

**Purpose:**

To get stamped off for this lab, we needed to prove that we were able to connect our mobile device to an AP hooked up to our Fortinet firewall with two separate SSIDs configured to broadcast internet connection. The purpose of this lab is to apply the necessary configurations and policies to allow for our AP to support connectivity for both an Enterprise SSID and a PSK SSID.

**Background:**

Fortinet is a cybersecurity company that is based in Sunnyvale, California that sells and innovates cybersecurity solutions. It is known for its FortiGate firewalls, which are considered one of the most deployed network firewalls in the world due to its condensed and easy-to-understand interface.

Enterprise SSIDs typically use authentication with a RADIUS server or a local database (we are doing the latter) to allow individuals to create their own access credentials. On the other hand, Pre-Shared Key (PSK) SSIDs use one shared password for everyone to access, which is less secure but more ideal for large scale environments.

A Wide Area Network (WAN) is a network that typically spans very large geographical areas and allows communication between remote users. On a firewall, it is typically thought of as the port for communicating on the Internet.

Dynamic Host Configuration Protocol (DHCP) is a process that automatically assigns devices with an IP address from a predetermined pool of IP addresses. This simplifies network assignments and reduces the potential for manually configured errors.

Firewall Policies are rules that control network traffic flow based off whether or not the packets meet the set criteria (source IP, destination IP, port, protocol, etc.). The firewall will then allow or deny access to certain areas of the network accordingly.

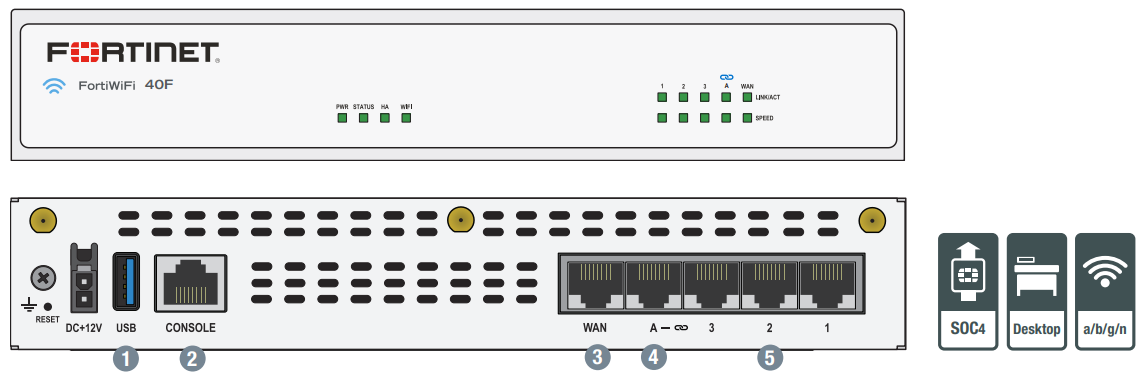
An Access Point (AP) is a device that extends WiFi coverage to an area around it, allowing devices not near the source of the internet signal to connect. Each AP has a certain amount of bandwidth, which is the total amount of data that can be transmitted per second over WiFi.

**Lab Summary:**

Since we were using Fortinet firewalls for the first time, we had to first power and connect our firewall and AP. We then created our Enterprise and PSK SSIDs and configured them appropriately. After that, we created 4 rules under Firewall Policy to make sure that the inflow and outflow of network traffic was monitored and redirected accordingly. Finally, we will check our interfaces to make sure our WAN is configured with DHCP.

**Lab Procedure:**

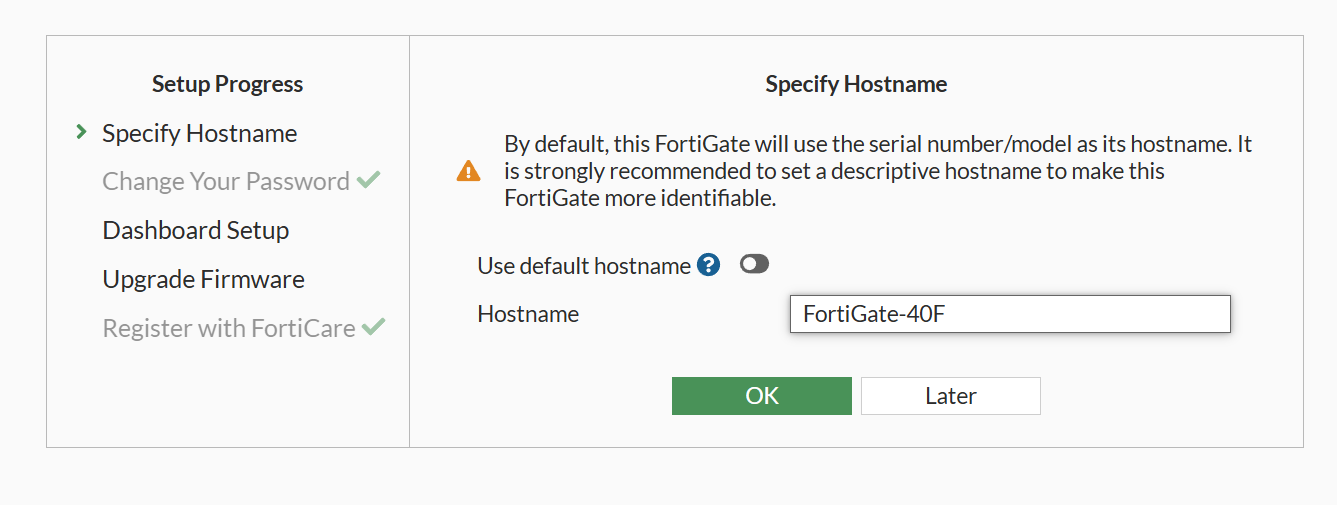
1. Plug in our FortiGate 40F with its power cord to an outlet. Plug one end of an ethernet cord into the WAN port and the other into an ISP. Plug another ethernet cord into Port 1 of the firewall and into a POE switch. Plug Another ethernet cord into Port 2 of the firewall and into an AP. Plug one final ethernet cord from the host computer’s ethernet cord into another port on the POE switch.



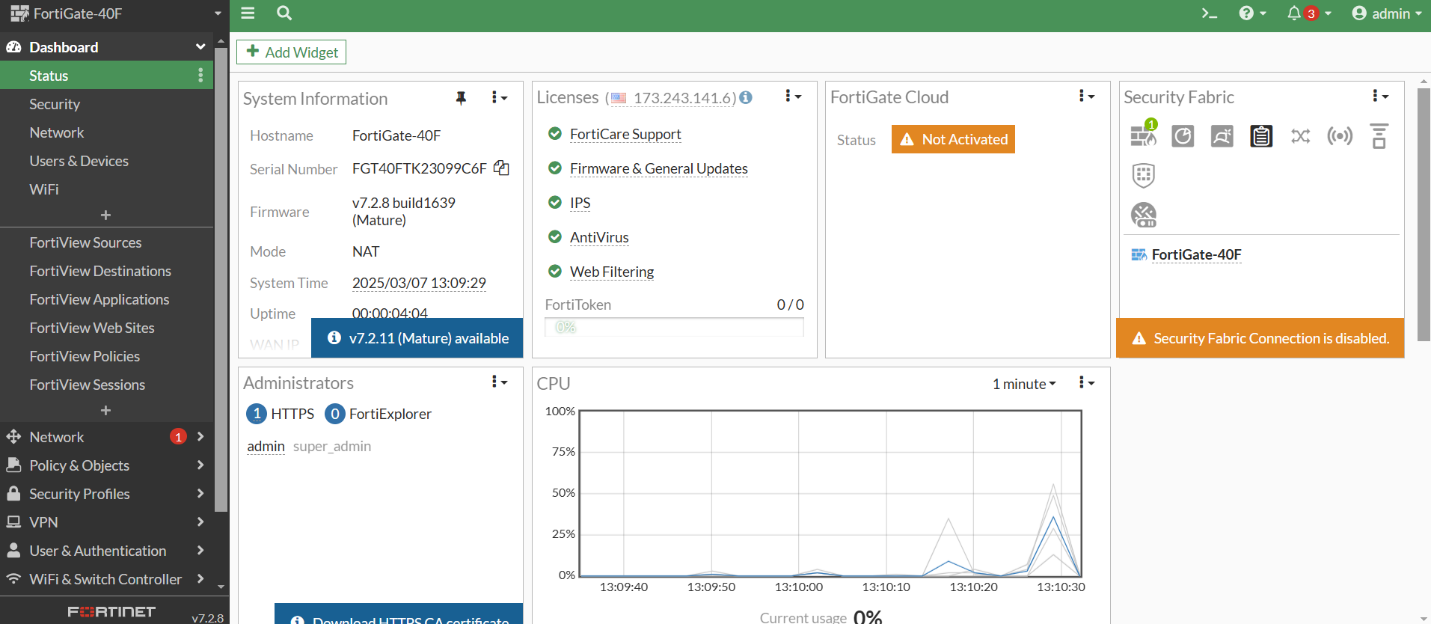
1. Log in to your FortiGate 40F with the default username “admin” and default password “admin”. Once successful, you will then be prompted to enter a new personal password for security purposes.



