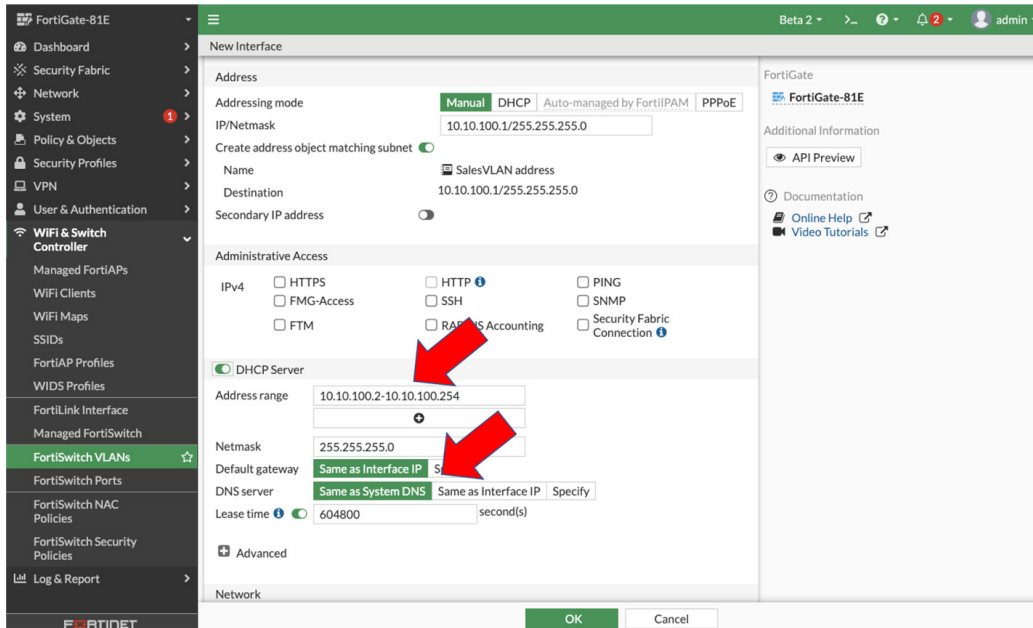
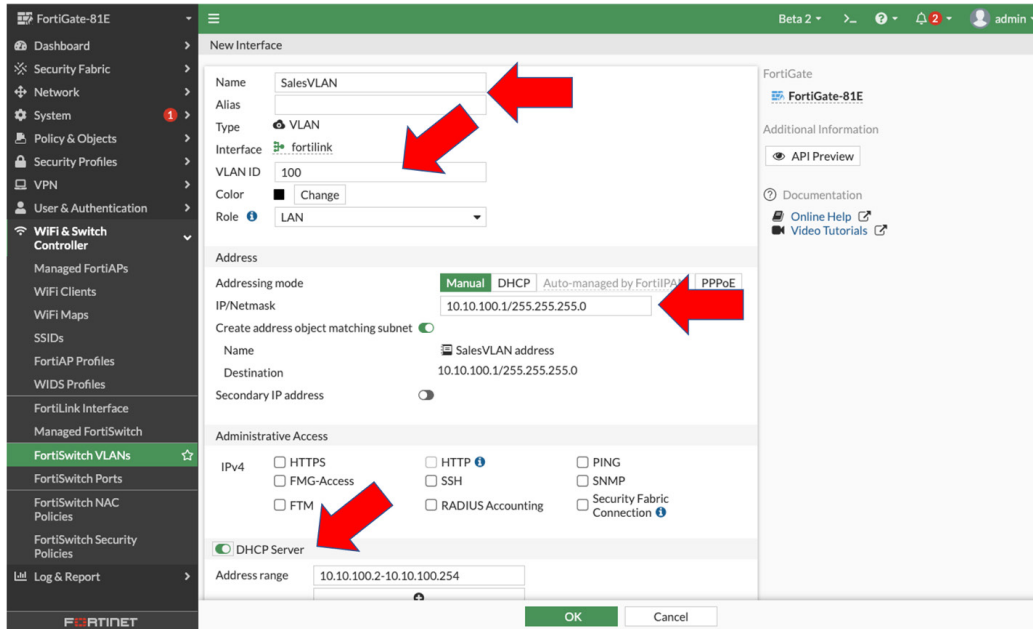
Name	VLAN ID	IP	Administrative Access	Ref
default.fortilink (default)	1	0.0.0.0/0.0.0		28
quarantine.fortilink (quarantine)	4093	10.255.11.1/255.255.255.0		57
voice.fortilink (voice)	4091	10.255.12.1/255.255.255.0		3
video.fortilink (video)	4090	10.255.13.1/255.255.255.0		1
rspan.fortilink (rspan)	4092	10.255.14.1/255.255.255.0		1
onboarding.fortilink (onboarding)	4089	10.255.15.1/255.255.255.0		2

There are several predefined VLANs for NAC purposes. We will dive deeper into that in a later section. For now, we will create two example VLANs.

