

# Portfolio – Newport Advanced Cisco Networking Academy – Newport Cybersecurity Academy

Colin J. Faletto



## Table of Contents

Building Network Infrastructure/Donating IT Equipment in Antigua: Rotary Club of Antigua/BBRC/RCKD .....	5
AWS Academy Cloud Foundations: Configuring Elastic Block Store, Relational Database Service, and Elastic Cloud Compute Auto Scaling.....	12
Palo Alto Networks Cybersecurity Academy: Configuring GlobalProtect RAVPN on a PA220 Firewall.....	52
AWS Academy Cloud Foundations: Configuring Identity and Access Management, Virtual Private Cloud, and Elastic Compute Cloud .....	83
Advanced Cisco Networking Academy: Configuring a Cisco Wireless Access Point and WLC with WPA2-PSK and WPA2-Enterprise with a RADIUS Server .....	130
Fortinet Cybersecurity Academy: Configuring a FortiGate 40F Firewall for a SOHO Environment/Configuring a Fortinet 421E AP with WPA2-PSK and WPA2-Enterprise Local Auth .....	160
Advanced Cisco Networking Academy: Configuring a Network with the IS-IS Routing Protocol .....	188
Fortinet Cybersecurity Academy: Configuring an IPSec Site-to-Site VPN on a FortiGate 40-F Firewall.....	201
Fortinet Cybersecurity Academy: Configuring an SSL Remote Access VPN on a FortiGate 40-F Firewall.....	210
Advanced Cisco Networking Academy: Designing a Multi-Area OSPF Network .....	230
Advanced Cisco Networking Academy: Designing a Multiprotocol Network with BGP .....	246
Advanced Cisco Networking Academy: Designing a Multiprotocol Network with Internal/External BGP .....	269
Palo Alto Networks Cybersecurity Academy: Factory Resetting a PA220 Firewall .....	304

Advanced Cisco Networking Academy: Installing and Preparing Windows 11 .....	310
Advanced Cisco Networking Academy: Layer 2 Attacks and Mitigations.....	322
Palo Alto Networks Cybersecurity Academy: Setting up Web Filtering .....	339
Palo Alto Networks Cybersecurity Academy: Setting up a PA220 Firewall for a SOHO Environment.....	356





# Building Network Infrastructure/Donating IT Equipment in Antigua – Rotary Club of Antigua/BBRC/RCKD

Steve Lingenbrink, Colin J. Faletto, Jeffrey Cheung, Eric Xia



ROTARY CLUB  
OF KIRKLAND DOWNTOWN

Bellevue Breakfast



## Sites Visited

### Clare Hall (Living Hope) Christian Union Church

Address: 45GC+HWX, Wireless Rd, Piggotts

Days Visited: 17-Feb

Completed Tasks:

- Donated Laptops

Equipment Used/Donated:

- 15 Laptops/chargers

Comments:

Our team was originally told to install new networking equipment in an external building, but this work had already been done by a third-party contractor.

### Post-Millennial Academy

Address: 35QP+4PJ, All Saints Rd, Potters Village

Days Visited: 17-Feb

Completed Tasks:

- Donated Laptops
- Donated Projectors

Equipment Used/Donated:

- 44 Laptops/chargers
- 4 Projectors

Comments:

Big, well-funded private school (244 students); they need a lot of equipment but can likely afford to buy a lot of it themselves

### Christ the King High School

Address: 45G8+2P6, Old Parham Rd, St John's

Days Visited: 17-Feb, 18-Feb

Other teams at school: Sara, Norm

Completed Tasks:

- Assisted Sara's team in mounting APs along back hallway
- Installed point-to-point to art room, connected to an AP mounted on the wall
- Assisted Norm's team in re-running cables to APs in back room



ROTARY CLUB  
OF KIRKLAND DOWNTOWN

Bellevue Breakfast



- Fixed AP/point-to-point in music room

Equipment Used/Donated (just our team):

- 1 Ubiquiti point-to-point set
- Cisco AP/mounting bracket
- 2 Ubiquiti Power Injectors
- 1 Cisco power injector
- 1 power strip

Comments:

Heavy collaboration with other teams, CTK is routinely a major project for the rotary club

### **New Bethel Seventh Day Adventist Academy**

Address: 26R4+XGH, Liberta

Days Visited: 19-Feb, 20-Feb

Completed Tasks:

- Replaced old faulty switch (restored internet to computer lab)
- Installed new wall-mounted Cisco AP in computer lab
- Pulled old, broken cable
- Installed point-to-point from computer lab to external classroom, connected to wall-mounted AP

Equipment Used/Donated:

- 12 Laptops/chargers
- 1 Cisco PoE switch
- 2 Cisco APs
- 1 Cisco AP mounting bracket
- 1 Ubiquiti point-to-point set
- 2 Ubiquiti power injectors
- 1 Cisco power injector

Comments: Computer lab is very well-maintained; school was getting accredited within a few days so fixing their internet was well-appreciated

### **Liberta Primary School**

Address: 26M5+RR8, Liberta

Days Visited: 19-Feb

Completed Tasks:

- Donated Laptops



Bellevue Breakfast



Equipment Used/Donated:

- 24 Laptops/chargers

Comments: Very brief visit, our team was only there for ~10 minutes

### **Freeman's Village Primary School**

Address: 26M5+RR8, Liberta

Days Visited: 20-Feb

Completed Tasks:

- Donated Laptops

Equipment Used/Donated:

- 24 Laptops/chargers

Comments: Another very brief visit

### **Sunshine Home**

Address: 24J6+3FR, Urlings (On Valley Road, Across from Turners Beach, big painted mural out front)

Days Visited: 21-Feb, 25-Feb

Completed Tasks:

- Replaced old Linksys router with Cisco AP
- Ran new cable to computer lab
- Installed AP in computer lab
- Ran cable to dormitory building
- Installed AP in dormitory building

Equipment Used/Donated:

- 12 Laptops/chargers
- 3 Cisco APs
- 2 Cisco AP mounting brackets
- 3 Cisco power injectors

Comments:

Seemed like this was rotary's first time at this school, they didn't have any of our equipment

### **Boys' Training School / Denis Bowers Rehabilitation Center**

Address: 37JP+97H, Willikies



ROTARY CLUB  
OF KIRKLAND DOWNTOWN

Bellevue Breakfast



Phone: 463-2029

Dates Visited: 24-Feb

Other teams at school: Sara

Completed Tasks:

- Ran cable from fiber router in office to switch in break room
- Installed AP in break room
- Ran cable from switch to circular room, installed wall-mounted AP
- Ran cable from switch to middle of circular hallway, installed ceiling-mounted AP

Equipment used/donated:

- (Around) 24 laptops/chargers
- 3 Cisco APs
- 3 Cisco AP mounting brackets

Comments:

Rotary will assuredly be coming back to this school in the future, they still need internet in the external classroom, dining hall, guard room, and laundry room

### **Trinity Academy**

Address: 34FP+943, Jennings, Saint Mary

Dates Visited: 25-Feb

Completed Tasks:

- Donated Projectors

Equipment Used/Donated:

- 2 Fudoni Projectors

Comments:

We walked into some sort of emergency situation; police were there, so we didn't stay long

### **Golden Grove Primary School**

Address: 4545+P3H, Valley Rd, St John's

Dates Visited: 25-Feb

Other teams at school: Sara, Hansen

Completed Tasks:



Bellevue Breakfast



- Installed new wall-mounted switch in classroom block, installed APs
- Installed point-to-point to switch in block of classrooms, installed 3 wall-mounted APs

#### Equipment Used/Donated:

- Refer to documentation from Sara's team/Hansen's team, our team only came in at the tail end of the project and was not here long enough to collect this information



ROTARY CLUB  
OF KIRKLAND DOWNTOWN

Bellevue Breakfast







# AWS Academy Cloud Foundations: Configuring Elastic Block Store, Relational Database Service, and Elastic Cloud Compute Auto Scaling

Colin J. Faletto, CCNA

## Purpose

This write-up is intended to document and explain the fourth, fifth, and sixth in the AWS Academy Cloud Foundations course. These labs are intended to provide additional knowledge in the field of cloud computing, such as block-level file storage for virtual machines, basic relational database configuration, and automatic infrastructure scaling to meet user demand. These concepts are essential for new cloud engineers to provide parallels to more advanced facets of traditional IT. These labs also provide a strong foundation of knowledge for the AWS management console, as they all take place primarily inside this console.

## Background

Amazon is a company based in Seattle that runs the biggest e-commerce platform in the world. They were started in 1994 by former CEO Jeff Bezos, and have grown from a small online bookstore to a giant online store offering a wide variety of products. Amazon also has a strong physical retail presence in the grocery space with their Amazon Fresh and Whole Foods chains, and has a strong online media presence through Twitch, Prime Video, and Amazon Music, which provide entertainment in the form of livestreams, movies and television shows, and music respectively. Amazon also has a popular line of e-readers and tablets with their Kindle brand and has a successful brand of artificial intelligence assistants with their Amazon Alexa A.I. and their Amazon Echo line of smart speakers.

Amazon Web Services, or AWS, is Amazon's cloud computing division. It was created in 2002 to provide simple web services to customers and expanded to cloud storage and computing in 2006. It is the leading cloud service provider and is popular for its pay-as-you-go service model. AWS provides services to everyone from small businesses to massive companies like Coca-Cola and Apple, and even provides web infrastructure to government branches. AWS takes the responsibility and cost of managing a data center out of the hands of businesses and maintains a massive global network of Amazon data centers that split customer traffic among them. AWS currently has 34 geographic regions, each of which have multiple availability zones which themselves contain multiple data centers. These data centers are in undisclosed locations for security reasons, though their general position is published. AWS offers services for virtual machines, cloud storage, database management, machine learning, IoT services, cloud networking, and much more.

Amazon Elastic Compute Cloud, or EC2, is an AWS service that allows customers to create virtual machines in the AWS cloud. These machines are very versatile, as they can be allocated as many or as few resources (CPU, RAM, GPU) as needed and can run nearly any operating system. By default, EC2 instances will run Amazon Linux, which is a version of Linux optimized for AWS servers. Amazon's e-commerce platform, its primary source of revenue, has been running on EC2 instances for over a decade. EC2 instances have a variety of different types, which are optimized for different purposes such as memory (R series, X series), compute (C series), and storage (H series, I series, D series).

Amazon Virtual Private Cloud, or VPC, is an AWS service that provides a virtual network inside the AWS cloud. This service allows AWS objects, such as EC2 instances, to communicate with each other. In a VPC, each EC2 machine is assigned a unique private IPv4 address, which is then connected via NAT to a public address on an internet gateway. Using this gateway, machines in the VPC can communicate with other AWS VPCs and other Internet-connected machines. Amazon VPC is provided at no additional charge to customers using EC2 instances.

Amazon Identity and Access Management, or IAM, is an AWS service that provides a layer of security to customers by limiting the resources different users can access. IAM follows the principle of least privilege, meaning that by default, all AWS controls are blocked for users unless they have been explicitly granted permissions. IAM represents a portion of the customer responsibilities in the AWS shared responsibility model, which is a model outlining that AWS is responsible for the physical security of data centers and networks while the customer is responsible for keeping their customer data and configurations safe. One of IAM's unique features is its role feature, which creates identities with elevated permissions that can be temporarily assigned to users. This feature works similarly to the "sudo" command in unix-based operating systems.

Amazon Elastic Block Store, or EBS, is an AWS service that allows virtual block-level storage to be attached to an EC2 instance. These drives can be formatted with any number of different file systems, such as ext3, ext4 (used with Linux), NTFS (used with Windows), and APFS (used with macOS). Depending on the partitioning scheme, EBS drives can be up to 16 tebibytes in size. EBS Volumes come as either solid-state or hard disk storage, with SSDs coming in high-performance IOPS and general-purpose GP variants, and HDDs coming in throughput-optimized (ST) and cold low-cost (SC) variants. EBS volumes are set up in a way that ensures redundancy, meaning that component failure in AWS data centers doesn't result in data loss for the customer.

A relational database is a type of database that stores information in terms of keys and values. A value is a specific data point that can be accessed by referencing its corresponding key. Relational databases can be divided further into any number of different tables. Amazon Relational Database Service, or RDS, is an AWS service that allows relational databases to be created and managed in the AWS cloud. RDS supports several database types, such as MySQL, Oracle Database, MariaDB, PostgreSQL, and Microsoft SQL Server. Amazon also offers their own database type, Aurora, which is compatible with MySQL and optimized for performance and availability. RDS databases can also be deployed across multiple availability zones, which can optionally create multiple instances of an RDS database in different locations.

AWS Elastic Load balancing, or ELB, is an AWS service that automatically balances traffic across multiple devices in the AWS cloud. It is often used in conjunction with EC2 instances. This service creates more consistency in how AWS resources are distributed, which ensures a more stable experience for end users.

AWS Auto Scaling is an AWS service that allows applications to automatically be created or deleted based on a variety of targets, such as CPU utilization or bandwidth. This service facilitates scalability of cloud computing services and adapts AWS

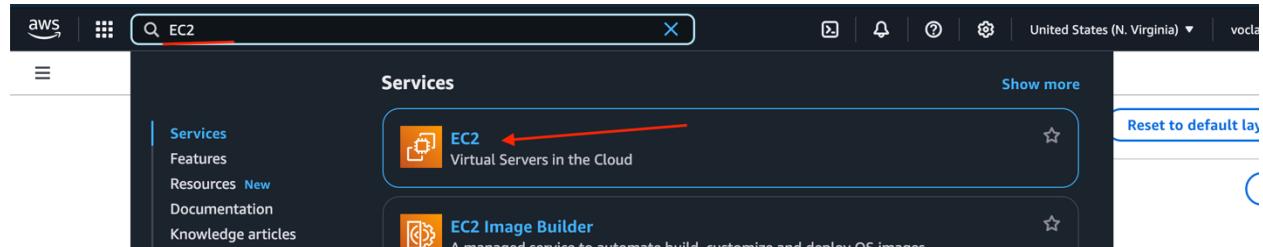
resources to better fit the needs of customers at any given time. This service is also economical for AWS users as it allows them to pay only for resources required for any given moment in time. Auto Scaling can automatically create and delete resources, EC2 instances, DynamoDB databases, and Aurora RDS databases.

## Lab Summary

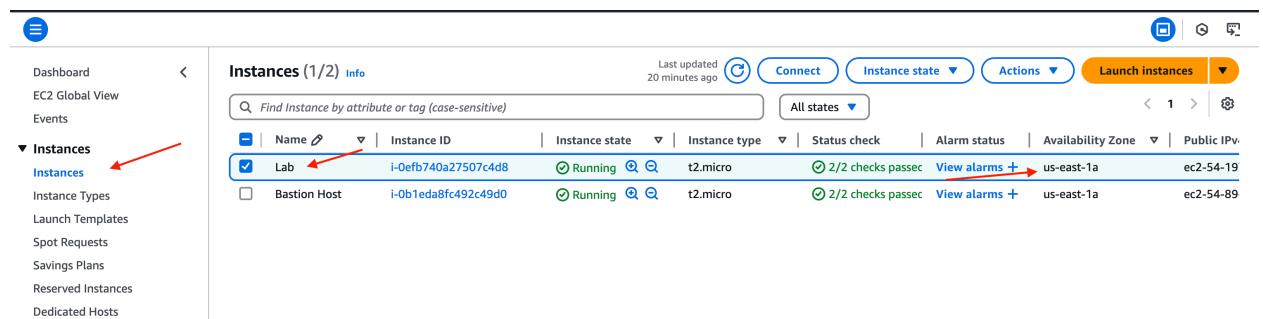
This write-up covers three different AWS labs. The first lab involves creating an EBS volume, attaching it to an EC2 instance, instantiating a new file system on the volume, then creating and restoring a snapshot of the volume. The second lab involves building and launching an RDS address book database, connecting it to a pre-existing web server, then manipulating the database with a web server GUI. The third lab involves creating a load balancer and auto scaling group based on an EC2 instance AMI, then testing the auto scaling feature by simulating excess CPU usage.

## Lab Commands (EBS)

From the AWS search bar, type in and launch “EC2”.



From the Instances tab, make sure that the EC2 instance named “Lab” has been created. Make sure to write down the EC2 instance’s availability zone, which is “us-east-1a” in this case.



Go to the “Volumes” section and click “Create Volume”.

Volumes (2) Info

<input type="checkbox"/>	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Created
<input type="checkbox"/>	-	vol-09102cbfa618ed794	gp3	8 GiB	3000	125	snap-07c32f7...	2025/01/14 15:28 GMT-8
<input type="checkbox"/>	-	vol-0467495f93c918dc4	gp3	9 GiB	3000	125	snap-07c32f7...	2025/01/14 15:28 GMT-8

Fault tolerance for all volumes in this Region

**Snapshot summary**

Recently backed up volumes / Total # volumes **0 / 2**

Last updated on Tue, Jan 14, 2025, 04:18:36 PM (GMT-08:00)

Data Lifecycle Manager default policy for EBS Snapshots status  
No default policy set up | Create policy

Set the volume type to “gp2”, the size to 1 gigabyte, and the availability zone to the same zone as the Lab instance.

**Volume settings**

Volume type Info  
**General Purpose SSD (gp2)**

Size (GiB) Info  
**1**

IOPS Info  
**100 / 3000**  
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

Throughput (MiB/s) Info  
Not applicable

Availability Zone Info  
**us-east-1a**

Snapshot ID - optional Info  
Don't create volume from a snapshot

Encryption Info  
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.  
 Encrypt this volume

Under “Tags”, click “Add Tag”.

**Tags - optional** Info

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

**Add tag**

You can add 50 more tags.

Set the key to “Name” and the value to “My Volume”.

**Tags - optional** [Info](#)

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/> <a href="#">X</a>	<input type="text" value="My Volume"/> <a href="#">X</a>
<a href="#">Remove</a>	
<a href="#">Add tags</a>	

Click “Create Volume”.

**Snapshot summary** [Info](#)

⌚ Click refresh to view backup information  
The volume type that you select and the tags that you assign determine whether the volume will be backed up by any Data Lifecycle Manager policies.

[Cancel](#) [Create volume](#)

You should now be redirected to the Volumes page. Click the checkbox next to My Volume, then under Actions, click Attach Volume.

The screenshot shows the AWS Volumes page with three volumes listed. The second volume, "My Volume" (Volume ID: vol-04310c6ab006881e7), has a checked checkbox next to its name. A red arrow points from this checkbox to the "Actions" button in the top right corner of the volume card. A second red arrow points from the "Actions" button to the "Attach volume" option in the dropdown menu that appears when it is clicked. The "Attach volume" option is highlighted with a blue box.

Set the instance to the Lab instance and the device name to /dev/sdf, then click Attach volume.

**Basic details**

**Volume ID**

**Availability Zone**  
us-east-1a

**Instance** [Info](#)

Only instances in the same Availability Zone as the selected volume are displayed.

**Device name** [Info](#)

Recommended device names for Linux: /dev/xvda for root volume. /dev/sd[f-p] for data volumes.

ⓘ Newer Linux kernels may rename your devices to /dev/xvdf through /dev/xvdp internally, even when the device name entered here (and shown in the details) is /dev/sdf through /dev/sdp.

[Cancel](#) [Attach volume](#)

Go to the “Instances” section, click the checkbox next to “Lab”, and click “Connect”.

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with 'Instances' selected. The main area displays 'Instances (1/2) Info' with two entries:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
Lab	i-0efb740a27507c4d8	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	us-east-1a	ec2-54-19
Bastion Host	i-0b1eda8fc492c49d0	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a>	us-east-1a	ec2-54-89

Select “EC2 instance connect”, select “Public IPv4 address”, then click “Connect”.

The screenshot shows the EC2 Instance Connect configuration page. It has tabs for 'EC2 Instance Connect', 'Session Manager', 'SSH client', and 'EC2 serial console'. Under 'Connection Type', the 'Connect using EC2 Instance Connect' option is selected. Below it, the 'Public IPv4 address' option is selected, showing the IP address 54.197.37.249. The 'Username' field is set to 'ec2-user'. A note at the bottom states: 'Note: In most cases, the default username, ec2-user, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.' A red arrow points to the 'Connect' button at the bottom right.

Run the command `df -h` to list the mounted volumes; you should see output like this:

```

[ec2-user@ip-10-1-11-198 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M    0  4.0M   0% /dev
tmpfs          475M    0  475M   0% /dev/shm
tmpfs          190M  452K 190M   1% /run
/dev/xvda1      8.0G  1.6G  6.4G  20% /
tmpfs          475M    0  475M   0% /tmp
/dev/xvda128    10M  1.3M  8.7M  13% /boot/efi
tmpfs          95M    0   95M   0% /run/user/1000

```

Run the command `sudo mkfs -t ext3 /dev/sdf` to create an ext3 file system on the volume you created.

```
[ec2-user@ip-10-1-11-198 ~]$ sudo mkfs -t ext3 /dev/sdf
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 262144 4k blocks and 65536 inodes
Filesystem UUID: d545580a-928e-4063-ad5d-bda7ee246ba3
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376

Allocating group tables: done
Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done
```

Run the command `sudo mkdir /mnt/data-store` to create a new folder at `/mnt/data-store`.

```
[ec2-user@ip-10-1-11-198 ~]$ sudo mkdir /mnt/data-store
```

Run the command `sudo mount /dev/sdf /mnt/data-store` to mount your volume at the created folder.

```
[ec2-user@ip-10-1-11-198 ~]$ sudo mount /dev/sdf /mnt/data-store
```

Run the command `echo "/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab` to add this mount binding to `/etc/fstab`, a file that automatically mounts volumes at startup.

```
[ec2-user@ip-10-1-11-198 ~]$ echo "/dev/sdf /mnt/data-store ext3 defaults,noatime 1 2" | sudo tee -a /etc/fstab
```

Run the command `cat /etc/fstab` to confirm that the line was added.

```
[ec2-user@ip-10-1-11-198 ~]$ cat /etc/fstab
#
UUID=73e034f4-2887-4ec9-8b40-0d35c0091a37   /
          xfs     defaults,noatime 1 1
UUID=9F37-3C35   /boot/efi   vfat    defaults,noatime,uid=0,gid=0,umask=0077,shortname=winnt,x-systemd.automount 0 2
/dev/sdf   /mnt/data-store ext3 defaults,noatime 1 2
```

Run the command `sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"` to create a file with the text “some text has been written” at the specified location.

```
[ec2-user@ip-10-1-11-50 ~]$ sudo sh -c "echo some text has been written > /mnt/data-store/file.txt"
```

Run the command `cat /mnt/data-store/file.txt` to confirm that the file was written.

```
[ec2-user@ip-10-1-11-50 ~]$ cat /mnt/data-store/file.txt
some text has been written
```

Go back to the main AWS console tab. Under Volumes, check My Volume, then click Actions > Create Snapshot.

The screenshot shows the AWS Lambda console with a success message: "Successfully attached volume vol-0918321c092d50b99 to instance i-0e35f74c96c3fce5". On the left, the navigation pane includes sections for Instances, Images, and Elastic Block Store (with Volumes selected). The main area displays a table of volumes, with one row highlighted. A red arrow points to the "Actions" menu icon for the selected volume.

Under Tags, click Add Tag, set the key to Name, set the value to My Snapshot, then click Create Snapshot.

The screenshot shows the "Create snapshot" dialog. It includes fields for "Source volume" (set to "vol-0918321c092d50b99 (My Volume)"), "Availability Zone" (set to "us-east-1a"), "Snapshot details" (with a description placeholder and encryption info), and a "Tags" section. The "Tags" section has an "Add tag" button highlighted with a red arrow. A large red arrow points to the "Create snapshot" button at the bottom right.

Switch back to the console and run the command `sudo rm /mnt/data-store/file.txt` to remove the file you created earlier.

```
[ec2-user@ip-10-1-11-50 ~]$ sudo rm /mnt/data-store/file.txt
```

Run the command `ls /mnt/data-store` to confirm that the file has been deleted.

```
[ec2-user@ip-10-1-11-50 ~]$ ls /mnt/data-store
lost+found      no mention of file.txt
```

Back in the AWS console, go to Snapshots > Check My Snapshot > Actions > Create volume from snapshot.

Snapshots (1 / 1) Info

Name	Snapshot ID	Volume size	Description	Storage tier	Snapshot status	Started	Progress	Encrypted
<input checked="" type="checkbox"/> My Snapshot	snap-08d374bc52f3d4244	1 GiB	-	Standard	Completed	2025/01/16 14:09 GMT-8	100%	No

**Actions**

- Create volume from snapshot (highlighted)
- Create image from snapshot
- Copy snapshot
- Launch copy duration calculator
- Delete snapshot
- Manage tags
- Snapshot settings
- Archiving

**Snapshot ID: snap-08d374bc52f3d4244 (My Snapshot)**

**Details** Snapshot settings Storage tier Tags

Snapshot ID <input checked="" type="checkbox"/> snap-08d374bc52f3d4244 (My Snapshot)	Progress 100%	Snapshot status Completed	Owner 652635526343
Started <input checked="" type="checkbox"/> Thu Jan 16 2025 14:09:20 GMT-0800 (Pacific Standard Time)	Product codes	Fast snapshot restore	Description
Source volume <input checked="" type="checkbox"/> Volume ID vol-0918321d092d50b99	Volume size <input checked="" type="checkbox"/> 1 GiB	KMS key alias	KMS key ARN
Encryption Not encrypted	KMS key ID		

Set the volume type to gp2 (everything else should be correct by default), then click Add Tag, set the key to Name, set the value to Restored Volume, then click Create Volume.

**Volume settings**

**Snapshot ID**  
 snap-08d374bc52f3d4244 (My Snapshot)

**Volume type** [Info](#)  
 General Purpose SSD (gp2)

**Size (GiB)** [Info](#)  
  
Min: 1 GiB, Max: 16384 GiB.

**IOPS** [Info](#)  
100 / 3000  
Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS.

**Throughput (MiB/s)** [Info](#)  
Not applicable

**Availability Zone** [Info](#)  
 us-east-1a

**Fast snapshot restore** [Info](#)  
Not enabled for selected snapshot

**Encryption**  
Use Amazon EBS encryption as an encryption solution for your EBS resources associated with your EC2 instances.  
 Encrypt this volume

**Tags - optional** [Info](#)  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="Restored Volume"/>

**Add tag** (highlighted with a red arrow)

You can add 49 more tags.

**Snapshot summary**

[Click refresh to view backup information](#)  
The volume type that you select and the tags that you assign determine whether the volume will be backed up by any Data Lifecycle Manager policies.

**Create volume** (highlighted with a red arrow)

Under Volumes, check Restored Volume, then click Actions > Attach Volume

Volumes (1/4) Info

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Created	Availability Zone	Volume state
-	vol-0b7f54f4c6fb73819a	gp3	9 GiB	3000	125	snap-055e2a2...	2025/01/16 13:55 GMT-8	us-east-1a	<span style="color: #0072bc;">In-use</span>
Restored Volu...	vol-05032b41f7ecaa218	gp2	1 GiB	100	-	snap-06d574b...	2025/01/16 14:19 GMT-8	us-east-1a	<span style="color: #0072bc;">In-use</span>
-	vol-0f38dbd354483571	gp3	9 GiB	3000	125	snap-055e2a2...	2025/01/16 13:55 GMT-8	us-east-1a	<span style="color: #0072bc;">In-use</span>
My Volume	vol-0918321c092d50b99	gp2	1 GiB	100	-	-	2025/01/16 13:56 GMT-8	us-east-1a	<span style="color: #0072bc;">In-use</span>

Volume ID: vol-05032b41f7ecaa218 (Restored Volume)

**Details** Status checks Monitoring Tags

Volume ID <input type="text" value="vol-05032b41f7ecaa218 (Restored Volume)"/>	Size <input type="text" value="1 GiB"/>	Type <input type="text" value="gp2"/>	Volume status <span style="color: #0072bc;">Okay</span>
Volume state <input type="text" value="Available"/>	IOPS <input type="text" value="100"/>	Throughput	Multi-Attach enabled <input type="text" value="No"/>
Fast snapshot restored <input type="text" value="No"/>	Availability Zone <input type="text" value="us-east-1a"/>	Outposts ARN	Operator
Attached resources	Created <input type="text" value="Thu Jan 16 2025 14:19:47 GMT-0800 (Pacific Standard Time)"/>	Managed	

Set the instance to Lab, the device name to /dev/sdg, then click Attach Volume.

**Basic details**

Volume ID

Availability Zone  
us-east-1a

Instance Info

Device name Info

Attach volume

Run the command `sudo mkdir /mnt/data-store2` to make a new folder for the restored drive.

```
[ec2-user@ip-10-1-11-50 ~]$ sudo mkdir /mnt/data-store2
```

Run the command `sudo mount /dev/sdg /mnt/data-store2` to mount the restored volume at the specified point.

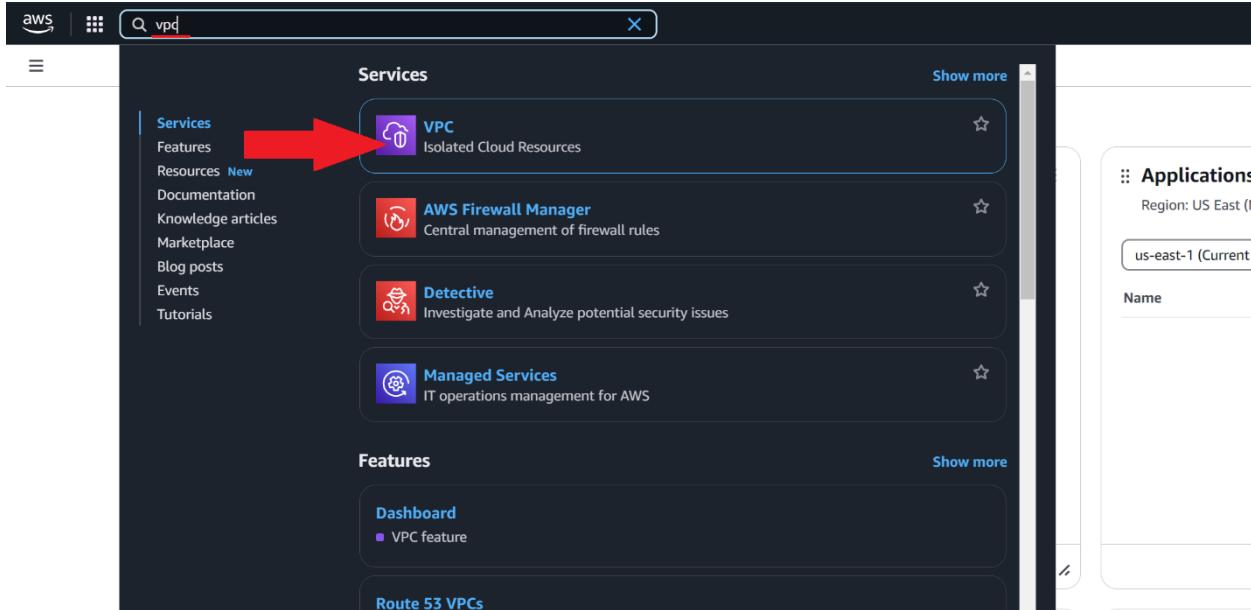
```
[ec2-user@ip-10-1-11-50 ~]$ sudo mount /dev/sdg /mnt/data-store2
```

Run the command `ls /mnt/data-store2/` and ensure that file.txt shows up.

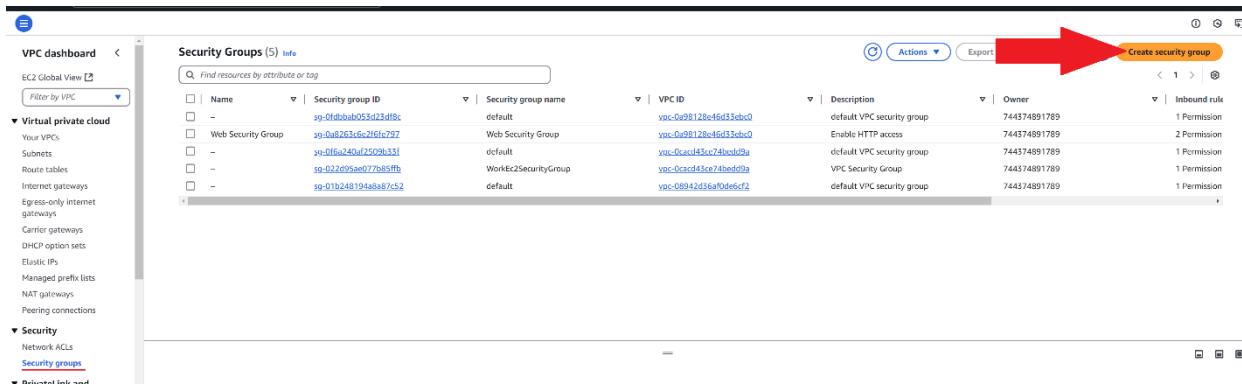
```
[ec2-user@ip-10-1-11-50 ~]$ ls /mnt/data-store2/
file.txt lost+found
```

## Lab Commands (RDS)

From the AWS console search bar, open VPC.



Under Security Groups, click Create Security Group.



Set the name to DB Security Group, the description to Permit access from Web Security Group, and the VPC to Lab VPC. Under Inbound Rules, click Add Rule, set the type to MySQL/Aurora, and set the source to the Web Security Group. Click Create security group.

**Basic details**

Security group name [Info](#)  
DB Security Group  
Name cannot be edited after creation.

Description [Info](#)  
Permit access from Web Security Group

VPC [Info](#)  
vpc-0a98128e46d33ebc0 (Lab VPC)

**Inbound rules** [Info](#)

Type	Protocol	Port range	Source	Description - optional
MySQL/Aurora	TCP	3306	Custom	sg-0a8263c6e2f6fe79 X sg-0a8263c6e2f6fe797 X Web Security Group

[Add rule](#) ←

Go to RDS from the search bar.

aws | [VPC](#) >

**VPC dashboard**

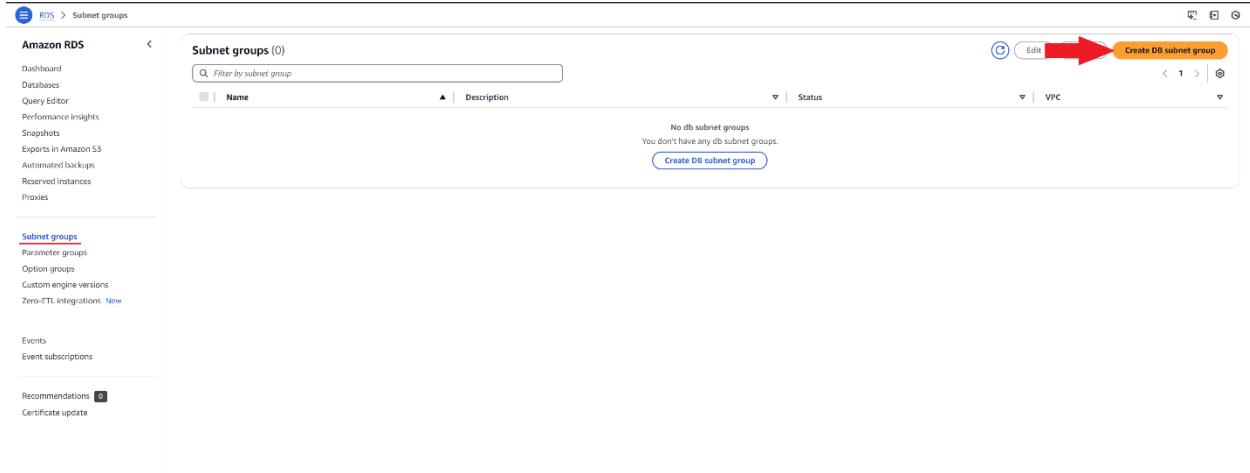
- Services
- Features
- Resources [New](#)
- Documentation
- Knowledge articles
- Marketplace
- Blog posts
- Events
- Tutorials

**Services**

- RDS ← Managed Relational Database Service
- Database Migration Service Managed Database Migration Service
- Kinesis Work with Real-Time Streaming Data

Show more

Go to Subnet groups > Create DB Subnet Group.



Set the name to DB-Subnet-Group, the description to DB Subnet Group, and the VPC to Lab VPC. Set the availability zones to us-east-1a and us-east-1b, and set the subnets to Private Subnet 1 and Private Subnet 2. Click Create.

### Subnet group details

<b>Name</b>	<input type="text" value="DB-Subnet-Group"/>
You won't be able to modify the name after your subnet group has been created.	
<b>Description</b>	<input type="text" value="DB Subnet Group"/>
<b>VPC</b>	
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.	
<input type="text" value="Lab VPC (vpc-0a98128e46d55ebc0)"/> 4 Subnets, 2 Availability Zones	

### Add subnets

<b>Availability Zones</b>	Choose the Availability Zones that include the subnets you want to add.												
<input type="text" value="Choose an availability zone"/> us-east-1a X us-east-1b X													
<b>Subnets</b>	Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.												
<input type="text" value="Select subnets"/> <div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">           Private Subnet 1            Subnet ID: subnet-0b6d2f04e4b4ef8b2 CIDR: 10.0.1.0/24         </div>													
<small>(i) For Multi-AZ DB clusters, you must select 3 subnets in 3 different Availability Zones.</small>													
<b>Subnets selected (2)</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Availability zone</th> <th>Subnet name</th> <th>Subnet ID</th> <th>CIDR block</th> </tr> </thead> <tbody> <tr> <td>us-east-1b</td> <td>Private Subnet 2</td> <td>subnet-0b6d2f04e4b4ef8b2</td> <td>10.0.3.0/24</td> </tr> <tr> <td>us-east-1a</td> <td>Private Subnet 1</td> <td>subnet-089f0ad02ef871ca8</td> <td>10.0.1.0/24</td> </tr> </tbody> </table>		Availability zone	Subnet name	Subnet ID	CIDR block	us-east-1b	Private Subnet 2	subnet-0b6d2f04e4b4ef8b2	10.0.3.0/24	us-east-1a	Private Subnet 1	subnet-089f0ad02ef871ca8	10.0.1.0/24
Availability zone	Subnet name	Subnet ID	CIDR block										
us-east-1b	Private Subnet 2	subnet-0b6d2f04e4b4ef8b2	10.0.3.0/24										
us-east-1a	Private Subnet 1	subnet-089f0ad02ef871ca8	10.0.1.0/24										

➡ **Create**

Go to Databases > Create Database.

The screenshot shows the Amazon RDS Dashboard. On the left, there's a sidebar with links like Dashboard, Databases (which is selected), Query Editor, Performance Insights, Snapshots, Export to Amazon S3, Automated backups, Reserved instances, and Proxies. Below that are Subnet groups, Parameter groups, Option groups, Custom engine versions, and Zero-ETL Integrations. The main area has a green banner at the top saying 'Successfully created DB-Subnet-Group. View subnet group'. Below it is a table titled 'Databases (0)' with columns for DB identifier, Status, Role, Engine, Region & ... (dropdown), Size, Recommendations, CPU, Current activity, Maintenance, VPC, and Multi-AZ. A red arrow points to the 'Create database' button in the top right corner.

Set the engine type to MySQL.

The screenshot shows the 'Engine options' section. It has four options: 'Aurora (MySQL Compatible)', 'Aurora (PostgreSQL Compatible)', 'MySQL' (which is selected and highlighted with a blue border and a red arrow pointing to it), and 'PostgreSQL'. Each option has a small icon next to it.

Set the template to Dev/Test.

The screenshot shows the 'Templates' section. It has three options: 'Production' (with a note: 'Use defaults for high availability and fast, consistent performance.'), 'Dev/Test' (which is selected and highlighted with a blue border and a red arrow pointing to it), and 'Free tier' (with a note: 'Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS.').

Set the deployment options to Multi-AZ DB instance.

The screenshot shows the 'Availability and durability' section. It has three deployment options: 'Multi-AZ DB Cluster' (with a note: 'Creates a DB cluster with a primary DB instance and two readable standby DB instances, with each DB instance in a different Availability Zone (AZ). Provides high availability, data redundancy and increases capacity to serve read workloads.'), 'Multi-AZ DB instance' (which is selected and highlighted with a blue border and a red arrow pointing to it), and 'Single DB instance' (with a note: 'Creates a single DB instance with no standby DB instances.').

Set the DB instance identifier to lab-db, the master username to main, the credentials management to self-managed, and the master password to lab-password.

**Settings**

**DB instance identifier** [Info](#)  
Type a name for your DB instance. The name must be unique across all DB instances owned by your AWS account in the current AWS Region.  
The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 63 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

**Credentials Settings**

**Master username** [Info](#)  
Type a login ID for the master user of your DB instance.  
To 16 alphanumeric characters. The first character must be a letter.

**Credentials management**  
You can use AWS Secrets Manager or manage your master user credentials.

**Managed in AWS Secrets Manager - most secure**  
RDS generates a password for you and manages it throughout its lifecycle using AWS Secrets Manager.

**Self managed**  
Create your own password or let RDS generate one for you and manage it.

**Auto generate password**  
Amazon RDS can generate a password for you, or you can specify your own password.

**Master password** [Info](#)  
Password strength: **Neutral**  
Minimum constraints: At least 8 printable ASCII characters. Can't contain any of the following symbols: / \ ^ @

**Confirm master password** [Info](#)



Under Instance configuration, set the instance class to Burstable classes, and select db.t3.micro.

**Instance configuration**  
The DB instance configuration options below are limited to those supported by the engine that you selected above.

**DB instance class** [Info](#)  
**Hide filters**

**Show instance classes that support Amazon RDS Optimized Writes** [Info](#)  
Amazon RDS Optimized Writes improves write throughput by up to 2x at no additional cost.

**Include previous generation classes**

Standard classes (includes m classes)  
 Memory optimized classes (includes r and x classes)  
 **Burstable classes (includes t classes)**

**db.t3.micro**  
2 vCPUs 1 GiB RAM Network: Up to 2,085 Mbps



Under storage, set the storage type to General Purpose SSD and the allocated storage to 20 GiB.

**Storage**

**Storage type** [Info](#)  
Provisioned IOPS SSD (io2) storage volumes are now available.  
 **General Purpose SSD (gp3)**  
Performance scales independently from storage

**Allocated storage** [Info](#)  
 GiB  
Minimum: 20 GiB, Maximum: 6,144 GiB

**Provisioned IOPS** [Info](#)  
3000 IOPS

**Storage throughput** [Info](#)  
125 MiBps

**To provision additional IOPS and throughput, increase the allocated storage to 400 GiB or greater.**

**Additional storage configuration**

Under connectivity, set the VPC to Lab VPC and set the existing security groups to DB security group.

**Connectivity [Info](#)**  
**Compute resource**  
 Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.  
 **Don't connect to an EC2 compute resource**  
 Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.  
 **Connect to an EC2 compute resource**  
 Set up a connection to an EC2 compute resource for this database.

**Virtual private cloud (VPC) [Info](#)**  
 Choose the VPC. The VPC defines the virtual networking environment for this DB instance.  
 Lab VPC (vpc-098128e46d35ebc0)  
 4 Subnets, 2 Availability Zones  
 Only VPCs with a corresponding DB subnet group are listed.

**VPC security group (firewall) [Info](#)**  
 Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.  
 **Choose existing**  
 Choose existing VPC security groups  
 **Create new**  
 Create new VPC security group

**Existing VPC security groups**  
 Choose one or more options  
 DB Security Group [X](#)

Under monitoring, disable Enhanced monitoring.

**Monitoring**  
 **Enable Enhanced Monitoring**  
 Enabling Enhanced Monitoring metrics are useful when you want to see how different processes or threads use the CPU.

Under additional configuration, set the initial database name to lab, and disable automated backups and encryption.

**▼ Additional configuration**  
 Database options, encryption turned off, backup turned off, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

**Database options**  
**Initial database name [Info](#)**  
 lab  
 If you do not specify a database name, Amazon RDS does not create a database.

**DB parameter group [Info](#)**  
 default.mysql8.0

**Option group [Info](#)**  
 default:mysql-8.0

**Backup**  
 **Enable automated backups**  
 Creates a point-in-time snapshot of your database.

**Encryption**  
 **Enable encryption**  
 Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console. [Info](#)

Click create database.

You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

**Create database**

Click on lab-db.

	DB identifier	Status	Role	Engine
	<a href="#">lab-db</a>	Creating	Instance	MySQL Co

Wait until the status says Modifying or Available

Scroll down to the Connectivity and security section and copy the Endpoint value.

Connect to the Lab's web server IP, and click on RDS.

Paste the endpoint URL, and enter the database name, username, and password from earlier.

If done correctly, you should see an address book database. Click "Remove" to remove an entry.

## Address Book

Last name	First name	Phone	Email	Admin
Doe	Jane	010-110-1101	janed@someotheraddress.org	<a href="#">Edit</a> <a href="#">Remove</a>
Johnson	Roberto	123-456-7890	robertoj@someaddress.com	<a href="#">Edit</a> <a href="#">Remove</a>

You should see a message saying that the entry has been removed. Next, click the “Edit” button next to the remaining entry.

## Address Book

Entry has been removed

Last name	First name	Phone	Email	Admin
Doe	Jane	010-110-1101	janed@someotheraddress.org	<a href="#">Edit</a> <a href="#">Remove</a>

Change the details of the entry and click “Submit”.

## Address Book

### Edit Contact

Last name:

First name:

Phone:

Email:

Last name	First name	Phone	Email	Admin
Doe	Jane	010-110-1101	janed@someotheraddress.org	<a href="#">Edit</a> <a href="#">Remove</a>

You should see a success message. Click “Add contact” to add a new contact.

## Address Book

Data Updated!

Last name	First name	Phone	Email	Admin
Mason	Jeffrey	010-110-1101	janed@someotheraddress.org	<a href="#">Edit</a> <a href="#">Remove</a>

Add some information for the new contact and click “Submit”.

## Address Book

### Add Contact

Last Name:	Hansen
First Name:	Michael
Phone:	4254561111
Email:	realemail@email.com
<a href="#">Submit</a>	

Last name	First name	Phone	Email	Admin
Mason	Jeffrey	010-110-1101	janed@someotheraddress.org	<a href="#">Edit</a> <a href="#">Remove</a>

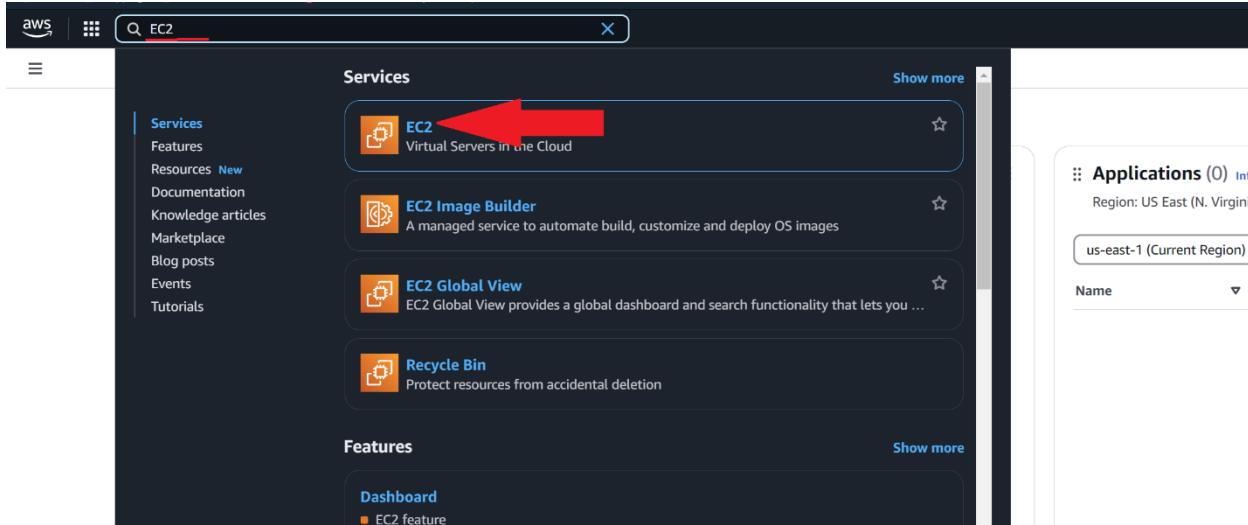
You should see both your newly created and newly modified entry in the address book.

## Address Book

Last name	First name	Phone	Email	Admin
Hansen	Michael	4254561111	realemail@email.com	<a href="#">Edit</a> <a href="#">Remove</a>
Mason	Jeffrey	010-110-1101	janed@someotheraddress.org	<a href="#">Edit</a> <a href="#">Remove</a>

## Lab Commands (Auto Scaling)

Go to the AWS management console and select “EC2”.



Go to Instances, ensure that Web Server 1's status is 2/2 checks passed, then click on the checkbox next to the web server and click Actions > Image and Templates > Create Image.

The screenshot shows the AWS Instances page. On the left, there's a sidebar with 'Instances' selected. The main table lists two instances: 'Bastion Host' and 'Web Server 1'. A red arrow points to the checkbox next to 'Web Server 1'. Another red arrow points to the 'Actions' dropdown menu, which is open and shows options like 'Create image', 'Create template from instance', and 'Launch more like this'. The 'Create image' option is highlighted.

Set the image name to WebServerAMI and the image description to Lab AMI for Web Server, then click Create image.

The screenshot shows the 'Create Image' configuration dialog. It includes fields for 'Instance ID' (selected), 'Image name' (set to 'WebServerAMI'), 'Image description - optional' (set to 'Lab AMI for Web Server'), and a 'Reboot instance' checkbox (unchecked). Under 'Instance volumes', there's a table with one volume row. At the bottom, there's a note about snapshot creation and a 'Create image' button highlighted with a red arrow.

Go to Target Groups > Create target group.