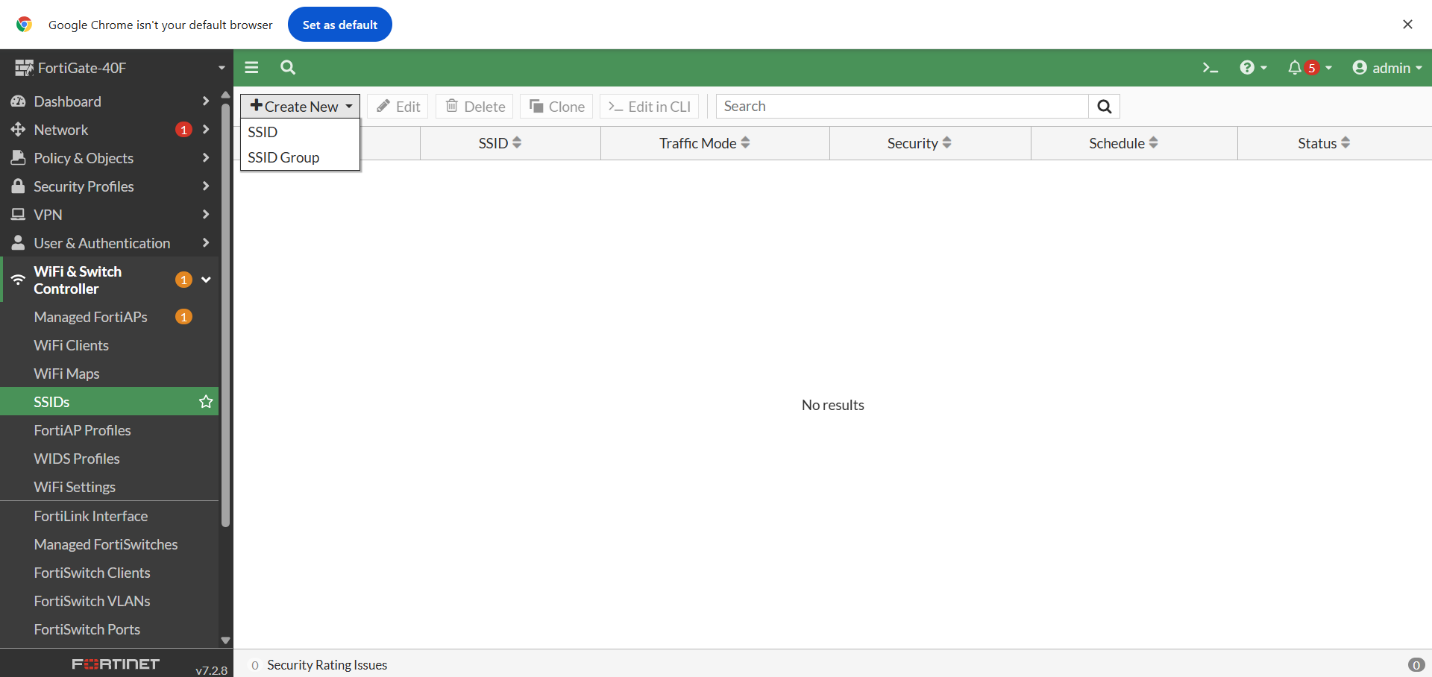
1. You will be given the option to change your hostname as part of setting up the firewall.



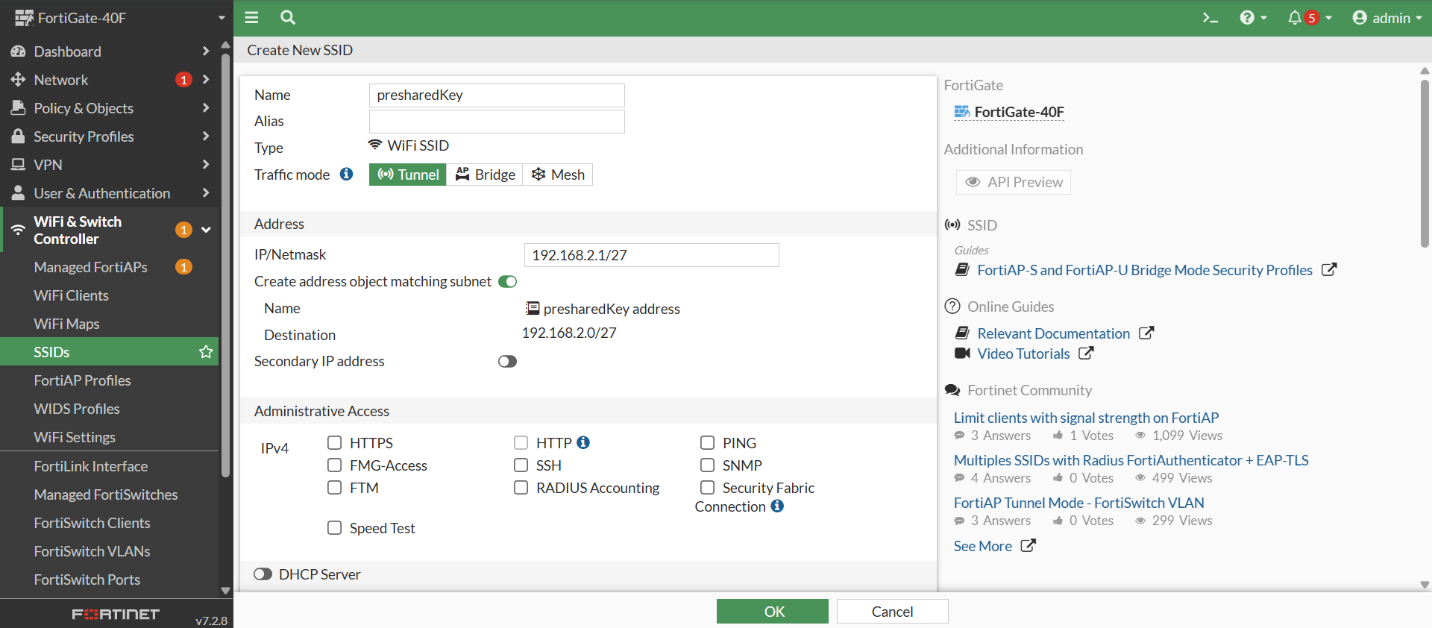
1. Once you are logged in, check that your version is 7.2. In our case, we used v7.2.8 (Mature).