Keep in mind that up to this point, the recommended configuration has been virtually identical to this guide. Now, specific deployments may have more reason to deviate from the guide. This may be due to a preferred IP address scheme and the number of VLANs needed, and if inter-VLAN routing is required. The following configuration is for two internal VLANs, both with internet access and routing between them allowed.

- Navigate to WiFi & Switch Controller → FortiSwitch VLANs.
- Click on Create New.
- Assign a VLAN name, e.g., VLAN100, Sales.
- Type is already set to VLAN, interface is FortiLink.
- Assign VLAN ID, a number between 2 and 4094 not already in use.
 - The default config is using high numbers 4089-4093 for the predefined VLANs.
- Choose the desired color.
- Role = LAN.
- Assign an IP address.
 - Choose manual for the addressing mode.
 - Enter IP/Netmask, e.g., 10.10.100.1/255.255.255.0.
 - Create address object matching subnet should be enabled. This will be useful in Policies later.

- Enable DHCP server
 - Accept the default address range, or adjust for the environment.
 - Accept Same as interface IP.
 - Accept Same as system DNS.
- Click OK.



For the second VLAN, repeat the above procedure with a different Interface address, e.g., VLAN200, 10.10.200.0/255.255.255.0, etc.



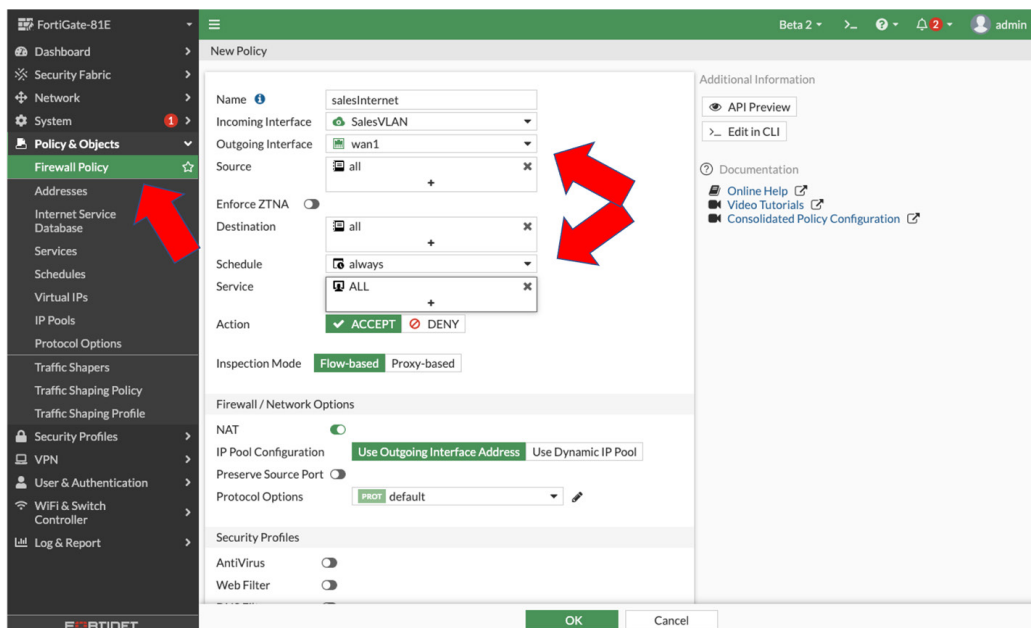
Enable firewall policies for internet access and inter-VLAN routing

Enable internet access from a VLAN

The internet access policies will mirror the LAN internet policy above.

- Go to Policy & Objects → Firewall Policy.
- Create New.
- Configure the policy according to your names.
 - Name – e.g., VLAN100-Internet
 - Incoming interface – VLAN100
 - Outgoing interface – WAN1
 - Source – all
 - Destination – all
 - Schedule – always
 - Service – all
 - Accept
- In Firewall/Network Options, NAT is enabled, and Use Outgoing Interface Address is selected.
- Accept the rest of the defaults. Click OK.

