Fortinet: Configuring a FortiGate 40F Firewall for a SOHO Environment/Configuring a Fortinet 421E AP with WPA2-PSK and WPA2-Enterprise Local Auth

Colin J. Faletto, CCNA

FORTINET

Purpose

This lab is intended to introduce the Fortinet ecosystem, providing basic knowledge of the FortiGate firewall console and GUI interface. The lab also provides insight into the default configuration of a FortiGate firewall and how it can be used for a SOHO environment. In addition, the lab teaches how to set up a FortiAP access point, connect it to a FortiGate, and configure WLANs with a variety of different security options.

Background

SOHO, short for Small Office/Home Office, is a network type commonly used by individuals or small businesses with less than 10 employees. This network type commonly uses smaller-scale routers, switches, and firewalls compared to their large enterprise counterparts. SOHO networks provide numerous advantages to teams of 1-10 people as they are easier to set up and are more affordable than full-size network equipment. SOHO networks often only have a single router, and may contain switches, wireless access points, and end devices such as computers and printers.

Wi-Fi Protected Access, or WPA, is a security standard developed and maintained by the Wi-Fi alliance. There are three versions of WPA, being named WPA, WPA2, and WPA3 respectively. The first generation of WPA was released in 2003, with the second version releasing just a year later in 2004. In 2018, the third generation was released. WPA uses TKIP (Temporal Key Integrity Protocol) as its encryption method, while WPA2 uses CCMP (Counter-Mode/CBC-Mac Protocol) for encryption. WPA3 keeps support for CCMP but introduces GCMP (Galois/Counter Mode Protocol) as a stronger encryption method as well.

WPA can use two different methods of authentication: Personal and Enterprise. Personal authentication uses a pre-shared 256 bit key, meaning that all devices authenticate using the same password. Enterprise authentication uses a RADIUS (Remote Authentication Dial In User Service) server, meaning that each user authenticates using their own username and password.

Fortinet is a cybersecurity company founded in 2000 in Sunnyvale, CA. They are known for their flagship product, the FortiGate firewall, as well as a wide variety of other networking and security devices, such as the FortiSwitch and the FortiAP, and services such as FortiSandbox, FortiAuthenticator, FortiVoice, and FortiDDoS. Fortigate is an S&P 500 component and is listed on the NASDAQ as $FTNT.

The FortiGate 40-F is a firewall developed by Fortinet. It has capabilities expected of a modern firewall such as full routing capability, DHCP server capability, and support for a variety of filtering methods. **The 40-F also supports running its own local RADIUS server with a feature called Local Auth (Authentication).** The 40-F uses a fanless design, allowing it to operate silently. The 40-F has a small form factor at 1.5 x 8.5 x 6.3 inches, meaning it can easily fit into existing networking setups. By

default, the 40-F gives out DHCP addresses in the 192.168.1.0/24 subnet to its clients (from .110-.210, specifically) and its GUI client can be accessed via HTTPS at 192.168.1.99.

The FortiAP 421E is an access point developed by Fortinet. It has 8 internal antennae and 2 internal radios broadcasting on 2.4 GHz and 5 GHz respectively. It supports a variety of authentication methods, including WPA and WPA2 with either 802.1X or PSK, WEP, and a MAC blacklist/whitelist. It can form a mesh with other FortiAP devices to ensure more uniform connectivity across a site. The 421E can also handle a maximum of 512 clients per radio split across a maximum of 16 SSIDs.

Lab Summary

In this lab, we factory reset a FortiGate 40F firewall and upgraded it to version 7.4, which was the most recent mature version of FortiOS at the time, striking a balance between new features and stability. We configured basic settings and verified that essential firewall functions were working. We then connected a FortiAP 421E and set up two WLANs, running WPA2-Personal with PSK and WPA2-Enterprise with Local Authentication respectively.

Lab Commands

Cable all lab devices according to the topology.

Turn on your firewall and wait for the login screen to show. Within 60 seconds, press the reset button next to the firewall's power connector. You will see a message like this:

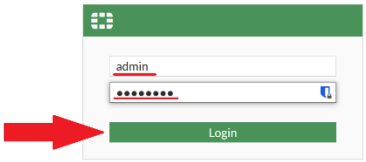
```
AadiAndKevin login:
System is resetting to factory default...
```

You should see the prompt `Fortigate-40F login:` Type in the username `admin` with no password. Change your password when prompted.

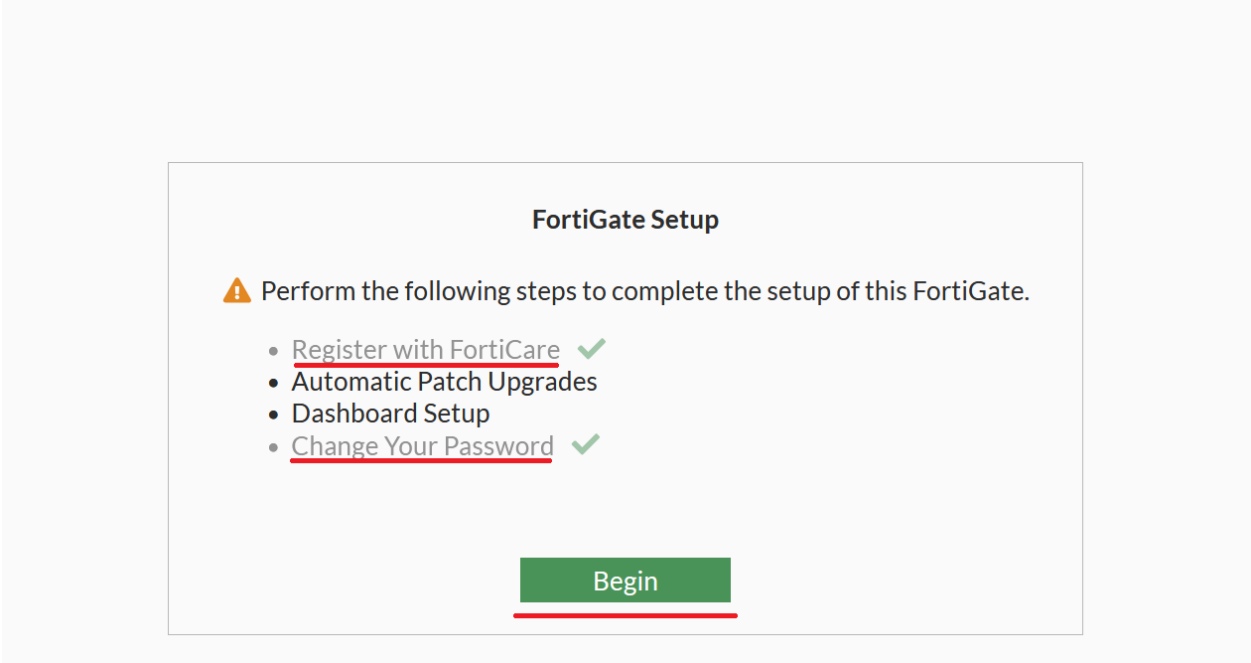
```
FortiGate-40F login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!

FortiGate-40F #
```

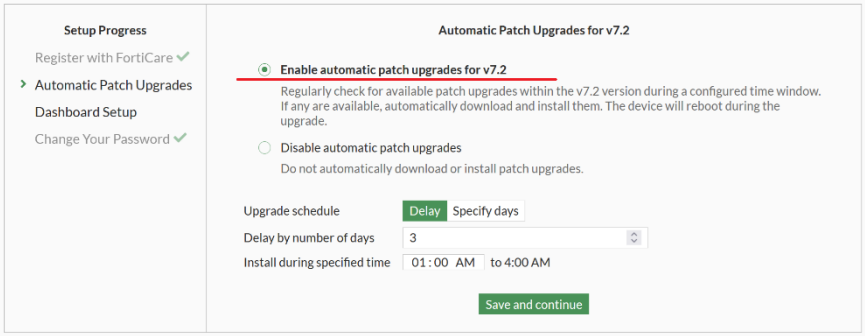
Connect your PC to the firewall via ethernet. Go to https://192.168.1.99 and log in with the username and password you set.



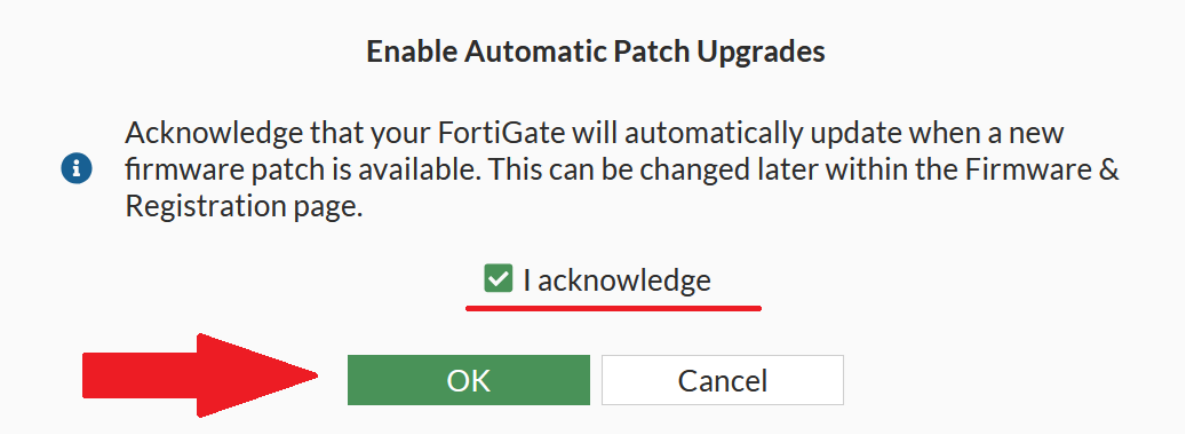
You should see the following setup screen. Note that the Change Your Password checklist item has already been completed, as we completed this earlier. (Also, the firewall used in this lab had already been registered to my cybersecurity academy, so the Register with Forticare item is also checked off.) Click Begin.



