Homelab for Security Detection & Monitoring

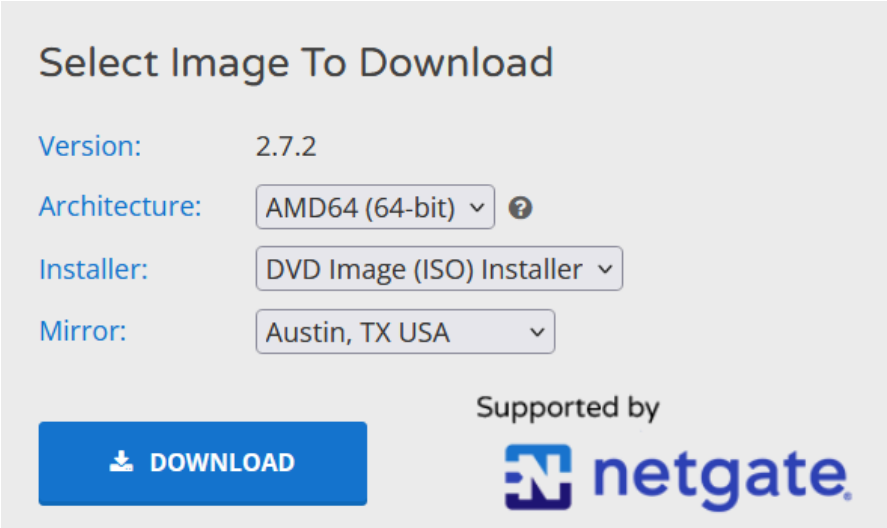
This is a homelab created following Day CyberWox's blueprint and documentation, available on his website. It's been changed slightly to use the more recent, up-to-date software versions and technologies. The lab was created using VMWare Workstation Pro 17; you don't need to buy a licence upfront since VMWare offers a 30-day free trial, which is what I will be using.

Contents:

Configuring pfSense as a Firewall

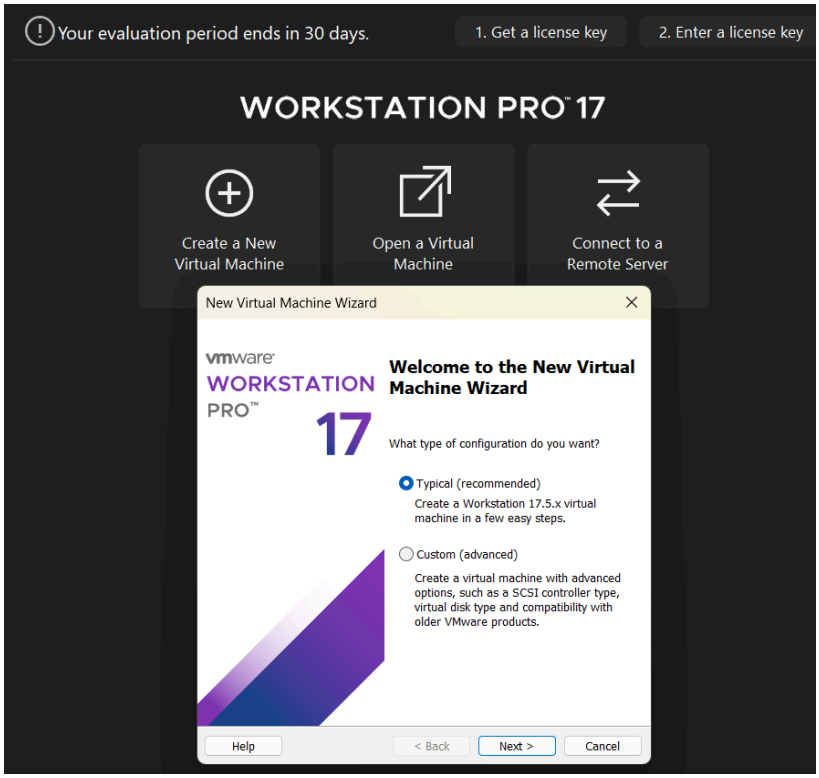
To create the pfSense firewall, we first need to download the ISO file, available on their website.

For 64-bit machines, the following should be selected before downloading (select the nearest location to you from the 'Mirror' dropdown):

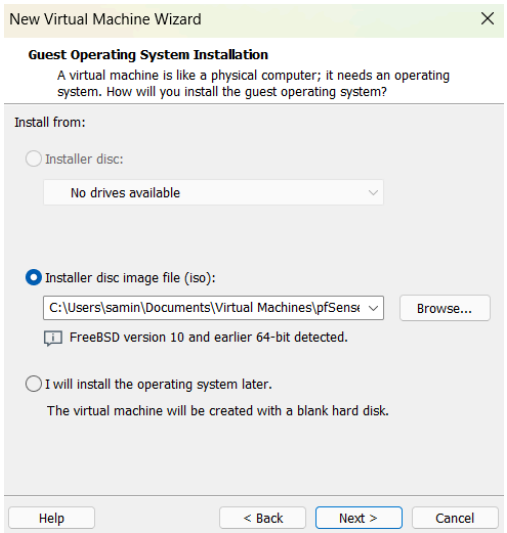


Extracting the downloaded file using the Windows Extractor gave an error, so I used 7zip instead

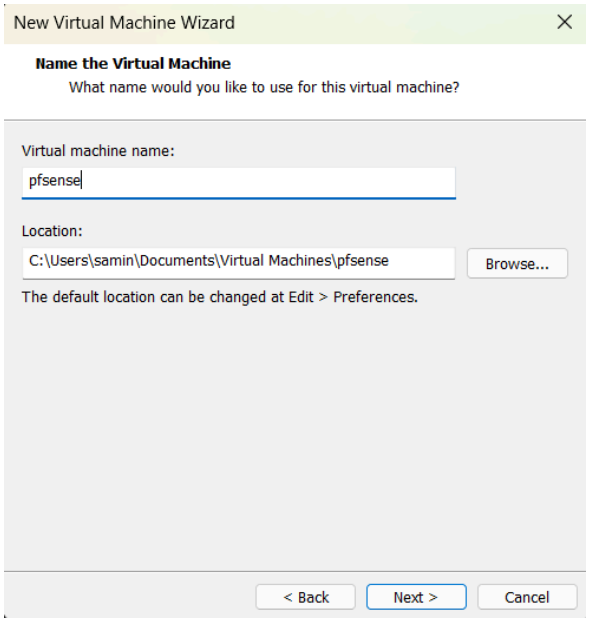
Open up VMWare and click "Create a New Virtual Machine" - ensure the "Typical" is selected before clicking "Next":



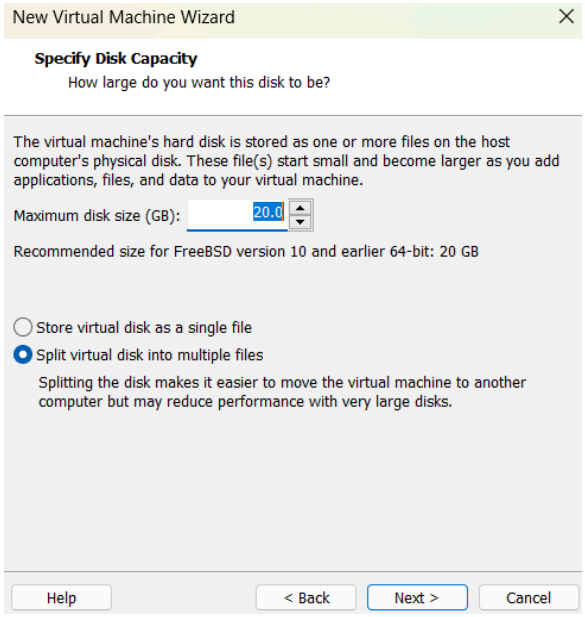
Select the ISO file by clicking “Browse” and browsing to where the file is located before clicking “Next”:



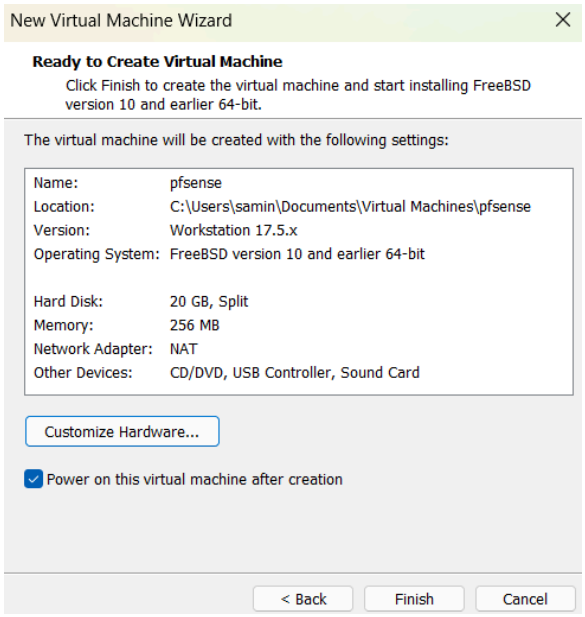
Give your virtual machine a name and a location before clicking next:

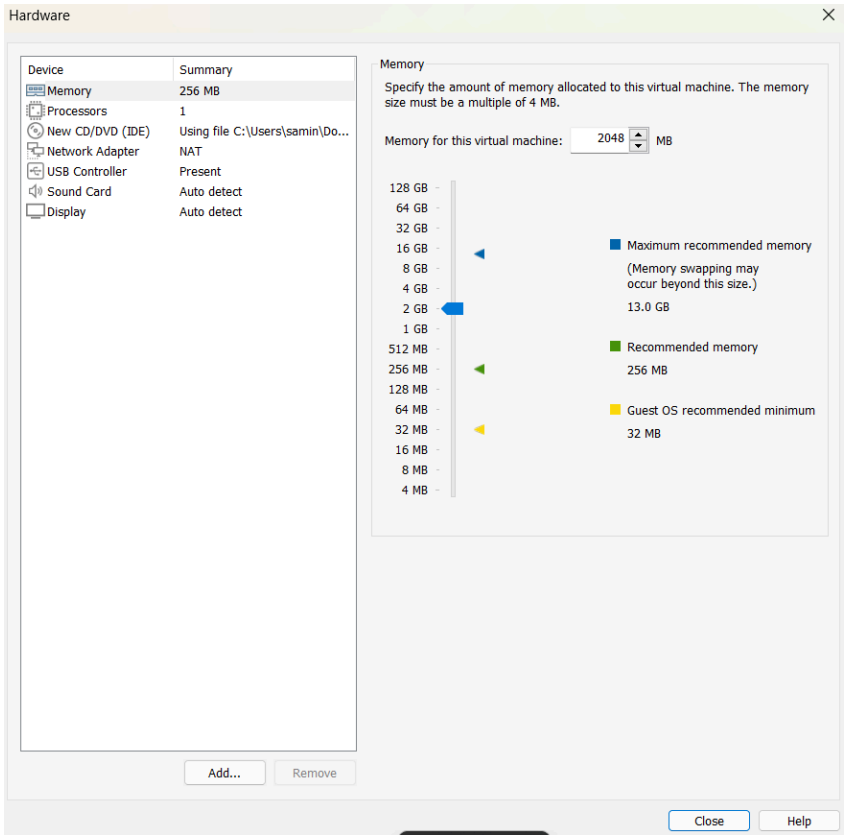


Keep the preselected options and click “Next”:

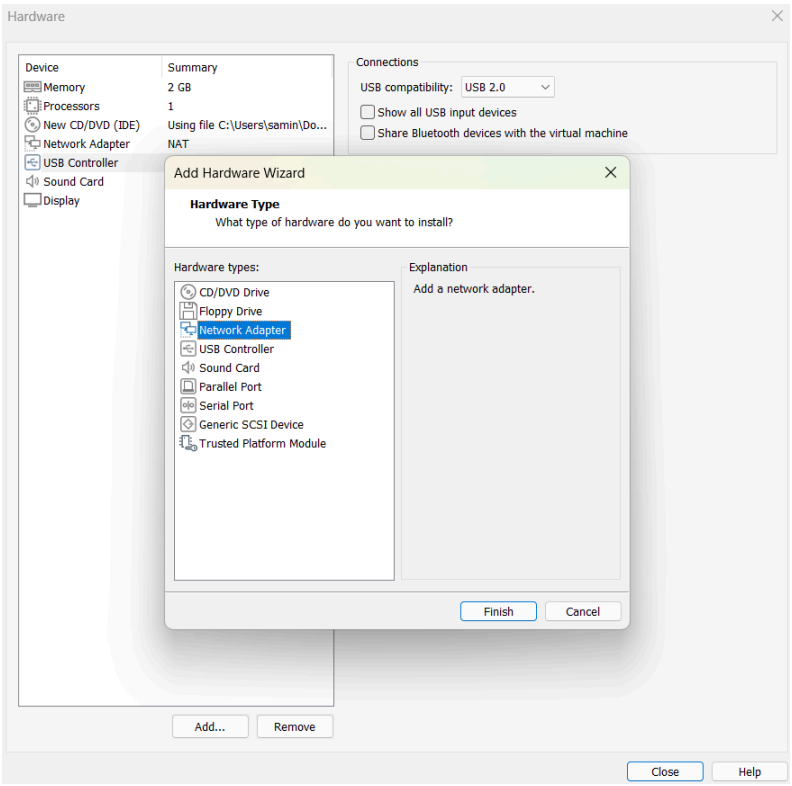


On the next screen, click “Customize Hardware” and give it around 2GB RAM.

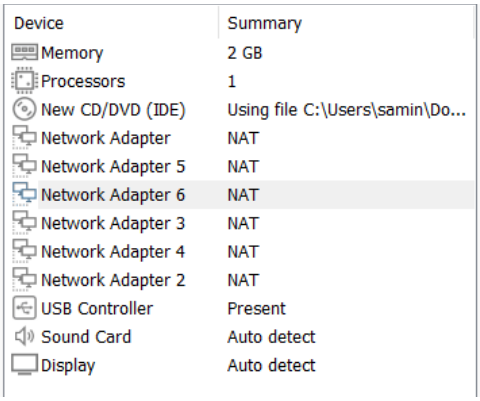




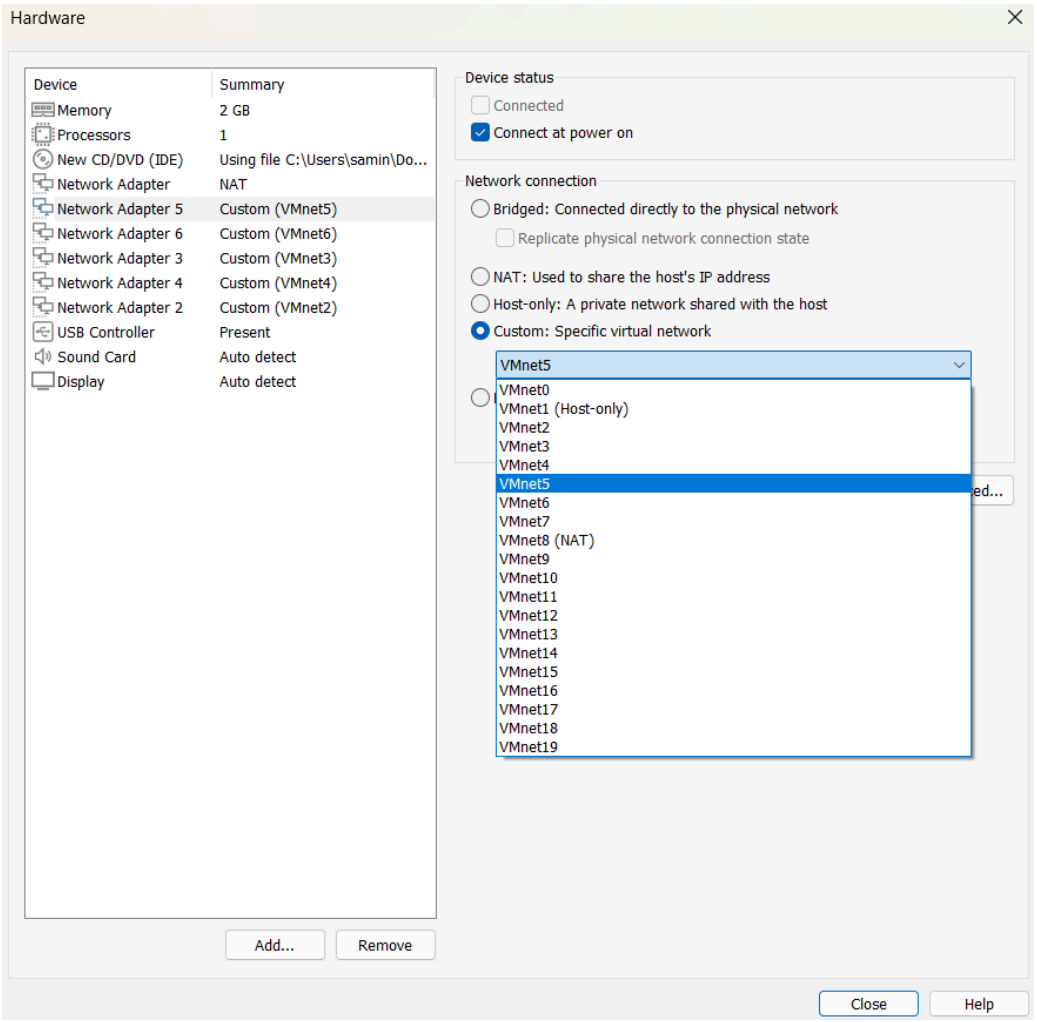
Add a network adapter by clicking “Add”, selecting “Network Adapter” and clicking “Finish”:



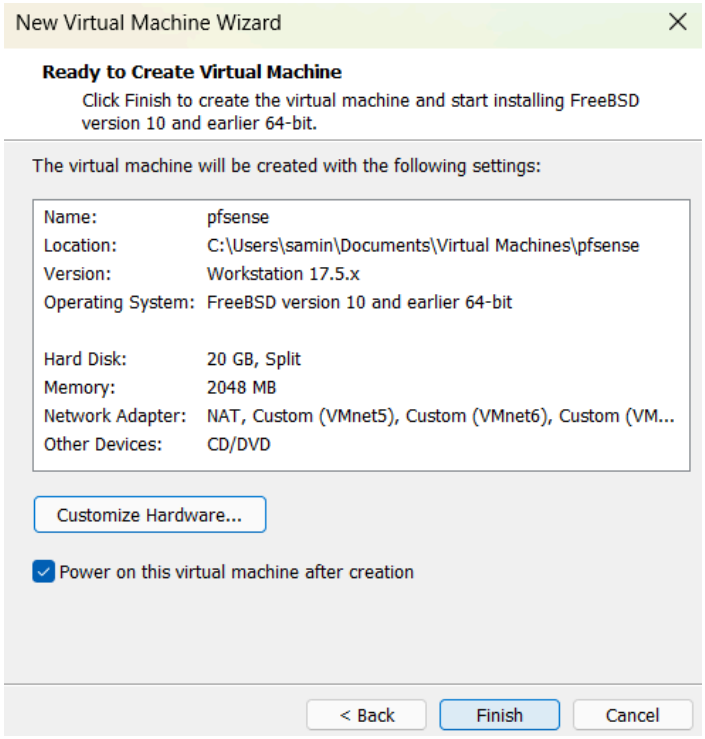
Repeat this 4 more times so that you have 6 network adapters total:



For each of the Network adapters, click on them and choose the custom network connection of “VMnetX” where “X” is the network adapter number (eg. for “Network Adapter 5”, choose “VMnet5”, as shown below). Leave the original Network adapter (the one with no number) as NAT:

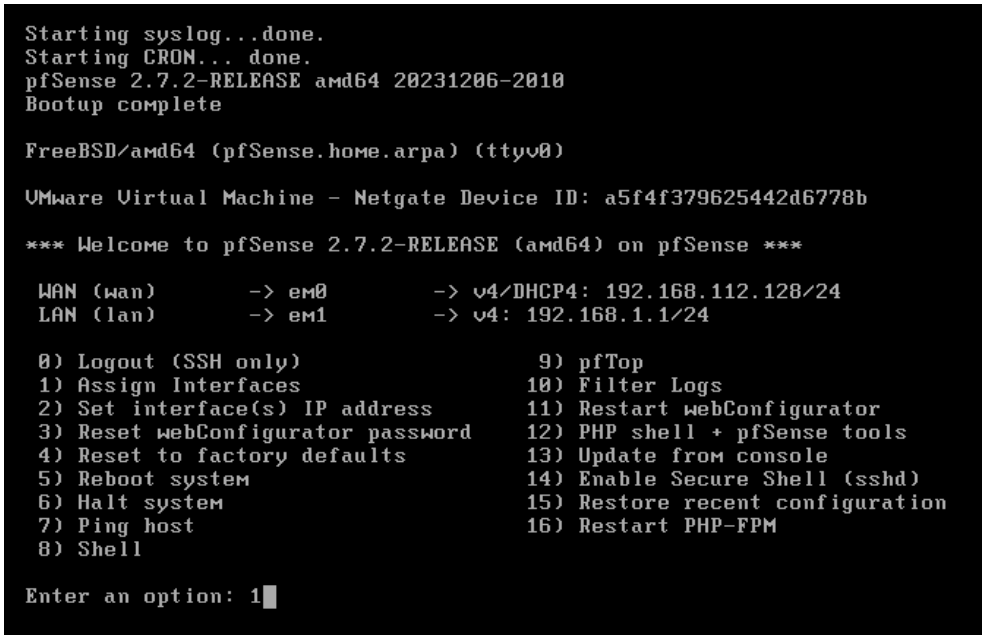


You can remove the “Sound Card” and “USB Controller” if you wish. Otherwise, you can click “Close” and then “Finish”:

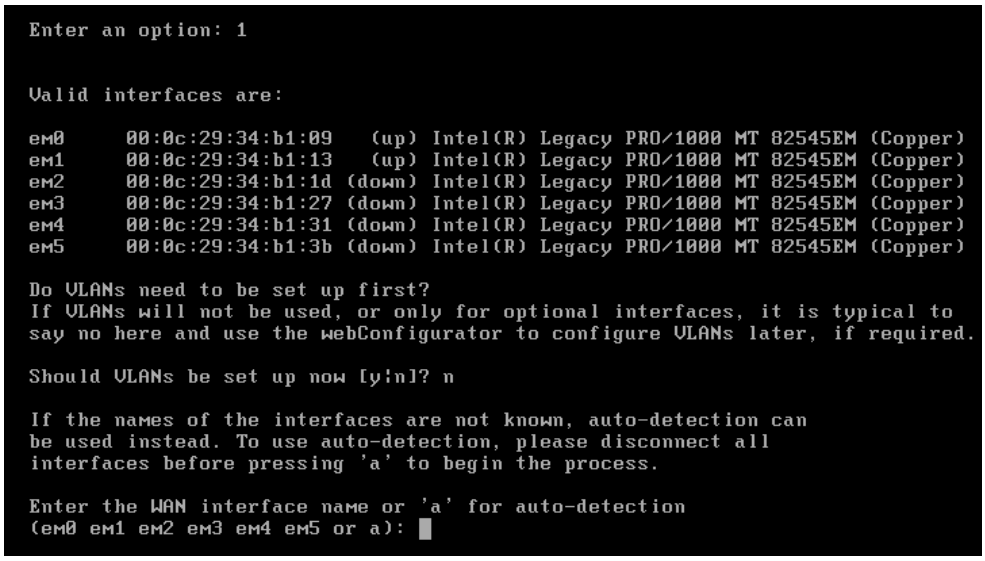


The pfSense machine should launch. Except for the default partition option, where you should select "Auto (UFS) BIOS" from the list, you can press "Enter" through each screen to select the default for the rest of the options. Any warnings about overwriting disk content permanently can be safely disregarded.

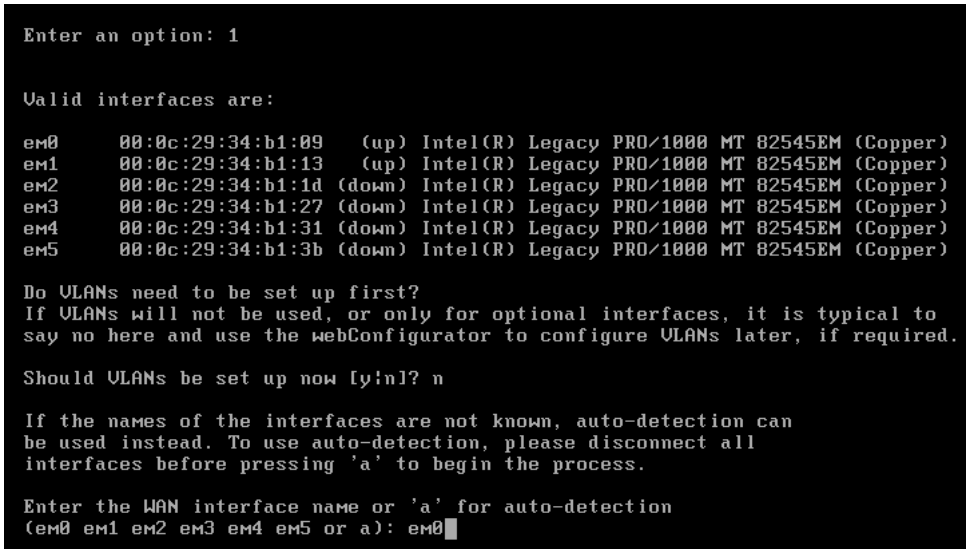
Once you reboot the machine and are prompted with "Enter an option", enter "1":

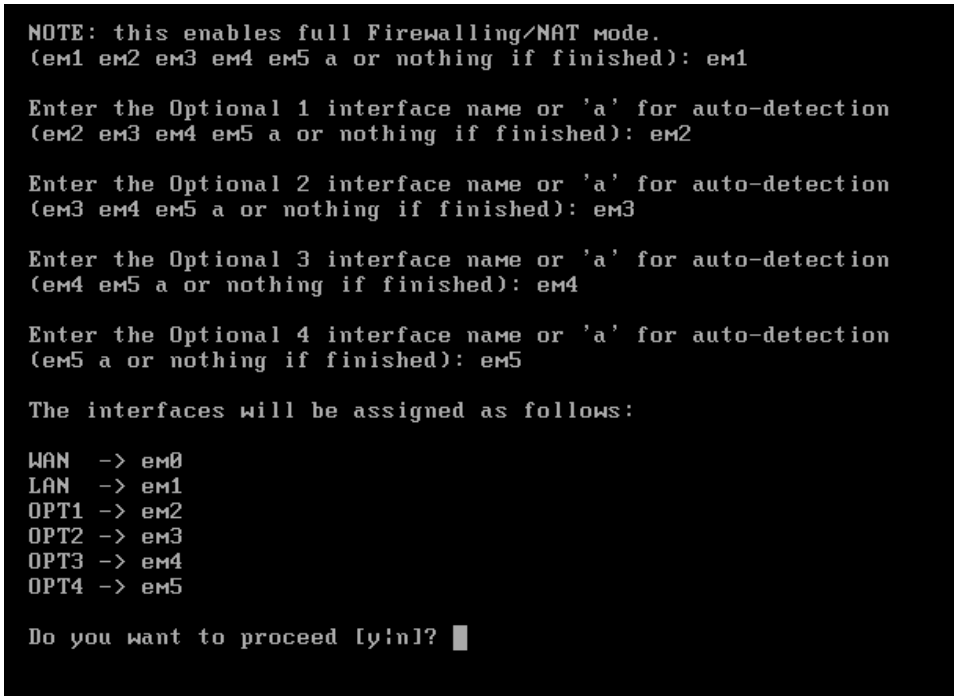


Enter “n” at the next prompt when it asks about setting up VLANs:



Enter each of the “emX” at the subsequent prompts (ie. em0, em1, …, em5):



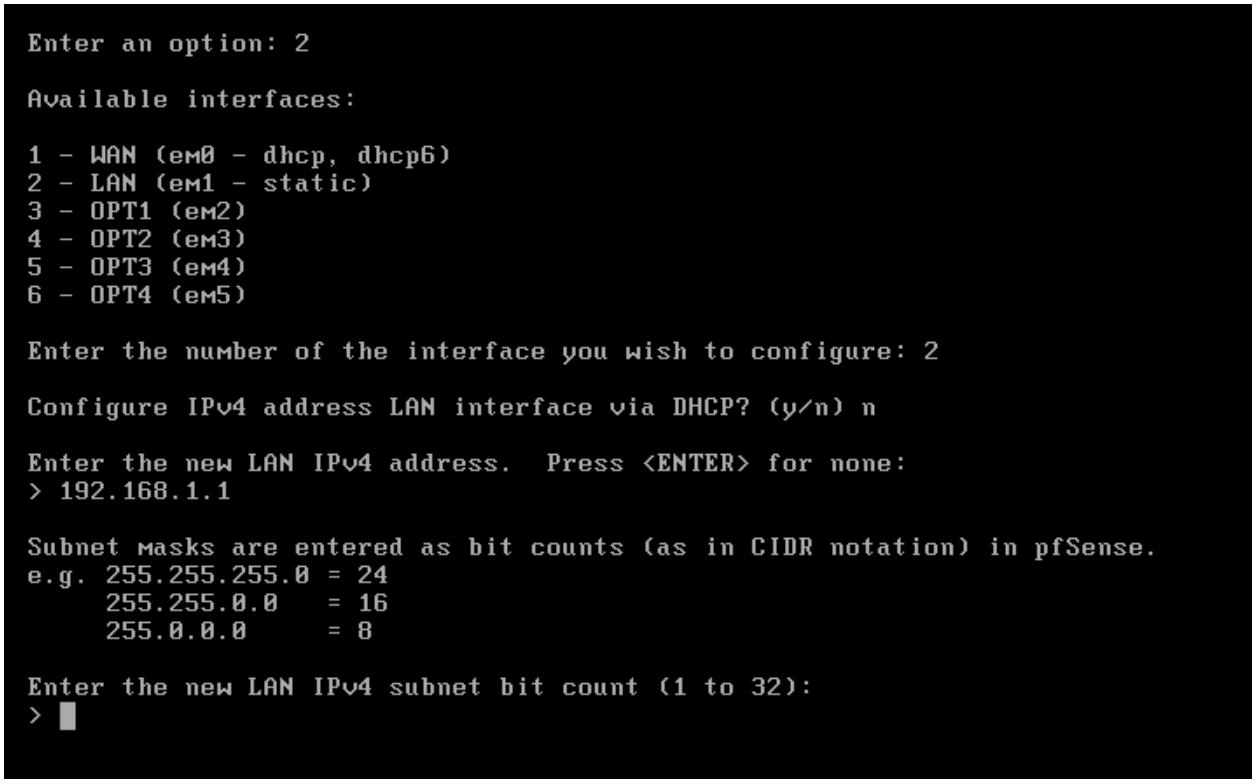


Enter “y” at the prompt asking if you want to proceed.

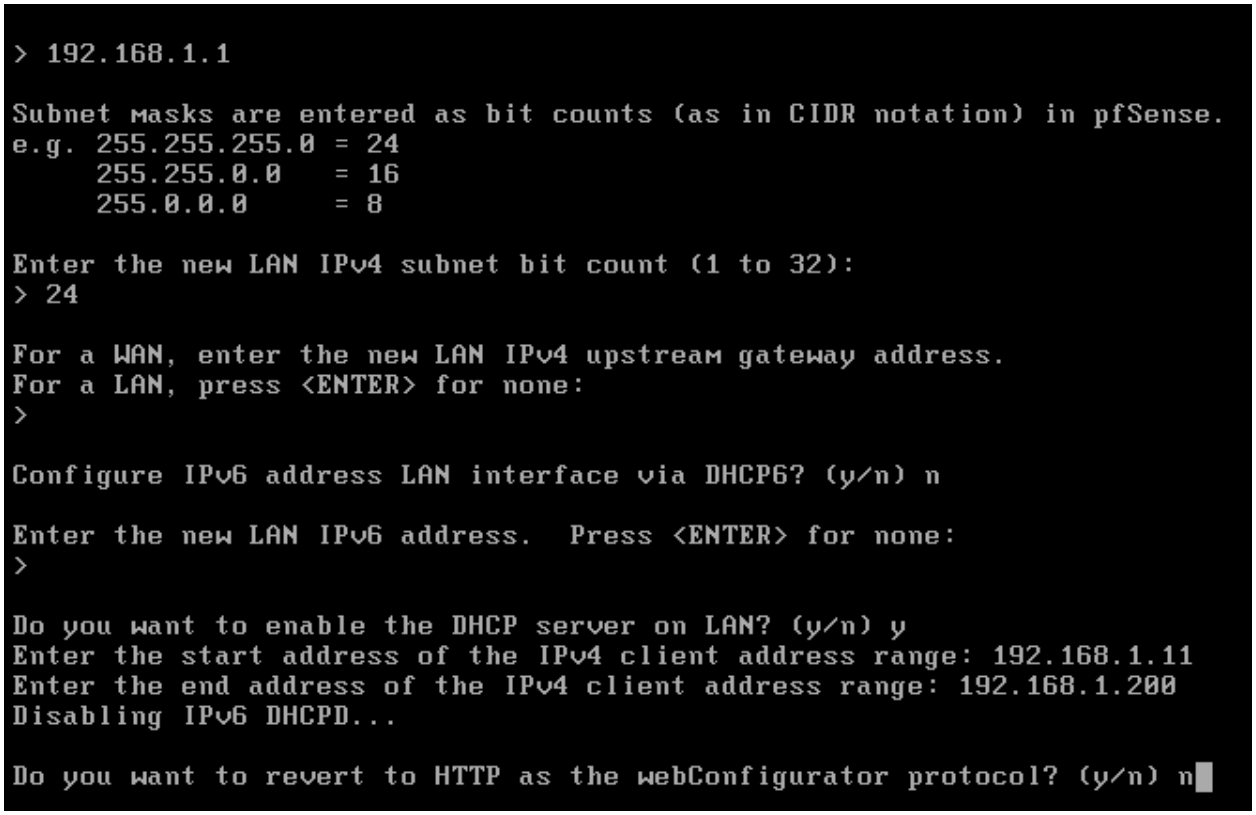
Next, to set the interface IP addresses, enter “2” at the prompt:

To configure the LAN, enter the associated number (in the screenshot below, it's ‘2’) and enter ‘n’ when asked about configuring the IPv4 address via DHCP. Enter the IP address that is going

to be used to access the pfSense WebGUI (in this case, we are using 192.168.1.1):



Configure as follows (the start and end addresses are 192.168.1.11 - 192.168.1.200):



Press “Enter” at the next prompt to continue.