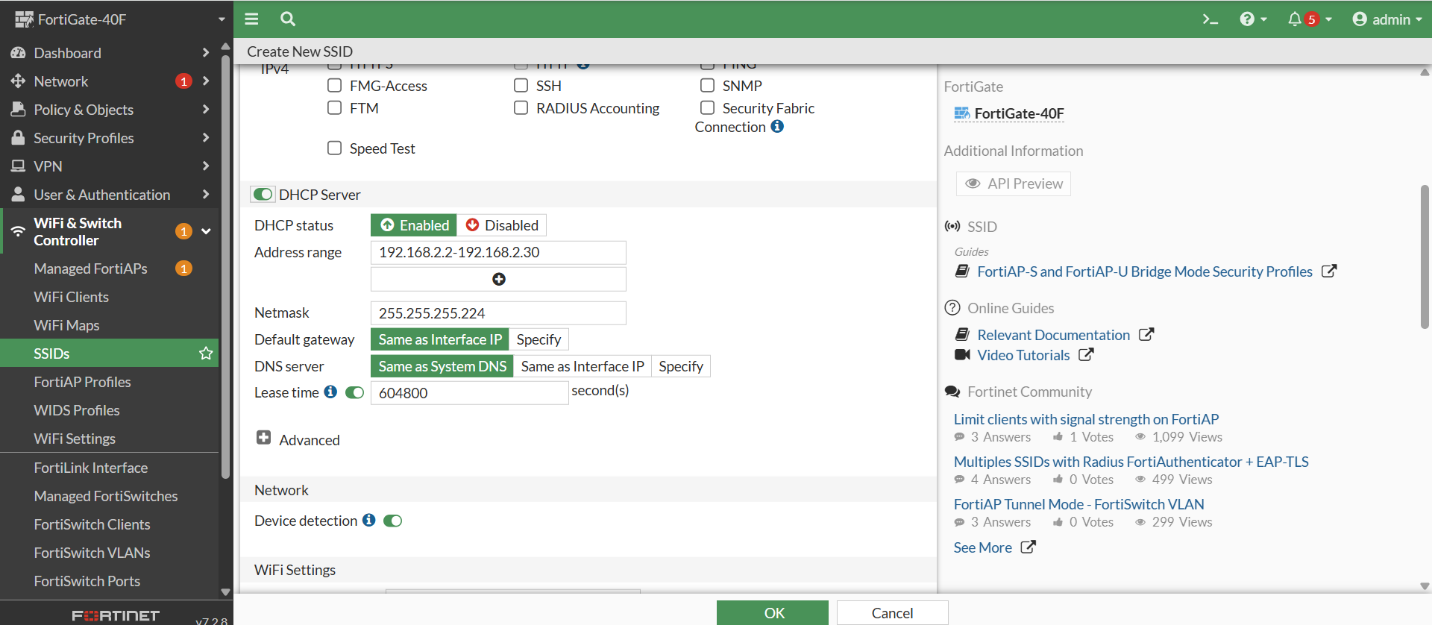
1. Go to WiFi & Switch Controller > SSIDs. Click the Create New dropdown and pick “SSID”.



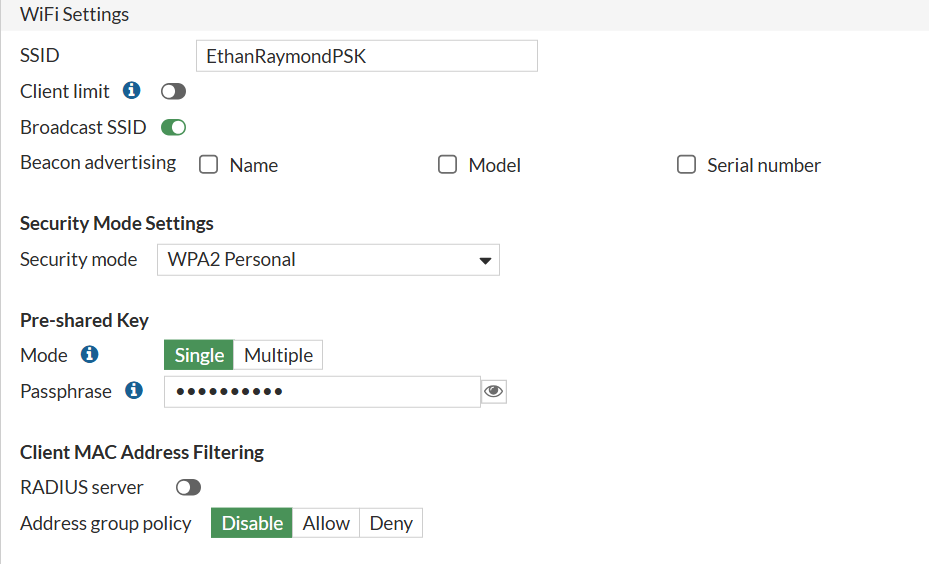
1. We will make our PSK SSID first. Set a name for our SSID, then set our IP/Netmask to a range of 32 addresses (we used 192.168.2.1/27).



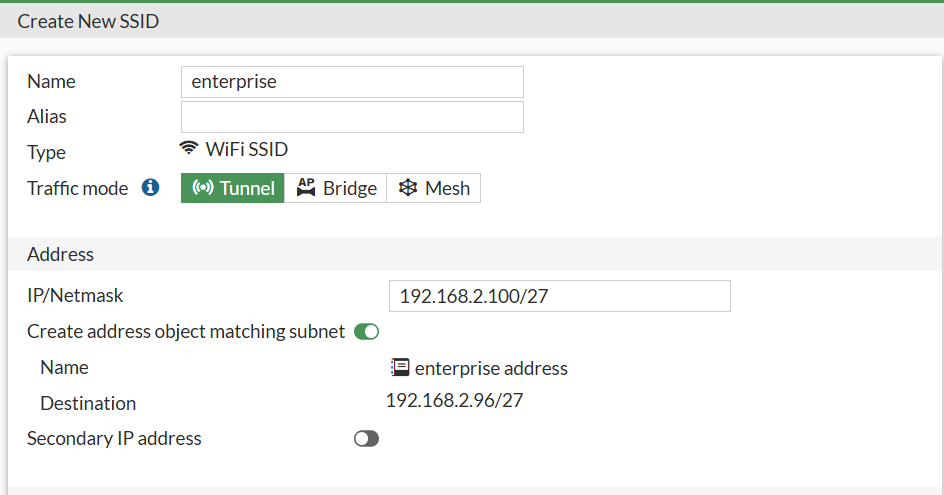
1. Scroll down and turn on DHCP server, then set the range to all available addresses for the IP/Netmask that we set earlier.



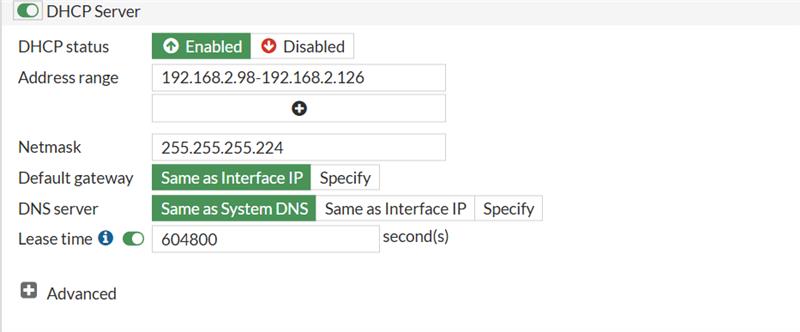
1. Scroll down some more to our WiFi settings and set an SSID. Select “WPA2 Personal” under the Security mode dropdown and set a Pre-shared Key of your choosing. Click “Ok” once all configurations have been made.