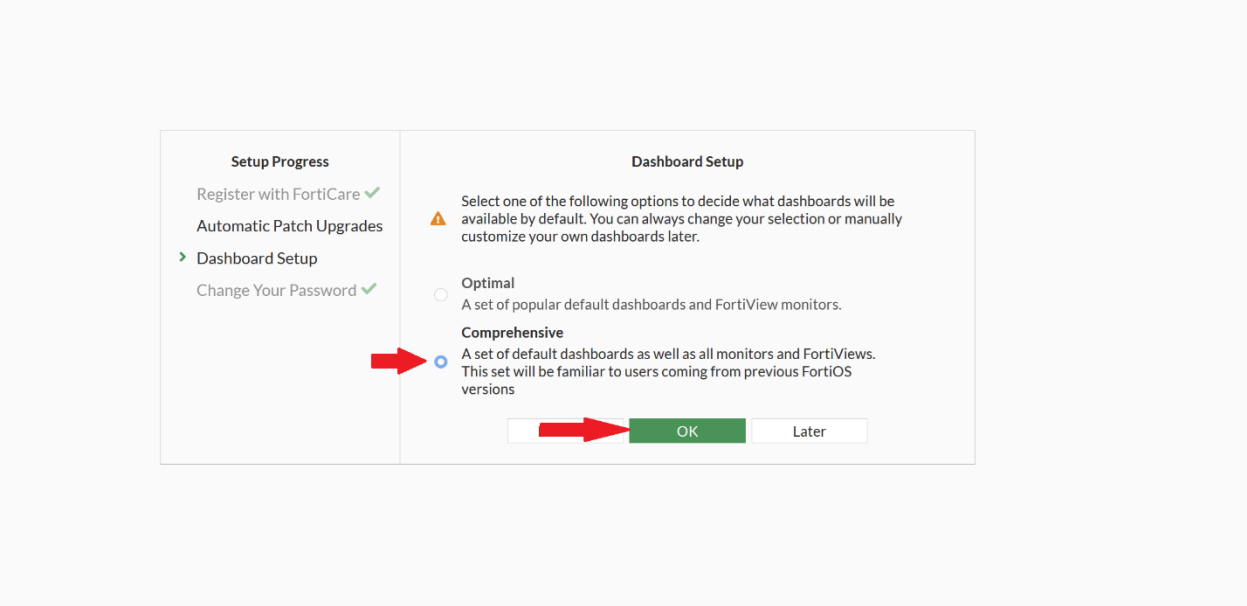
Click Enable Automatic Patch Upgrades and leave the other settings as default.



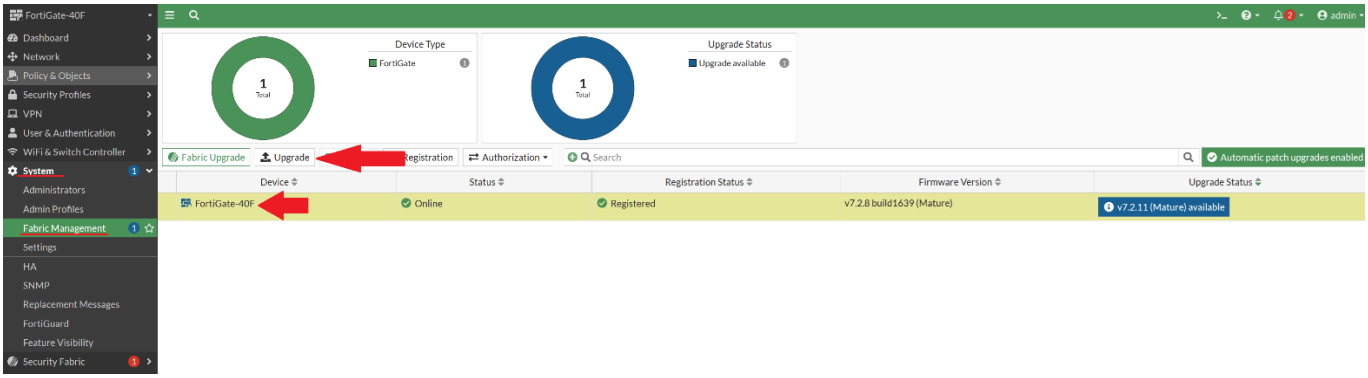
Click I acknowledge and click OK.



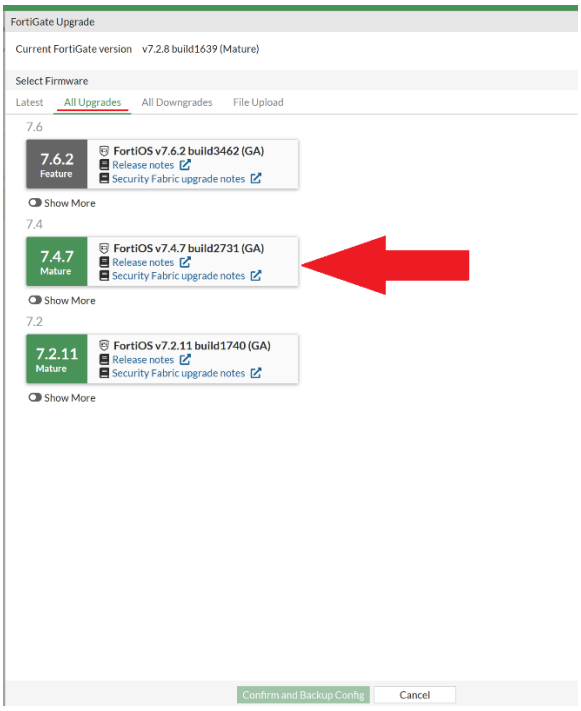
Choose the comprehensive dashboard and click OK.



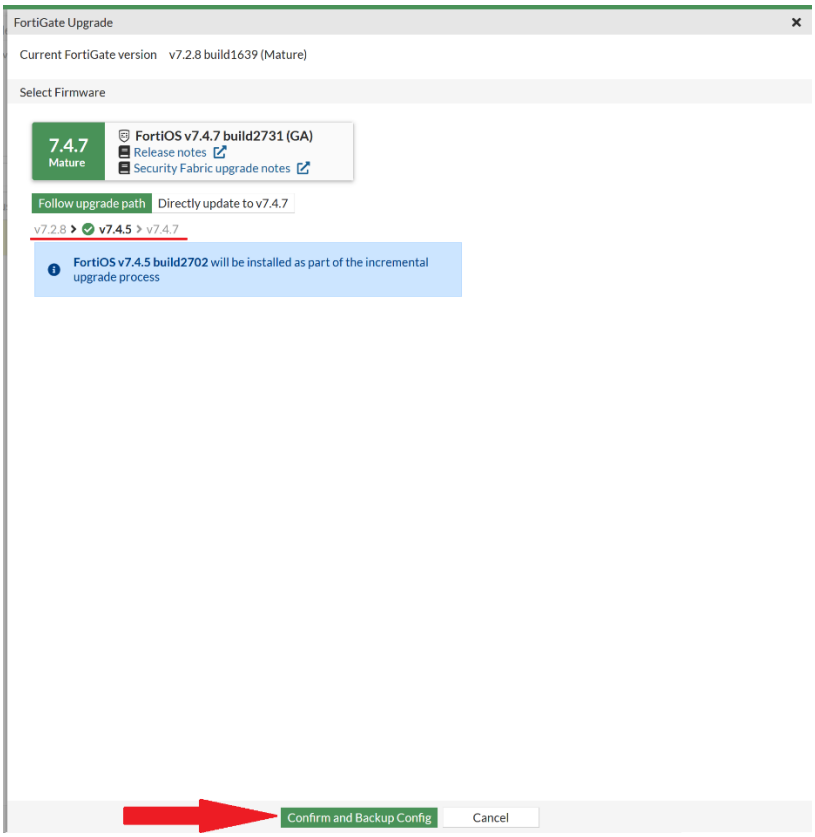
You should now see the main fortigate dashboard page. Next, we will update the system firmware. Click on System > Fabric Management (may be called Firmware and Registration in newer versions), click on the Fortigate 40F, then click Upgrade.



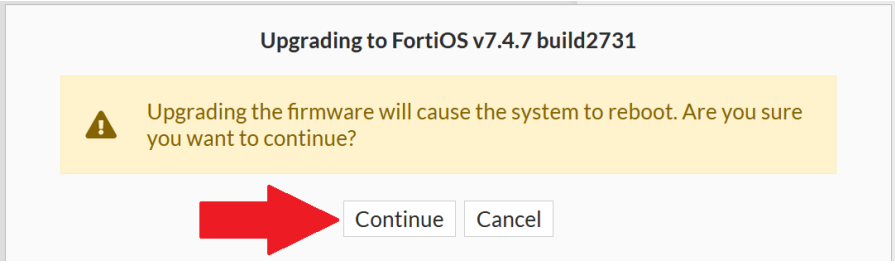
Click All Upgrades, then select the version you would like to upgrade to. In this lab, we opted to update to the latest version of FortiOS 7.4, as at the time, it was the latest version with a focus on bugfixes and stability (7.6 focused on feature updates, and wasn't as stable)



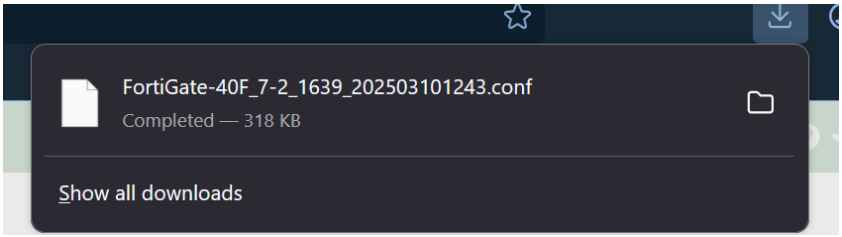
Click Confirm and Backup Config. Note that in most cases, multiple different versions of FortiOS will be installed as part of an incremental upgrade process. While there is an option to directly update between versions, following an upgrade path can decrease the chances of corrupting your configuration.



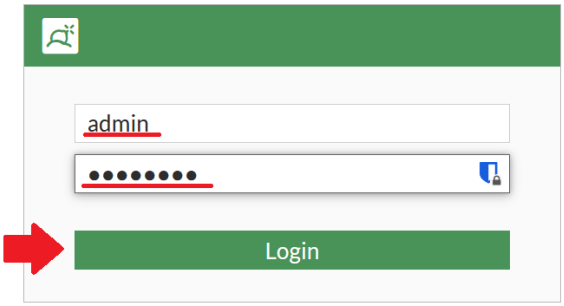
Click Continue, and wait for the upgrade process to complete.



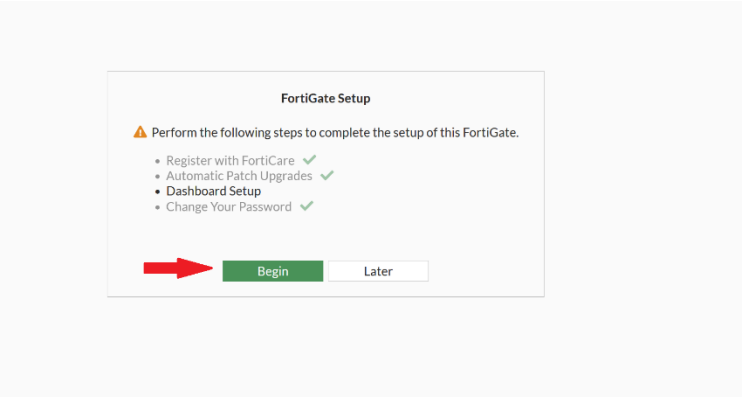
Note that a backup configuration file will be downloaded locally.