Configure each of the remaining interfaces as follows. OPT1:

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static, dhcp6)
3 - OPT1 (em2)
4 - OPT2 (em3)
5 - OPT3 (em4)
6 - OPT4 (em5)

Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address.  Press <ENTER> for none:
> 192.168.2.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
>
```

```
      255.255.0.0   = 16
      255.0.0.0     = 8

  Enter the new OPT1 IPv4 subnet bit count (1 to 32):
  > 24

  For a WAN, enter the new OPT1 IPv4 upstream gateway address.
  For a LAN, press <ENTER> for none:
  >

  Configure IPv6 address OPT1 interface via DHCP6? (y/n) n

  Enter the new OPT1 IPv6 address.  Press <ENTER> for none:
  >

  Do you want to enable the DHCP server on OPT1? (y/n) n
  Disabling IPv4 DHCPD...
  Disabling IPv6 DHCPD...

  Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

  Please wait while the changes are saved to OPT1...
   Reloading filter...
   Reloading routing configuration...
   DHCPD...
```

OPT2:

```
Enter the number of the interface you wish to configure: 4

Configure IPv4 address OPT2 interface via DHCP? (y/n) n

Enter the new OPT2 IPv4 address.  Press <ENTER> for none:
> 192.168.3.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT2 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT2 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT2 interface via DHCP6? (y/n) n

Enter the new OPT2 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT2? (y/n)
```

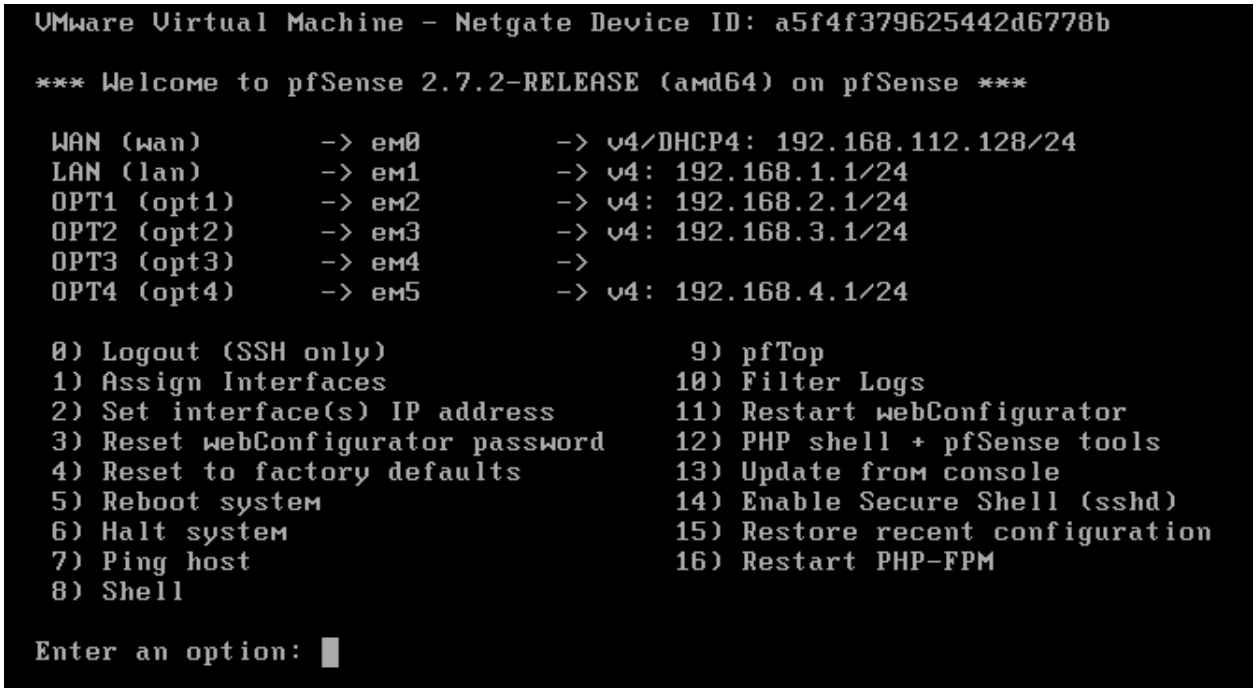
```
Configure IPv6 address OPT2 interface via DHCP6? (y/n) n

Enter the new OPT2 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT2? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to OPT2...[fib_algo] inet.0 (bsearch4#90
) rebuild_fd_flm: switching algo to radix4_lockless

 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 OPT2 address has been set to 192.168.3.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.3.1/

Press <ENTER> to continue.
```

OPT4: (note that we are not touching OPT3 for now)

```
Enter the number of the interface you wish to configure: 6

Configure IPv4 address OPT4 interface via DHCP? (y/n) n

Enter the new OPT4 IPv4 address.  Press <ENTER> for none:
> 192.168.4.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT4 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT4 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT4 interface via DHCP6? (y/n) n

Enter the new OPT4 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT4? (y/n) n
```

```
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT4 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT4 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT4 interface via DHCP6? (y/n) n