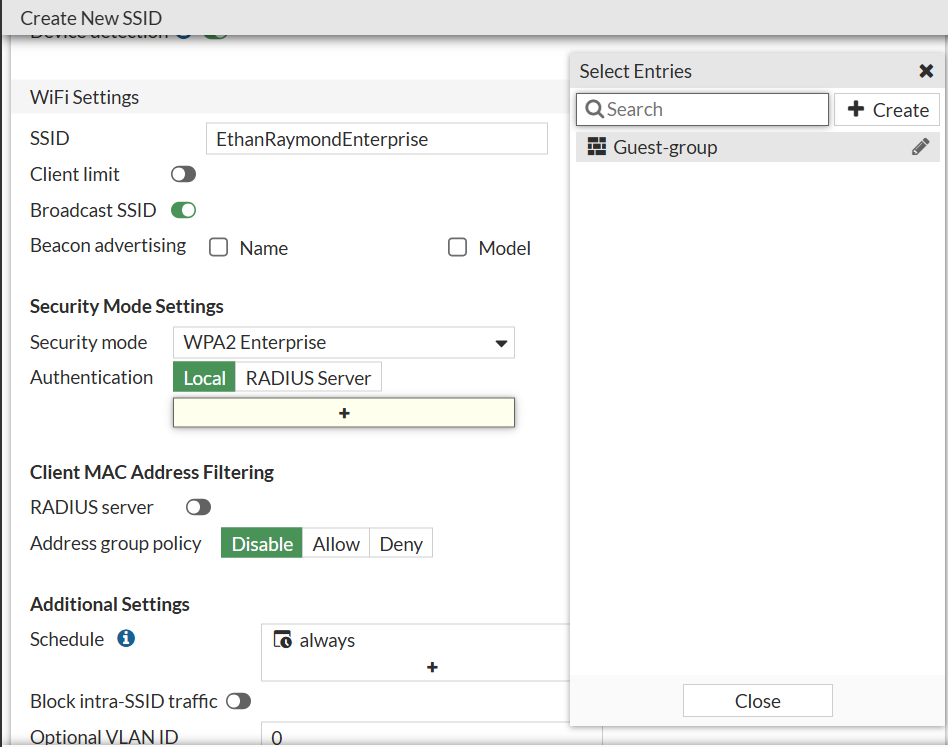
1. Go back and create another SSID using the dropdown. This time, we will be making our Enterprise SSID. Set the IP/Netmask to another range of 32 addresses (we did 192.168.2.100/27).



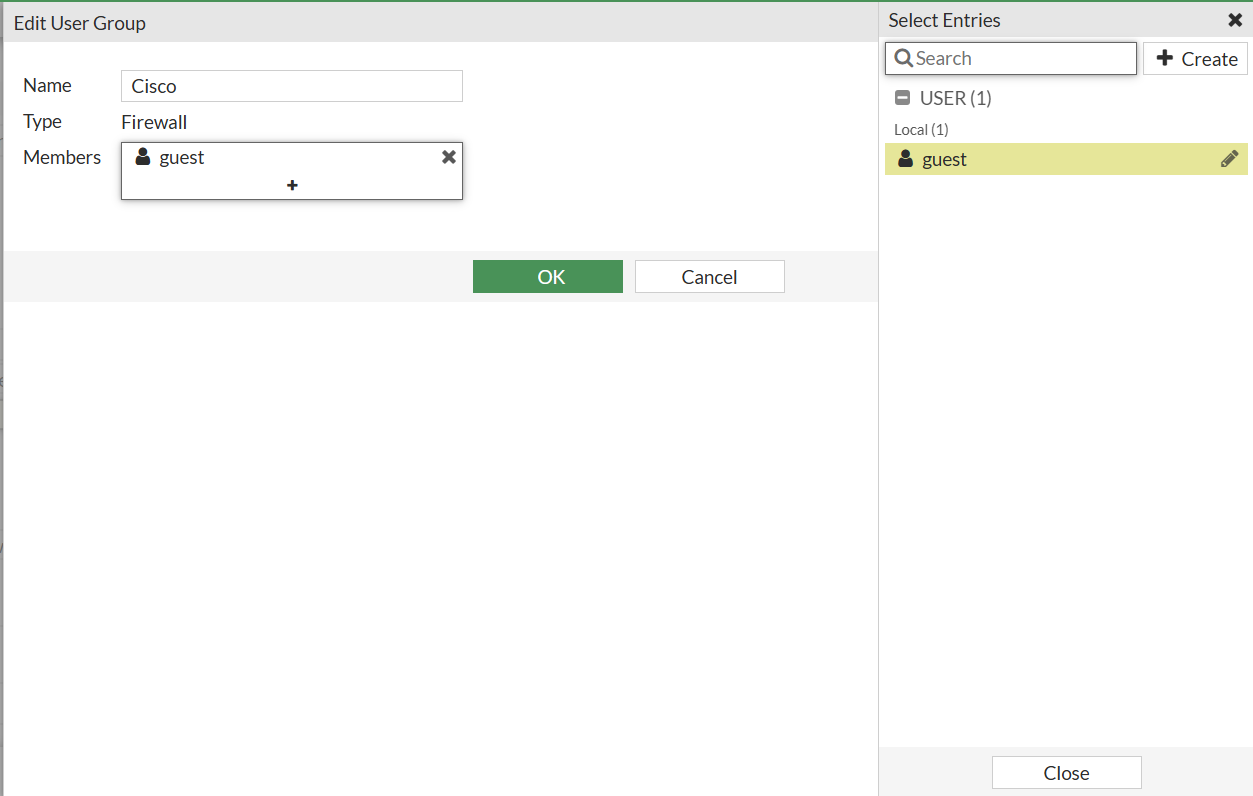
1. Turn on DHCP server and set the range to all available addresses for the IP/Netmask.



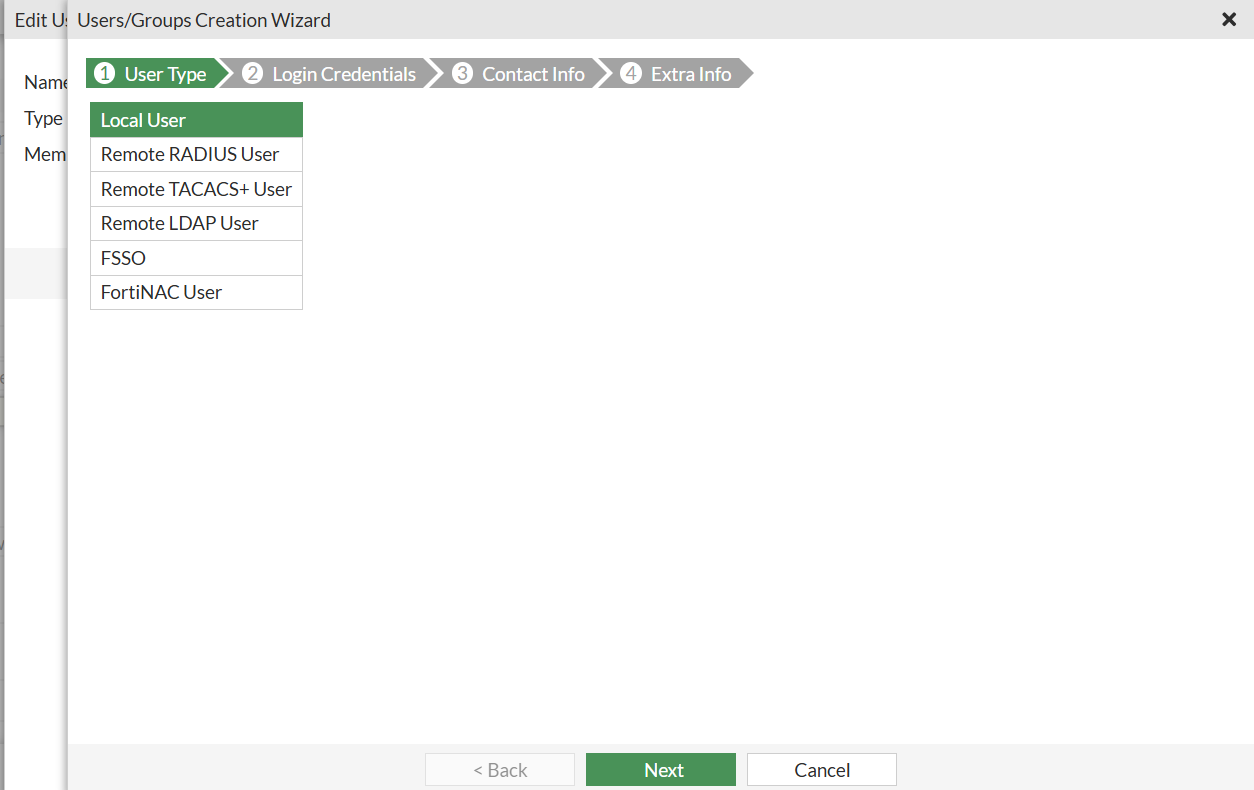
1. Set an SSID, then click the Security mode dropdown and select “WPA2 Enterprise”. Press the highlighted “+” to open this side panel titled Select Entries. Click the “Create” button.