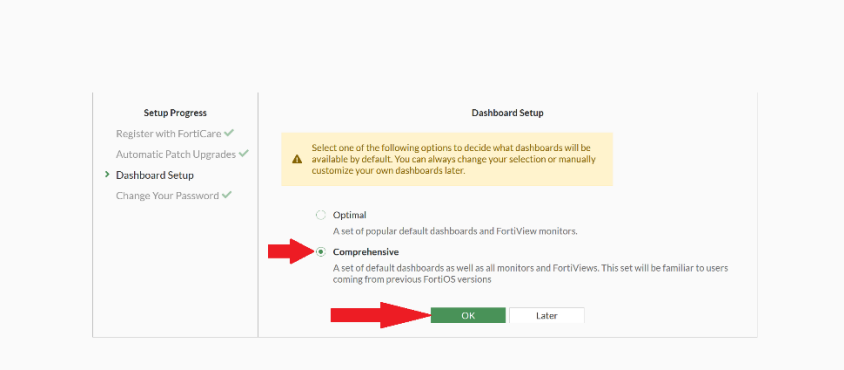


When the upgrade process is complete, reload the page and log in again.

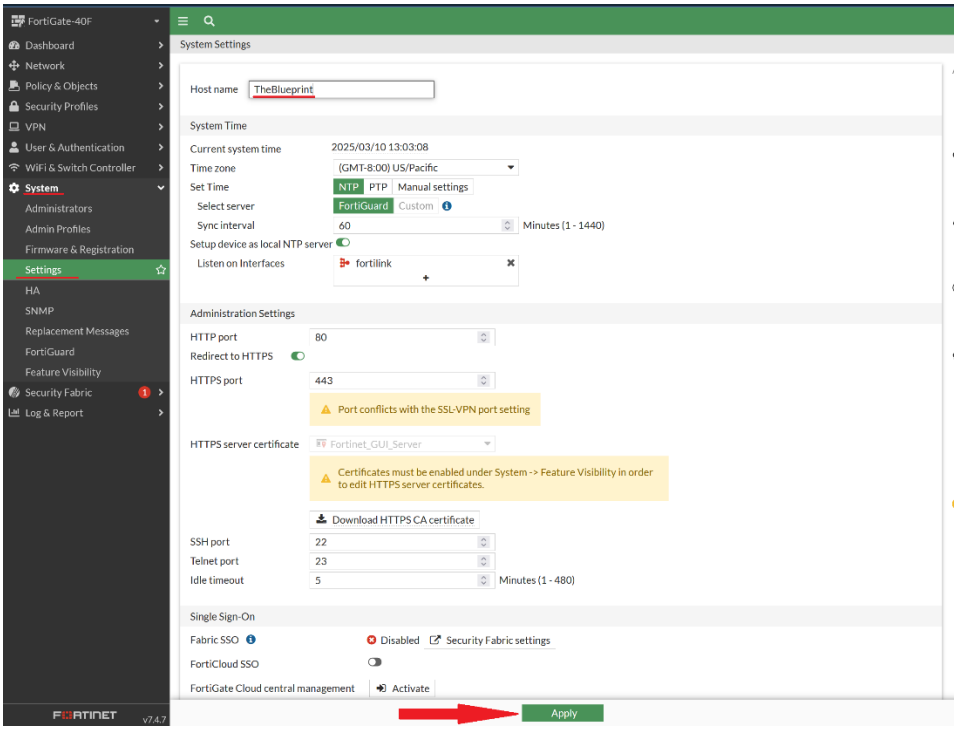


You may be asked to complete dashboard setup again. In this case, choose the Comprehensive dashboard like before.

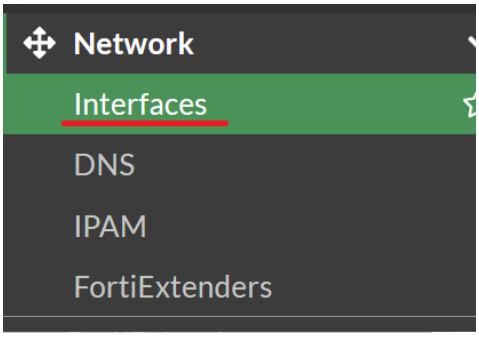




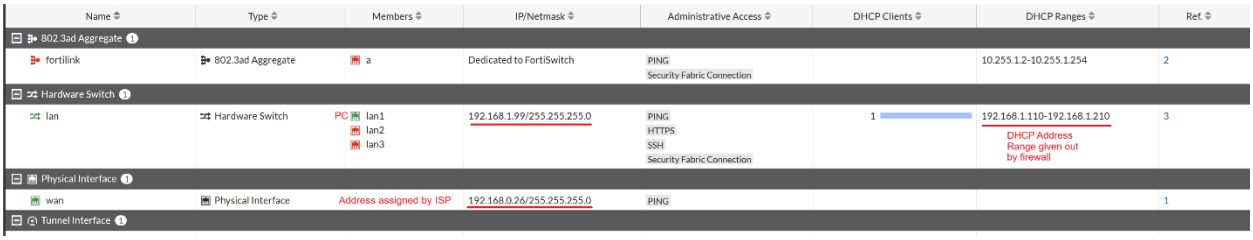
You should now see the firewall's dashboard. Next, we will configure a hostname for the firewall. Go to System > Settings, enter a host name, and click Apply.



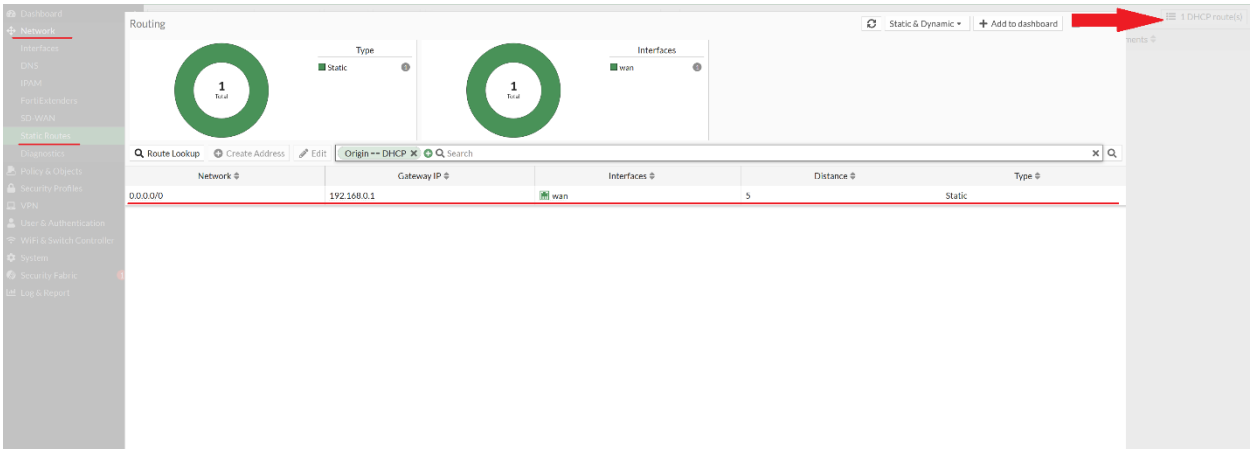
We will now verify the firewall's basic configuration. Go to Network > Interfaces.



You should see that the LAN interface is configured to give out addresses on the 192.168.1.0/24 network, with one device (your PC) connected. You should also see that the WAN interface has an IP given out by your ISP.



Next, click on Network > Static Routes and click on DHCP routes. You should see that a default route out the WAN interface has automatically been configured.



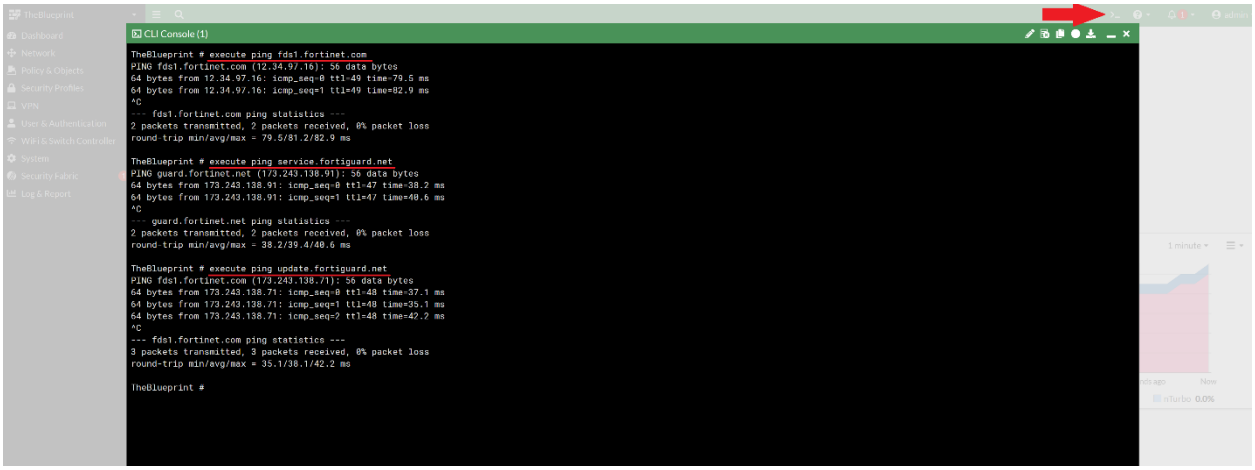
Click the CLI Console icon in the top right corner and run the following commands:

```
execute ping fds1.fortinet.com
```

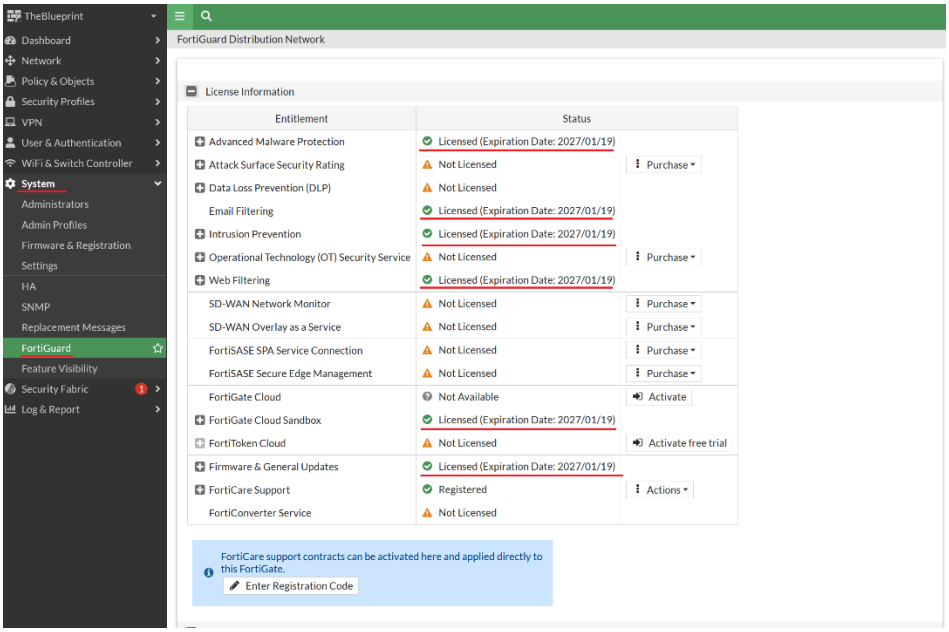
```
execute ping service.fortiguard.net
```

```
execute ping update.fortiguard.net
```