The screenshot shows the AWS EC2 Target Groups page. On the left, there's a navigation sidebar with various EC2-related options like Dashboard, Instances, Images, and Network & Security. Under Load Balancing, 'Target Groups' is selected. The main area is titled 'Target groups info' and shows a table with columns for Name, ARN, Port, Protocol, Target type, Load balancer, and VPC ID. A message at the top says 'No target groups' and 'You don't have any target groups in us-east-1'. Below the table is a blue 'Create target group' button. A large red arrow is overlaid on the page, pointing to the 'Create target group' button.

Set the target type to Instances and the target group name to LabGroup.

**Basic configuration**  
Settings in this section can't be changed after the target group is created.

**Choose a target type**

Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

**Target group name**

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Set the VPC to Lab VPC, then click Next.

VPC  
Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.  
 Lab VPC  
vpc-0000000000000000  
IPv4 VPC CIDR: 10.0.0.0/16

Protocol  
 HTTP1  
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.  
 HTTP2  
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.  
 gRPC  
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks  
The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol  
 HTTP

Health check path  
Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.  
 /  
Up to 1024 characters allowed.

Advanced health check settings

Attributes  
Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

Tags - optional  
Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

**Next Step**

Click “Create target group”.

Review targets

Targets (0)

Filter targets  Show only pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
No instances added yet Specify instances above, or leave the group empty if you prefer to add targets later.								

0 pending

**Create target group**

Go to Load Balancers > Create load balancer.

EC2 > Load balancers

Load balancers

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Filter load balancers

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
No load balancers You don't have any load balancers in us-east-1						

**Create load balancer**

0 load balancers selected

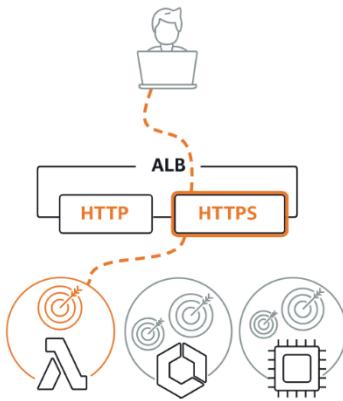
Select a load balancer above.

Under Application Load Balancer, click Create.

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

## Load balancer types

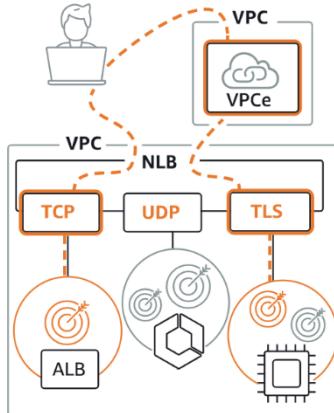
### Application Load Balancer [Info](#)



Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

[Create](#)

### Network Load Balancer [Info](#)



Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

[Create](#)

### Gateway Load Balancer [Info](#)



Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

[Create](#)

Under Basic configuration, set the load balancer name to LabELB.

#### Basic configuration

##### Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

LabELB

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Under Network mapping, set the VPC to Lab VPC, check both availability zones, and set them to Public Subnets 1 and 2 respectively.

#### Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

##### VPC [Info](#)

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#). For a new VPC, create a VPC.

Lab VPC  
vpc-008b28f7a7c4a4266  
IPv4 CIDR: 10.0.0.0/16



##### Mappings [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

##### Availability Zones

us-east-1a (use1-az2)

Subnet

subnet-0168f37adddecfa2b0  
IPv4 subnet CIDR: 10.0.0.0/24

Public Subnet 1

IPV4 address  
Assigned by AWS

us-east-1b (use1-az4)

Subnet

subnet-09ee7b908570d1175  
IPv4 subnet CIDR: 10.0.2.0/24

Public Subnet 2

IPV4 address  
Assigned by AWS

Under Security groups, select Web Security Group and unselect default.

The screenshot shows the AWS Security Groups page. At the top, it says "Select up to 5 security groups". Below is a search bar with a magnifying glass icon. A list of security groups is shown:
 

- ~~Default~~ sg-00fbf0c02422c58c9 VPC: vpc-008b28f7a7c4a4266
- DB Security Group sg-0464bf7e75572f3ec VPC: vpc-008b28f7a7c4a4266
- Web Security Group sg-06dc1ae2846dc7037 VPC: vpc-008b28f7a7c4a4266
- c138865a355074919004965t1w110584150310-BastionSecurityGroup-nEzkE28fhoGv sg-0888aad175bb951f5 VPC: vpc-008b28f7a7c4a4266

 A blue box highlights the "Web Security Group" entry. A red arrow points to the "Default" checkbox in the first entry, indicating it should be unselected.

Under Listeners and routing, set the default action to LabGroup

The screenshot shows the "Listeners and routing" section. It lists a single listener "Listener HTTP:80" with the following settings:
 

- Protocol: HTTP, Port: 80
- Default action: Forward to **LabGroup** (HTTP)

 A red arrow points to the "LabGroup" target group name, indicating it should be selected.

Click Create load balancer.

The screenshot shows the "Creation workflow and status" section. It includes a "Server-side tasks and status" box which states: "After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring." To the right, there is a large orange button labeled "Create load balancer" with a red arrow pointing towards it.

Go to Launch Templates > Create launch template.

The screenshot shows the AWS EC2 Launch Templates page. On the left, there's a navigation sidebar with various EC2 services like Instances, Images, and Auto Scaling. The main content area is titled 'EC2 launch templates' with the subtitle 'Streamline, simplify and standardize instance launches'. Below this, there's a section for 'Benefits and features' with three items: 'Streamline provisioning', 'Simplify permissions', and 'Governance'. To the right, there's a callout box with a 'New launch template' button and a 'Create launch template' button, which is highlighted with a red arrow.

Set the launch template name to LabConfig and click the checkbox under Auto Scaling Guidance.

This screenshot shows the 'Launch template name and description' form. It includes fields for 'Launch template name - required' (containing 'LabConfig'), 'Template version description' (containing 'A prod webserver for MyApp'), and 'Auto Scaling guidance' (with a checked checkbox). There are also sections for 'Template tags' and 'Source template'.

Under the Application and OS images section, click My AMIs and select the AMI you created earlier.

This screenshot shows the 'Application and OS Images (Amazon Machine Image) - required' section. It includes a search bar, tabs for 'Recents', 'My AMIs' (which is selected and highlighted with a red arrow), and 'Quick Start'. Below these are filters for 'Owned by me' and 'Shared with me'. On the right, there's a 'Browse more AMIs' section and a table for 'Amazon Machine Image (AMI)' showing one entry: 'WebServerAMI' with details like 'ami-0ee2c6c5a33359823', 'Virtualization: hvm', 'ENAv2 enabled: true', 'Root device type: ebs', and 'Boot mode: uefi-preferred'.

Set the instance type to t2.micro, the Key pair name to vockey, the Firewall (security groups) section to Select existing security group, and the Security groups dropdown to Web Security Group.

The screenshot shows the AWS CloudFormation Create New Stack wizard at Step 3: Set instance type, key pair, and network settings. The instance type is set to t2.micro, which is described as having 1 vCPU, 1 GiB Memory, and being part of the t2 family. It is marked as 'Free tier eligible'. The key pair is set to 'vokey'. In the network settings, the subnet is set to 'Don't include in launch template'. The firewall (security groups) section is set to 'Select existing security group', and the chosen group is 'Web Security Group sg-06dc1ae2846dc7037'. Advanced details are collapsed, showing an option to enable Detailed CloudWatch monitoring.

Under Advanced details, enable Detailed CloudWatch monitoring.

▼ Advanced details [Info](#)

IAM instance profile | [Info](#)

Don't include in launch template C G

Hostname type | [Info](#)

Don't include in launch template ▼

DNS Hostname | [Info](#)

Enable resource-based IPv4 (A record) DNS requests  
 Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery | [Info](#)

Don't include in launch template ▼

Shutdown behavior | [Info](#)

Don't include in launch template ▼

Not applicable for EC2 Auto Scaling

Stop - Hibernate behavior | [Info](#)

Don't include in launch template ▼

Not applicable for Amazon EC2 Auto Scaling.

Termination protection | [Info](#)

Don't include in launch template ▼

Stop protection | [Info](#)

Don't include in launch template ▼

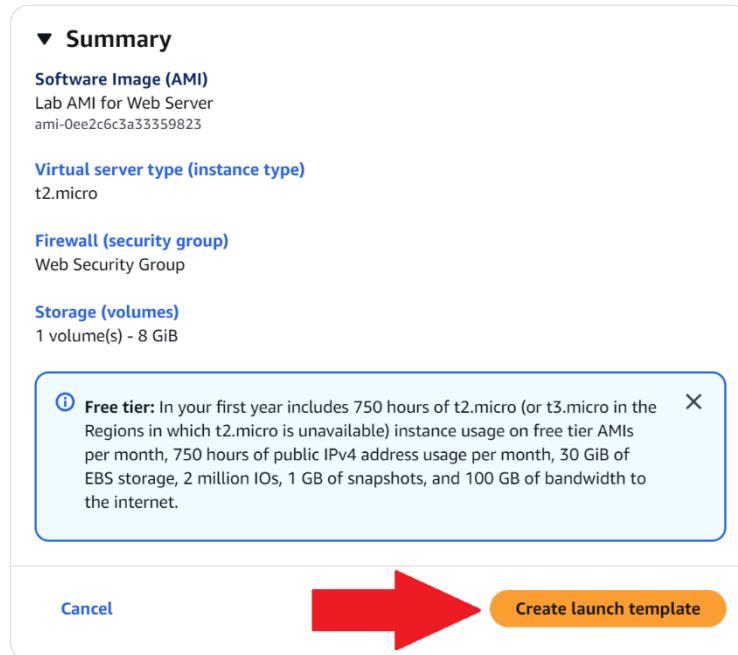
Detailed CloudWatch monitoring | [Info](#)

Enable ▼

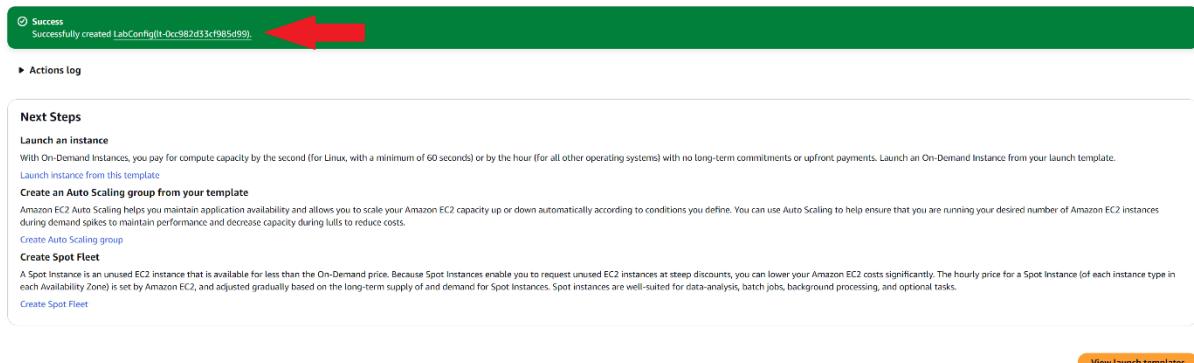
Additional charges apply

Elastic GPU | [Info](#)

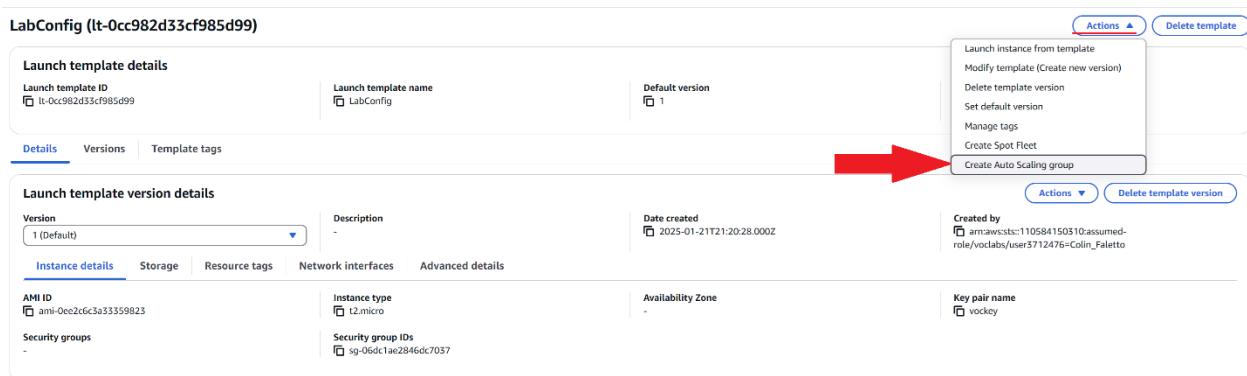
Under Summary, click Create launch template.



Click the hyperlink in the success dialog.



Click Actions > Create auto scaling group.



Set the name to Lab Auto Scaling Group, ensure that the Launch template is set to LabConfig, and click Next.

**Name**

**Auto Scaling group name**  
Enter a name to identify the group.  
Lab Auto Scaling Group

Must be unique to this account in the current Region and no more than 255 characters.

**Launch template** [Info](#)

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

**Launch template**  
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.  
LabConfig [C](#)

Create a launch template [C](#)

**Version**  
Default (1) [C](#)

Create a launch template version [C](#)

<b>Description</b> -	<b>Launch template</b> <u>LabConfig</u> <a href="#">C</a> lt-0cc982d33cf985d99	<b>Instance type</b> t2.micro
<b>AMI ID</b> ami-0ee2c6c3a33359823	<b>Security groups</b> -	<b>Request Spot Instances</b> No
<b>Key pair name</b> vockey	<b>Security group IDs</b> <u>sg-06dc1ae2846dc7037</u> <a href="#">C</a>	

**Additional details**

<b>Storage (volumes)</b> -	<b>Date created</b> Tue Jan 21 2025 13:20:28 GMT-0800 (Pacific Standard Time)
-------------------------------	--

Set the VPC to Lab VPC, select both private subnets under Availability Zones and subnets, then click Next.

**Network** [Info](#)

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

**VPC**  
Choose the VPC that defines the virtual network for your Auto Scaling group.  
vpc-008b28f7a7c4a4266 (Lab VPC) [C](#)  
10.0.0.0/16

Create a VPC [C](#)

**Availability Zones and subnets**  
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets [C](#)

us-east-1a | subnet-0cf4fa3635252d474 (Private Subnet 1) [X](#)  
10.0.1.0/24

us-east-1b | subnet-00857cd0f2678a98f (Private Subnet 2) [X](#)  
10.0.3.0/24

Create a subnet [C](#)

**Availability Zone distribution - new**  
Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy.

**Balanced best effort**  
If launches fail in one Availability Zone, Auto Scaling will attempt to launch in another healthy Availability Zone.

**Balanced only**  
If launches fail in one Availability Zone, Auto Scaling will continue to attempt to launch in the unhealthy Availability Zone to preserve balanced distribution.

[Cancel](#) [Skip to review](#) [Next](#)

Under load balancing, select attach to an existing load balancer, and under existing load balancer target groups, select LabGroup

**Load balancing** Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer  
Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer  
Choose from your existing load balancers.

Attach to a new load balancer  
Quickly create a basic load balancer to attach to your Auto Scaling group.

**Attach to an existing load balancer**

Select the load balancers that you want to attach to your Auto Scaling group.

Choose from your load balancer target groups  
This option allows you to attach Application, Network, or Gateway Load Balancers.

Choose from Classic Load Balancers

**Existing load balancer target groups**

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups ▼

LabGroup | HTTP X

Application Load Balancer: LabELB

Click Next.

**Health checks**

Health checks increase availability by replacing unhealthy instances. When you use multiple health checks, all are evaluated, and if at least one fails, instance replacement occurs.

**EC2 health checks**

Always enabled

**Additional health check types - optional** Info

Turn on Elastic Load Balancing health checks Recommended  
Elastic Load Balancing monitors whether instances are available to handle requests. When it reports an unhealthy instance, EC2 Auto Scaling can replace it on its next periodic check.

Turn on VPC Lattice health checks  
VPC Lattice can monitor whether instances are available to handle requests. If it considers a target as failed a health check, EC2 Auto Scaling replaces it after its next periodic check.

Turn on Amazon EBS health checks  
EBS monitors whether an instance's root volume or attached volume stalls. When it reports an unhealthy volume, EC2 Auto Scaling can replace the instance on its next periodic health check.

**Health check grace period** Info

This time period delays the first health check until your instances finish initializing. It doesn't prevent an instance from terminating when placed into a non-running state.

300 seconds

Cancel Skip to review Next

Set the Desired capacity to 2, the minimum capacity to 2, and the maximum capacity to 6. Set the automatic scaling policy to target tracking scaling policy, set the name to LabScalingPolicy, the metric type to Average CPU utilization, and the target value to 60. This setting will automatically scale the number of EC2 instances to maintain an average of 60% CPU utilization across instances.

**Group size** [Info](#)

Set the initial size of the Auto Scaling group. After creating the group, you can change its size to meet demand, either manually or by using automatic scaling.

**Desired capacity type**

Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances) ▾

**Desired capacity**

Specify your group size.

**Scaling** [Info](#)

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

**Scaling limits**

Set limits on how much your desired capacity can be increased or decreased.

**Min desired capacity**  Equal or less than desired capacity

**Max desired capacity**  Equal or greater than desired capacity

**Automatic scaling - optional**

Choose whether to use a target tracking policy [Info](#)

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

No scaling policies  
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

Target tracking scaling policy   
Choose a CloudWatch metric and target value and let the scaling policy adjust the desired capacity in proportion to the metric's value.

**Scaling policy name**

**Metric type** [Info](#)

Monitored metric that determines if resource utilization is too low or high. If using EC2 metrics, consider enabling detailed monitoring for better scaling performance.

Average CPU utilization ▾

**Target value**

Under Additional settings, click Enable group metrics collection within CloudWatch, then click Next.

**Additional settings**

**Instance scale-in protection**

If protect from scale in is enabled, newly launched instances will be protected from scale in by default.

Enable instance scale-in protection

**Monitoring** [Info](#)

Enable group metrics collection within CloudWatch 

**Default instance warmup** [Info](#)

The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

Enable default instance warmup

Cancel [Skip to review](#)  Next

Under Add notifications, click Next.

**Add notifications - optional** [Info](#)

Send notifications to SNS topics whenever Amazon EC2 Auto Scaling launches or terminates the EC2 instances in your Auto Scaling group.

[Add notification](#)

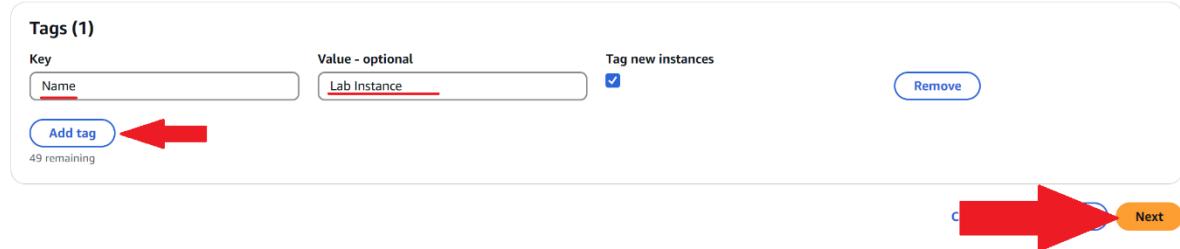
Cancel [Skip to review](#)  Next

Under Add tags, click Add tag, set the key to Name, an

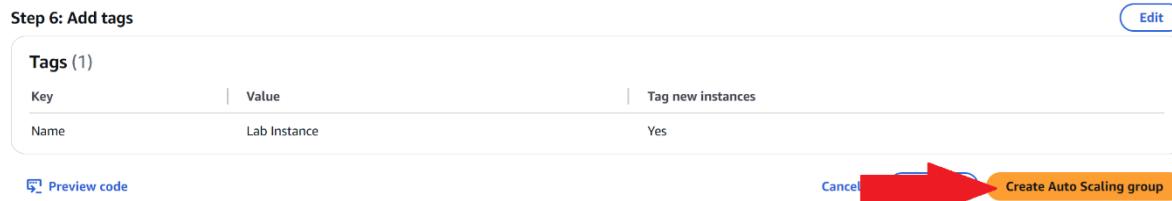
### Add tags - optional Info

Add tags to help you search, filter, and track your Auto Scaling group across AWS. You can also choose to automatically add these tags to instances when they are launched.

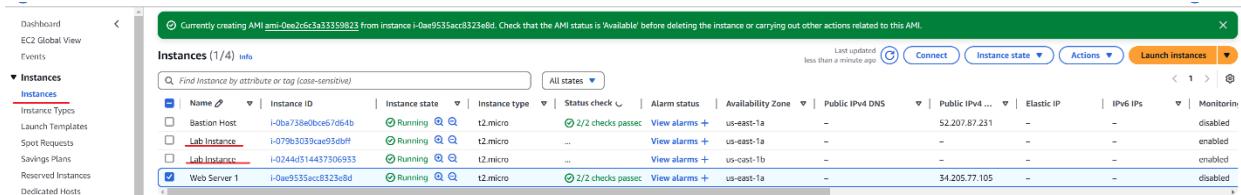
ⓘ You can optionally choose to add tags to instances (and their attached EBS volumes) by specifying tags in your launch template. We recommend caution, however, because the tag values for instances from your launch template will be overridden if there are any duplicate keys specified for the Auto Scaling group.



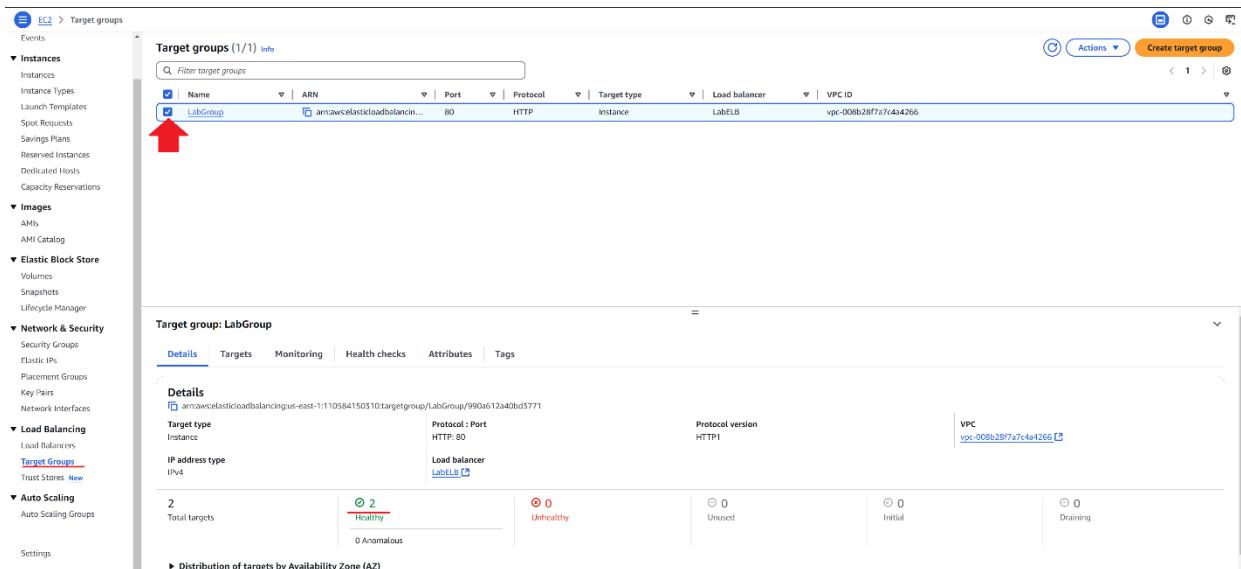
Click Create Auto Scaling Group.



Click Instances and ensure that two copies of Lab Instance have been launched.



Go to Target Groups, check LabGroup, and ensure that both targets are healthy.



Go to Load balancers, select LabELB, then copy the DNS name.

**Load balancers (1/1)**

Name	DNS name	Status	VPC ID	Availability Zones	Type	Date created
LabELB	LabELB-1904038358.us... (Active) vpc-008b28f7a7cfa4266 2 Availability Zones application January 21, 2025, 13:10 (UTC-08:00)					

**Load balancer: LabELB**

**Details**

Load balancer type: Application	Status: Active	VPC: vpc-008b28f7a7cfa4266	Load balancer IP address type: IPv4
Scheme: Internet-facing	Hosted zone: Z55SXDOOTRQ7XK	Availability Zones: subnet-0168f737addeefax2b0 (us-east-1a (use1-az2)) subnet-09ec07908570d1175 (us-east-1b (use1-az4))	Date created: January 21, 2025, 13:10 (UTC-08:00)
Load balancer ARN: arn:aws:elasticloadbalancing:us-east-1:110584150310:loadbalancer/app/LabELB/2fb12fe2d2a5da	DNS name info: LabELB-1904038358.us-east-1.elb.amazonaws.com (A Record)		

Open the DNS server in a new browser tab and ensure that you see the EC2 instance web server as shown below.

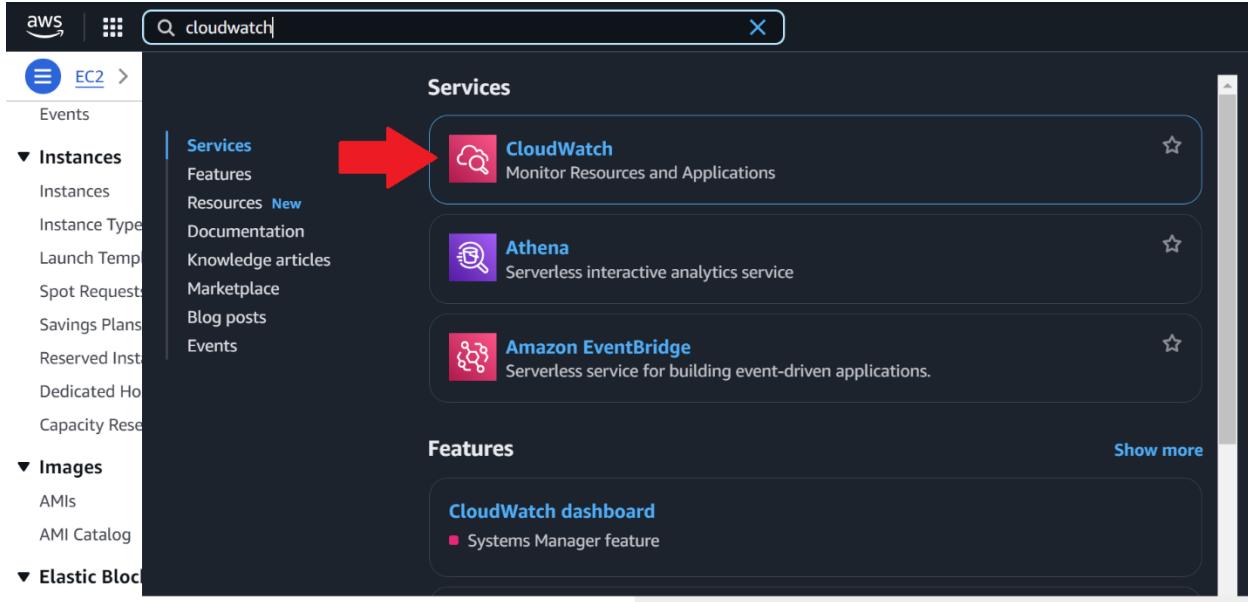
Meta-Data

InstanceID	i-079b3039cae93dbff
Availability Zone	us-east-1a

Value

Current CPU Load: 2%

In the search bar, search for and open Cloudwatch.



Click Alarms > All alarms, and ensure that the AlarmHigh alarm reports OK.

The screenshot shows the 'Alarms (2)' page under the CloudWatch navigation. It lists two alarms: 'TargetTracking-Lab Auto Scaling Group-AlarmHigh' and 'TargetTracking-Lab Auto Scaling Group-AlarmLow'. Both alarms are currently in an 'OK' state. The 'Actions enabled' column indicates that actions are enabled for both.

Name	State	Last state update (UTC)	Conditions	Actions
TargetTracking-Lab Auto Scaling Group-AlarmHigh-9d75edda-35a2-4ff0-9e5d-9e7fe6030329b	OK	2025-01-21 22:21:56	CPUUtilization > 60 for 3 datapoints within 3 minutes	Actions enabled
TargetTracking-Lab Auto Scaling Group-AlarmLow-abef9ddc-18015-4467-a92a-82b2f53ab998	Insufficient data	2025-01-21 22:19:51	CPUUtilization < 54 for 15 datapoints within 15 minutes	Actions enabled

Go back to EC2 from the search bar.

The screenshot shows the AWS search interface with 'ec2' typed into the search bar. The left sidebar has sections for CloudWatch, Favorites and recent, Dashboards, AI Operations, Alarms, In alarm, All alarms, and Billing. The main area displays 'Services' and 'Features'. The 'EC2' service card is highlighted with a red arrow. It includes a server icon, the name 'EC2', and the description 'Virtual Servers in the Cloud'.

Select Auto Scaling groups, select Lab Auto Scaling group, click the Automatic Scaling tab, select LabScalingPolicy, then click Actions > Edit.

Auto Scaling groups (1/1) info

Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
<input checked="" type="checkbox"/> Lab Auto Scaling Group	LabConfig   Version Default	2	-	2	2	6	us-east-1a, us-east-1b

Auto Scaling group: Lab Auto Scaling Group

Automatic scaling

Scaling policies resize your Auto Scaling group to meet changes in demand. With reactive dynamic scaling policies, you can track specific CloudWatch metrics and take action when the CloudWatch alarm threshold is met. Use predictive scaling policies along with dynamic scaling policies in the following situations: when your application demand changes quickly, but with a recurring pattern, or when your EC2 instances require more time to initialize.

Dynamic scaling policies (1/1) info

LabScalingPolicy

Policy type: Target tracking scaling

Enabled or disabled: Enabled

Execute policy when: As required to maintain Average CPU utilization at 60

Actions ▾

- Enable
- Disable
- Execute
- Edit
- Delete

Set the target value to 50 and click Update.

#### Edit dynamic scaling policy

Policy type: Target tracking scaling

Scaling policy name: LabScalingPolicy

Metric type: Average CPU utilization

Target value: 50

Instance warmup: 300 seconds

Disable scale in to create only a scale-out policy

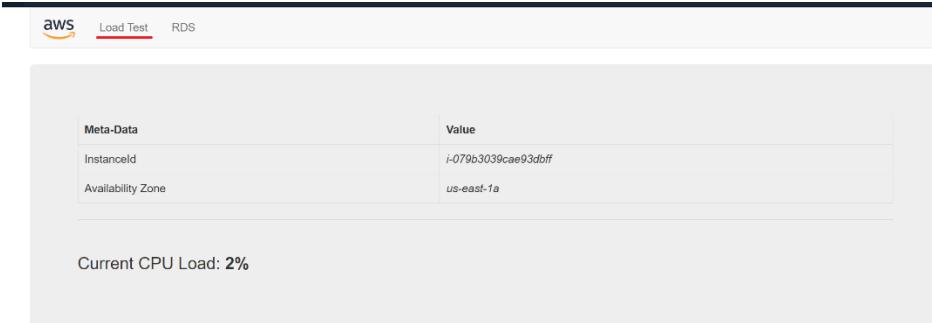
Update

Return to Cloudwatch > Alarms > All alarms and ensure the updated AlarmHigh alarm still reports OK.

Alarms (2)

Name	State	Last state update (UTC)	Conditions	Actions
TargetTracking-Lab Auto Scaling Group-AlarmHigh-889540cb-69cc-4c1b-89ce-f6c8208964b3	OK	2025-01-21 22:35:22	CPUTUtilization > 50 for 3 datapoints within 3 minutes	Actions enabled
TargetTracking-Lab Auto Scaling Group-AlarmLow-bacd6bae-7e5c-4494-b1fa-c50c6ae63bae	Insufficient data	2025-01-21 22:31:58	CPUTUtilization < 45 for 15 datapoints within 15 minutes	Actions enabled

Return to the EC2 web server tab and click Load Test.



Return to the AWS console and continually press the refresh button on the alarms page. Eventually, the AlarmHigh will report that it is in alarm.

The screenshot shows the 'Alarms (2)' page in the AWS CloudWatch Metrics Alarms section. It lists two alarms:

- TargetTracking-Lab Auto Scaling Group-AlarmHigh-889540cb-69cc-4c61-89ce-f6c8208964b3**: State: **In alarm**, Last state update: 2025-01-21 22:37:22, Condition: CPUUtilization > 50 for 3 datapoints within 3 minutes, Actions: Actions enabled.
- TargetTracking-Lab Auto Scaling Group-AlarmLow-bacd6bae-7e3c-4494-b1fa-c50c6ae63bae**: State: **OK**, Last state update: 2025-01-21 22:36:47, Condition: CPUUtilization < 37.5 for 15 datapoints within 15 minutes, Actions: Actions enabled.

Return to EC2 > Instances. You should see that the Auto Scaling Group has automatically created more instances of the Lab Instance AMI.

The screenshot shows the 'Instances (6) Info' page in the AWS EC2 Instances section. It lists six instances:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring
Bastion Host	i-0ba738e0bce67d64b	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	us-east-1a	-	52.207.87.231	-	-	disabled
Lab Instance	i-079b5039cae93dbff	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	us-east-1a	-	-	-	-	enabled
Lab Instance	i-0244d314437306933	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	us-east-1b	-	-	-	-	enabled
Lab Instance	i-0aa31259d68950f2	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	us-east-1b	-	-	-	-	enabled
Web Server 1	i-0ae9535acc8323e8d	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	us-east-1a	-	34.205.77.105	-	-	disabled
Lab Instance	i-02360934f11c0e16c	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	us-east-1a	-	-	-	-	enabled

Next, to clean up, select Web Server 1 and click Actions > Terminate (delete) instance.

The screenshot shows the 'Instances (1/6) Info' page in the AWS EC2 Instances section. It lists the same six instances. A red arrow points to the 'Actions' dropdown menu for the 'Web Server 1' instance, which contains the option 'Terminate (delete) instance'.

Click Terminate.

## Terminate (delete) instance?

X

**⚠️** On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

Are you sure you want to terminate these instances?

Instance ID	Termination protection
<input type="checkbox"/> i-0ae9535acc8323e8d (Web Server 1)	<input checked="" type="checkbox"/> Disabled

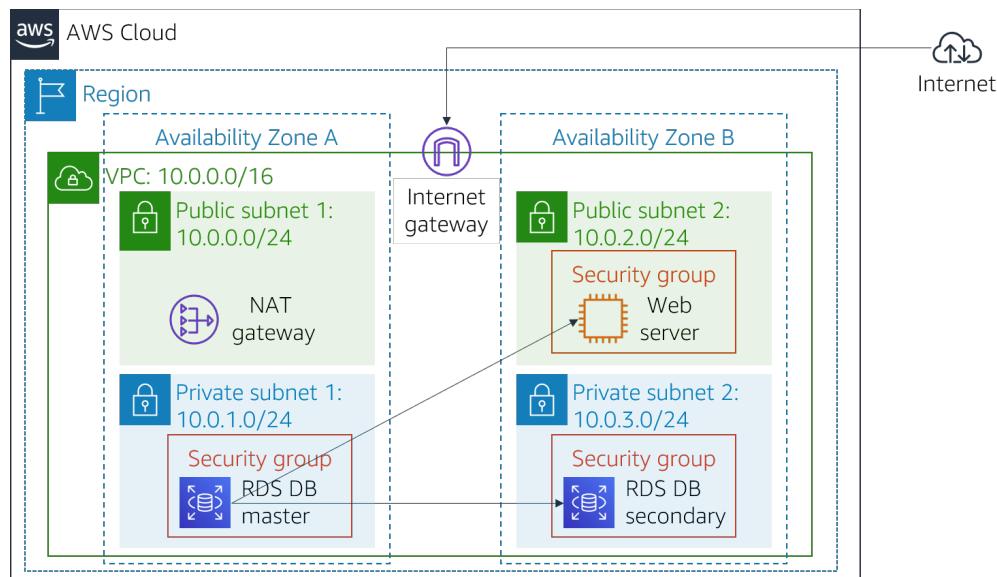
To confirm that you want to delete the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone.

**Terminate (delete)**

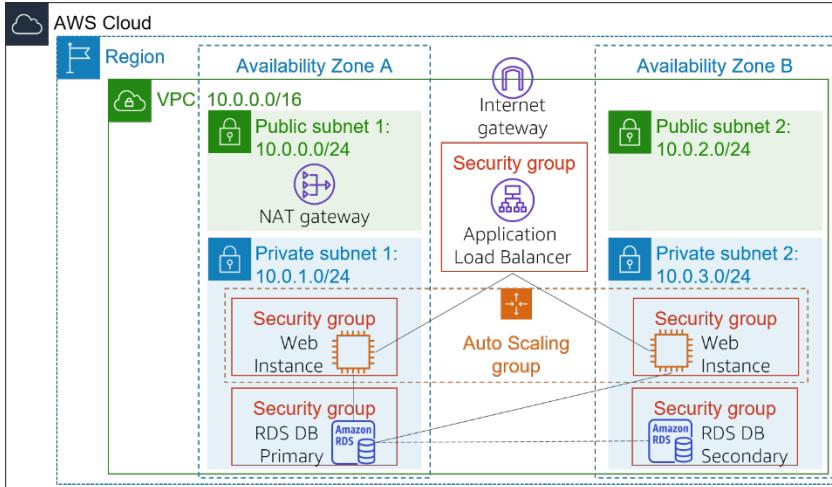
## Topology (EBS)



## Topology (RDS)



## Topology (Auto Scaling)



## Problems

No problems were encountered in this lab.

## Conclusion

To wrap up, these three labs were a great addition to my understanding of the AWS cloud and management console. Through learning about Elastic Block store, I now have a deeper understanding of the inner workings of Elastic Compute Cloud. Through learning about RDS, I now have a solid foundation of knowledge about how large amounts of data with a consistent structure are stored. Through learning about auto scaling, I'm now confident that I could scale AWS services for use at a company with heavy reliance on cloud resources.





# Palo Alto Networks Cybersecurity Academy – Configuring GlobalProtect RAVPN on a PA220 Firewall

Colin J. Faletto, CCNA

## Purpose

This lab expands upon our knowledge of the PA220 by introducing us to the world of VPNs. Setting up a remote access VPN provides valuable insight on how to create and secure a private tunnel into a firewall's internal network, which is extremely valuable to businesses requiring work-from-home cybersecurity solutions.

## Background

Palo Alto Networks is a networking and cybersecurity company from Santa Clara, California. They are a member of the S&P 500. They focus mainly on the business market, creating scalable security solutions for many of the largest companies worldwide.

The Palo Alto PA220 is a firewall sold by Palo Alto Networks. Contrary to Palo Alto's main market, the PA220 is intended for small office/home office solutions. Marketed as a NGFW, or Next-Generation Firewall, the PA220 uses machine learning to identify attacks instead of relying on a simple signature check like traditional firewalls. This technology allows the PA220 to identify undocumented threats and brand-new exploits without intervention from Palo Alto networks themselves. The PA220 also prevents threats by filtering URLs and securing against DNS-based attacks. As of January 31, 2023, it is no longer being sold, and it will reach end-of-life on January 31, 2028.

The PA220 doesn't have a fan, and instead uses hexagon-shaped vents to passively filter air. The firewall's compact form factor allows it to easily fit alongside existing network devices.

Palo Alto firewalls run on an operating system called PAN-OS. PAN-OS can be controlled through two methods: a Graphical User Interface (GUI) and a Command-Line Interface (CLI). The GUI is accessible through an HTTP connection and displays in any modern web browser. The HTTP connection is available through the firewall's MGT port and by default, is accessible at <http://192.168.1.1>. The firewall has a default username and password of *admin*.

The latest version of PAN-OS is PAN-OS 11.2 Quasar, which was released in May 2024. In this lab, our firewall is running PAN-OS 8, which has reached end of life and is no longer supported.

PAN-OS's GUI has a variety of settings and tools to control advanced functionality of the router. The GUI's default page is a dashboard that displays vital information, such as console messages and link states of ports.

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.

A virtual private network, or a VPN, is a method of creating a secure tunnel between networks. VPNs allow computers that are physically located offsite to be treated the same as computers physically inside of a network. There are two primary types of VPNs: remote access (RAVPN) and site-to-site, which create private tunnels for individual computers and entire networks respectively. In the business world, VPNs are often used to allow employees working from home to access company resources located on internal servers. VPN services are commonly sold commercially, allowing consumers to connect to private network-sharing servers. These servers are often located in multiple countries or regions, enabling consumers to spoof their location and hide network traffic from their ISP.

GlobalProtect is a Remote Access VPN service developed by Palo Alto Networks. The service requires a client program which runs on outside computers and supports all three major operating systems. GlobalProtect is heavily integrated into Palo Alto firewalls such as the PA220, which includes a gateway to allow connections from the service and a web portal to download the client. GlobalProtect puts a large emphasis on security, exemplifying the principle of least-privilege access and including a wide variety of configurable security options.

Remote Desktop Protocol, or RDP, is a Microsoft-proprietary protocol that allows a user to remotely view and control a connected Windows PC. RDP employs a client/server model, with the client being included on all versions of Windows and the server being exclusive to the operating system's higher tiers. RDP uses port 3389 with both TCP and UDP. RDP was introduced during Microsoft's transition from MS-DOS to the NT kernel with Windows NT 4.0 Terminal Services Edition, and the server has been included on every version of Windows (other than Home) since XP.

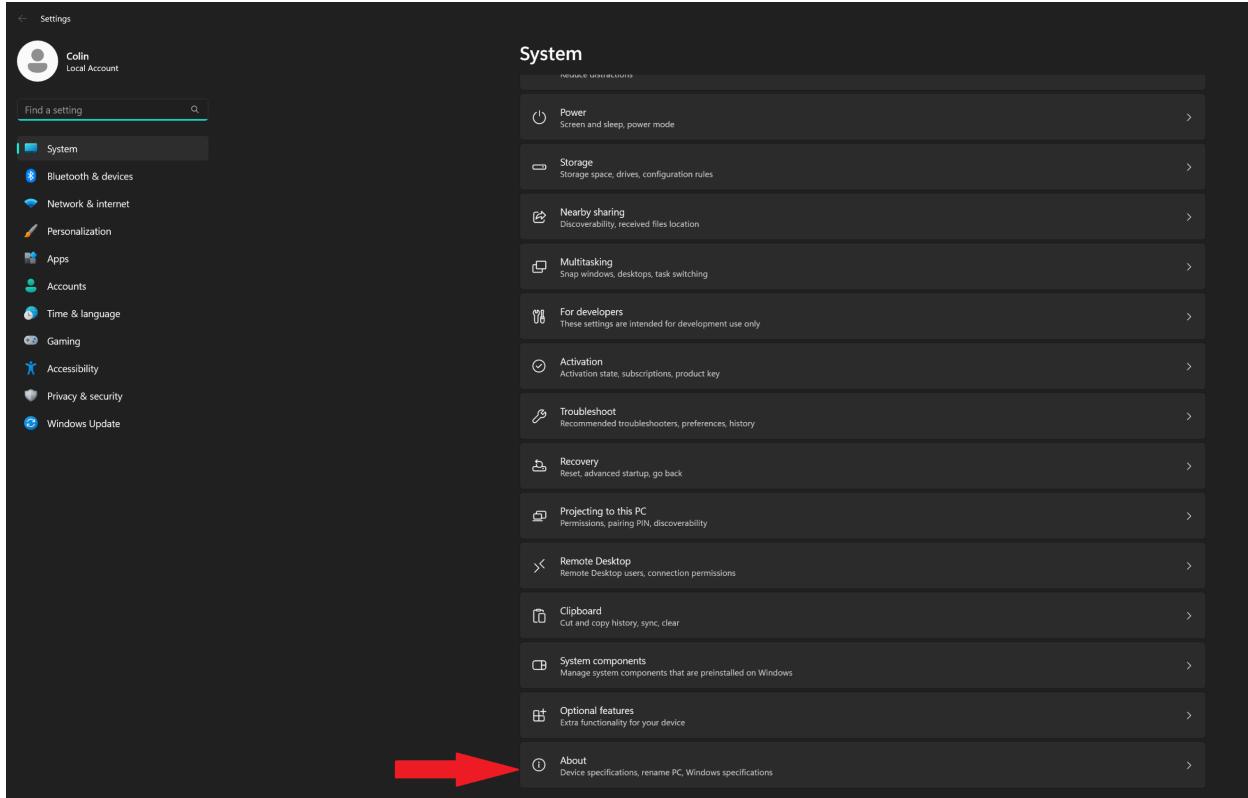
## Lab Summary

In this lab, we configured Microsoft's remote desktop protocol (RDP) on two Windows computers: one on the PA220's internal network and one just outside the PA220's network. We then set up Palo Alto's GlobalProtect remote access VPN on the firewall, including credentials for the outside user and a portal page to download the GlobalProtect client.

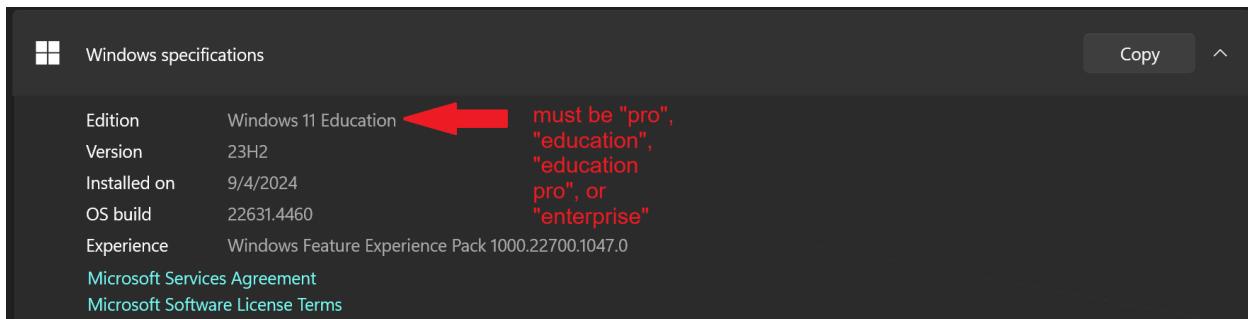
## Lab Commands

### Configuring Remote Desktop

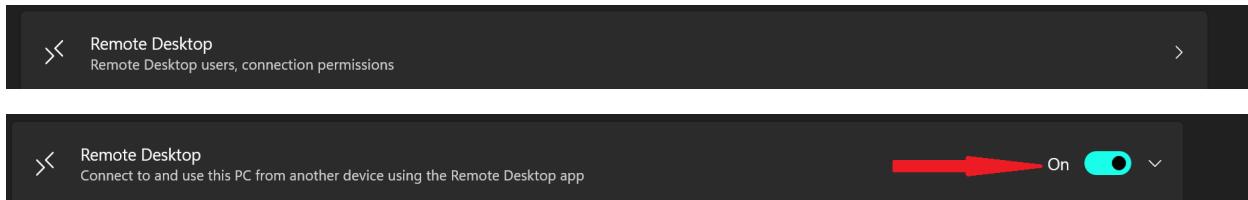
On the internal Windows PC, press (Win+I) to open the settings app. Click into the "About" section.



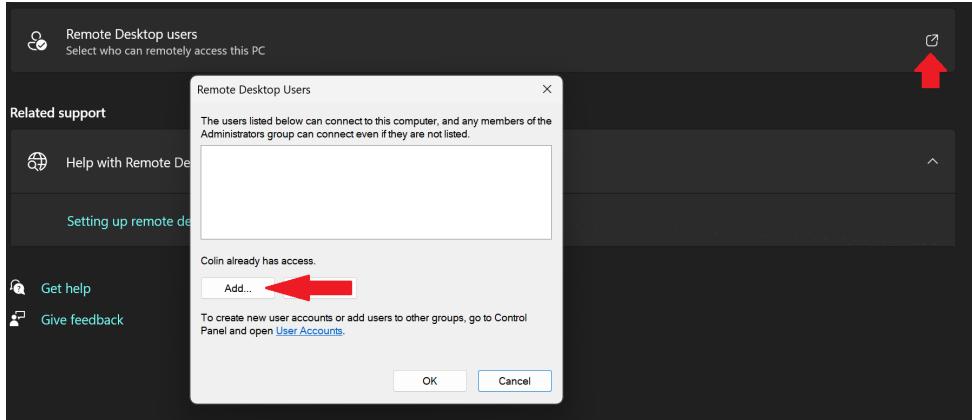
Make sure that you are running Windows 11 Pro, Education, Education Pro, or Enterprise. **Windows 11 Home doesn't support a Remote Desktop Server connection.** It can, however, be used on the external client PC.



In the settings menu, go to System > Remote Desktop and turn on “Remote Desktop”.

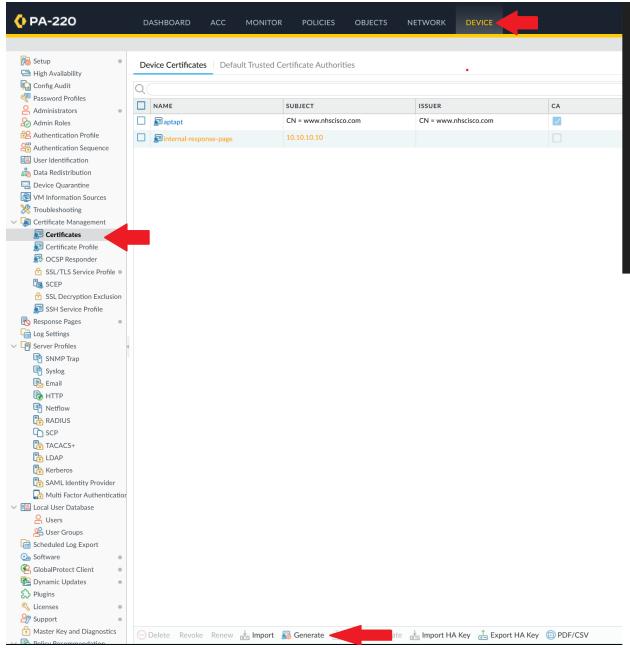


Click on “Remote Desktop Users”. If the user account you want to connect to isn’t an administrator, you will have to manually add it here using the “Add” button.