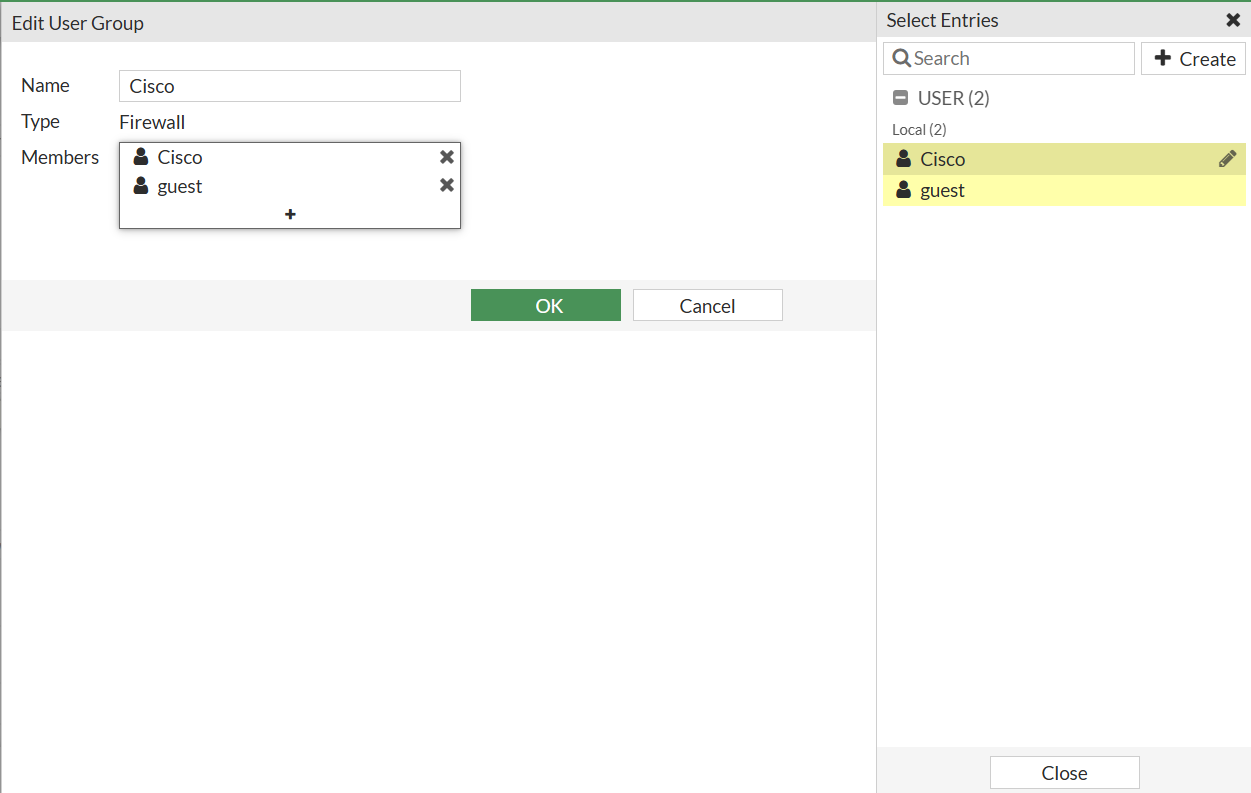
1. Set a name for the User Group. Next, click the button labeled “Create” in the top right corner.



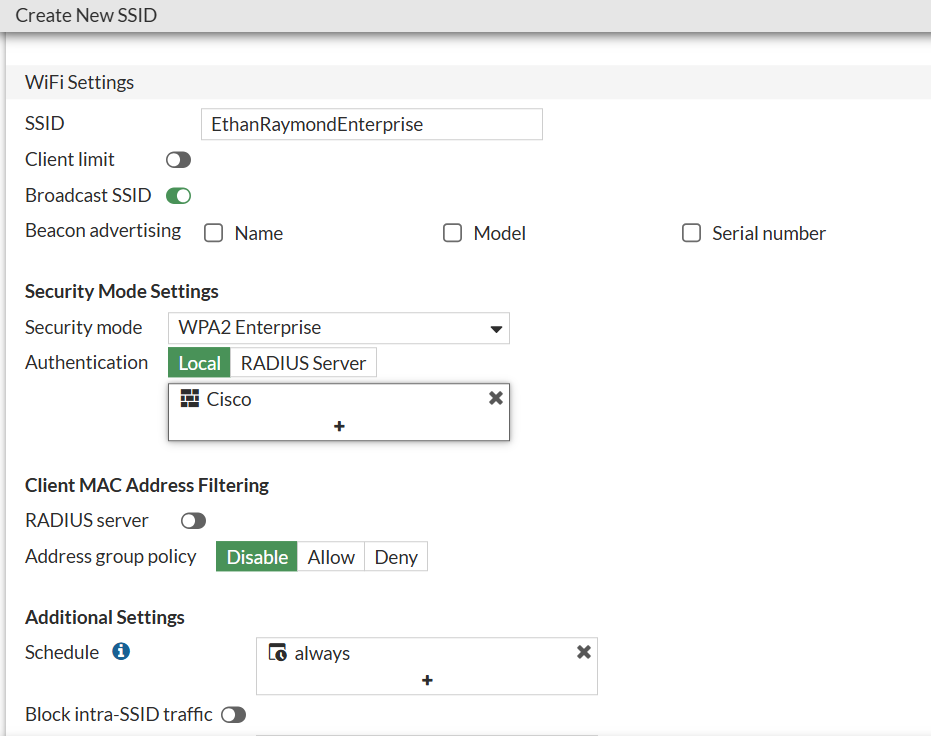
1. For User Type, select “Local User”. Click “Next” all the way through the rest of the steps under Users/Groups Creation Wizard.