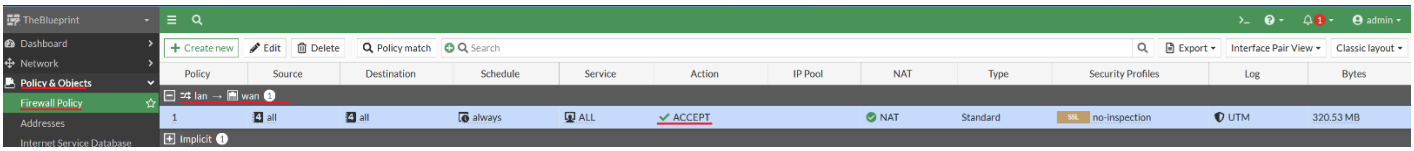
Ensure that you receive a response from each of these servers.



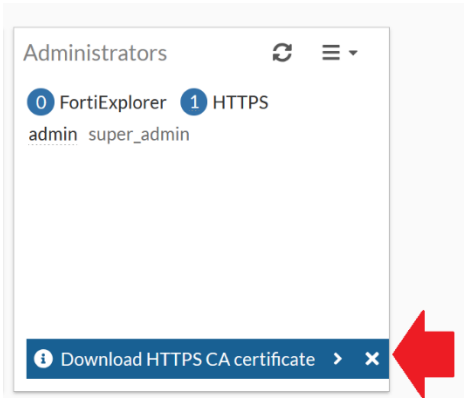
Next, go to System > FortiGuard and ensure your firewall has licenses for essential firewall functions, such as Email filtering, Web filtering, and Firmware updates.



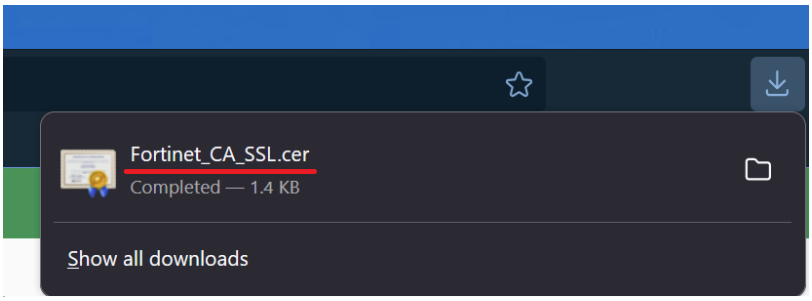
Next, go to Policy & Objects > Firewall Policy and ensure there is a policy allowing traffic between the LAN and WAN interfactes.



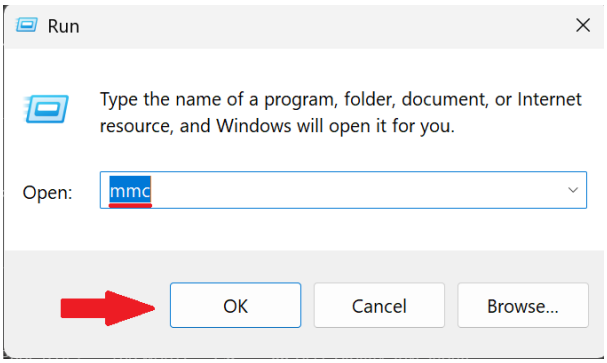
Return to the dashboard page, and under Administrators, click Download HTTPS CA certificate.



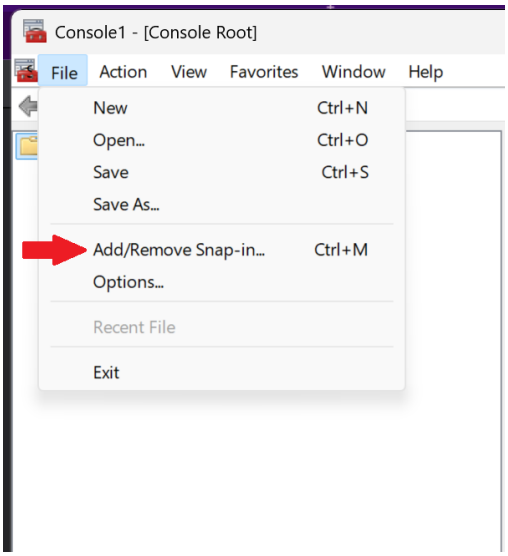
You should see a certificate file download to your PC.



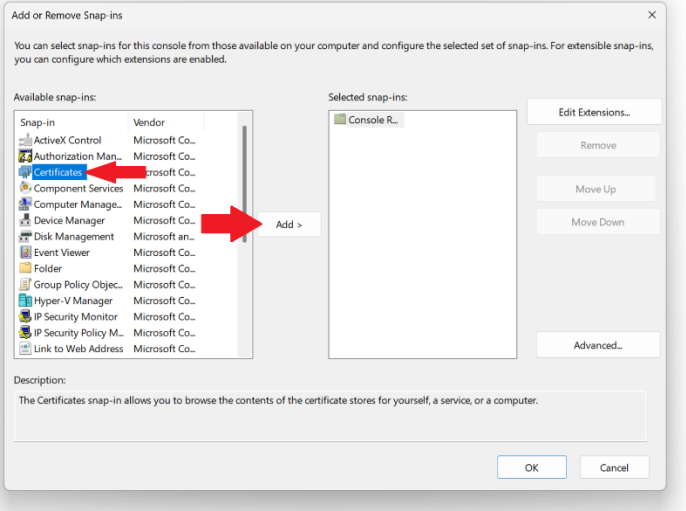
Next, we will install this certificate. On your PC, open the Run dialog (Windows+R) and type “mmc”.



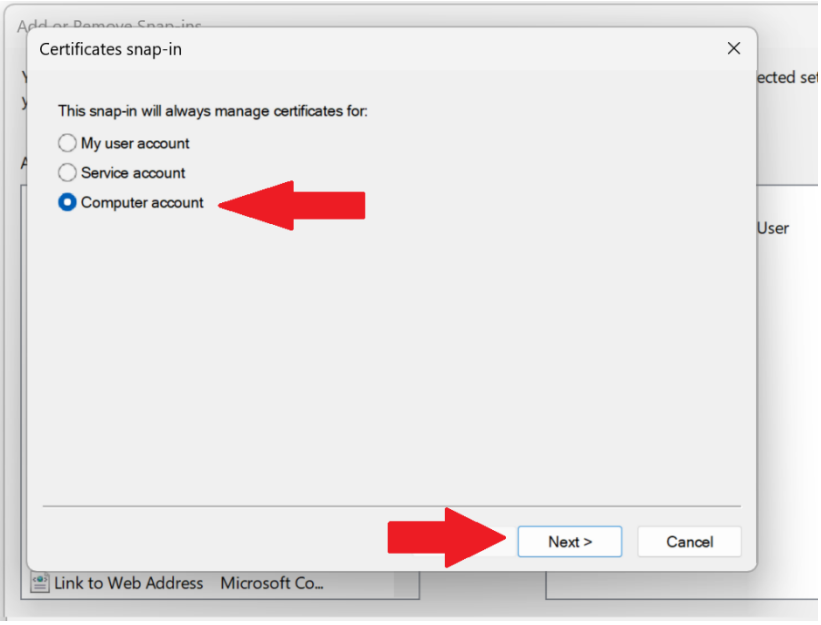
In the resulting window, click File > Add/Remove Snap-in.



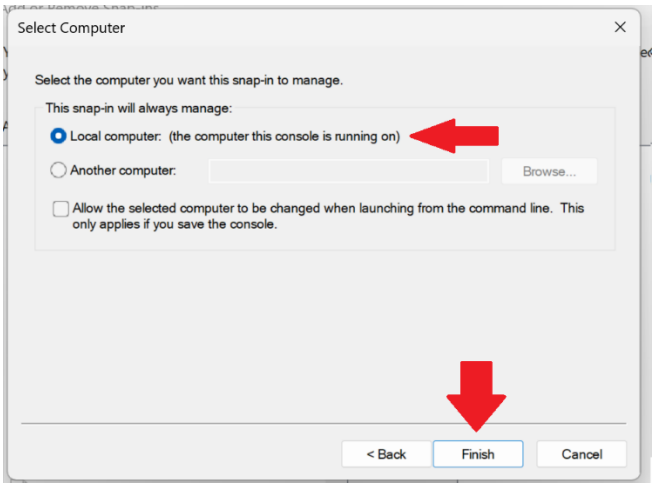
In the resulting window, click on Certificates > Add.



In the resulting window, click on Computer Account > Next.

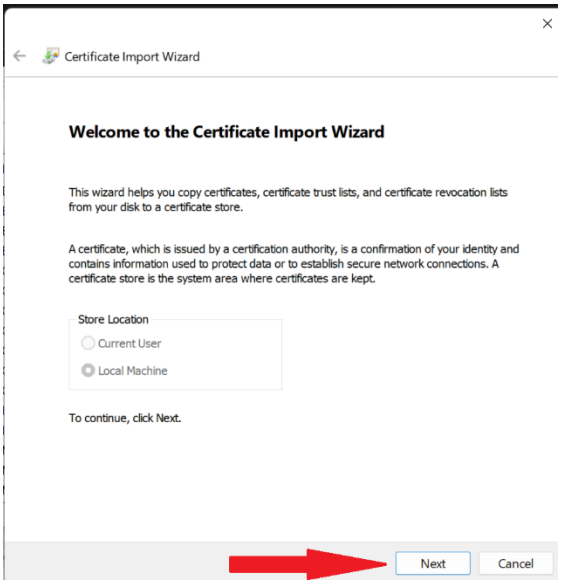


Make sure Local Computer is selected and click Finish.