## Generate Certificates

In the PA220 web interface, navigate to Device > Certificate Management > Certificates and click Generate.



First, generate a root certificate. Give a Certificate Name and Common Name that make sense for the context, and make sure that the Certificate Authority box is checked. Under Certificate Attributes, assign appropriate values for the Country, State, Locale, Organization, and Department Fields, and make sure that the IP Address field is set to the outward-facing IP of the firewall. Optionally, increase the default cryptographic settings to higher values to increase the security of your certificates.

Generate Certificate

Certificate Type  Local  SCEP

Certificate Name **GlobalProtectStrongerRoot**

Common Name **GlobalProtectStrongerRoot**

IP or FQDN to appear on the certificate

Signed By **Certificate Authority**

Certificate Authority

Block Private Key Export

OCSP Responder

**Cryptographic Settings**

Algorithm	<b>RSA</b>
Number of Bits	<b>4096</b>
Digest	<b>sha512</b>
Expiration (days)	<b>365</b>

**Certificate Attributes**

TYPE	VALUE
Organization = "OU"	Newport High School
"Subject" field	
Department = "OU" from "Subject" field	Palo Alto Networks Cybersecurity Academy
<input checked="" type="checkbox"/> IP = "IP Address" from Subject Alternative Name (SAN) field	<b>192.168.40.180</b>

**Add** **Delete**

**Generate** **Cancel**

Next, generate your server certificate. Make sure that the Common Name is the outward-facing IP address of the firewall, and that the certificate is signed by the root certificate you generated earlier. Match the cryptographic settings and certificate attributes with the values configured in the root certificate.

Generate Certificate

Certificate Type  Local  SCEP

Certificate Name **GlobalProtectStrongerServer**

Common Name **192.168.40.180**

IP or FQDN to appear on the certificate

Signed By **GlobalProtectStrongerRoot**

Certificate Authority

Block Private Key Export

OCSP Responder

**Cryptographic Settings**

matched with root certificate	Algorithm: RSA
	Number of Bits: 4096
	Digest: sha512
	Expiration (days): 365

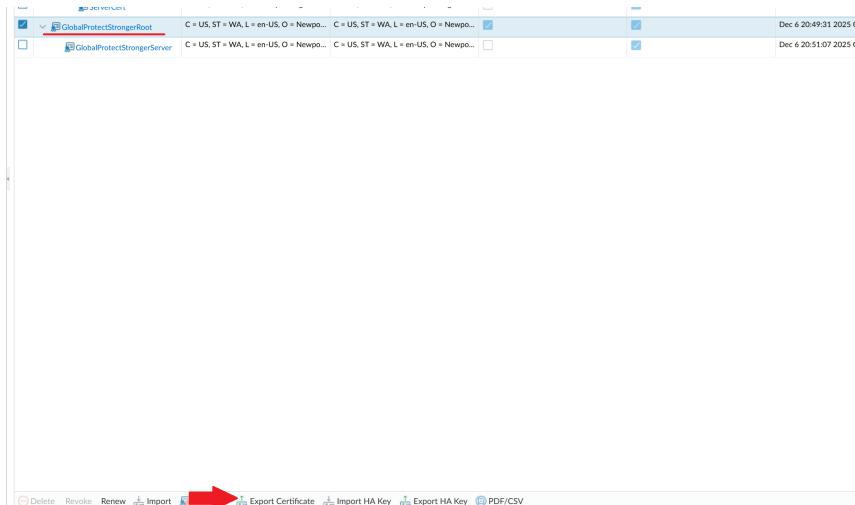
**Certificate Attributes**

TYPE	VALUE
Organization = "OU"	Newport High School
"Subject" field	
Department = "OU" from "Subject" field	Palo Alto Networks Cybersecurity Academy
<input checked="" type="checkbox"/> IP = "IP Address" from Subject Alternative Name (SAN) field	<b>192.168.40.180</b>

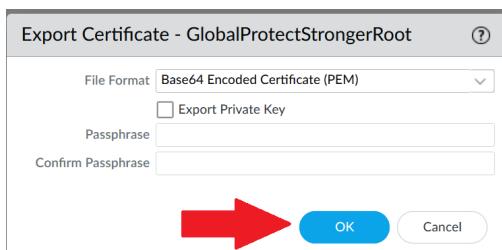
**Add** **Delete**

**Generate** **Cancel**

Export your root certificate by selecting it and clicking Export Certificate.

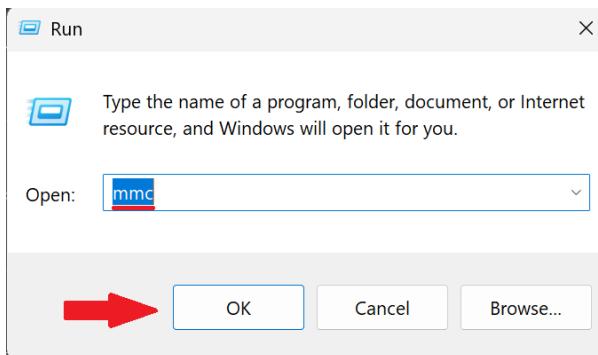


Click “OK” to confirm downloading the certificate. Make sure to note down the file’s download location.

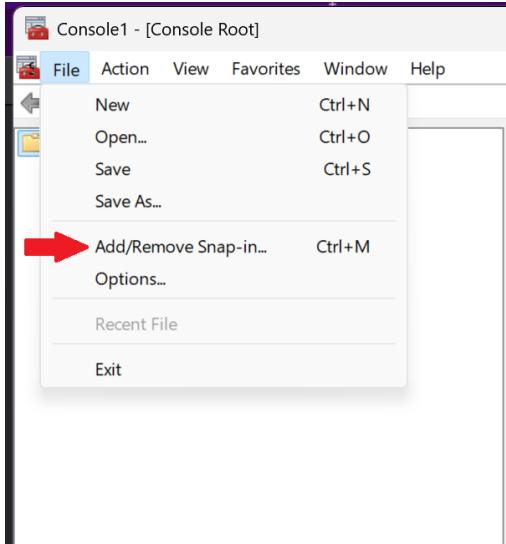


## Import Certificates

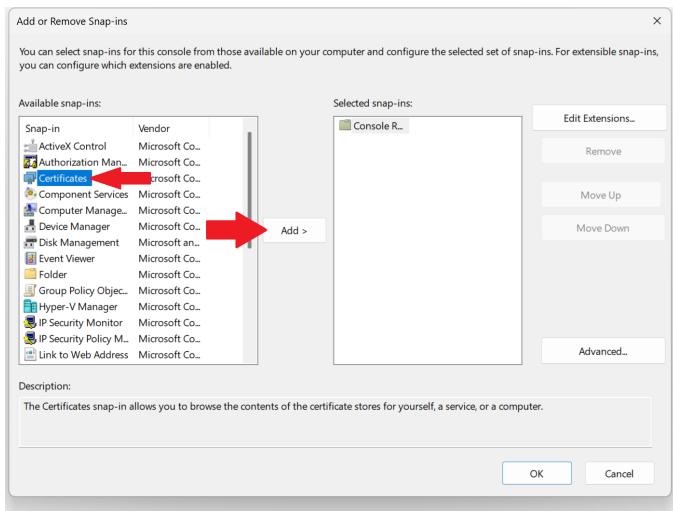
On your outside PC, open the Run dialog (Windows+R) and type “mmc”.



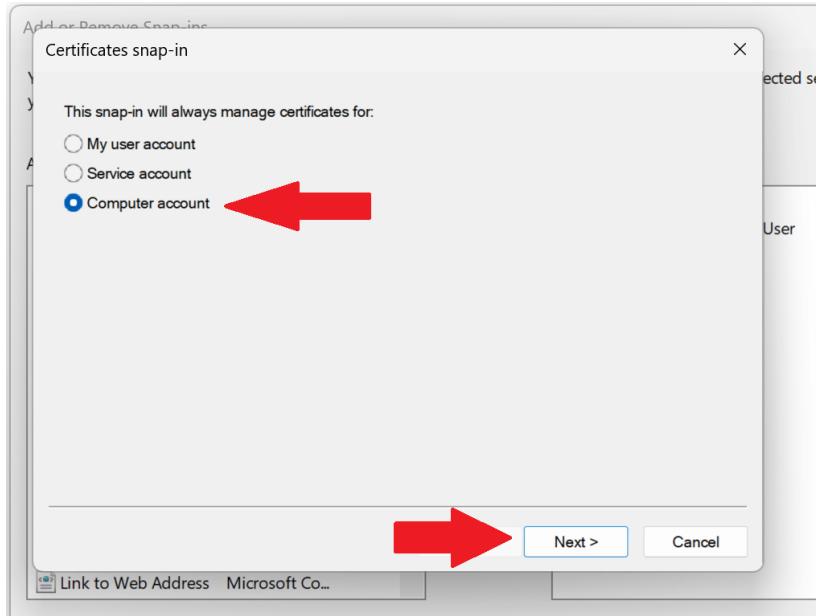
In the resulting window, click File > Add/Remove Snap-in.



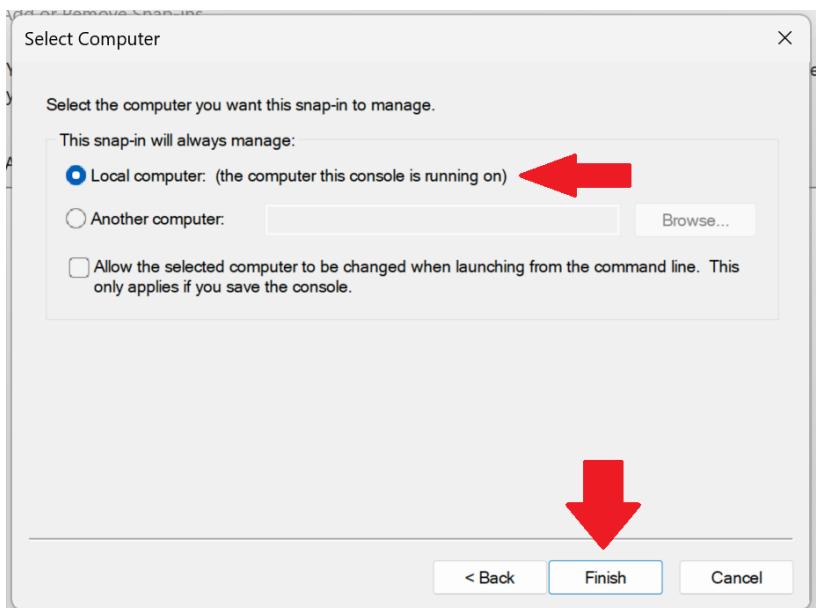
In the resulting window, click on Certificates > Add.



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



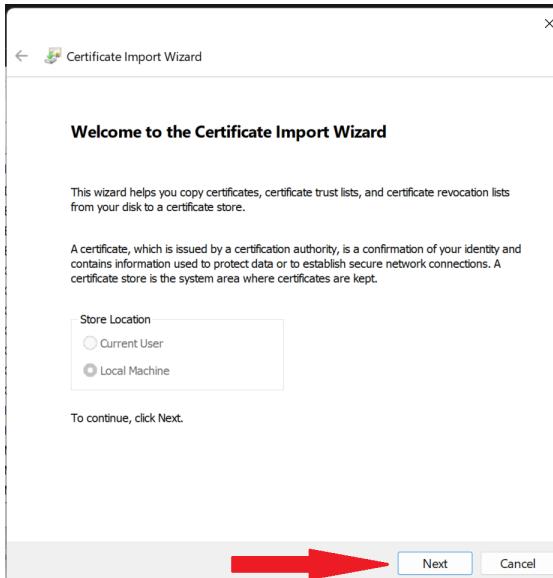
Make sure Local Computer is selected, and click Finish.



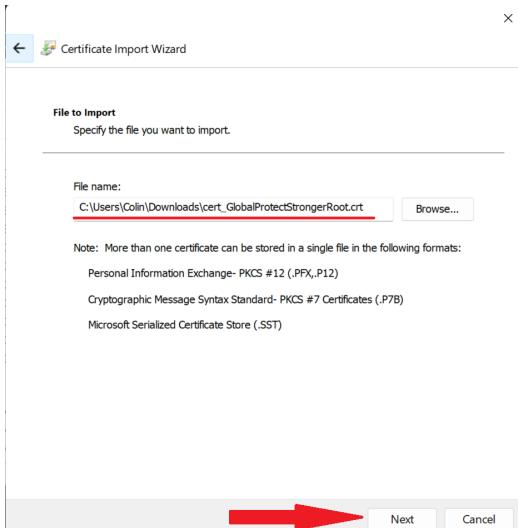
Inside Trusted Root Certification Authorities, right-click on Certificates and click on All Tasks > Import.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Type
AAA Certificate Services	AAA Certificate Services	12/31/2028	Client Authentication, Server Authentication	Sectigo (AAA)	Valid	Smart Card
Baltimore CyberTrust Root	Baltimore CyberTrust Root	5/12/2025	Client Authentication, Server Authentication	DigiCert Baltimore R...	Valid	Smart Card
CCNPBigBoy	CCNPBigBoy	1/7/2024	Client Authentication, Server Authentication	<None>	Valid	Smart Card
CCNPBigBoy	CCNPBigBoy	4/4/2024	Client Authentication, Server Authentication	<None>	Valid	Smart Card
Certum Trusted Network CA	Certum Trusted Network CA	12/31/2029	Client Authentication, Client Authentication, Server Authentication	Certum Trusted Net...	Valid	Smart Card
Certum Trusted Network CA 2	Certum Trusted Network CA 2	10/6/2046	Client Authentication, Client Authentication, Client Authentication	Certum Trusted Net...	Valid	Smart Card
Class 3 Public Primary Certification	Copyright (c) 1997 Microsoft Corp.	8/1/2028	Client Authentication, Time Stamping	VerSign Class 3 Pub...	Valid	Smart Card
Copyright (c) 1997 Microsoft Corp.	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timestamp...	Valid	Smart Card
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authentication	DigiCert	Valid	Smart Card
DigiCert CS RSA4096 Root G5	DigiCert CS RSA4096 Root G5	1/14/2046	Code Signing, Time S...	DigiCert CS RSA4096...	Valid	Smart Card
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authentication	DigiCert	Valid	Smart Card
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authentication	DigiCert Global Roo...	Valid	Smart Card
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authentication	DigiCert Global Roo...	Valid	Smart Card
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	11/9/2031	Time Stamping, Sec...	DigiCert	Valid	Smart Card
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authentication	DigiCert Trusted Ro...	Valid	Smart Card
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authentication	DST Root CA X3	Valid	Smart Card

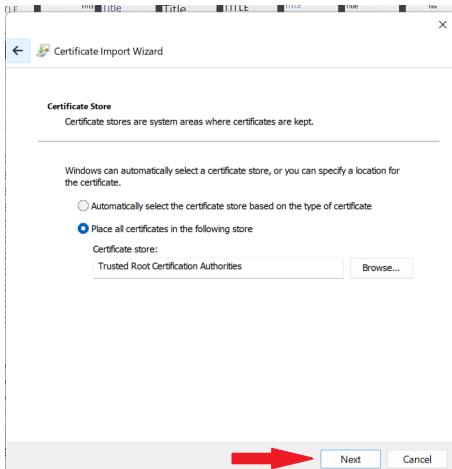
Click “Next”.



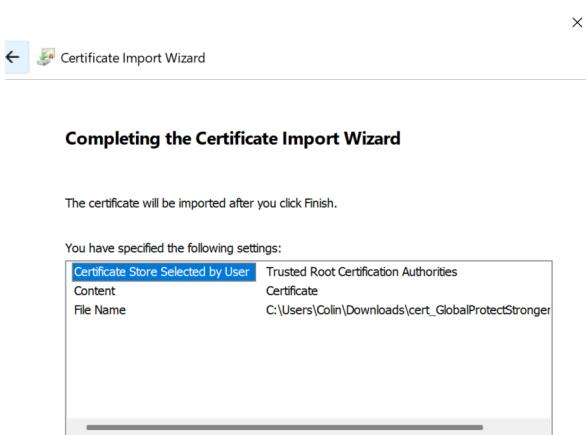
Select the certificate file downloaded earlier, then click “Next” again.



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

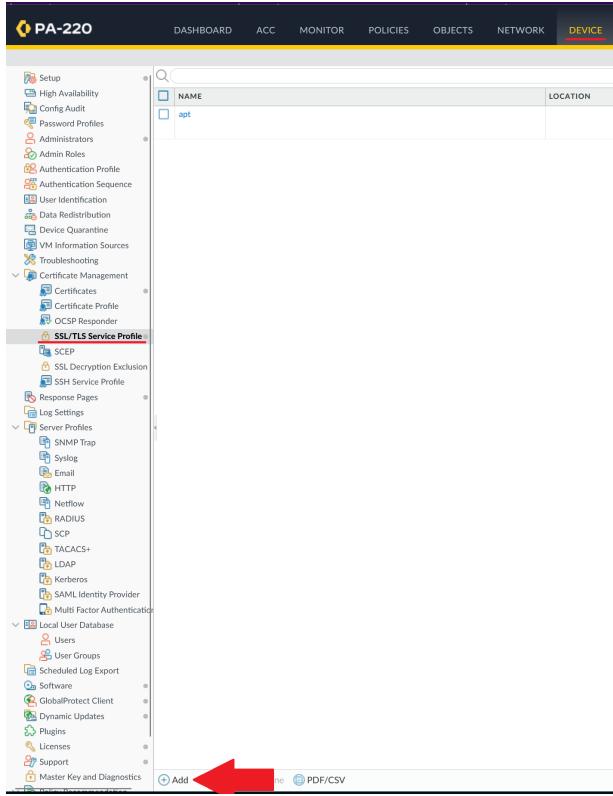


Click “Finish” to confirm the certificate import.



## Firewall Configuration

Back on the PA220, go to Device > SSL/TLS Service Profile, and click “Add”.



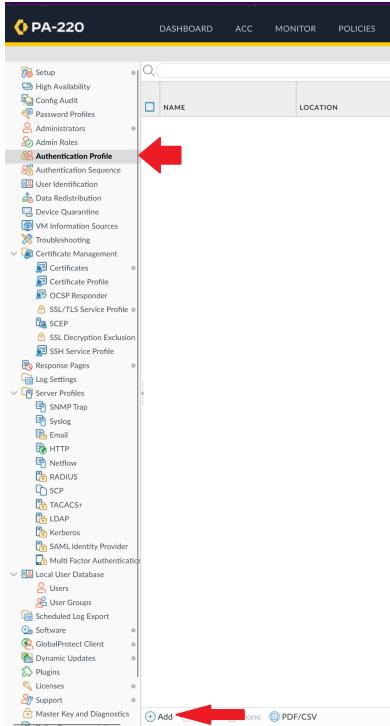
Make sure this profile uses the server certificate you set up earlier. Optionally, set the minimum TLS version to a more secure version (in this case, we used TLS 1.2)

### SSL/TLS Service Profile

Name	GlobalProtect
Certificate	GlobalProtectStrongerServer
<b>Protocol Settings</b>	
Min Version	TLSv1.2
Max Version	Max

**OK**      **Cancel**

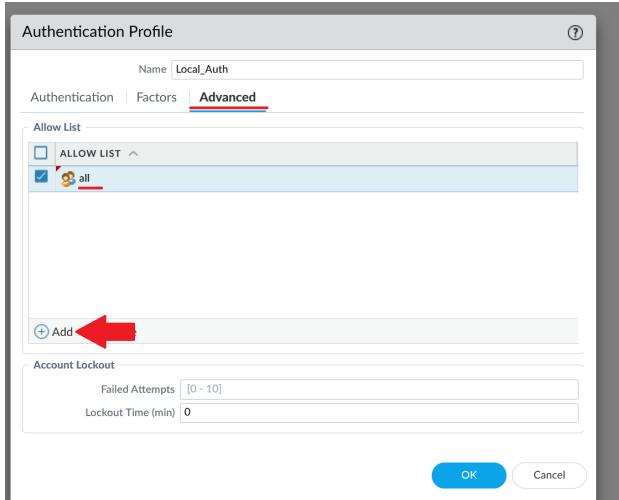
Next, go to “Authentication Profile” (still under Device) and click “Add”.



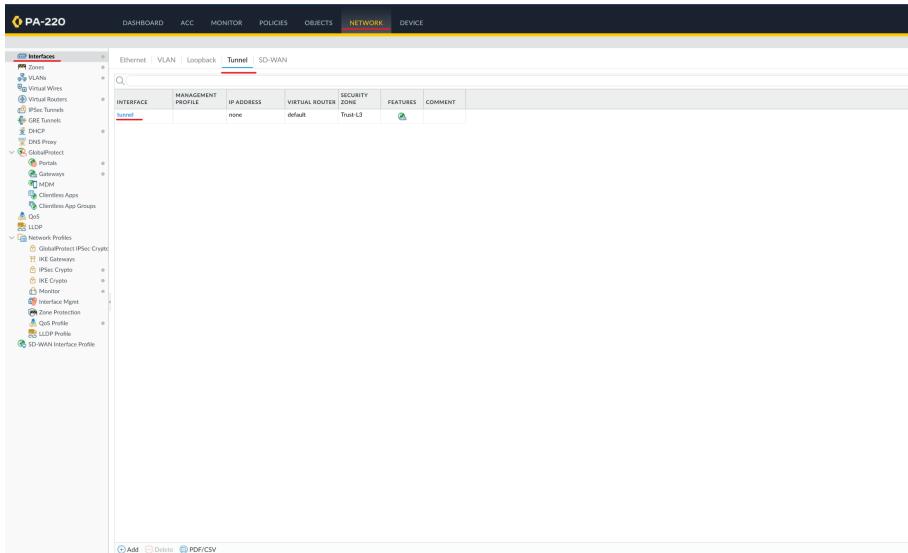
Give this profile an appropriate name and set the database type to “Local Database”.

The screenshot shows the 'Authentication Profile' configuration dialog. The 'Name' field is populated with 'Local\_Auth'. The 'Type' dropdown is set to 'Local Database'. The 'OK' and 'Cancel' buttons are visible at the bottom of the dialog.

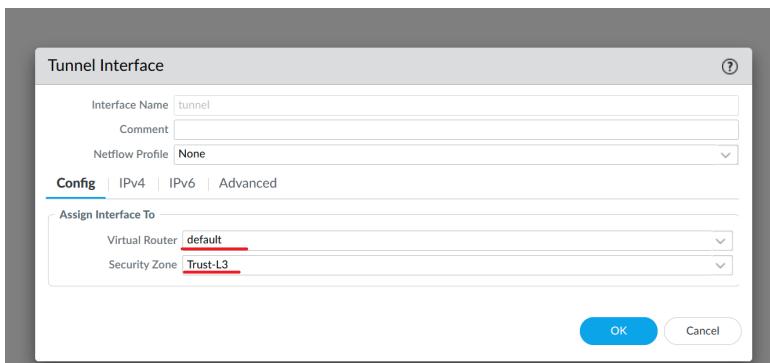
Under “Advanced”, click “Add” and type “all”.



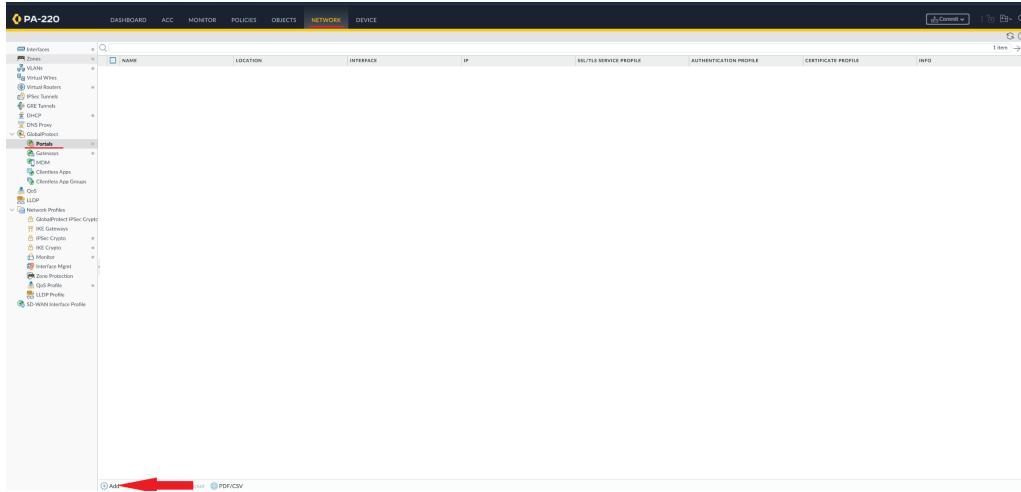
Go to Network > Interfaces > Tunnel and click on the “tunnel” interface.



Under “Config”, configure the same virtual router and Layer 3 security zone used on your inside network.



Go to Network > GlobalProtect > Portals and click “Add”.



Specify the outward-facing ethernet interface and set the address type to “IPv4 only”.

### GlobalProtect Portal Configuration

**General**

Name	Portal
Authentication	Network Settings
Portal Data Collection	Interface: ethernet1/1
Agent	IP Address Type: IPv4 Only
Clientless VPN	IPv4 Address: None
Satellite	Appearance
	Portal Login Page: factory-default
	Portal Landing Page: factory-default
	App Help Page: None
	Log Settings
	<input type="checkbox"/> Log Successful SSL Handshake
	<input checked="" type="checkbox"/> Log Unsuccessful SSL Handshake
	Log Forwarding: None

**OK** **Cancel**

Under the “Authentication” tab, specify the SSL/TLS service profile you created earlier and click “Add”.<sup>21</sup>

### GlobalProtect Portal Configuration

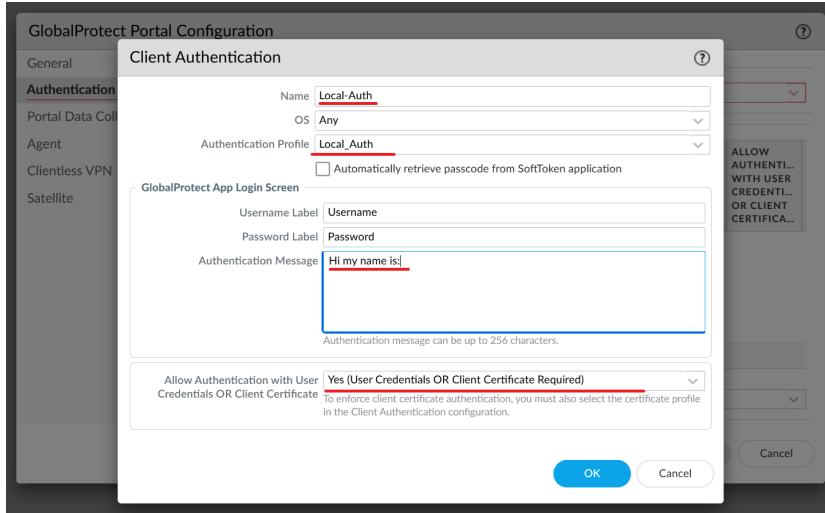
**General**

**Authentication**

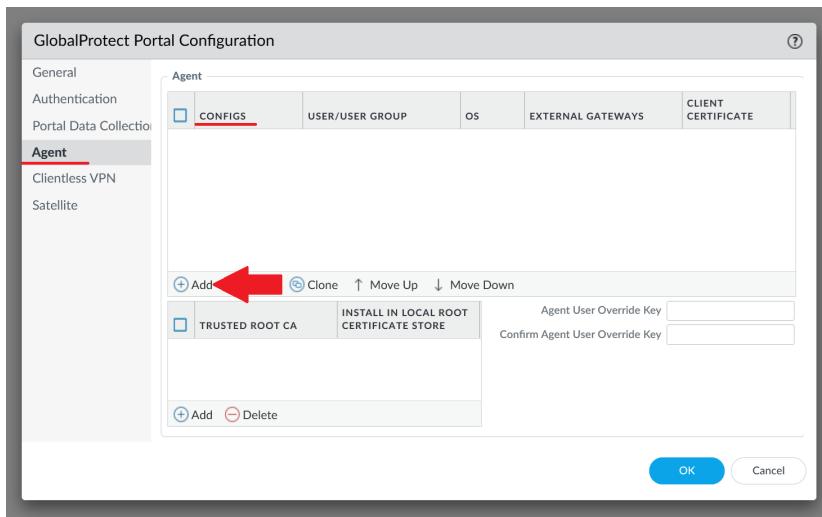
Server Authentication	SSL/TLS Service Profile: GlobalProtect																
Client Authentication	<table border="1"> <thead> <tr> <th>NAME</th> <th>OS</th> <th>AUTHENTIC... PROFILE</th> <th>AUTO RETRIEVE PASSCODE</th> <th>USERNAME LABEL</th> <th>PASSWORD LABEL</th> <th>AUTHENTI... MESSAGE</th> <th>ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFICAT...</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	NAME	OS	AUTHENTIC... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTI... MESSAGE	ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFICAT...								
NAME	OS	AUTHENTIC... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTI... MESSAGE	ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFICAT...										
<b>Add</b> <input type="button"/> Move Up <input type="button"/> Move Down																	
Certificate Profile: None																	

**OK** **Cancel**

Give the client authentication profile an appropriate name and specify the authentication profile you created earlier. Create an appropriate authentication message and make sure clients can either authenticate with user credentials or client certificates.



Under Agent > Configs, click “Add”.



Give the config an appropriate name, and make sure to save the user credentials. Make sure the Authentication Override certificate is set to the root certificate created earlier.

Configs

**Authentication** | Config Selection Criteria | Internal | External | App | HIP Data Collection

Name: GP-client-conf1

Client Certificate: None

The selected client certificate including its private key will be installed on client machines.

Save User Credentials: Yes

**Authentication Override**

- Generate cookie for authentication override
- Accept cookie for authentication override

Cookie Lifetime: Hours 24

Certificate to Encrypt/Decrypt Cookie: GlobalProtectStrongerRoot

**Components that Require Dynamic Passwords (Two-Factor Authentication)**

- Portal
- Internal gateways-all
- External gateways-manual only
- External gateways-auto discovery

Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.

OK Cancel

Under “External”, click “Add”.

Configs

Authentication | Config Selection Criteria | Internal | **External** | App | HIP Data Collection

Cutoff Time (sec): 5

**External Gateways**

<input type="checkbox"/>	NAME	ADDRESS	PRIORITY RULE	MANUAL
<input type="checkbox"/>				

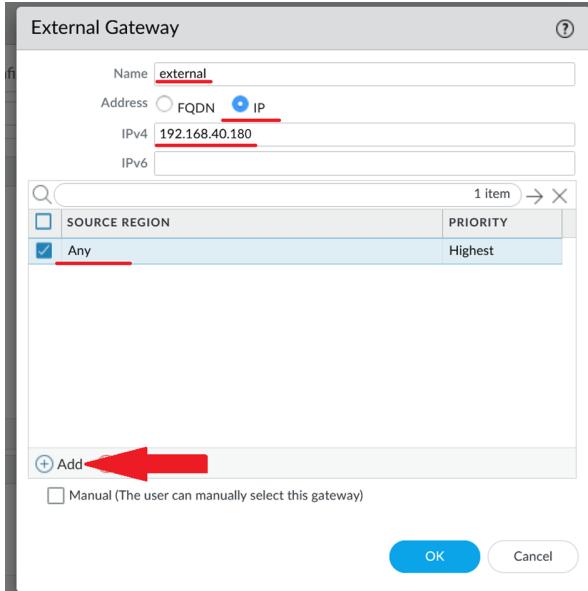
+ Add

THIRD PARTY VPN

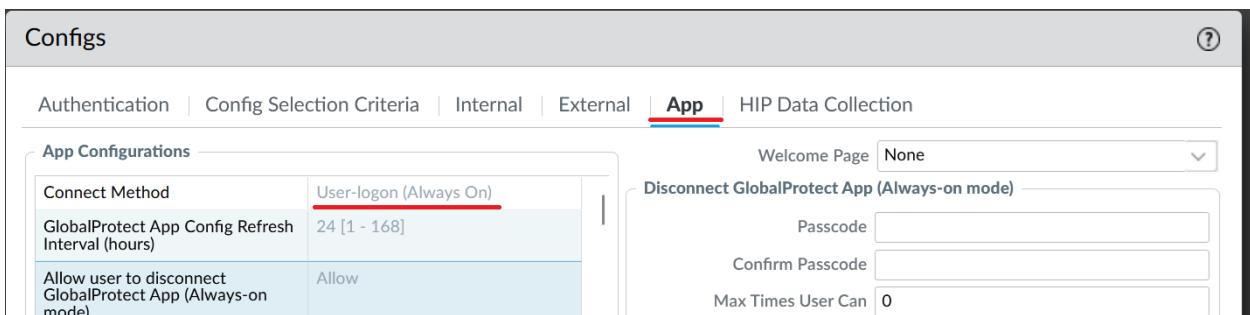
<input type="checkbox"/> + Add	<input type="checkbox"/> Delete
--------------------------------	---------------------------------

OK Cancel

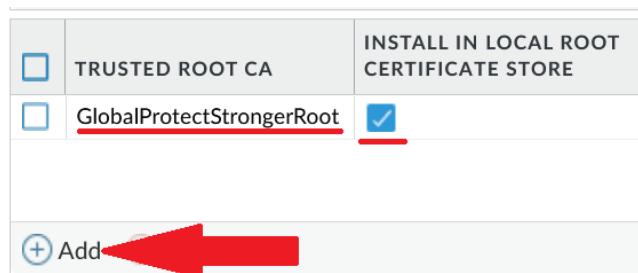
Give the gateway an appropriate name, set the mode to “IP”, and set the IP to the outward-facing IP of the gateway. Under “Source Region”, click “Add” and set it to “Any”.



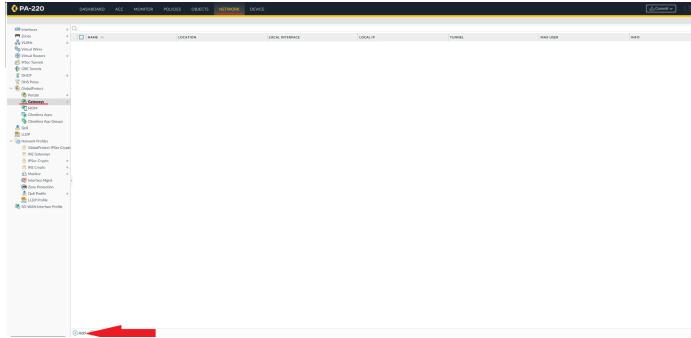
Click “OK” on the External Gateway window. Under “App”, set the connect method to “User-logon (Always On)”.



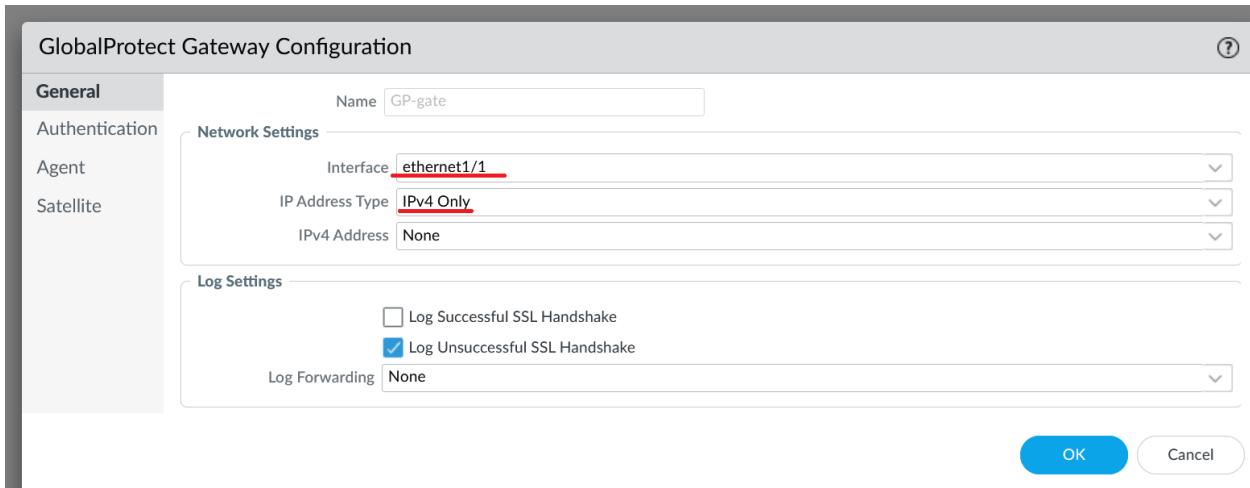
Click ok on the Configs window. Under “Trusted Root CA”, click “Add”, add the root certificate created earlier, and click “Install in local root certificate store”.



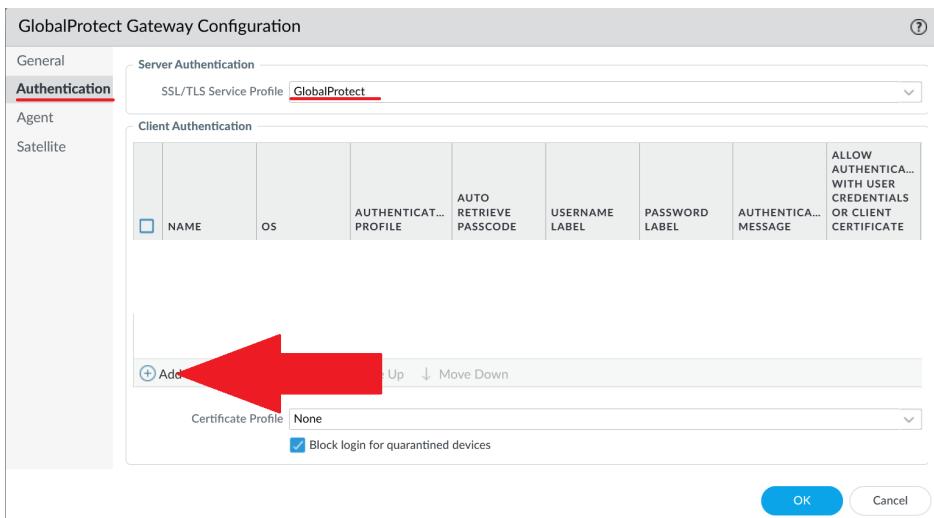
Go to Network > Gateways and click “Add”.



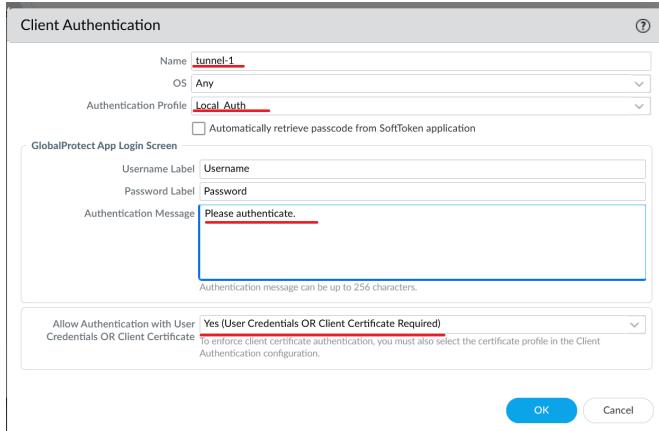
Set the interface to the outward facing interface of the firewall and leave the IP address type as “IPv4 only”.



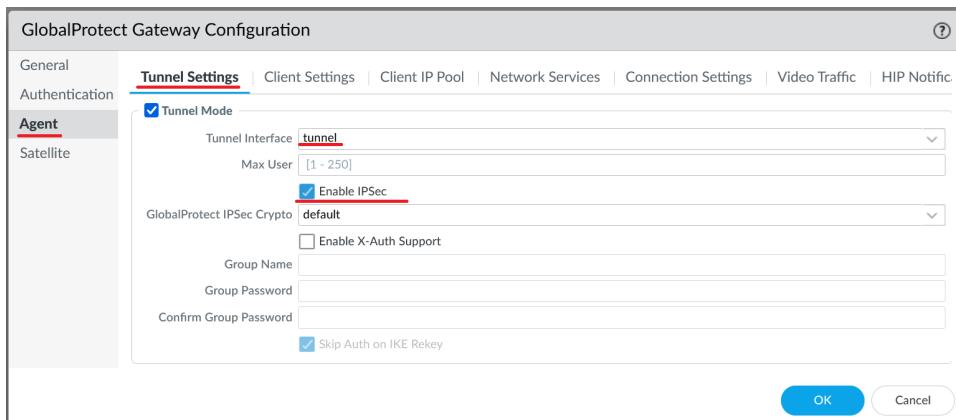
Under “Authentication”, set the SSL/TLS service profile to the profile you created earlier, and under client authentication, click “Add”.



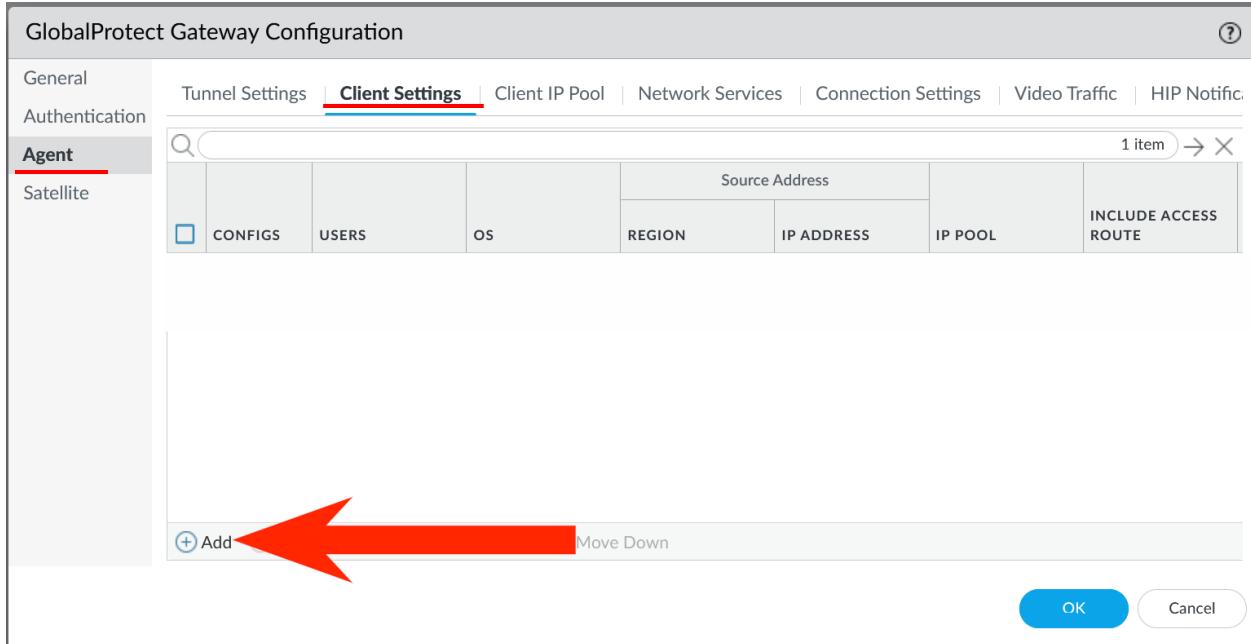
Configure an appropriate tunnel name, and set the authentication profile to the profile created earlier. Configure an appropriate authentication message, and allow authentication with user credentials OR a client certificate.



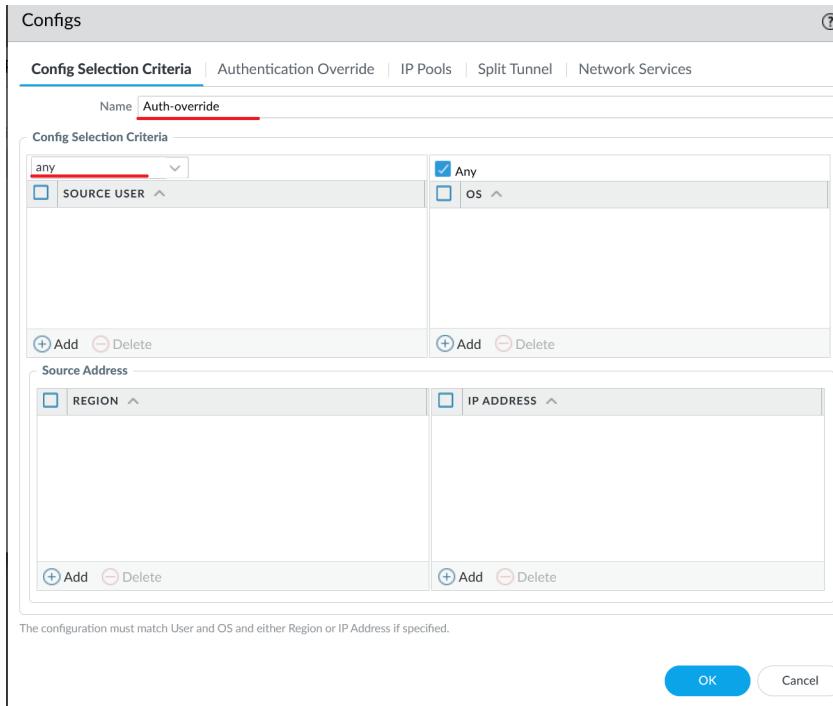
Under Agent > Tunnel Settings, set the tunnel interface to the interface created earlier, and make sure to enable IPsec.



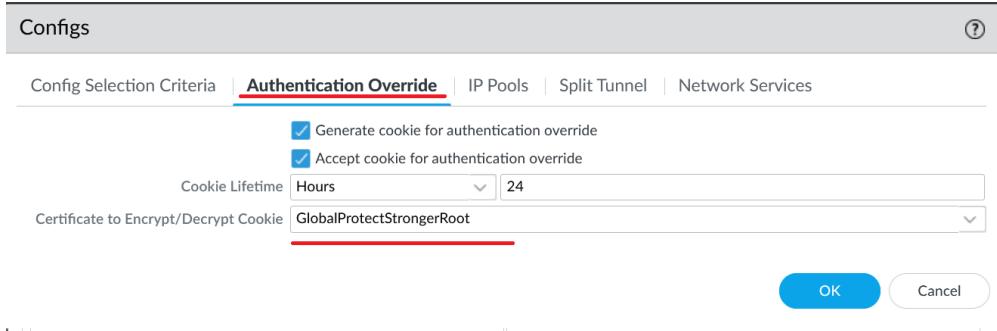
Under "Client Settings", click "Add".



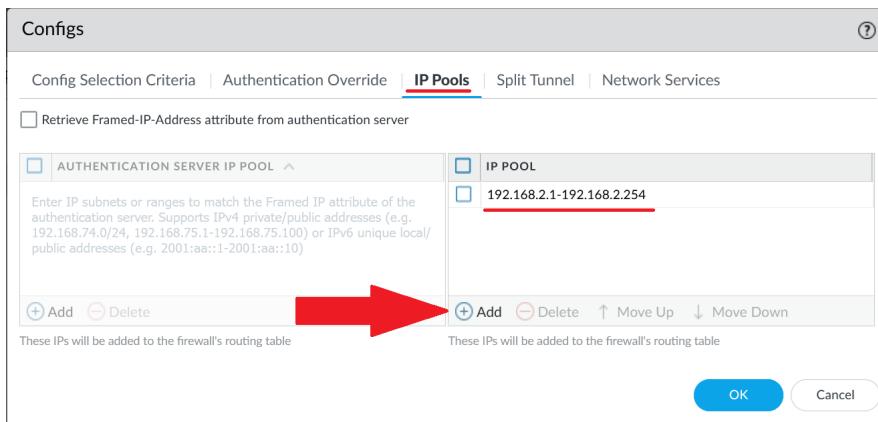
Give the configuration an appropriate name, and set the config selection criteria to “any”.



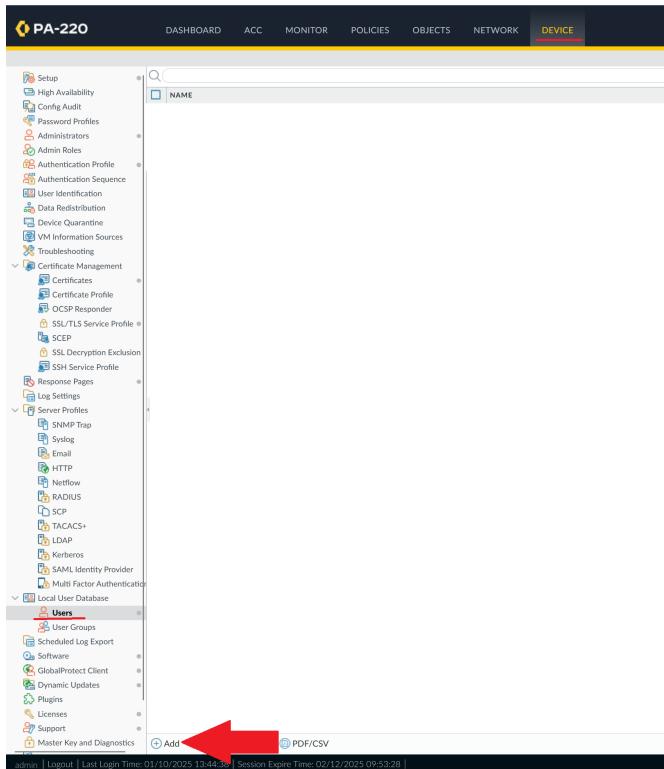
Under “Authentication Override”, set the certificate to decrypt/encrypt the cookie to the root certificate created earlier.