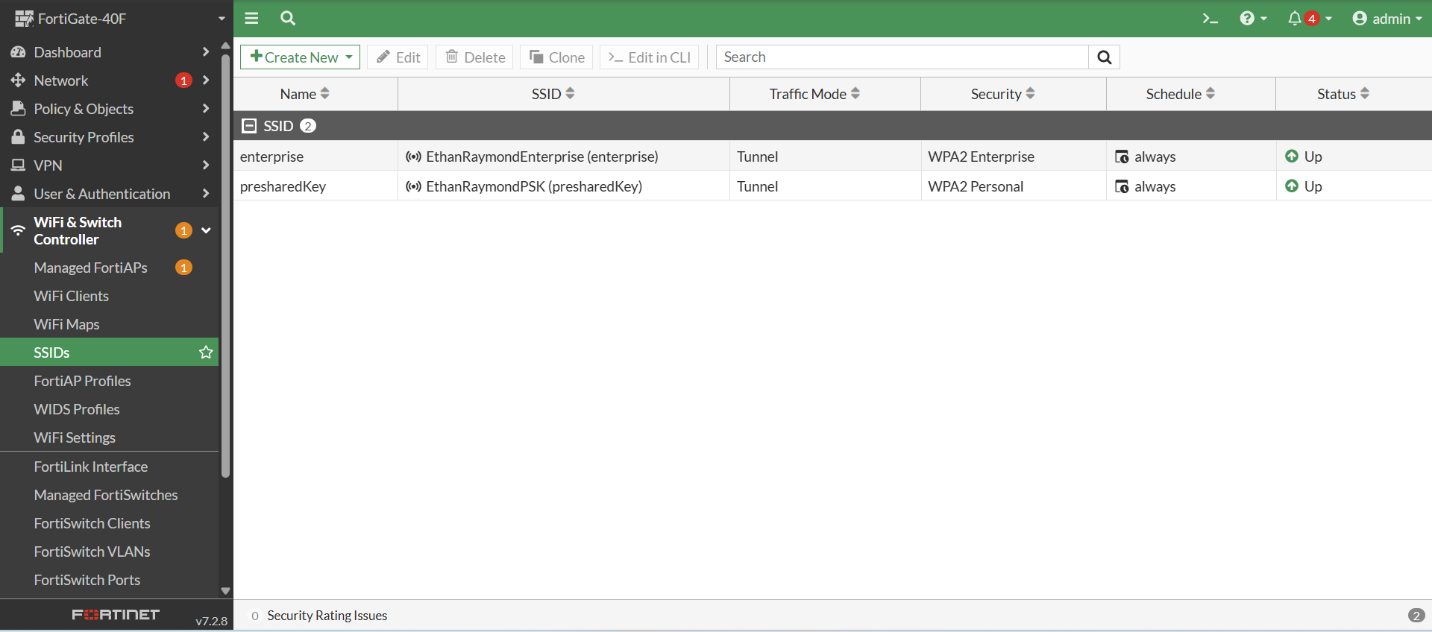
1. You should now see our newly created user, “Cisco”. Add it to the Members for this User Group. Click “Ok”.



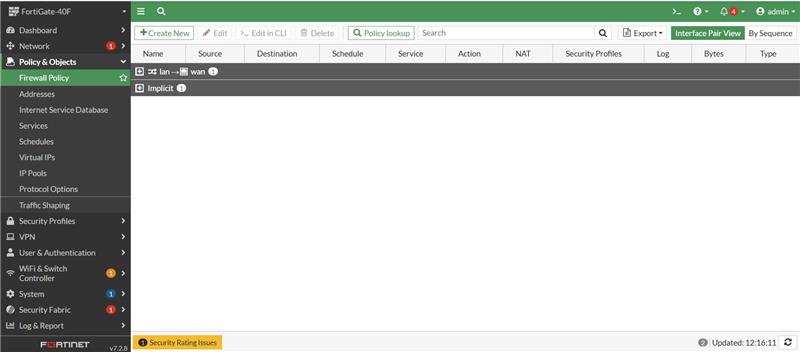
Our User Group named Cisco should now be under our WPA2 Enterprise Security Mode Settings.



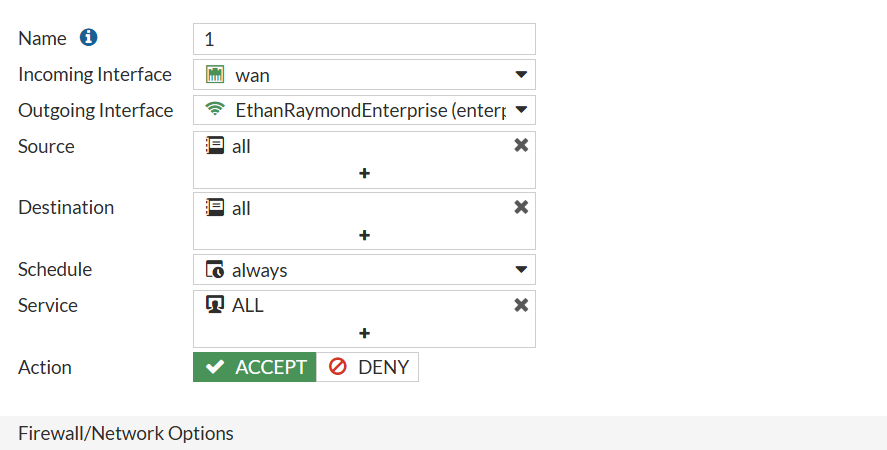
This is what our SSID screen should look like after we have finished setting both of them up.



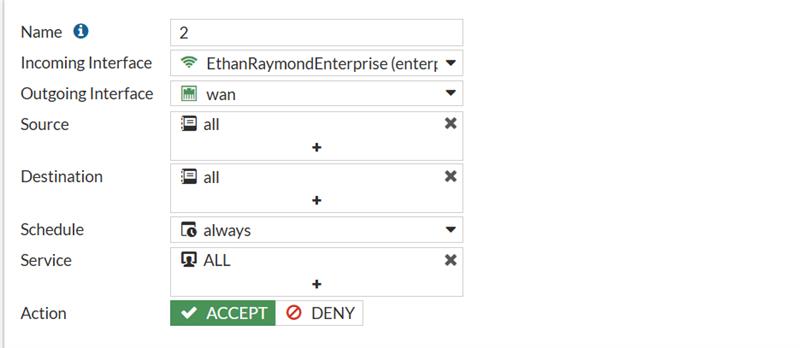
1. Go to Policy & Objects > Firewall Policy. Click “Create New”.



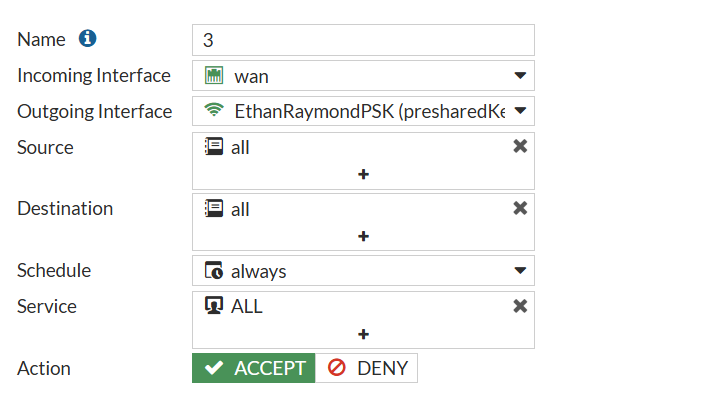
1. We will make 4 separate rules. Our first one should have our WAN as our incoming interface, our Enterprise SSID as our outgoing. For all 4 of these rules, our Source should be All, our Destination should be All, our Schedule should be always, and our Service should be ALL. Click “Ok” once you make these configurations.



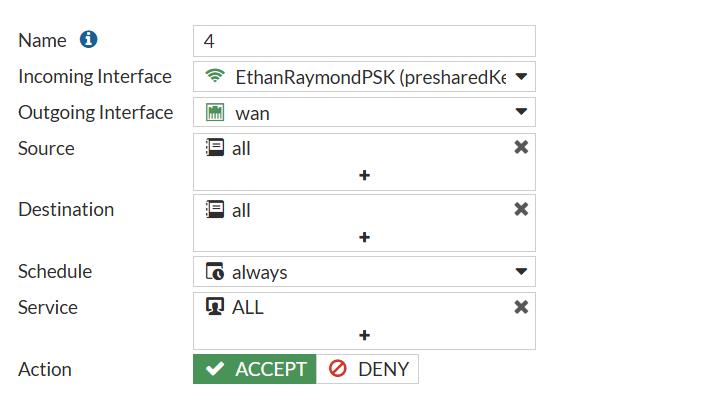
1. For rule 2, we are swapping the incoming and outgoing interface from our 1st rule. This time, set Enterprise to Incoming Interface and WAN to Outgoing Interface.



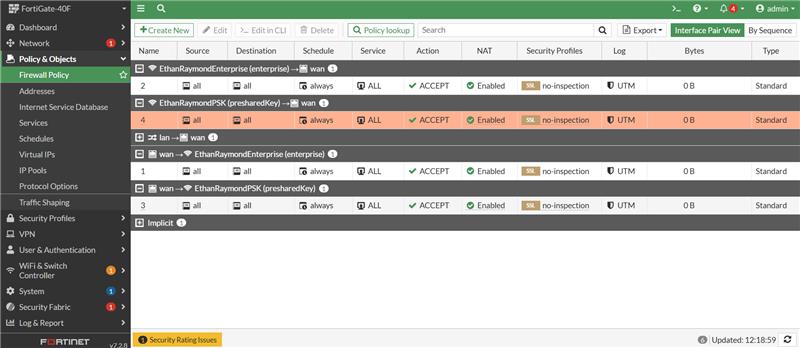
1. Our 3rd rule. Make sure the Incoming Interface is the WAN and the Outgoing Interface is our PSK SSID.