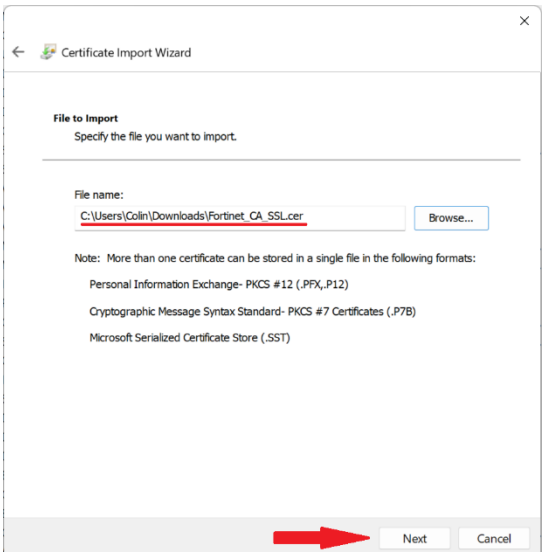


Inside Trusted Root Certification Authorities, right-click on Certificates and click on All Tasks > Import.

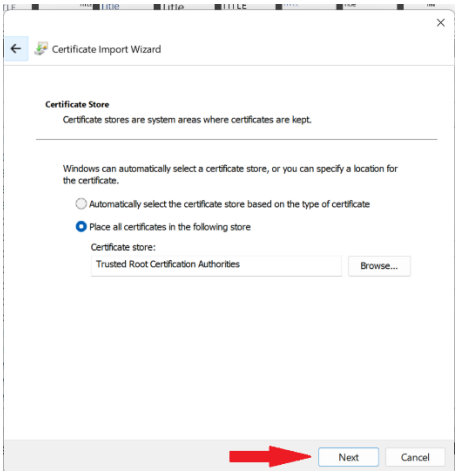
Click “Next”.



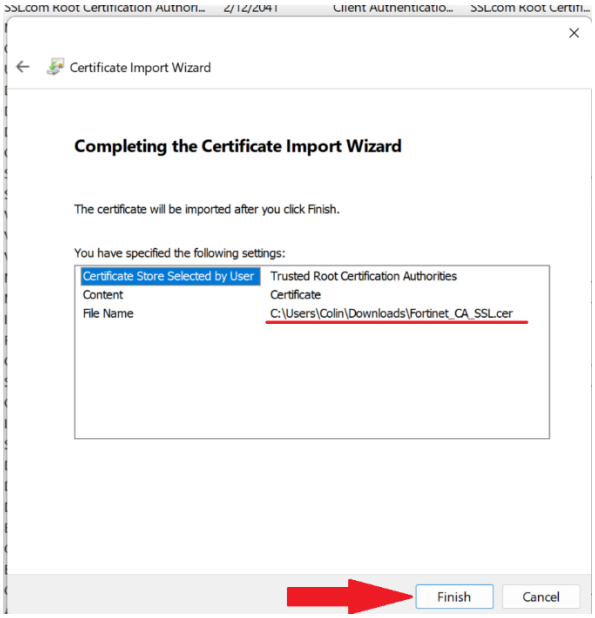
Select the certificate file downloaded earlier, then click “Next” again.



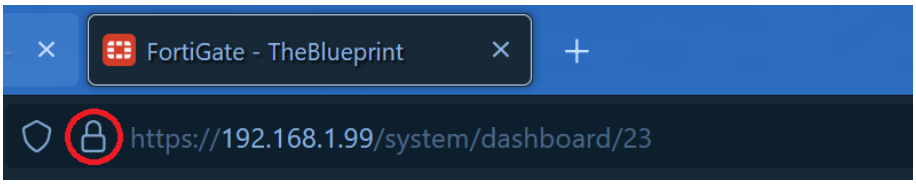
Leave the certificate store location setting as the default value, then click “Next”.



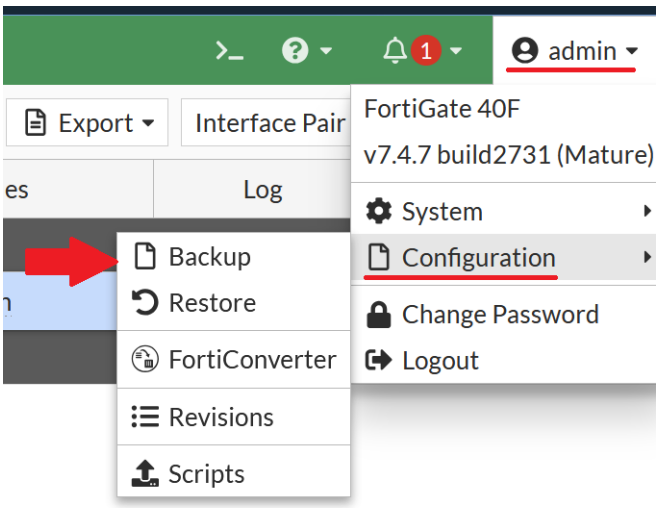
Click “Finish” to confirm the certificate import.



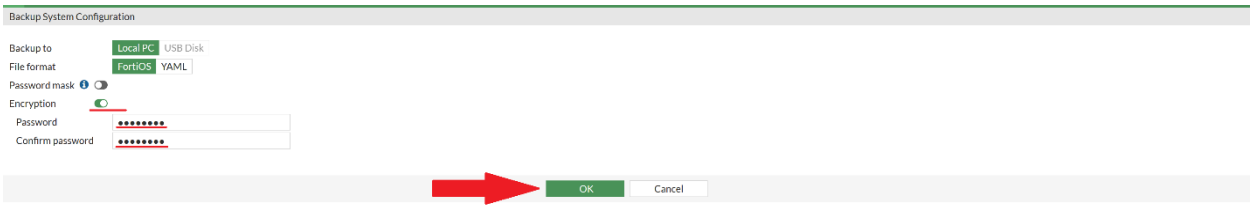
Close and reopen your browser, and ensure that the HTTPS lock icon appears when opening the firewall's management page.



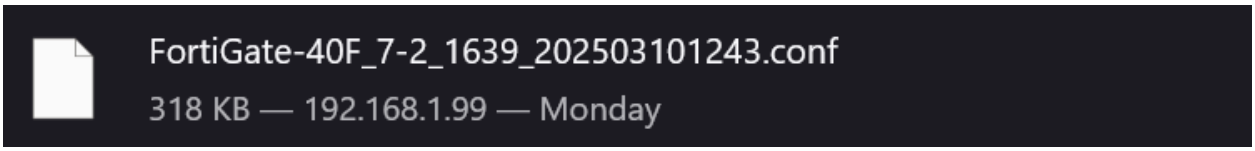
Next, we will back up the firewall's configuration. Click on the admin profile picture in the top right, then click on Configuration > Backup.



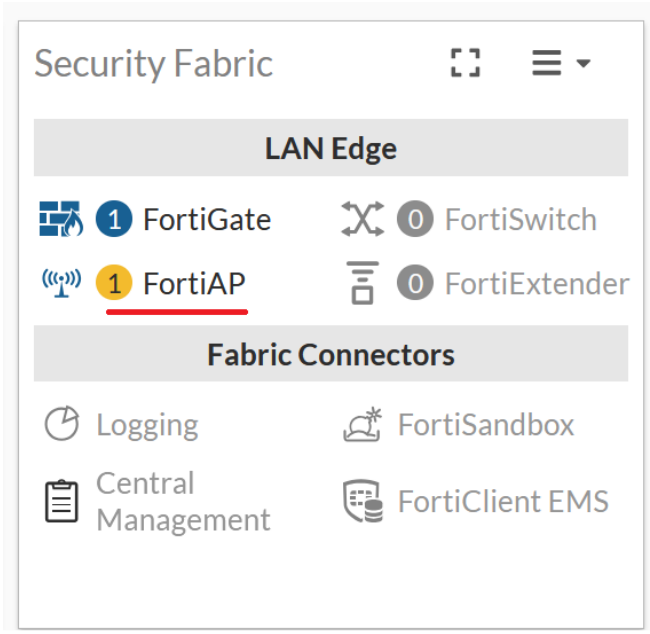
Enable Encryption and enter a secure password for the backup. Click OK.



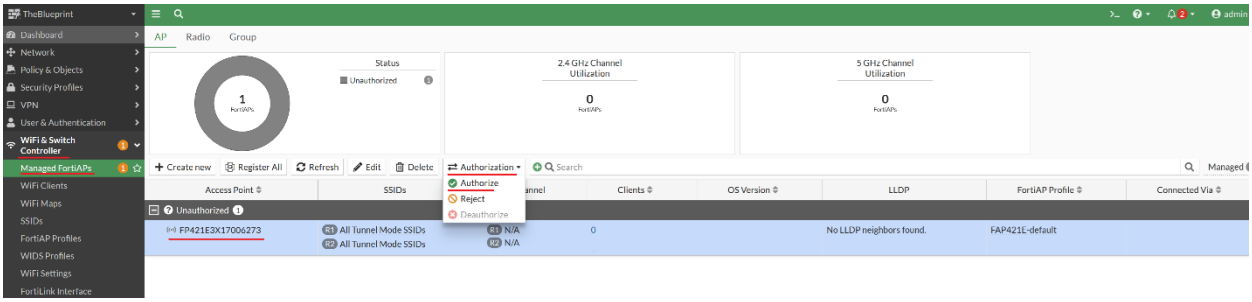
The backup file will be downloaded to your PC.



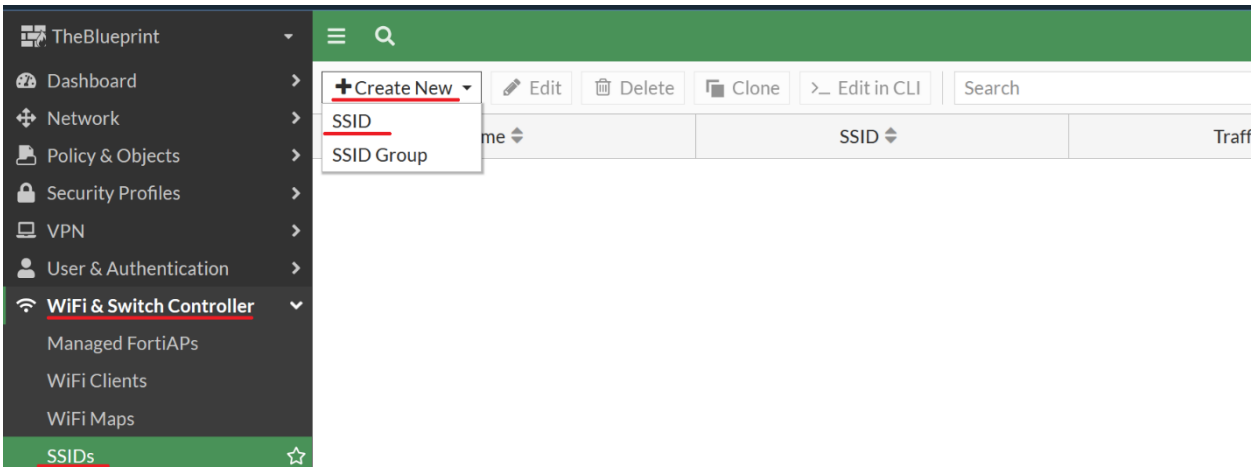
Next, we will set up the AP. Return to the Dashboard, and under Security Fabric, ensure that one (1) FortiAP device is visible.