Under “IP Pools”, click “Add” and specify a valid range of IP addresses. These addresses will be dynamically allocated to clients by the GlobalProtect gateway.



Under Device > Local User Database > Users, click “Add”.



Configure an appropriate username and password.

Name:	test-user
Mode:	<input checked="" type="radio"/> Password <input type="radio"/> Password Hash
Password:	[REDACTED]
Confirm Password:	[REDACTED]
<input checked="" type="checkbox"/> Enable	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

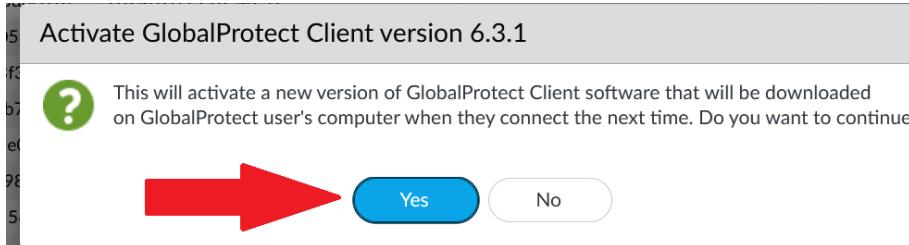
Under GlobalProtect Client, download the latest client version.

VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION
6.3.1-1383	231 MB	2024/01/09 13:20:16			Download
6.2.6	226 MB	2024/01/09 13:10:46			Download
6.2.5-788	226 MB	2024/01/09 13:10:28			Download
6.2.4	229 MB	2024/01/17 18:15:08			Download
6.2.3	222 MB	2024/01/17 11:55:34			Download
6.2.2	220 MB	2024/01/09 02:58:14			Download
6.2.1-287	220 MB	2024/01/04 10:32:11			Download
6.2.1	209 MB	2023/11/22 05:58:19			Download
6.2.0	209 MB	2023/10/09 07:22:05			Download
6.1.5	219 MB	2024/01/07 07:45:59			Download
6.1.4-720	211 MB	2024/01/07 07:45:52			Download
6.1.3	292 MB	2023/11/25 08:28:57			Download
6.1.2	290 MB	2023/08/03 07:15:29			Download
6.1.1	250 MB	2023/07/14 07:32:48			Download
6.1.0	124 MB	2022/09/01 14:06:19			Download
6.0.1-1825	229 MB	2022/08/30 14:06:07			Download
6.0.1-1826	221 MB	2024/11/04 14:21:16			Download
6.0.10	211 MB	2024/07/09 04:45:54			Download
6.0.8	206 MB	2023/10/19 04:44:11			Download
6.0.7	289 MB	2023/05/22 11:19:59			Download
6.0.5	283 MB	2023/04/28 08:41:34			Download
6.0.4-26	281 MB	2022/07/27 08:23:24			Download
6.0.3	155 MB	2022/06/02 12:26:13			Download
6.0.1	152 MB	2022/05/04 06:37:23			Download
6.0.0	150 MB	2022/04/26 11:15:50			Download
5.2.13	222 MB	2023/02/12 07:42:48			Download
5.2.12	235 MB	2023/01/11 07:08:37			Download
5.2.11	100 MB	2022/05/26 07:38:08			Download
5.2.10	99 MB	2022/03/09 11:49:56			Download
5.2.9	99 MB	2021/12/14 14:20:18			Download
5.2.8	96 MB	2021/11/30 09:57:03			Download
5.2.7	94 MB	2021/10/30 14:41:40			Download
5.2.6	87 MB	2021/09/06 03:44:12			Download

Once downloaded, click “Activate”.

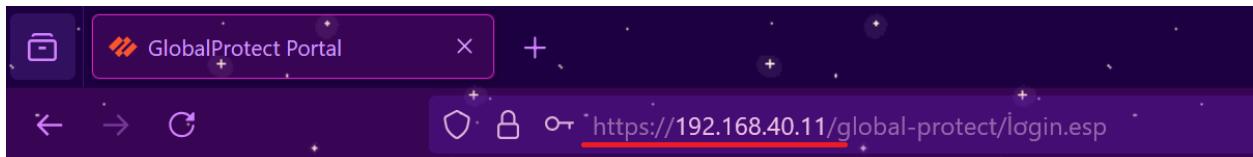


Click “Yes” to confirm.



## Connecting to the VPN

Switch to the outside computer. From a web browser, navigate to the outward-facing IP of the firewall.



Log in with the username and password created earlier.



Download the appropriate GlobalProtect agent for the OS/architecture of the outside computer (in this case, Windows 64 bit).

[Download Windows 32 bit GlobalProtect agent](#)

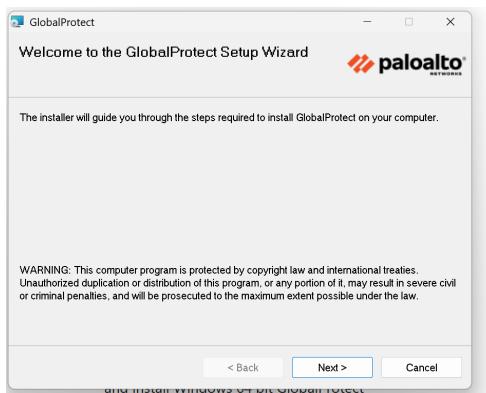
[Download Windows 64 bit GlobalProtect agent](#)

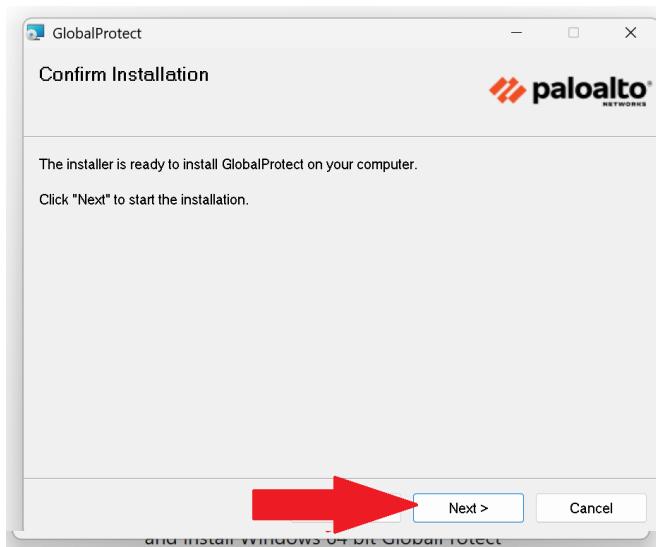
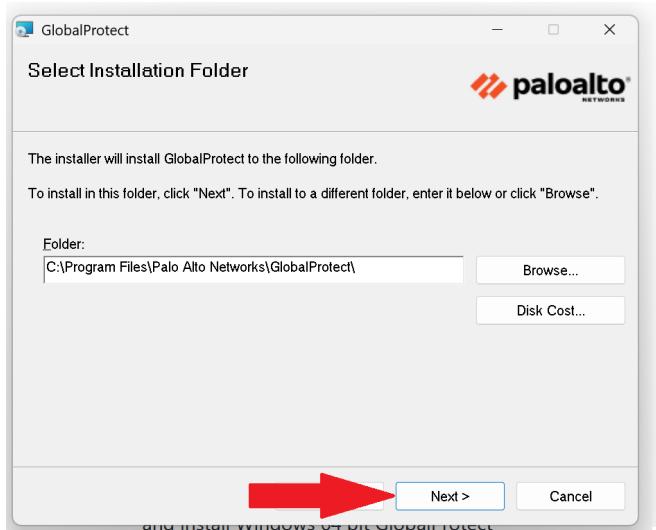
[Download Mac 32/64 bit GlobalProtect agent](#)

Open the downloaded installer file.

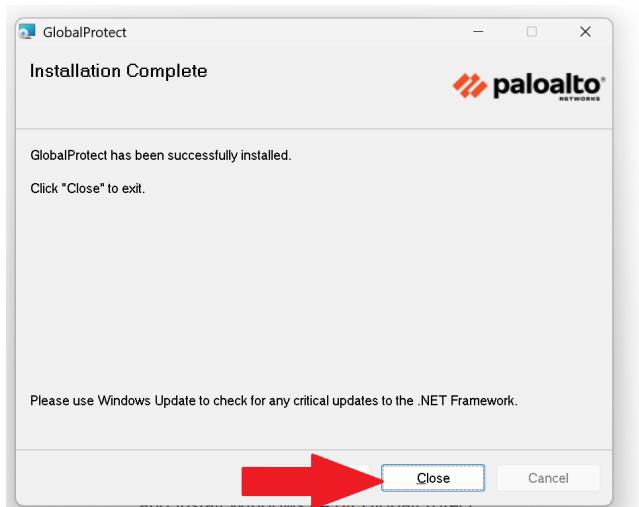


Click "Next" through the installation process.

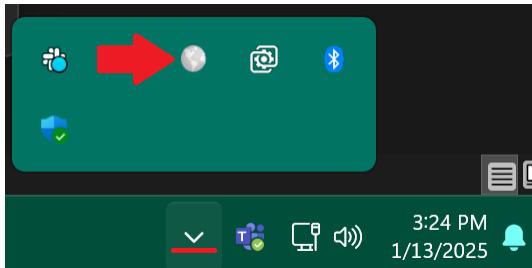




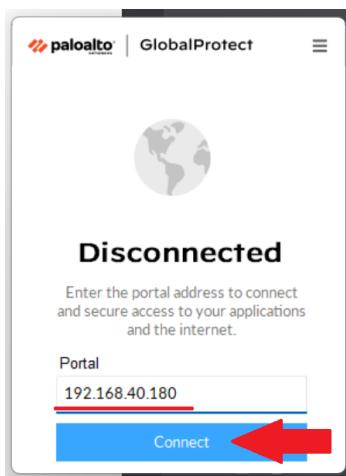
Click "Close" once the installer finishes.



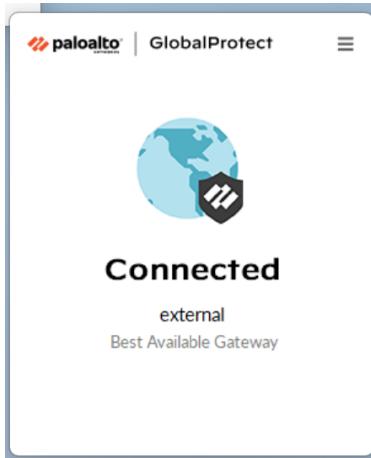
Open the GlobalProtect client from the system tray (it may be in the overflow section).



Enter the outward-facing IP of the firewall and click “Connect”.



You should see the following success message:



From the command prompt, run the `ipconfig` command. You should see that an address has been assigned from the IP range configured earlier.

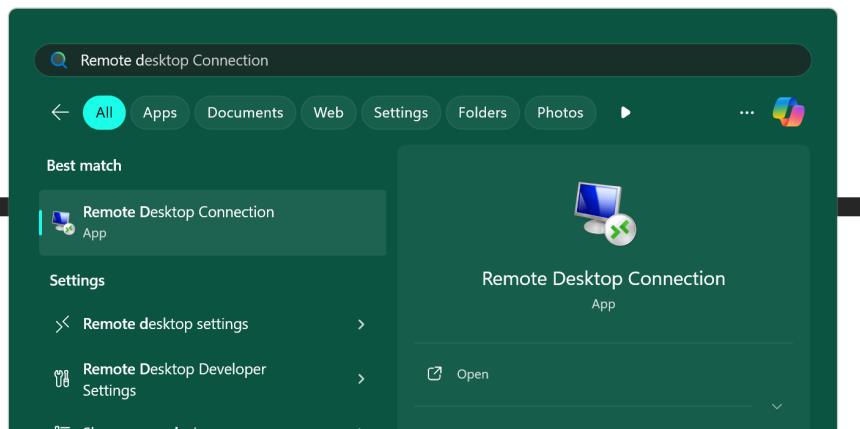
```
C:\Users\Ram>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet 5:

  Connection-specific DNS Suffix . :
  IPv4 Address . . . . . : 192.168.2.3
```

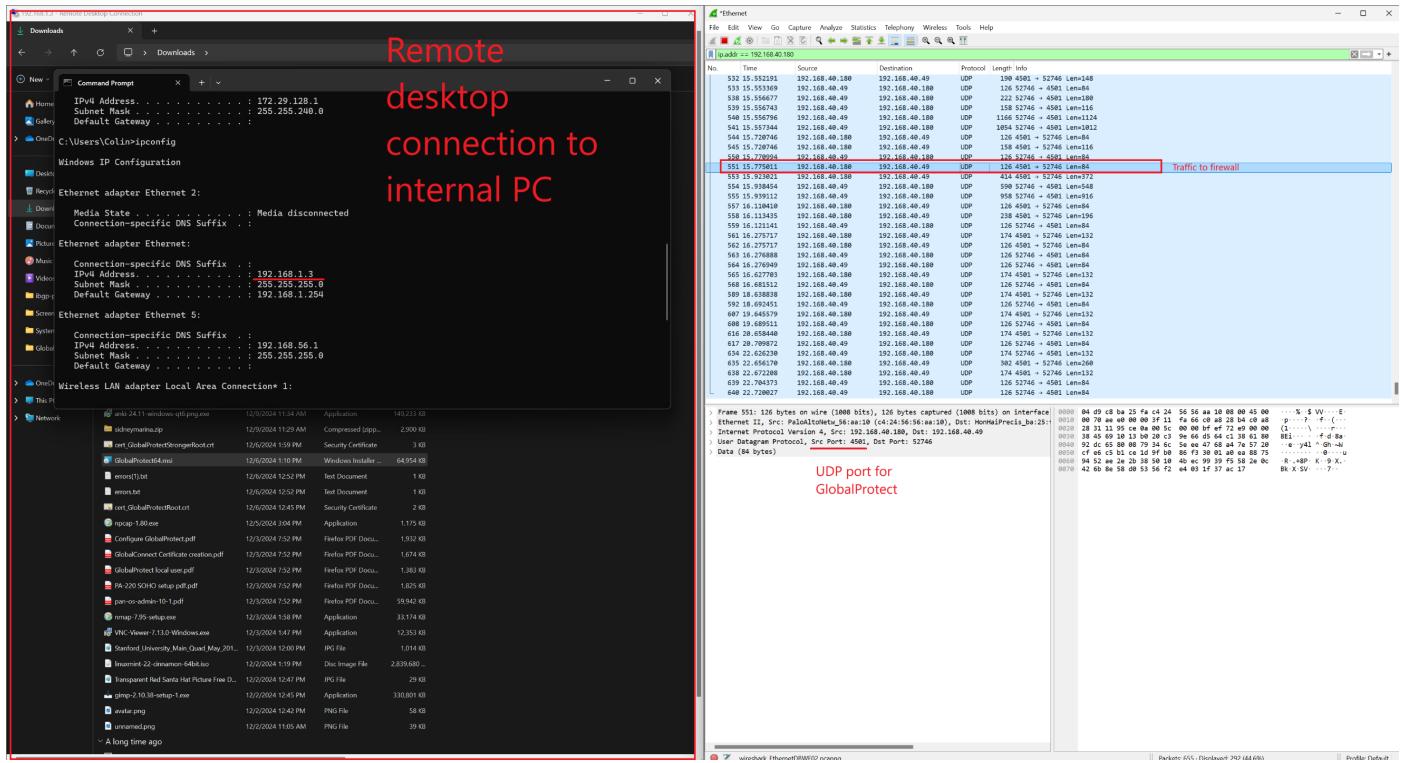
Open the remote desktop connection client.



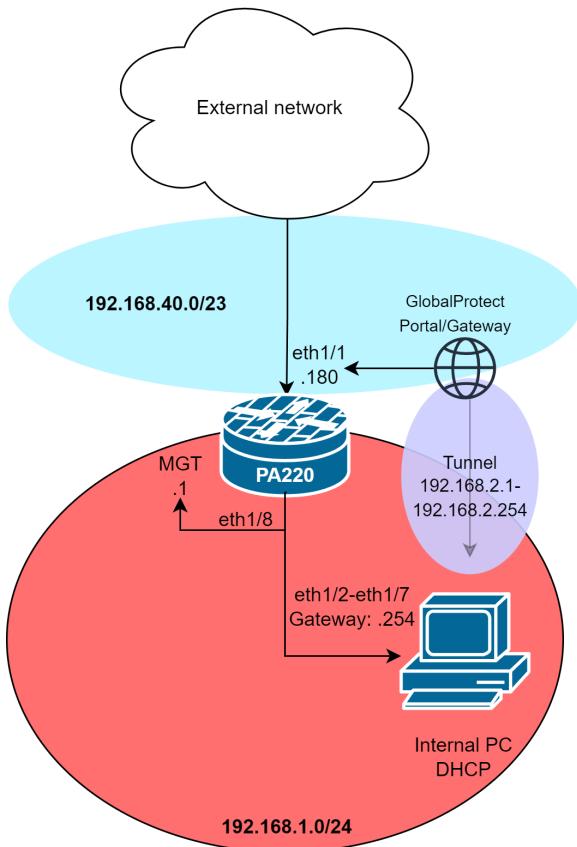
Enter the private IP of the internal computer, and click “connect”.



The remote desktop connection should establish, as shown below. By opening wireshark, you should see traffic to the firewall using port 4501 (the UDP port GlobalProtect uses).



## Network Diagram



## Problems

- We originally had issues with Windows RDP, which refused to connect even with both computers on the internal network. The fix for this was simply restarting both PCs.

## Conclusion

To wrap up, this lab provided ample insight into the GlobalProtect VPN client and server, and how to create a secure private tunnel into a Palo Alto firewall. This information, being both niche and in-demand, is highly valued in the networking industry, and I'm very grateful to have had this opportunity to learn. Overall, this lab wasn't too difficult, and I'm very confident I could replicate this lab's setup in a real-life SOHO environment.





# AWS Academy Cloud Foundations: Configuring Identity and Access Management, Virtual Private Cloud, and Elastic Compute Cloud

Colin J. Faletto, CCNA

## Purpose

This write-up is intended to document and explain the first three labs in the AWS Academy Cloud Foundations course. These labs are intended to provide an introduction to very basic AWS concepts, such as basic security, cloud networking, and virtual machines. These concepts are essential for new cloud engineers to provide parallels to the core skills of traditional IT. These labs also provide a strong foundation of knowledge for the AWS management console, as they all take place primarily inside this console.

## Background

Amazon is a company based in Seattle that runs the biggest e-commerce platform in the world. They were started in 1994 by former CEO Jeff Bezos and have grown from a small online bookstore to a giant online store offering a wide variety of products. Amazon also has a strong physical retail presence in the grocery space with their Amazon Fresh and Whole Foods chains, and has a strong online media presence through Twitch, Prime Video, and Amazon Music, which provide entertainment in the form of livestreams, movies and television shows, and music respectively. Amazon also has a popular line of e-readers and tablets with their Kindle brand and has a successful brand of artificial intelligence assistants with their Amazon Alexa A.I. and their Amazon Echo line of smart speakers.

Amazon Web Services, or AWS, is Amazon's cloud computing division. It was created in 2002 to provide simple web services to customers and expanded to cloud storage and computing in 2006. It is the leading cloud service provider and is popular for its pay-as-you-go service model. AWS provides services to everyone from small businesses to massive companies like Coca-Cola and Apple, and even provides web infrastructure to government branches. AWS takes the responsibility and cost of managing a data center out of the hands of businesses and maintains a massive global network of Amazon data centers that split customer traffic among them. AWS currently has 34 geographic regions, each of which have multiple availability zones which themselves contain multiple data centers. These data centers are in undisclosed locations for security reasons, though their general position is published. AWS offers services for virtual machines, cloud storage, database management, machine learning, IoT services, cloud networking, and much more.

Amazon Elastic Compute Cloud, or EC2, is an AWS service that allows customers to create virtual machines in the AWS cloud. These machines are very versatile, as they can be allocated as many or as few resources (CPU, RAM, GPU) as needed and can run nearly any operating system. By default, EC2 instances will run Amazon Linux, which is a version of Linux optimized for AWS servers. Amazon's e-commerce platform, its primary source of revenue, has been running on EC2 instances for over a decade. EC2 instances have a variety of different types, which are optimized for different purposes such as memory (R series, X series), compute (C series), and storage (H series, I series, D series).

Amazon Virtual Private Cloud, or VPC, is an AWS service that provides a virtual network inside the AWS cloud. This service allows AWS objects, such as EC2 instances, to communicate with each other. In a VPC, each EC2 machine is assigned a

unique private IPv4 address, which is then connected via NAT to a public address on an internet gateway. Using this gateway, machines in the VPC can communicate with other AWS VPCs and other Internet-connected machines. Amazon VPC is provided at no additional charge to customers using EC2 instances.

Amazon Identity and Access Management, or IAM, is an AWS service that provides a layer of security to customers by limiting the resources different users can access. IAM follows the principle of least privilege, meaning that by default, all AWS controls are blocked for users unless they have been explicitly granted permissions. IAM represents a portion of the customer responsibilities in the AWS shared responsibility model, which is a model outlining that AWS is responsible for the physical security of data centers and networks while the customer is responsible for keeping their customer data and configurations safe. One of IAM's unique features is its role feature, which creates identities with elevated permissions that can be temporarily assigned to users. This feature works similarly to the "sudo" command in unix-based operating systems.

## Lab Summary

This write-up covers three different AWS labs. The first lab covers AWS IAM. The lab entails assigning permissions to three different users to allow them to interact with S3 and EC2 services. Two of these users are support users, who are assigned read-only permissions to EC2 and S3 respectively. The other user is an administrator with start and stop access to EC2 instances. The second lab covers AWS VPC, and entails creating a VPC with four different subnets, two public and two private, spread across two different availability zones. The lab also involves creating a security group to allow HTTP access to machines in the second public subnet. The third lab involves creating a web server EC2 instance, allowing HTTP access through a security group, then resizing the instance and testing the stop protection feature.

## Lab Commands (Lab 1 IAM)

Log into the AWS management console.

Console Home | Console Help

us-east-1.console.aws.amazon.com/console/home

aws | Q IAM

Console Home Info

Recently visited Info

No recently visited services

Explore one of these commonly visited AWS services.

EC2 S3 RDS Lambda

View all services

Welcome to AWS

Getting started with AWS

Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification

Learn from AWS experts and advance your skills and knowledge.

AWS Health Info

Open issues 0 Past 7 days

Scheduled changes 0 Upcoming and past 7 days

Other notifications 0 Past 7 days

Cost and usage Info

Current month costs \$0.00 Cost (\$)

Forecasted month end costs

Savings opportunities Enable Cost Optimization Hub

EC2 - Compute Virtual Private Cloud Service Catalog EC2 - Other S3 Others

CloudShell Feedback Privacy Terms Cookie preferences

In the search bar, search for “IAM” and open the first result.

Q IAM

N. Virginia voclabs/user3712476=Colin\_Faletto @ 8589-358

Services

Show more

Services Features Resources New

IAM Manage access to AWS resources

In the IAM dashboard, open the “User Groups” tab from the sidebar.

## ▼ Access management

User groups

Users

Roles

Open the “S3-Support” group.

<input type="checkbox"/> Group name	▲ Users	▼ Permissions	▼ Creation time
<a href="#">EC2-Admin</a>	⚠ 0	✓ Defined	7 minutes ago
<a href="#">EC2-Support</a>	⚠ 0	✓ Defined	7 minutes ago
<a href="#">S3-Support</a>	⚠ 0	✓ Defined	7 minutes ago

Click “Add Users”.

**S3-Support** [Info](#)

Summary		<a href="#">Edit</a>
User group name S3-Support	Creation time December 13, 2024, 12:09 (UTC-08:00)	ARN <a href="#">arn:aws:iam::858935888409:group/spl66/S3-Support</a>

[Users](#) [Permissions](#) [Access Advisor](#)

**Users in this group (0)**  
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

[Search](#)  [User name](#)

No resources to display

[Add users](#)



Check the box next to “user-1”.

[user-1](#) 0 None 13 minutes ago

Click “Add Users”.

[Add users](#)

Return to the “User Groups” section and select “EC2-Support”.

<input type="checkbox"/>	Group name	▲   Users	▼   Permissions	▼   Creation time
<input type="checkbox"/>	<a href="#">EC2-Admin</a>	⚠ 0	✓ Defined	7 minutes ago
<input type="checkbox"/>	<a href="#">EC2-Support</a>	⚠ 0	✓ Defined	7 minutes ago
<input type="checkbox"/>	<a href="#">S3-Support</a>	⚠ 0	✓ Defined	7 minutes ago

Click “Add Users”.

**EC2-Support** [Info](#)

Summary		<a href="#">Edit</a>
User group name EC2-Support	Creation time December 13, 2024, 12:09 (UTC-08:00)	ARN <a href="#">arn:aws:iam::858935888409:group/spl66/EC2-Support</a>

[Users](#) [Permissions](#) [Access Advisor](#)

**Users in this group (0)**  
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

[Search](#)  [User name](#)

No resources to display

[Add users](#)



Select “user-2” and click “Add Users”.

The screenshot shows the 'User Groups' section of the AWS IAM console. It lists five groups: 'user-2' (selected), 'user-3', 'EC2-Admin', 'EC2-Support', and 'S3-Support'. Each group has a status bar at the top indicating 0 users, none of whom have been added. The 'EC2-Admin' group is highlighted with a blue border. At the bottom right, there is a blue 'Edit' button and an orange 'Add users' button.

Return to the “User Groups” section and click on “EC2-Admin”.

The screenshot shows the 'User Groups' section with the 'EC2-Admin' group selected. The table header includes columns for Group name, Users, Permissions, and Creation time. The 'EC2-Admin' row shows 0 users, defined permissions, and was created 7 minutes ago. Below the table is a horizontal scrollbar. At the bottom right, there is a blue 'Edit' button and an orange 'Add users' button.

Click “Add Users”.

The screenshot shows the 'EC2-Admin' group details page. It includes sections for Summary (User group name: EC2-Admin, Creation time: December 13, 2024, 12:09 (UTC-08:00), ARN: arnawsiam:85893588409:group/spl66/EC2-Admin), Users (selected), Permissions, and Access Advisor. Under 'Users in this group (0)', there is a search bar and a table with columns for User name and creation time. The table shows 'No resources to display'. At the bottom right, there is a blue 'Edit' button and an orange 'Add users' button.

Click the checkbox next to “user-3” and click “Add Users”.

The screenshot shows the 'User Groups' section with the 'user-3' checkbox selected. The table header includes columns for Group name, Users, Permissions, and Creation time. The 'user-3' row shows 1 user added, defined permissions, and was created 16 minutes ago. At the bottom right, there is a blue 'Edit' button and an orange 'Add users' button.

If done correctly, each user group should have a “1” next to it.

The screenshot shows the 'User Groups' section with three groups selected: 'EC2-Admin', 'EC2-Support', and 'S3-Support'. The table header includes columns for Group name, Users, Permissions, and Creation time. The 'EC2-Admin' row shows 1 user added, defined permissions, and was created 15 minutes ago. The 'EC2-Support' and 'S3-Support' rows also show 1 user added, defined permissions, and were created 15 minutes ago. At the bottom right, there is a blue 'Edit' button and an orange 'Create group' button.

Return to the dashboard.

## Identity and Access Management (IAM)

Search IAM

Dashboard



On the dashboard page, find and copy the sign-in URL for IAM users. This URL will be used to test the permissions that have just been set up.

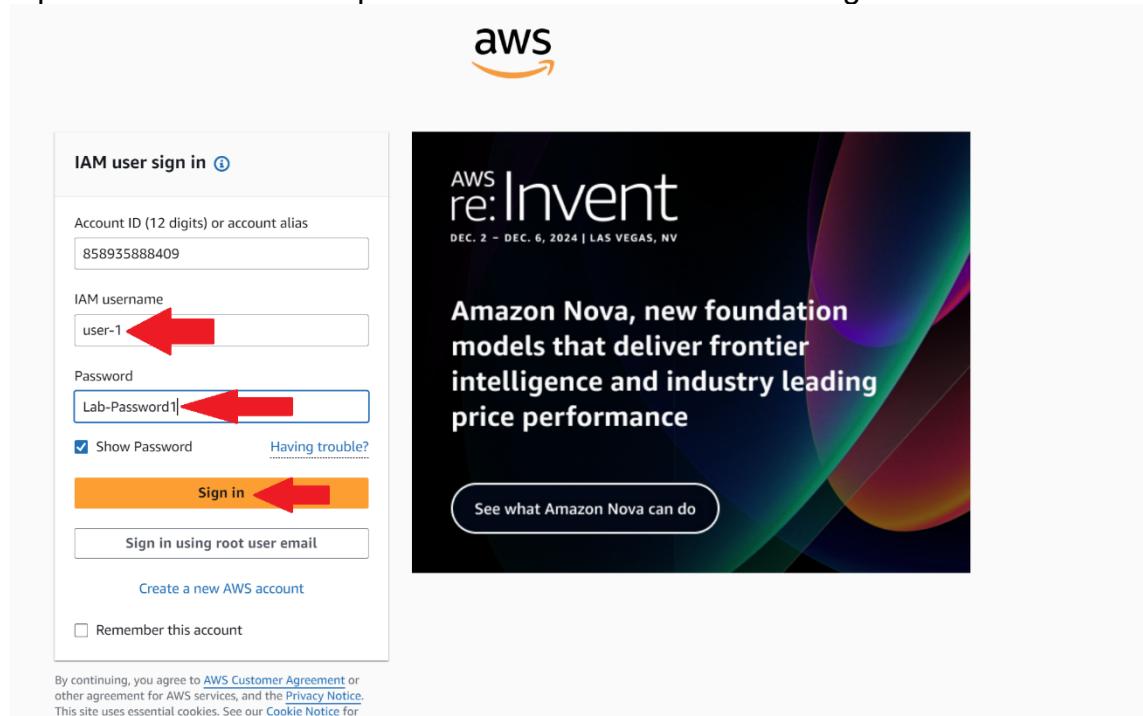
### Sign-in URL for IAM users in this account

https://858935888409.signin.aws.amazon.com/console

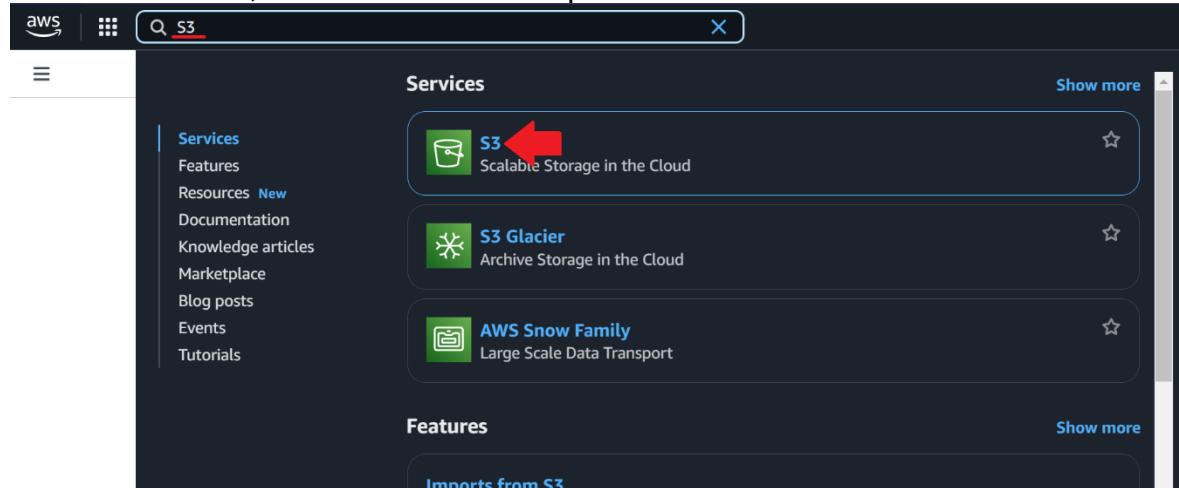
Open a new private browser window and input the URL.



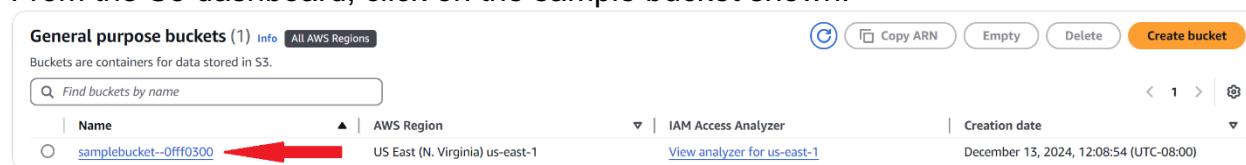
Input the username and password for “user-1” and click “Sign In”.



In the search bar, search for “S3” and open the S3 dashboard.



From the S3 dashboard, click on the sample bucket shown.



If permissions have been set correctly, user-1 should be able to see the objects in the bucket. In this case, there are no objects in the bucket, which should be evident in a message displayed to the user.

samplebucket--0fff0300 [Info](#)

[Objects](#) [Metadata - Preview](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

**Objects (0) [Info](#)**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions.

[Learn more](#)

[Actions](#) [Create folder](#) [Upload](#)

Name	Type	Last modified	Size	Storage class
No objects You don't have any objects in this bucket.				

[Upload](#)

In the search bar, search for “EC2” and open the EC2 dashboard.

aws | [EC2](#)

[Amazon S3](#) [Services](#) [Features](#) [Resources New](#) [Documentation](#)

**Services**

[EC2 Virtual Servers in the Cloud](#)  [EC2 Image Builder](#)

[Show more](#)

**Amazon S3**

**General purpose**

Directory buckets

Table buckets

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access

**Resources**

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

<a href="#">Instances (running)</a>	0	<a href="#">Auto Scaling Groups</a>	API Error	<a href="#">Capacity Reservations</a>	API Error
<a href="#">Dedicated Hosts</a>	API Error	<a href="#">Elastic IPs</a>	API Error	<a href="#">Instances</a>	API Error
<a href="#">Key pairs</a>	API Error	<a href="#">Load balancers</a>	API Error	<a href="#">Placement groups</a>	API Error
<a href="#">Security groups</a>	API Error	<a href="#">Snapshots</a>	API Error	<a href="#">Volumes</a>	API Error

[EC2 Global View](#)

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) [Migrate a server](#)

Note: Your instances will launch in the US East (N. Virginia) Region

**Service health**

An error occurred  
An error occurred retrieving service health information

[Diagnose with Amazon Q](#)

If permissions are set up correctly, the following error will occur:

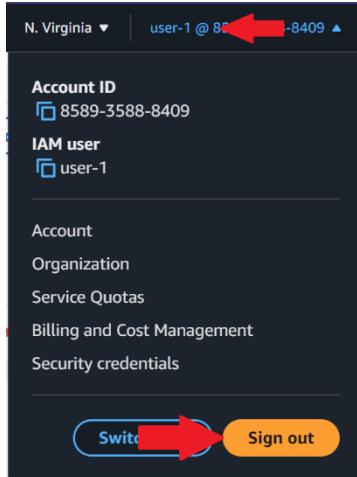
[Instances](#) [Info](#)

[All states](#)

[Instance state = running](#)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP	IPv6 IPs	Monitoring
You are not authorized to perform this operation. User: arn:aws:iam:858935888409:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action											

This is intended behavior, as user-1 is only authorized to access S3 services. Click the “user-1” button in the top right corner and click “Sign Out”.



In the resulting window, click "Sign In".

This screenshot shows the main AWS Management Console page. At the top, there's a navigation bar with links for 'Overview', 'Features', 'Mobile Application', and 'FAQs'. Below that, a breadcrumb trail shows 'Products > Management and Governance > Management Console'. The main title 'AWS Management Console' is prominently displayed. A sub-headline says 'Everything you need to access and manage the AWS Cloud — in one web interface'. At the bottom left, there's a large 'Sign in' button, which has a red arrow pointing to it from the left.

Enter the username and password for user-2 and click "Sign In". Your AWS account ID should be automatically filled, but if it isn't, you can paste the same sign-in URL from before.

This screenshot shows the 'IAM user sign in' form. On the left, there's a sidebar with links for 'Create a new AWS account' and 'Remember this account'. The main form area has fields for 'Account ID (12 digits) or account alias' (containing '858935888409'), 'IAM username' (containing 'user2'), and 'Password' (containing 'Lab-Password2'). There are also checkboxes for 'Show Password' and 'Having trouble?'. At the bottom of the form is an 'Enhance your security' button. To the right of the form is a promotional banner for 're:Invent' with the text 'Explore how to prepare, respond, and recover from security events with AWS Security Incident Response'. A red arrow points to the 'user2' field, another to the 'Lab-Password2' field, and a third to the orange 'Sign in' button at the bottom of the form.

Return to the EC2 dashboard.

Click on “Instances (running)”. You’ll notice a distinct lack of “API Error” messages, unlike the page for user-1.

Resources	
You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:	
<a href="#">Instances (running)</a>	2
<a href="#">Auto Scaling Groups</a>	0
<a href="#">Capacity Reservations</a>	0
<a href="#">Dedicated Hosts</a>	0
<a href="#">Elastic IPs</a>	0
<a href="#">Instances</a>	2
<a href="#">Key pairs</a>	1
<a href="#">Load balancers</a>	0
<a href="#">Placement groups</a>	0
<a href="#">Security groups</a>	3
<a href="#">Snapshots</a>	0
<a href="#">Volumes</a>	2

You’ll notice that the instances will properly display this time. Select the “LabHost” instance.

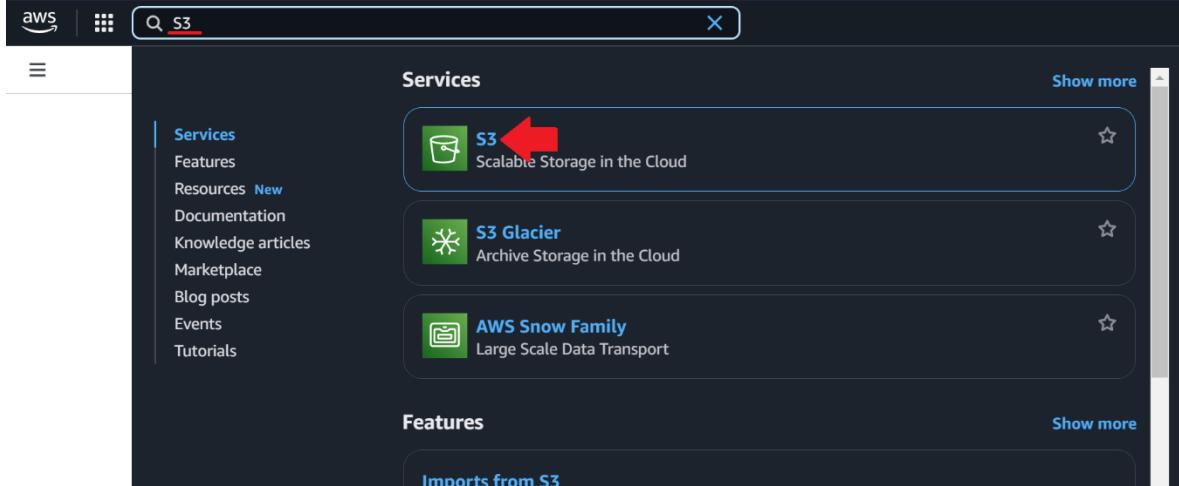
Click on “Instance state” > “Stop Instance”.

Click “Stop”.

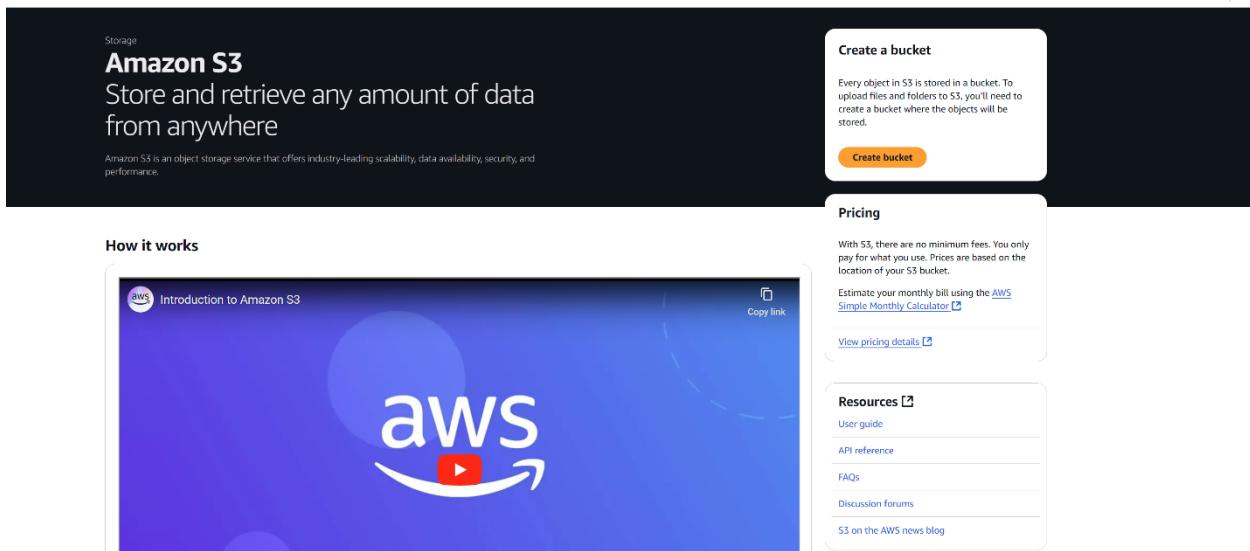
Since user-2 doesn’t have the appropriate permissions, you should get the following error message:



To confirm that user-2 doesn't have access to S3, access the S3 dashboard from the search bar.



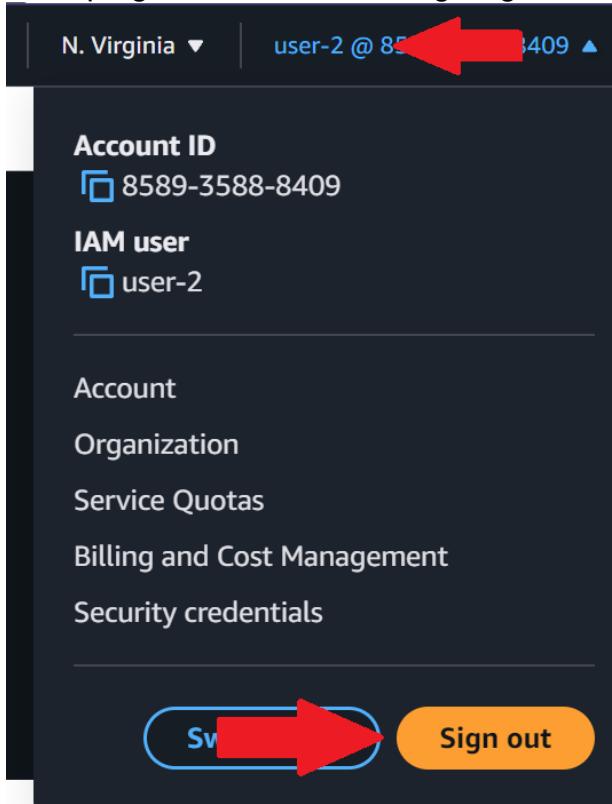
You should see the following page, where it appears that no S3 buckets have been set up (user-2 is unable to see these buckets, so AWS treats them as if they don't exist here).



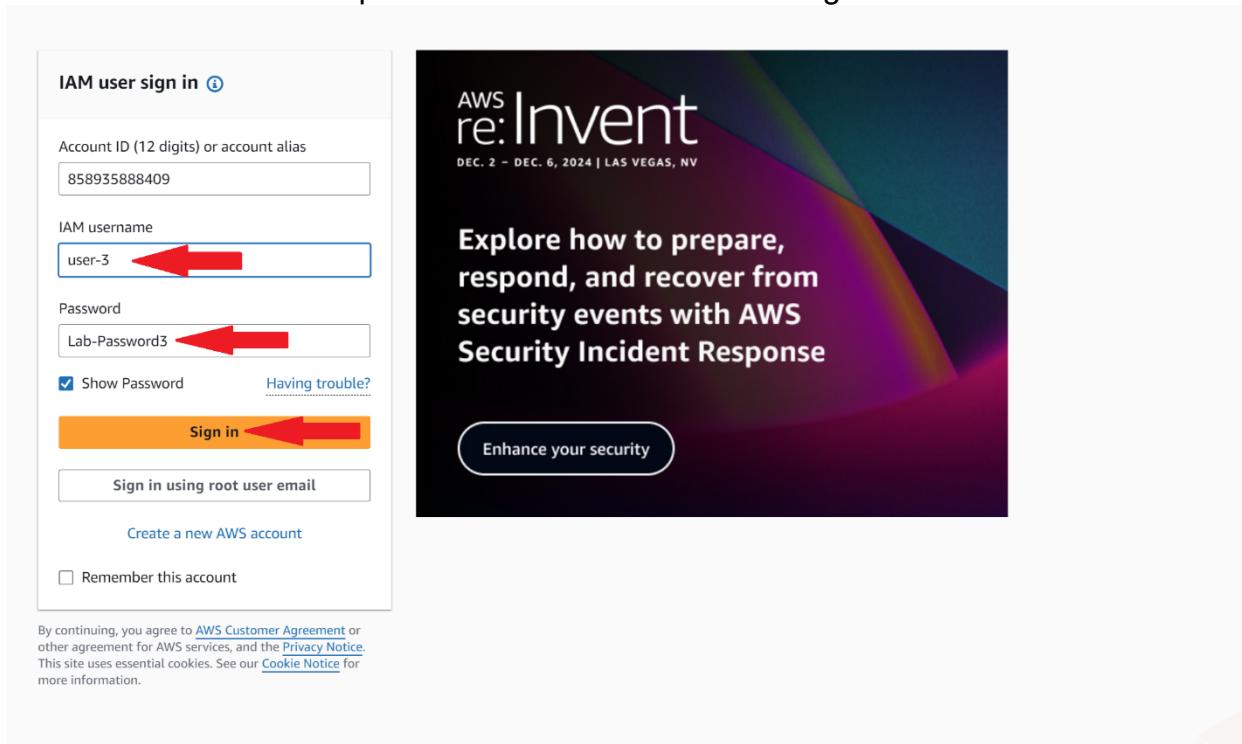
Attempting to create a bucket as user-2 will result in the following error message:



Now, switch to user-3. Sign out of the user-2 account by clicking the “user-2” button in the top right corner and clicking “Sign Out”.



Enter the username and password for user-3 and click “Sign In”.



Return to the EC2 dashboard.

Return to the “Instances (running)” tab.

**Resources**

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	2	Auto Scaling Groups	0 API Error	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	2
Key pairs	1	Load balancers	0 API Error	Placement groups	0
Security groups	3	Snapshots	0	Volumes	2

Select “LabHost” again, and try to stop the instance again.

Instances (1/2) Info

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

Clear filters

Instance state = running

Instance state ▲ Actions ▾

Stop instance

Start instance

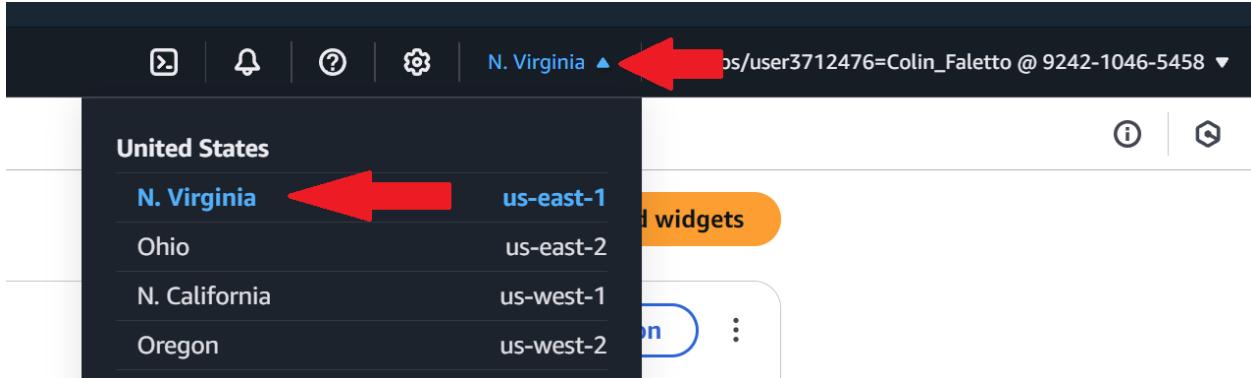
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring
LabHost	i-02157c36a0a841d1c	Running	t2.micro	2/2 checks passed	User: arnaws:	us-east-1a	ec2-44-195-46-204.co...	44.195.46.204	-	-	disabled
Bastion Host	i-0caf67c66b8993fc	Running	t2.micro	2/2 checks passed	User: arnaws:	us-east-1a	ec2-54-234-208-187.co...	34.234.208.187	-	-	disabled

If user-3's permissions are correctly set up, you should see the following success message:

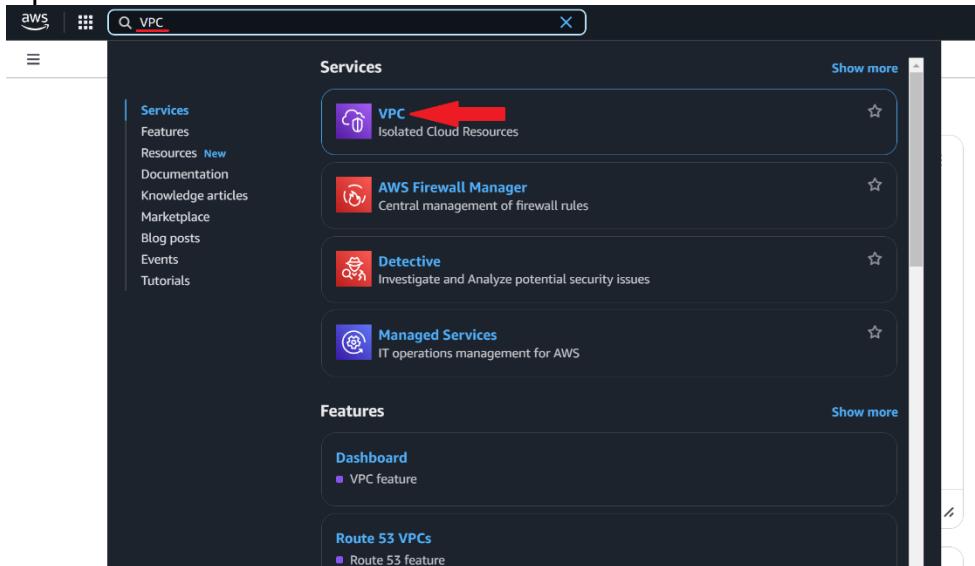
Successfully initiated stopping of i-02157c36a0a841d1c

## Lab Commands (Lab 2 VPC)

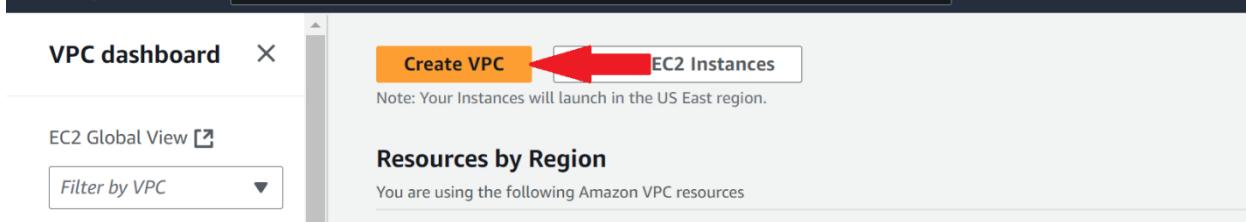
In the AWS management console, ensure that you have the “N. Virginia (us-east-1)” region selected.