Enter the new OPT4 IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT4? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to OPT4...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...
```

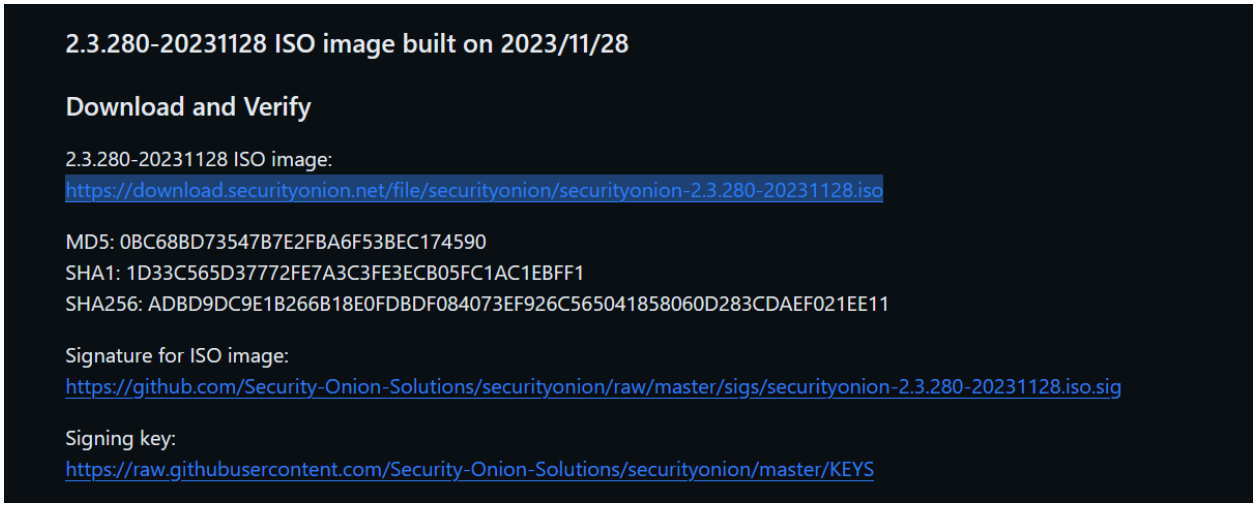
This is what it should look like at the end:



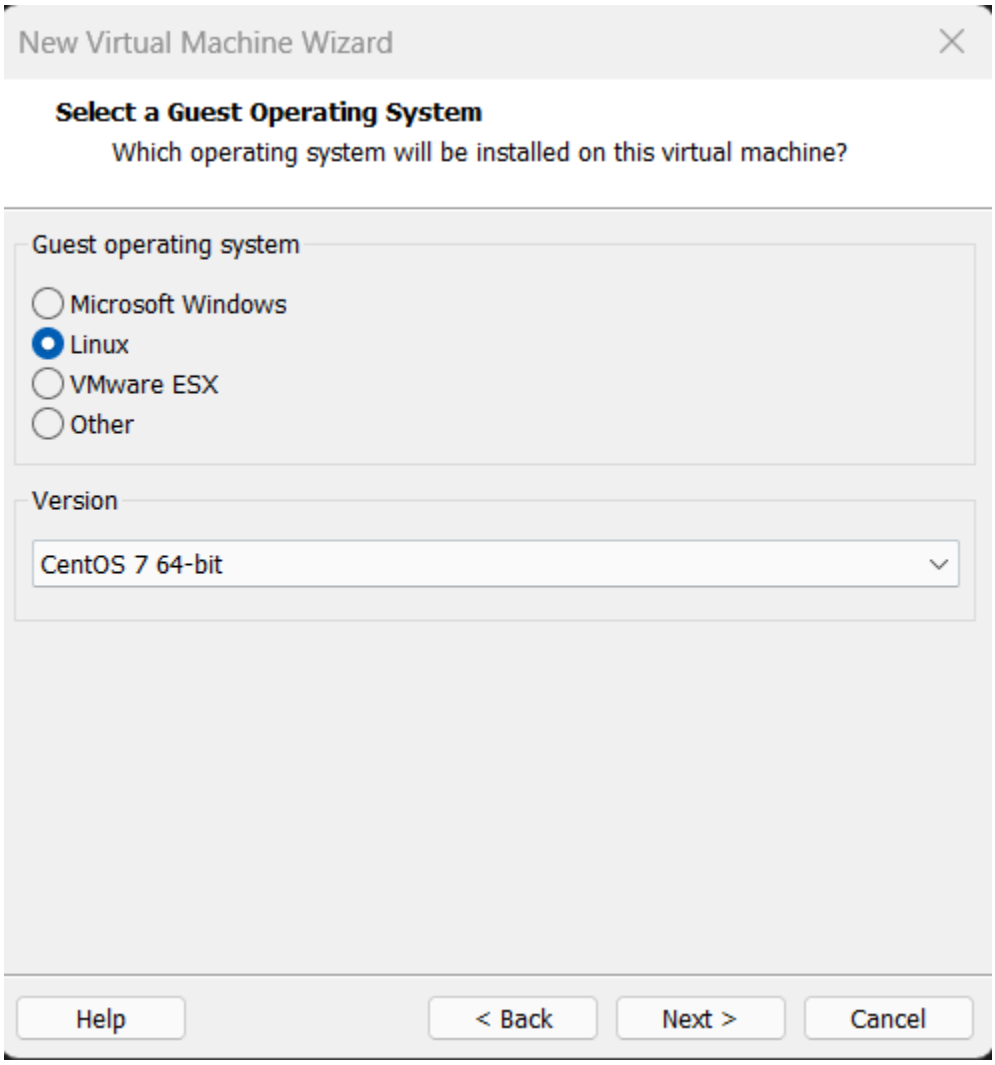
Configuring Security Onion

Security Onion will be acting as the IDS and Log Management solution.

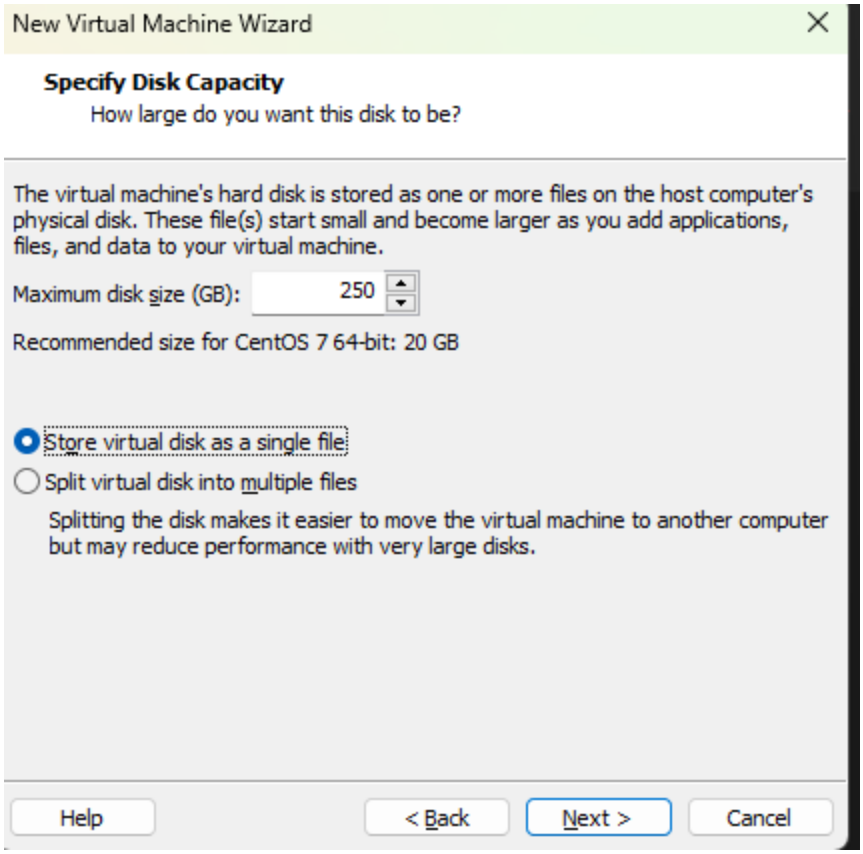
Download the security onion iso from the Github repo (https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md)



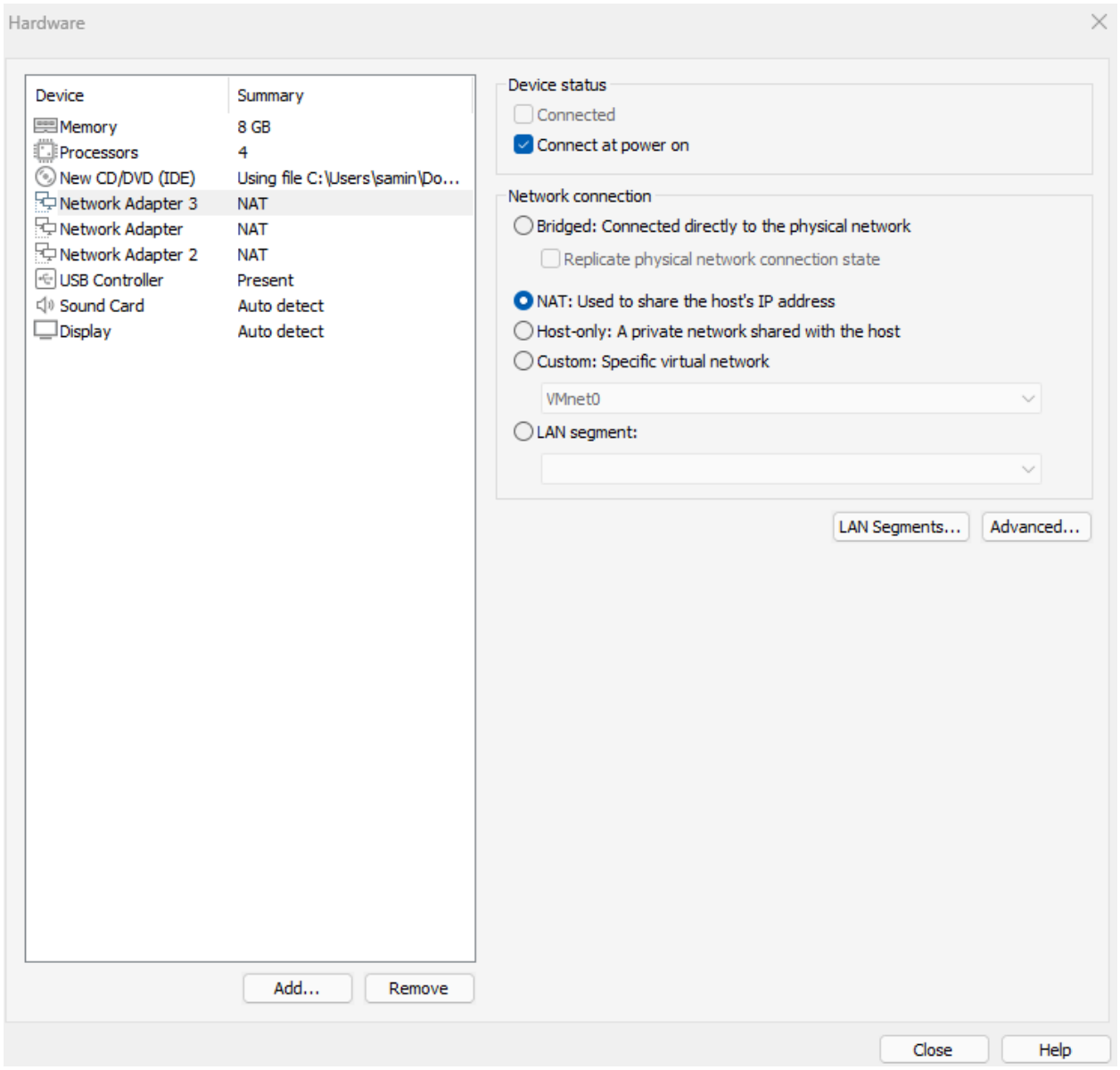
Set up a new virtual machine in VMWare as done above (with pfSense) with “Typical” selected on the first screen, and then select the disc image from where you downloaded it. When it asks to select a guest operating system, use the configuration below:



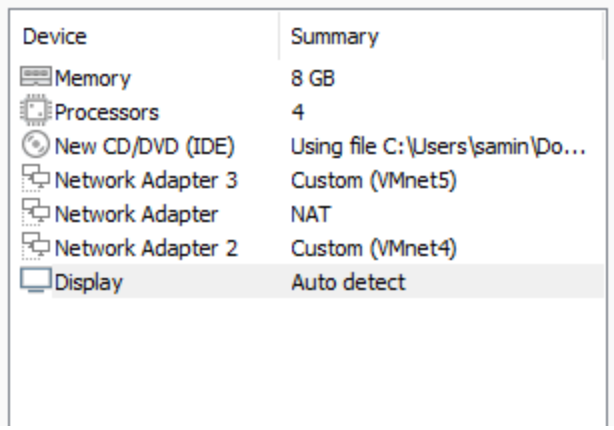
After clicking “Next”, use the following configuration for the next screen (give the machine at least 200 GB, the more the better):



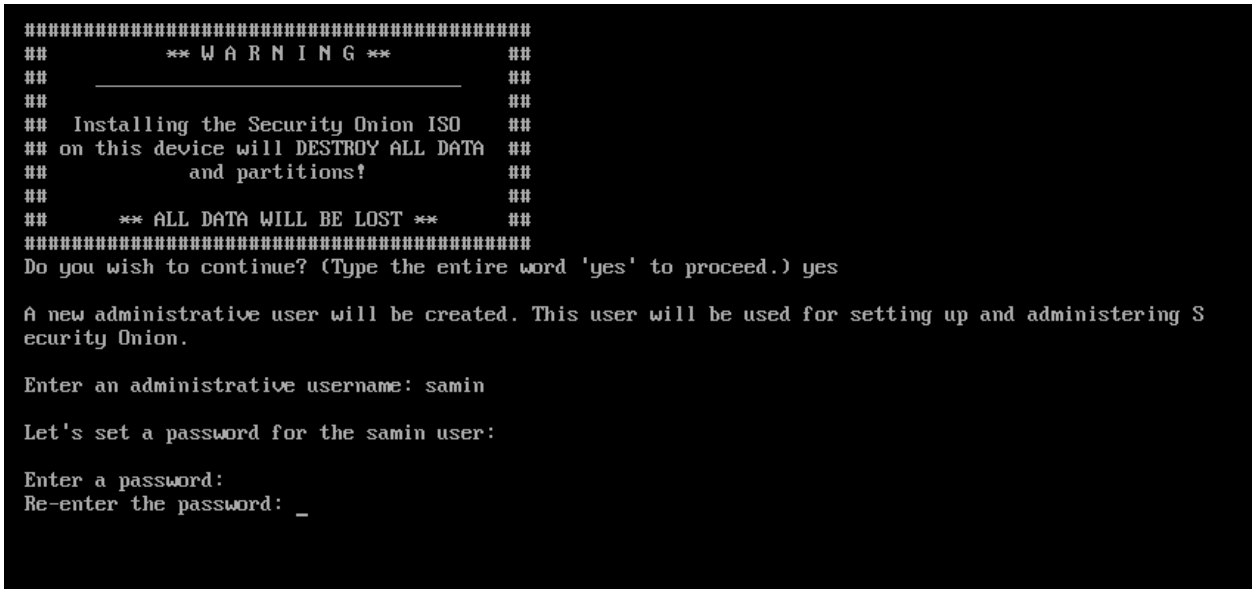
On the next screen, click “Customize Hardware” and give it more RAM - they recommend 12 GB, but I’ll be giving it 8. Also, give it at least 4 processors and create 2 new network adapters:



Configure Network adapter 2 to VMnet 4, and Network adapter 3 to VMnet 5. You can delete extra pieces like the Sound Card or USB Controller. The final screen looks like this:

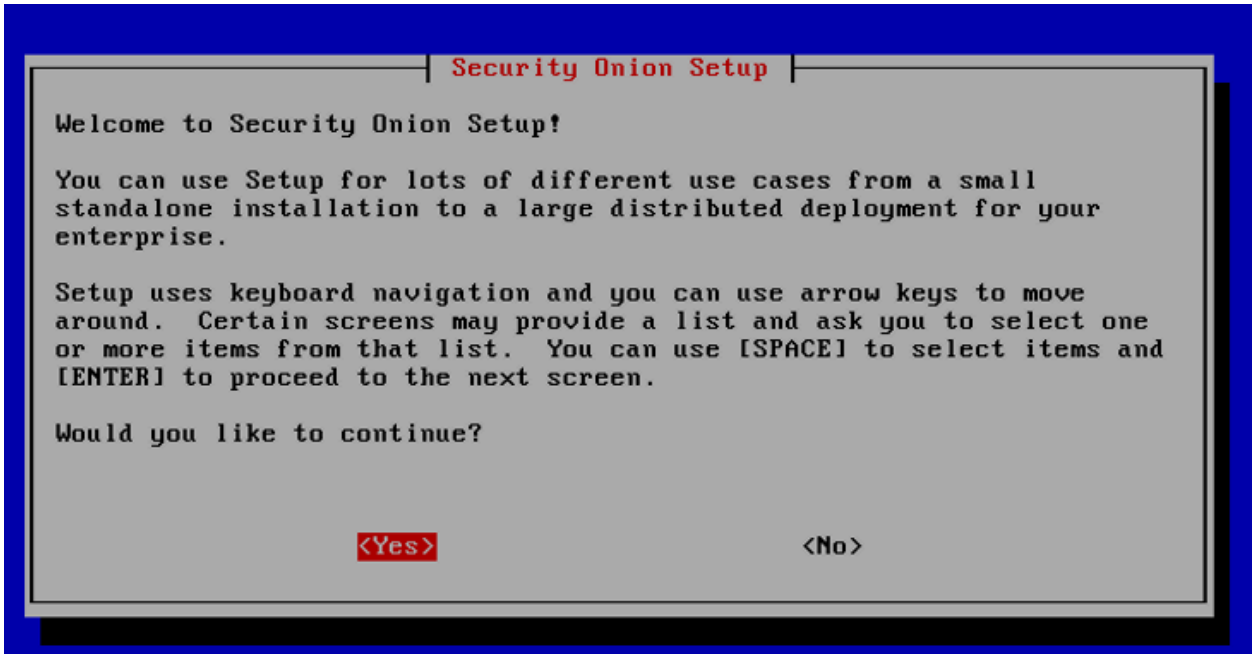


You can click “Close” and then “Finish” before powering on the VM.
Once turned on, let the VM load through everything and then enter “yes” when prompted.
Enter a username and password as prompted as well.

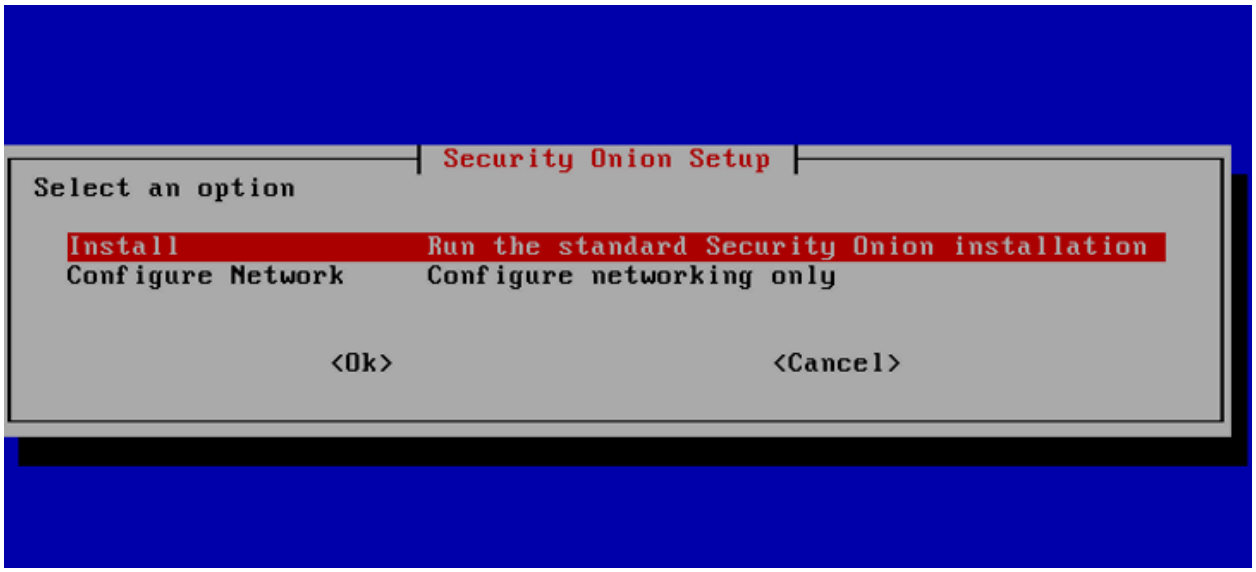


After entering and waiting, press enter when prompted. Enter your login information once you get to the prompt asking you for it.

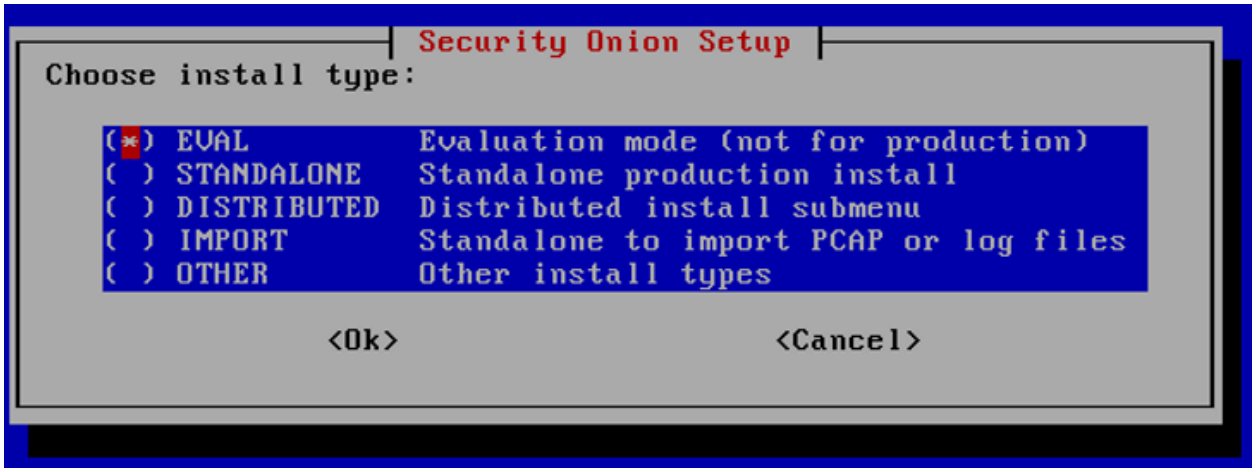
Select “Yes” by pressing enter on the next screen:



Press enter on the “Install” option on the next screen:

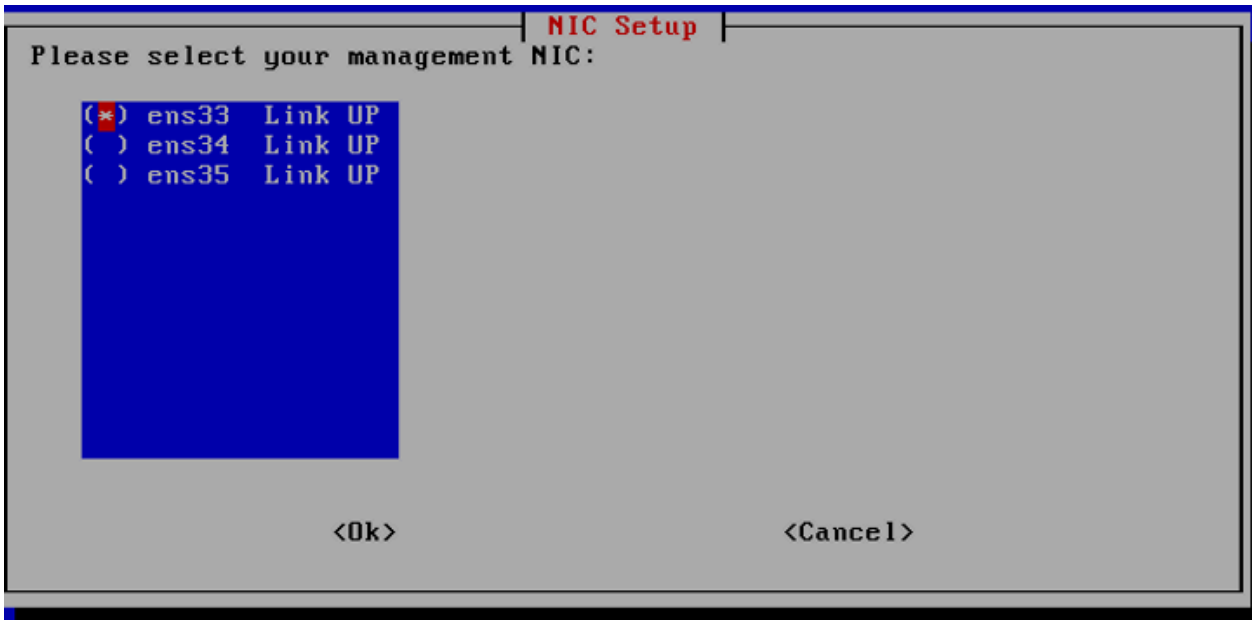


Ensure the “EVAL” option is selected before pressing enter on the screen after:

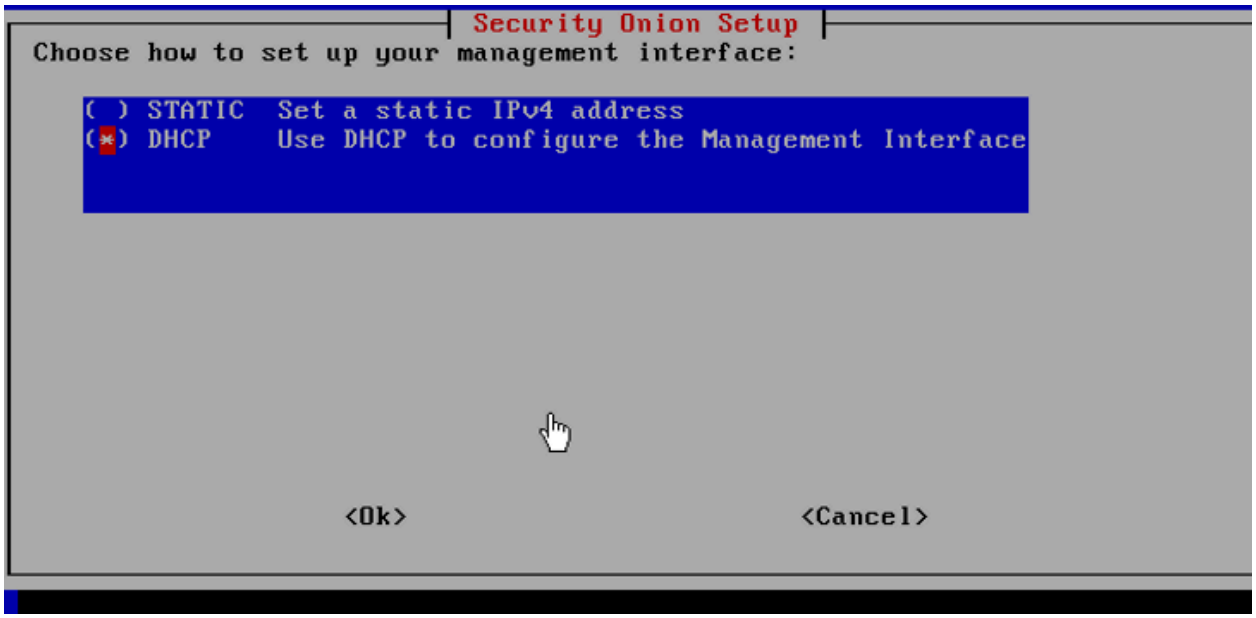


Type out “AGREE” when prompted. Select “Standard” on the next screen:

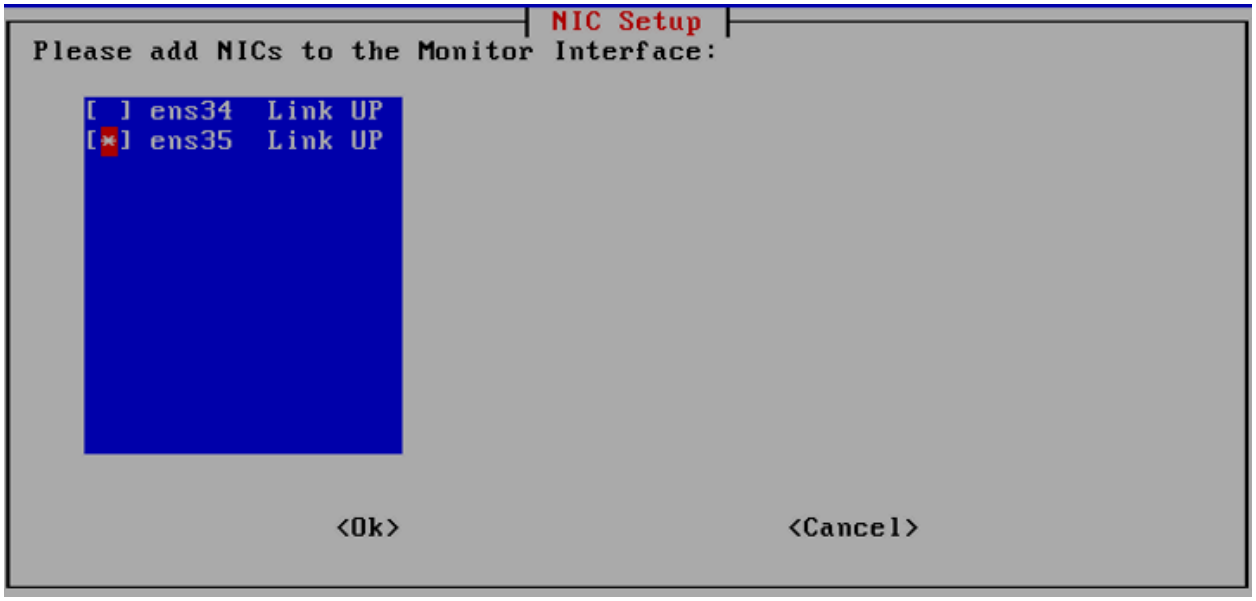
Create a hostname when asked. Select “ens33” on the next screen:



Select “DHCP” on the next screen:

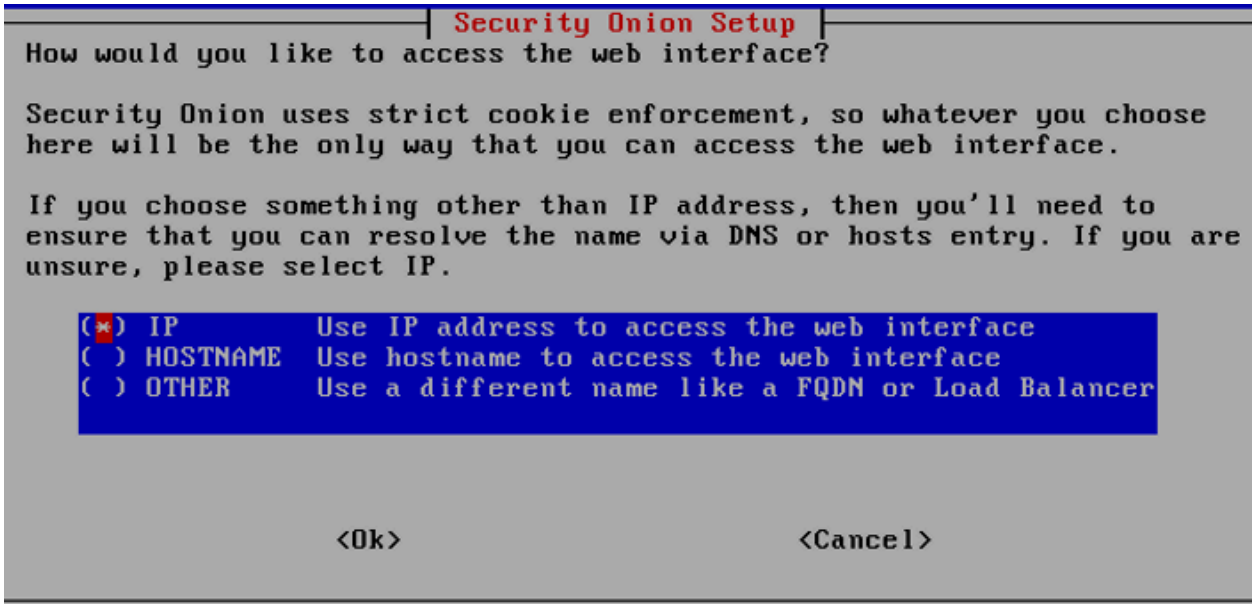


Select “YES”, “OK”, and then “Direct” for the next 3 prompts. Then select “ens35” at the next prompt:



Select “Automatic” at the next screen. Select the default options for the next couple of screens before reaching the prompt asking for an email. Enter an email and password of your choosing.

Select “IP” at the next screen:



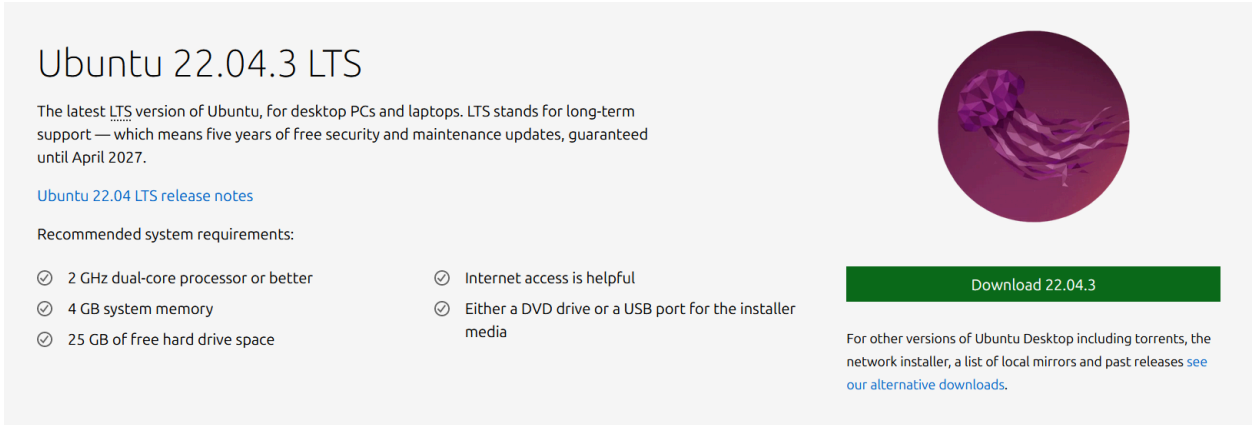
Select “Yes” for the NTP server on the next screen and then select all the default options.

When you get to the final screen, save the information displayed; importantly, ensure you know the IP address for web access (next to “Access URL”). Press “Tab” and select “Yes” once you are done. The installation will begin, and it will likely take a long time (it took around 20 minutes for me).

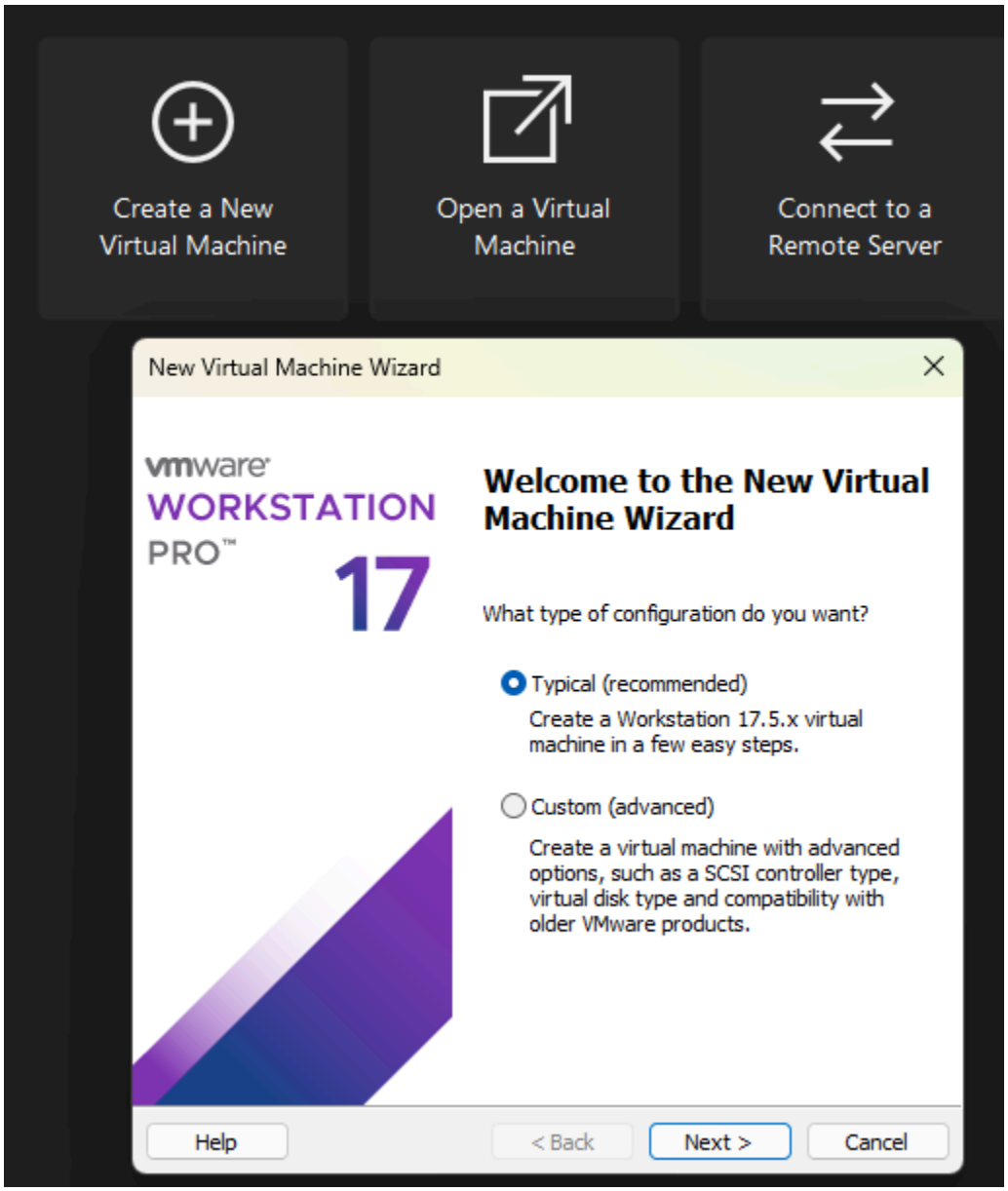
Configure the Security Onion Analyst Machine