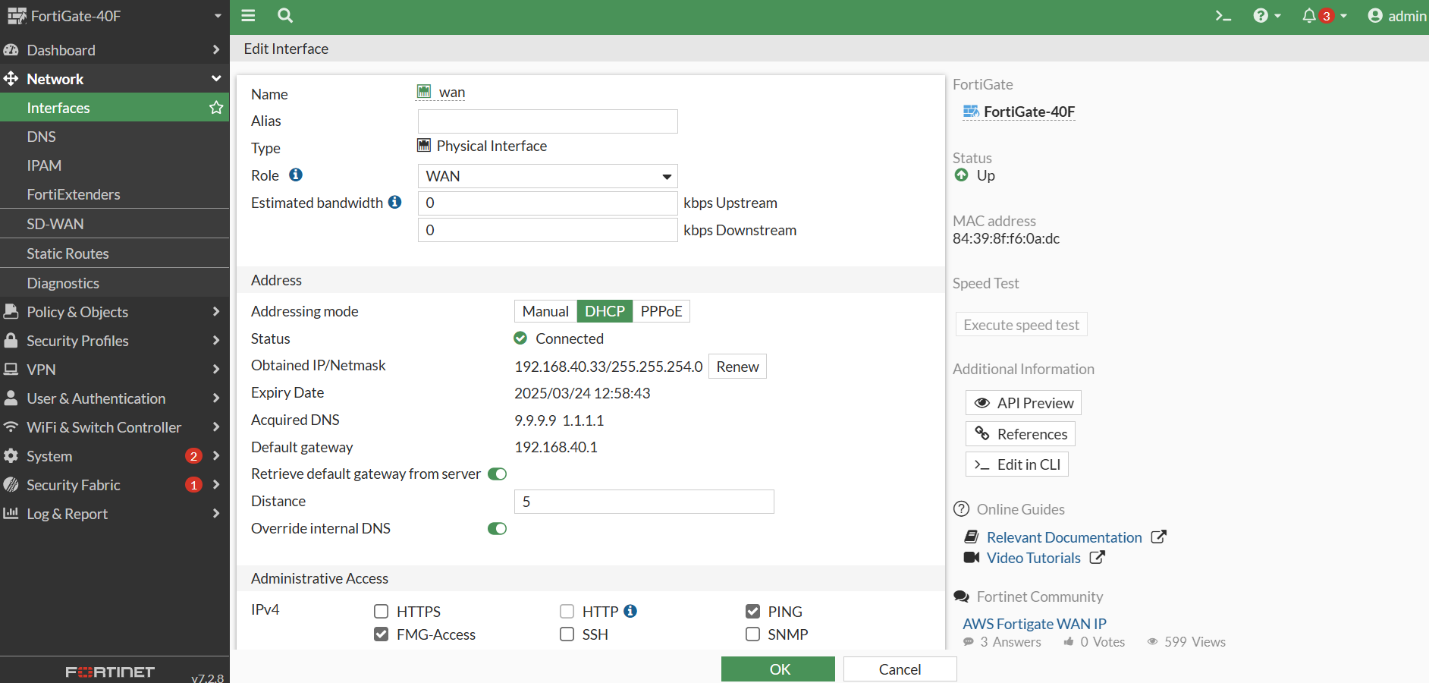
1. Finally, the 4th and final rule. Make sure the Incoming Interface is our PSK SSID and our Outgoing Interface is the WAN.



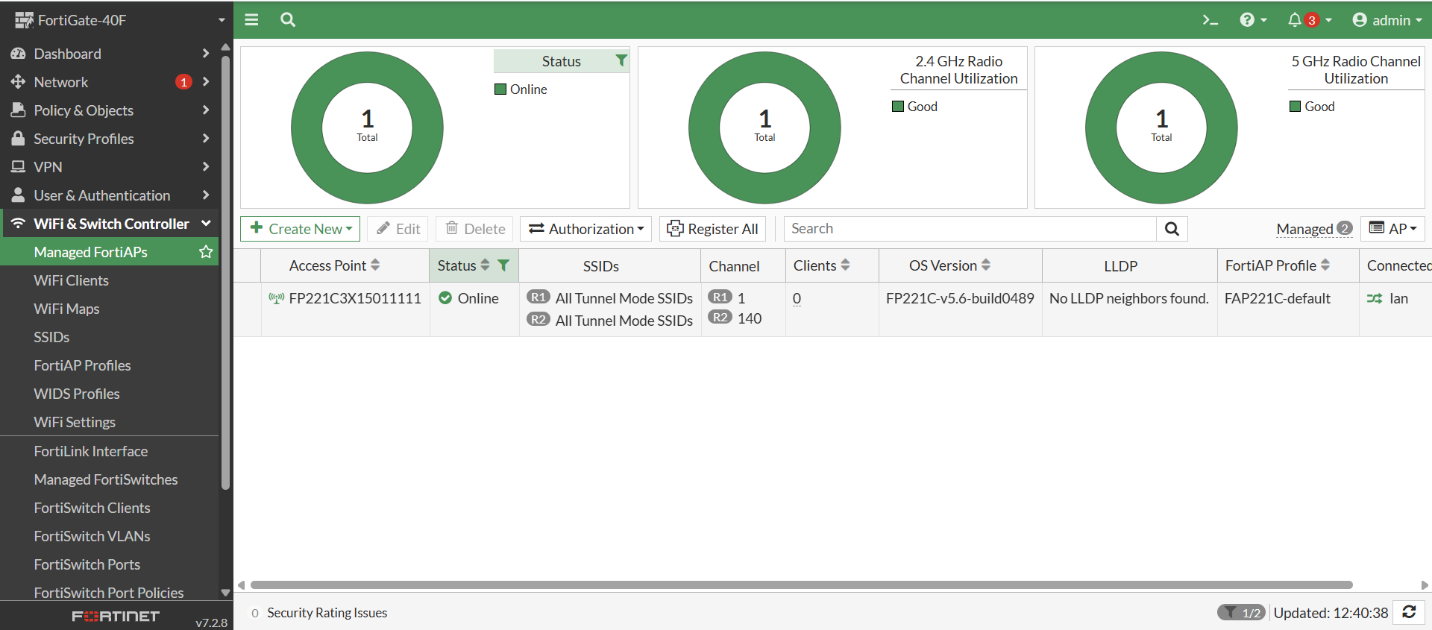
This is what our Firewall Policy section should look like after all our rules have been established and are operational.



1. For our last step to make sure our system is fully operational, go to Network > Interfaces. Click into the WAN interface and make sure that it is set to DHCP. Switch it to DHCP if it isn’t already.



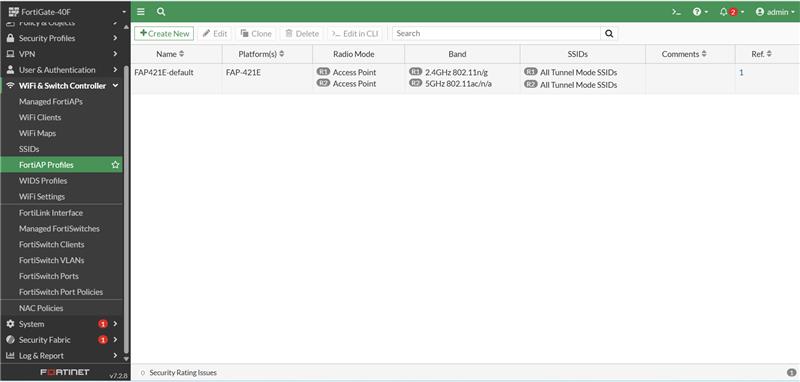
If you go to WiFi & Switch Controller > Managed FortiAPs, this is what the menu should look like if our APs are currently active.