Open the VPC dashboard from the search bar.



Click "Create VPC".



Keep all settings on their default values (ensure they match with the screenshot below) besides the following:

- Set "Resources to create" to "VPC and more"
- Set "Name tag auto-generation" to "lab"
- Set "Number of Availability Zones (AZs)" to "1"

**VPC settings**

Resources to create [Info](#)  
Create only the VPC resource or the VPC and other networking resources.

VPC only  VPC and more

Name tag auto-generation [Info](#)  
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

Auto-generate  
lab

IPv4 CIDR block [Info](#)  
Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)  
 No IPv6 CIDR block  
 Amazon-provided IPv6 CIDR block

Tenancy [Info](#)  
Default

Number of Availability Zones (AZs) [Info](#)  
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1  2  3

[▶ Customize AZs](#)

Number of public subnets [Info](#)  
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0  1

Number of private subnets [Info](#)  
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0  1  2

Open the “Customize subnets CIDR blocks” section and ensure that the public and private subnet CIDR blocks are set to 10.0.0.0/24 and 10.0.1.0/24 respectively.

▼ Customize subnets CIDR blocks



Public subnet CIDR block in us-east-1a

10.0.0.0/24

256 IPs

Private subnet CIDR block in us-east-1a

10.0.1.0/24

256 IPs

Set “NAT gateways” to “In 1 AZ”, set “VPC Endpoints” to “None”, and ensure that both boxes under “DNS options” are checked. Verify that the Subnets, Route Tables, and Network connections in the “Preview” section match the screenshot below, then click “Create VPC”.

**NAT gateways (\$)** [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

**None** **In 1 AZ** **1 per AZ**

**VPC endpoints** [Info](#)

Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

**None** **S3 Gateway**

**DNS options** [Info](#)

Enable DNS hostnames  
 Enable DNS resolution

**► Additional tags**

**Cancel** **Preview code** **Create VPC**

**Click after verifying information in "Preview"**

**Preview**

**VPC** [Show details](#)  
Your AWS virtual network  
lab-vpc

**Subnets (2)**  
Subnets within this VPC  
**us-east-1a**  
A lab-subnet-public1-us-east-1a  
A lab-subnet-private1-us-east-1a

**Route tables (2)**  
Route network traffic to resources  
lab-rtb-public  
lab-rtb-private1-us-east-1a

**Network connections (2)**  
Connections to other networks  
lab-igw  
lab-nat-public1-us-east-1a

You should see a window like this while the VPC is being created:

## Create VPC workflow

↳ Create subnet 22%

▼ Details

- Create VPC: vpc-0b119727c01eb831d [🔗](#)
- Enable DNS hostnames
- Enable DNS resolution
- Verifying VPC creation: vpc-0b119727c01eb831d [🔗](#)
- Create subnet
- Create subnet
- Create internet gateway
- Attach internet gateway to the VPC
- Create route table
- Create route
- Associate route table
- Allocate elastic IP
- Create NAT gateway
- Wait for NAT Gateways to activate
- Create route table
- Create route
- Associate route table
- Verifying route table creation

You should see a screen like this when the VPC has finished being created:

VPC > Your VPCs > vpc-0b119727c01eb831d / lab-vpc Actions ▾

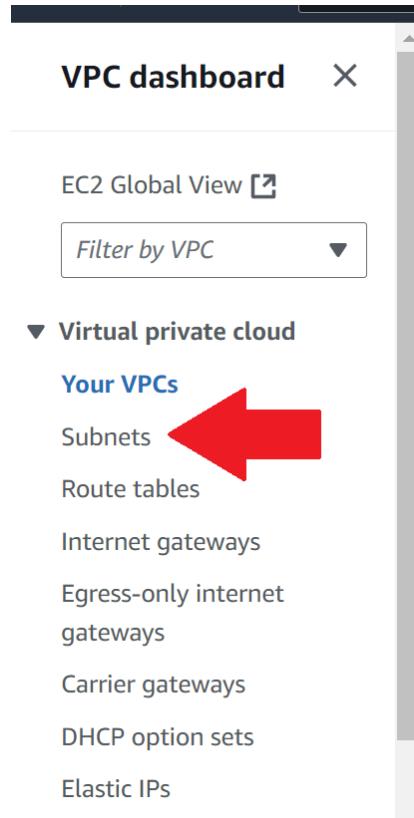
Details		Info	
VPC ID	vpc-0b119727c01eb831d	State	<input checked="" type="radio"/> Available
DNS resolution	Enabled	Tenancy	default
Main network ACL	ad-0766d6c0ef345680e	Default VPC	No
IPv6 CIDR (Network border group)	-	Network Address Usage metrics	Disabled
		Block Public Access	<input type="radio"/> Off
		DHCP option set	dopt-0803267abe9d2ea4e
		IPv4 CIDR	10.0.0.0/16
		Route 53 Resolver DNS Firewall rule groups	-
		Main route table	rtb-073694f2c5b876a0f
		IPv6 pool	-
		Owner ID	924210465458

**Resource map** Info

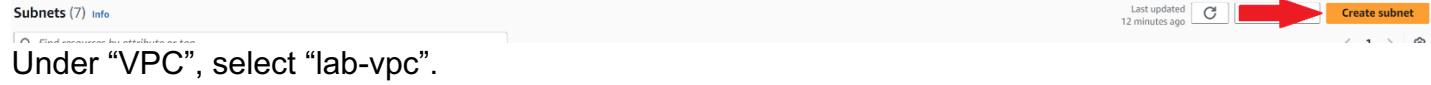
```

graph LR
    VPC[VPC] --- Subnet1[Subnet 1]
    VPC --- Subnet2[Subnet 2]
    Subnet1 --- RTB1[Route Table 1]
    Subnet2 --- RTB2[Route Table 2]
    Subnet2 --- RTB3[Route Table 3]
    RTB1 --- NC1[Network Connection 1]
    RTB2 --- NC2[Network Connection 2]
    RTB3 --- NC3[Network Connection 3]
  
```

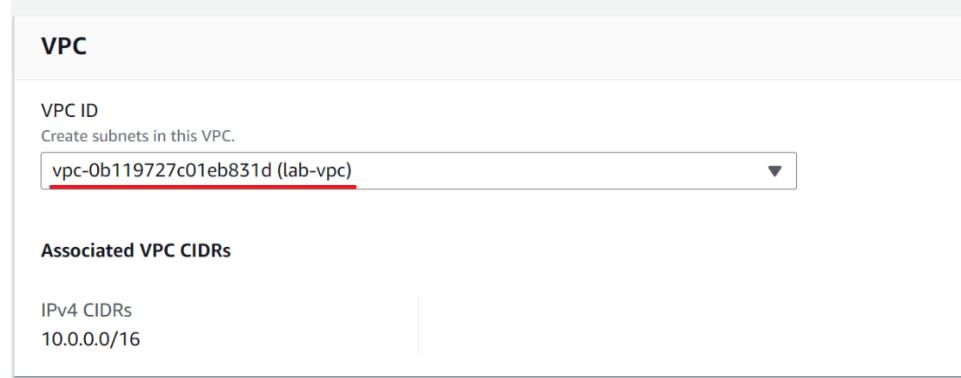
You will now create additional subnets in a second availability zone. From the sidebar, click on “Subnets”.



Click “Create Subnet”.



Under “VPC”, select “lab-vpc”.



Under “Subnet settings”, set the name to “lab-subnet-public2”, the availability zone to “us-east-1b”, and the IPv4 subnet CIDR block to 10.0.2.0/24. Click “Create Subnet”.

**Subnet settings**  
Specify the CIDR blocks and Availability Zone for the subnet.

**Subnet 1 of 1**

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.  
lab-subnet-public2  
The name can be up to 256 characters long.

**Availability Zone** [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.  
US East (N. Virginia) / us-east-1b

**IPv4 VPC CIDR block** [Info](#)  
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.  
10.0.0.0/16

**IPv4 subnet CIDR block**  
10.0.2.0/24 256 IPs

**Tags - optional**

Key	Value - optional
<input type="text" value="Name"/> X	<input type="text" value="lab-subnet-public2"/> X
<a href="#">Add new tag</a>	

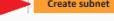
You can add 49 more tags.  
[Remove](#)

[Add new subnet](#)

 **Create subnet**

From the subnet dashboard again, select “Create Subnet” and set the VPC to “lab-vpc” again.

**Subnets (7) [Info](#)**

Last updated  12 minutes ago  **Create subnet**

**VPC**

**VPC ID**  
Create subnets in this VPC.  
vpc-0b119727c01eb831d (lab-vpc)

**Associated VPC CIDRs**

IPv4 CIDRs  
10.0.0.0/16

Under “Subnet settings” this time, set the name to “lab-subnet-private2”, the Availability Zone to “us-east-1b”, and the IPv4 Subnet CIDR block to 10.0.3.0/24. Click “Create Subnet”.

**Subnet settings**  
Specify the CIDR blocks and Availability Zone for the subnet.

**Subnet 1 of 1**

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

**Availability Zone** Info  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

**IPv4 VPC CIDR block** Info  
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

**IPv4 subnet CIDR block**  
 256 IPs

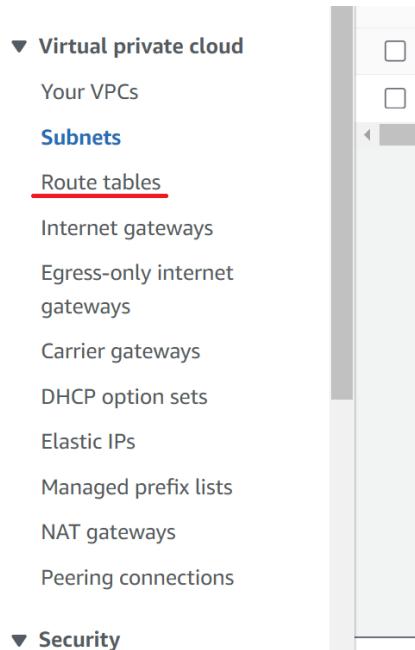
**Tags - optional**

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="lab-subnet-private2"/>

**Add new tag**  
You can add 49 more tags.



Next, set the second private subnet to share a routing table with the first private subnet. Go to the “Route tables” section from the sidebar.



Click on the “Route table ID” hyperlink associated with “lab-rtp-private1-us-east-1a”.

Route tables (6) [Info](#)

Last updated less than a minute ago [Actions](#) [Create route table](#)

[Find resources by attribute or tag](#)

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
-	<a href="#">rtb-073694f2c5b876a0f</a>	-	-	Yes	<a href="#">vpc-0b119727c01eb831d   lab...</a>	924210465458
-	<a href="#">rtb-0a1558d5466896a5</a>	-	-	Yes	<a href="#">vpc-09ec9f5893e09458   Wor...</a>	924210465458
<a href="#">lab-rtb-private1-us-east-1a</a>	<a href="#">rtb-0ac581ded2cd7ba2d</a>	<a href="#">subnet-09f084179558fc...</a>	-	No	<a href="#">vpc-0b119727c01eb831d   lab...</a>	924210465458
-	<a href="#">rtb-04a73cd2d4d287f1c1</a>	-	-	Yes	<a href="#">vpc-072bfefaa0f069148</a>	924210465458
Work Public Route Table	<a href="#">rtb-0be92c5b756f2604</a>	<a href="#">subnet-08cc5bc299a44...</a>	-	No	<a href="#">vpc-09ec9f5893e09458   Wor...</a>	924210465458
<a href="#">lab-rtb-public</a>	<a href="#">rtb-0fa868d8374751624</a>	<a href="#">subnet-04eeff38a38c12...</a>	-	No	<a href="#">vpc-0b119727c01eb831d   lab...</a>	924210465458

Click “Subnet associations”.

rtb-Dac581ded2cd7ba2d / lab-rtb-private1-us-east-1a

[Details](#) [Routes](#) [Subnet associations](#) [Route propagation](#) [Tags](#)

**Details**

Route table ID <a href="#">rtb-0ac581ded2cd7ba2d</a>	Main No	Explicit subnet associations <a href="#">subnet-09f084179558fc24 / lab-subnet-private1-us-east-1a</a>	Edge associations
VPC <a href="#">vpc-0b119727c01eb831d   lab-vpc</a>	Owner ID 924210465458		

Click “Edit subnet associations”.

Explicit subnet associations (1)

[Find subnet association](#)

Name <a href="#">lab-subnet-private1-us-east-1a</a>	Subnet ID <a href="#">subnet-09f084179558fc24</a>	IPv4 CIDR 10.0.1.0/24	IPv6 CIDR
--	--	--------------------------	-----------

Select both private subnets, then click “Save associations”.

Available subnets (2/2)

<input checked="" type="checkbox"/> Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/> lab-subnet-public2	<a href="#">subnet-087125fb16f87168a</a>	10.0.2.0/24	-	Main (rtb-073694f2c5b876a0f)
<input checked="" type="checkbox"/> lab-subnet-private1-us-east-1a	<a href="#">subnet-09f084179558fc24</a>	10.0.1.0/24	-	<a href="#">rtb-0ac581ded2cd7ba2d / lab-rtb-private1-us-east-1a</a>
<input type="checkbox"/> lab-subnet-public1-us-east-1a	<a href="#">subnet-04eeff38a38c122797</a>	10.0.0.0/24	-	<a href="#">rtb-0fa868d8374751624 / lab-rtb-public</a>
<input checked="" type="checkbox"/> lab-subnet-private2	<a href="#">subnet-03c1c5e984e277901</a>	10.0.3.0/24	-	Main (rtb-073694f2c5b876a0f)

Selected subnets

<a href="#">subnet-09f084179558fc24 / lab-subnet-private1-us-east-1a</a>	<a href="#">subnet-03c1c5e984e277901 / lab-subnet-private2</a>
--	--

[Save associations](#)

Return to the “Route tables” page. Click on the “Route table ID” hyperlink of the “lab-rtp-public” table.

Route tables (6) [Info](#)

Last updated less than a minute ago [Actions](#) [Create route table](#)

[Find resources by attribute or tag](#)

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	Owner ID
-	<a href="#">rtb-073694f2c5b876a0f</a>	-	-	Yes	<a href="#">vpc-0b119727c01eb831d   lab...</a>	924210465458
-	<a href="#">rtb-0a1558d5466896a5</a>	-	-	Yes	<a href="#">vpc-09ec9f5893e09458   Wor...</a>	924210465458
<a href="#">lab-rtb-private1-us-east-1a</a>	<a href="#">rtb-0ac581ded2cd7ba2d</a>	<a href="#">subnet-09f084179558fc...</a>	-	No	<a href="#">vpc-0b119727c01eb831d   lab...</a>	924210465458
-	<a href="#">rtb-04a73cd2d4d287f1c1</a>	-	-	Yes	<a href="#">vpc-072bfefaa0f069148</a>	924210465458
Work Public Route Table	<a href="#">rtb-0be92c5b756f2604</a>	<a href="#">subnet-08cc5bc299a44...</a>	-	No	<a href="#">vpc-09ec9f5893e09458   Wor...</a>	924210465458
<a href="#">lab-rtb-public</a>	<a href="#">rtb-0fa868d8374751624</a>	<a href="#">subnet-04eeff38a38c12...</a>	-	No	<a href="#">vpc-0b119727c01eb831d   lab...</a>	924210465458

Click “Subnet associations”.

rtb-0fa868d8374751624 / lab-rtb-public

- [Details](#)
- [Routes](#)
- [Subnet associations](#) (highlighted)
- [Route propagation](#)
- [Tags](#)

**Details**

Route table ID rtb-0fa868d8374751624	Main No	Explicit subnet associations subnet-04eef38a38c122297 / lab-subnet-public1-us-east-1a	Edge -
VPC vpc-0b119727c01eb851d   lab-vpc	Owner ID 924210465458		

Click “Edit subnet associations”.

Explicit subnet associations (1)

[Edit subnet associations](#) (highlighted)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lab-subnet-public1-us-east-1a	subnet-04eef38a38c122297	10.0.0.0/24	-

Select both public subnets, then click “Save associations”.

Available subnets (2/4)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
lab-subnet-public2	subnet-097125fb16f8716ba	10.0.2.0/24	-	Main (rtb-073694f2c5b476a0f)
lab-subnet-private1-us-east-1a	subnet-09f0841795588f24	10.0.1.0/24	-	rtb-0ac581ded2cd7ba2d / lab-rtb-private1-us-east-1a
lab-subnet-public1-us-east-1a	subnet-04eef38a38c122297	10.0.0.0/24	-	rtb-0fa868d8374751624 / lab-rtb-public
lab-subnet-private2	subnet-05c13e984c277901	10.0.3.0/24	-	rtb-0ac581ded2cd7ba2d / lab-rtb-private1-us-east-1a

Selected subnets

[Filter by VPC](#)

[Save associations](#) (highlighted)

Next, you will configure a security group to permit HTTP access to a web server. Go to the “Security groups” page from the sidebar.

- [▼ Virtual private cloud](#)
  - [Your VPCs](#)
  - [Subnets](#)
- [Route tables](#)
  - [Internet gateways](#)
  - [Egress-only internet gateways](#)
  - [Carrier gateways](#)
  - [DHCP option sets](#)
  - [Elastic IPs](#)
  - [Managed prefix lists](#)
  - [NAT gateways](#)
  - [Peering connections](#)
- [▼ Security](#)
  - [Network ACLs](#)
  - [Security groups](#) (highlighted)

Click “Create security group”.

Security Groups (4) [Info](#)

[Actions](#) (highlighted) [Create security group](#)

Under “Basic details”, set the name to “Web Security Group”, the description to “Enable HTTP Access”, and the VPC to “lab-vpc”.

**Basic details**

Security group name [Info](#)  
Web Security Group  
Name cannot be edited after creation.

Description [Info](#)  
Enable HTTP access

VPC [Info](#)  
vpc-0b119727c01eb831d (lab-vpc)

Under “Inbound rules”, click “Add rule”.

**Inbound rules** [Info](#)

This security group has no inbound rules.

Add rule

Set the rule type to “HTTP”, the source to “Anywhere-IPv4”, and the description to “Permit web requests”. Click “Add rule”.

**Inbound rules** [Info](#)

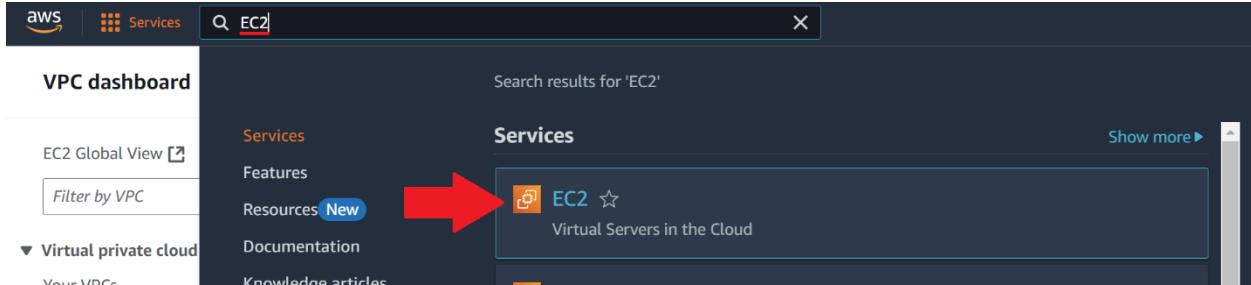
Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Anywhere-IPv4	Permit web requests

Add rule

Click “Create security group”.

Create security group

Next, we will create a web server with this security group applied. Open the EC2 dashboard from the search bar.



Click “Launch instance”.

A screenshot of the 'Launch instance' page. The title is 'Launch instance'. Below it, a sub-instruction says 'To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.' There are two buttons: 'Launch instance' (highlighted with a red border) and 'Migrate a server'. A note below states 'Note: Your instances will launch in the US East (N. Virginia) Region'.

Set the name to “Web Server 1” and set the Amazon Machine Image to “Amazon Linux 2023 AMI”.

A screenshot of the 'Launch an instance' configuration page. It starts with a 'Name and tags' section where 'Web Server 1' is entered into the 'Name' field. Below that is the 'Application and OS Images (Amazon Machine Image)' section, which is currently expanded. It shows a search bar and a grid of OS icons. One icon for 'Amazon Linux' is highlighted with a red border. The 'Amazon Machine Image (AMI)' section shows 'Amazon Linux 2023 AMI' selected, with its details: AMI ID 'ami-045sec754f44f9a4a', 'Free tier eligible', and 'Virtualization: hvm'. At the bottom, there are dropdowns for 'Architecture' (set to '64-bit (x86)'), 'Boot mode' ('uefi-preferred'), 'AMI ID' ('ami-045sec754f44f9a4a'), 'Username' ('ec2-user'), and 'Verified provider'.

Set the instance type to “t2.micro”.

## ▼ Instance type [Info](#) | [Get advice](#)

### Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true  
On-Demand Windows base pricing: 0.0162 USD per Hour  
On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour  
On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.026 USD per Hour  
On-Demand Linux base pricing: 0.0116 USD per Hour

Free tier eligible

All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

Set the Key pair to “vockey”.

## ▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

### Key pair name - required

vockey

[Create new key pair](#)

Under “Network settings”, set the VPC to “lab-vpc”, the subnet to “lab-subnet-public2”, and “Auto-assign public IP” to “Enable”. Set the “Firewall (security groups)” to “Select existing security groups” and add the “Web Security Group” created earlier.

## ▼ Network settings [Info](#)

### VPC - required [Info](#)

vpc-0b119727c01eb831d (lab-vpc)  
10.0.0.0/16

[Create new VPC](#)

### Subnet [Info](#)

subnet-0b7125fb16f87168a lab-subnet-public2  
VPC: vpc-0b119727c01eb831d Owner: 924210465458 Availability Zone: us-east-1b  
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.2.0/24

[Create new subnet](#)

### Auto-assign public IP [Info](#)

Enable

Additional charges apply when outside of free tier allowance

### Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

### Common security groups [Info](#)

Select security groups

[Compare security group rules](#)

Web Security Group sg-0380efff0878eebab X  
VPC: vpc-0b119727c01eb831d

Security groups that you add or remove here will be added to or removed from all your network interfaces.

### ► Advanced network configuration

Under “Configure storage”, set the storage to 8 Gibabytes.

**Configure storage** [Info](#) [Advanced](#)

1x  GiB [gp3](#) [▼](#) Root volume (Not encrypted)

[Free tier eligible customers can get up to 30 GB of EBS General Purpose \(SSD\) or Magnetic storage](#) [X](#)

[Add new volume](#)

[Click refresh to view backup information](#)

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

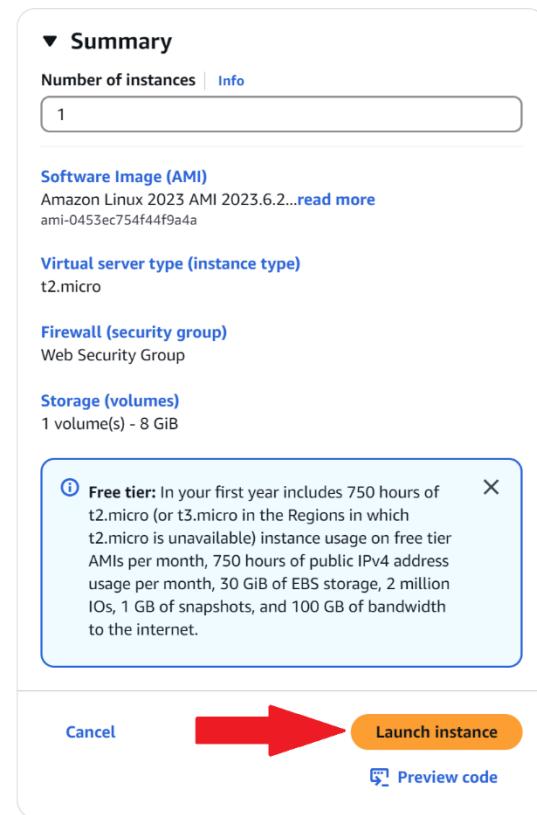
Open the “Advanced details” tab.

## ▼ Advanced details [Info](#)

Scroll down to the “User data” section.

Add the following script:

```
#!/bin/bash
# Install Apache Web Server and PHP
dnf install -y httpd wget php mariadb105-server
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-
TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
Click “Launch Instance”.
```



Click “View All Instances”.

**View all instances**

Click the checkbox next to “Web Server 1”.



After the “Status Check” section says “2/2 checks passed”, look for the public IPv4 address of the server and click the button to open the URL in a new tab:

i-0f8cef3e324f29f82 (Web Server 1)

**Details** Status and alarms | Monitoring | Security | Networking | Storage | Tags

**Instance summary** [Info](#)

**Instance ID** [i-0f8cef3e324f29f82](#)

**IPv6 address** —

**Hostname type** IP name: ip-10-0-2-165.ec2.internal

**Answer private resource DNS name** —

**Auto-assigned IP address** [3.237.181.14 \[Public IP\]](#)

**Public IPv4 address** [3.237.181.14 | open address](#)

**Instance state** [Running](#)

**Private IP DNS name (IPv4 only)** [ip-10-0-2-165.ec2.internal](#)

**Instance type** t2.micro

**VPC ID** [vpc-0b119727c01eb831d \(lab-vpc\)](#)

**Private IPv4 addresses** [10.0.2.165](#)

**Public IPv4 DNS** [ec2-3-237-181-14.compute-1.amazonaws.com | open address](#)

**Elastic IP addresses** —

**AWS Compute Optimizer finding** [Opt-in to AWS Compute Optimizer for recommendations.](#) | Learn more

If done correctly, a page like this should open:

Instances | EC2 | us-east-1 | Welcome to AWS Technical +

← → Q ⓘ Not Secure ec2-3-237-181-14.compute-1.amazonaws.com

Home Shopping Travel Bookmarks AWS Canvas

aws Load Test RDS

Meta-Data	Value
InstanceId	i-0f8cef3e324f29f82
Availability Zone	us-east-1b

Current CPU Load: 7%

## Lab Commands (Lab 3 EC2)

Open the EC2 console from the search bar.

aws | EC2

Services

**EC2** Virtual Servers in the Cloud

**EC2 Image Builder** A managed service to automate build, customize and deploy OS images

Show more

Ensure you have the North Virginia region selected.

N. Virginia ▲

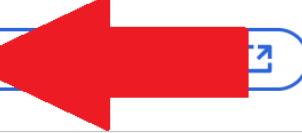
Region	Region Name
United States	
<b>N. Virginia</b>	<b>us-east-1</b>
Ohio	us-east-2
N. California	us-west-1
S. California	us-west-2

From the EC2 homepage, select “Launch Instance”.

## Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

**Launch instance**



Note: Your instances will launch in the US East (N. Virginia) Region

Name this instance “Web Server”.

### Name and tags Info

Name

**Web Server**

[Add additional tags](#)

Set the AMI to “Amazon Linux 2023 AMI” and set the instance type to “t2.micro”.

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Q Search our full catalog including 1000s of application and OS images

Recent [Quick Start](#)

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI ami-04d3e754f4495a4a (64-bit x86, uefi preferred) / ami-0fb53c778a23014a (64-bit x86, uefi) Free tier eligible

Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20241121.0.x86\_64 HVM kernel-6.1

Architecture Boot mode AMI ID Username

64-bit (x86) uefi-preferred ami-04d3e754f4495a4a ec2-user Verified provider

▼ Instance type Info | Get advice

Instance type

t2.micro 1 vCPU 1 GB Memory Current generation: true

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour On-Demand RHEL base pricing: 0.0216 USD per Hour

All generations Compare instance types

Set the key pair to “vockey”.

### ▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - **required**

**vockey**

[Create new key pair](#)

Under “Network Settings”, click “Edit”.

### ▼ Network settings Info



**Edit**

Set the VPC to “Lab VPC”, the subnet to “Public Subnet 1”, and the “Auto-Assign Public IP” setting to “enable”. Create a new security group with the name “Web Server security group” and the description “Security group for my web server”.

**▼ Network settings [Info](#)**

**VPC - required [Info](#)**  
vpc-0880e90346060a779 (Lab VPC)  
10.0.0.0/16

**Subnet [Info](#)**  
subnet-03978ef8e7d5c0fa7  
VPC: vpc-0880e90346060a779 Owner: 938883298313 Availability Zone: us-east-1a  
Zone type: Availability Zone IP addresses available: 1 CIDR: 10.0.1.0/28

**Auto-assign public IP [Info](#)**  
Enable

Additional charges apply when outside of free tier allowance

**Firewall (security groups) [Info](#)**  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group    Select existing security group

**Security group name - required**  
Web Server security group

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-:/()#,@[]+=&;!\$^\*

**Description - required [Info](#)**  
Security group for my web server

**Inbound Security Group Rules**

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
ssh	TCP	22
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere	Add CIDR, prefix list or security group 0.0.0.0/0 X	e.g. SSH for admin desktop

Make sure to remove “Security group rule 1”.

**Inbound Security Group Rules**

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>
ssh	TCP	22
Source type <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
Anywhere	Add CIDR, prefix list or security group 0.0.0.0/0 X	e.g. SSH for admin desktop

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. X

[Add security group rule](#)

Under “Configure storage”, select 8 GiB of gp3.

Configure storage [Info](#)

1x  GiB  Root volume (Not encrypted)

[Add new volume](#)

ⓘ Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage [X](#)

ⓘ Click refresh to view backup information  
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

Go to the Advanced Details section.

Advanced details [Info](#)

Termination protection [Info](#)

[Edit](#)

Enter the following into the “User Data” section:

```
#!/bin/bash
dnf install -y httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hello From Your Web Server!</h1></html>' >
/var/www/html/index.html
```

**User data - optional** | [Info](#)

Upload a file with your user data or enter it in the field.

[Choose file](#)

```
#!/bin/bash
dnf install -y httpd
systemctl enable httpd
systemctl start httpd
echo <html><h1>Hello From Your Web Server!</h1></html>' >
/var/www/html/index.html
```

Under the “Summary” section, click “Launch Instance”.

▼ **Summary**

Number of instances | [Info](#)

1

Software image (AMI)

Amazon Linux 2023 AMI 2023.6.2...[read more](#)

ami-0452cc754f44f9a4a

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 GiB

**ⓘ Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GiB of bandwidth to the internet.

[Cancel](#)  [Launch instance](#) [Preview code](#)

After launching the EC2 instance, click “View all instances”.

**View all instances**

Wait for your web server to have the instance state of “Running”, then click the checkbox next to it.

<input type="checkbox"/>  Web Server	i-010cc7662e674e509	 <a href="#">Running</a>  	t2.micro	 2/2 checks passed	
---	---------------------	---	----------	---	---

Under the “Status and Alarms” tab, ensure that both reachability checks have passed.

i-010cc7662e674e509 (Web Server)

Status and alarms | Monitoring | Security | Networking | Storage | Tags

**Status checks info**

Status checks detect problems that may impair i-010cc7662e674e509 (Web Server) from running your applications.

**System status checks**

- System reachability check passed** (Green)

**Instance status checks**

- Instance reachability check passed** (Green)

Metrics | Alarms

Click “Actions > Monitor and troubleshoot > Get system log”.

Instances (1/2) info

Last updated 8 minutes ago

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4...	Elastic IP
Bastion Host	i-0d1ef06d0dcf8b63	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	us-east-1a	ec2-54-175-224-0.com...	-	-
Web Server	i-010cc7662e674e509	Running	t2.micro	2/2 checks passed	<a href="#">View alarms +</a>	us-east-1a	ec2-54-166-154-62.co...	54.166.154.62	-

**Actions**

- Connect
- Instance state
- Launch instances
- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

**Get system log**

- Get Instance screenshot
- Manage detailed monitoring
- Manage CloudWatch alarms
- Configure CloudWatch agent
- EC2 serial console
- Replace root volume
- Fleet Manager
- Instance audit

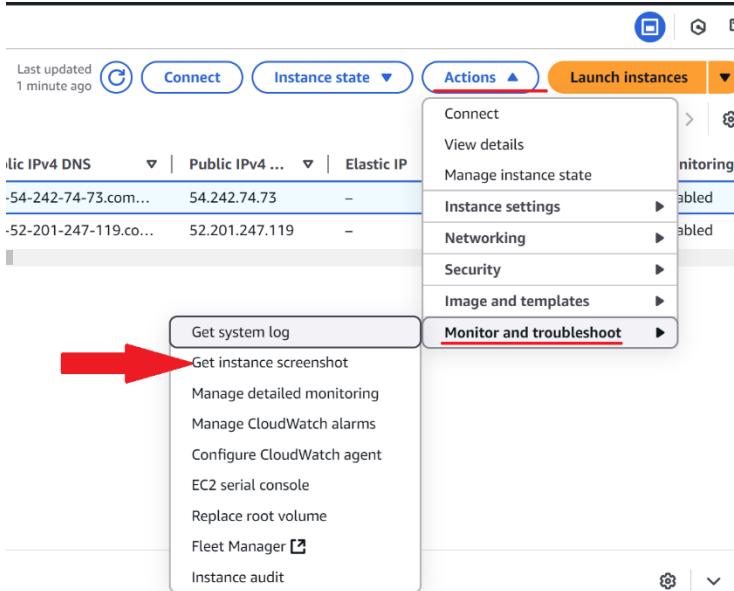
If done correctly, you should see a reference to the “httpd” service started in the User Data section.

**System log**

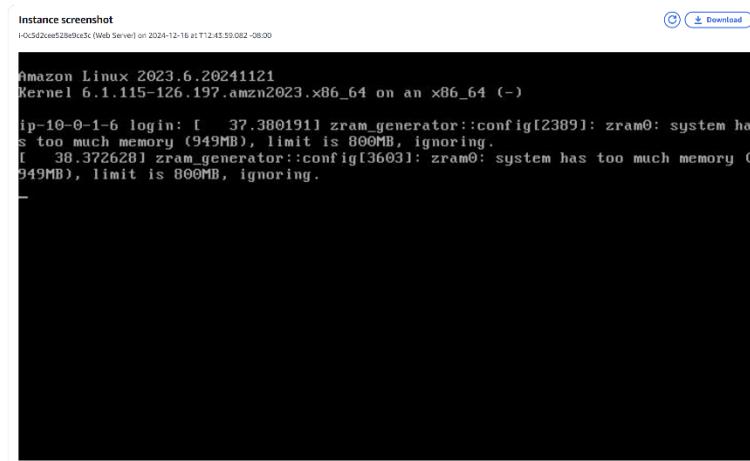
Review system log for instance i-0c5d2cee528e9ce5c as of Mon Dec 16 2024 12:48:21 GMT-0800 (Pacific Standard Time)

```
[ 38.935061] cloud-init[2221]: mod_lua-2.4.62-1.amzn2023.x86_64
[ 38.937650] cloud-init[2221]: Complete!
[ 39.045738] cloud-init[2221]: Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ 38.372628] zram_generator::config[3603]: zram0: system has too much memory (949MB), limit is 800MB, ignoring.
ci-info: +-----+-----+-----+-----+-----+
ci-info: | Keypair | Fingerprint (sha256) | Options | Comment |
ci-info: +-----+-----+-----+-----+-----+
ci-info: | ssh-rsa | e6:7b:08:96:5e:49:f2:5a:1c:c0:35:50:60:64:57:60:66:aa:ac:a4:07:51:83:14:b2:fd:80:47:a1:a0:19:15 | - | vockey |
ci-info: +-----+-----+-----+-----+-----+
<14>Dec 16 20:38:32 cloud-init: #####
<14>Dec 16 20:38:32 cloud-init: #####
<14>Dec 16 20:38:32 cloud-init: BEGIN SSH HOST KEY FINGERPRINTS-----
<14>Dec 16 20:38:32 cloud-init: 256 SHA256:R8/o3wyXrKCFjeB/xH4XTcarGv1tx8FfdNl13ZaONQ root@ip-10-0-1-6.ec2.internal (EDDSA)
<14>Dec 16 20:38:32 cloud-init: 256 SHA256:9mpjPVLFvEfuQosx2rt8mjZv6cc2iZNzSj1l002AA root@ip-10-0-1-6.ec2.internal (ED25519)
<14>Dec 16 20:38:32 cloud-init: END SSH HOST KEY FINGERPRINTS-----
<14>Dec 16 20:38:32 cloud-init: #####
----BEGIN SSH HOST KEY KEYS-----
ecdsa-sha2-nistp256 AAAEAV2Vj7HNnLXwYTIbm1zdHAyNTYAAAAIbmlzdHJhdHByb3VtYAAABBBlw1A0AOw964nDAw9TYFmV1vspG09QU3gtfBQjyOT/q+QbBGFGE2Gy5m8pkSGtngcmJB8c7DbaN7td4Hgq= root@ip-10-0-1-6
ssh-ed25519 AAAAC3zaC1lZDI1NTE5AAAAIj5BFhhqnjdXkajb6+H0Woy1SVi+HTgdFnMzdimEk root@ip-10-0-1-6.ec2.internal
----END SSH HOST KEY KEYS-----
[ 39.695104] cloud-init[2221]: Cloud-init v. 22.2.2 finished at Mon, 16 Dec 2024 20:38:32 +0000. Datasource DataSourceEc2. Up 39.68 seconds
```

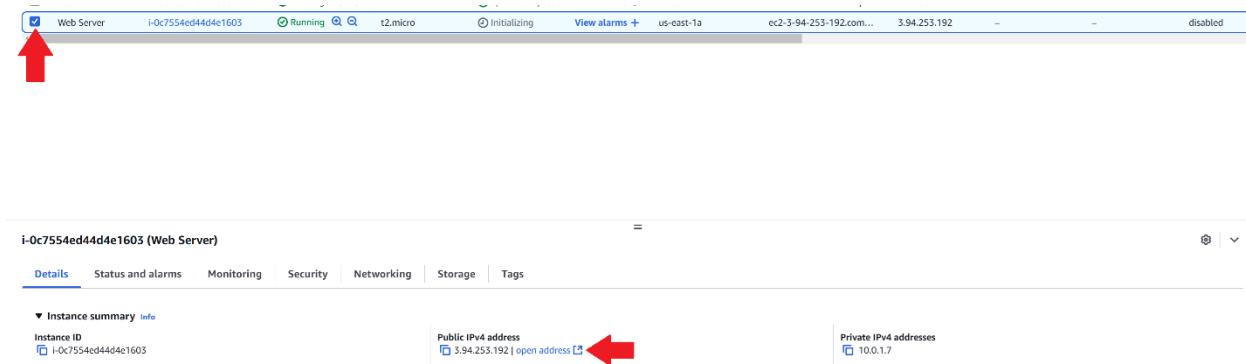
Return to the instances page and click Actions > Monitor and troubleshoot > Get instance screenshot.



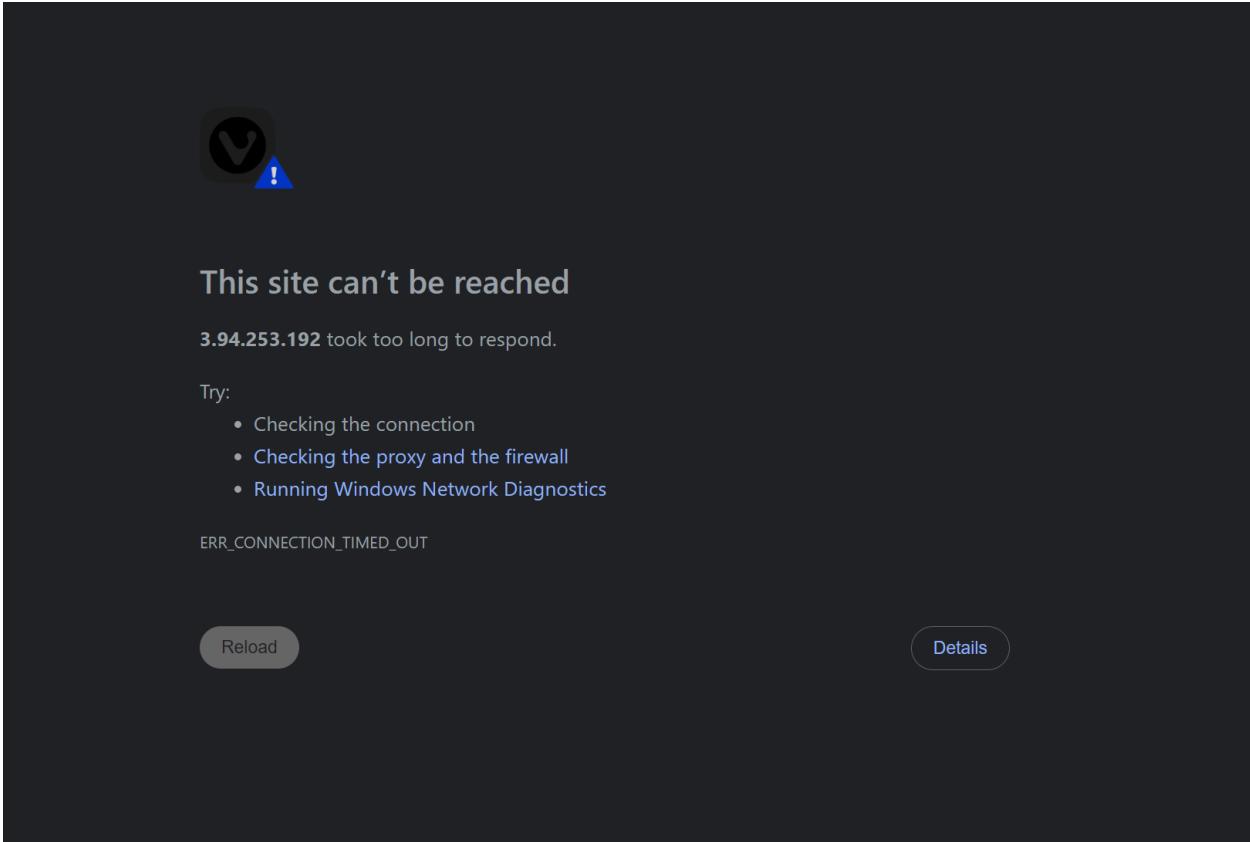
You should see a screenshot similar to this:



On the instances page, select Web Server and click open address under the Public IPv4 address field.



You should see an error message. This is because the security group for the instance has not yet been configured to permit HTTP access.



Next, you will configure a security group for the EC2 instance. Go to Security Groups > Select Web server security group > Inbound rules > Edit inbound rules.

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
-	sg-0695acd804598b6cf	Web Server security group	vpc-0a6beeb89ad58a20	Security group for my web server	938883298313	0 Permission entries
-	sg-067074f8bd45cbea	default	vpc-08999b8a094549728	default VPC security group	938883298313	1 Permission entry
-	sg-09faef115c87cc67	default	vpc-077657e50047d703b	default VPC security group	938883298313	1 Permission entry
-	sg-0ff7f7777d4e81b1	I25SecurityGroup	vpc-08999b8a094549728	VPC Security Group	938883298313	1 Permission entry
-	sg-0ddaa46a8e70ca0b	default	vpc-0a6beeb89ad58a20	default VPC security group	938883298313	1 Permission entry

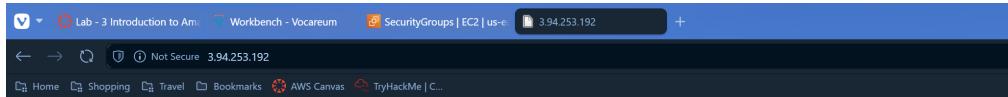
Click Add rule, set the type to HTTP, the source to Anywhere-IPv4, then click Save rules.

### Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

The screenshot shows the 'Edit inbound rules' section of the AWS Security Groups interface. It includes fields for Security group rule ID, Type (HTTP), Protocol (TCP), Port range (80), Source (Anywhere...), and Description (optional). A note at the bottom says: '⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.' The 'Save rules' button is highlighted with a red arrow.

Refresh the web server page. You should see the following message:

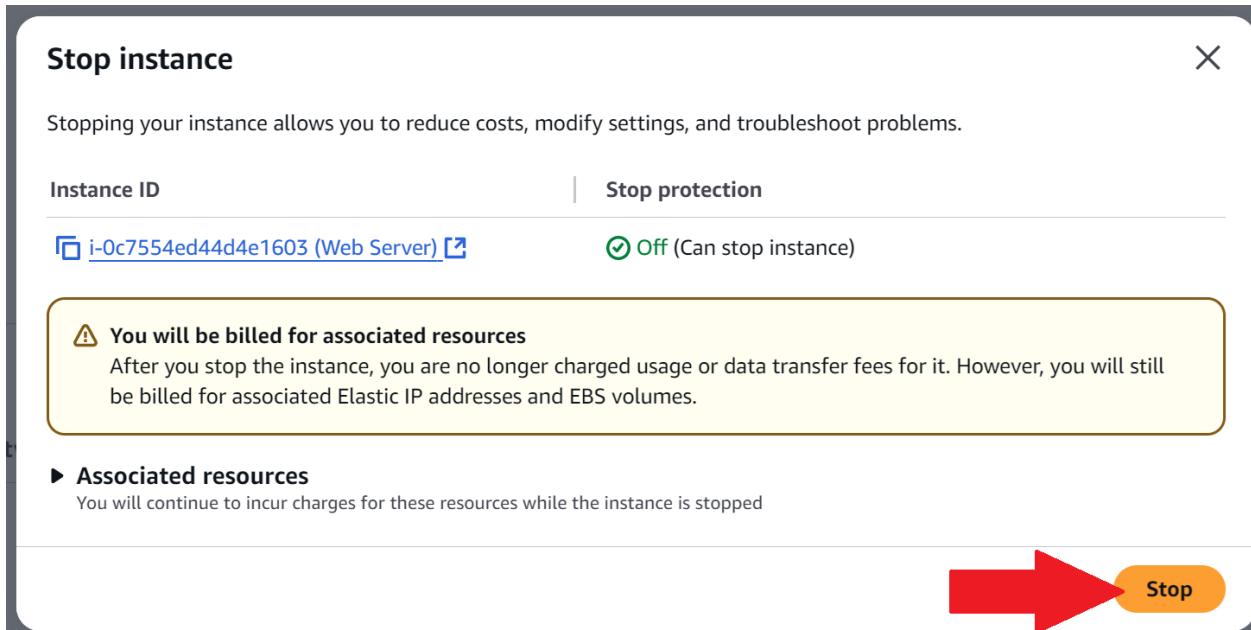


Hello From Your Web Server!

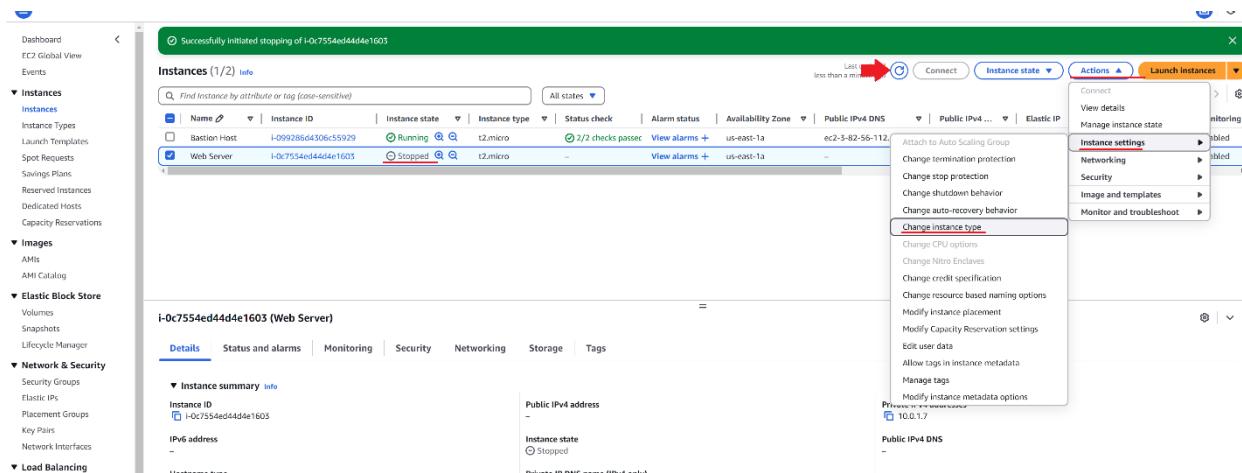
Next, you will resize the instance. Go to Instances > Select Web Server > Instance state > Stop instance.