Repeat for the 2nd VLAN.



Enable inter-VLAN routing (if desired)

Both VLANs now have internet access. If they need to reach each other (inter-VLAN routing), then two more policies are required. Repeat the above firewall rules, but with interface changes:

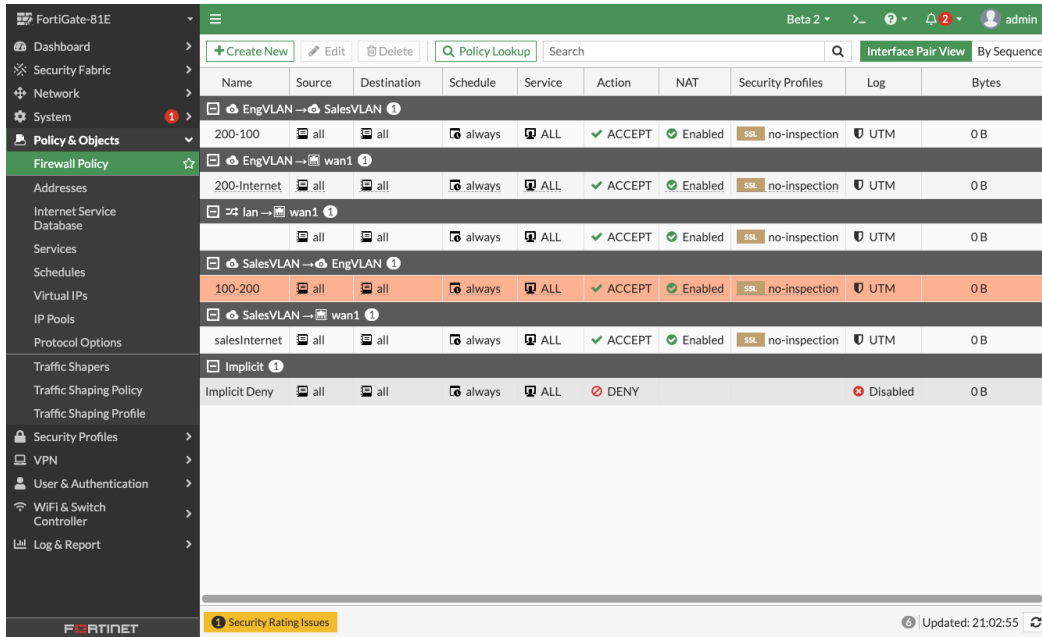
1st inter-VLAN routing rule, for example:

- Incoming interface = VLAN100
- Outgoing interface = VLAN200



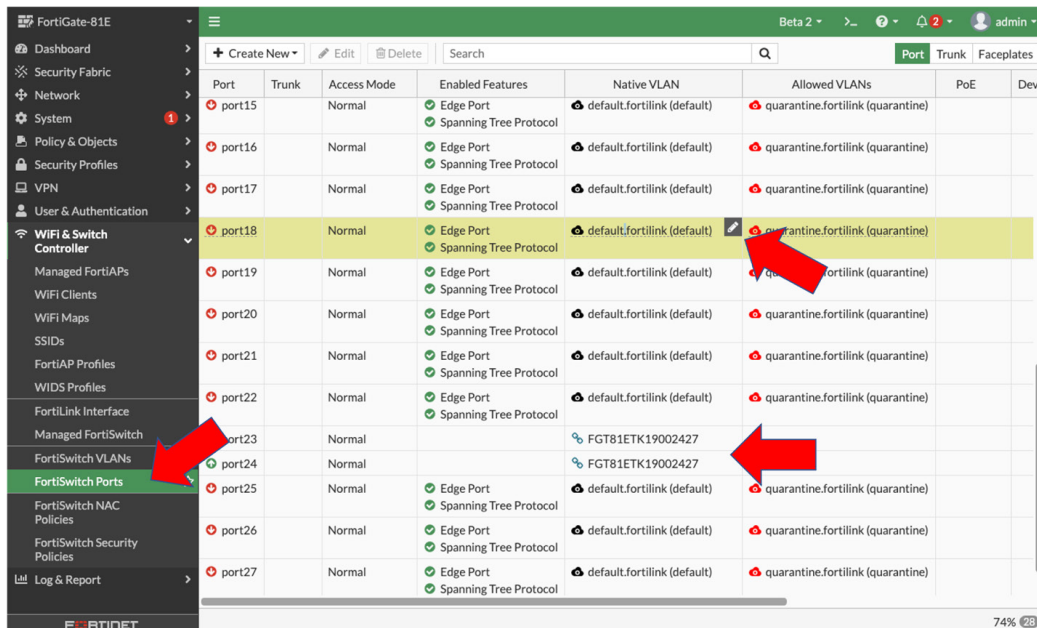
2nd inter-VLAN routing rule, for example:

- Incoming interface = VLAN200
- Outgoing interface = VLAN100



Assign VLANs to switch ports

- Go to WiFi & Switch Controller → FortiSwitch Ports.
- Notice that the FortiLink ports show the FortiGate in the native VLAN column. No need to configure a trunk port.
- To change the VLAN assigned to any given port, hover the mouse over the current native VLAN of that port. A pencil icon will appear. Click on that to edit.
 - The Select Entries window appears. Choose the VLAN to assign to this port.
 - If that VLAN hasn't been defined yet, the Create New button can be used to create a new VLAN from here.
 - Click Apply to save the change.



Set up NAC and create NAC policies

NAC identifies a device by certain criteria, such as operating system or MAC address, and then assigns it to a policy-defined VLAN.

By default, an Onboarding VLAN is designated. For NAC, the Onboarding VLAN is treated differently than other VLANs. When a device connects to a switchport in NAC mode, it goes through a NAC process:

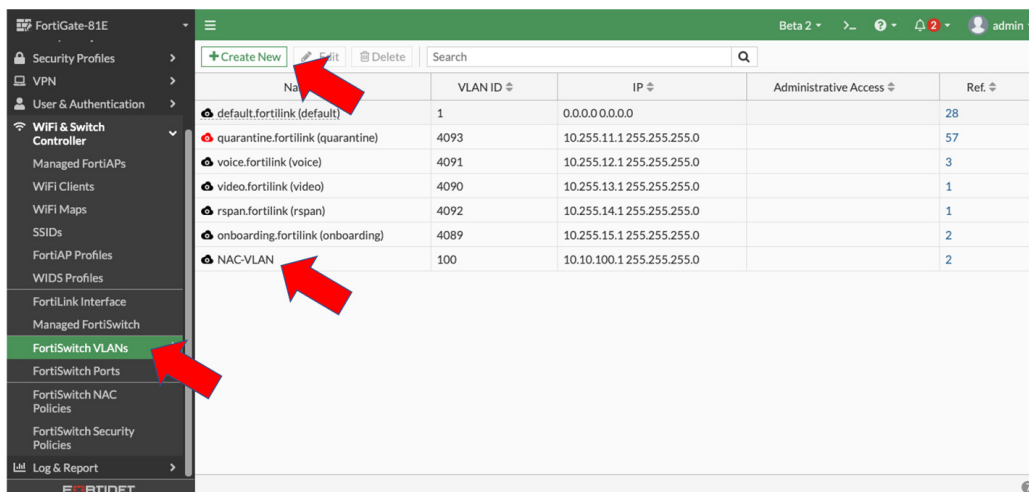
- The device gets a DHCP address on the Onboarding VLAN.
- The device gets categorized by a NAC policy.
- The device gets a new DHCP address on the assigned VLAN.

IMPORTANT: NAC settings **must** be configured before creating a NAC Policy.

Add VLANs for NAC purposes

Create a VLAN (as above) to assign devices to NAC.

- Navigate to WiFi & Switch Controller → FortiSwitch VLANs.
- Click on Create New.
- Assign a VLAN name – e.g., NAC-VLAN.
- Type is already set to VLAN. Interface is FortiLink.
- Assign VLAN ID – a number between 2 and 4094 not already in use.
 - The default config is using high numbers 4089-4093 for the predefined VLANs.
- Choose the desired color.
- Role = LAN.
- Assign an IP address.
 - Choose manual for the addressing mode.
 - Enter IP/Netmask – e.g., 10.10.100.1/255.255.255.0.
 - Create address object matching subnet should be enabled. This will be useful in Policies later.
 - Enable DHCP server.
 - Accept the default address range, or adjust for the environment.
 - Accept Same as interface IP.
 - Accept Same as system DNS.
- Click OK.