Here we will be configuring an Ubuntu machine that will be used to access the Security Onion web interface, simulating how a SOC Analyst would access a SIEM.

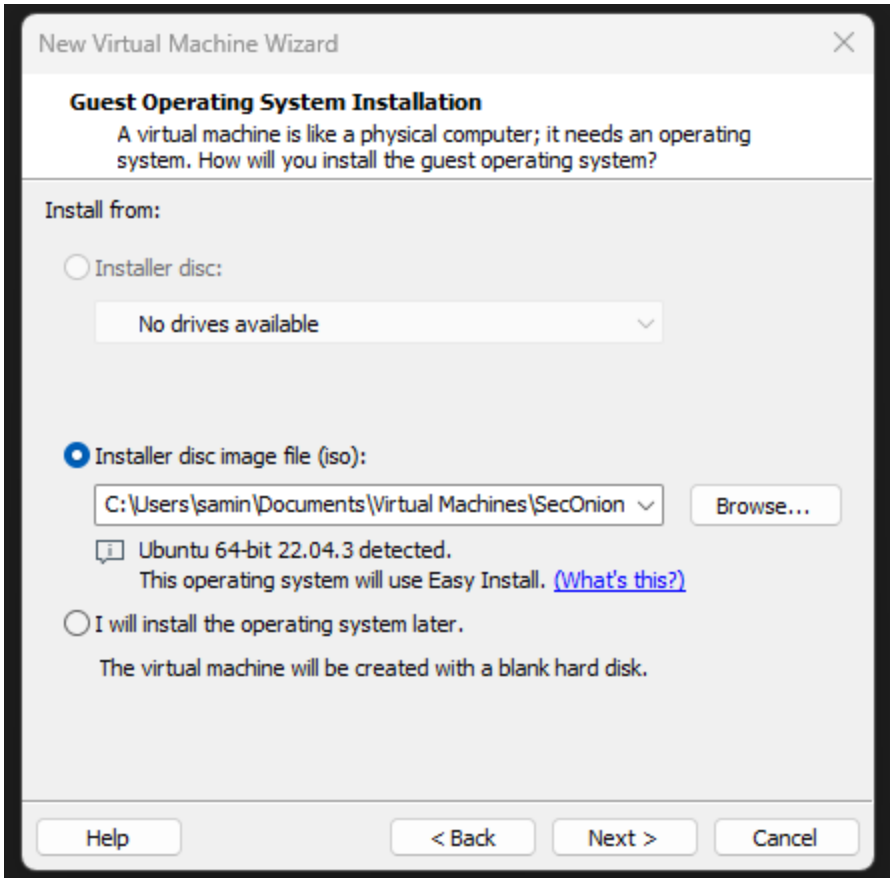
First, we download the Ubuntu Desktop image from their website:



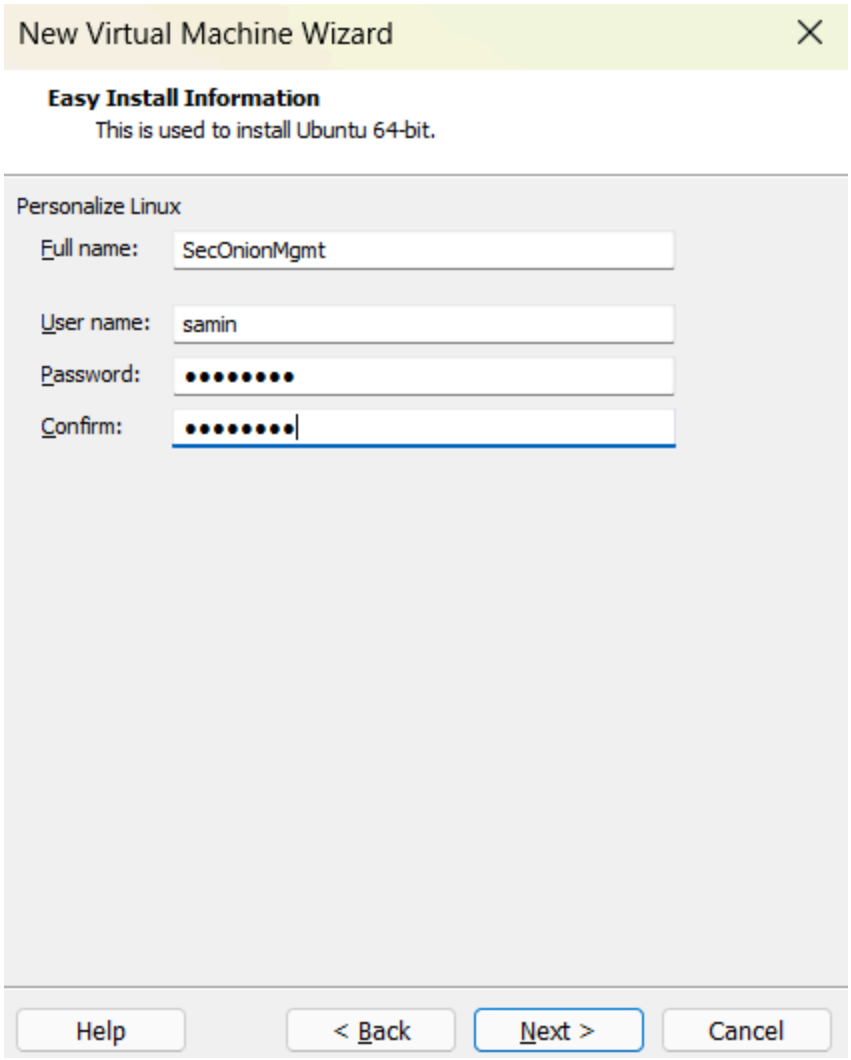
On VMware, create a new virtual machine with typical selected before clicking “Next”:



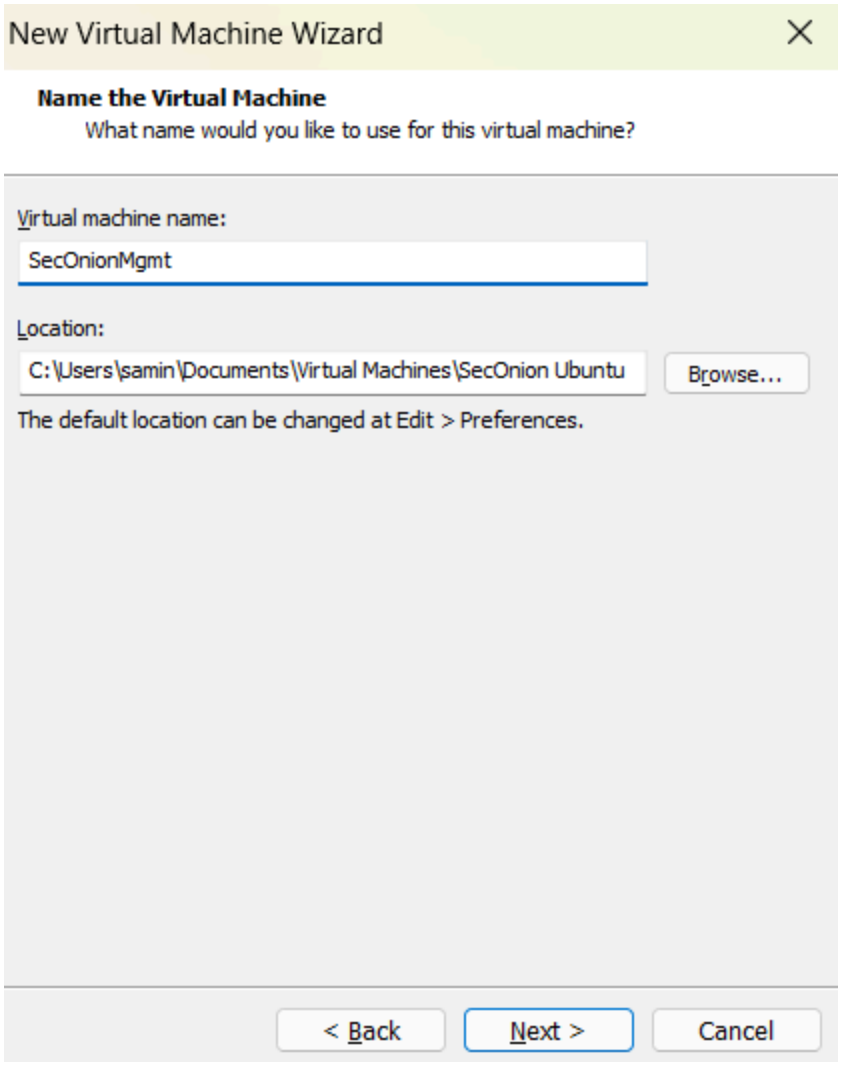
Select the disk image from where you downloaded it before clicking “Next”:



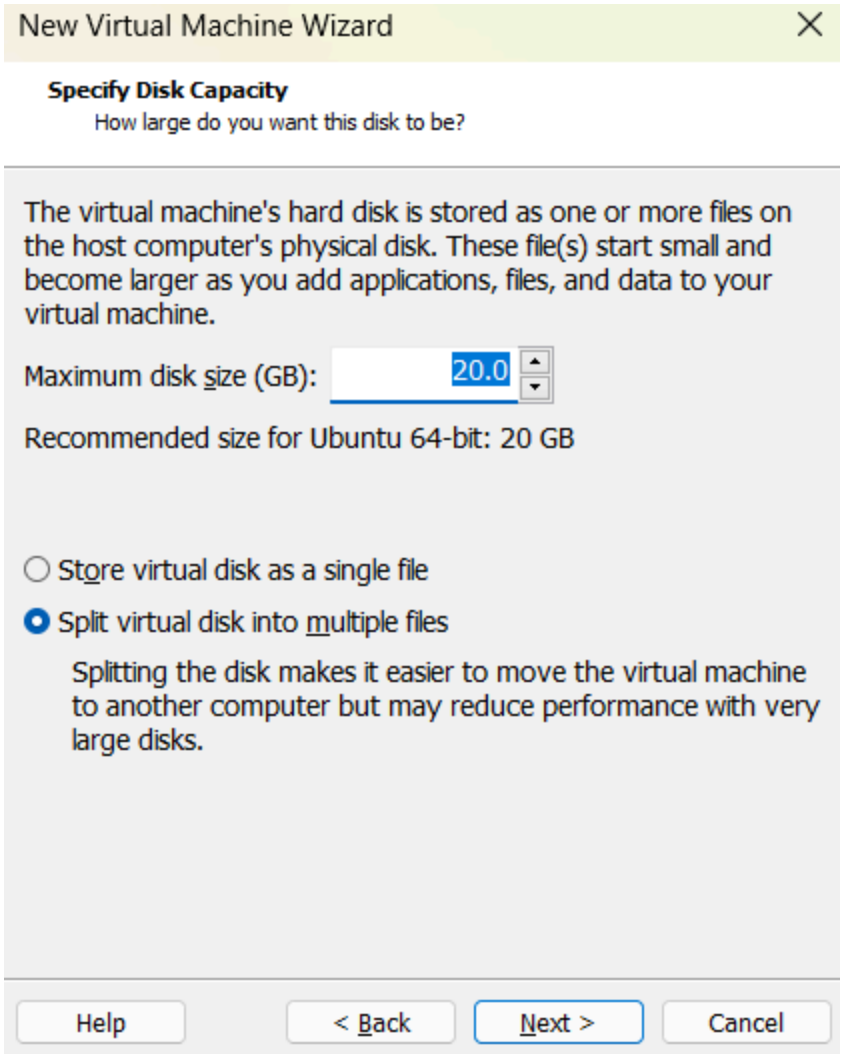
Fill in the fields as you choose, then click “Next”:

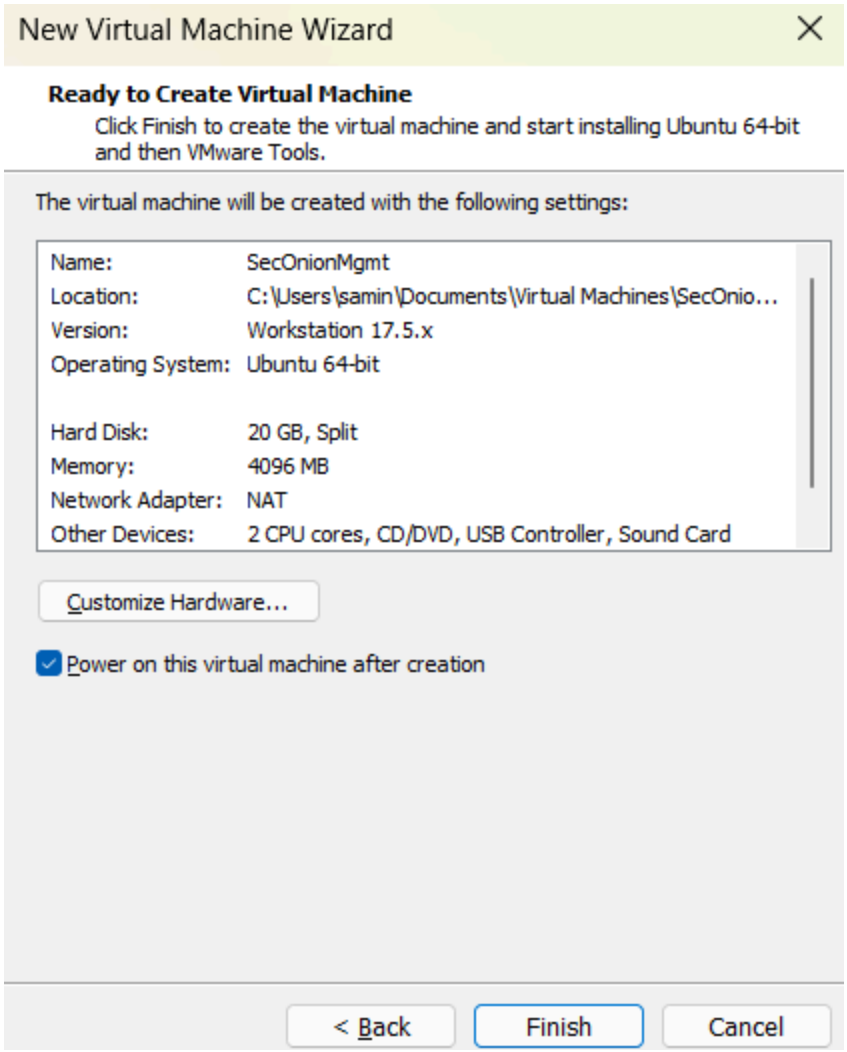


Give the machine a name and choose the location to store it before clicking “Next”:

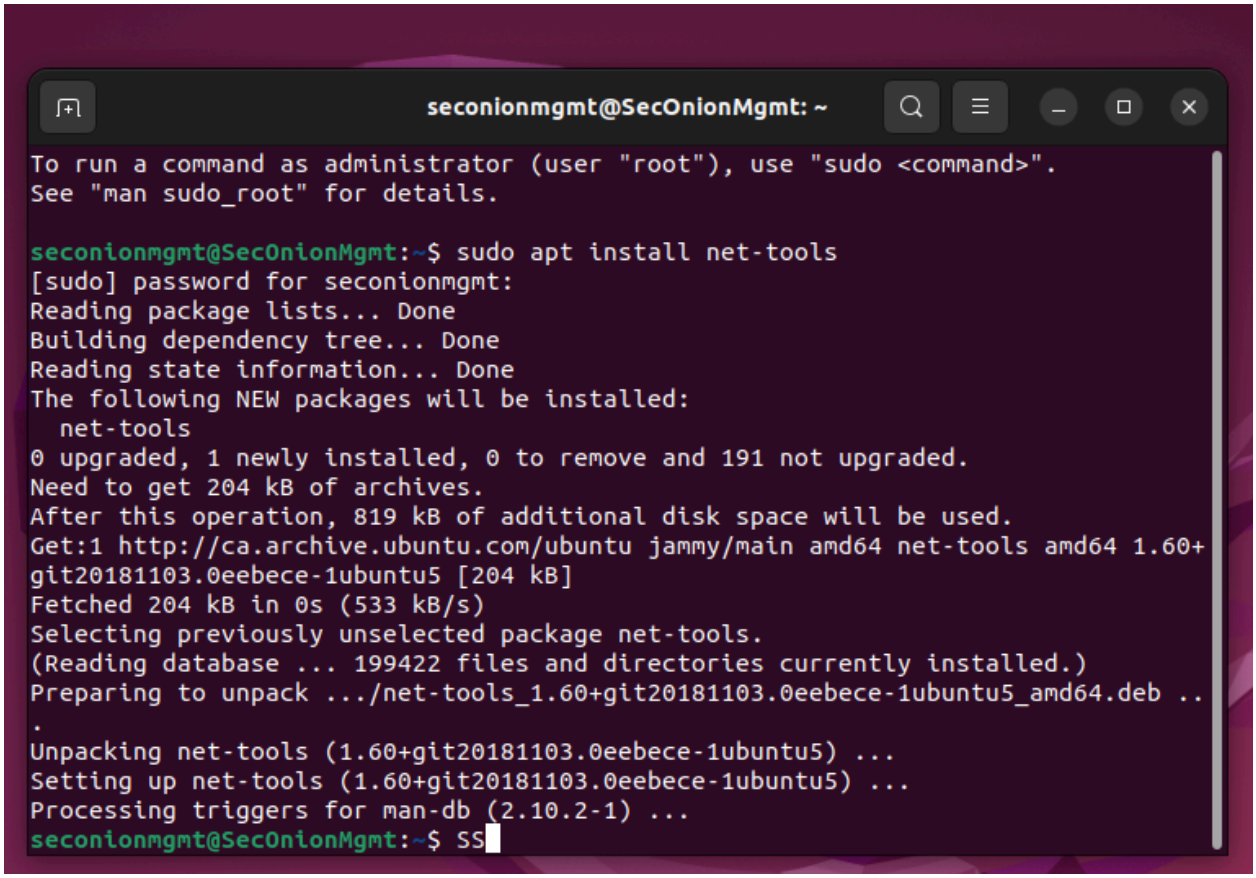


The next two screens you can leave at the defaults:

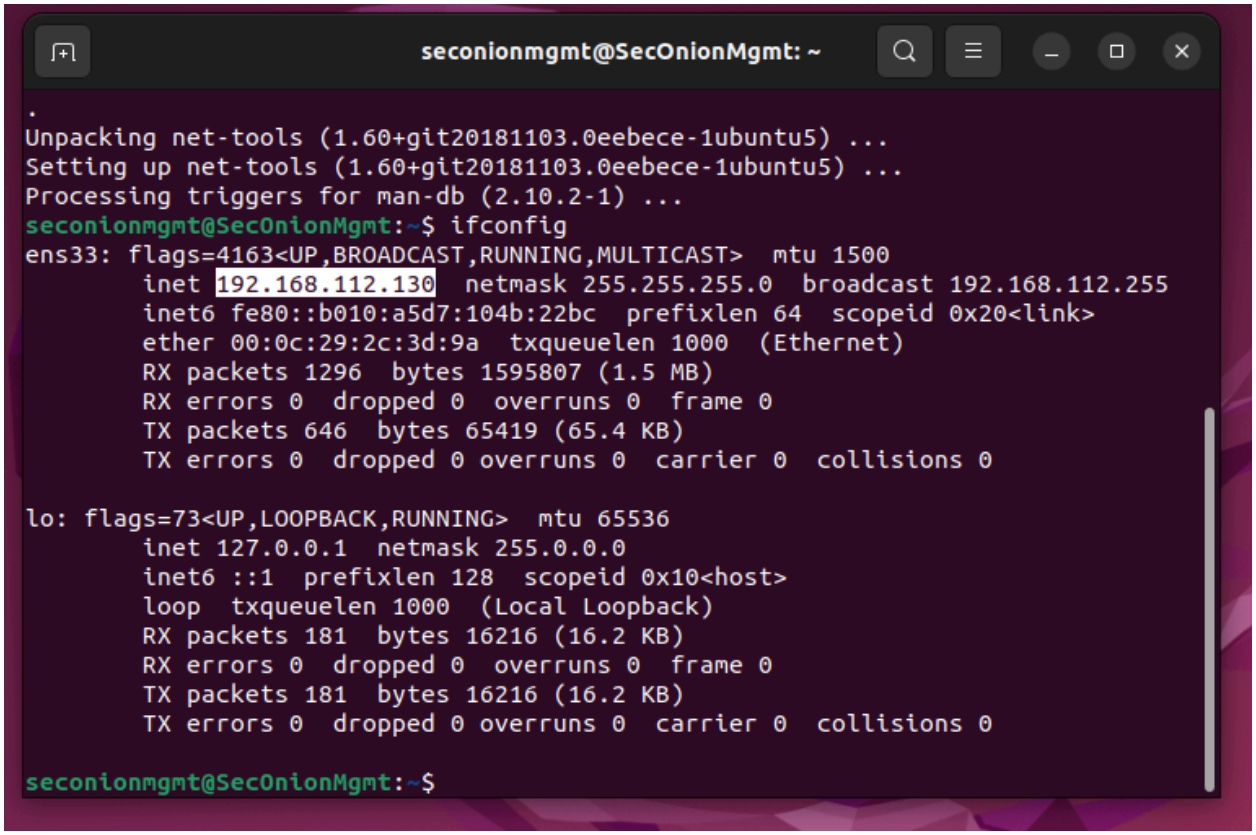

New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.
Maximum disk size (GB):
20.0
Recommended size for Ubuntu 64-bit: 20 GB
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel



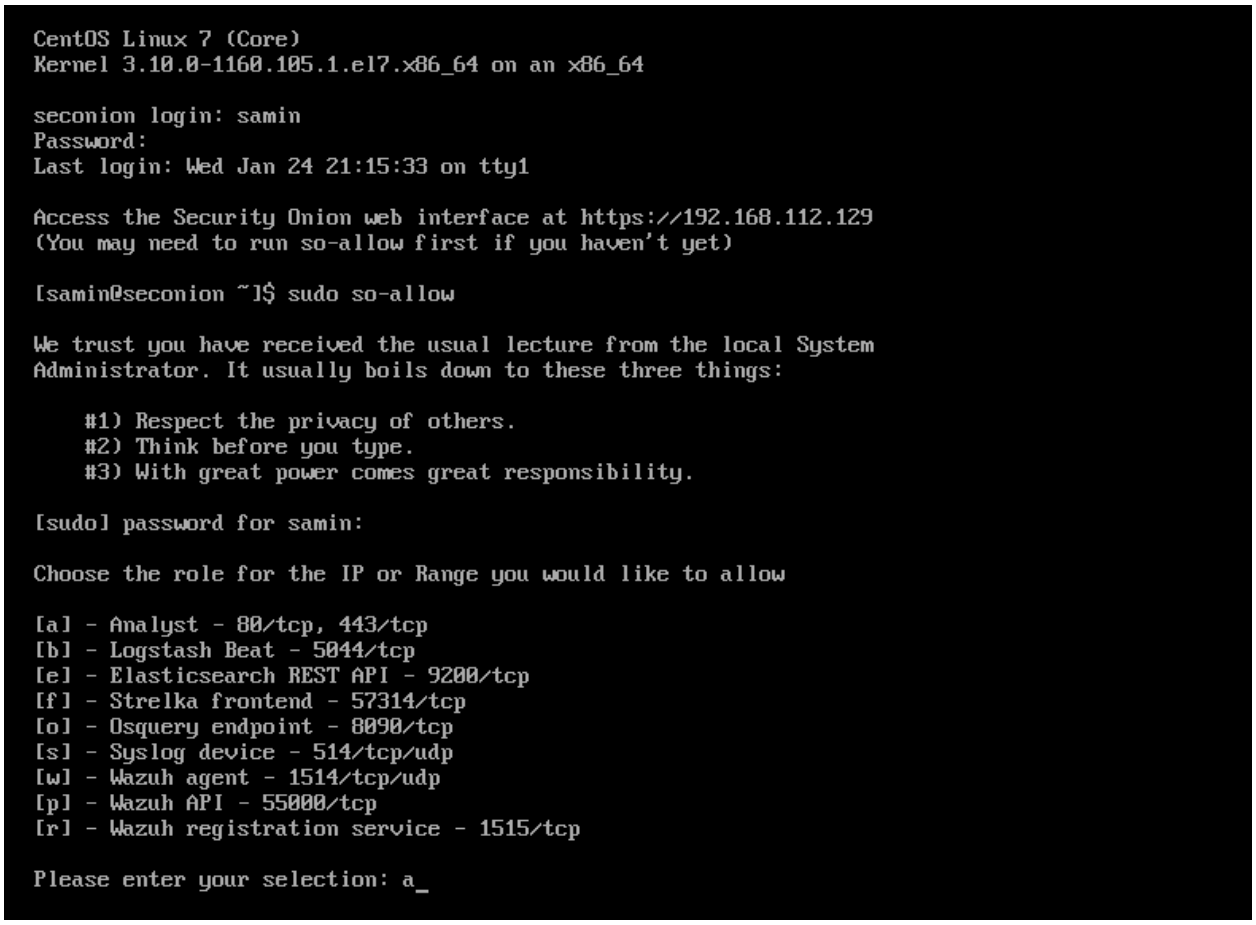
Load up the virtual machine and configure it as you wish; for this lab, all the default options were used (ignore any warnings about overwriting the defaults). Once you are able to log into the machine, open up a terminal and enter “sudo apt install net-tools”:


seconionmgmt@SecOnionMgmt: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
seconionmgmt@SecOnionMgmt:~$ sudo apt install net-tools
[sudo] password for seconionmgmt:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
net-tools
0 upgraded, 1 newly installed, 0 to remove and 191 not upgraded.
Need to get 204 kB of archives.
After this operation, 819 kB of additional disk space will be used.
Get:1 http://ca.archive.ubuntu.com/ubuntu jammy/main amd64 net-tools amd64 1.60+
git20181103.0eebece-1ubuntu5 [204 kB]
Fetched 204 kB in 0s (533 kB/s)
Selecting previously unselected package net-tools.
(Reading database ... 199422 files and directories currently installed.)
Preparing to unpack .../net-tools_1.60+git20181103.0eebece-1ubuntu5_amd64.deb ..
.
Unpacking net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Setting up net-tools (1.60+git20181103.0eebece-1ubuntu5) ...
Processing triggers for man-db (2.10.2-1) ...
seconionmgmt@SecOnionMgmt:~$ SS

Run “ifconfig” next and then note the following IP address:

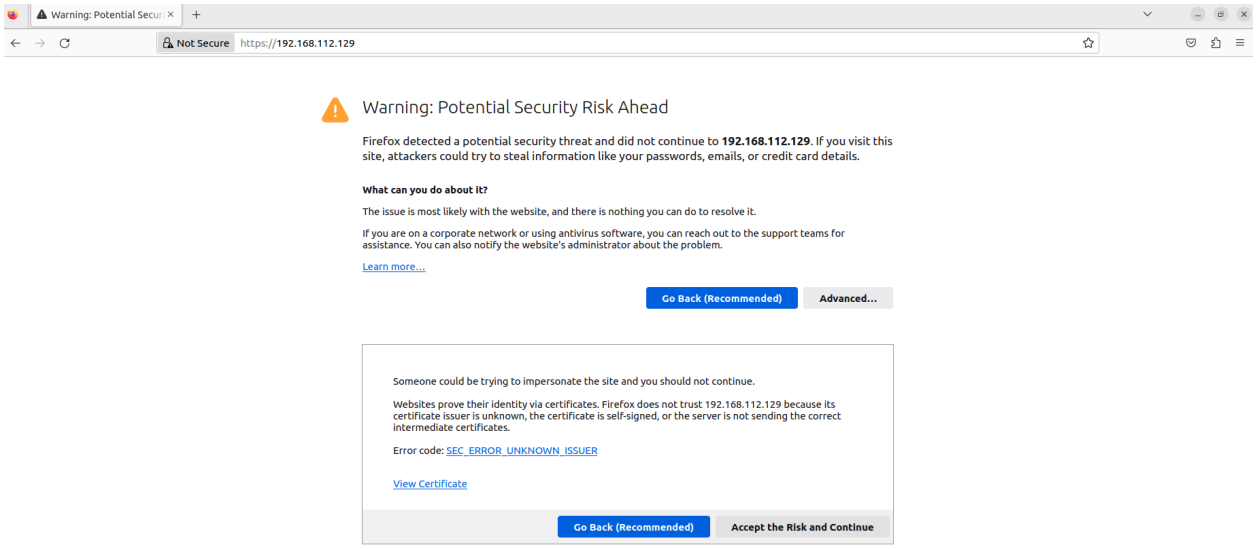


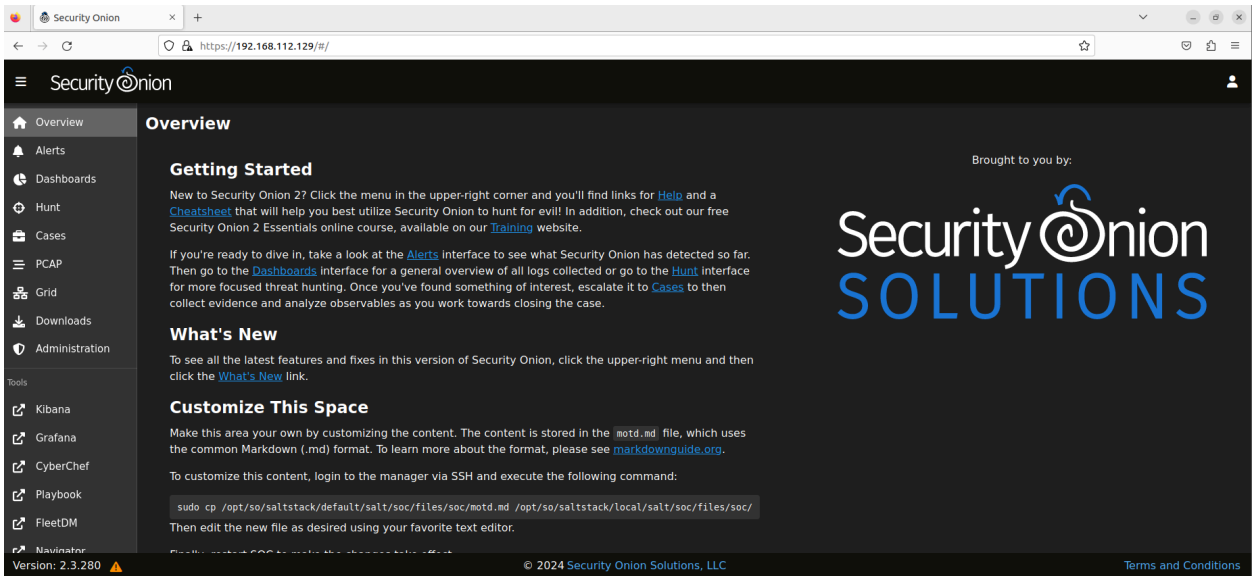
Now, log into the Sec Onion machine and enter “sudo so-allow”, then enter “a”:



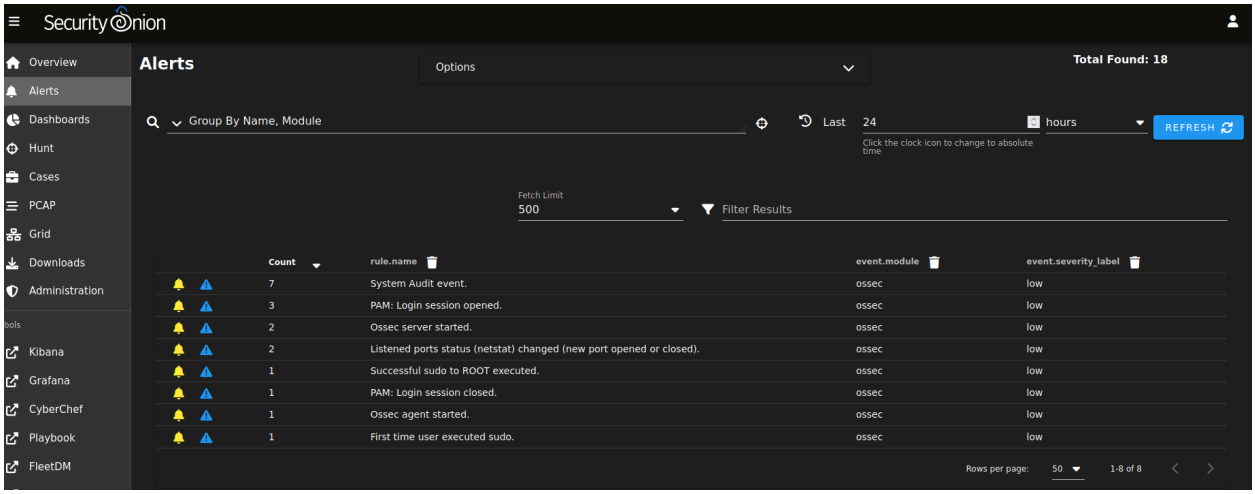
When prompted, enter in the the IP address of the Ubuntu Desktop noted above (this will allow traffic from your Ubuntu machine through to the Security Onion web instance).

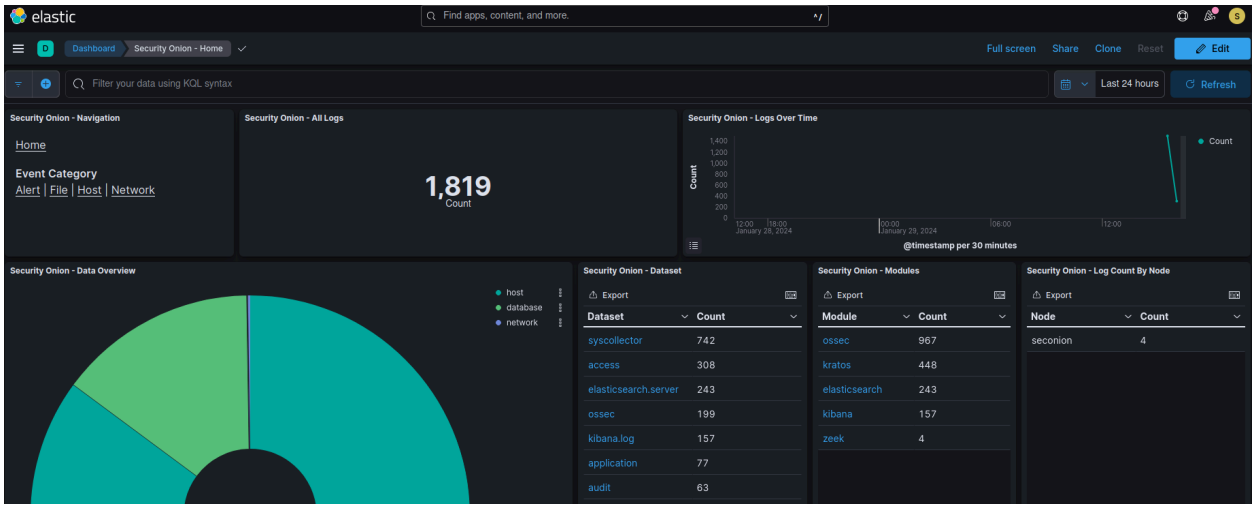
Now navigate to the access URL of the Security Onion machine noted previously from the Ubuntu Desktop. You will be warned about a potential security risk, but you can ignore that and continue to the login page where you will be prompted to login with the email and password you defined earlier on:





From here, you navigate between the tabs on the left side to see the “Alerts”, “Dashboards”, and “Hunt” pages, among others; tools like Kibana and Grafana can also be opened from this sidebar (you may be prompted to log in with your email again when opening up tools like Kibana):