The screenshot shows the AWS Instances page with one instance listed: 'Web Server' (i-0c7554ed44d4e1603). The 'Actions' dropdown menu is open, and the 'Stop instance' option is highlighted with a red arrow.

Click Stop.



Click the refresh icon until the instance state shows Stopped, then go to Actions > Instance settings > Change instance type.



Set the instance type to t2.small, then click Change.

**Change instance type** [Info](#) | [Get advice](#)

You can change the instance type only if the current instance type and the instance type that you want are compatible.

Instance ID	i-0c755e4d44de1603 (Web Server)	
Current instance type	t2.micro	
New instance type	<input type="text" value="t2.small"/> <a href="#">X</a>	
<input checked="" type="checkbox"/> EBS-optimized		
EBS-optimized is not supported for this instance type.		
<b>Instance type comparison</b>		
Attribute	t2.micro	t2.small
On-Demand Linux pricing	0.0116 USD per Hour	0.0230 USD per Hour
On-Demand Windows pricing	0.0162 USD per Hour	0.0320 USD per Hour
vCPUs	1 (1 core)	1 (1 core)
Memory (MB)	1024	2048
Storage (GB)	-	-
Supported root device types	ebs	ebs
Network performance	Low to Moderate	Low to Moderate
Architecture	32-bit	32-bit
Runnable	true	true
Free-tier eligible	true	false
Current generation	true	true

[Compare more instance type attributes](#)

**Advanced details**

The t2.small instance type does not support changing CPU options.

[Change](#)

Go to Actions > Instance settings > Change stop protection.

Instance type changed successfully.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP	Elastic IP	IPv6 IPs	Monitoring	Security group name
Bastion Host	i-0923661506c5529	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a> +	us-east-1a	ec2-5-82-56-112.comp...	58.256.112	-	-	<input type="checkbox"/>	<a href="#">Attach to Auto Scaling Group</a>
Web Server	i-0c755e4d44de1603	Stopped	t2.small	-	<a href="#">View alarms</a> +	us-east-1a	-	-	-	-	<input type="checkbox"/>	<a href="#">Change termination protection</a>

[Change stop protection](#)

Actions ▾ [Connect](#) [Launch instances](#)

- [View details](#)
- [Manage instance state](#)
- [Instance settings](#) **Change stop protection**
- [Networking](#)
- [Security](#)
- [Image and templates](#)
- [Monitor and troubleshoot](#)

Click Enable, then click save.

**Change stop protection** [Info](#)

Enable stop protection to prevent your instance from being accidentally stopped.

Instance ID	i-0c5d2cee528e9ce3c (Web Server)
Stop protection	<input checked="" type="checkbox"/> Enable

[Save](#)

Next, go to the web server's Storage tab..

### i-0c5d2cee528e9ce3c (Web Server)

[Details](#) [Status and alarms](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

Select the volume created earlier, then click Actions > Modify volume.

Volumes (1/1) [Info](#)

Saved filter sets [Choose filter set](#)

<input checked="" type="checkbox"/>	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Created	Availability Zone	Volume state	Actions
<input checked="" type="checkbox"/>	vol-090fbf8a754c4cf2a	gp3	8 GiB	3000	125		snap-0938e31...	2024/12/16 12:37 GMT-8	us-east-1a	<span>In-use</span>	<a href="#">Actions</a> <a href="#">Create volume</a>

Change the size to 10 GiB.

Volume type | [Info](#)

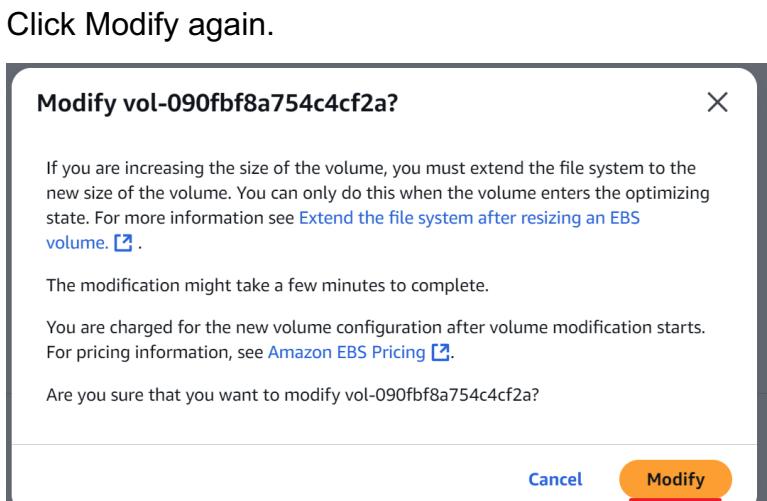
General Purpose SSD (gp3)

Size (GiB) | [Info](#)

Min: 1 GiB, Max: 16384 GiB.

Click Modify.

[Cancel](#) [Modify](#)



Return to the Instances section of the EC2 dashboard.

## ▼ Instances

### Instances

Instance Types

Launch Templates

Spot Requests

Select Web Server and click Instance state > Start instance.

Name	Instance ID	Instance state	Instance type	Status check t	Alarm status	Availability Zone	Public IPv4 DNS	Public IP
Web Server	i-0c5d2cee528e9ce3c	Stopped	t2.small	-	<a href="#">View alarms</a>	us-east-1a	-	-
Bastion Host	i-09e4cc6b7f5fee95c	Running	t2.micro	...	<a href="#">View alarms</a>	us-east-1a	ec2-52-201-247-119.co...	52.201.247.119

While the EC2 instance is starting, go to the Service Quotas dashboard from the search bar.

aws | Q Service Quotas

**Services**

- Dashboard
- EC2 Global View
- Events
- Instances**
  - Instances**

**Services**

- Service Quotas
- Features
- Resources New
- Documentation
- Knowledge articles
- Marketplace

**Show more**

Select AWS services from the sidebar.

## Service Quotas

Dashboard

### AWS services

Quota request history

### ▼ Organization

Quota request template

Search for and select Amazon Elastic Compute Cloud (Amazon EC2).

## AWS services

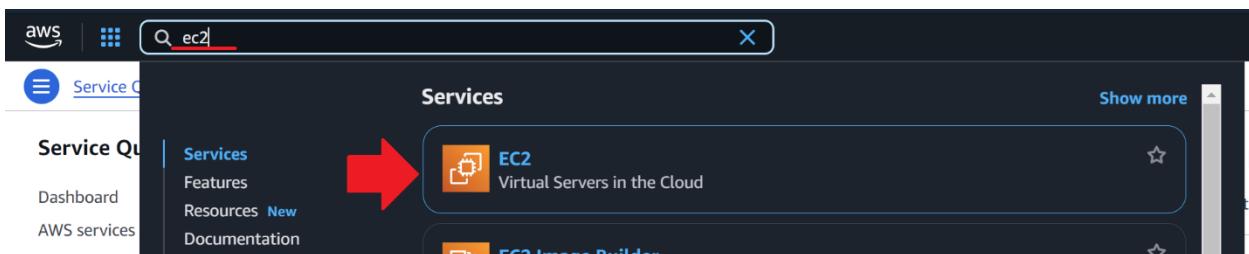
The screenshot shows a search bar at the top with the text 'ec2' and a count of '5 matches'. Below the search bar is a list of services, with 'Amazon Elastic Compute Cloud (Amazon EC2)' highlighted in red. Other listed services include Amazon EC2 Auto Scaling, EC2 Fast Launch, EC2 Image Builder, and EC2 VM Import/Export.

Search for running on-demand. Note the limits applied to how many concurrent EC2 instances can be run based on the instance type. Ensure that you do not surpass these limits while working with EC2.

The screenshot shows the 'Service quotas' page with a search bar for 'running on-demand' which finds 10 matches. The table lists various EC2 instance types with their applied account-level quota values, AWS default quota values, utilization, and adjustability. A red box highlights the 'Applied account-level quota value' column.

Quota name	Applied account-level quota value	AWS default quota value	Utilization	Adjustability
Running On-Demand DL instances	96	0	0	Account level
Running On-Demand F instances	64	0	0	Account level
Running On-Demand G and VT instances	0	0	0	Account level
Running On-Demand High Memory instances	0	0	0	Account level
Running On-Demand HPC instances	192	0	0	Account level
Running On-Demand Inf instances	8	0	0	Account level
Running On-Demand P instances	0	0	0	Account level
Running On-Demand Standard (A, C, D, H, I, M, R, T, Z) instances	256	5	1	Account level
Running On-Demand Trn instances	8	0	0	Account level
Running On-Demand X instances	0	0	0	Account level

Return to the EC2 dashboard from the search bar.



From the homepage, click Instances (running) under the Resources tab.

The screenshot shows the 'Resources' section of the EC2 dashboard. It displays a message about using EC2 resources and a link to 'Instances (running)'. A red arrow points to this link.

Select Web Server.

**Instances (1/2) [Info](#)**

[Find Instance by attribute or tag \(case-sensitive\)](#)

	Name	Instance ID
<input checked="" type="checkbox"/>	Web Server	i-0c5d2cee528e9ce3c
<input type="checkbox"/>	Bastion Host	i-09e4cc6b7f5fee95c

Select Instance state > Stop instance.

Instance state ▲

Actions ▼

- Stop instance** ←
- Start instance
- Reboot instance
- Hibernate instance

IPv4 IP IPv6 IP

Terminate (delete) instance

Click stop. Note the warning that stop protection is on.

**Stop instance**

Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.

Instance ID	Stop protection
<input type="checkbox"/> <a href="#">i-0c5d2cee528e9ce3c (Web Server)</a> <a href="#">?</a>	<a href="#">⚠️ On (Can't stop instance)</a>

**⚠️ You will be billed for associated resources**  
After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.

**▶ Associated resources**  
You will continue to incur charges for these resources while the instance is stopped

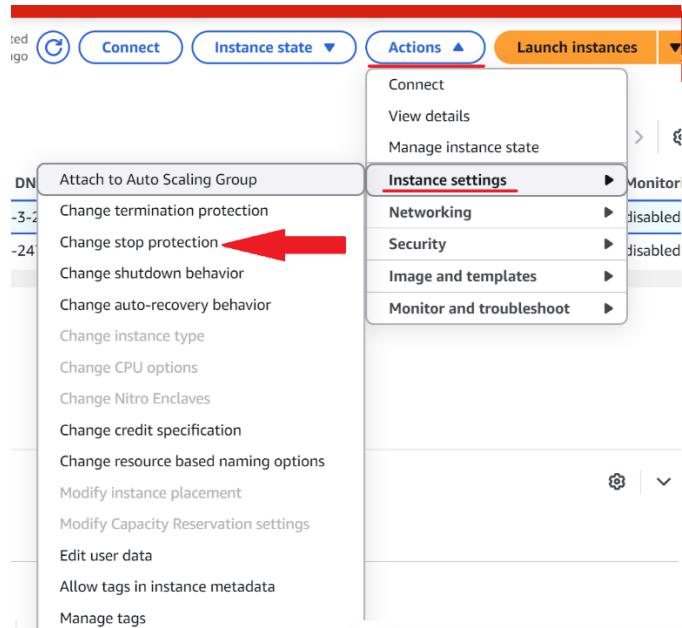
→ **Stop**

You will see the following error message.

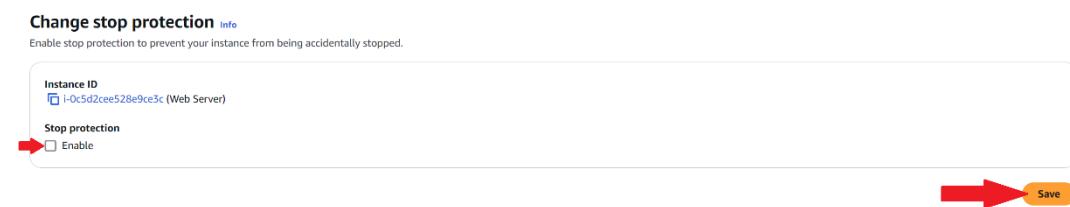
Failed to stop the instance i-0c5d2cee528e9ce3c  
The instance 'i-0c5d2cee528e9ce3c' may not be stopped. Modify its 'disableApiStop' instance attribute and try again.

[Diagnose with Amazon Q](#) ×

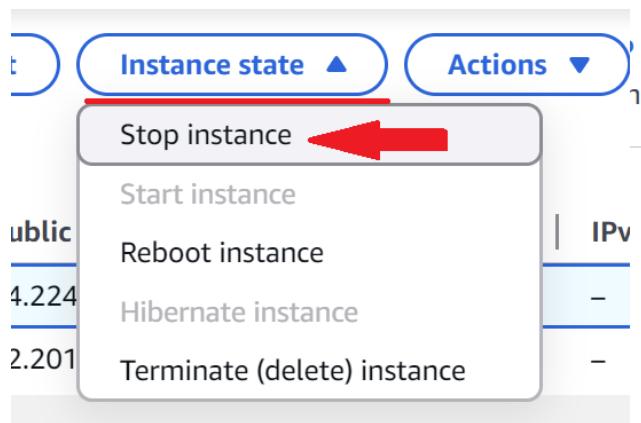
Next, you will disable stop protection. Go to Actions > Instance settings and click Change stop protection.



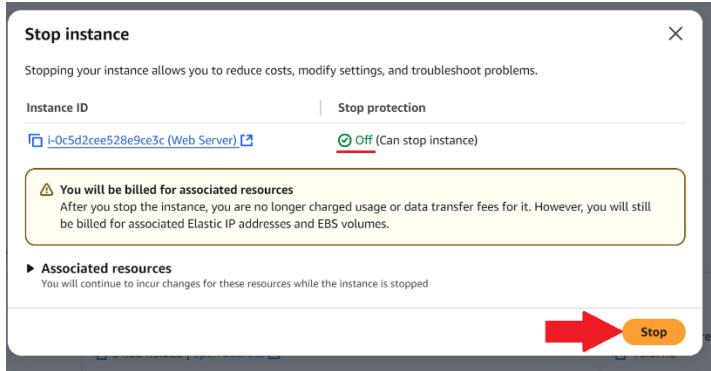
Uncheck Enable and click Save.



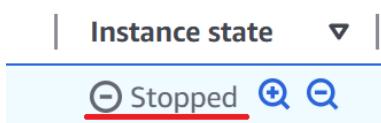
Now, click Instance state > Stop instance.



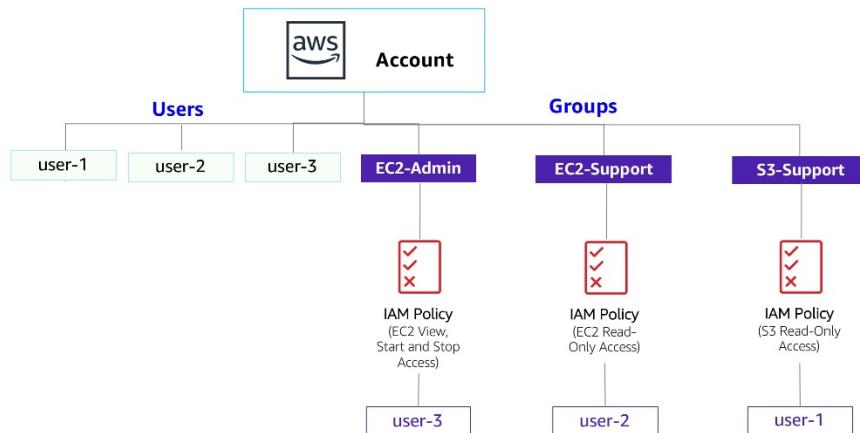
Click Stop. Note the confirmation that stop protection is now off.



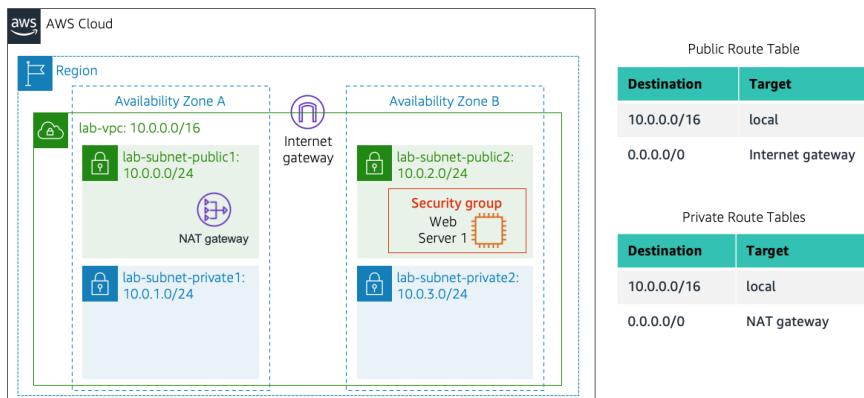
Wait a few minutes and refresh the Instances page. The web server's instance state should now show as Stopped.



## Network Diagram (Lab 1 IAM)



## Network Diagram (Lab 2 VPC)



## Network Diagram (Lab 3 EC2)



## Problems

One problem I encountered was in Lab 3 (the EC2 lab), where even after correctly updating the Web server security group, the server's webpage refused to connect. This is because my web browser attempted to connect with HTTPS instead of HTTP. This was fixed simply by modifying the protocol in the URL to connect over HTTP.

## Conclusion

To wrap up, this lab was a very useful introduction to the world of cloud computing. I'm grateful to have learned about exciting new cloud computing concepts such as complex security mechanisms, virtual routing through a private cloud, and easily scalable virtual machines. I'm now confident that I could help a company migrate basic services from traditional IT to the cloud, I'm hopeful that these foundational skills will help me secure a career in cloud services in the future.





# Advanced Cisco Networking Academy – Configuring a Cisco Wireless Access Point and WLC with WPA2-PSK and WPA2- Enterprise with a RADIUS Server

Colin J. Faletto, CCNA

## Purpose

This lab is intended to reintroduce the concept of managing wireless connectivity with a WLAN Controller, a concept we visited briefly in CCNA but haven't learned about since. This lab is also meant to introduce RADIUS and the process of setting it up as an external server, which indirectly teaches basic Linux skills such as navigating the terminal. This lab also revisits aspects from the CCNA course such as subinterfaces/VLANs and virtualization.

## Background

Aironet is a division of Cisco that develops wireless access points. It was founded in 1986 as an independent company and acquired by Cisco 13 years later. The Cisco Aironet 1040 series was a series of access points developed by Cisco in the early 2010s, which was discontinued in 2013 and dropped from support in 2018. As of 2025, the Aironet line appears to be inactive or discontinued, replaced fully by the Catalyst and Meraki lines of wireless products.

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.

Ubuntu is a distribution of Linux developed by Canonical. It is built on the older Debian distribution, including well-known features from that distribution such as the package manager Advanced Package Tool (APT). It is the most popular Linux distribution by far, with a multitude of spin-off distributions. By default, Ubuntu uses the GNOME desktop environment, which is designed with accessibility and readability in mind.

Lubuntu is a Linux distribution built on Ubuntu known for being lightweight, both in terms of CPU/Memory utilization and storage usage. Lubuntu uses the LXQt desktop environment, which is a lightweight desktop environment that still provides all the tools necessary for basic productivity and development.

## Lab Summary

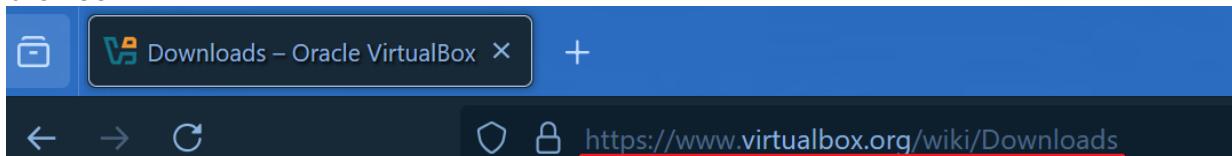
In this lab, we configured a Cisco 2504 WLAN Controller and Cisco Aironet AIR-LAP1042N Access Point with three WLANs – one configured with no security (CrunchwrapSupreme), one with WPA2-PSK (NachosBellGrande), and one with WPA2-Enterprise (CheesyGorditaCrunch). Each of these WLANs is connected to its own

VLAN, with a central router giving out addresses for each VLAN via DHCP. The central router is also connected to a management VLAN where the AP, WLAN Controller, and management PC reside.

The management PC is also running a virtualized instance of Lubuntu through Virtualbox. Lubuntu is a Linux distribution we chose for its lightweight nature and similarity to the widely supported Ubuntu distribution. The Lubuntu instance runs an instance of FreeRADIUS that is used for authentication for the CheesyGorditaCrunch WLAN.

### Lab Commands (Configure RADIUS Server)

On your host PC, navigate to <https://www.virtualbox.org/wiki/Downloads> in a web browser.



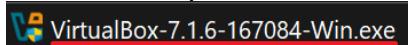
Download the appropriate version of Virtualbox for your operating system (in this case, we are running Windows).

**VirtualBox Platform Packages**

VirtualBox 7.1.6 platform packages

- [\*\*Windows hosts\*\*](#)
- [macOS / Intel hosts](#)
- [macOS / Apple Silicon hosts](#)
- [Linux distributions](#)
- [Solaris hosts](#)
- [Solaris 11 IPS hosts](#)

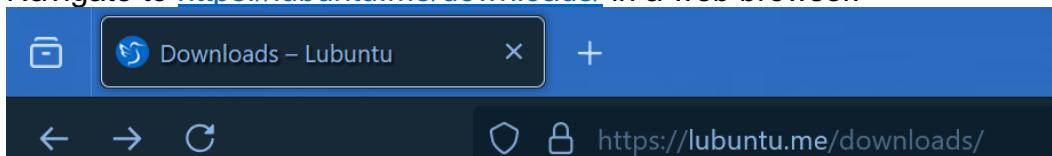
Run the setup file once it has downloaded.



Be agreeable through the setup process, clicking Next and Install when prompted.



Navigate to <https://lubuntu.me/downloads/> in a web browser.



Download the ISO image for the latest stable release of the operating system.

## 24.10 (Oracular Oriole)

**Latest stable release**

*Supported until July 2025*

**Please read [the release announcement.](#)**

**LXQt Version: 2.0**

It's better to use the  (magnet) link first (auto-verified downloads).

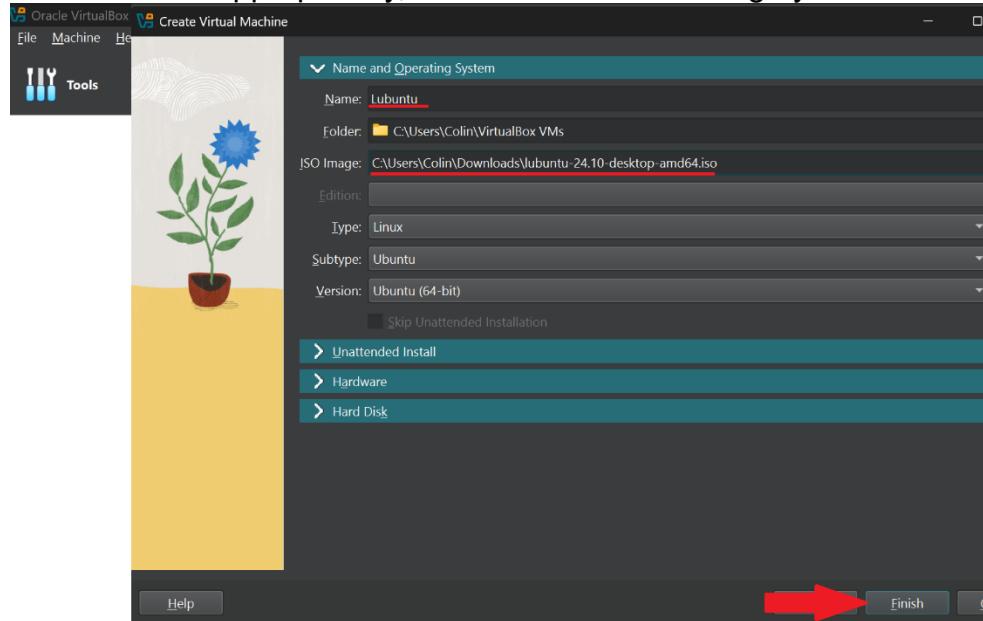
**Note:** make sure to verify the integrity ([SHA256SUMS](#)) of your downloads and that they come from an official source. More info [here](#).

[Desktop 64-bit](#)

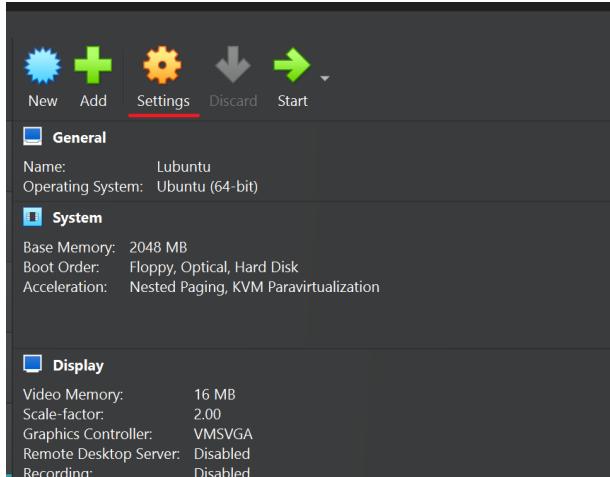
Open Virtualbox and click New.



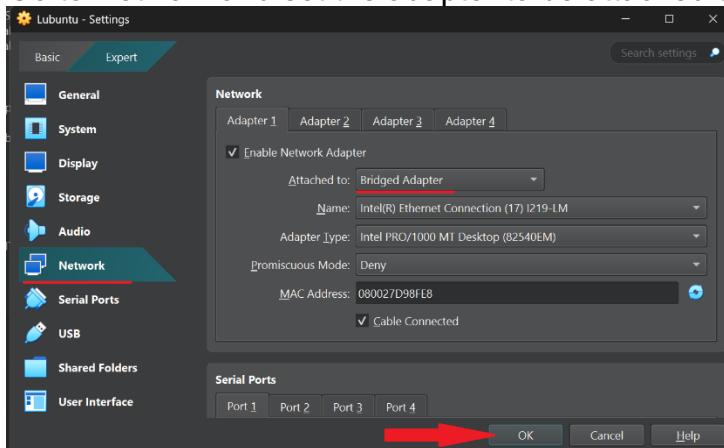
Name the VM appropriately, then select the ISO image you downloaded earlier.



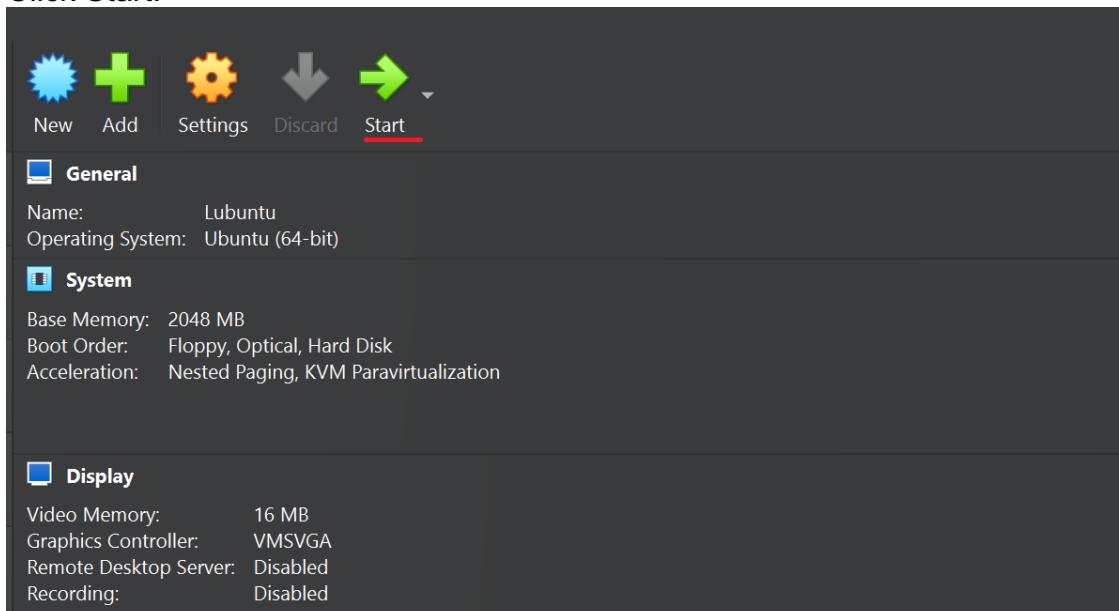
Click Settings.



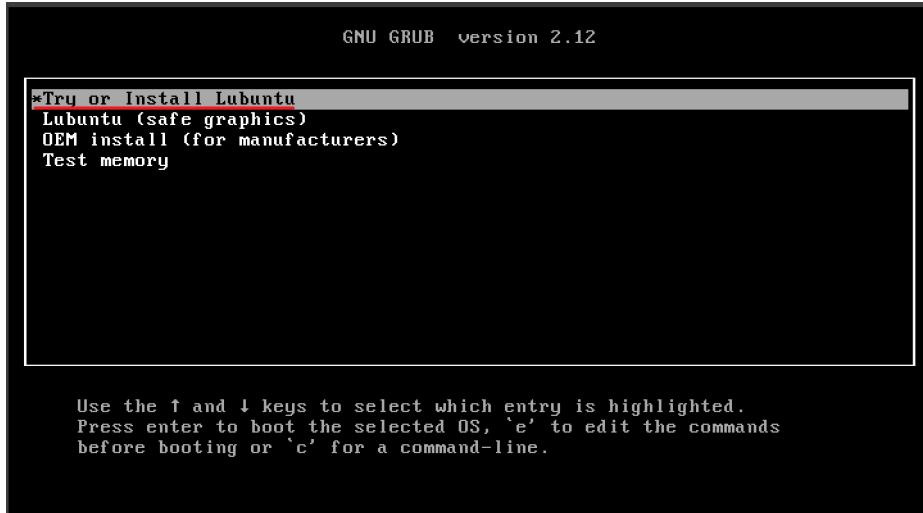
Go to Network and set the adapter to be attached to a Bridged Adapter. Click OK.



Click Start.



Select Try or Install Lubuntu.



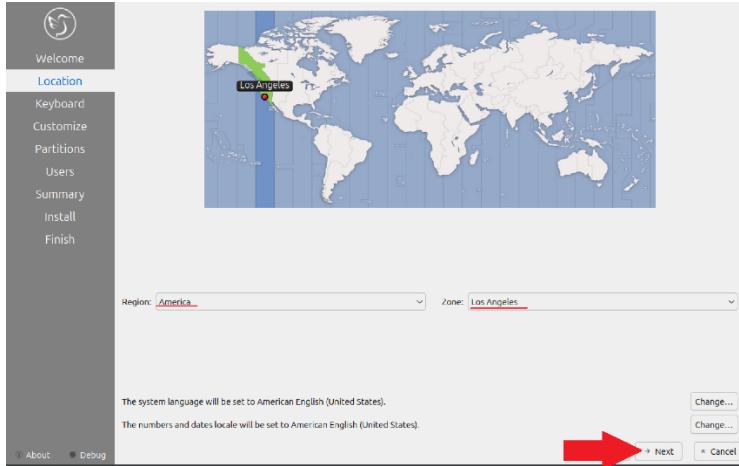
Select Install Lubuntu.



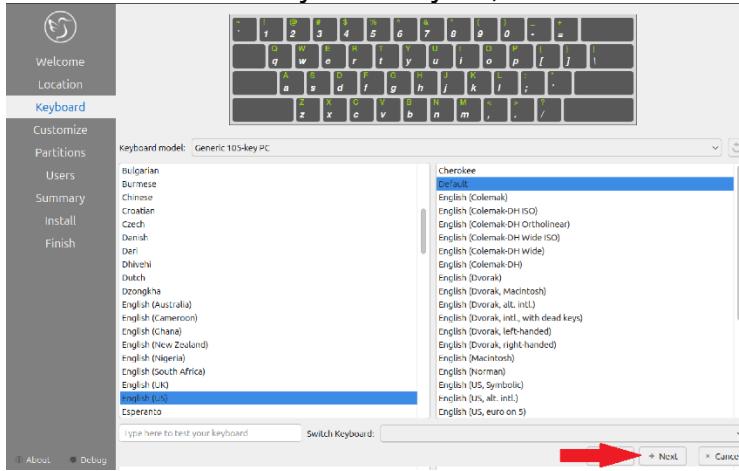
Click Next.



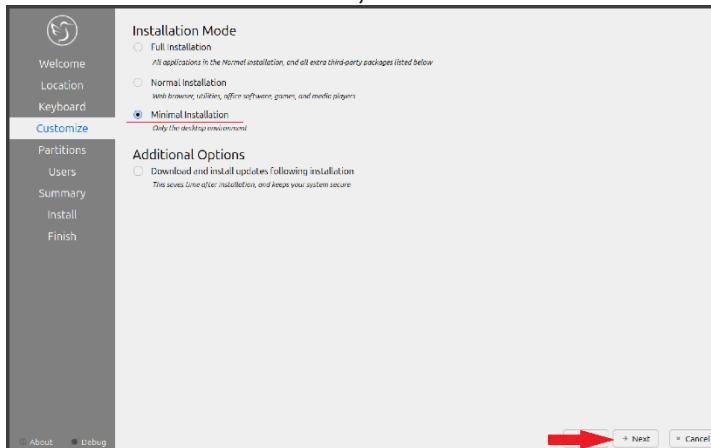
Set the correct time zone, then click Next.



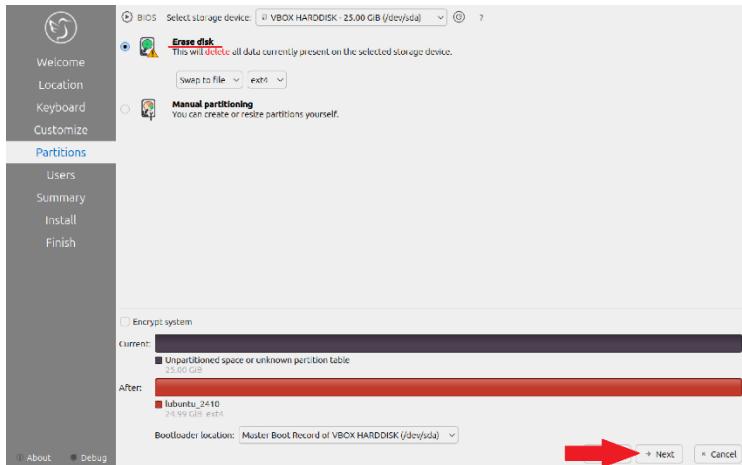
Select the correct keyboard layout, then click Next.



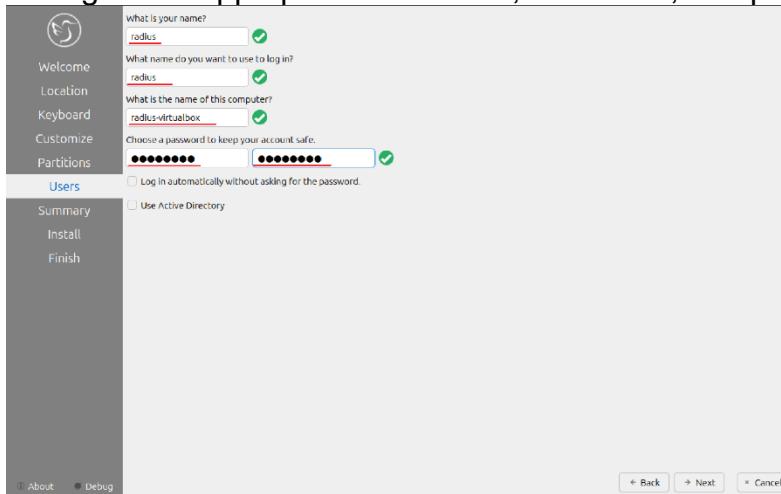
Click Minimal Installation, then click Next.



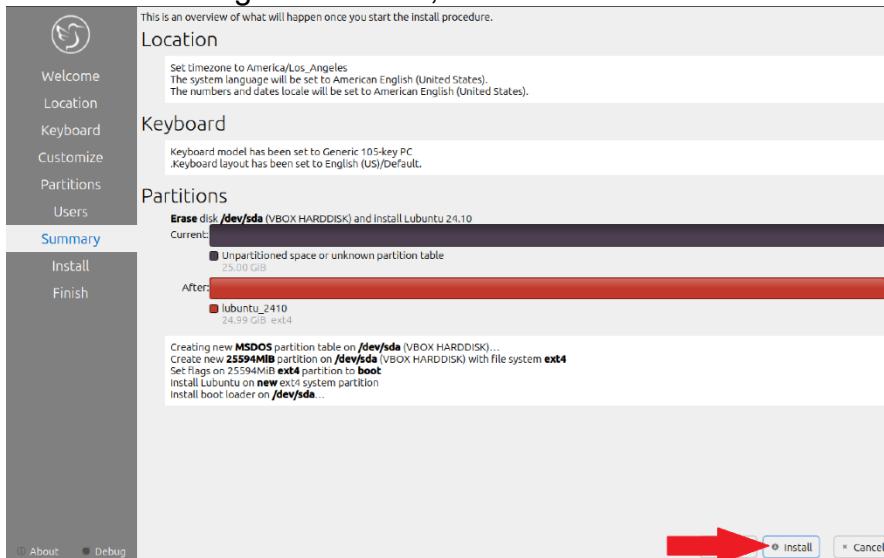
Select Erase disk, then click Next.



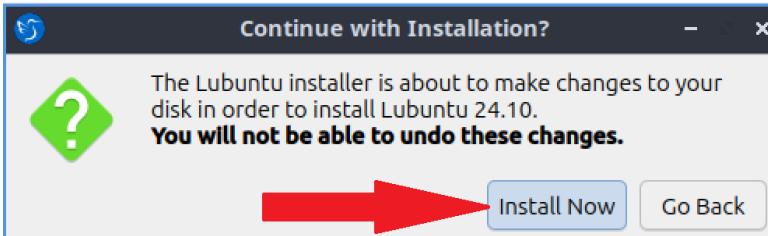
Configure an appropriate username, hostname, and password, then click Next.



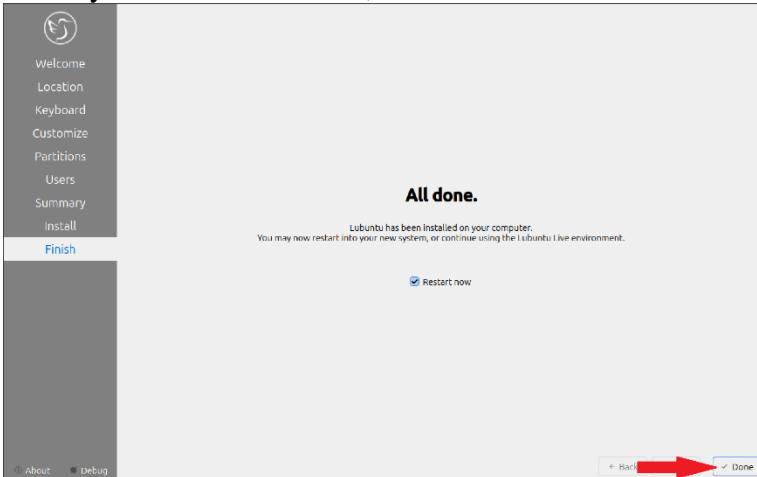
Ensure all settings are correct, then click Install.



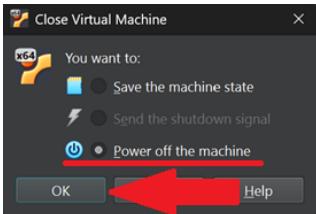
Click Install Now.



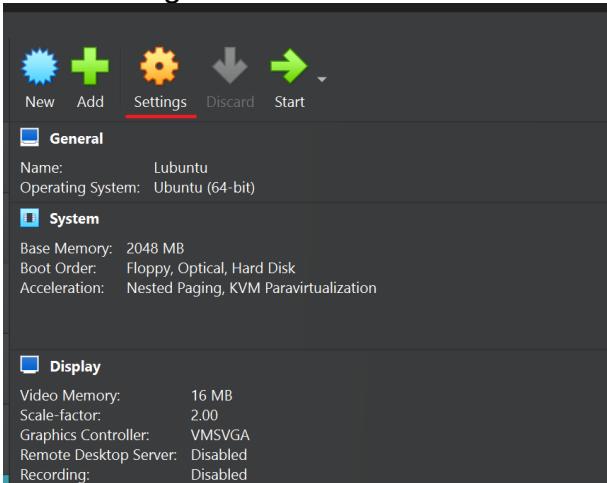
Once you see this screen, click Done.



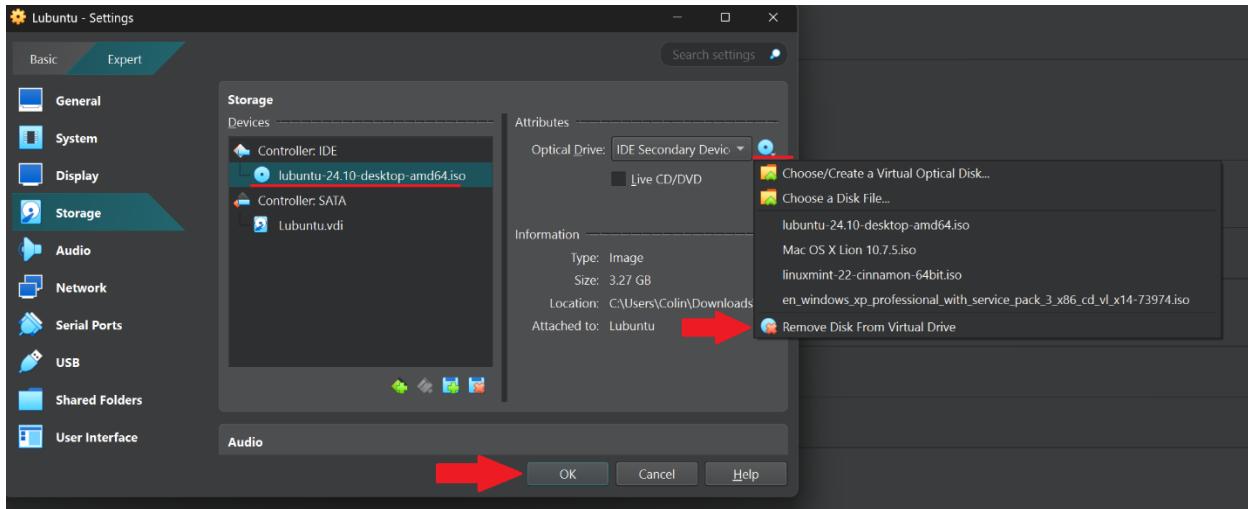
Press Right CTRL, then ALT+F4 to exit out of the VM. Select Power off the Machine, then click OK.



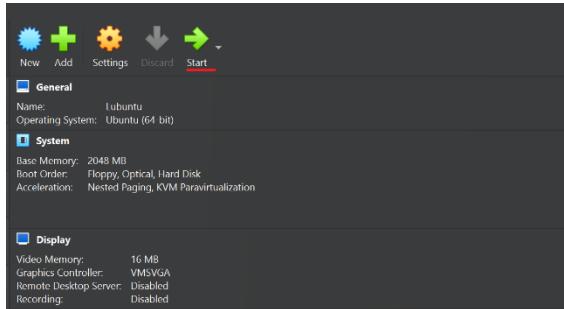
Click Settings.



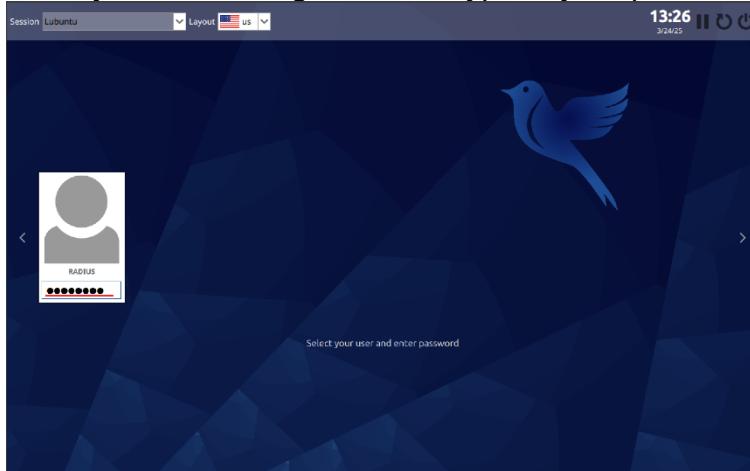
Go to Storage and click on the ISO file, click on the disk icon, then click Remove Disk from Virtual Drive. Click OK.



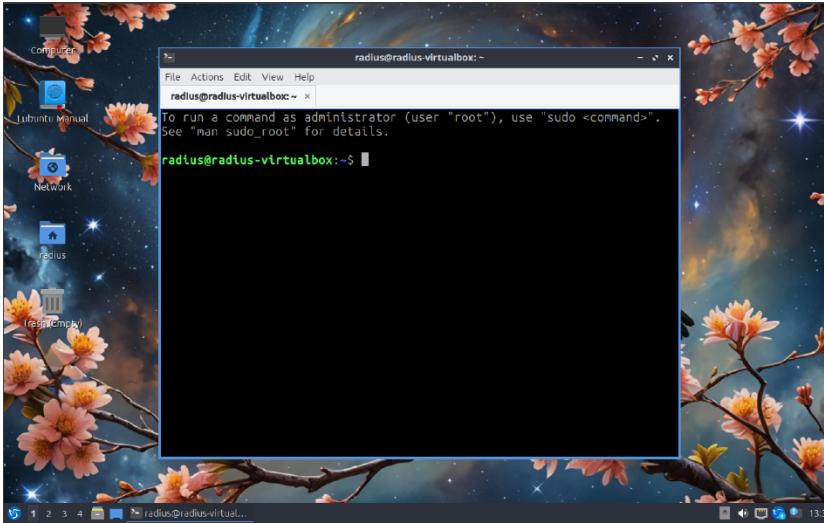
Click Start.



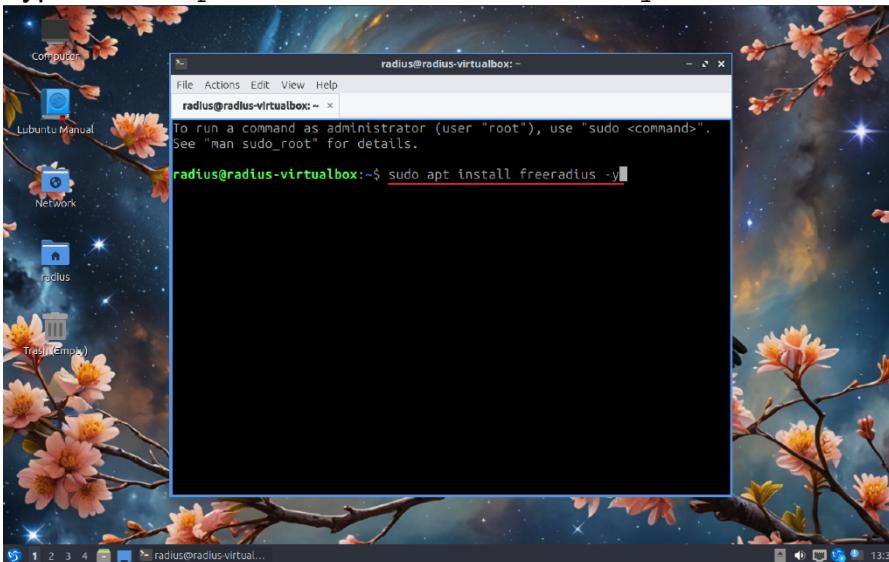
Once you see the login screen, type in your password and press Enter.



Press CTRL + ALT + T to open the terminal.



Type `sudo apt install freeradius -y`.



Type your password.

[`sudo`] password for radius: [REDACTED]

Once freeradius has installed, type `sudo nano /etc/freeradius/3.0/clients.conf`.

**radius@radius-virtualbox:~\$ sudo nano /etc/freeradius/3.0/clients.conf**

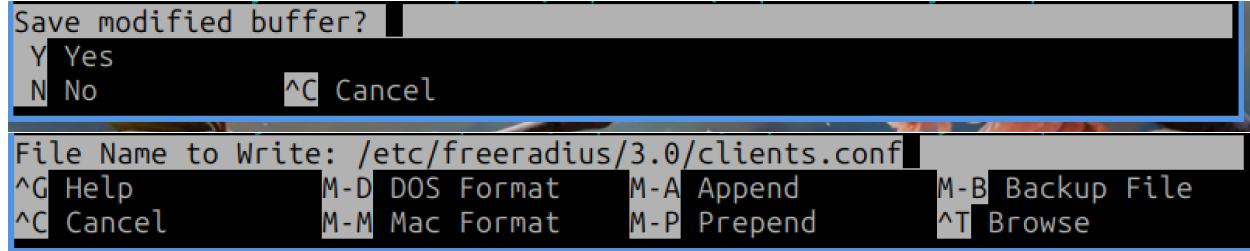
Add the following lines:

```
client wlc {
    ipaddr = 192.168.0.254
    secret = <secret>
}
```

With `<secret>` being replaced with a secure password to be specified later on the WLC.

```
client wlc {
    ipaddr = 192.168.0.254
    secret = Redbull6
}
```

Press CTRL + X, Y, then ENTER to save.