Enable internet access from the NAC-assigned VLAN

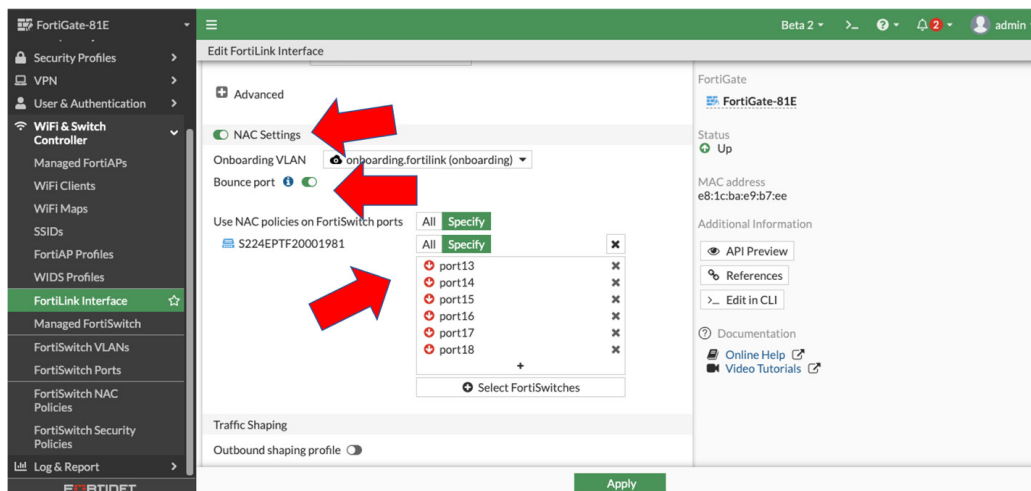
As in the earlier sections:

- Go to Policy & Objects → Firewall Policy.
- Create New.
- Configure the policy according to your names.
 - Name – e.g., VLAN100-Internet
 - Incoming interface – VLAN100
 - Outgoing interface – WAN1
 - Source – all
 - Destination – all
 - Schedule – always
 - Service – all
 - Accept
- In Firewall/Network Options, NAT is enabled, and Use Outgoing Interface Address is selected.

Accept the rest of the defaults. Click OK.

Configure NAC settings in switch controller → FortiLink Interface

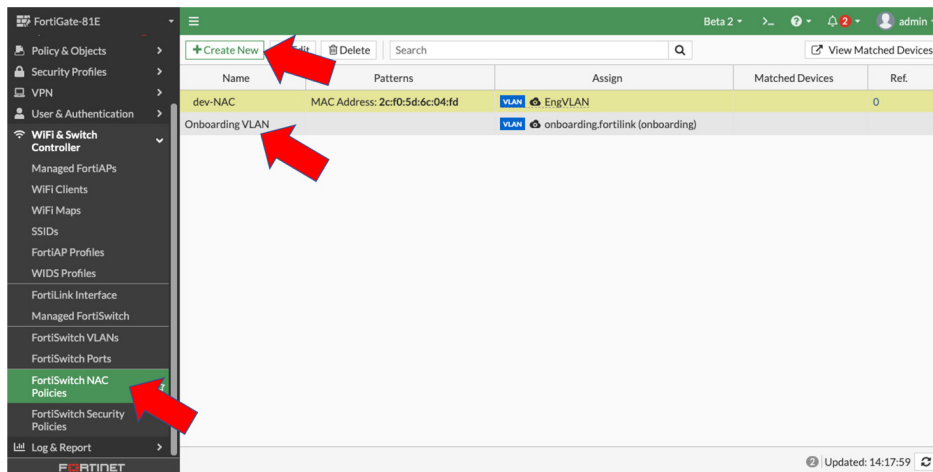
- Navigate to WiFi & Switch Controller → FortiLink Interface.
 - This is an alternate f=view of the already created FortiLink, but includes the switch NAC settings.
- Scroll down, if necessary, to the NAC settings section.
 - If necessary, enable NAC settings.
 - Accept the default onboarding VLAN.
 - Bounce port should be enabled.
 - Specify the switch (our single switch).
 - Select the port or ports to apply the NAC policy to.