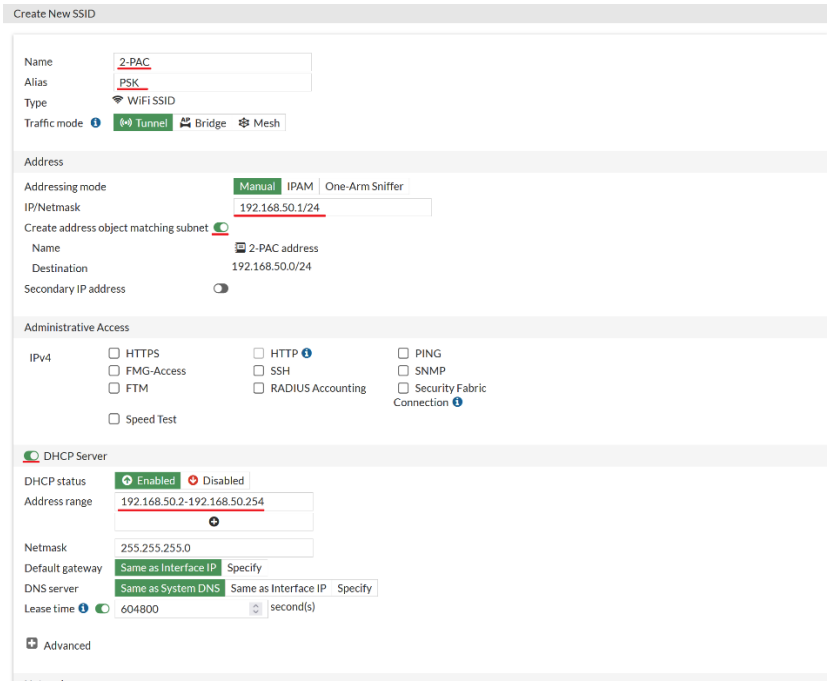
Go to WiFi & Switch Controller > Managed FortiAPs, click on the unauthorized AP, and click Authorization > Authorize.



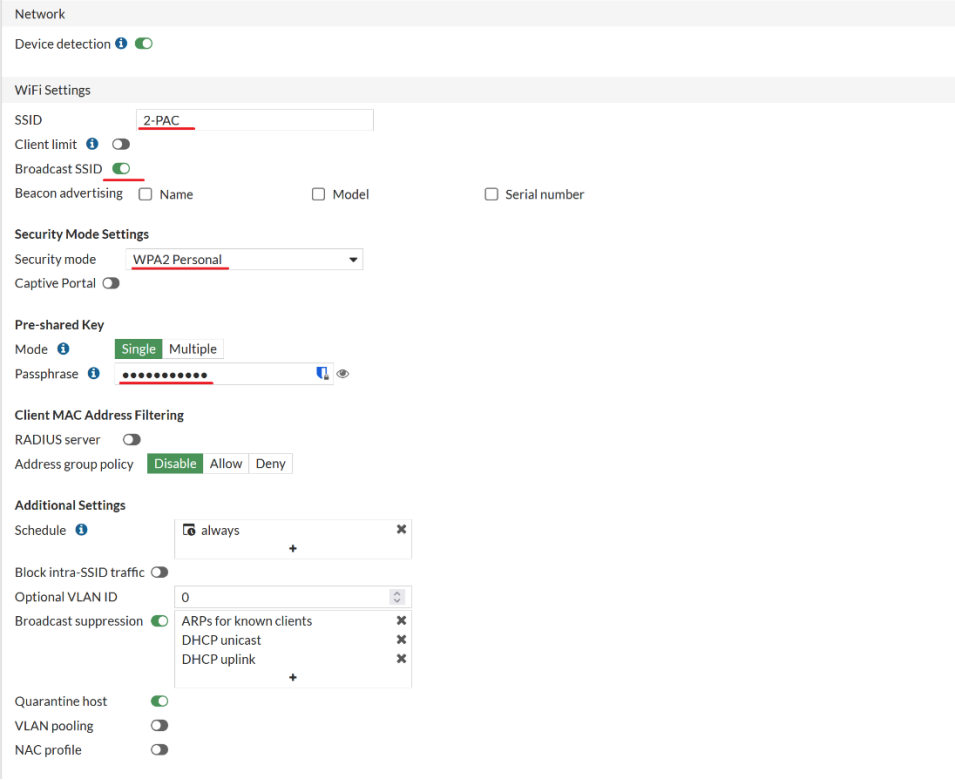
Next, we will set up the WPA2-PSK SSID. Go to WiFi & Switch Controller > SSIDs, and click Create New > SSID.



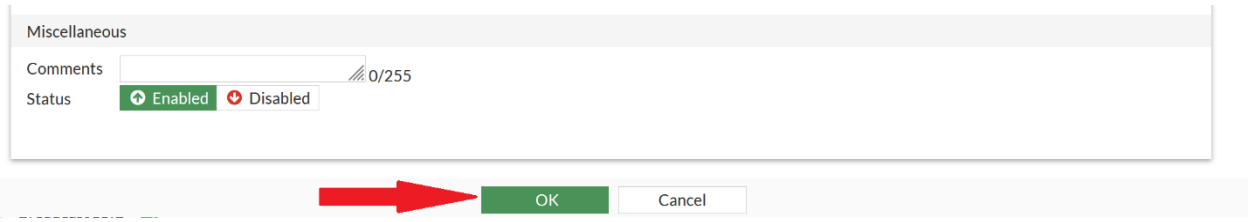
Configure an appropriate name (in this case, we called it 2-PAC) and alias. Give the SSID an appropriate IP and netmask, and ensure that an address object matching the subnet is created. Ensure that the DHCP server option is enabled. The DHCP server settings should automatically match the network settings configured in the Address section.



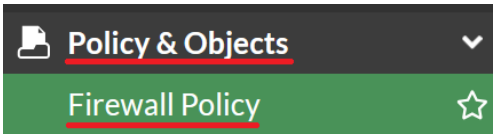
Set the SSID to the same as the name, ensure that the SSID is being broadcasted, set the security mode to WPA2 Personal, and configure an appropriate passphrase.



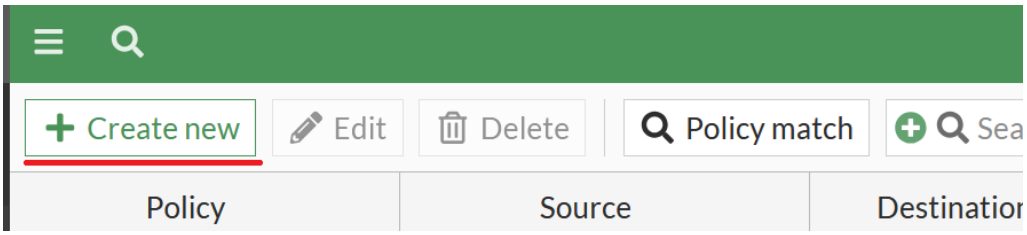
Click OK.



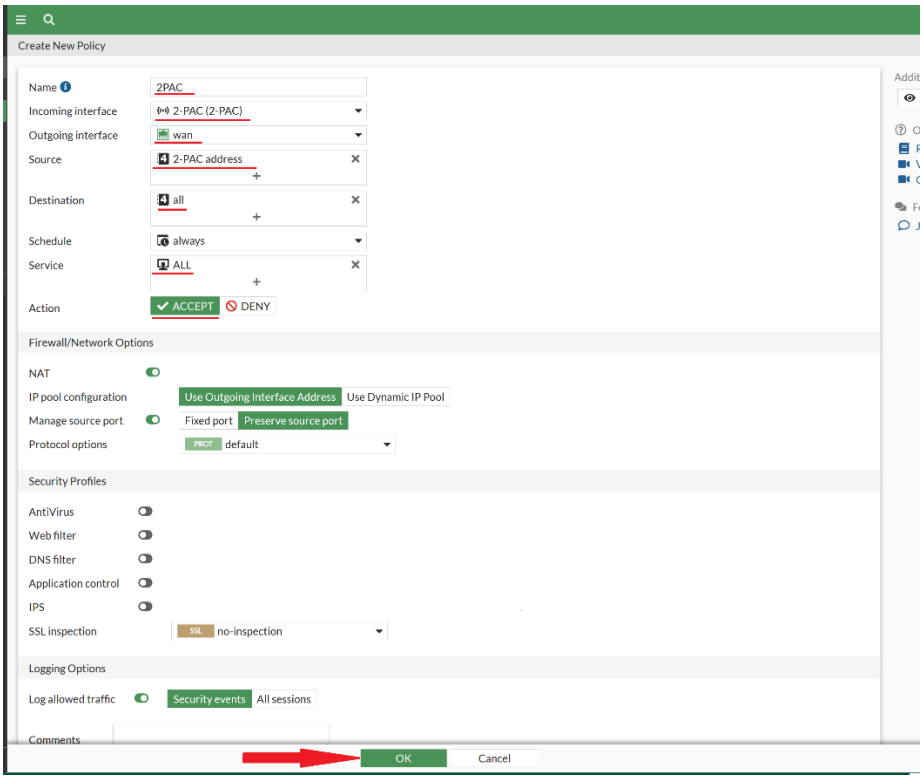
Go to Policy & Objects > Firewall Policy.



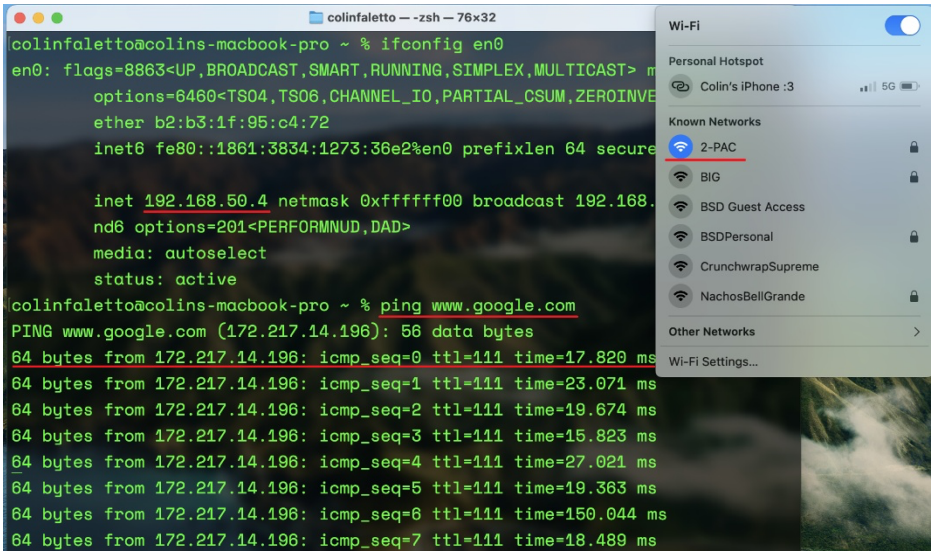
Click Create new.