Next, type sudo nano /etc/freeradius/3.0/users.

```
radius@radius-virtualbox:~$ sudo nano /etc/freeradius/3.0/users
```

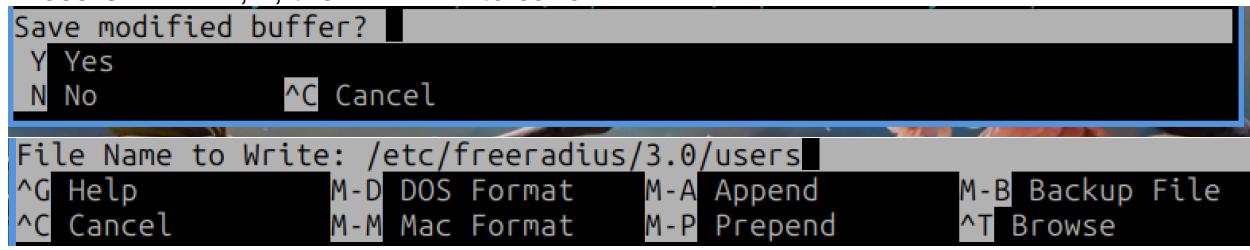
Add the following lines:

```
<user>    Cleartext-Password := "<password>"
            Reply-Message := "Hello, <user>"
```

With <user> being replaced with a username and <password> being replaced with a secure password.

```
colin    Cleartext-Password := "squabbleup"
            Reply-Message := "Hello, Colin"
```

Press CTRL + X, Y, then ENTER to save.



### Lab Commands (Configuring WLC)

Connect your AP, WLC, Router, and PC to your switch as specified in the network diagram below.

Configure your switch according to the switch configuration below (Note: the WLC should be connected to port f0/1 as a trunk, and all other devices should be on access VLAN 99.).

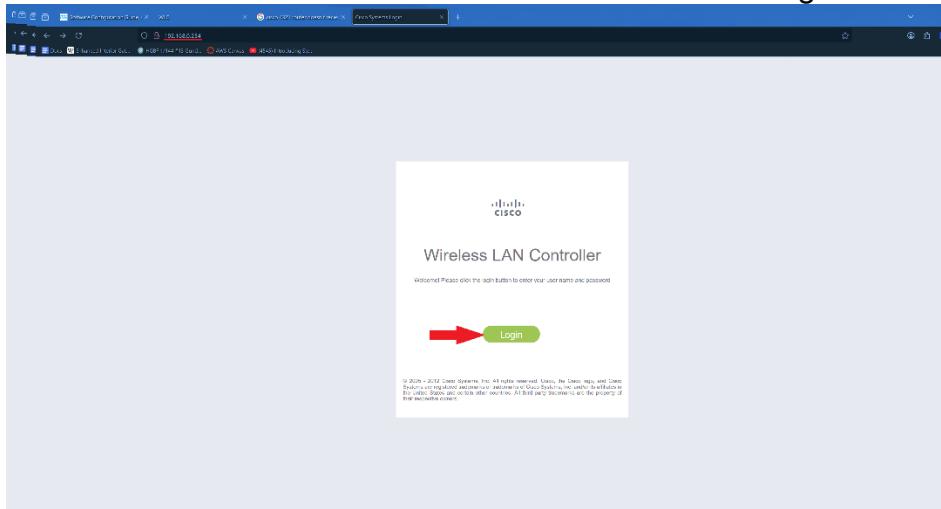
Configure your router according to the configuration below.

Ensure that PC is receiving an IP and that internet works.

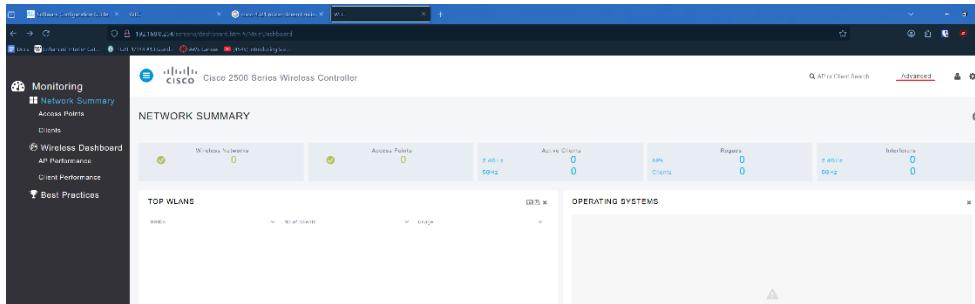
### Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . : 
IPv4 Address . . . . . : 192.168.0.3
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
```

Connect to the WLC's IP address via HTTP and click Login.



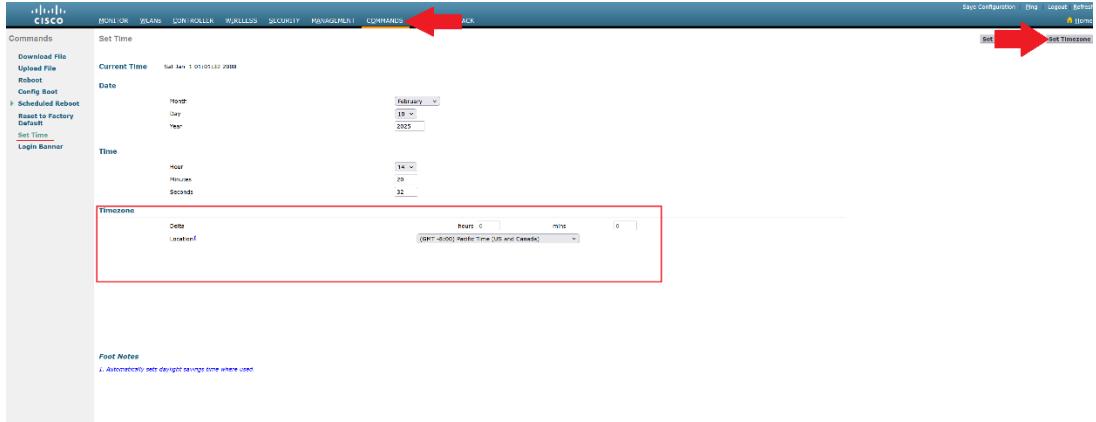
Click Advanced.



Go to Commands > Set Time. Set the correct time, then click Set Date and Time.



Set the timezone and click Set Timezone.



Once the correct timezone is set, the AP should automatically discover and connect to your WLC. In our case, the AP automatically downloaded and installed a software update as shown in the console log below (the image name is underlined in red):

```
Feb 16 14:28:48.000: %CAPWAP-5-DTLSREQUEST: DTLS connection request sent peer_ip: 192.168.0.254 peer_port: 5246
Feb 16 14:28:48.000: %CAPWAP-5-CHANGED: CAPWAP changed state to 00000000000000000000000000000000
Feb 16 14:28:48.000: %CAPWAP-5-CHANGED: CAPWAP changed state to 00000000000000000000000000000000
extracting 1020... (289 bytes)
Image info:
Version suffix: k9w-mx.153-3.JC14
Image Name: c1140-k9w-mx.153-3.JC14
Version Directory: c1140-k9w-mx.153-3.JC14
Image Size: 8684932
Image Type: C1140-k9w-mx.153-3.JC14
Image Feature: WIRELESS LAN|WAPP
Image Family: C1140
Alarms|Switch Management Version: 8.2.166.0
Extracting files...
c1140-k9w-mx.153-3.JC14/ (directory) 0 (bytes)
extracting c1140-k9w-mx.153-3.JC14/8001.htm (157732 bytes)
Feb 16 14:28:49.044: %CAPWAP-5-SENDJOIN: sending Join Request to 192.168.0.254
Feb 16 14:28:49.045: %CAPWAP-5-CHANGED: CAPWAP changed state to 01000000000000000000000000000000
Feb 16 14:28:49.045: %CAPWAP-5-CHANGED: CAPWAP changed state to 00000000000000000000000000000000
Feb 16 14:28:49.045: %CAPWAP-5-CHANGED: CAPWAP changed state to 00000000000000000000000000000000
Feb 16 14:28:49.046: %CAPWAP-5-CHANGED: CAPWAP changed state to 00000000000000000000000000000000
Feb 16 14:28:49.046: Loading file /c1140...
extracting c1140-k9w-mx.153-3.JC14/file_hashes (3030 bytes)
extracting c1140-k9w-mx.153-3.JC14/img_sign_rel_sha2.cert (1371 bytes)
extracting c1140-k9w-mx.153-3.JC14/final_hash.sig (511 bytes)
extracting c1140-k9w-mx.153-3.JC14/info (283 bytes)
extracting c1140-k9w-mx.153-3.JC14/info (283 bytes)
extracting c1140-k9w-mx.153-3.JC14/final_hash (141 bytes)
extracting c1140-k9w-mx.153-3.JC14/ (directory) 0 (bytes)
c1140-k9w-mx.153-3.JC14/html/ (directory) 0 (bytes)
extracting c1140-k9w-mx.153-3.JC14/html/1/images/ (directory) 0 (bytes)
extracting c1140-k9w-mx.153-3.JC14/html/1/images/txces-logo-2007.gif (1648 bytes)
extracting c1140-k9w-mx.153-3.JC14/html/level/1/images/background_wed41.jpg (732 bytes)
extracting c1140-k9w-mx.153-3.JC14/html/level/1/images/info.gif (399 bytes)
extracting c1140-k9w-mx.153-3.JC14/html/level/1/images/logo_wlc_160x160px.png (9871 bytes)!!!
extracting c1140-k9w-mx.153-3.JC14/html/level/1/siteside.js (17250 bytes)
extracting c1140-k9w-mx.153-3.JC14/html/level/1/favicon.js (20442 bytes)!!!
extracting c1140-k9w-mx.153-3.JC14/html/level/1/favicon.ico (1024 bytes)
extracting c1140-k9w-mx.153-3.JC14/html/level/1/index.html (511 bytes)
extracting c1140-k9w-mx.153-3.JC14/html/level/1/officeextendap.css (418 bytes)!!!
extracting c1140-k9w-mx.153-3.JC14/html/level/1/officehome.html (1370 bytes)
extracting c1140-k9w-mx.153-3.JC14/html/level/1/officesetup.js (653 bytes)
c1140-k9w-mx.153-3.JC14/html/level/15/ (directory) 0 (bytes)
extracting c1140-k9w-mx.153-3.JC14/html/level/15/officeextendap.html (3150 bytes)!!!
extracting c1140-k9w-mx.153-3.JC14/html/level/15/officeextendapconfig.html (2364 bytes)
extracting c1140-k9w-mx.153-3.JC14/html/level/15/officeextendapbanner.htm (7514 bytes)
extracting c1140-k9w-mx.153-3.JC14/html/level/15/officeextendapsummary.htm (985 bytes)!!!
extracting c1140-k9w-mx.153-3.JC14/html/level/15/offilextendapip.htm (921 bytes)
extracting c1140-k9w-mx.153-3.JC14/1140-k9w-mx.153-3.html (10777 bytes)!!!!!!
extracting c1140-k9w-mx.153-3.JC14/1140-k9w-mx.153-3.html (10777 bytes)
extracting c1140-k9w-mx.153-3.JC14/1140-k9w-mx.153-3.html (10777 bytes)
extracting c1140-k9w-mx.153-3.JC14/1140-k9w-mx.153-3.html (10777 bytes)!!!!!!
```

Once the AP has finished updating, go to Monitor > Summary and ensure the WLC can see the AP (indicated by a 1 next to the All APs section)

The screenshot shows the Cisco Wireless Controller's Monitor interface. The top navigation bar includes MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The MONITOR tab is selected. The left sidebar has sections like Monitor, Summary, Access Points, Statistics, CDP, Rogue, Clients, Sleeping Clients, Multicast, Applications, Local Profiling, and Cisco CleanAir. The main content area displays the Controller Summary and Access Point Summary. A red arrow points to the 'All APs' row in the Access Point Summary table.

	Total	Up	Down	
802.11a/n/ac Radios	1	1	0	<a href="#">Detail</a>
802.11b/g/n Radios	1	1	0	<a href="#">Detail</a>
Dual-Band Radios	0	0	0	<a href="#">Detail</a>
All APs	1	1	0	<a href="#">Detail</a>

Next, go to Controller > Interfaces > New.

The screenshot shows the 'Interfaces' section of the Controller configuration. The top navigation bar includes MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The CONTROLLER tab is selected. The left sidebar has sections like Controller, General, Icons, Inventory, Interfaces (which is highlighted), Interface Groups, Multicast, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, IPv6, mDNS, and Advanced. The main content area shows a table of existing interfaces. A red arrow points to the 'New...' button at the bottom right.

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
esmanagement	99	192.168.0.254	Static	Enabled	::/128
vlan10	N/A	192.0.2.1	Static	Not Supported	

Create the Guest VLAN, setting the VLAN ID to 10.

### Interfaces > New

Interface Name	<input type="text" value="Guest VLAN"/>
VLAN Id	<input type="text" value="10"/>

Configure the VLAN ID, IP Address, Netmask, Gateway, and Primary DHCP Server for VLAN 10:

## Interface Address

VLAN Identifier	<input type="text" value="10"/>
IP Address	<input type="text" value="192.168.10.254"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.10.1"/>

## DHCP Information

Primary DHCP Server	<input type="text" value="192.168.10.1"/>
Secondary DHCP Server	<input type="text"/>
DHCP Proxy Mode	<input type="button" value="Global"/>
Enable DHCP Option 82	<input type="checkbox"/>

Create the PSK and Enterprise VLANs, using the VLAN information for VLANs 20 and 30 respectively:

### Interfaces > New

Interface Name	<input type="text" value="psk vlan"/>
VLAN Id	<input type="text" value="20"/>

## Interface Address

VLAN Identifier	<input type="text" value="20"/>
IP Address	<input type="text" value="192.168.20.254"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.20.1"/>

## DHCP Information

Primary DHCP Server	<input type="text" value="192.168.20.1"/>
Secondary DHCP Server	<input type="text"/>
DHCP Proxy Mode	<input type="button" value="Global"/>
Enable DHCP Option 82	<input type="checkbox"/>

## Interfaces > New

Interface Name	<input type="text" value="enterprise vlan"/>
VLAN Id	<input type="text" value="30"/>

### Interface Address

VLAN Identifier	<input type="text" value="30"/>
IP Address	<input type="text" value="192.168.30.254"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.30.1"/>

### DHCP Information

Primary DHCP Server	<input type="text" value="192.168.30.1"/>
Secondary DHCP Server	<input type="text"/>
DHCP Proxy Mode	<input type="button" value="Global"/>
Enable DHCP Option 82	<input type="checkbox"/>

Next, go to the WLANS tab, set the dropdown to Create New, and click Go.

The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. The top navigation bar has tabs: MONITOR, WLANS (which is highlighted in orange), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. Below the navigation bar, there's a sidebar with 'WLANS' expanded, showing 'WLANS' and 'Advanced'. The main content area is titled 'WLANS' and shows a table with columns: Current Filter (None), [Change Filter] [Clear Filter]. On the right side of the content area, there's a 'Create New' dropdown menu and a 'Go' button, with a red arrow pointing to the 'Create New' dropdown.

Create WLAN ID 1, the Guest WLAN:

The screenshot shows the 'WLANS > New' configuration page. The top navigation bar is identical to the previous screenshot. The sidebar shows 'WLANS' expanded. The main form has fields: Type (WLAN), Profile Name (Guest), SSID (CrunchwrapSupreme), and ID (1). On the right, there's a 'Create New' dropdown and a 'Go' button, with a red arrow pointing to the 'Go' button.

Ensure the WLAN is enabled, and the interface is set to the guest VLAN:

Under Security > Layer 2, set Layer 2 Security to None.

Click Apply.



Next, configure the PSK WLAN (NachosBellGrande) with VLAN ID 2.

**WLANs > New**

Ensure the WLAN is enabled and the interface is set to the PSK VLAN.

## WLANS &gt; Edit 'PSK WLAN'

**General Security QoS Policy-Mapping Advanced**

Profile Name	PSK WLAN
Type	WLAN
SSID	NachosBellGrande
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(PSK)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	psk vlan
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled
NAS-ID	none

Under Security > Layer 2, Enable PSK, and under PSK Format, set a strong password.

**General Security QoS Policy-Mapping Advanced**

**Layer 2 Layer 3 AAA Servers**

PMF: Disabled

**WPA+WPA2 Parameters**

WPA Policy:

WPA2 Policy:

WPA2 Encryption:  AES  TKIP

OSEN Policy:

**Authentication Key Management**

802.1X:  Enable

CCKM:  Enable

PSK:  Enable

FT 802.1X:  Enable

FT PSK:  Enable

PSK Format: ASCII  
\*\*\*\*\*

WPA gtk-randomize State: Disable

Click Apply.



Next, Create the Enterprise WLAN.

## WLANS &gt; New

Type	WLAN
Profile Name	Enterprise WLAN
SSID	CheesyGorditaCrunch
ID	3

Ensure the WLAN is enabled and set the interface to the Enterprise VLAN.

General    Security    QoS    Policy-Mapping    Advanced

Profile Name: Enterprise WLAN  
Type: WLAN  
SSID: CheesyGorditaCrunch  
Status:  Enabled

Security Policies: [WPA2][Auth(802.1X)]  
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All  
Interface/Interface Group(G): enterprise vlan  
Multicast Vlan Feature:  Enabled  
Broadcast SSID:  Enabled  
NAS-ID: none

Under Security > Layer 2, set the Layer 2 security to WPA+WPA2, and under Authentication Key Management, ensure that 802.1X is enabled.

General    Security    QoS    Policy-Mapping    Advanced

Layer 2    Layer 3    AAA Servers

Layer 2 Security: WPA+WPA2  
MAC Filtering:

**Fast Transition**  
Fast Transition:

**Protected Management Frame**  
PMF: Disabled

**WPA+WPA2 Parameters**

WPA Policy:   
WPA2 Policy:   
WPA2 Encryption:  AES     TKIP  
OSEN Policy:

**Authentication Key Management**  
802.1X:  Enable  
CCKM:  Enable  
PSK:  Enable

Click Apply.



Apply

Go to Security > AAA > RADIUS > Authentication and click New.

MONITOR    WIANS    CONTROLLER    WIRELESS    SECURITY    MANAGEMENT    COMMANDS    HELP    FEEDBACK

Save Configuration    Ping    Logout    Refresh

Apply    New...   

**Security**

**RADIUS Authentication Servers**

**AAA**

- General
- Radius
- Radius Authentication
- Radius Accounting
- Radius Deauthentication

Auth Called Station ID Type: AP MAC Address(SSID)  
Use AES Key Wrap:  (Designed for EPPS customers and requires a key wrap compliant RADIUS server)  
MAC Delimiter: Hyphen

Enter the IP address of the RADIUS server, then enter the shared secret configured in the server's `clients.conf` file.

#### RADIUS Authentication Servers > New

Server Index (Priority)	<input type="text" value="1"/>
Server IP Address(Ipv4/Ipv6)	<input type="text" value="192.168.0.200"/>
Shared Secret Format	<input type="text" value="ASCII"/>
Shared Secret	<input type="text" value="*****"/>
Confirm Shared Secret	<input type="text" value="*****"/>
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	<input type="text" value="1812"/>
Server Status	<input type="text" value="Enabled"/>
Support for CoA	<input type="text" value="Disabled"/>
Server Timeout	<input type="text" value="2"/> seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
Management Retransmit Timeout	<input type="text" value="2"/> seconds
IPSec	<input type="checkbox"/> Enable

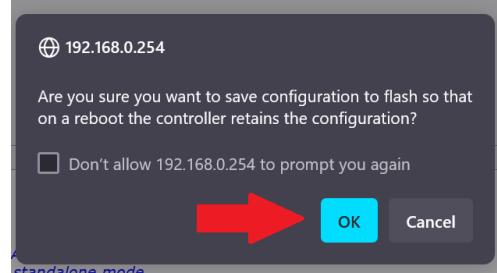
Click Apply.



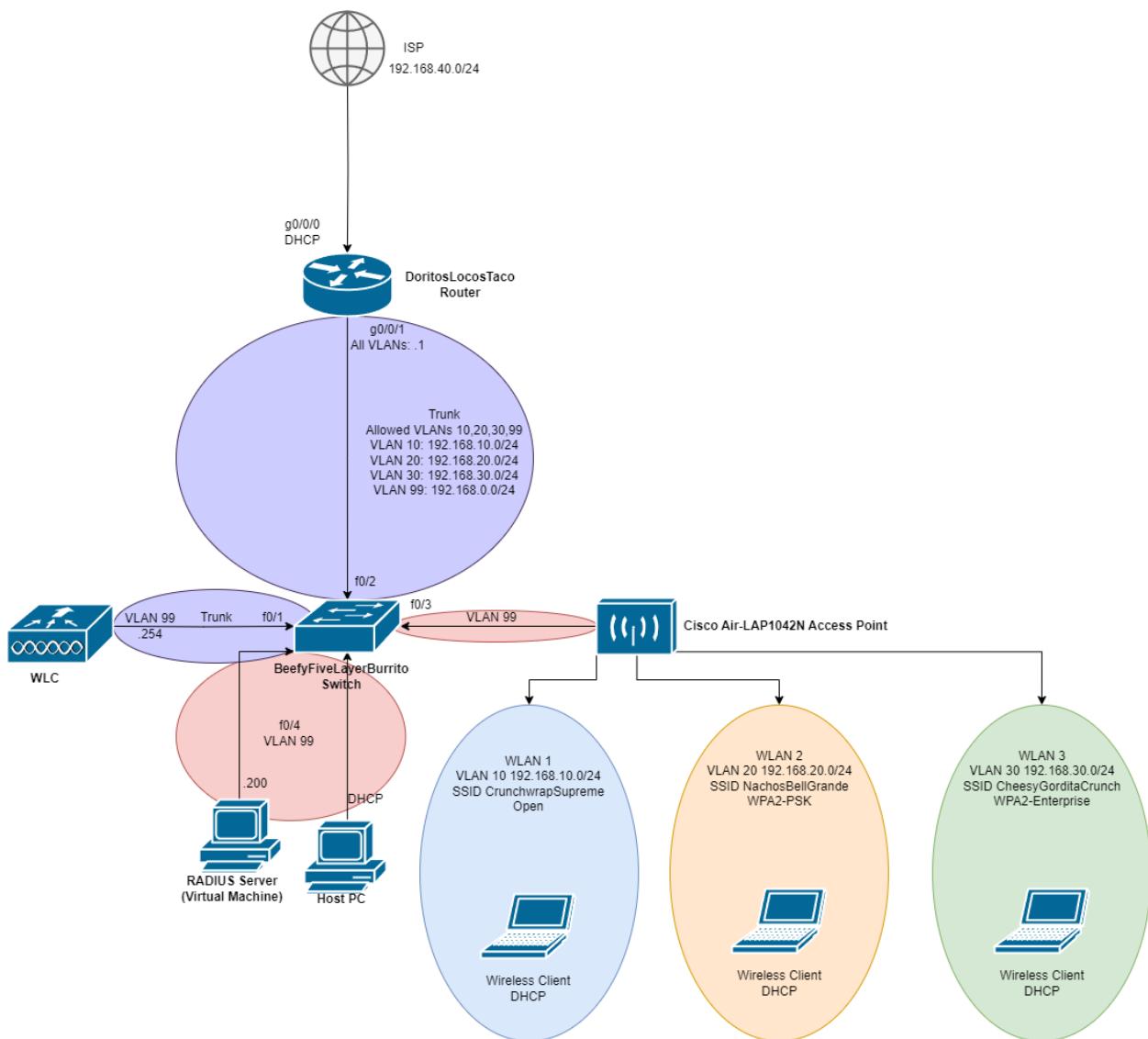
Finally, click Save Configuration.



Click OK.



Network Diagram



### Configuration for DoritosLocosTaco (Router)

Current configuration : 5312 bytes

Last configuration change at 22:07:55 UTC Tue Mar 11 2025

version 16.9

```
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
hostname DoritosLocosTaco
boot-start-marker
boot-end-marker
vrf definition Mgmt-intf
  address-family ipv4
  exit-address-family
  address-family ipv6
```

```
exit-address-family
no aaa new-model
ip name-server 8.8.8.8 1.1.1.1
ip dhcp excluded-address 192.168.0.254
ip dhcp excluded-address 192.168.0.1
ip dhcp excluded-address 192.168.0.1 192.168.0.10
ip dhcp excluded-address 192.168.0.30 192.168.0.254
ip dhcp excluded-address 192.168.10.1
ip dhcp excluded-address 192.168.20.1
ip dhcp excluded-address 192.168.30.1
ip dhcp excluded-address 192.168.0.200
ip dhcp pool AP-POOL
  network 192.168.0.0 255.255.255.0
  default-router 192.168.0.1
  dns-server 8.8.8.8 8.8.4.4
ip dhcp pool GUEST-VLAN
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
  dns-server 8.8.8.8
ip dhcp pool PSK-VLAN
  network 192.168.20.0 255.255.255.0
  default-router 192.168.20.1
  dns-server 8.8.8.8
ip dhcp pool ENTERPRISE-VLAN
  network 192.168.30.0 255.255.255.0
  default-router 192.168.30.1
  dns-server 8.8.8.8
login on-success log
subscriber templating
vtp domain cisco
vtp mode transparent
multilink bundle-name authenticated
license udi pid ISR4321/K9 sn FDO214421D1
no license smart enable
diagnostic bootup level minimal
spanning-tree extend system-id
redundancy
  mode none
interface GigabitEthernet0/0/0
  ip address dhcp
  ip nat outside
  negotiation auto
interface GigabitEthernet0/0/1
  no ip address
  negotiation auto
interface GigabitEthernet0/0/1.10
  encapsulation dot1Q 10
```

```
ip address 192.168.10.1 255.255.255.0
ip nat inside
interface GigabitEthernet0/0/1.20
encapsulation dot1Q 20
ip address 192.168.20.1 255.255.255.0
ip nat inside
interface GigabitEthernet0/0/1.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
ip nat inside
interface GigabitEthernet0/0/1.99
encapsulation dot1Q 99
ip address 192.168.0.1 255.255.255.0
ip nat inside
interface Serial0/1/0
interface Serial0/1/1
interface GigabitEthernet0
vrf forwarding Mgmt-intf
no ip address
negotiation auto
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip http client source-interface GigabitEthernet0/0/0
ip nat inside source list 1 interface GigabitEthernet0/0/0
overload
ip nat inside source list 10 interface GigabitEthernet0/0/0
overload
ip nat inside source list 20 interface GigabitEthernet0/0/0
overload
ip nat inside source list 30 interface GigabitEthernet0/0/0
overload
ip route 0.0.0.0 0.0.0.0 dhcp
access-list 1 permit 192.168.0.0 0.0.0.255
access-list 10 permit 192.168.10.0 0.0.0.255
access-list 20 permit 192.168.20.0 0.0.0.255
access-list 30 permit 192.168.30.0 0.0.0.255
ip access-list extended 101
control-plane
line con 0
transport input none
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
```

```
end
```

### **Configuration for BeefyFiveLayerBurrito (Switch)**

```
Current configuration : 5307 bytes
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname BeefyFiveLayerBurrito
boot-start-marker
boot-end-marker
no aaa new-model
system mtu routing 1500
authentication mac-move permit
ip subnet-zero
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
vlan internal allocation policy ascending
interface FastEthernet0/1
    switchport trunk encapsulation dot1q
    switchport mode trunk
interface FastEthernet0/2
    switchport access vlan 99
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 10,20,30,99
    switchport mode trunk
interface FastEthernet0/3
    switchport access vlan 99
interface FastEthernet0/4
    switchport access vlan 99
interface FastEthernet0/5
    switchport access vlan 99
interface FastEthernet0/6
    switchport access vlan 99
interface FastEthernet0/7
    switchport access vlan 99
interface FastEthernet0/8
    switchport access vlan 99
interface FastEthernet0/9
    switchport access vlan 99
interface FastEthernet0/10
    switchport access vlan 99
interface FastEthernet0/11
    switchport access vlan 99
interface FastEthernet0/12
```

```
switchport access vlan 99
interface FastEthernet0/13
  switchport access vlan 99
interface FastEthernet0/14
  switchport access vlan 99
interface FastEthernet0/15
  switchport access vlan 99
interface FastEthernet0/16
  switchport access vlan 99
interface FastEthernet0/17
  switchport access vlan 99
interface FastEthernet0/18
  switchport access vlan 99
interface FastEthernet0/19
  switchport access vlan 99
interface FastEthernet0/20
  switchport access vlan 99
interface FastEthernet0/21
  switchport access vlan 99
interface FastEthernet0/22
  switchport access vlan 99
interface FastEthernet0/23
  switchport access vlan 99
interface FastEthernet0/24
  switchport access vlan 99
interface FastEthernet0/25
  switchport access vlan 99
interface FastEthernet0/26
  switchport access vlan 99
interface FastEthernet0/27
  switchport access vlan 99
interface FastEthernet0/28
  switchport access vlan 99
interface FastEthernet0/29
  switchport access vlan 99
interface FastEthernet0/30
  switchport access vlan 99
interface FastEthernet0/31
  switchport access vlan 99
interface FastEthernet0/32
  switchport access vlan 99
interface FastEthernet0/33
  switchport access vlan 99
interface FastEthernet0/34
  switchport access vlan 99
interface FastEthernet0/35
  switchport access vlan 99
```

```

interface FastEthernet0/36
  switchport access vlan 99
interface FastEthernet0/37
  switchport access vlan 99
interface FastEthernet0/38
  switchport access vlan 99
interface FastEthernet0/39
  switchport access vlan 99
interface FastEthernet0/40
  switchport access vlan 99
interface FastEthernet0/41
  switchport access vlan 99
interface FastEthernet0/42
  switchport access vlan 99
interface FastEthernet0/43
  switchport access vlan 99
interface FastEthernet0/44
  switchport access vlan 99
interface FastEthernet0/45
  switchport access vlan 99
interface FastEthernet0/46
  switchport access vlan 99
  switchport mode access
interface FastEthernet0/47
  switchport access vlan 99
  switchport mode access
interface FastEthernet0/48
  switchport access vlan 99
interface GigabitEthernet0/1
interface GigabitEthernet0/2
interface GigabitEthernet0/3
interface GigabitEthernet0/4
interface Vlan1
  no ip address
ip classless
ip http server
ip http secure-server
ip sla enable reaction-alerts
line con 0
line vty 0 4
  login
line vty 5 15
  login
end

```

### **Routing Table for DoritosLocosTaco**

```

S*      0.0.0.0/0 [1/0] via 192.168.40.1
        192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks

```