Security Onion
Overview
Alerts
Dashboards
Hunt
Cases
PCAP
Grid
Downloads
Administration
Kibana
Grafana
CyberChef
Playbook
FleetDM
Alerts
Options
Total Found: 18
Group By Name, Module
Last 24 hours
REFRESH
Click the clock icon to change to absolute time
Fetch Limit
500
Filter Results
Count
rule.name
event.module
event.severity_label
7 System Audit event. ossec low
3 PAM: Login session opened. ossec low
2 Ossec server started. ossec low
2 Listened ports status (netstat) changed (new port opened or closed). ossec low
1 Successful sudo to ROOT executed. ossec low
1 PAM: Login session closed. ossec low
1 Ossec agent started. ossec low
1 First time user executed sudo. ossec low
Rows per page: 50
1-8 of 8

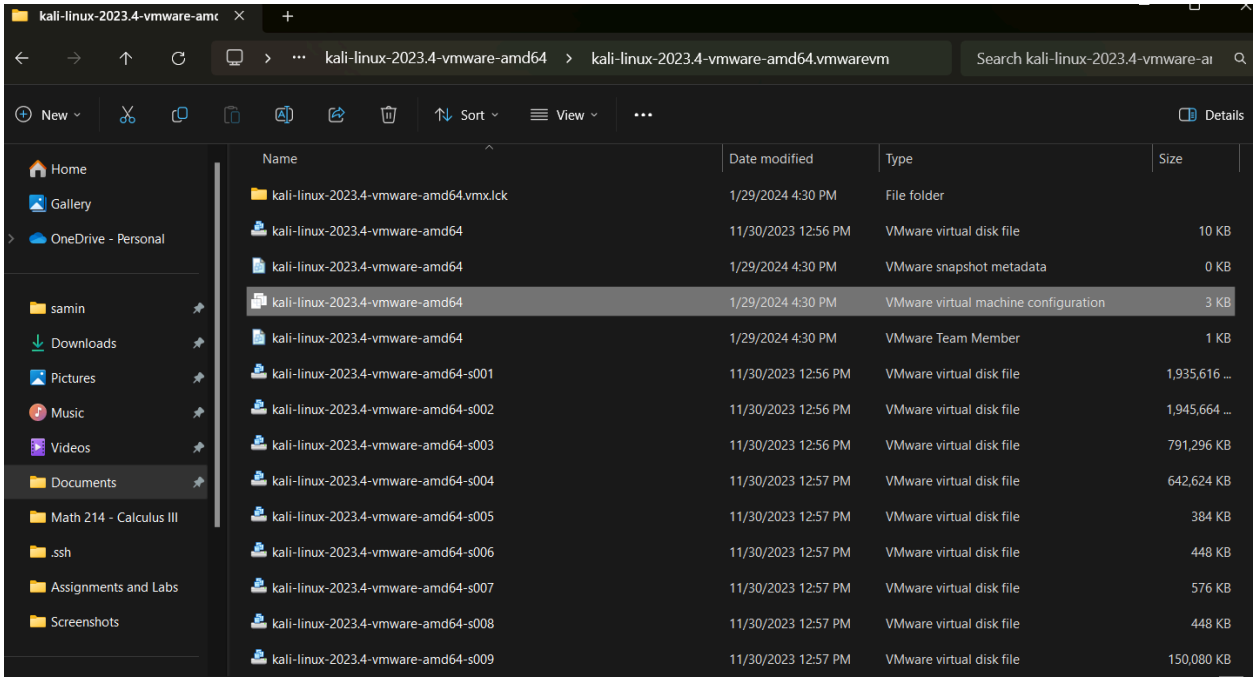

elastic
Find apps, content, and more.
Dashboard
Security Onion - Home
Full screen
Share
Clone
Reset
Edit
Filter your data using KQL syntax
Last 24 hours
Refresh
Security Onion - Navigation
Home
Event Category
Alert | File | Host | Network
Security Onion - All Logs
1,819
Count
Security Onion - Logs Over Time
Count
@timestamp per 30 minutes
Security Onion - Data Overview
host
database
network
Security Onion - Dataset
Export
Dataset
Count
syscollector 742
access 308
elasticsearch.server 243
ossec 199
kibana.log 157
application 77
audit 63
Security Onion - Modules
Export
Module
Count
ossec 967
kratos 448
elasticsearch 243
kibana 157
zeek 4
Security Onion - Log Count By Node
Export
Node
Count
seconion 4


Search or jump to...
Sign in
Home › Dashboards › Dashboards › Security Onion Grid Overview
Last 3 hours
5m
Node All
Role All
Docker Containers All
Disk All
Overview
System Uptime
current
seconion eval 25.6 min
Container Uptime Current
seconion eval so-playbook 19.9 min
seconion eval so-wazuh 19.9 min
seconion eval so-soctopus 20.0 min
seconion eval so-fleet 20.0 min
seconion eval so-redis 20.1 min
seconion eval so-elastalert 20.2 min
seconion eval so-curator 20.2 min
seconion eval so-filebeat 21.2 min
CPU Usage
Name
Max
Mean
Last *
seconion eval 78.6% 14.8% 14.6%

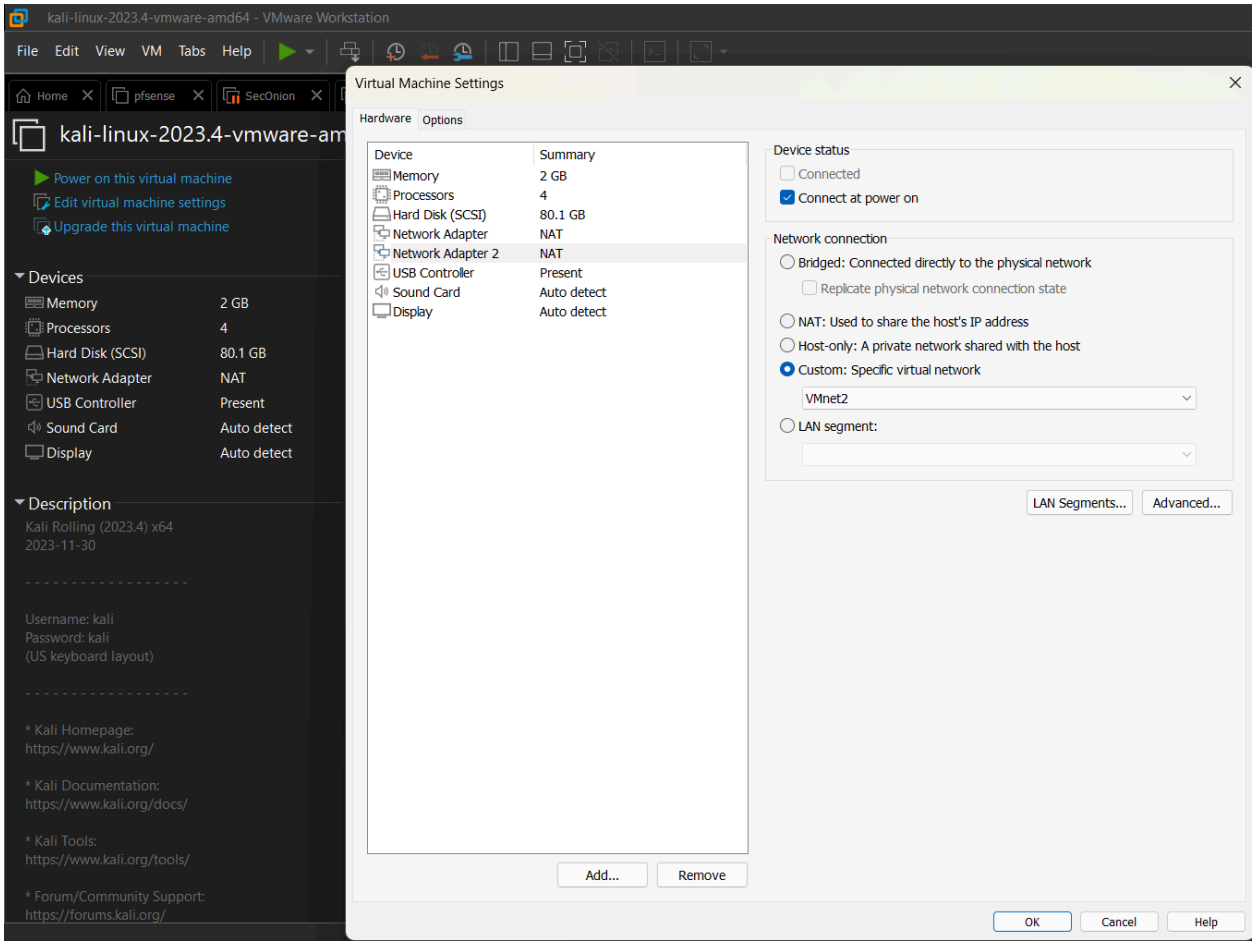
Configuring Kali as the Attack Box

First we will need to download the Kali image, which can be found on their website. For this lab, we will be downloading the VMware 64 bit version:

Once downloaded, extract the file to where you would like it to be, and then search for the file ending in .vmx (alternatively, look for the “VMware virtual machine configuration” file) and open it. It should open up the machine in VMware

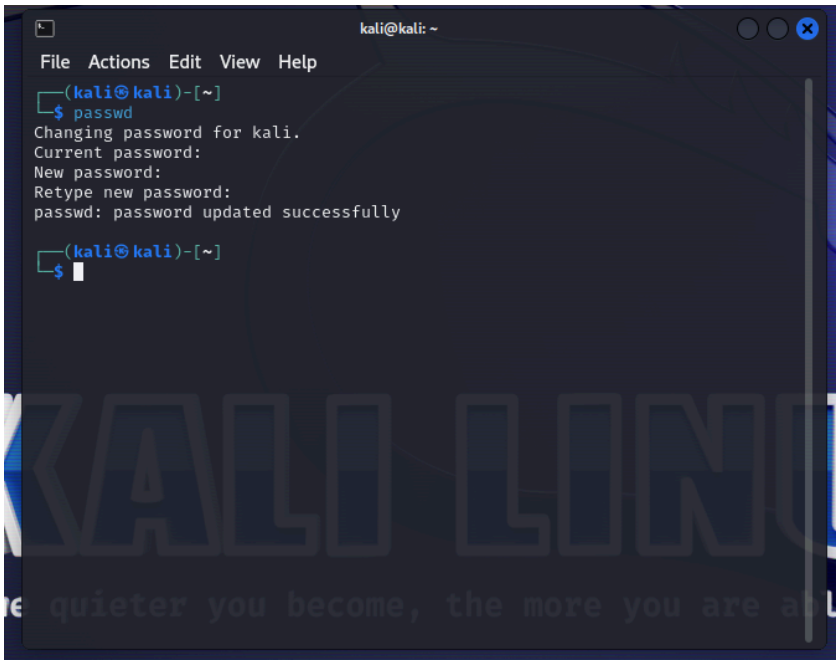


Edit the virtual machine settings to add another Network Adapter and map it to VMnet2:



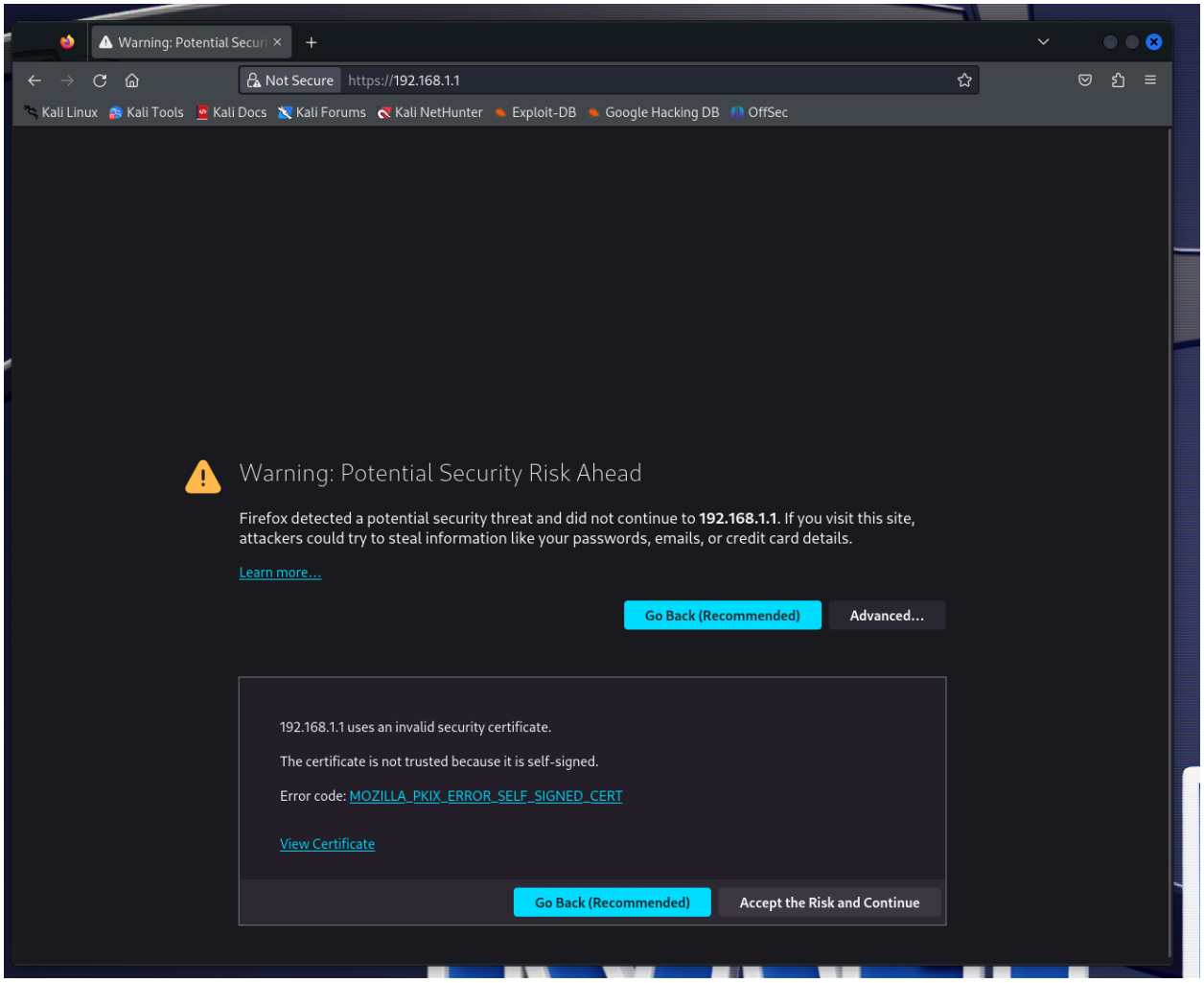
You can now boot up the machine and login with the default credentials (username and password are both “kali”)

You can change the password by running “passwd” on the terminal, where you will be prompted to enter the current password (“kali”) before you set the new password:

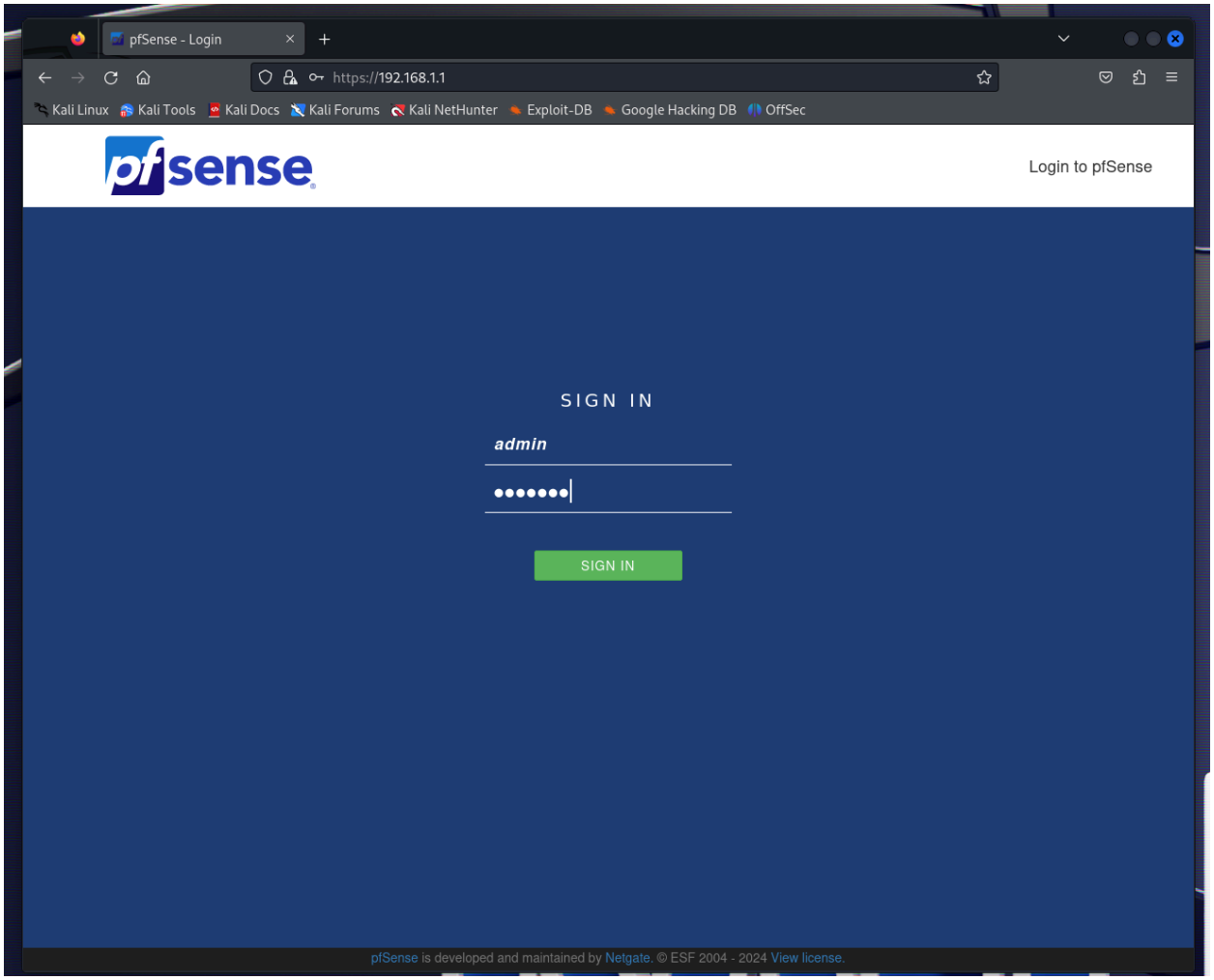


Configuring pfSense Interface and Firewall Rules

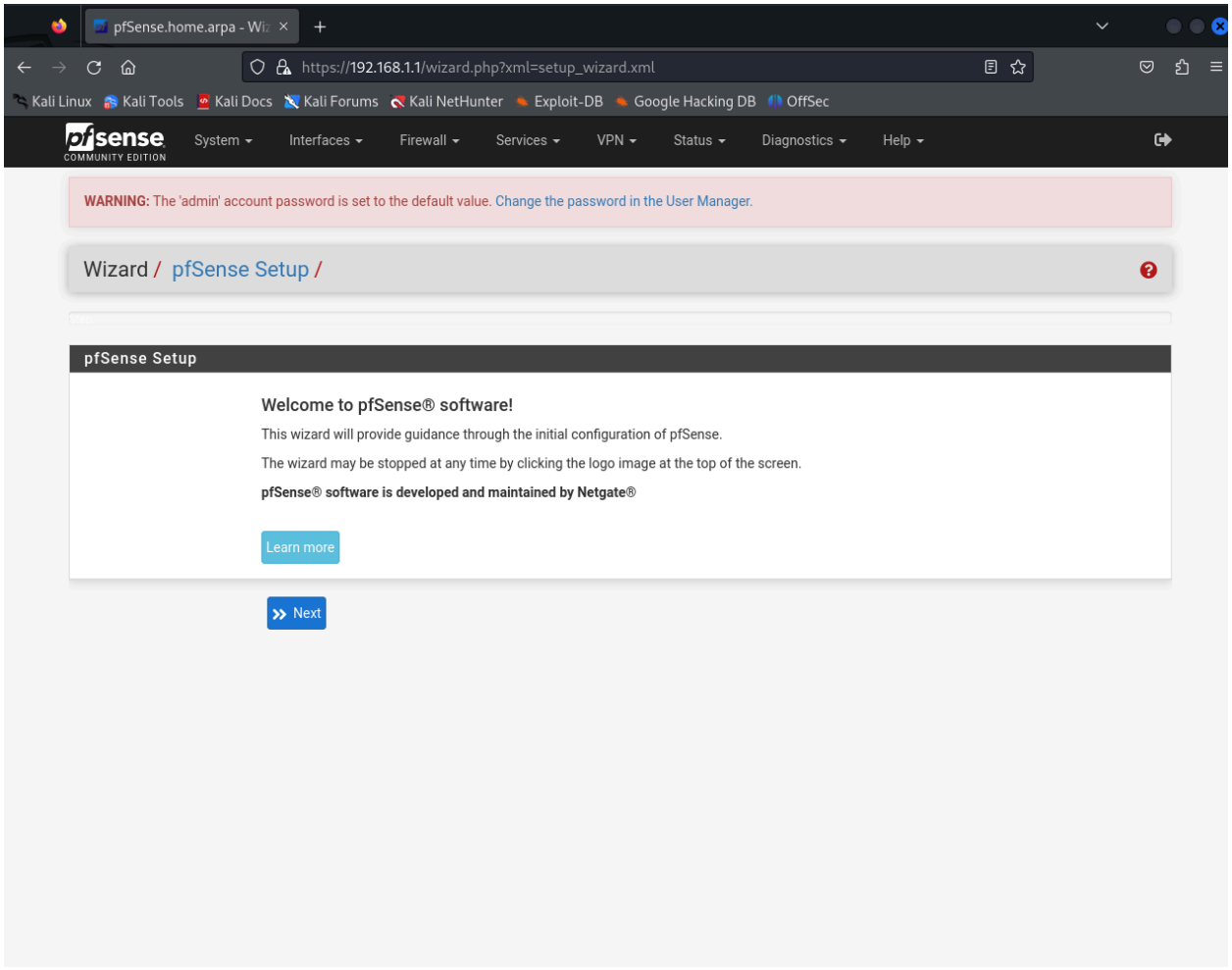
Log into the Kali machine and open up a web browser and navigate to 192.168.1.1. You will be warned about potential security risks, but you can accept and continue:

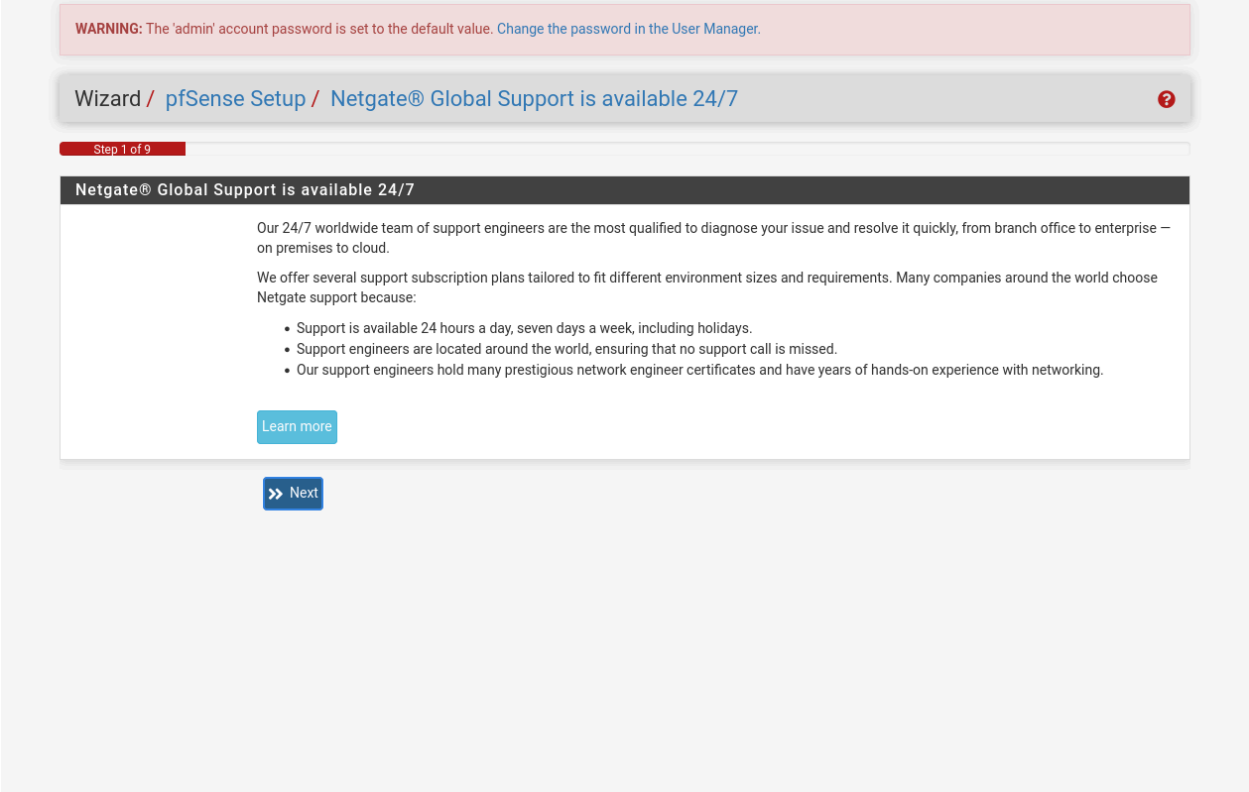


Login with the default credentials (“admin” and “pfsense” as username and password):

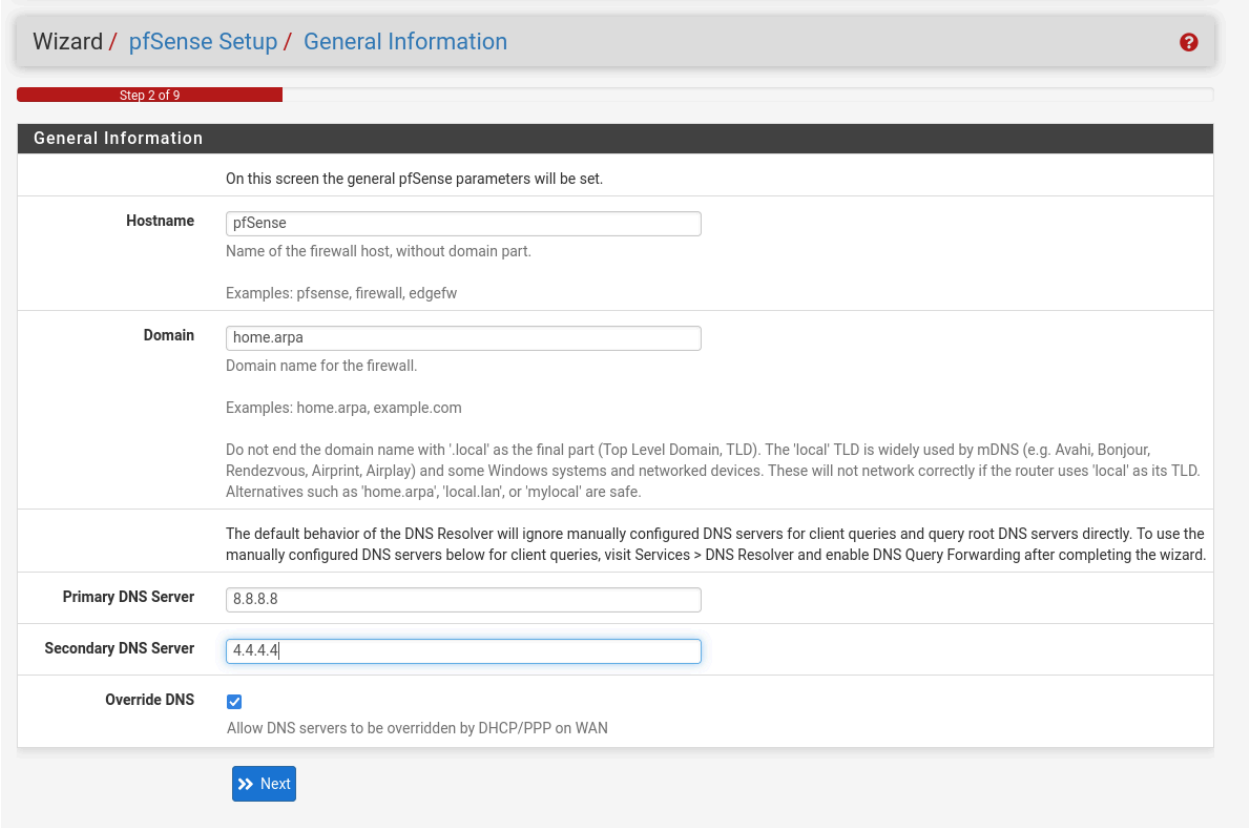


Click “Next” on the first two screens:

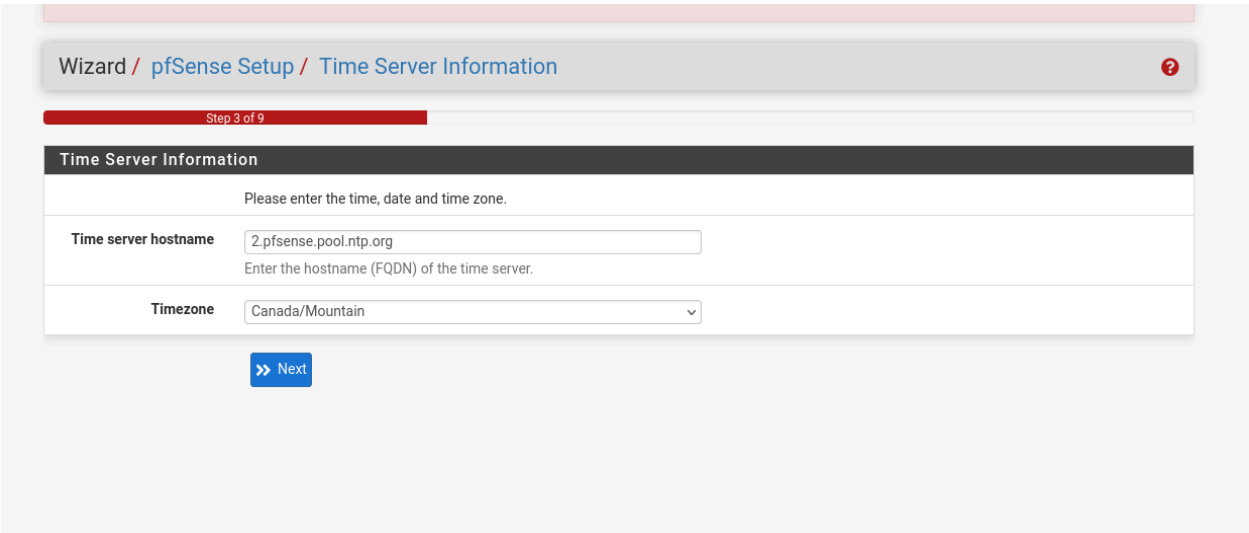

pfSense.home.arpa - Wiz
https://192.168.1.1/wizard.php?xml=setup_wizard.xml
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Wizard / pfSense Setup /
pfSense Setup
Welcome to pfSense® software!
This wizard will provide guidance through the initial configuration of pfSense.
The wizard may be stopped at any time by clicking the logo image at the top of the screen.
pfSense® software is developed and maintained by Netgate®
Learn more
Next



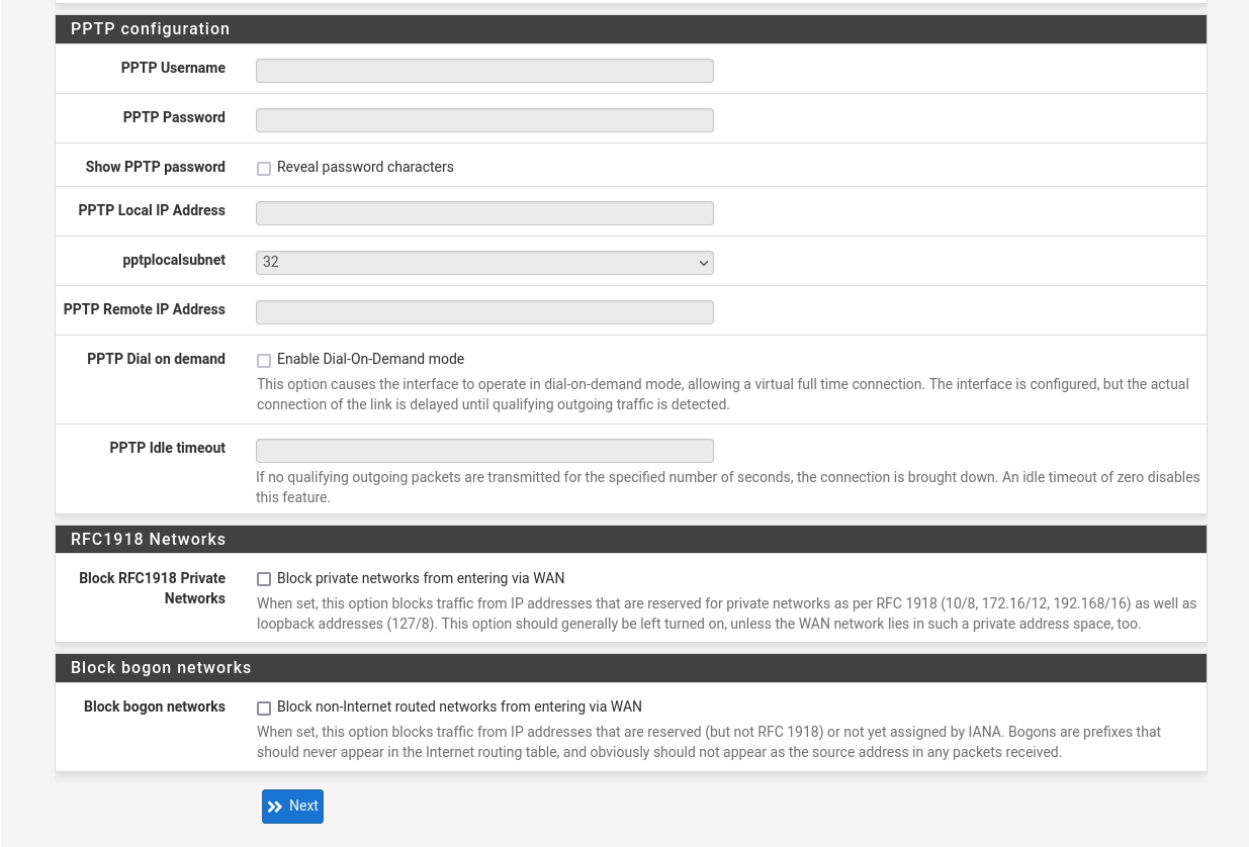
Enter “8.8.8.8” as the primary DNS server and “4.4.4.4” as the secondary before clicking “Next”:



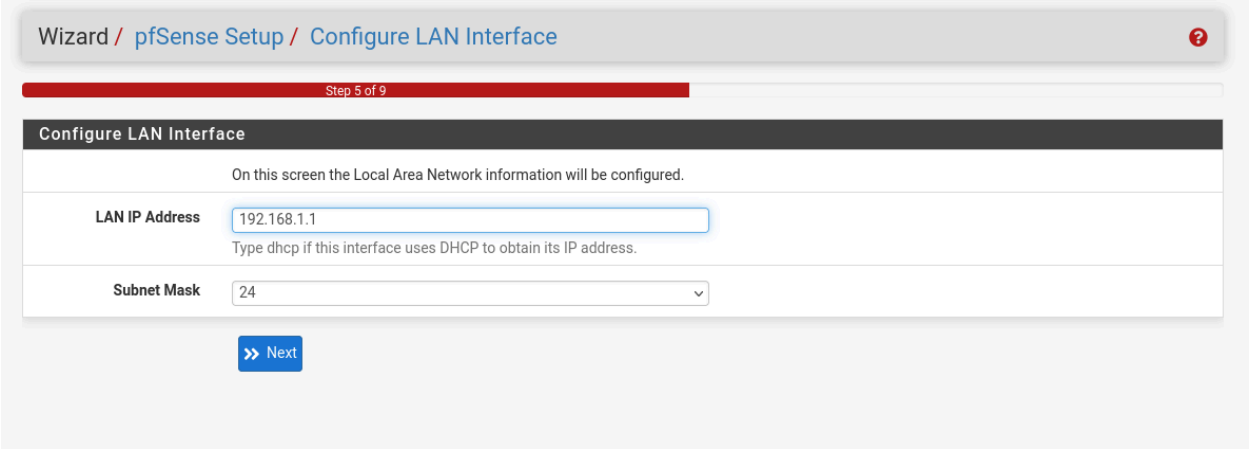
Select your timezone on the next screen and click “Next”:



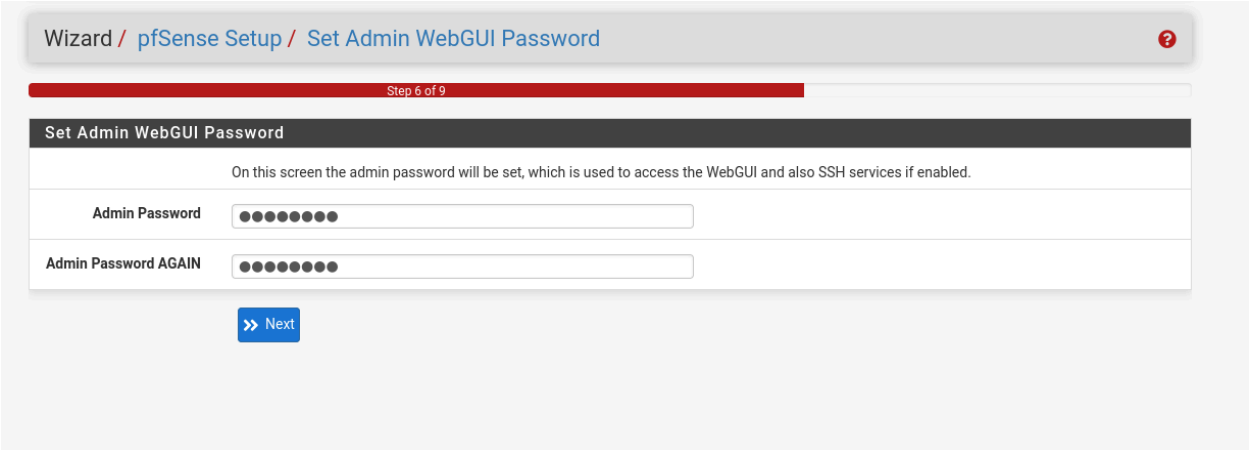
On the next screen, you can leave all the default selections. If you choose, you can unselect the two checkboxes at the bottom of the screen to see more alerts generated later on:



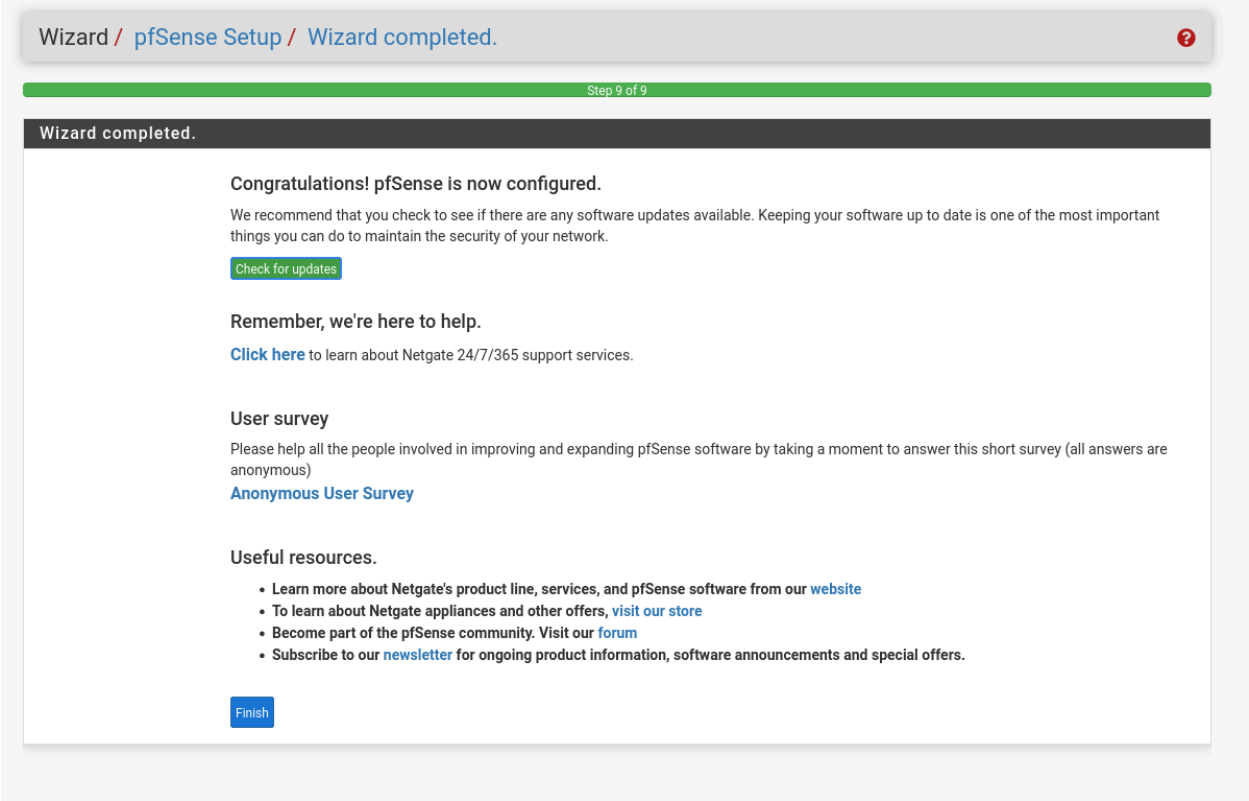
The next screen you should just click “Next”:



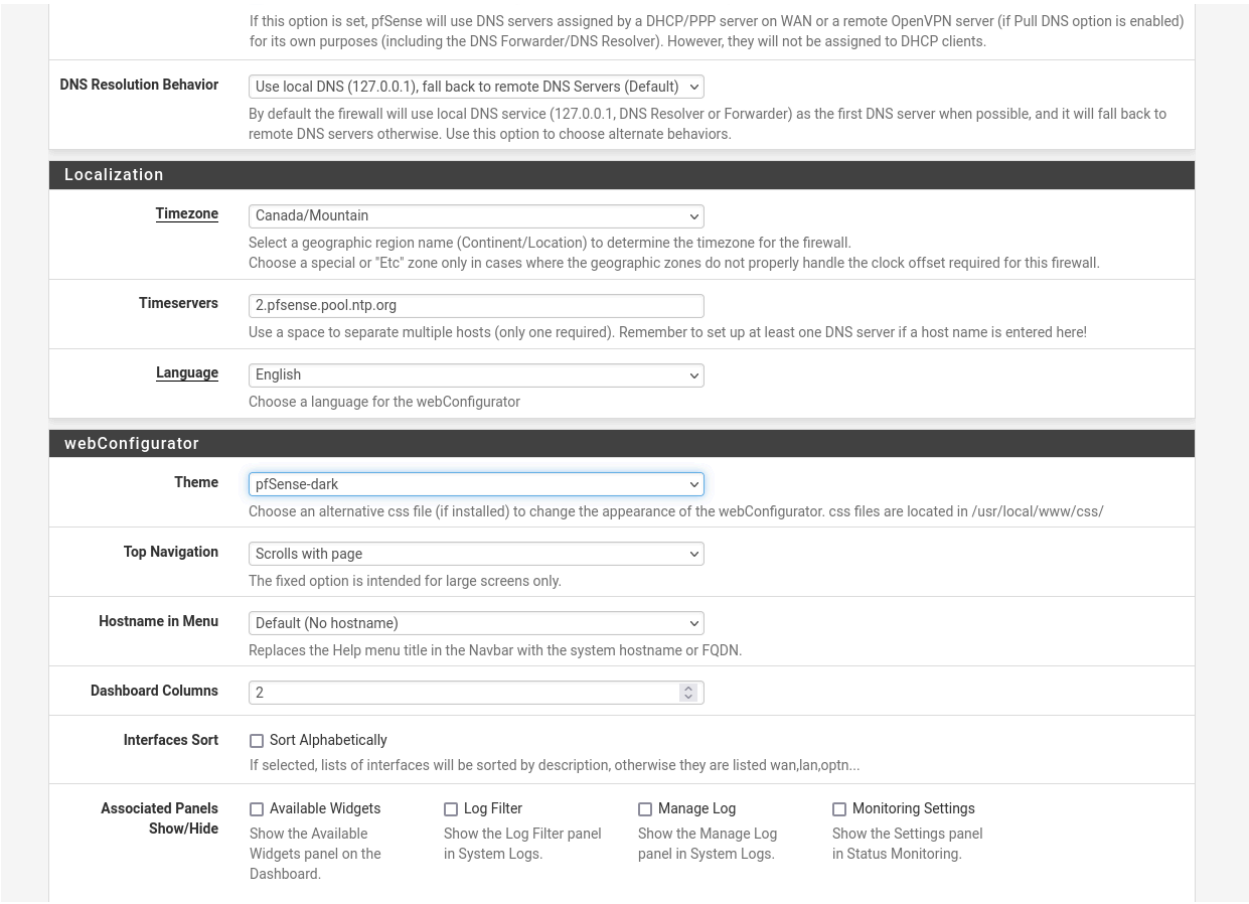
On the next screen, set a password before clicking “Next”:



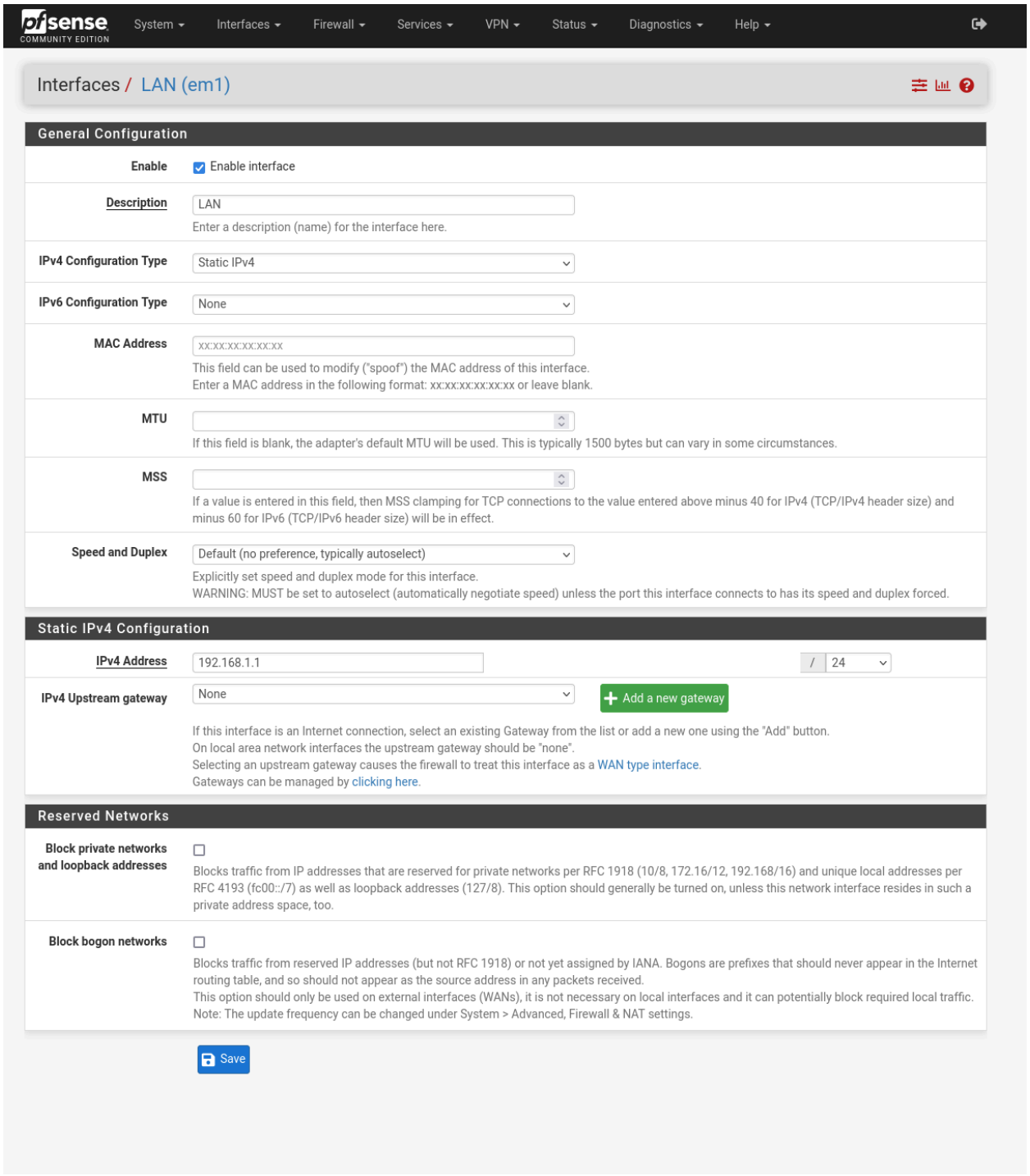
On the next screen, click “Reload” and it will reload pfSense with the new changes. You can then hit “Finish” when you are able to:



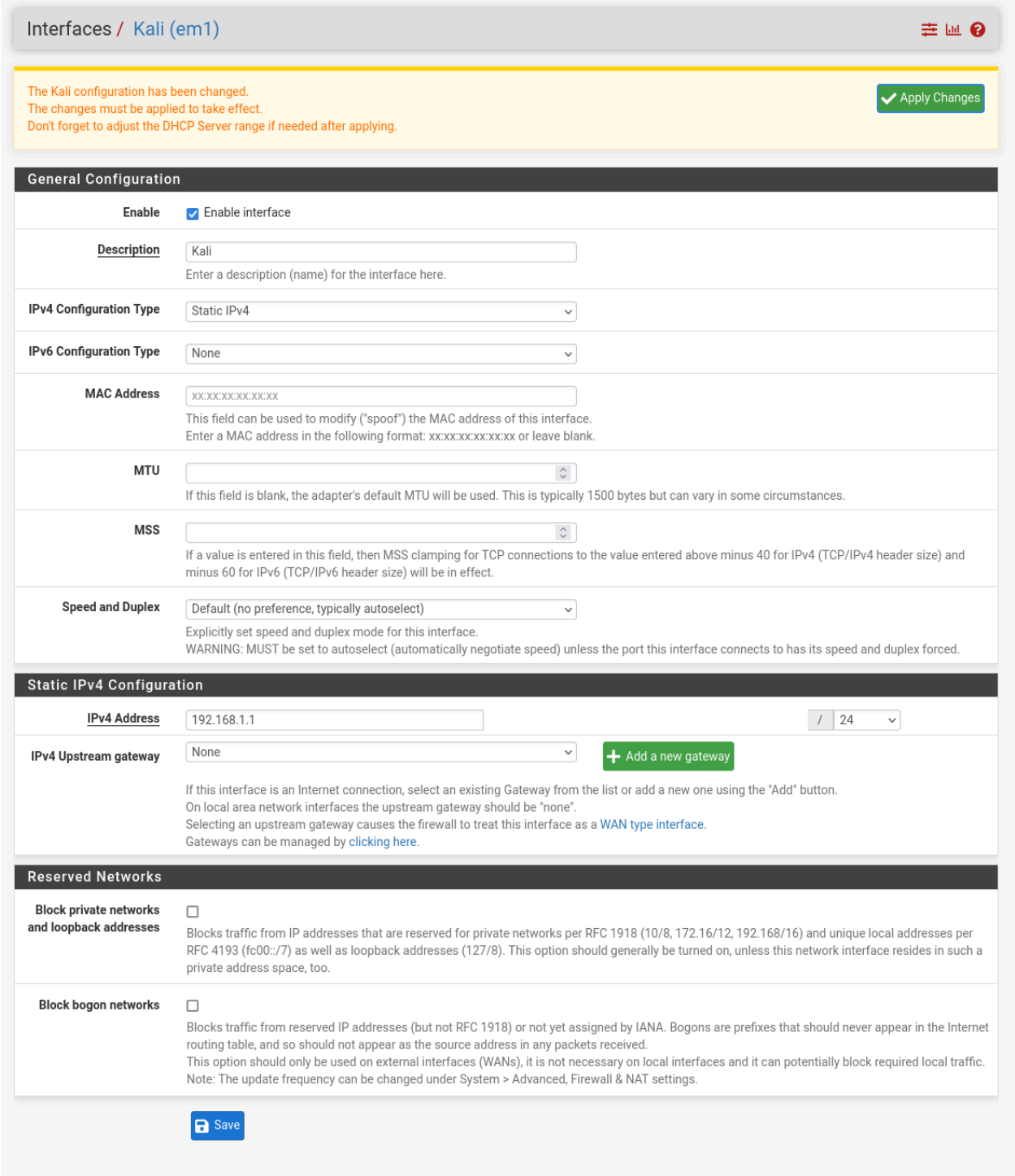
You can change to dark mode by selecting “General Setup” under “System” in the navigation bar at the top and changing the theme to pfSense-dark:



Under the “Intefaces” dropdown, select “Lan”:



This will be the Kali interface, so give it a description and hit “Apply Changes”:



Similarly, make the descriptions more descriptive for the remainder of the interfaces:

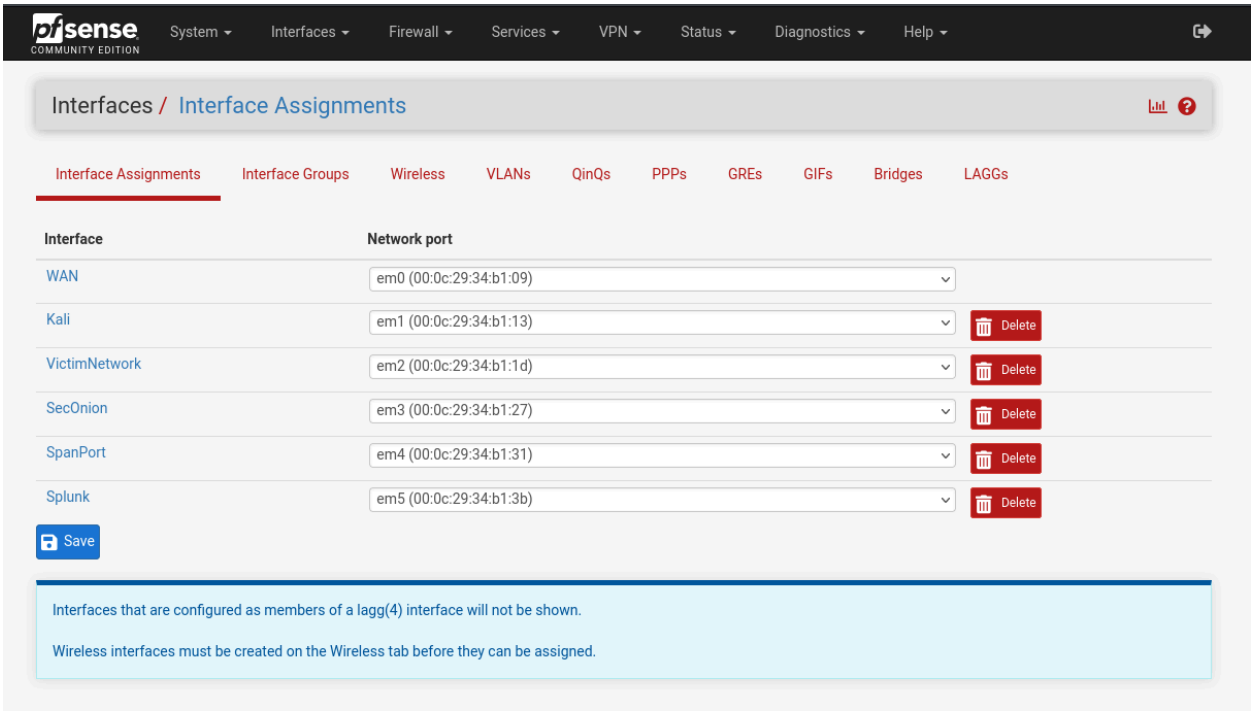
OPT1 will be for the victim network

OPT2 will be for Security Onion

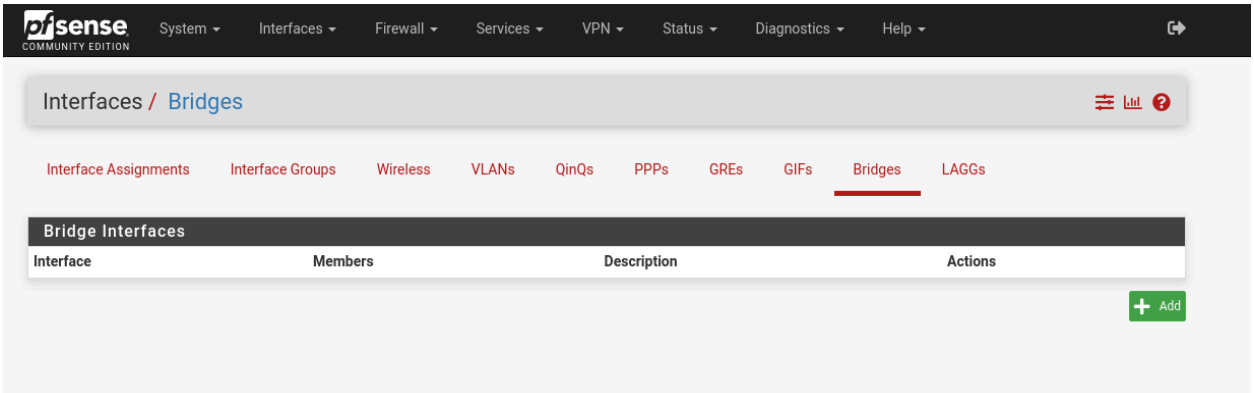
OPT3 will be for the span port

OPT4 will be for Splunk

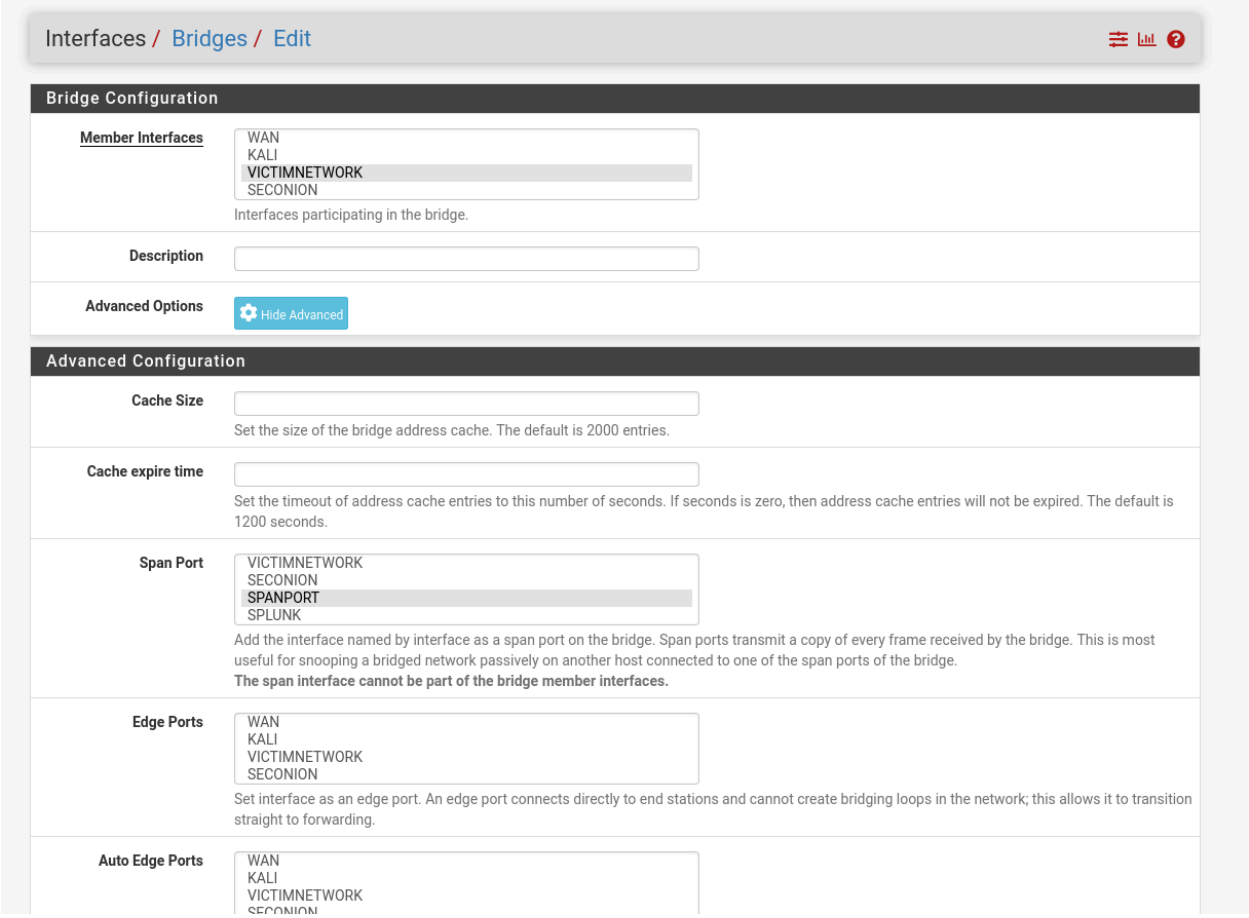
Make sure to check that “Enable interface” is checked for all of them, particularly OPT3. After you apply all changes, you should see the changes reflected under interface assignments:



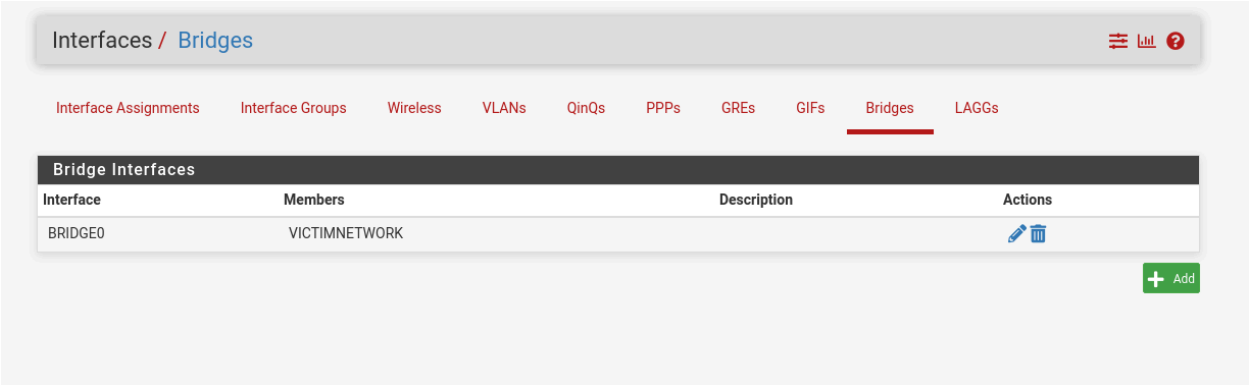
Enter the “Bridges” tab in the secondary navbar and click “Add”:



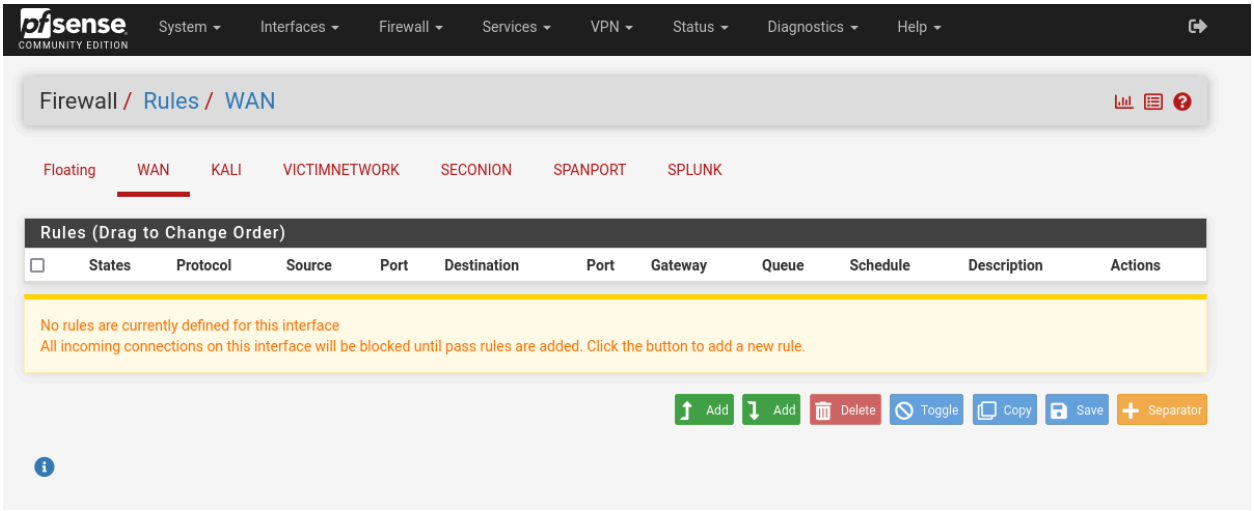
Select the victim network as the Member Interface and click “Display Advanced” so you can select the span port as the Span port:



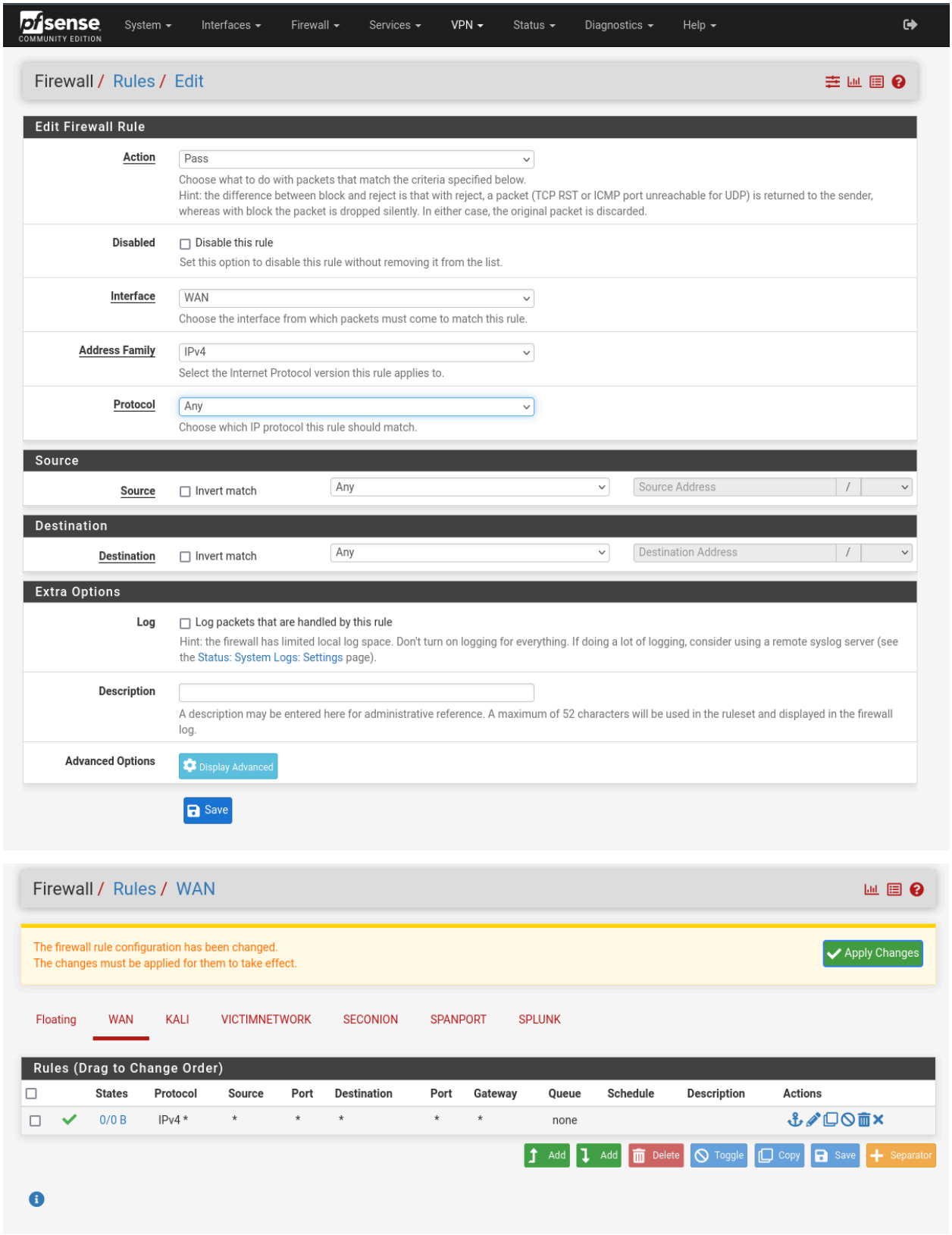
Press “Save” at the bottom of the screen after scrolling down:



Create a rule for the firewall under “Rules” in the “Firewall” dropdown from the main navbar (ensure that the “Wan” tab is selected) by pressing the “Add” with a downwards facing arrow:

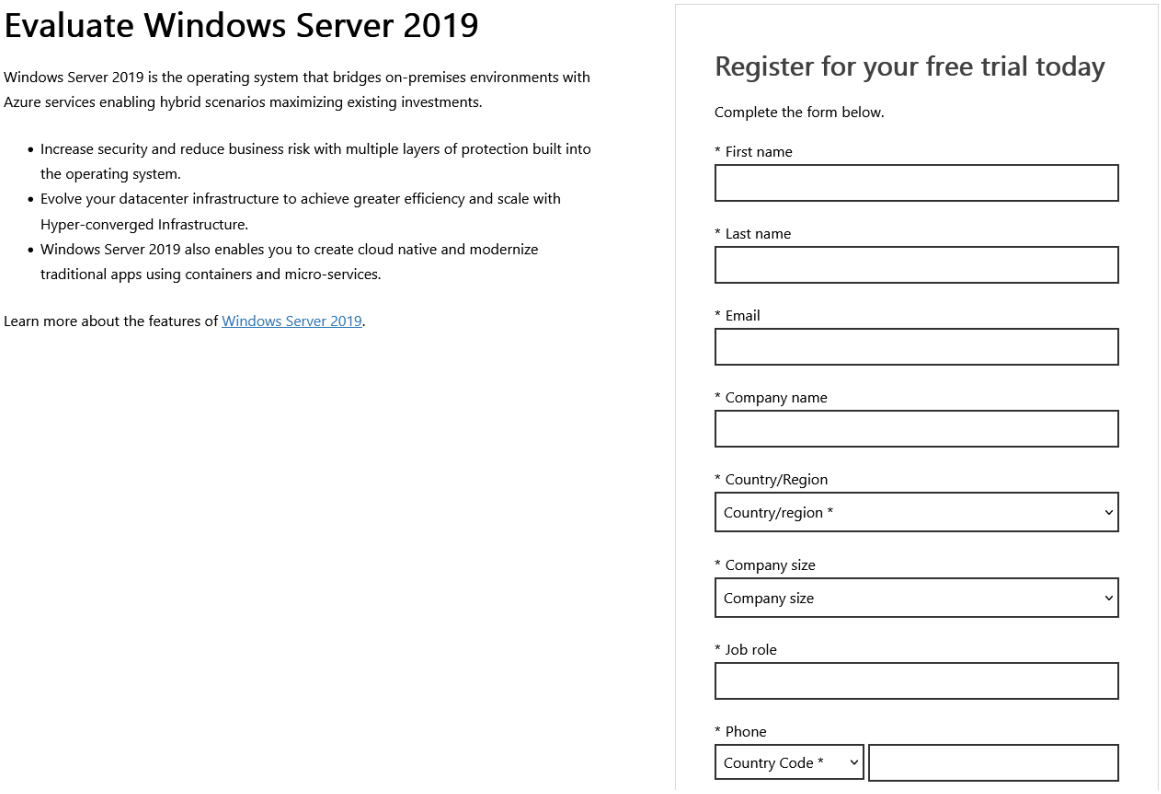


Change the protocol to “Any” and press save (this will allow for more alerts and logs to be generated). Click “Apply Changes” when brought back to the overview screen:


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / Edit
Edit Firewall Rule
Action
Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled
Disable this rule