Set up NAC policies on the FortiSwitch

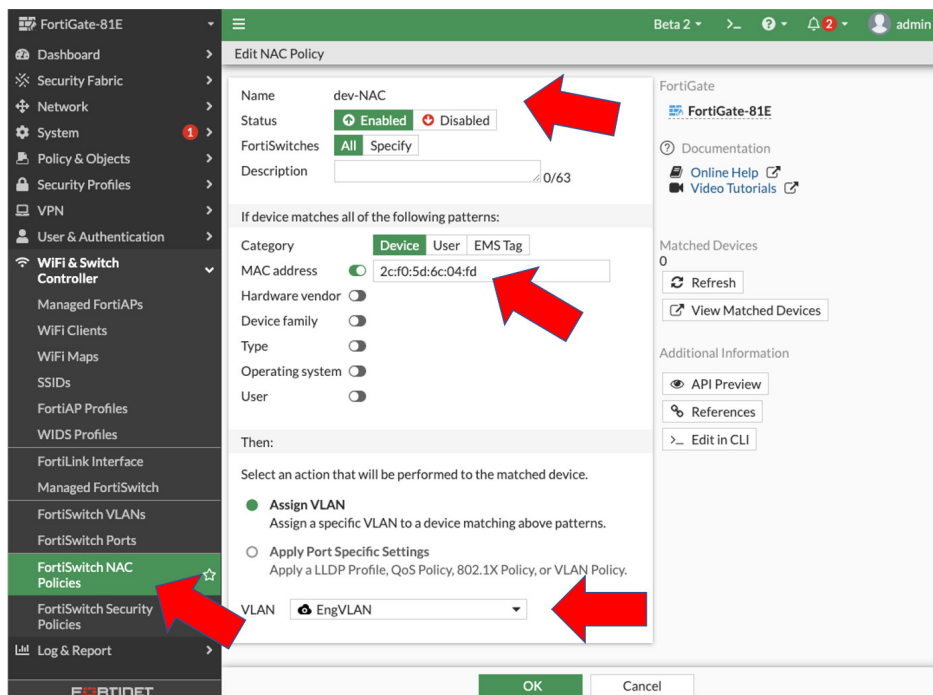
Again, complete the last section before configuring this section.

- Go to WiFi & Switch Controller → FortiSwitch NAC Policies.
- There will be an Onboarding VLAN already defined. Double-click to examine it. In this case, we have already used it in the NAC Settings and should not change it.
- Now, click Create New to create a FortiSwitch NAC Policy.



Example FortiOS NAC MAC address policy

- Name – devtype-VLAN
- Status – enabled
- Category device
- MAC Address – slider on – device MAC address in 00:00:00:00:00:00 format
 - Multiple criteria can be used
- Assign VLAN in the VLAN dropdown



Deploy Wi-Fi

This document will not go into details of hanging APs. Refer to their quick-start guides. However, some best practices to note follow.

- APs with integrated/internal antennas are intended for ceiling mounts. If wall mounting is necessary, an external antenna AP should be chosen with the appropriate antenna.
 - All antennas have a directional element. Omni-directional antennas propagate the signal in a kind of donut pattern (a torus) and have the strongest signal at the level of the AP. These are fine for 10- to 20-foot ceilings. Higher ceilings may be better off with down-pointed directional antennas. High-gain omni 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 APs should always have external antennas so the signal can be directed properly. Omni antennas (the standard “rubber ducks”) should be vertically aligned.
- Be sure the correct PoE level to power the APs is available from the switch and that the total PoE budget is sufficient for the total number of APs.
- Note the MAC address and/or a serial number of the APs and their locations. This will help with later documentation.
- When running cable for APs, leave plenty of loop at the AP end to allow them to be moved to adjust coverage. Sometimes a few feet can eliminate an unanticipated dead spot.

Add an AP VLAN

Prepare an AP VLAN by going to FortiSwitch VLANs and creating a VLAN as above for AP management (control plane). This VLAN is to create security isolation between the AP management (control channel) and user traffic (data channel).

- Set addressing to manual and assign a VLAN/GW IP.
- Enable Security Fabric Connection under administrative access #add others?
- Under Network settings, enable:
 - Device detection
 - Automatically authorize devices
 - Even in a high-security environment, it is usually best to enable this until initial deployment is done, then disable it to lock down the network.
- Click OK.