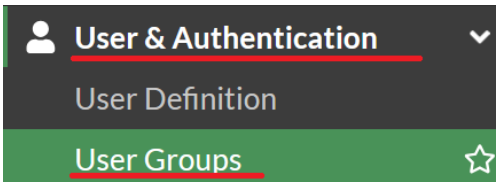
Configure an appropriate name. Set the incoming/outgoing interface to the PSK WLAN and the WAN respectively. Set the source and destination to the PSK address object and “all” respectively. Set the action to Accept and click OK.



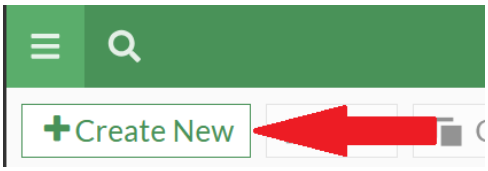
Your PSK WLAN should now be fully set up. Confirm that it works by connecting another device, inputting the password configured earlier. As seen in the screenshot below, when connected to the 2-PAC network, my laptop recieves an address in the 192.168.50.0/24 network, and can successfully ping outside of the network.



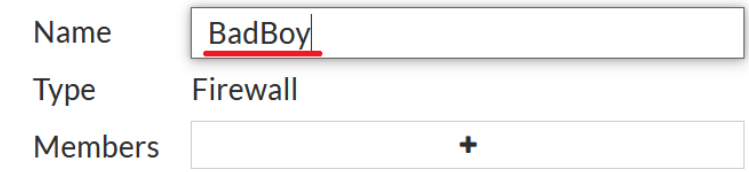
Next, you will configure Local User authentication for the WPA2 Enterprise WLAN. Go to User & Authentication > User Groups.



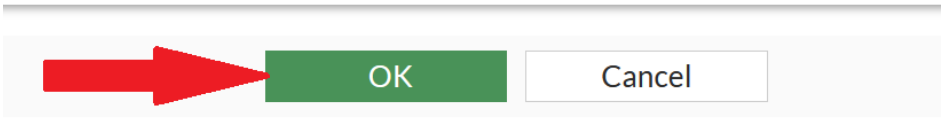
Click Create New.



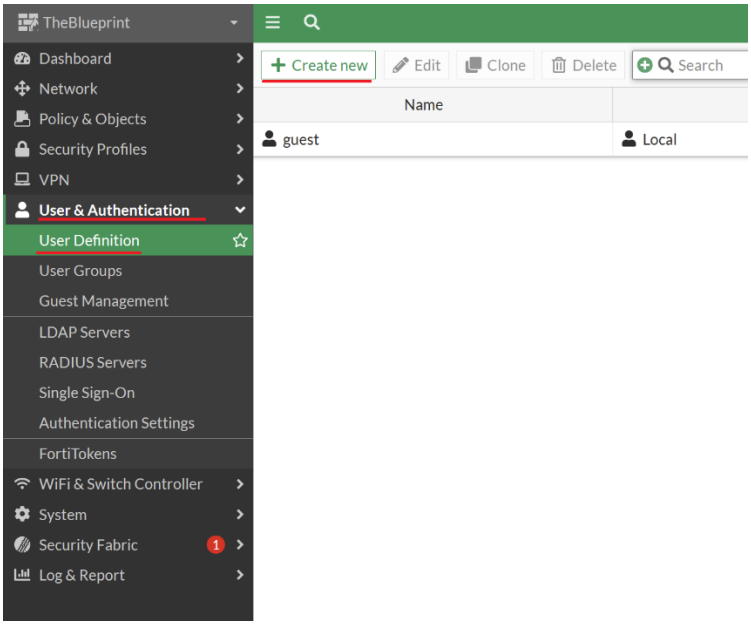
Choose an appropriate group name.



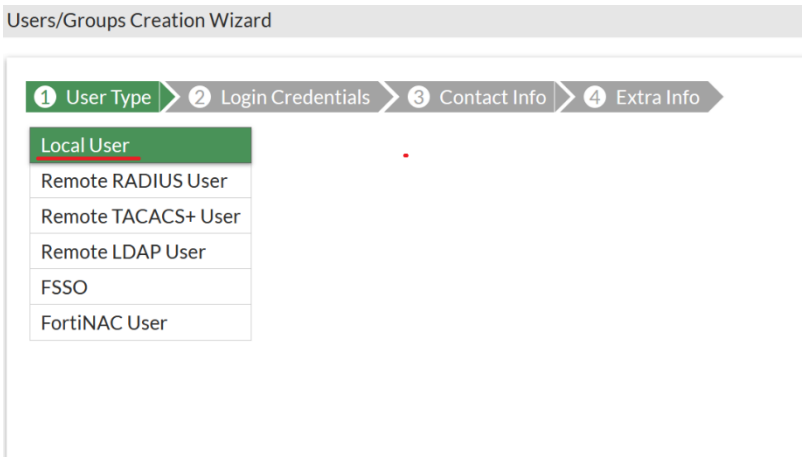
Click OK.



Go to User & Authentication > User Definition and click Create new.

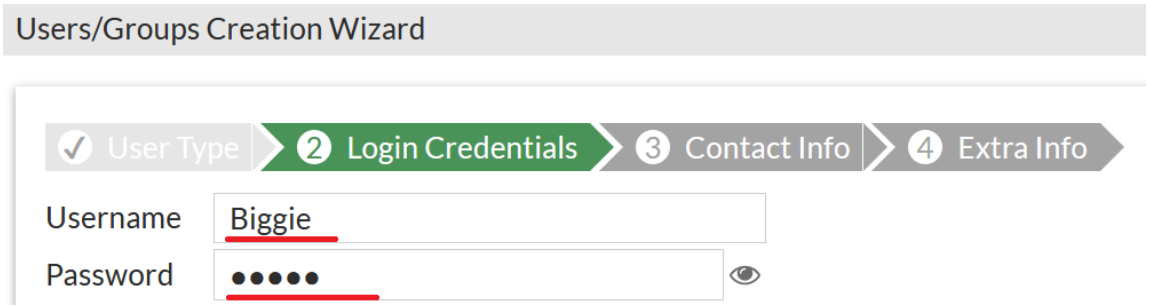


Set the User Type to Local User.



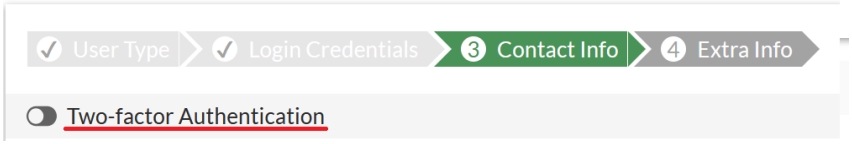
Click Next.

Set an appropriate username and password.



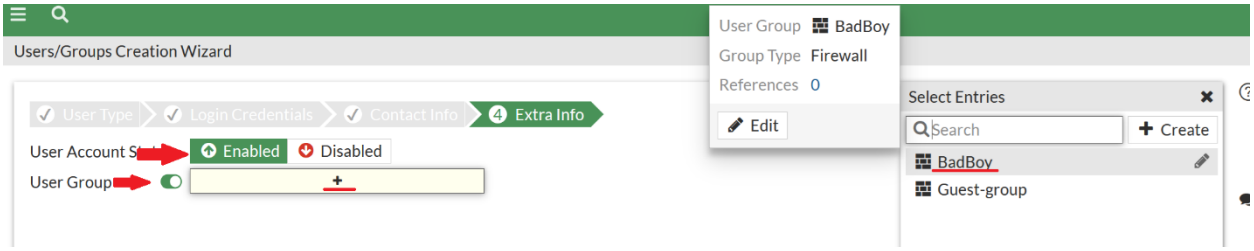
Click Next.

Under Contact Info, leave two-factor authentication off.

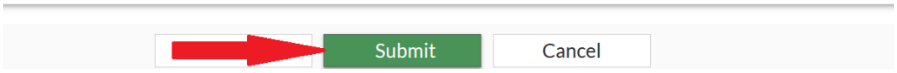


Click Next.

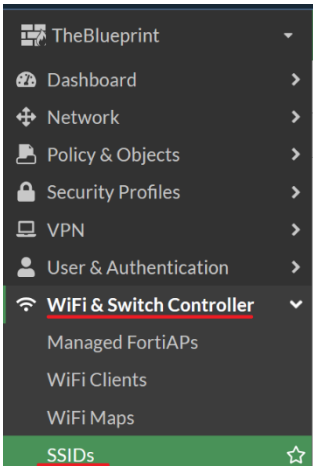
Set the User Account Status to Enabled, enable User Group, click the plus icon, and select the User Group created earlier.

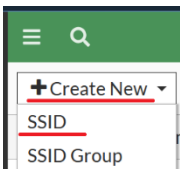


Click Submit.

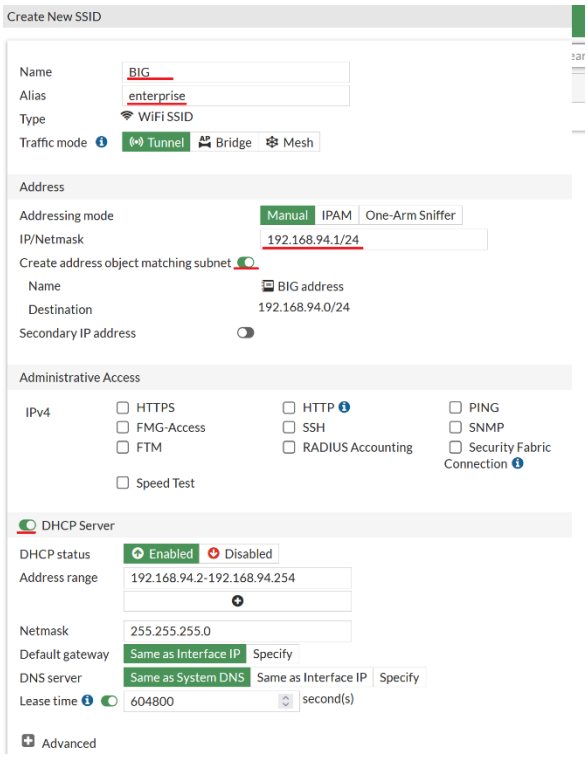


Next, we will set up the WPA2-Enterprise SSID. Go to WiFi & Switch Controller > SSIDs and click Create New > SSID.