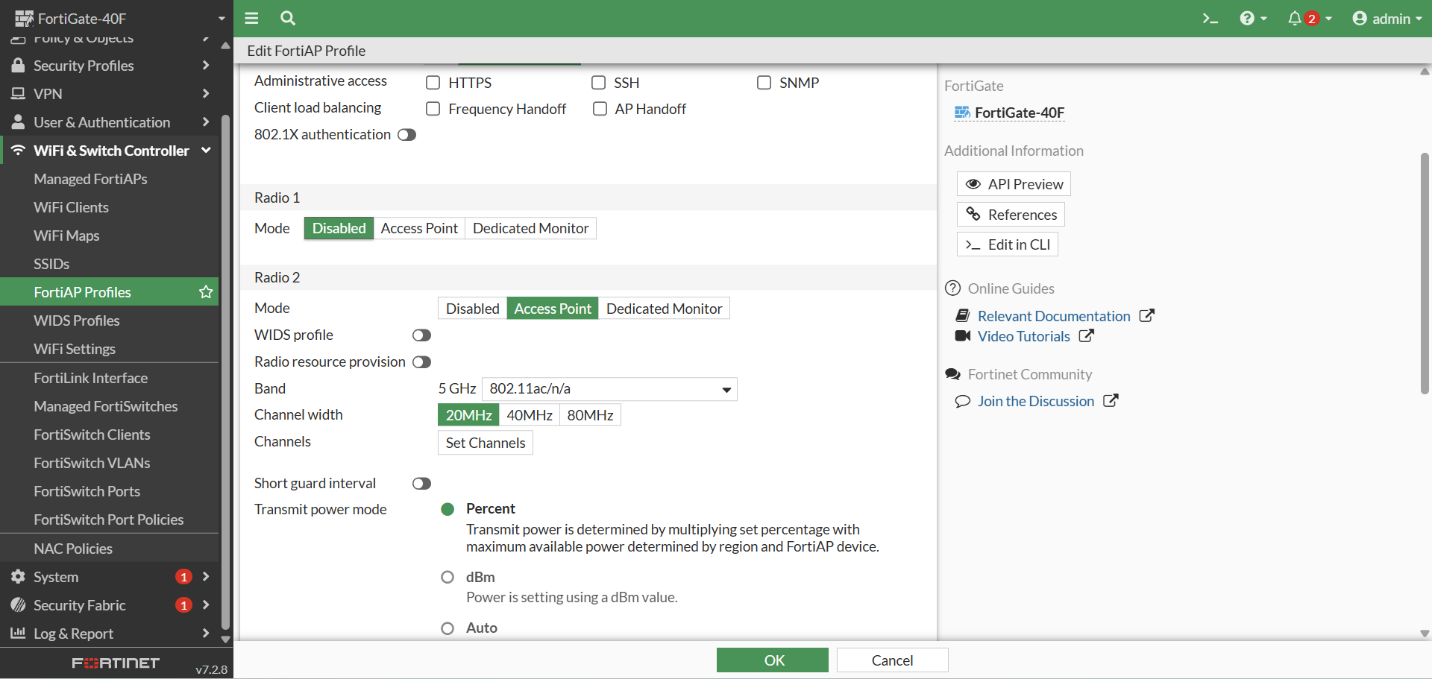


**Problems:**

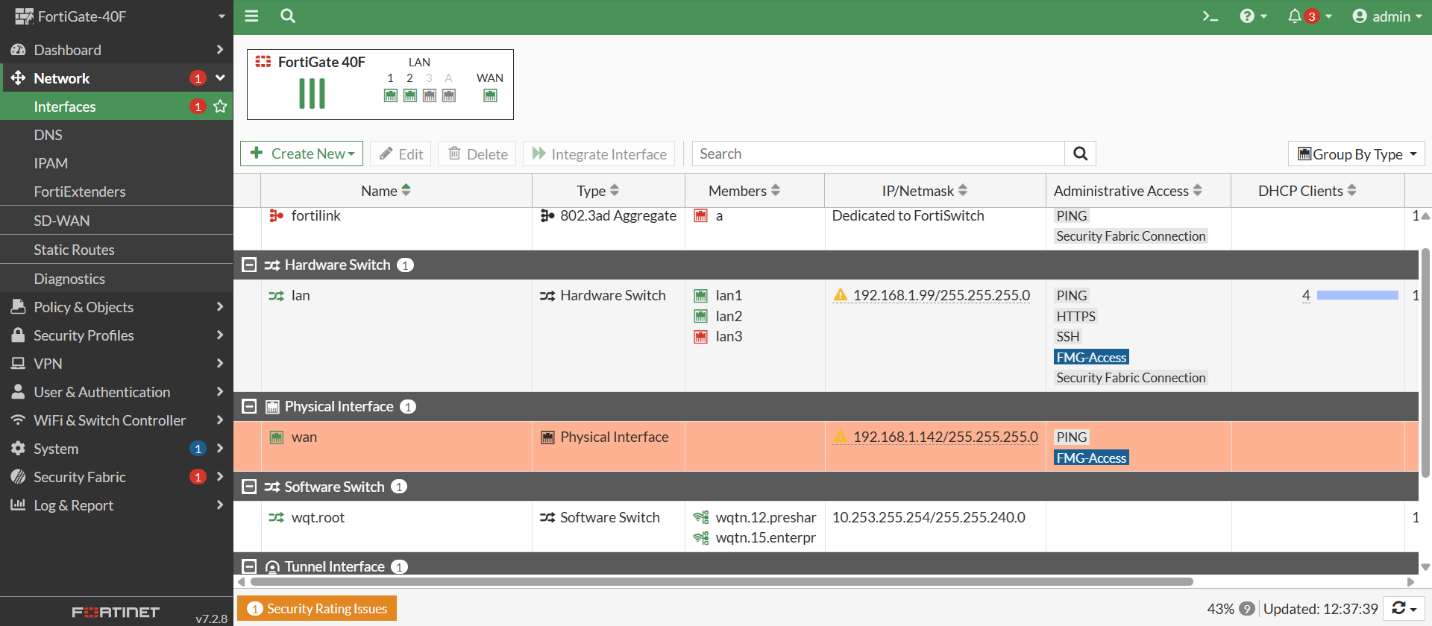
We had little trouble setting up the configurations for the AP thanks to Fortinet’s user-friendly design. The primary issue we ran into while testing afterwards was that our AP had incredibly low bandwidth (~5 kb/s). To tackle this issue, we tested 3 possible solutions.

1. AP Replacement: We first wanted to diagnose if this was a hardware issue, so we replaced the AP we were originally using with a newer model. However, this did not fix our issue.
2. Reduce Interference: With so many APs being set up and tested by our classmates around us, we thought that maybe we were experiencing too much interference when trying to connect our mobile devices. As a result, we turned off our 2.4 GHz 802.11n/g Band on Radio 1. However, this did not fix the issue either.





1. WAN Check: With the advice from Mr. Mason, we checked to make sure our WAN port was configured properly. Turns out, we had set a physical address as our WAN port and it was interfering with our LAN port as well. We quickly fixed this by changing the WAN port to DHCP. This fixed our bandwidth issue and we were able to connect to the AP through both SSIDs and we were receiving reasonable speeds on our mobile devices.



**Conclusion:**

In this lab, we successfully configured our FortiGate 40F firewall to support both an Enterprise SSID and a PSK SSID through an AP. We did this by creating SSIDs, firewall policies, and with DHCP to mimic a SOHO network. This lab helped us familiarize with using a different GUI and brand of cybersecurity tool (as we were previously using Palo Alto firewalls), as it is a useful skill to be experienced with different ways of achieving a familiar SOHO and AP configuration.

**Sign Off:**