Assign AP VLAN to AP ports on the FortiSwitch

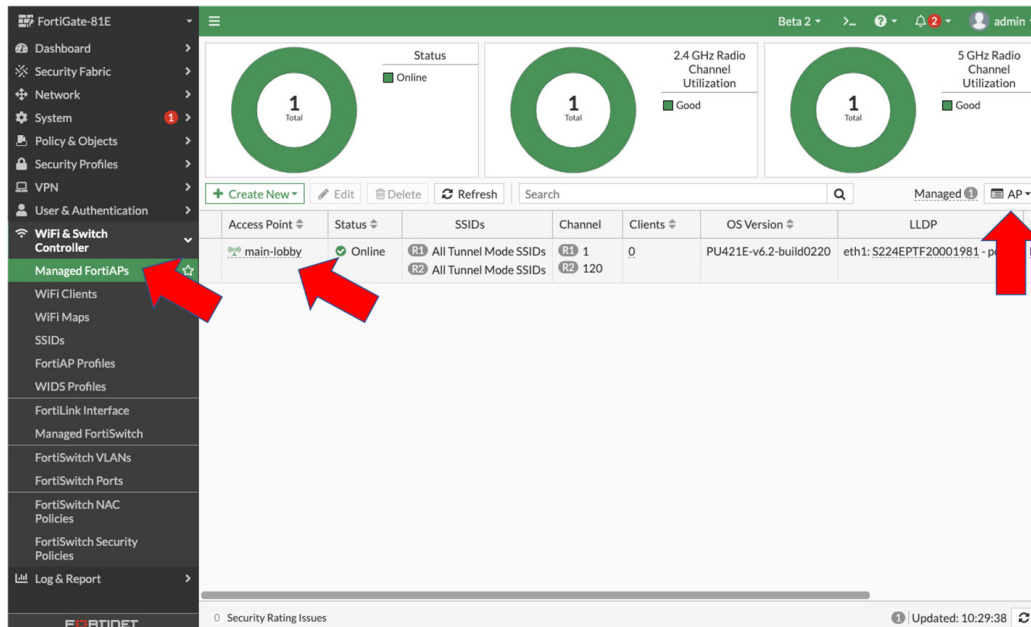
As above:

- Go to WiFi & Switch Controller → FortiSwitch Ports.
- Choose a port that is PoE capable.
- Change the native VLAN to the AP VLAN.



Connect the APs via Ethernet to the correct ports on the PoE capable FortiSwitch and give them a few minutes to boot and become authorized. Progress can be checked in Security Fabric → Physical Topology, or in WiFi & Switch Controller → Managed FortiAPs.

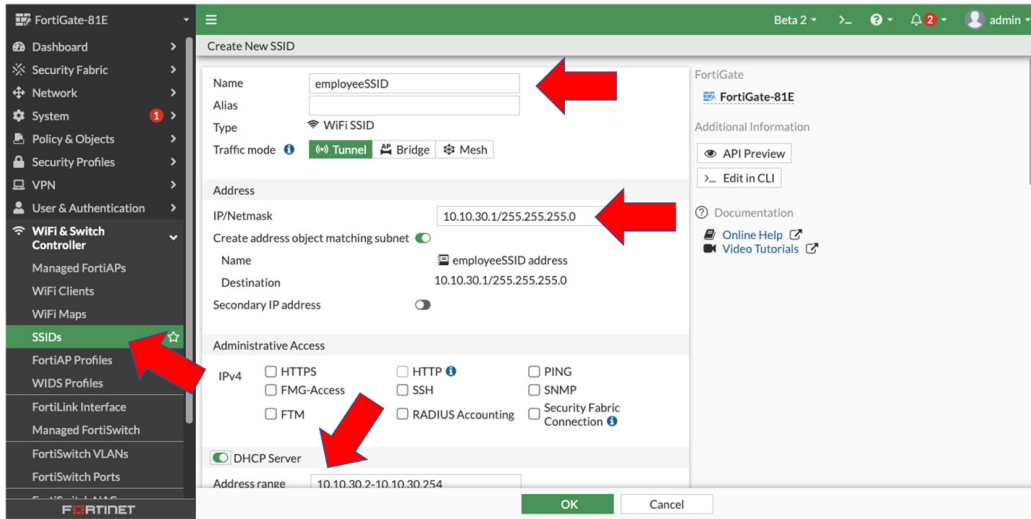
- Go to WiFi & Switch Controller → Managed FortiAPs.
- If necessary, change the view (right-hand drop-down) from Group to AP.
- If necessary, APs that have not been automatically authorized can be authorized via the right-click menu or the edit button.
- We recommend using the edit function to rename the APs to something helpful, such as MainLobby or breakroom.