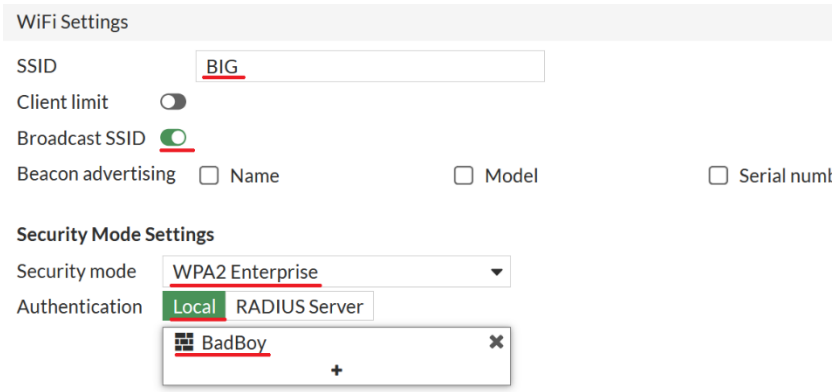




Assign an appropriate name (in this case, we chose BIG) and alias. Assign an appropriate IP/netmask, and ensure that an address object is created matching the subnet. Ensure that a DHCP server for the subnet is created.

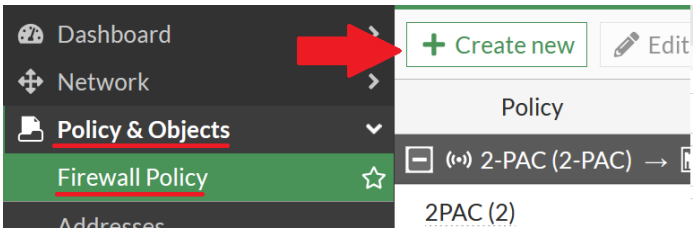


Set the SSID to the same as the name, ensure the SSID is broadcast, set the security mode to WPA2 Enterprise, set the authentication to Local, and add the user group created earlier.

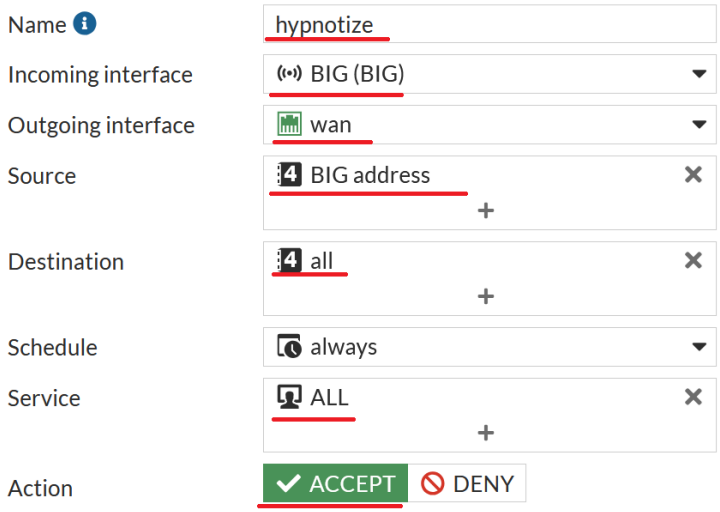


Click OK.

Next, we will configure a firewall policy to allow traffic from the Enterprise WLAN to reach the WAN.

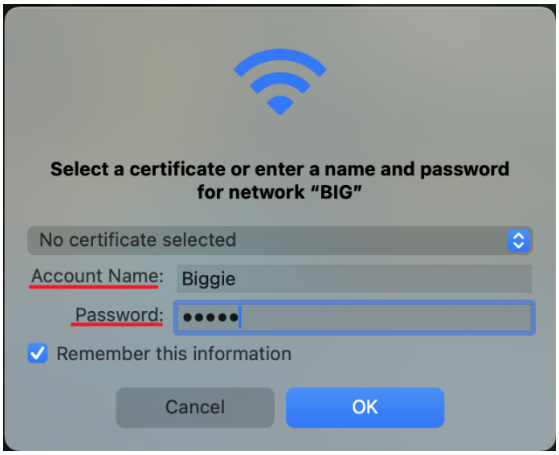


Configure an appropriate name. Set the incoming/outgoing interface to the Enterprise WLAN/WAN interfaces respectively. Set the source/destination to the address object for the WLAN and “all” respectively. Set the service to ALL and the action to ACCEPT.



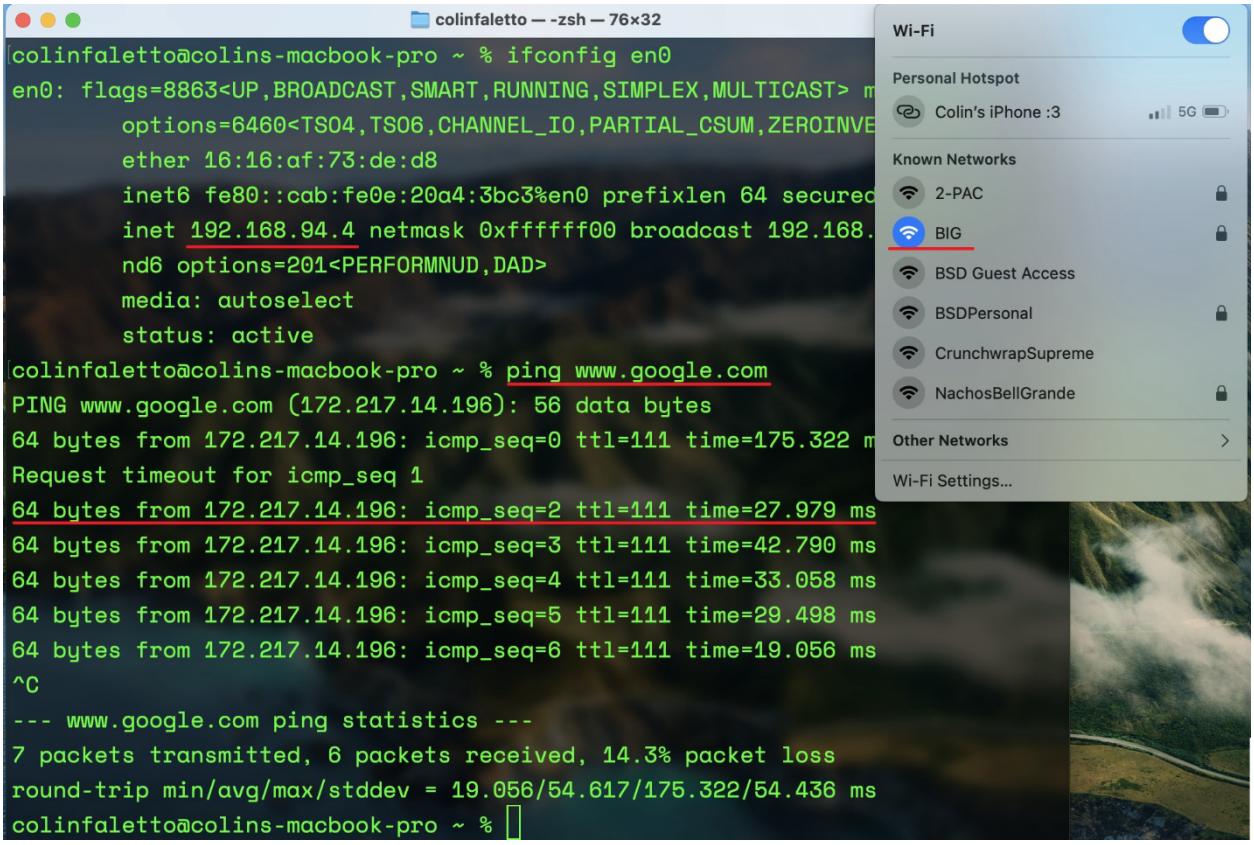
Click OK.

Your Enterprise WLAN has now been set up. To test it, connect from another WiFi-capable device. You should see a login prompt similar to this:

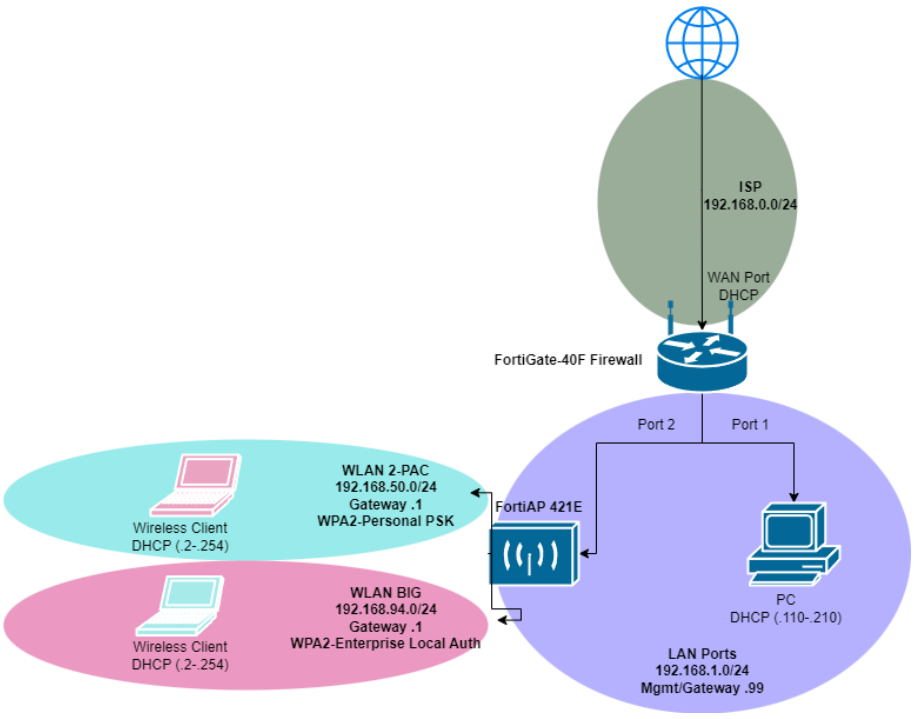


Enter the username and password configured for the local user, then connect. Ensure that you trust the firewall’s certificate when connecting. As seen in the screenshot

below, when connected to the BIG network, my laptop recieves an address in the 192.168.94.0/24 subnet and can successfully ping outside the network.



Network Diagram (IPv4)



Problems

We found that the FortiAP cannot be plugged directly into the FortiGate without a separate power source, as the FortiGate does not provide power over ethernet. We fixed this by placing a standard 48V PoE injector in between the firewall and the access point.

Conclusion

To wrap up, I now have a strong understanding of the basic Fortinet ecosystem, the FortiOS GUI interface, and various WPA2 security policies. I am now confident that I could replicate this setup in a real SOHO environment.

Signoff