```

C      192.168.0.0/24 is directly connected, GigabitEthernet0/0/1.99
L      192.168.0.1/32 is directly connected, GigabitEthernet0/0/1.99
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.10.0/24 is directly connected,
GigabitEthernet0/0/1.10
L      192.168.10.1/32 is directly connected,
GigabitEthernet0/0/1.10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.20.0/24 is directly connected,
GigabitEthernet0/0/1.20
L      192.168.20.1/32 is directly connected,
GigabitEthernet0/0/1.20
      192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.30.0/24 is directly connected,
GigabitEthernet0/0/1.30
L      192.168.30.1/32 is directly connected,
GigabitEthernet0/0/1.30
C      192.168.40.0/23 is directly connected, GigabitEthernet0/0/0
      192.168.40.0/32 is subnetted, 1 subnets
L      192.168.40.110 is directly connected, GigabitEthernet0/0/0

```

## Problems

Originally, our AP did not connect to the WLC, and we couldn't figure out why. It turns out that this was due to the time being set incorrectly on the WLC. The time is set to January 1, 2000 at 12:00AM by default, which prevents an HTTPS connection from being formed between the AP and the WLC as the AP's certificates are set to only work after a certain date. This problem is the reason that setting the time on the WLC is one of the first configuration steps we outline in this lab.

Originally, we checked the "Guest LAN" box for the Guest VLAN interface, assuming that this option was necessary. It turns out that the Guest Lan option is meant for guest authentication for wired clients, and will not work for a wireless guest network.

Interfaces > Edit

<b>General Information</b>	
Interface Name	Guest VLAN
MAC Address	00:9e:1e:8f:b0:20
<b>Configuration</b>	
Guest Lan	<input checked="" type="checkbox"/>
NAS-ID	none
<b>Physical Information</b>	
Port Number	0
Backup Port	0
Active Port	0
<b>Interface Address</b>	
VLAN Identifier	10
DHCP Proxy Mode	Global
Enable DHCP Option 82	<input type="checkbox"/>

## Conclusion

To wrap up, I am now much more confident in my skills setting up wireless networks, especially in their addressing and security settings. I also now understand RADIUS and its open-source implementations to a much greater extent, and am confident that I could replicate this setup in a real-world environment. This type of

network with three WLANs, one for guest use, personal use, and secure use, is especially useful in the real world, and is very similar to the WLAN configuration that our school district uses for tens of thousands of students and staff.





# **Fortinet Cybersecurity Academy: 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

## 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.

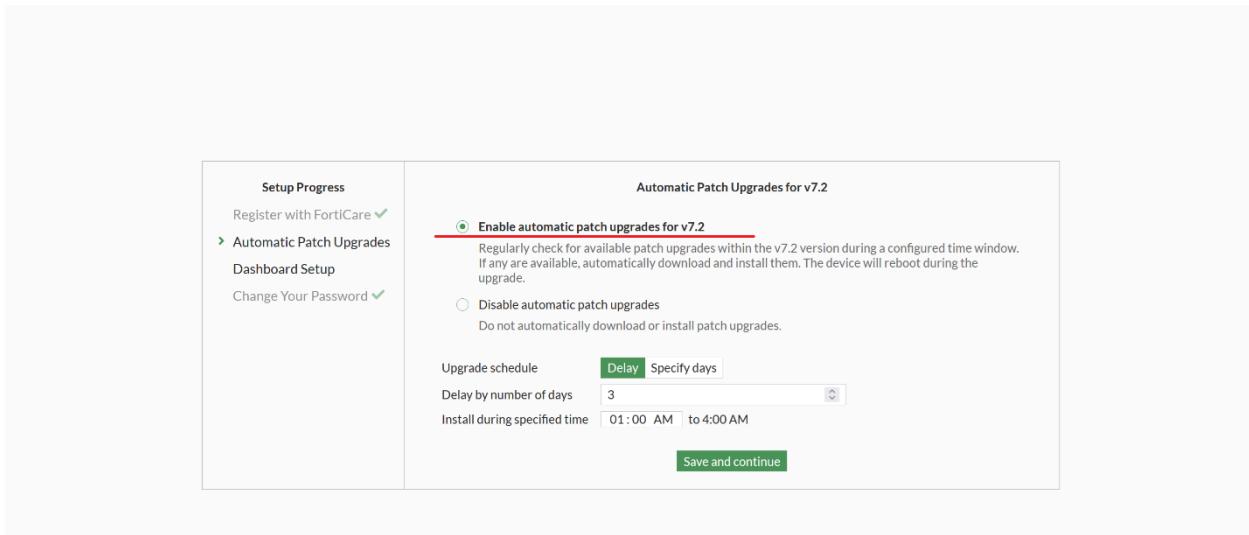
**FortiGate Setup**

**⚠** Perform the following steps to complete the setup of this FortiGate.

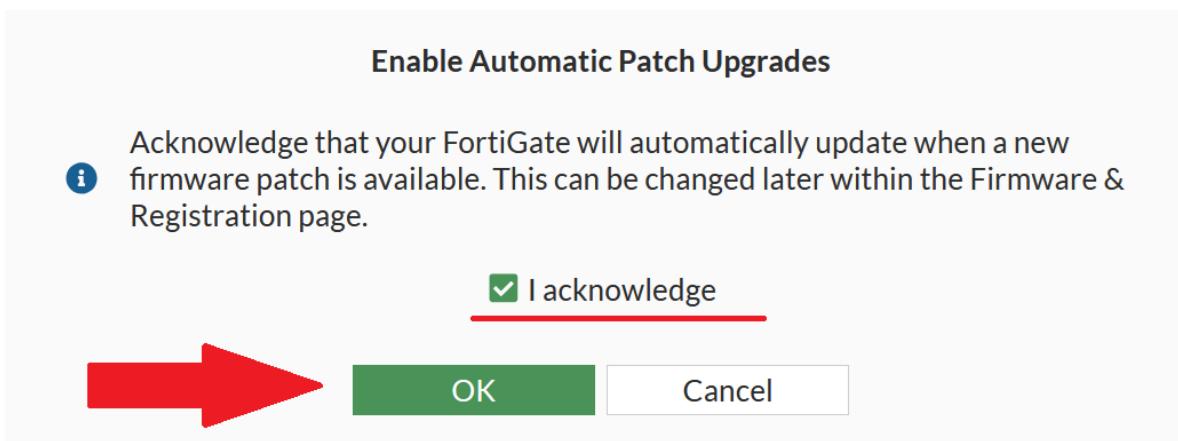
- Register with FortiCare ✓
- Automatic Patch Upgrades
- Dashboard Setup
- Change Your Password ✓

**Begin**

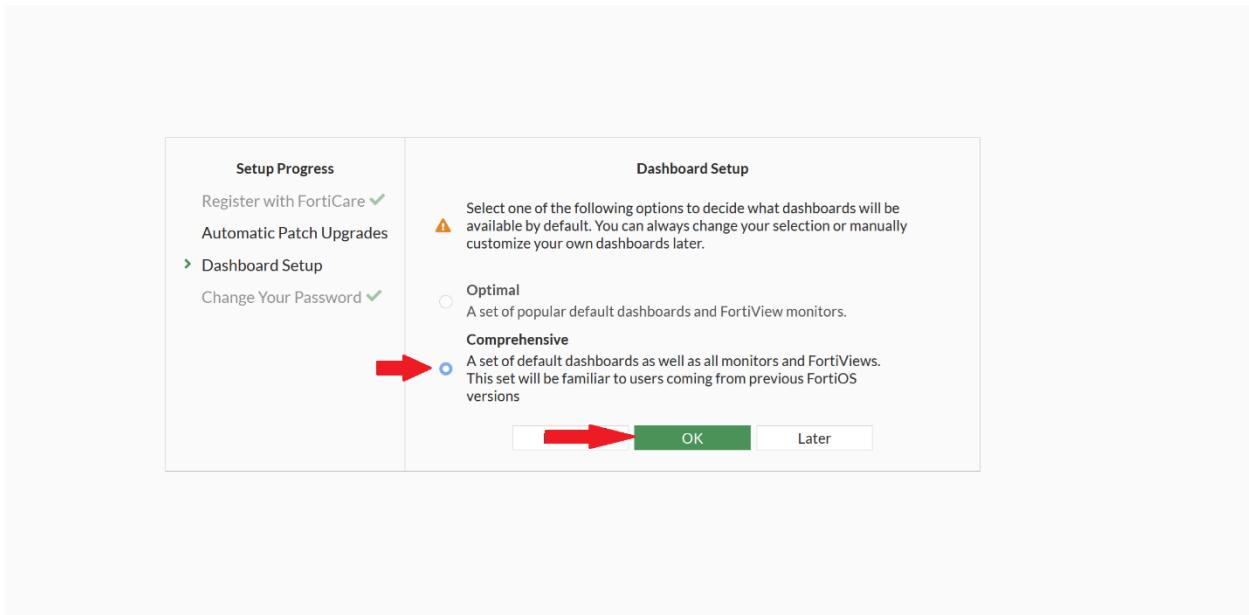
Click Enable Automatic Patch Upgrades and leave the other settings as default.



Click I acknowledge and click OK.



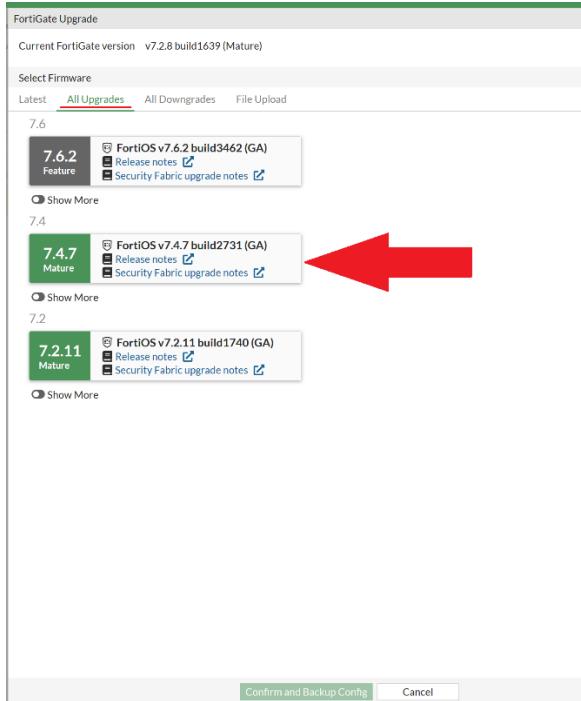
Choose the comprehensive dashboard and click OK.



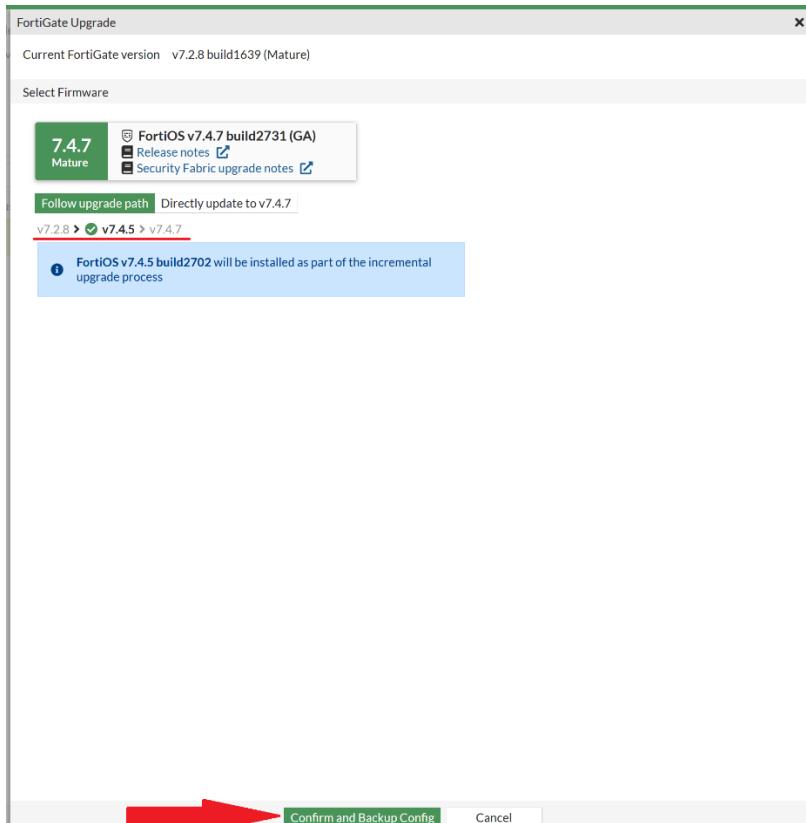
You should now see the main fortigate dashboard page. Next, we will update the system firmware. Click on System > Fabric Management (may be called Firmware and Registration in newer versions), click on the Fortigate 40F, then click Upgrade.

The screenshot shows the 'Fabric Management' page. On the left, the navigation menu is expanded to show 'System' and 'Fabric Management'. In the center, there are two circular dashboards: 'Device Type' (FortiGate) and 'Upgrade Status' (Upgrade available). Below these are buttons for 'Fabric Upgrade' and 'Upgrade'. A red arrow points to the 'Upgrade' button. The main table lists one device, 'FortiGate-40F', which is highlighted with a red arrow. The table columns include Device, Status, Registration Status, Firmware Version, and Upgrade Status. The 'FortiGate-40F' row shows 'Online', 'Registered', 'v7.2.8.build1639(Mature)', and 'v7.2.11(Mature) available'.

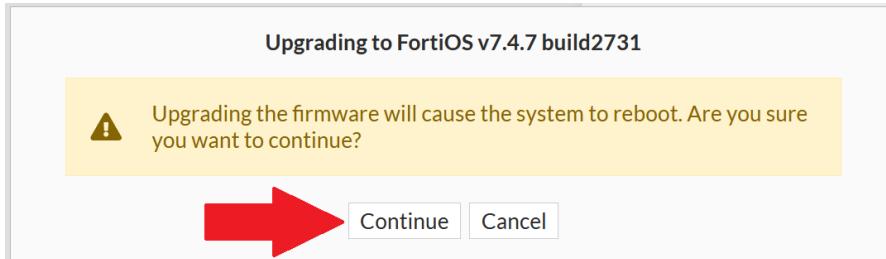
Click All Upgrades, then select the version you would like to upgrade to. In this lab, we opted to update to the latest version of FortiOS 7.4, as at the time, it was the latest version with a focus on bugfixes and stability (7.6 focused on feature updates, and wasn't as stable)



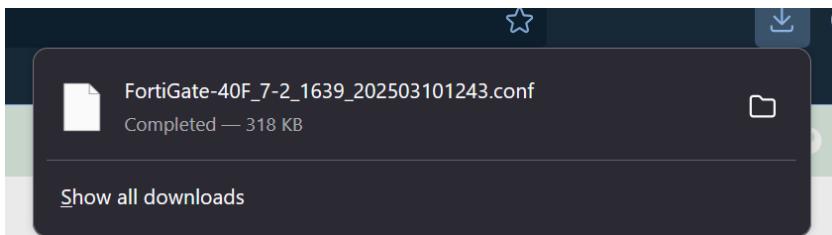
Click Confirm and Backup Config. Note that in most cases, multiple different versions of FortiOS will be installed as part of an incremental upgrade process. While there is an option to directly update between versions, following an upgrade path can decrease the chances of corrupting your configuration.



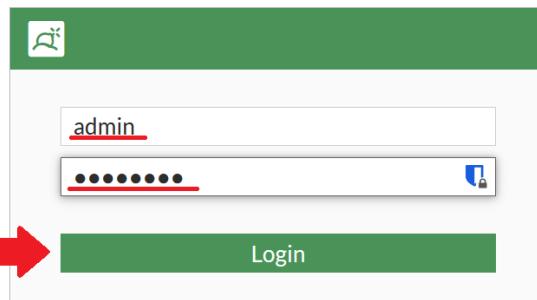
Click Continue, and wait for the upgrade process to complete.



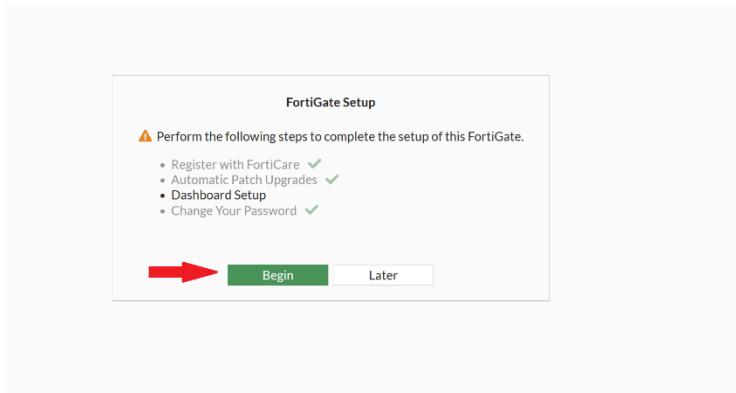
Note that a backup configuration file will be downloaded locally.

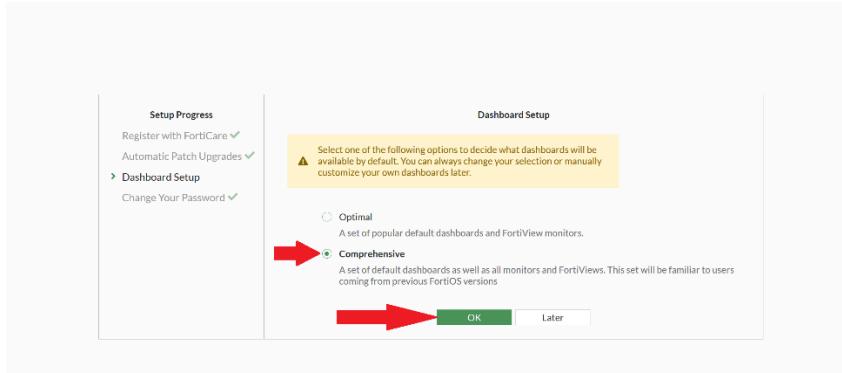


When the upgrade process is complete, reload the page and log in again.

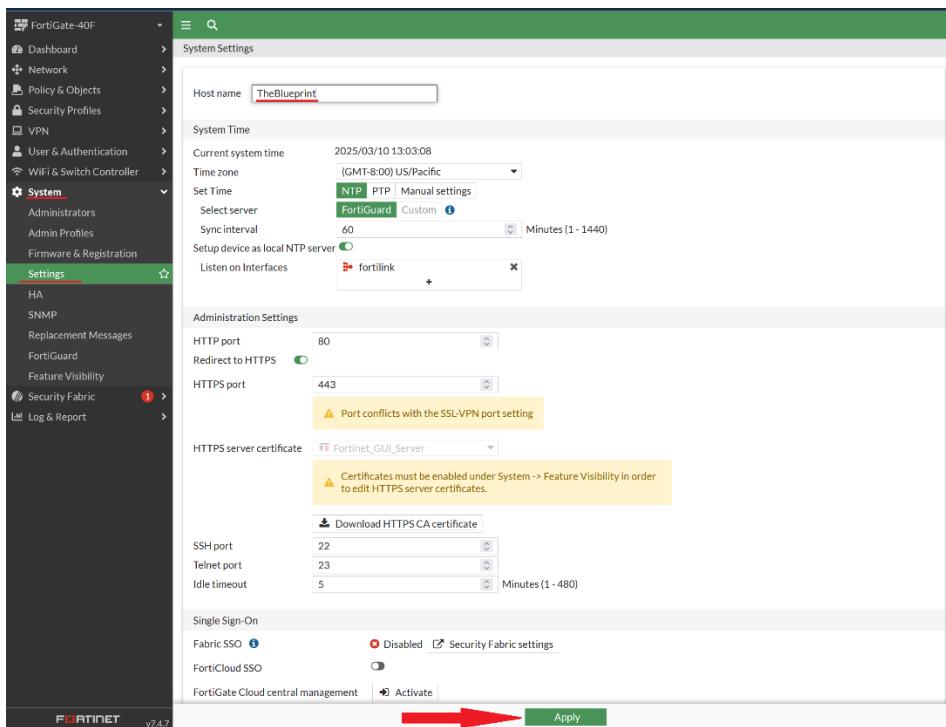


You may be asked to complete dashboard setup again. In this case, choose the Comprehensive dashboard like before.

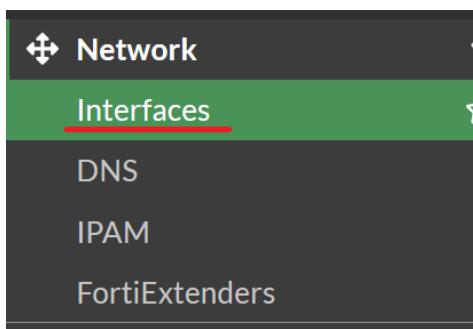




You should now see the firewall's dashboard. Next, we will configure a hostname for the firewall. Go to System > Settings, enter a host name, and click Apply.



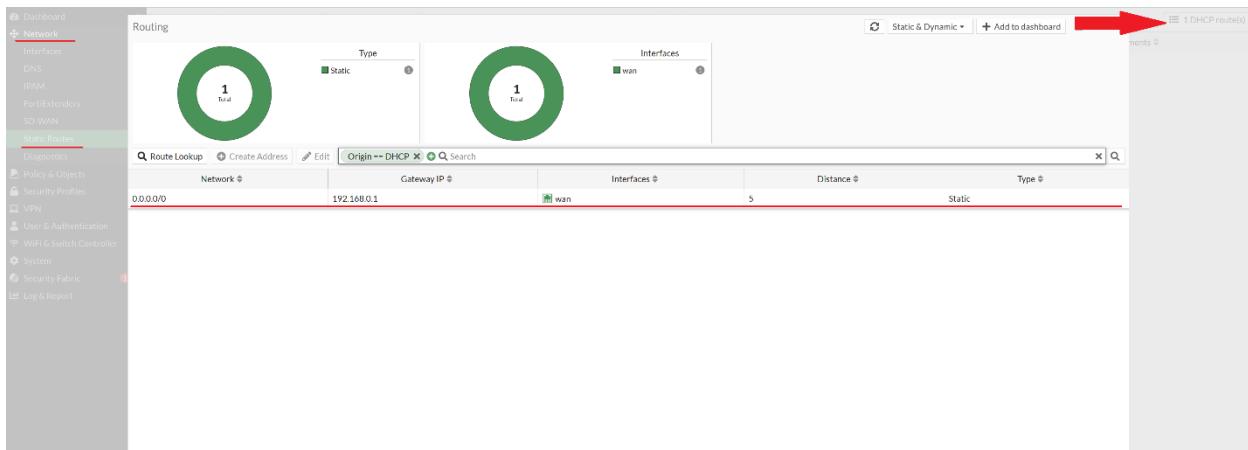
We will now verify the firewall's basic configuration. Go to Network > Interfaces.



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.

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref
802.3ad Aggregate 1	802.3ad Aggregate	fortilink	Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
Hardware Switch 1	Hardware Switch	lan	PC lan1 lan2 lan3	192.168.1.99/255.255.255.0 PING HTTPS SSH Security Fabric Connection	1	192.168.1.110-192.168.1.210 DHCP Address Range given out by firewall	3
Physical Interface 1	Physical Interface	wan	Address assigned by ISP 192.168.0.26/255.255.255.0	PING			1
Tunnel Interface 1	Tunnel Interface						

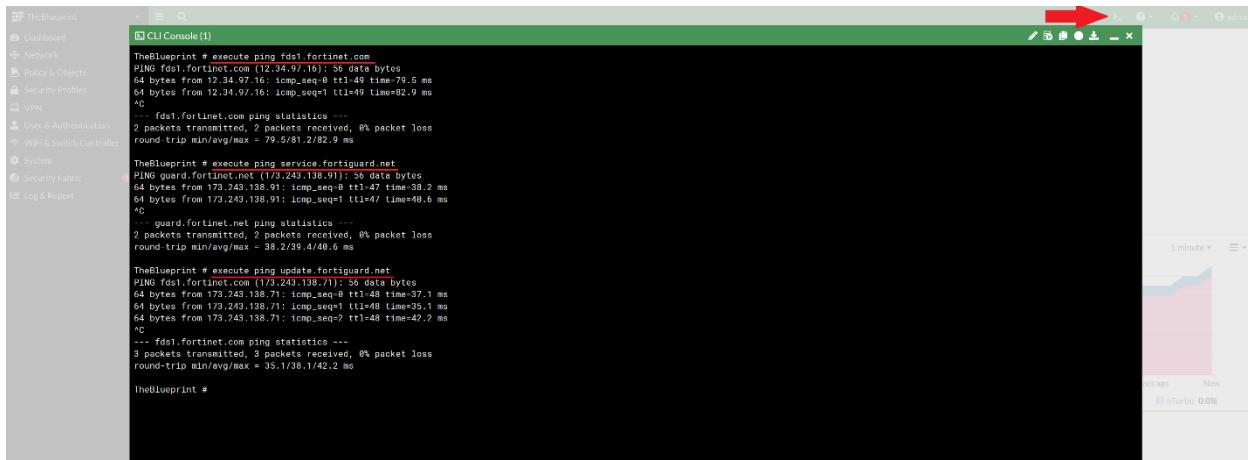
Next, click on Network > Static Routes and click on DHCP routes. You should see that a default route out the WAN interface has automatically been configured.



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.

The screenshot shows the 'License Information' section of the FortiGuard interface. It lists various services under 'Entitlement' and their current 'Status'. Services include Advanced Malware Protection, Attack Surface Security Rating, Data Loss Prevention (DLP), Email Filtering, Intrusion Prevention, Operational Technology (OT) Security Service, and Web Filtering. Most services are licensed, with some like DLP and Web Filtering having expiration dates in January 2027. Other services like SD-WAN Network Monitor and SD-WAN Overlay as a Service are not licensed. The 'Firmware & General Updates' section shows a license for January 2027. A note at the bottom indicates that FortiCare support contracts can be activated here and applied directly to this FortiGate, with an option to 'Enter Registration Code'.

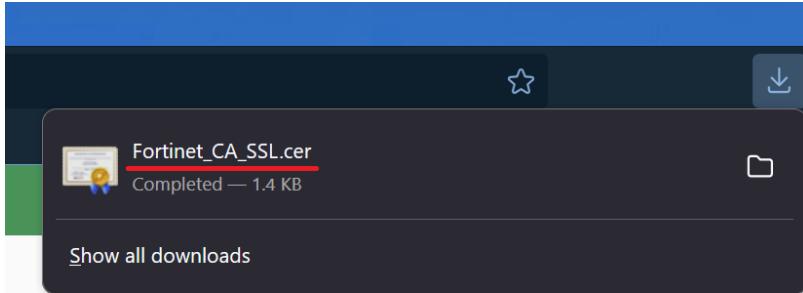
Next, go to Policy & Objects > Firewall Policy and ensure there is a policy allowing traffic between the LAN and WAN interfaces.

The screenshot shows the 'Firewall Policy' table. A single policy entry is visible, allowing traffic from 'lan' to 'wan'. The 'Action' column shows 'ACCEPT'. Other columns include 'Source' (all), 'Destination' (all), 'Schedule' (always), 'Service' (ALL), 'IP Pool' (NAT), 'NAT' (NAT), 'Type' (Standard), 'Security Profiles' (no-inspection), 'Log' (UTM), and 'Bytes' (320.53 MB).

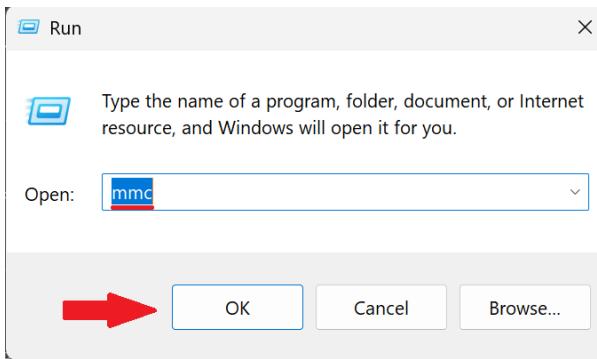
Return to the dashboard page, and under Administrators, click Download HTTPS CA certificate.

The screenshot shows the 'Administrators' page. It lists two users: 'FortiExplorer' and 'admin'. Under 'Actions', there is a blue button labeled 'Download HTTPS CA certificate' with a red arrow pointing to it. Below the button is a small 'x' icon.

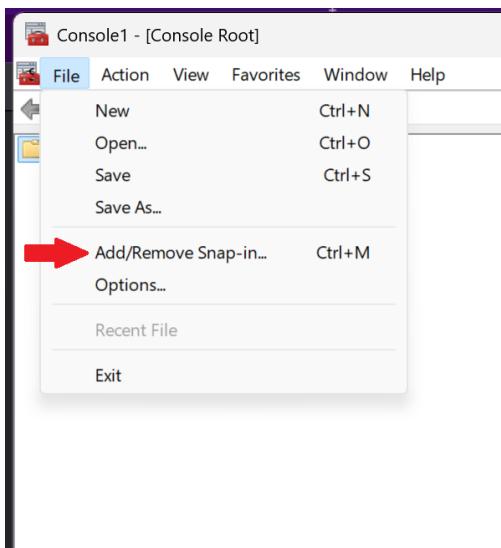
You should see a certificate file download to your PC.



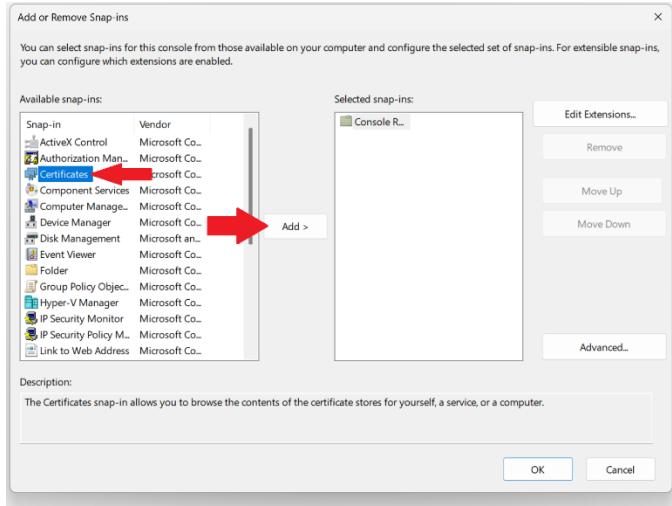
Next, we will install this certificate. On your PC, open the Run dialog (Windows+R) and type "mmc".



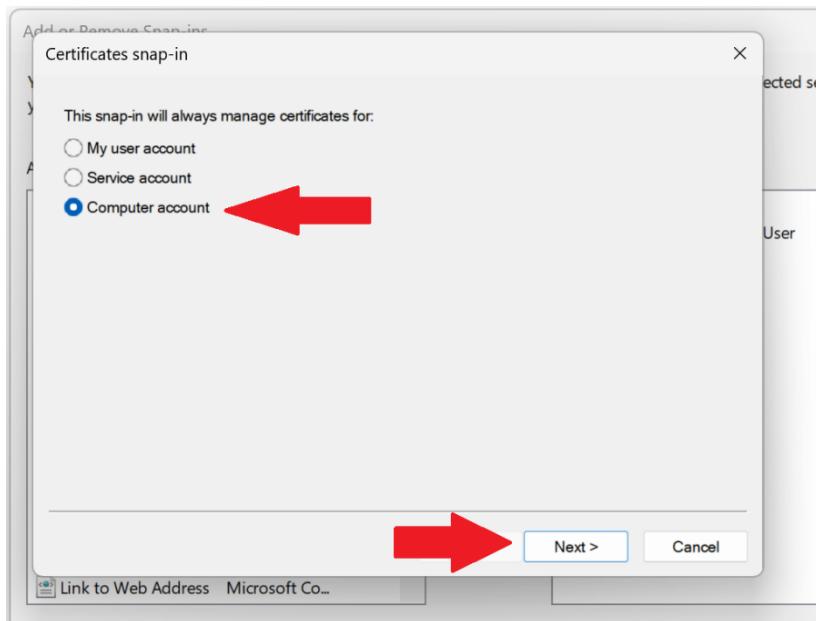
In the resulting window, click File > Add/Remove Snap-in.



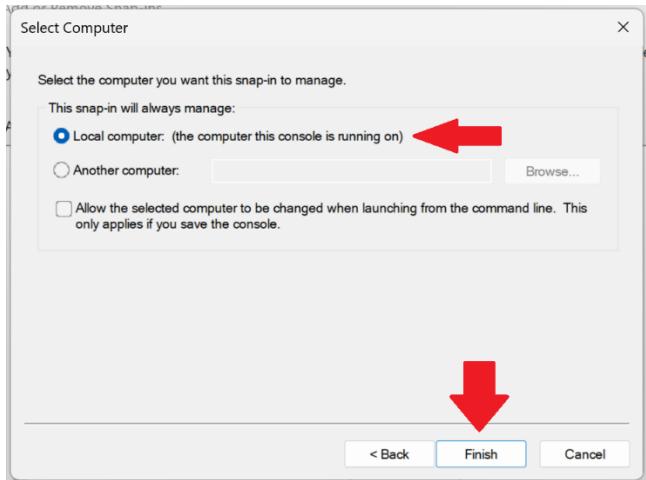
In the resulting window, click on Certificates > Add.



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



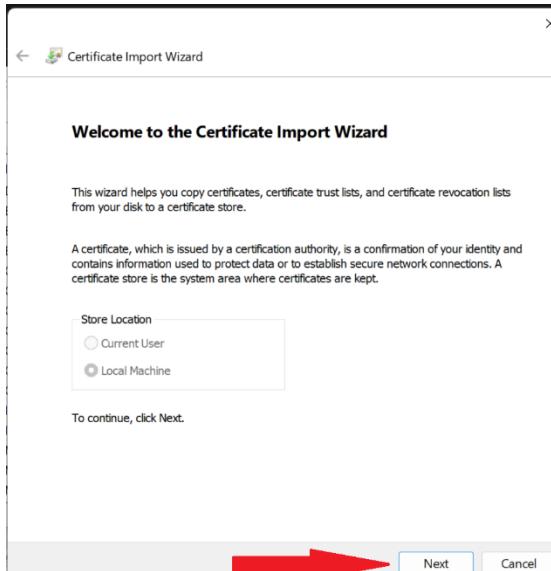
Make sure Local Computer is selected and click Finish.



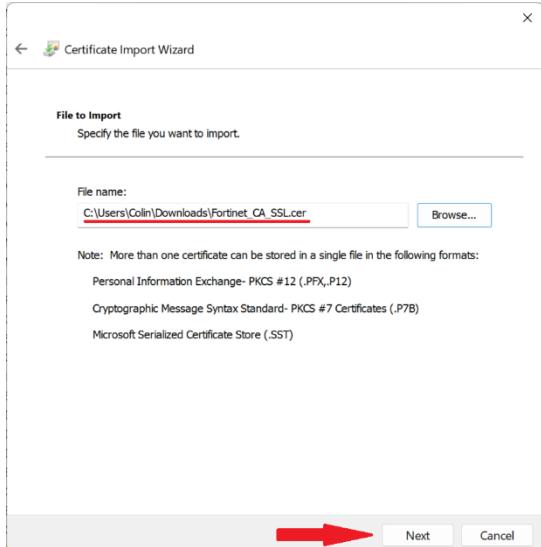
Inside Trusted Root Certification Authorities, right-click on Certificates and click on All Tasks > Import.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Type
AAA Certificate Services	Baltimore CyberTrust Root	12/31/2025	Client Authentication, Server Authentication	Sectigo (AAA)	Client Authentication, Server Authentication	DigiCert Baltimore R...
Baltimore CyberTrust Root		5/12/2025				<None>
CCNPBigBoy	CCNPBigBoy	1/7/2024				<None>
CCNPBigBoy	CCNPBigBoy	4/4/2024				<None>
Certum Trusted Network CA 2	Certum Trusted Network CA 2	12/31/2029	Client Authentication, Server Authentication	Certum Trusted Net...	Client Authentication, Server Authentication	Certum Trusted Net...
Class 3 Public Primary Certificate	Class 3 Public Primary Certificate	8/1/2028	Client Authentication, Time Stamping	VerSign Class 3 Pub...	Client Authentication, Time Stamping	Microsoft Timestamp...
DigiCert Assured ID Root CA	DigiCert Assured ID Root CA	11/9/2031	Client Authentication	DigiCert	Client Authentication	DigiCert
DigiCert CS RSA4096 Root G5	DigiCert CS RSA4096 Root G5	1/14/2046	Code Signing, Time S...	DigiCert CS RSA4096...	Code Signing, Time S...	DigiCert
DigiCert Global Root CA	DigiCert Global Root CA	11/9/2031	Client Authentication	DigiCert	Client Authentication	DigiCert
DigiCert Global Root G2	DigiCert Global Root G2	1/15/2038	Client Authentication	DigiCert Global Root...	Client Authentication	DigiCert Global Root...
DigiCert Global Root G3	DigiCert Global Root G3	1/15/2038	Client Authentication	DigiCert Global Root...	Client Authentication	DigiCert Global Root...
DigiCert High Assurance EV Root CA	DigiCert High Assurance EV Root CA	11/9/2031	Time Stamping, Sec...	DigiCert	Time Stamping, Sec...	DigiCert
DigiCert Trusted Root G4	DigiCert Trusted Root G4	1/15/2038	Client Authentication	DigiCert Trusted Ro...	Client Authentication	DigiCert Trusted Ro...
DST Root CA X3	DST Root CA X3	9/30/2021	Client Authentication	DST Root CA X3	Client Authentication	DST Root CA X3

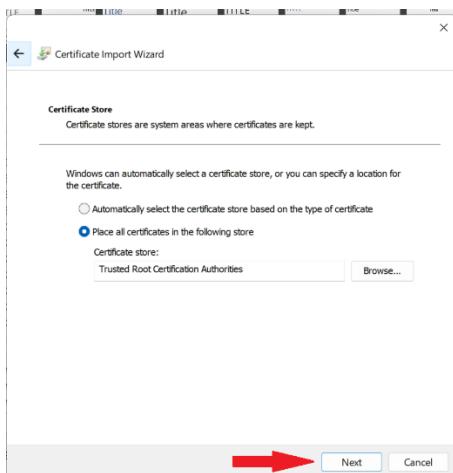
Click "Next".



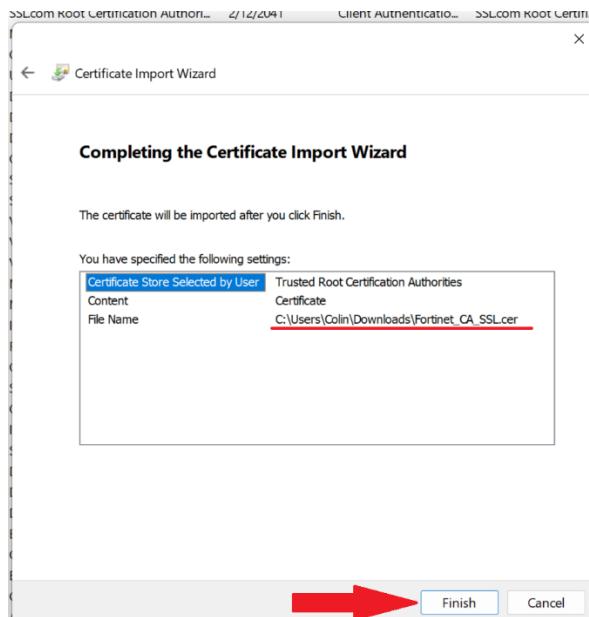
Select the certificate file downloaded earlier, then click "Next" again.



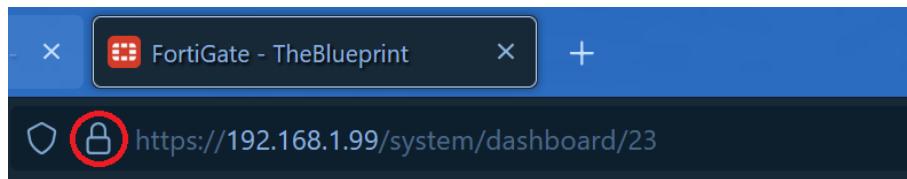
Leave the certificate store location setting as the default value, then click “Next”.



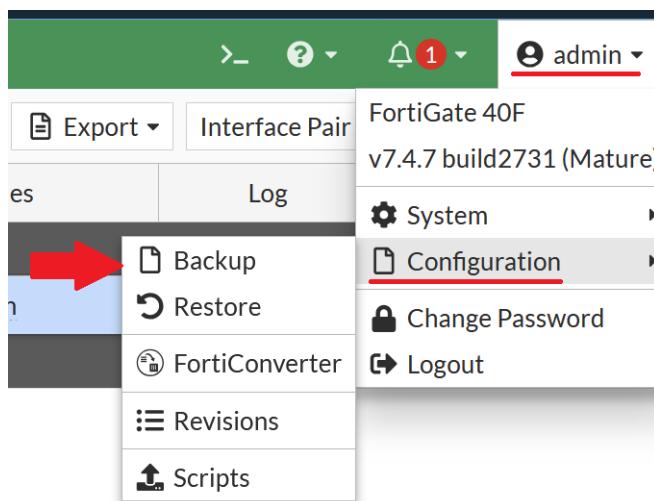
Click “Finish” to confirm the certificate import.



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



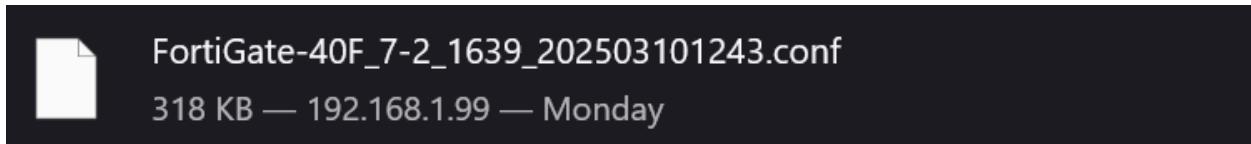
Next, we will back up the firewall's configuration. Click on the admin profile picture in the top right, then click on Configuration > Backup.



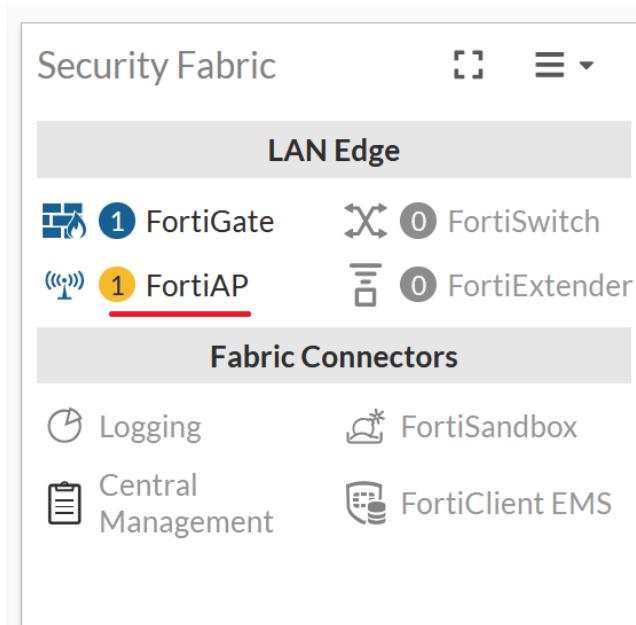
Enable Encryption and enter a secure password for the backup. Click OK.



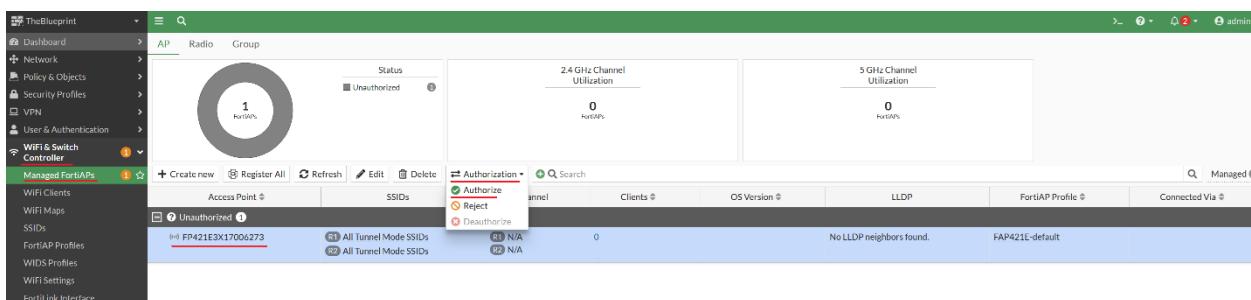
The backup file will be downloaded to your PC.



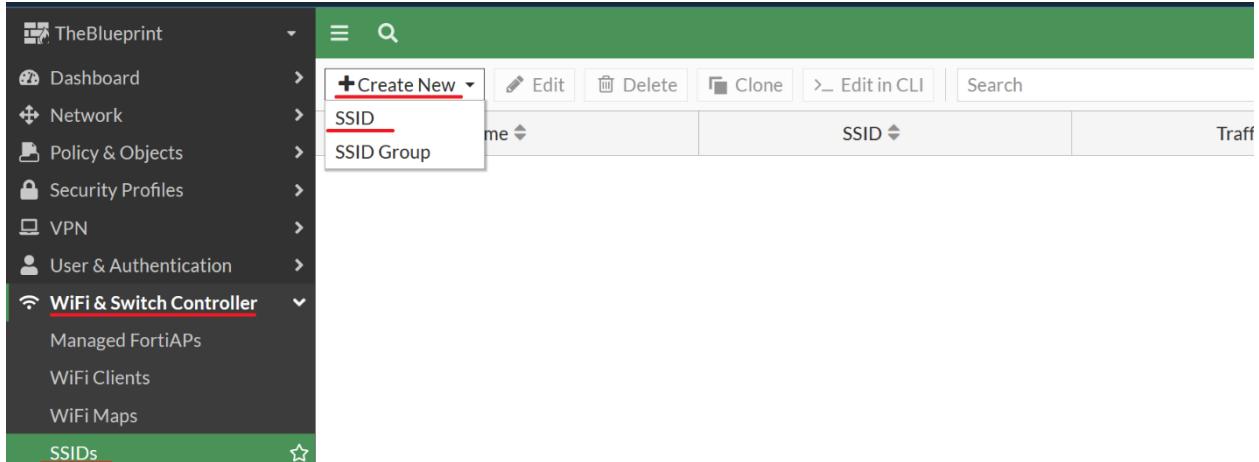
Next, we will set up the AP. Return to the Dashboard, and under Security Fabric, ensure that one (1) FortiAP device is visible.



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.

**Create New SSID**

**Name:** 2-PAC  
**Alias:** PSK  
**Type:** WiFi SSID  
**Traffic mode:** Tunnel

**Address**

**Addressing mode:** Manual | IPAM | One-Arm Sniffer  
**IP/Netmask:** 192.168.50.1/24  
Create address object matching subnet  
**Name:** 2-PAC address  
**Destination:** 192.168.50.0/24  
**Secondary IP address:** (disabled)

**Administrative Access**

**IPv4:**  HTTPS,  FMG-Access,  FTM,  Speed Test  
 HTTP,  SSH,  RADIUS Accounting,  PING,  SNMP,  Security Fabric Connection

**DHCP Server**

**DHCP status:** Enabled  
**Address range:** 192.168.50.2-192.168.50.254  
**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 seconds(s)

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.

Network  
Device detection

WiFi Settings  
SSID: 2-PAC  
Client limit:   
Broadcast SSID:   
Beacon advertising:  Name  Model  Serial number

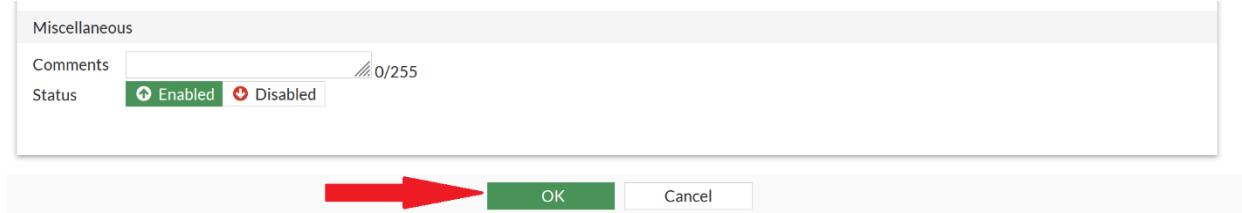
Security Mode Settings  
Security mode: WPA2 Personal  
Captive Portal:

Pre-shared Key  
Mode: Single  
Passphrase:

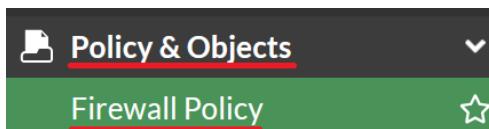
Client MAC Address Filtering  
RADeUS server:   
Address group policy: Allow Deny

Additional Settings  
Schedule:   
Block intra-SSID traffic:   
Optional VLAN ID: 0  
Broadcast suppression: ARP for known clients DHCP unicast DHCP uplink   
Quarantine host:   
VLAN pooling:   
NAC profile:

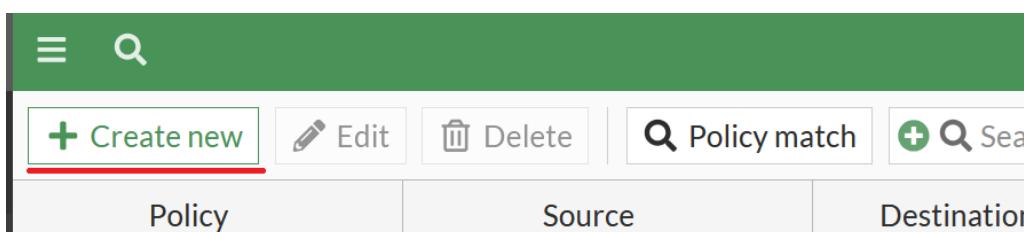
Click OK.



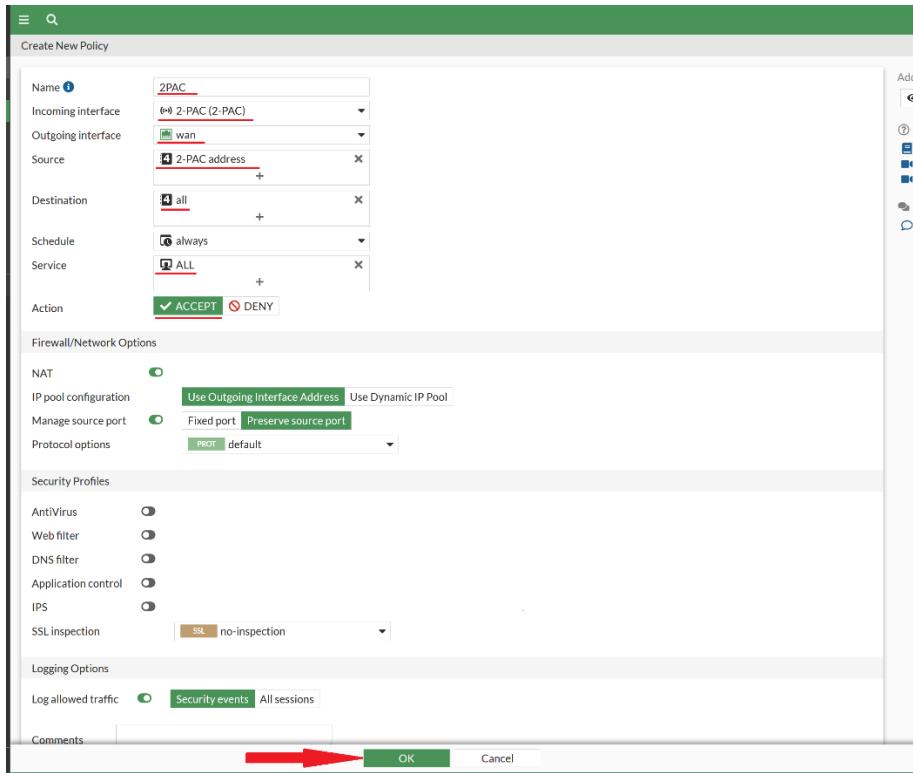
Go to Policy & Objects > Firewall Policy.



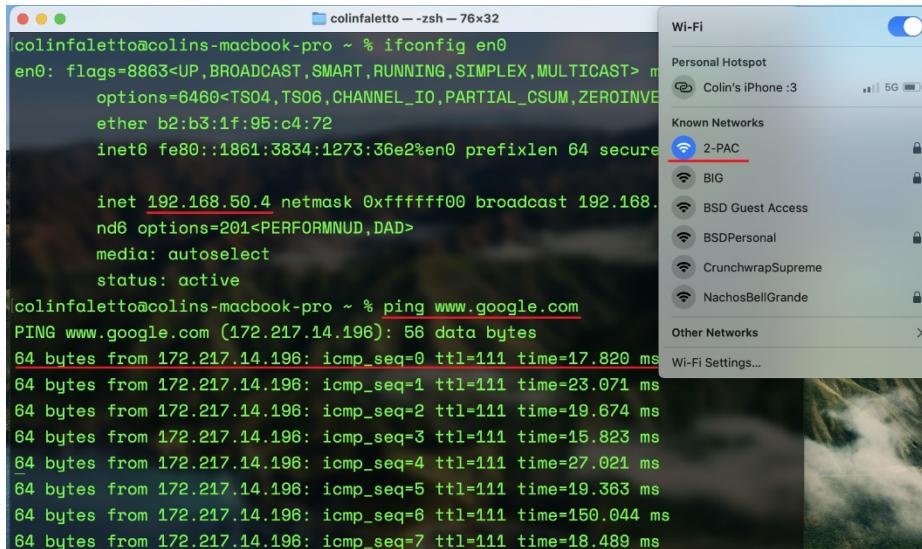
Click Create new.



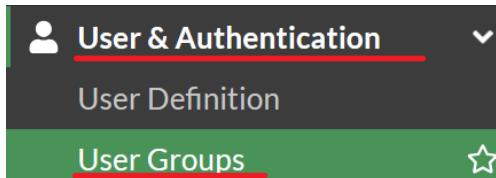
Configure an appropriate name. Set the incoming/outgoing interface to the PSK WLAN and the WAN respectively. Set the source and destination to the PSK address object and "all" respectively. Set the action to Accept and click OK.



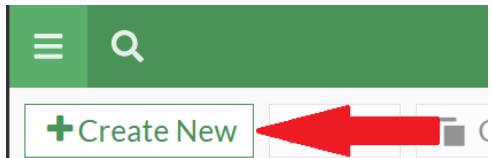
Your PSK WLAN should now be fully set up. Confirm that it works by connecting another device, inputting the password configured earlier. As seen in the screenshot below, when connected to the 2-PAC network, my laptop receives an address in the 192.168.50.0/24 network, and can successfully ping outside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



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



Click Create New.



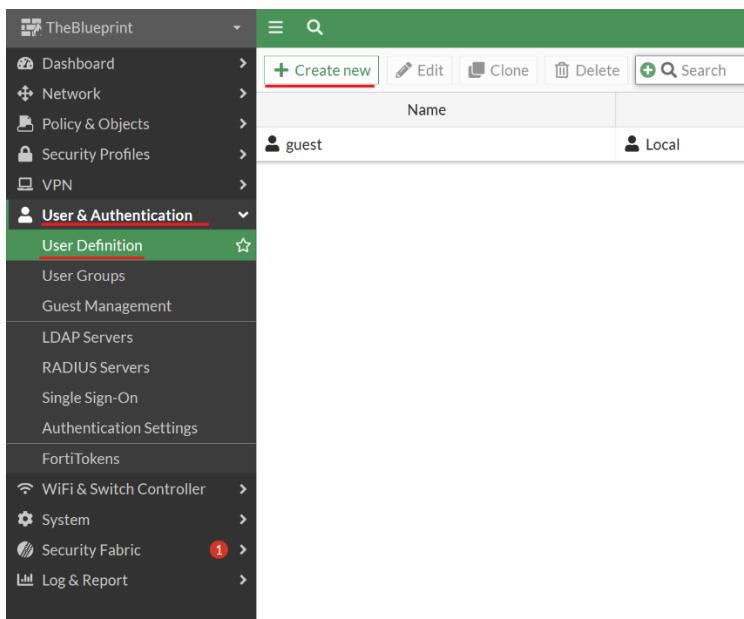
Choose an appropriate group name.

Name	<input type="text" value="BadBoy"/>
Type	Firewall
Members	<input type="button" value="+"/>

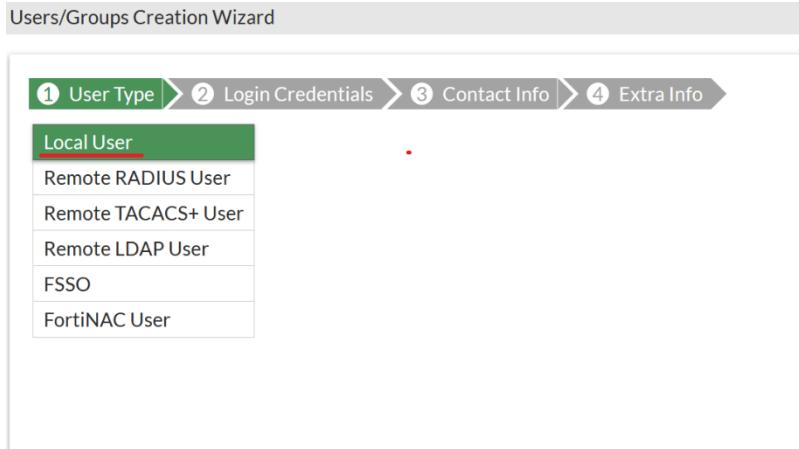
Click OK.



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



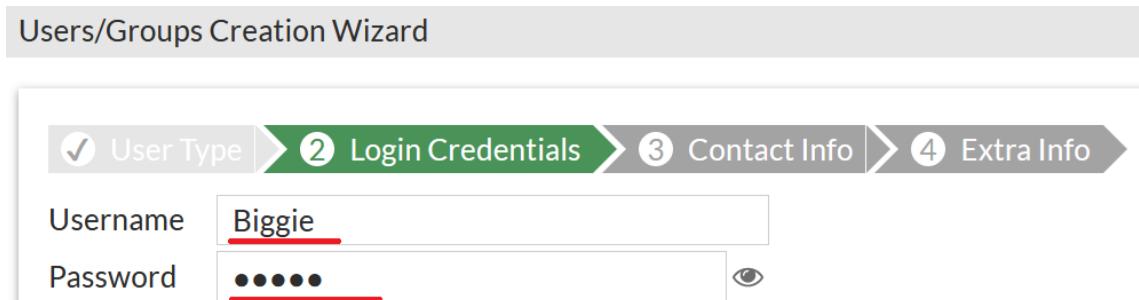
Set the User Type to Local User.



Click Next.



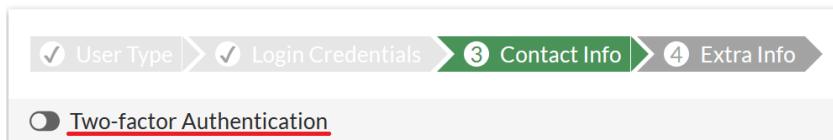
Set an appropriate username and password.



Click Next.



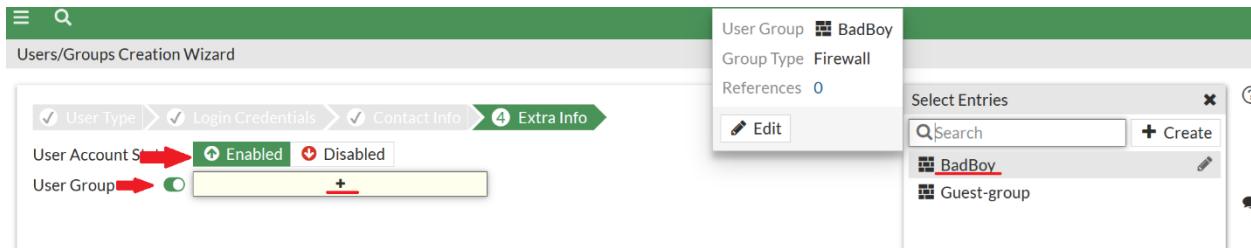
Under Contact Info, leave two-factor authentication off.



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.



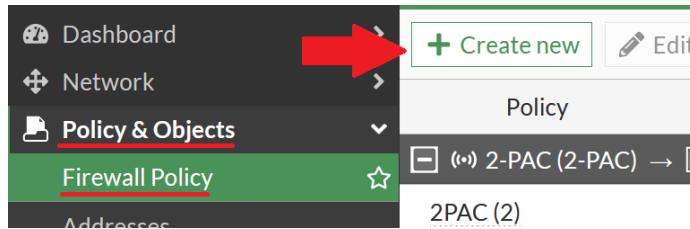
Assign an appropriate name (in this case, we chose BIG) and alias. Assign an appropriate IP/netmask, and ensure that an address object is created matching the subnet. Ensure that a DHCP server for the subnet is created.

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.

Name	<input type="text" value="hypnotize"/>
Incoming interface	<input type="text" value="BIG (BIG)"/>
Outgoing interface	<input type="text" value="wan"/>
Source	<input type="text" value="BIG address"/> <input type="button" value="+"/>
Destination	<input type="text" value="all"/> <input type="button" value="+"/>
Schedule	<input type="text" value="always"/>
Service	<input type="text" value="ALL"/> <input type="button" value="+"/>
Action	<input checked="" type="radio"/> ACCEPT <input type="radio"/> DENY

Click OK.

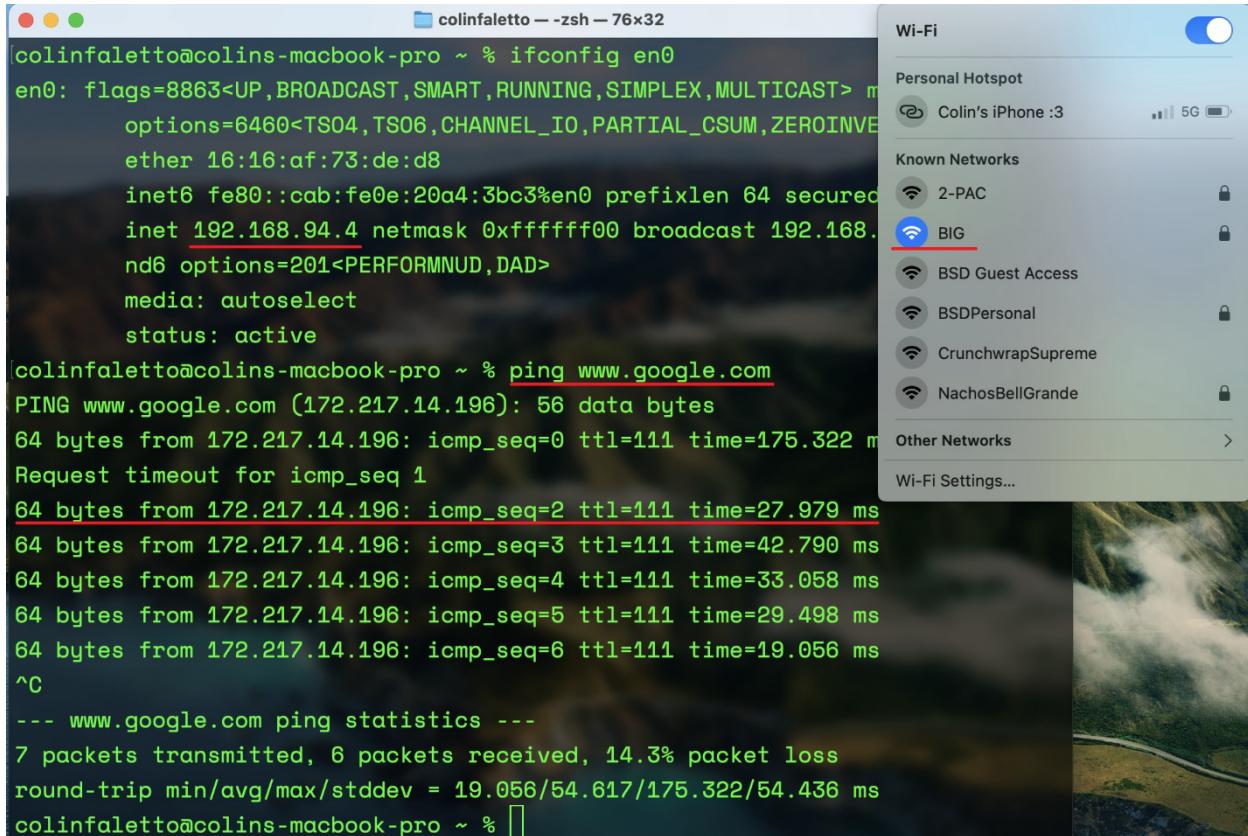


Your Enterprise WLAN has now been set up. To test it, connect from another WiFi-capable device. You should see a login prompt similar to this:



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 receives an address in the 192.168.94.0/24 subnet and can successfully ping outside the network.



The screenshot shows a Mac OS X desktop with a terminal window open and a Wi-Fi settings overlay.

**Terminal Output:**

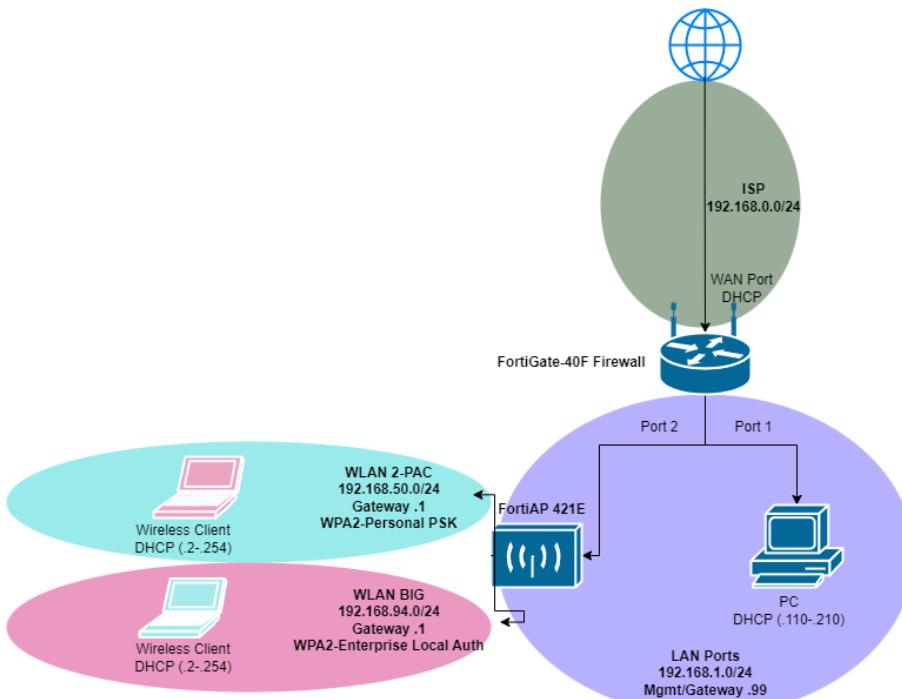
```
colinfaletto@colins-macbook-pro ~ % ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> media: autoselect status: active
    options=6460<TS04,TS06,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERTED>
    ether 16:16:af:73:de:d8
    inet6 fe80::cab:fe0e:20a4:3bc3%en0 prefixlen 64 secured
        inet 192.168.94.4 netmask 0xffffffff broadcast 192.168.94.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active

colinfaletto@colins-macbook-pro ~ % ping www.google.com
PING www.google.com (172.217.14.196): 56 data bytes
64 bytes from 172.217.14.196: icmp_seq=0 ttl=111 time=175.322 ms
Request timeout for icmp_seq 1
64 bytes from 172.217.14.196: icmp_seq=2 ttl=111 time=27.979 ms
64 bytes from 172.217.14.196: icmp_seq=3 ttl=111 time=42.790 ms
64 bytes from 172.217.14.196: icmp_seq=4 ttl=111 time=33.058 ms
64 bytes from 172.217.14.196: icmp_seq=5 ttl=111 time=29.498 ms
64 bytes from 172.217.14.196: icmp_seq=6 ttl=111 time=19.056 ms
^C
--- www.google.com ping statistics ---
7 packets transmitted, 6 packets received, 14.3% packet loss
round-trip min/avg/max/stddev = 19.056/54.617/175.322/54.436 ms
colinfaletto@colins-macbook-pro ~ %
```

**Wi-Fi Settings Overlay:**

- Personal Hotspot: Off
- Colin's iPhone :3 (5G)
- Known Networks:
  - 2-PAC (Locked)
  - BIG** (Selected, Locked)
  - BSD Guest Access
  - BSDPersonal
  - CrunchwrapSupreme
  - NachosBellGrande
- Other Networks: >
- Wi-Fi Settings...

## 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.