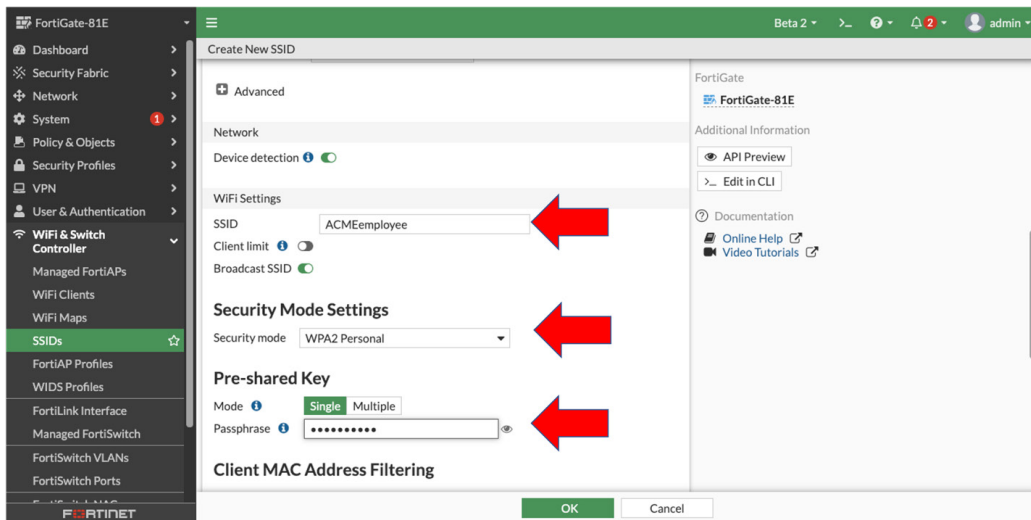
Create SSIDs

- Go to WiFi & Switch Controller → SSIDs.
- Click Create New → SSID.
- Name the SSID. This is an internal name and does not have to match over-the-air SSID.
- This will behave as a VLAN (although with the type WiFi SSID). Assign an IP address (VLAN GW) and set up the DHCP server as above.
- Traffic mode is tunnel (default).
- Up to here, this has matched setting up an interface. WLANs are treated as interfaces in FortiGate.
- Scroll down to WiFi settings and configure.
 - SSID – This is the over-the-air name.
 - Security settings. For simplicity, we will use WPA3 SAE or WPA2 personal.
 - Ideally, as security policies are refined, they will move on to one of the Enterprise settings. See the primary documentation for how to set up WPA2 and WPA3 Enterprise with a RADIUS server.
 - Enter a PSK.
 - Click OK.

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



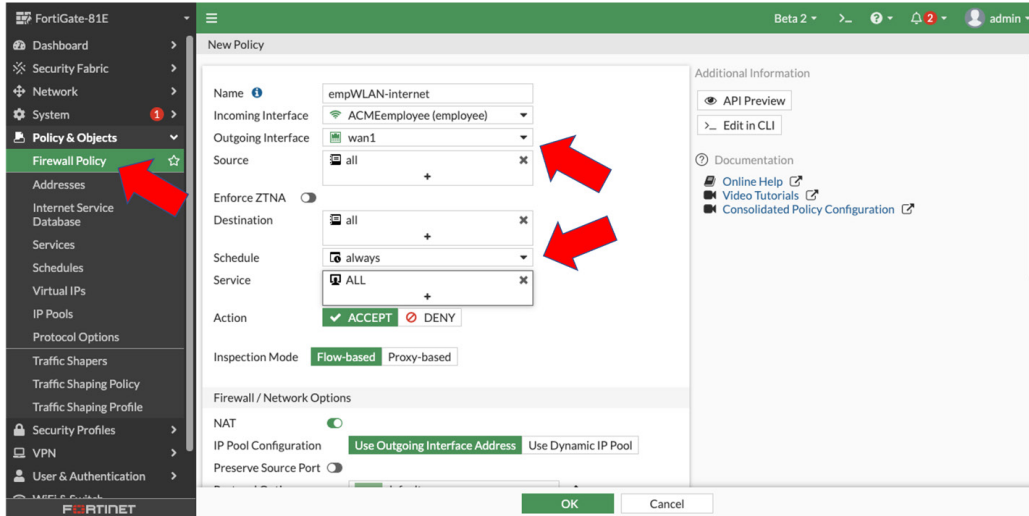
Scroll down for the settings shown below.



Firewall policies

There is one final step. Firewall policies must be configured, as in VLAN rules. See the relevant sections above.





Configuration Is Complete

The basic LAN edge network design is configured. The FortiGate is a gateway to the internet. A FortiSwitch is connected and communicating over a FortiLink, Wi-Fi is available, and an example NAC policy is configured. Take a look at other Fortinet documentation to refine and add appropriate firewall and security policies. Full documentation can be found at <https://docs.fortinet.com/>.