Set this option to disable this rule without removing it from the list.
Interface
WAN
Choose the interface from which packets must come to match this rule.
Address Family
IPv4
Select the Internet Protocol version this rule applies to.
Protocol
Any
Choose which IP protocol this rule should match.
Source
Source
Invert match
Any
Source Address
Destination
Destination
Invert match
Any
Destination Address
Extra Options
Log
Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options
Display Advanced
Save
Firewall / Rules / WAN
The firewall rule configuration has been changed.
The changes must be applied for them to take effect.
Apply Changes
Floating
WAN
KALI
VICTIMNETWORK
SECONION
SPANPORT
SPLUNK
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
0/0 B
IPv4 *
none
Add
Add
Delete
Toggle
Copy
Save
Separator

Configuring Windows Server as a Domain Controller

Download the ISO image from here (it doesn't matter what you fill the form in with):



Evaluate Windows Server 2019

Windows Server 2019 is the operating system that bridges on-premises environments with Azure services enabling hybrid scenarios maximizing existing investments.

- Increase security and reduce business risk with multiple layers of protection built into the operating system.
- Evolve your datacenter infrastructure to achieve greater efficiency and scale with Hyper-converged Infrastructure.
- Windows Server 2019 also enables you to create cloud native and modernize traditional apps using containers and micro-services.

Learn more about the features of Windows Server 2019.

Register for your free trial today

Complete the form below.

* First name

* Last name

* Email

* Company name

* Country/Region

Country/region *

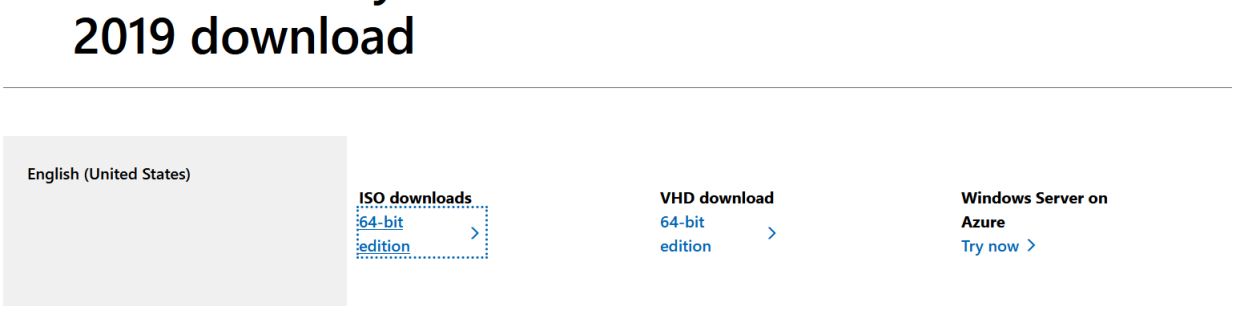
* Company size

Company size

* Job role

* Phone

Country Code *



Please select your Windows Server 2019 download

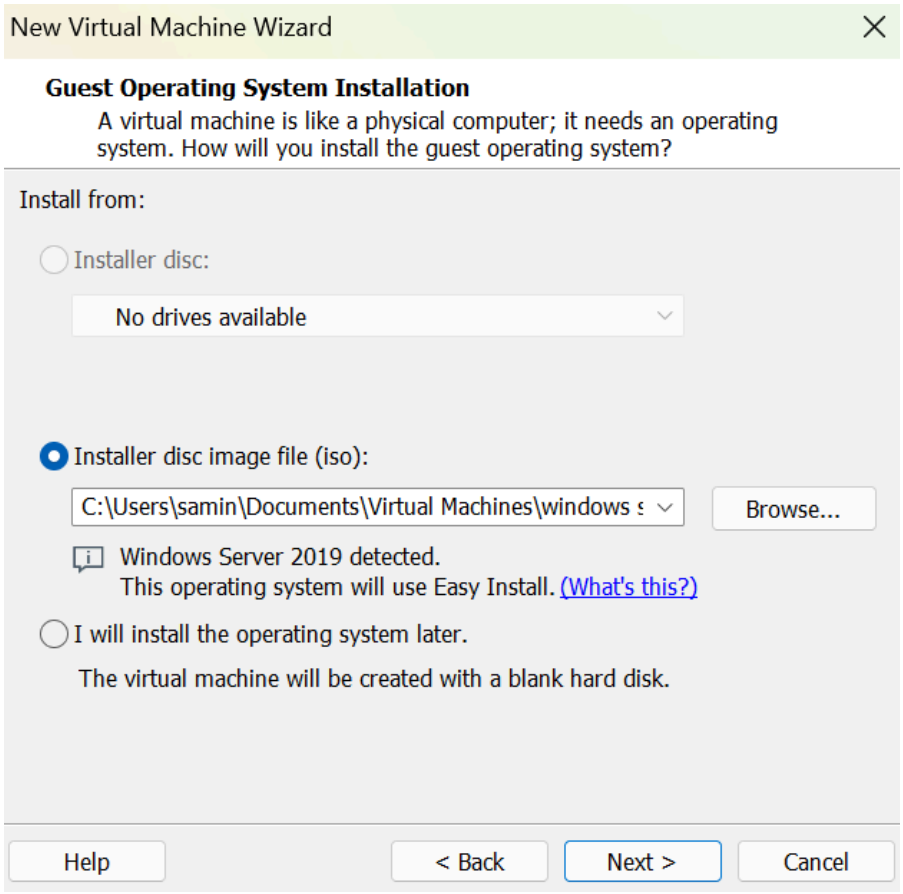
English (United States)

ISO downloads
64-bit edition >

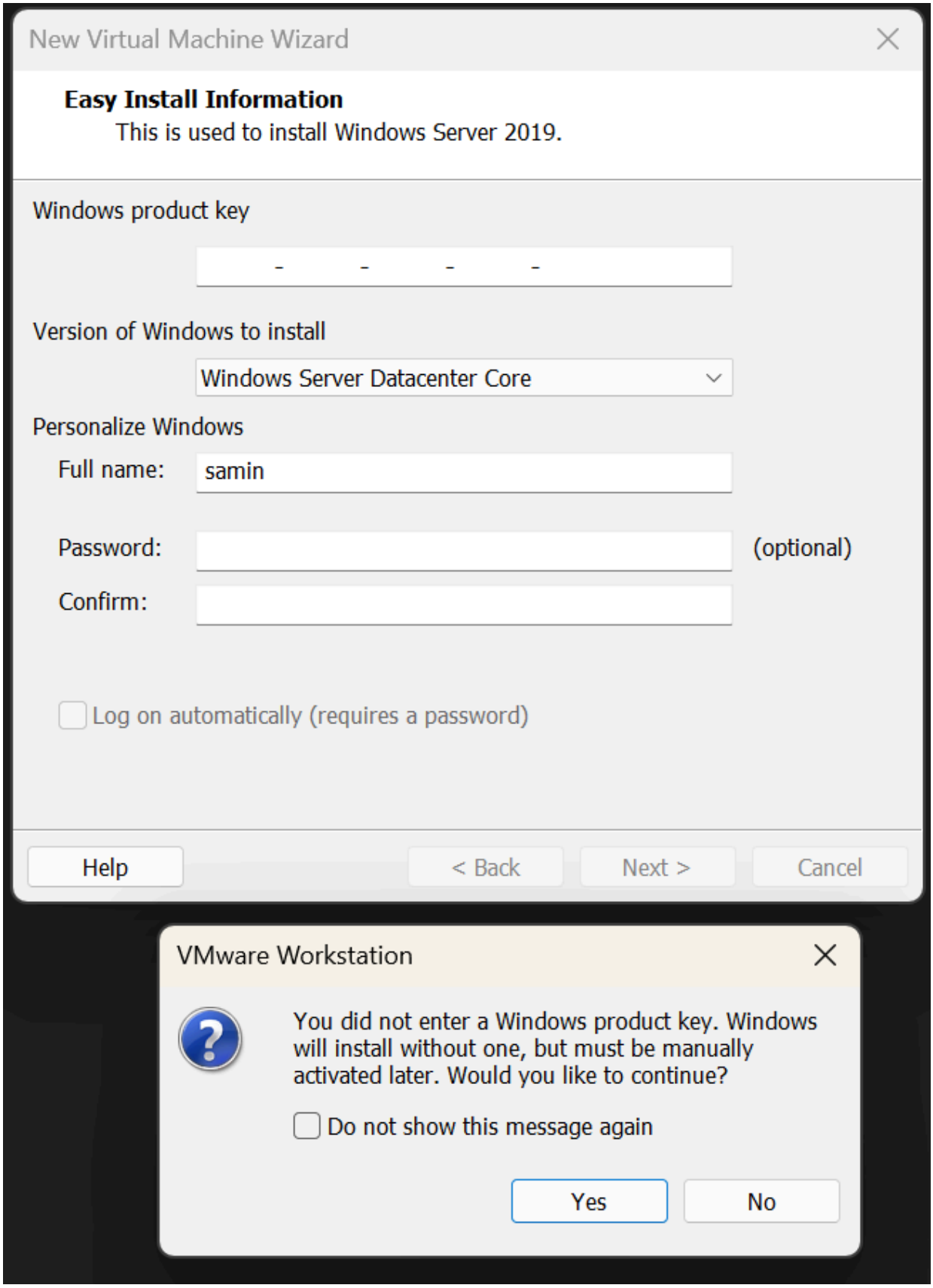
VHD download
64-bit edition >

Windows Server on Azure
Try now >

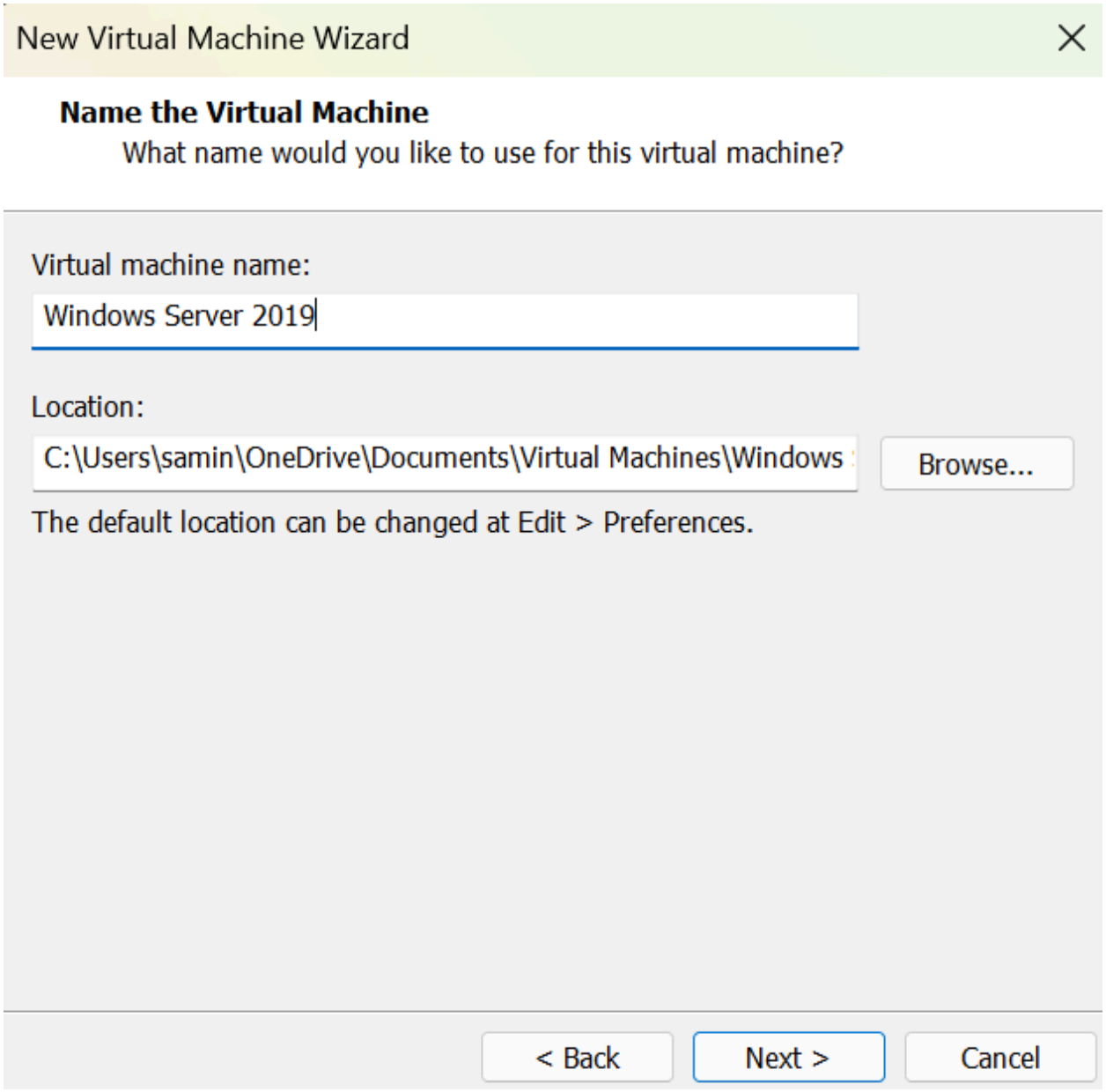
Create a new virtual machine with “Typical” configuration and select the iso file from where you downloaded it:



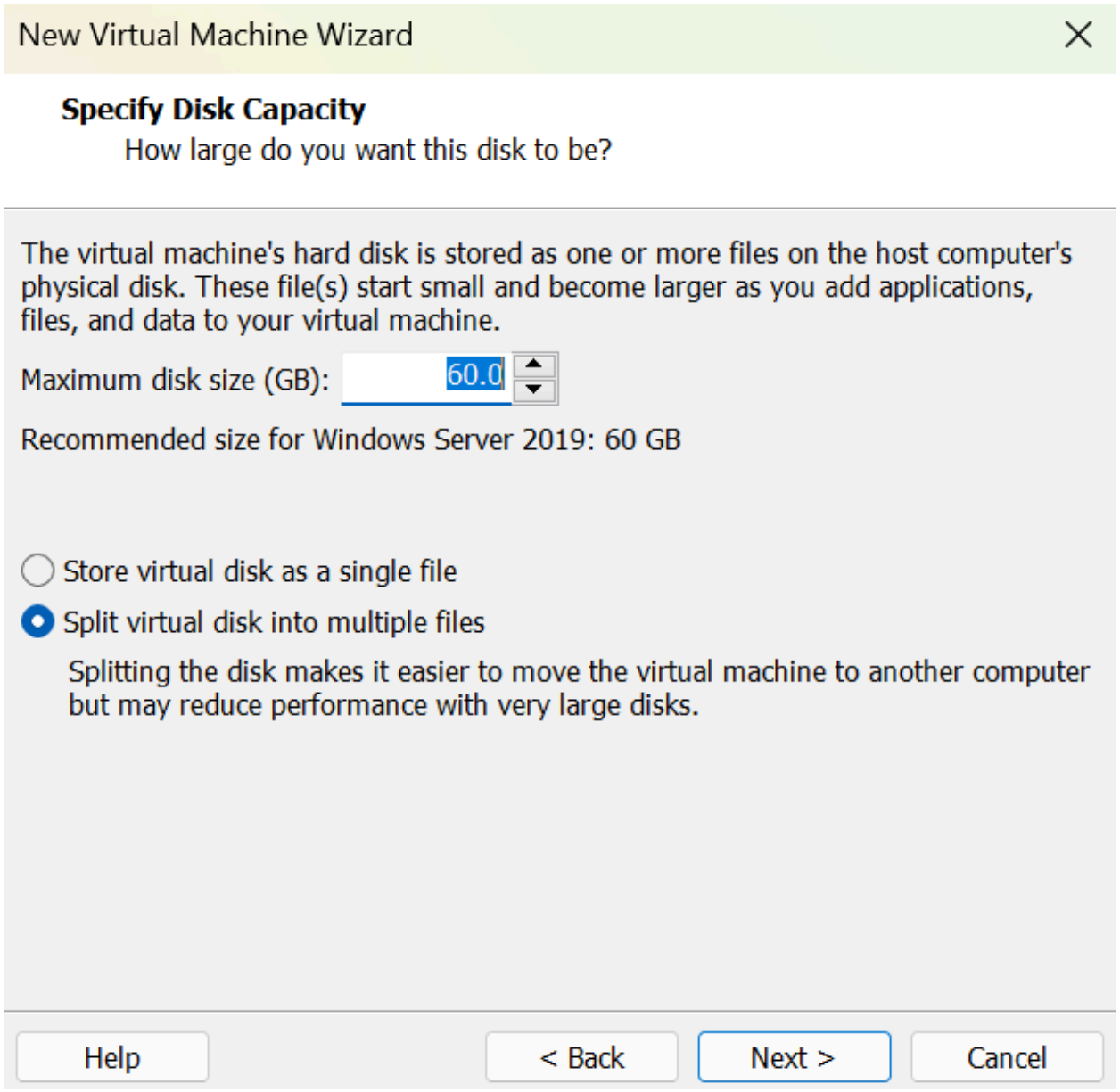
The next screen where you are asked for a product key you can ignore and continue:


New Virtual Machine Wizard
Easy Install Information
This is used to install Windows Server 2019.
Windows product key
- - - -
Version of Windows to install
Windows Server Datacenter Core
Personalize Windows
Full name:
samin
Password:
(optional)
Confirm:
Log on automatically (requires a password)
Help
< Back
Next >
Cancel
VMware Workstation
You did not enter a Windows product key. Windows will install without one, but must be manually activated later. Would you like to continue?
Do not show this message again
Yes
No

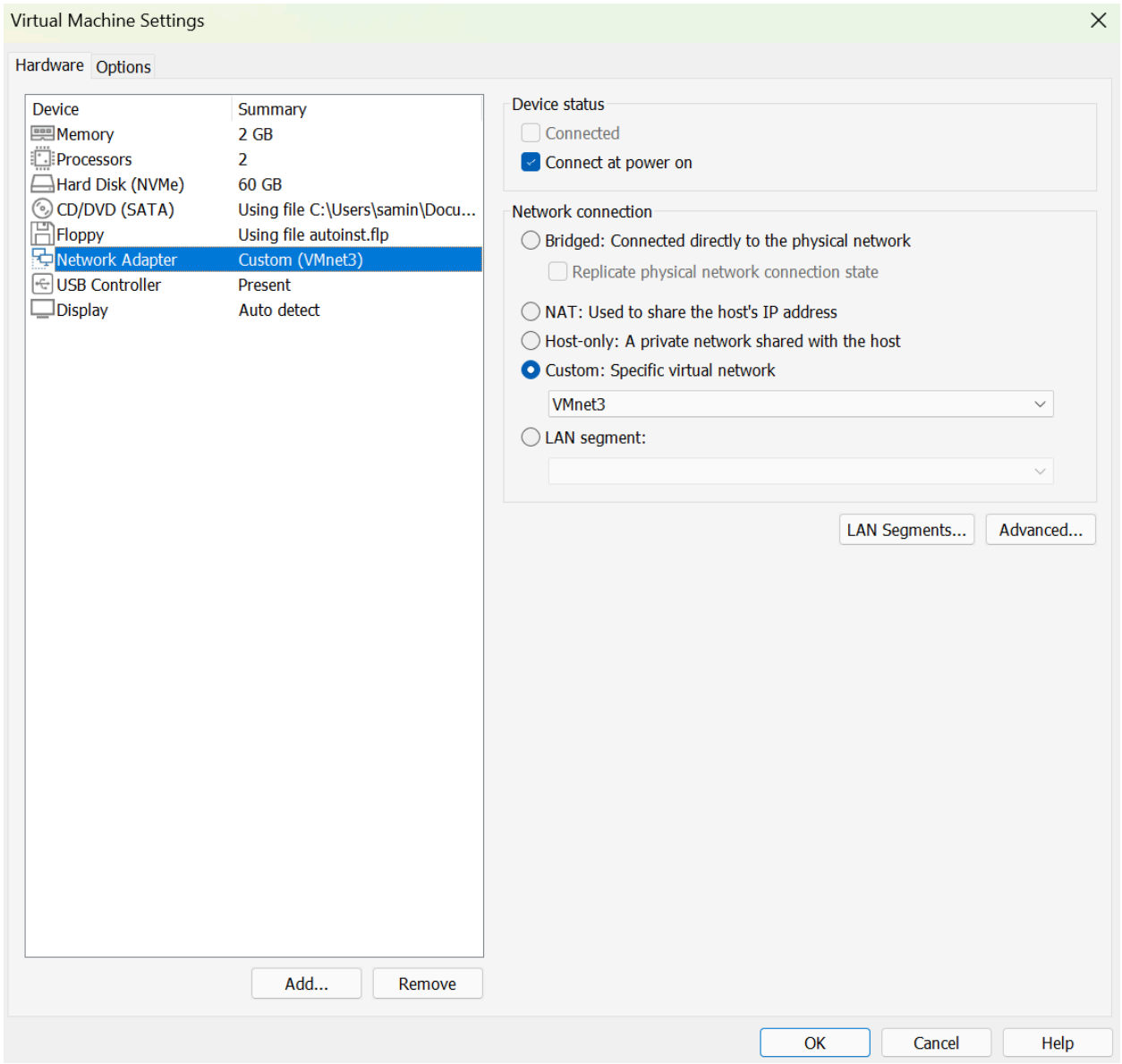
You can give the machine a name and choose the location to store it next:



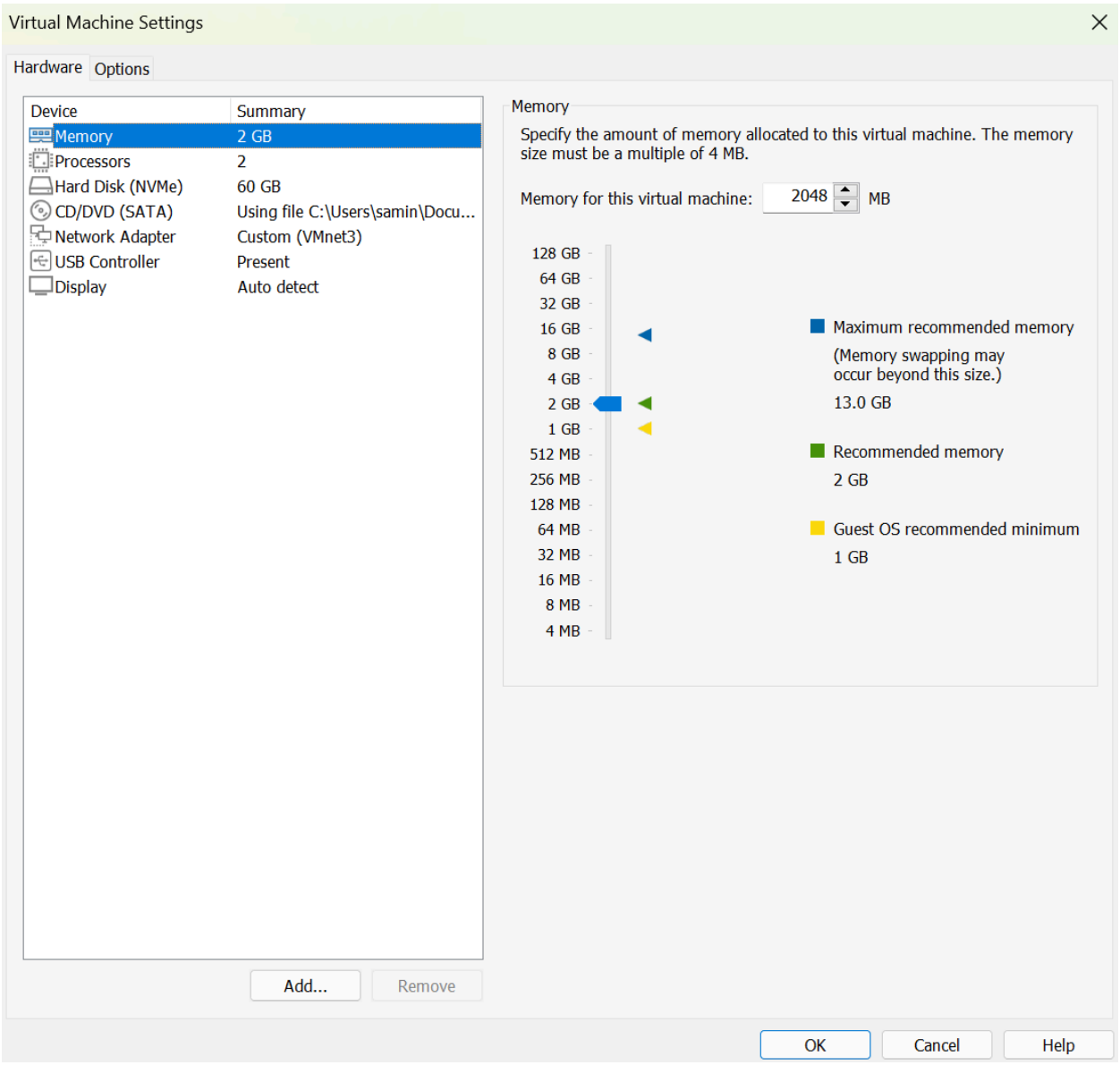
You can keep the default selections for the disk:



Uncheck the checkbox for powering on after completion, and customize the hardware to make the network adapter map to VMnet3:

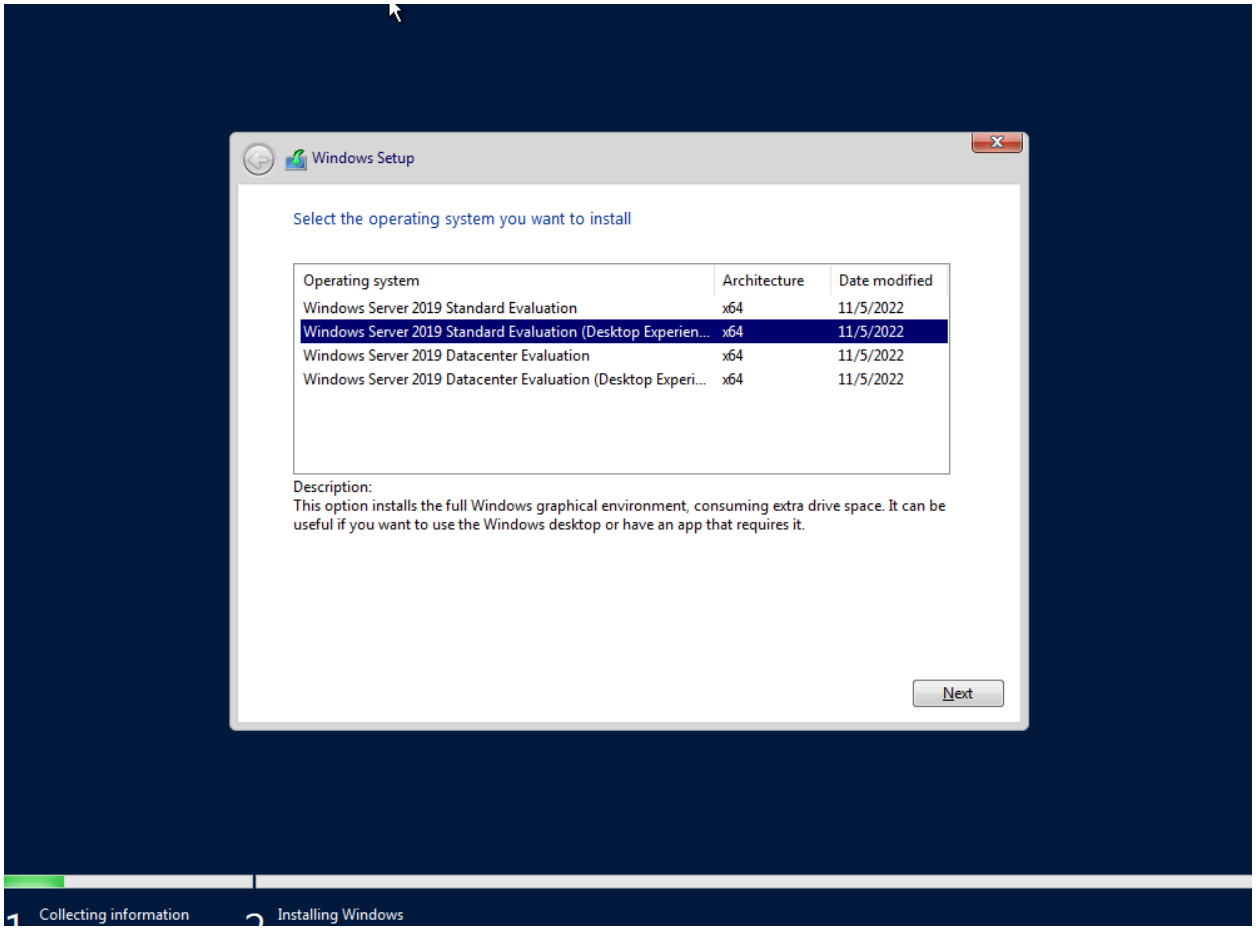


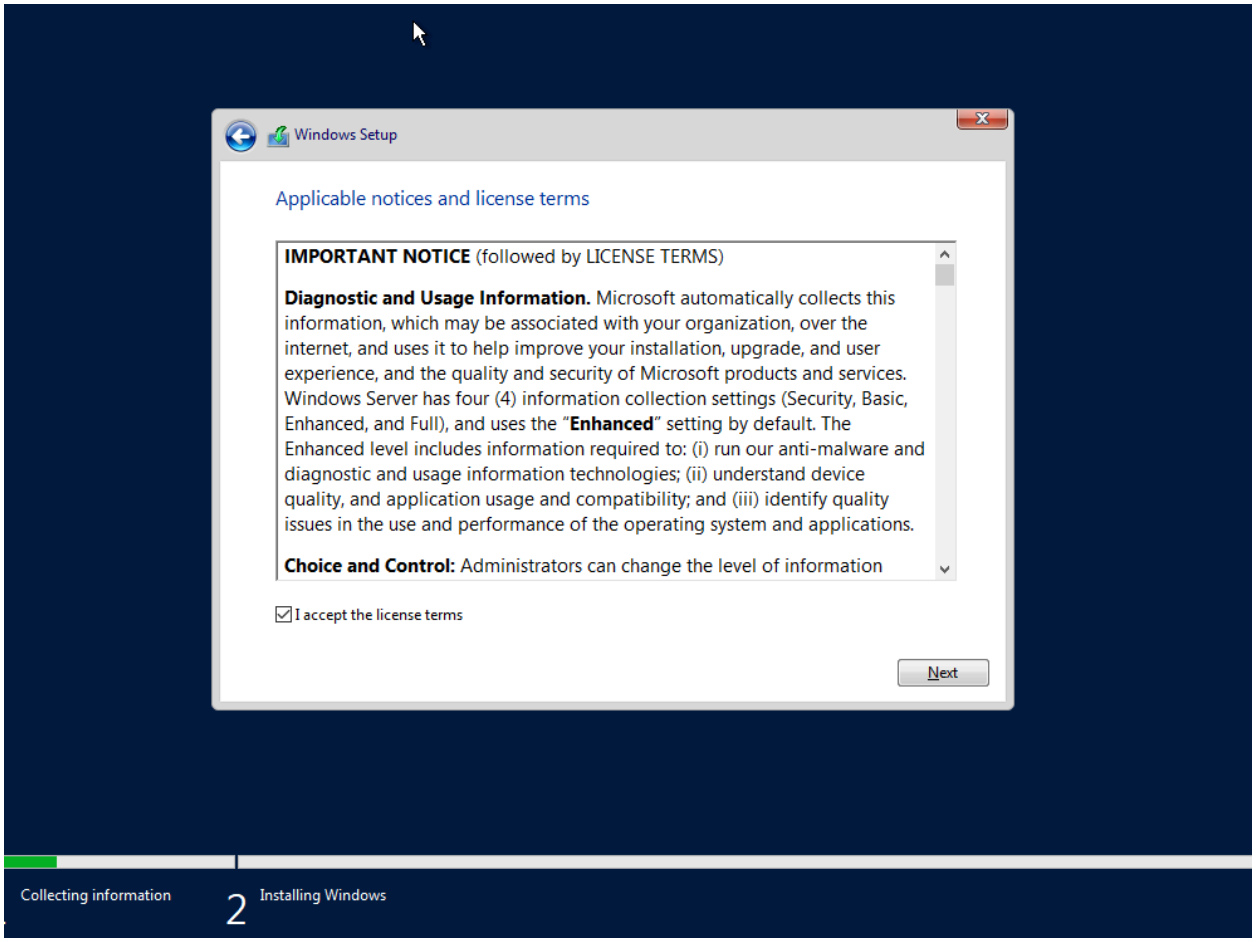
Remove the floppy drive:



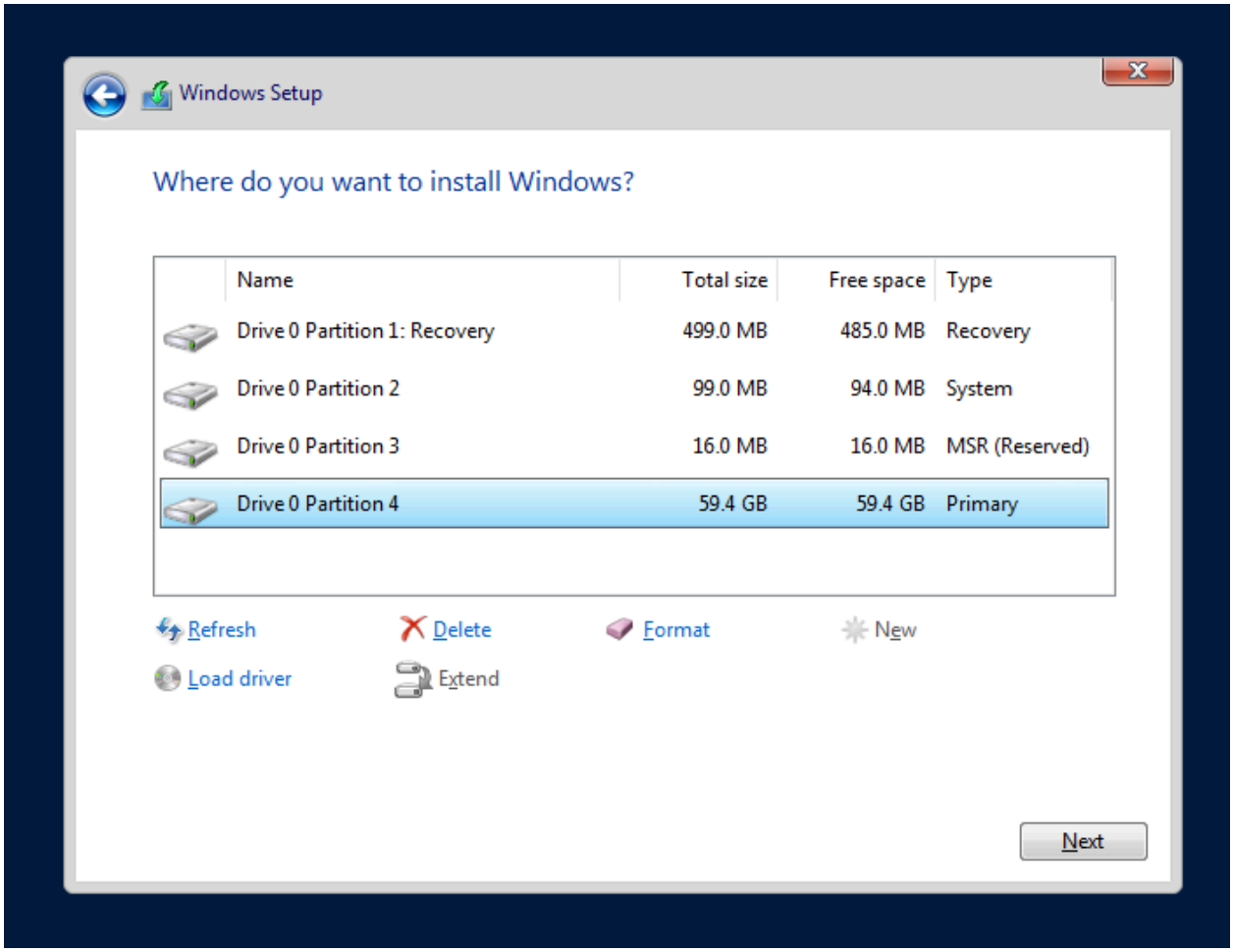
Power the machine on and press a key very quickly (otherwise it will time out). Click “Next” and then “Install Now”.

Select “Windows Server 2019 standard Evaluation (Desktop Experience)” before clicking “Next” and accepting the terms:

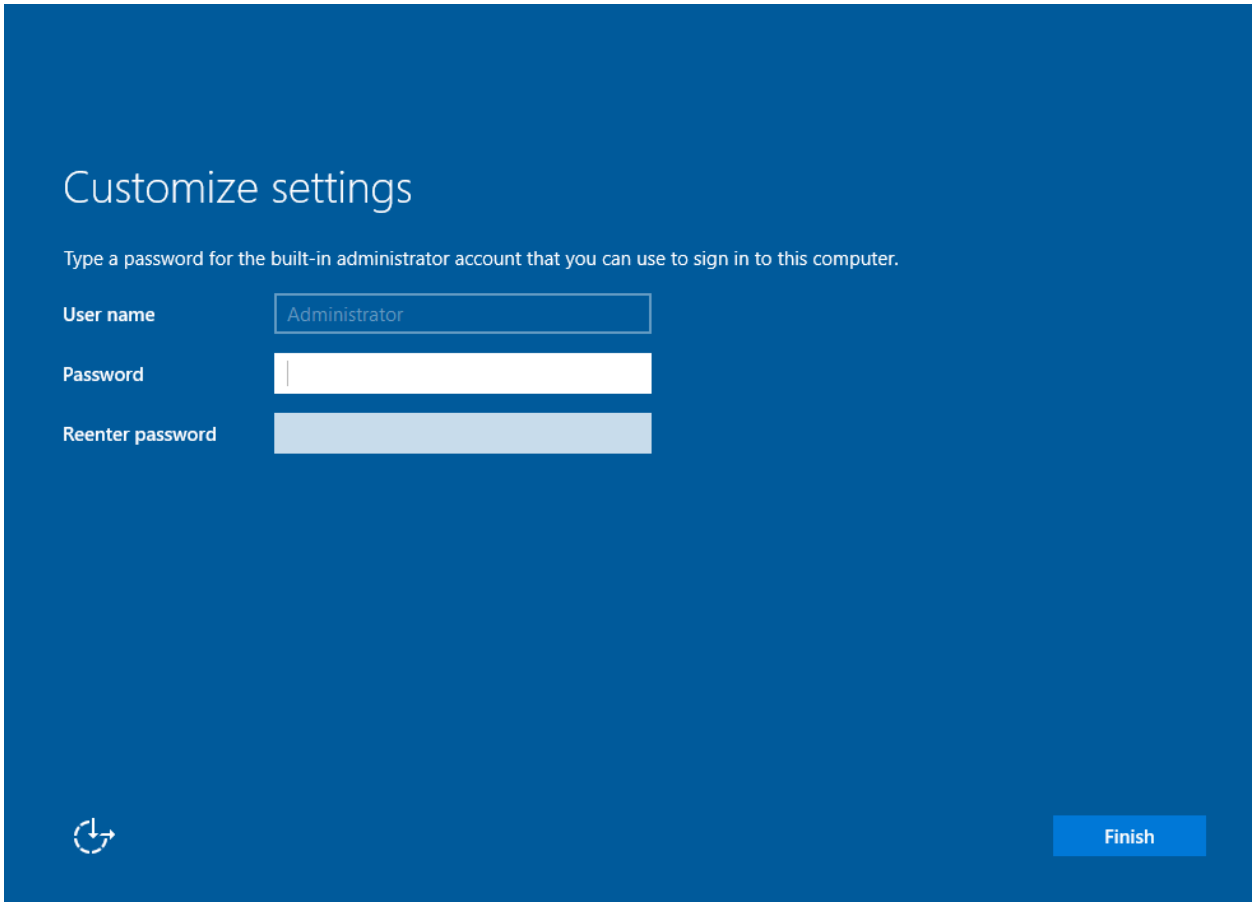

Windows Setup
Select the operating system you want to install
Operating system
Architecture
Date modified
Windows Server 2019 Standard Evaluation
x64
11/5/2022
Windows Server 2019 Standard Evaluation (Desktop Experien...
x64
11/5/2022
Windows Server 2019 Datacenter Evaluation
x64
11/5/2022
Windows Server 2019 Datacenter Evaluation (Desktop Experi...
x64
11/5/2022
Description:
This option installs the full Windows graphical environment, consuming extra drive space. It can be useful if you want to use the Windows desktop or have an app that requires it.
Next
1 Collecting information
2 Installing Windows



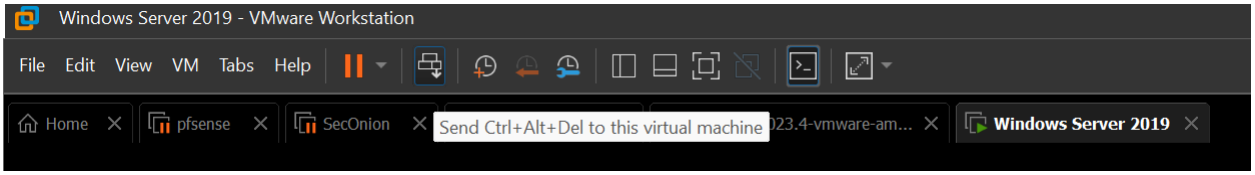
Click “New”, then “Apply”, and then “Ok” before clicking “Next”:



Once it finishes installing, create a password (does not need to be secure, since this is a lab environment):

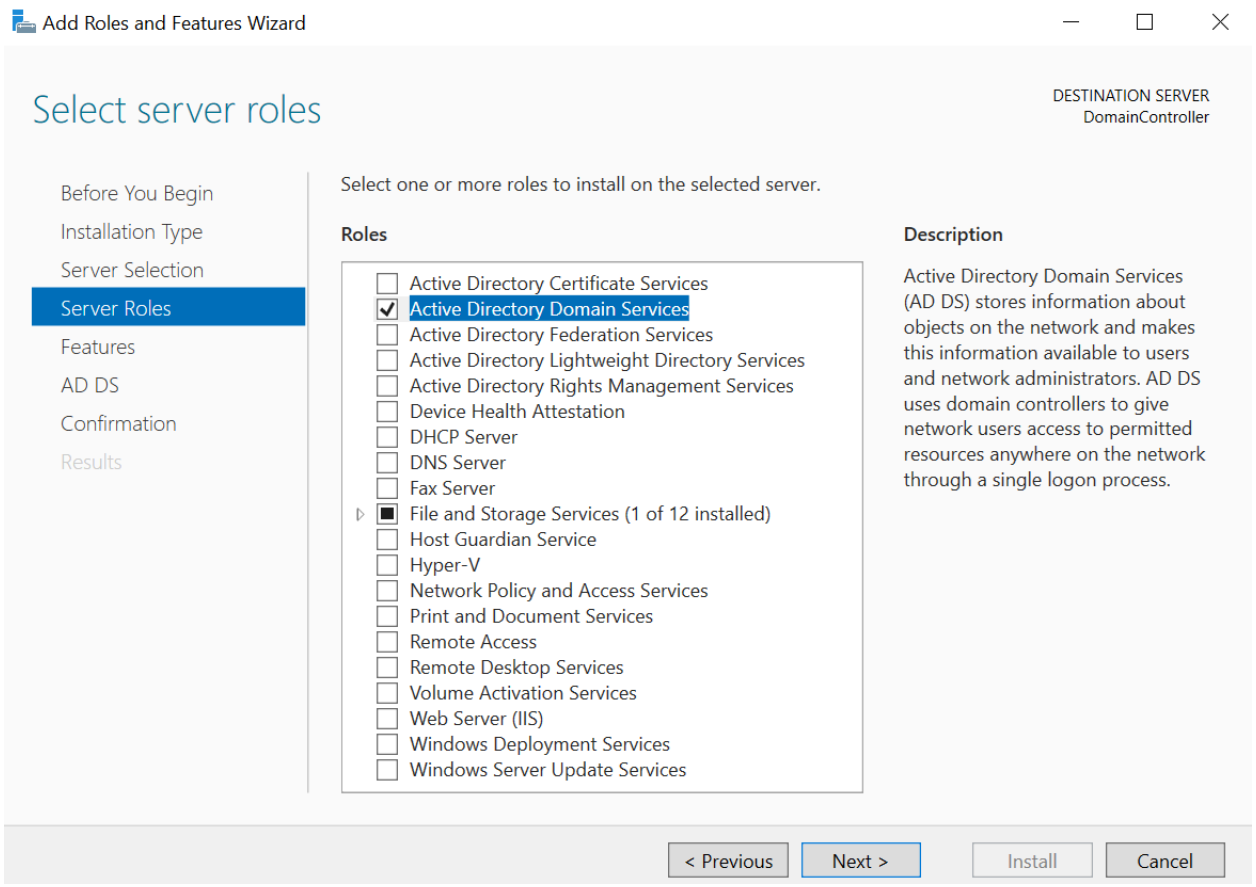


To log in, send CTRL-ALT-DELETE to the machine:

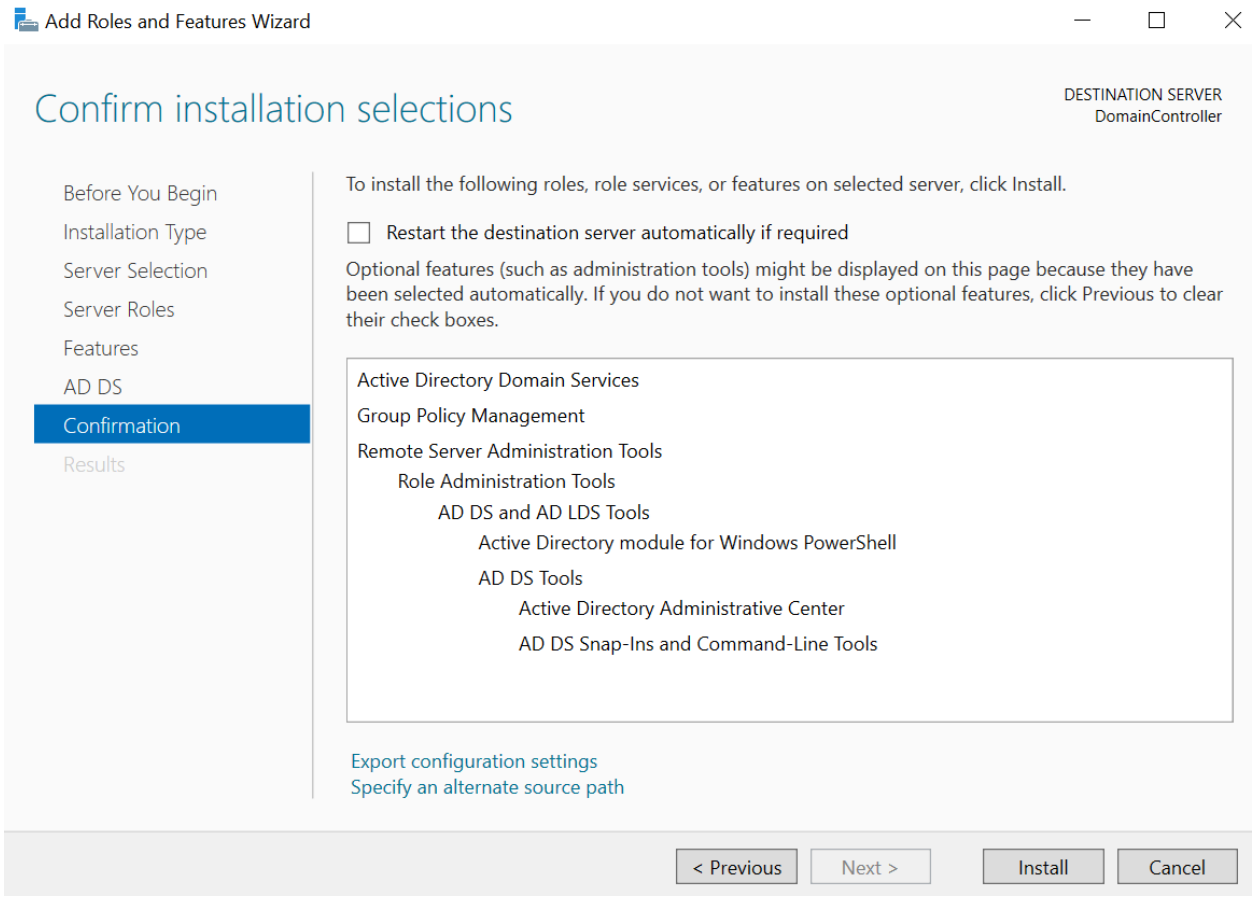


Once the Server Manager Dashboard loads up, Click “Add Roles and Features” under “Manage”

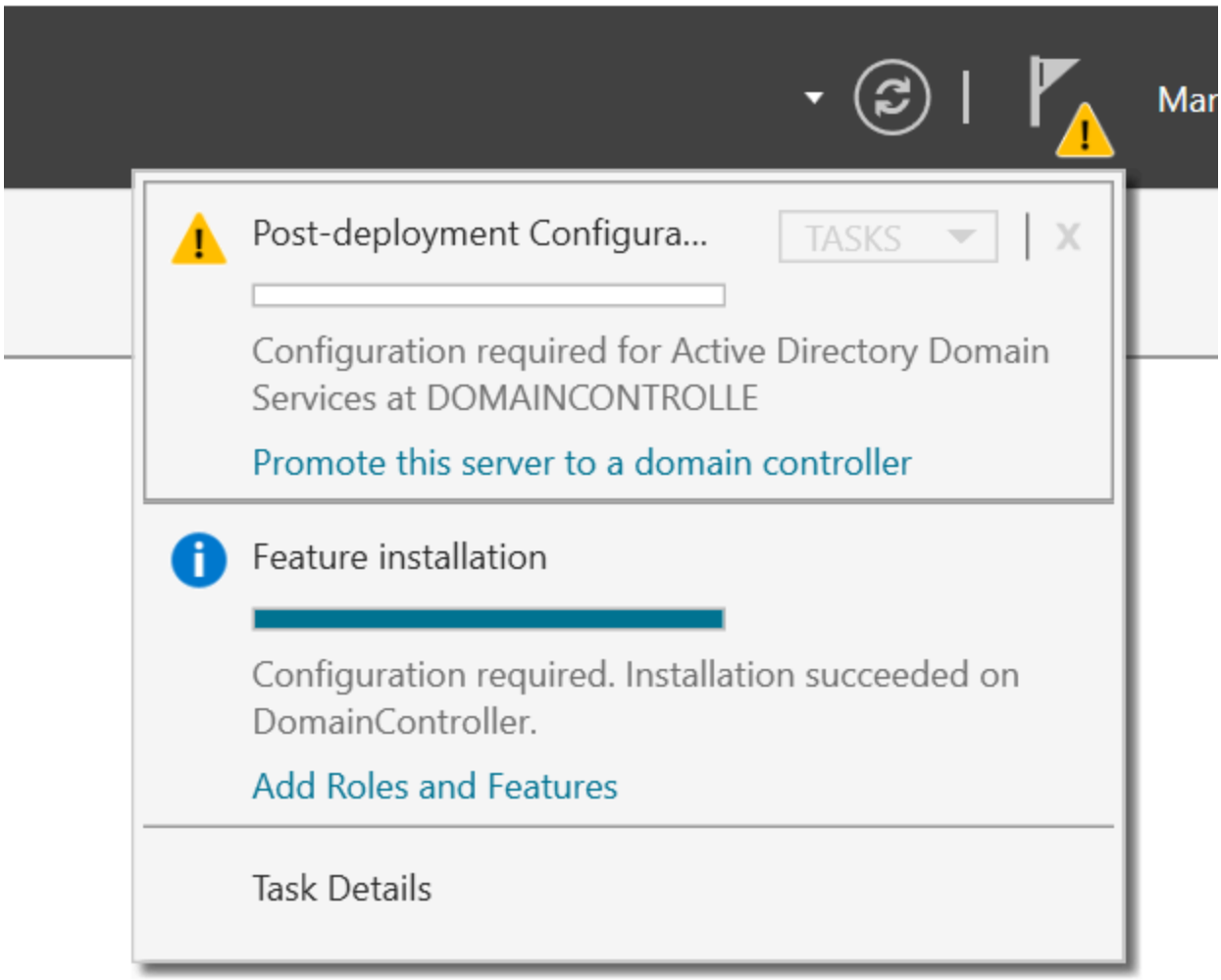
Click “Next” until you get to the following screen, where you can check the “Active Directory Domain Services” and then click “Add Features“:



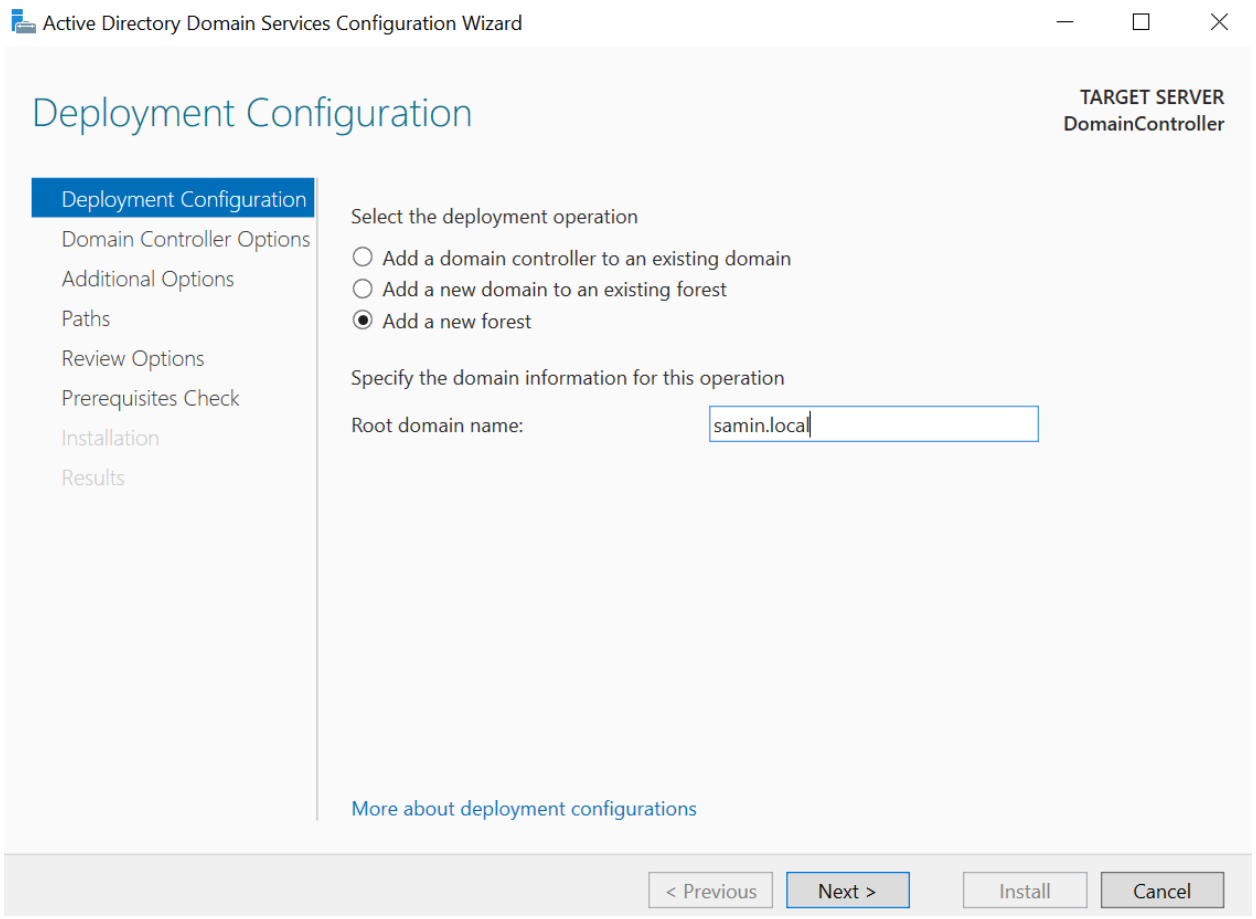
Continue clicking “Next” until you can click the “Install” button:



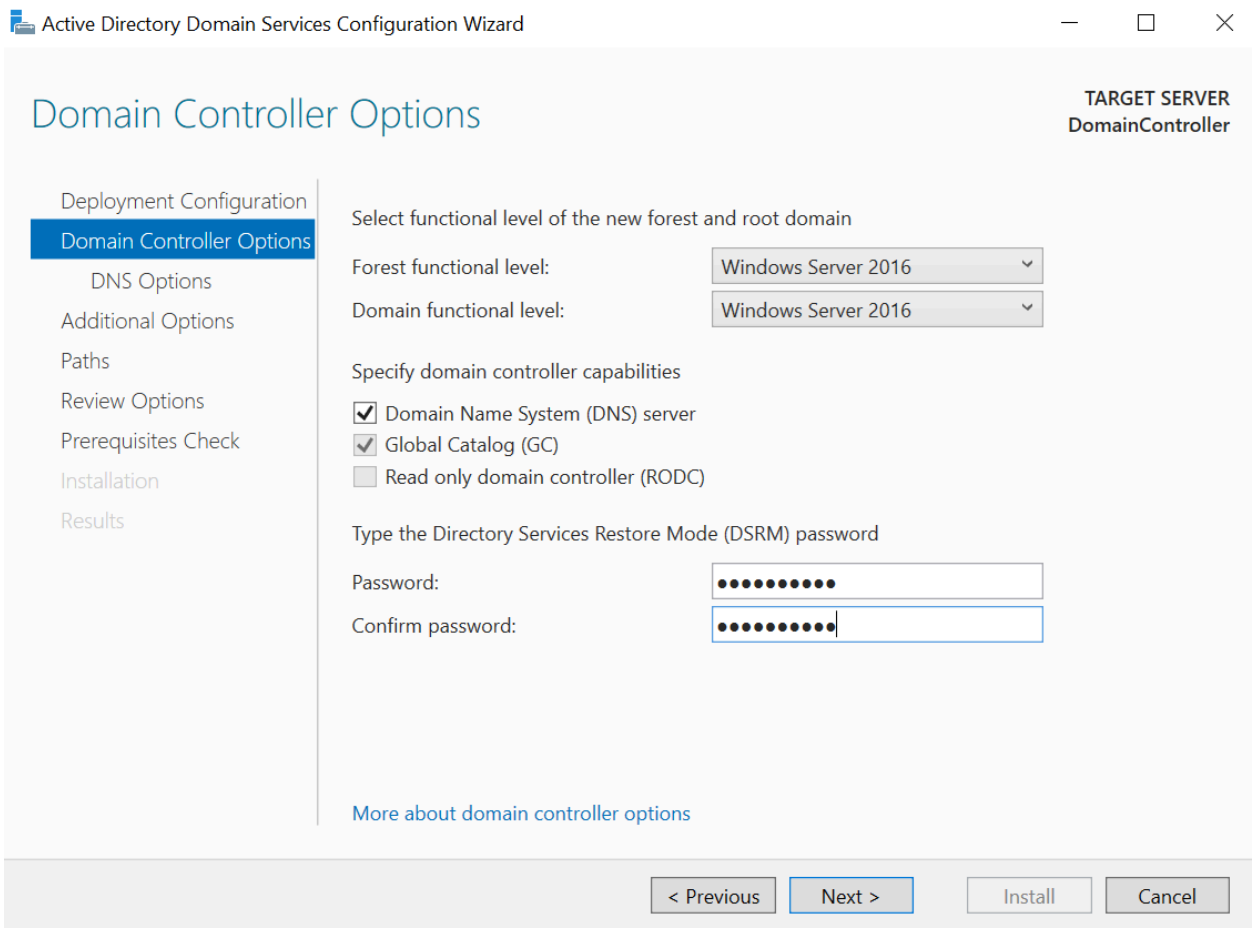
Once it appears, click the flag icon with the yellow marker and click “Promote this server to a domain controller“



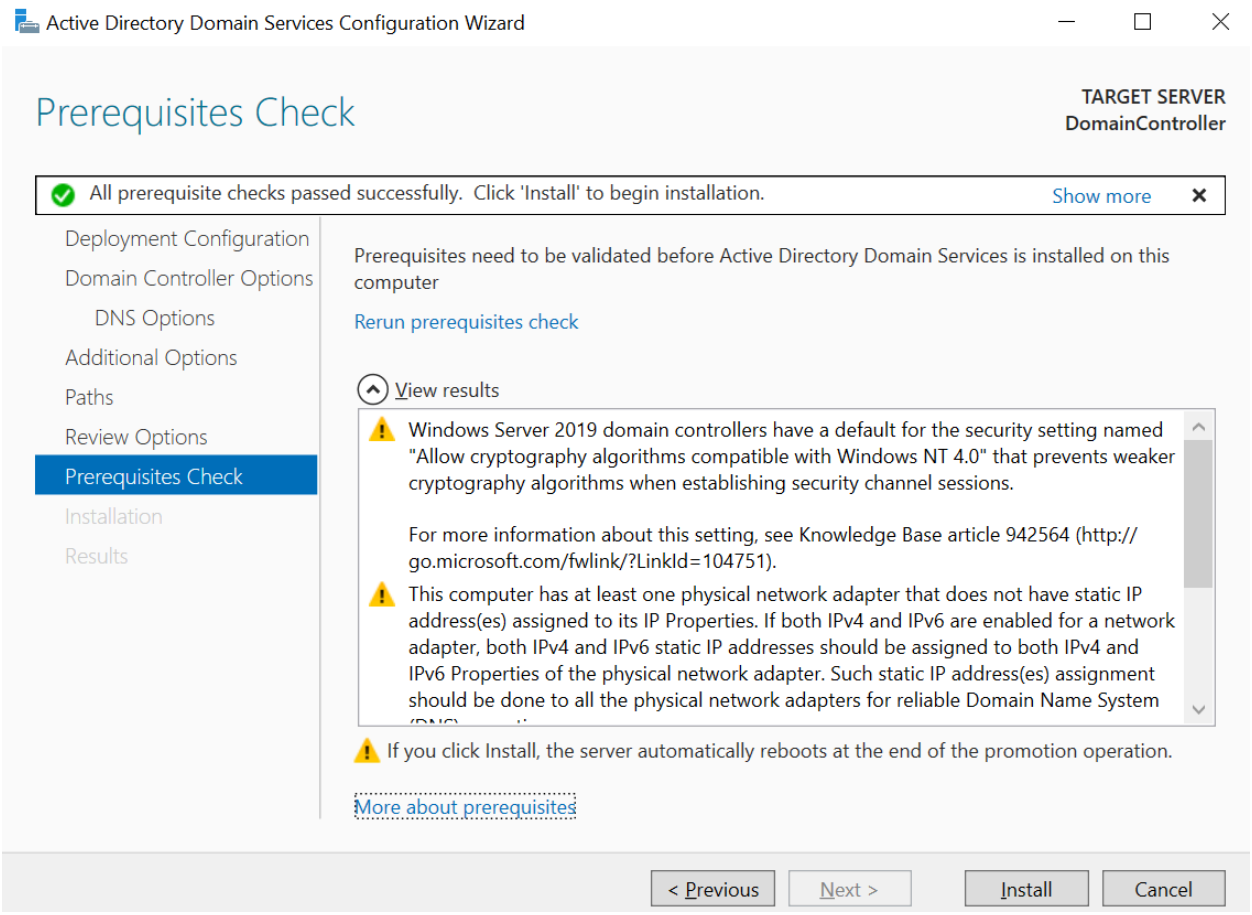
Click “ Add a new forest” and specify a domain name before clicking “Next”:



Set a password:



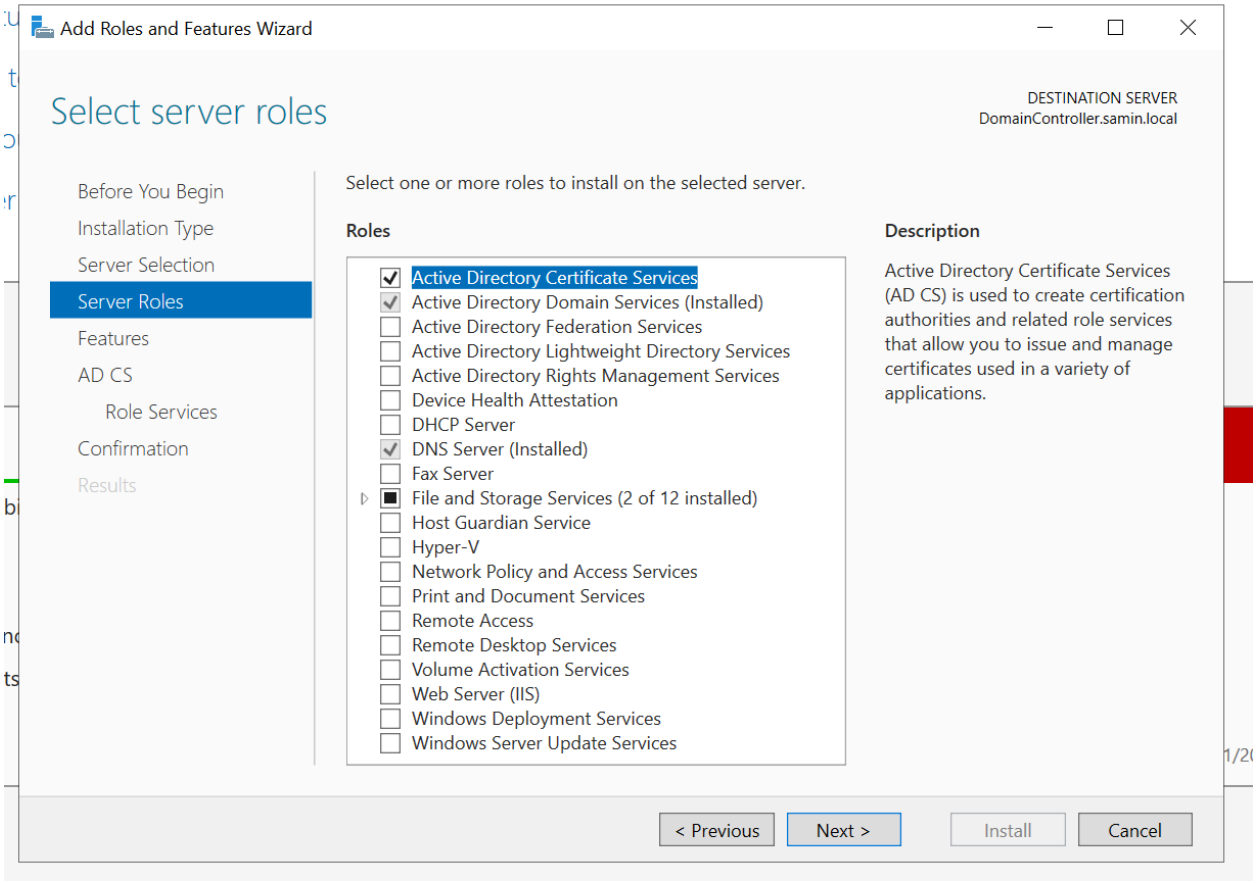
Click “Next” until you can click “Install”:



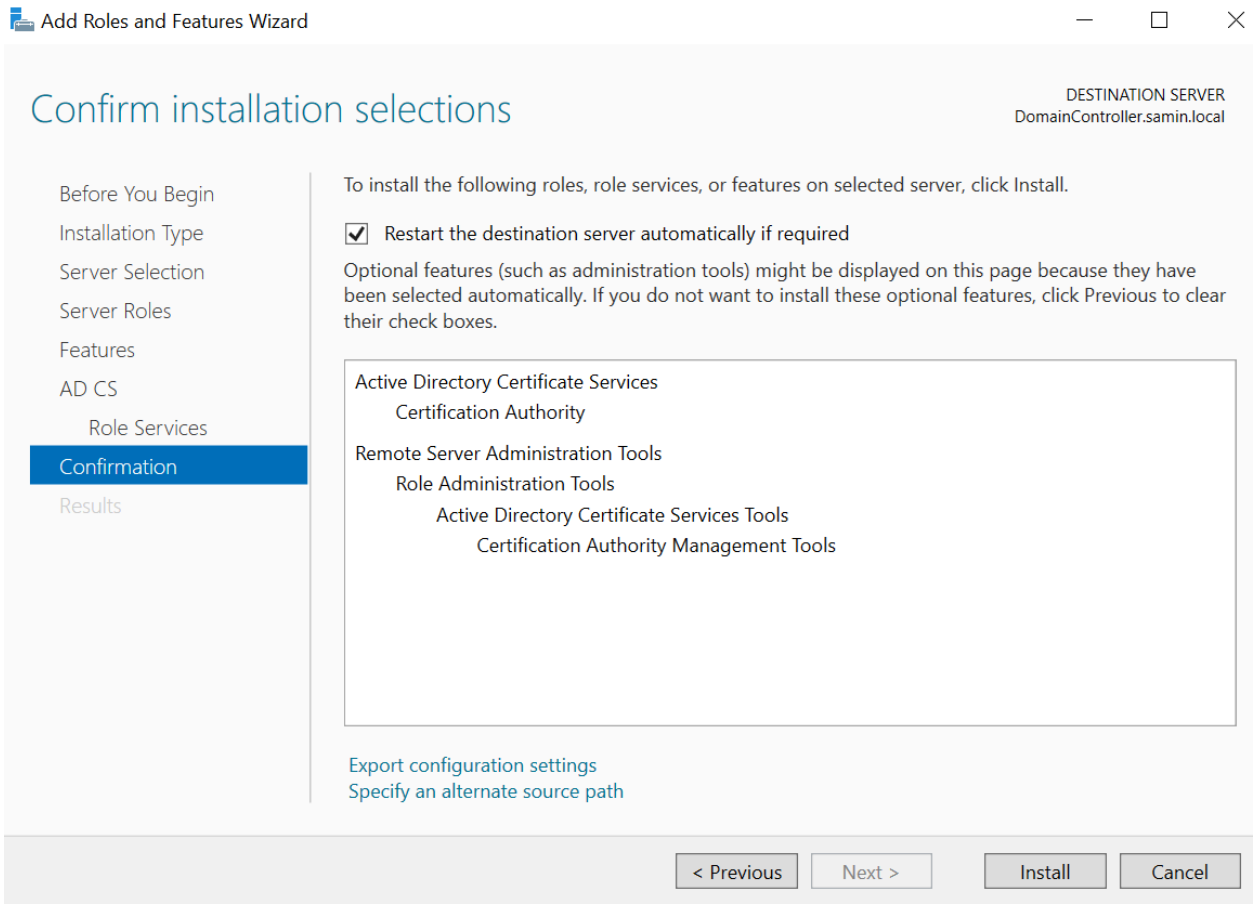
Click “Install”, then wait for the machine to reboot and log back in.

Once logged in, click “Add Roles and Features” under “Manage”

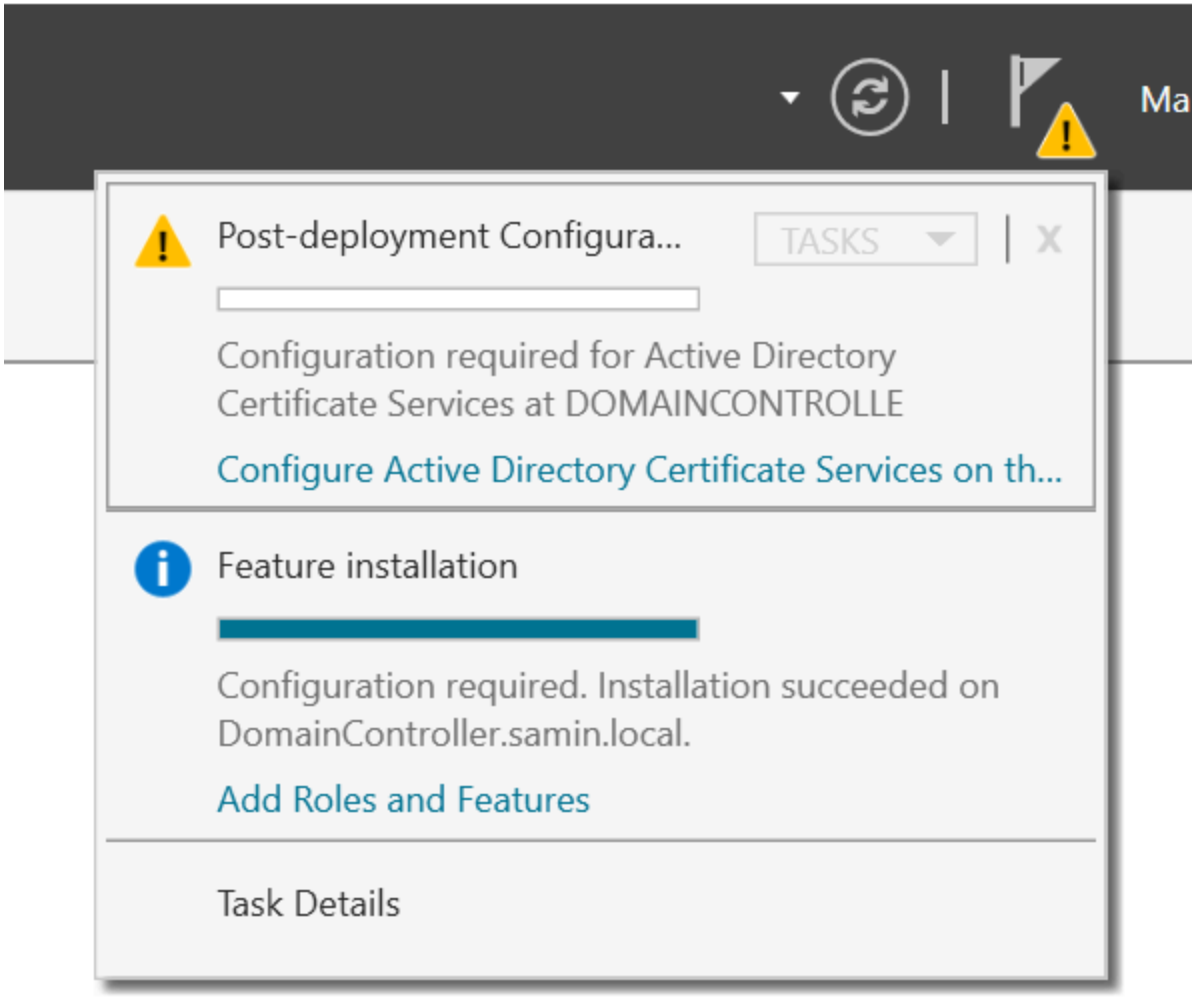
Click “Next” until you get to the screen below. Here, check off “Active Directory Certificate Services” and click “Add Features” before clicking “Next”:



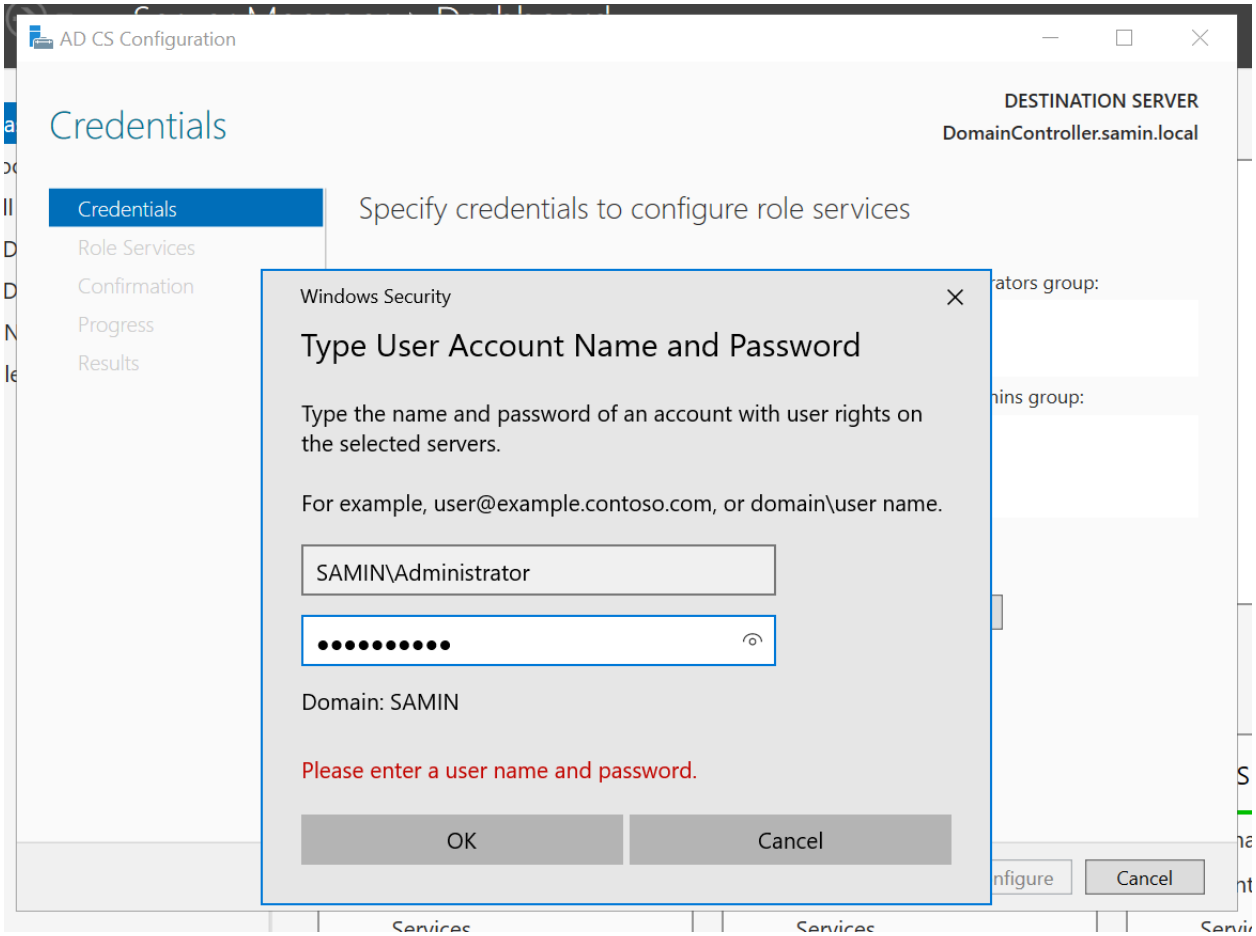
Click “Next” until you reach the screen with the install button. Here, check the box that says “Restart the destination server automatically if required” and click “Yes” before pressing the “Install” button:

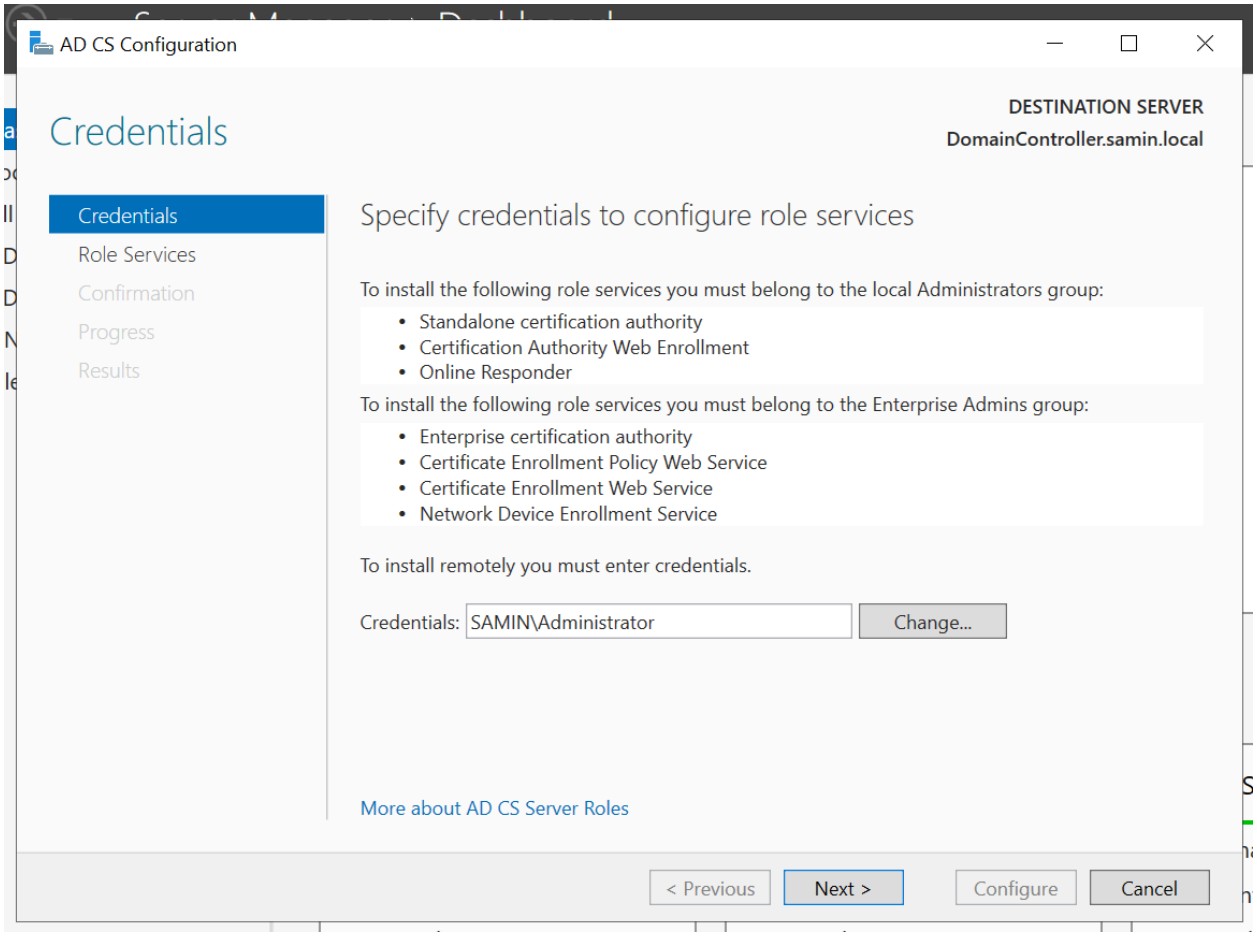


Click on the flag with the yellow triangle and click “Configure Active Directory Certificate Services on the destination server“:

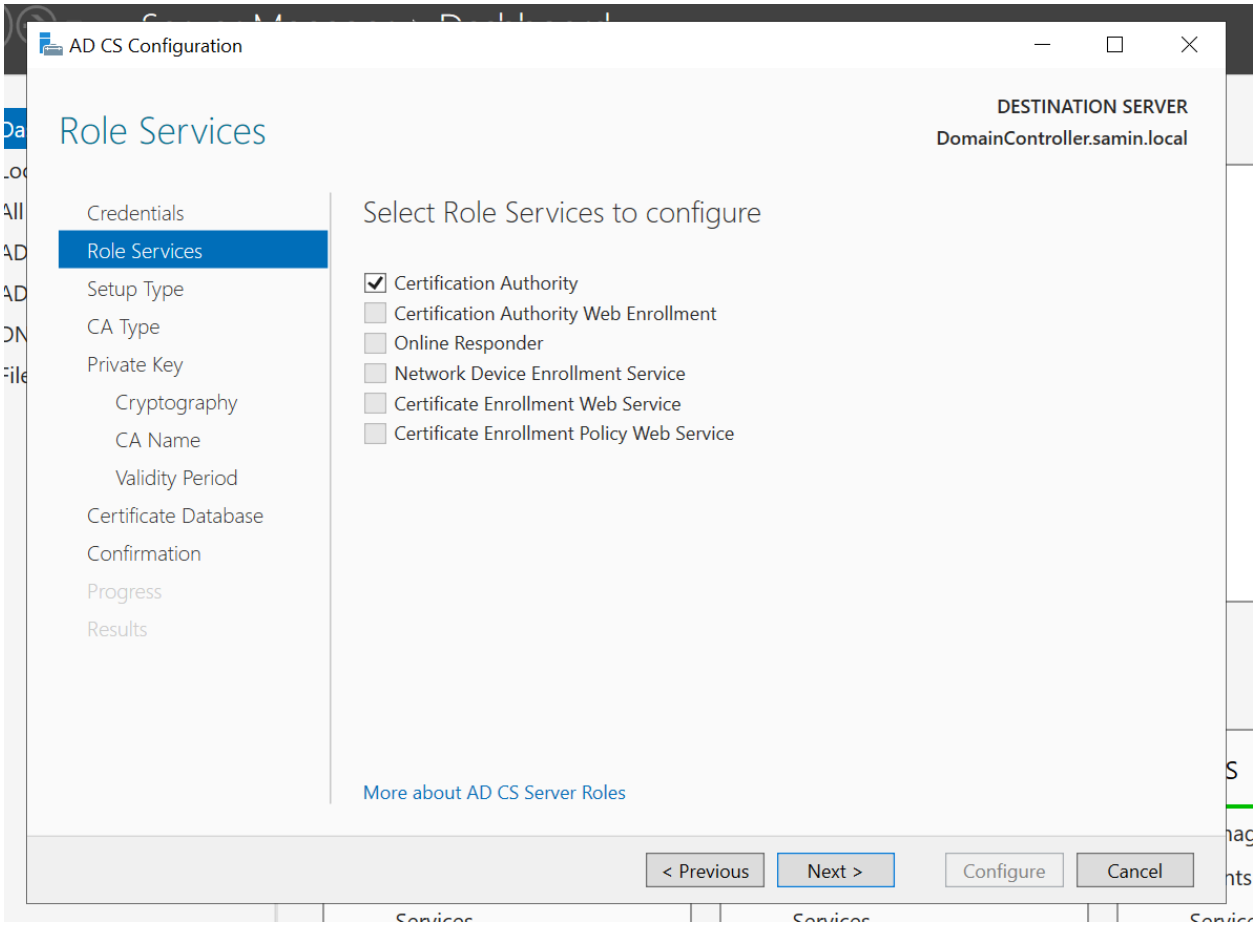


Enter you credentials before clicking next:

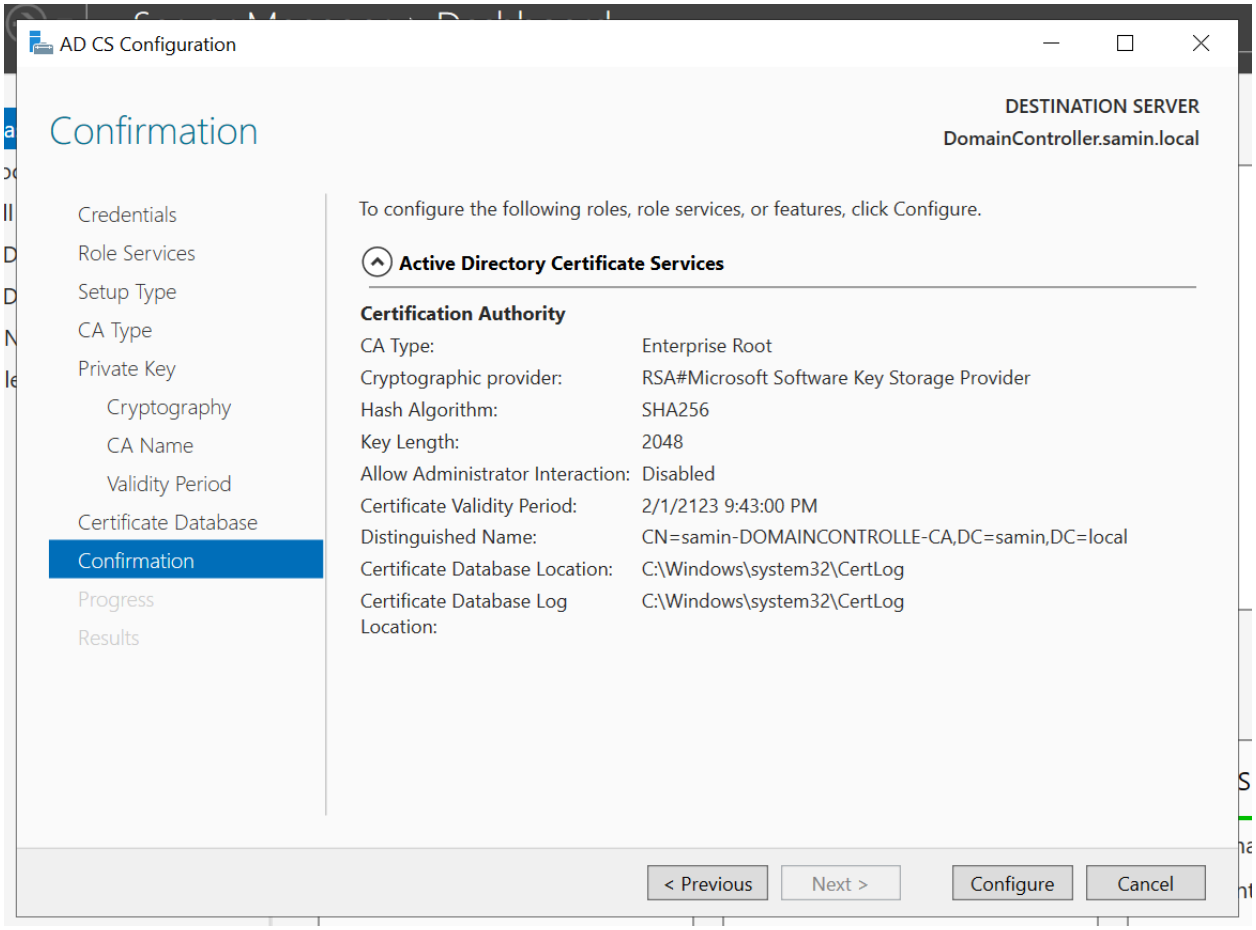

AD CS Configuration
Credentials
DESTINATION SERVER
DomainController.samin.local
Credentials
Role Services
Confirmation
Progress
Results
Specify credentials to configure role services
Windows Security
Type User Account Name and Password
Type the name and password of an account with user rights on the selected servers.
For example, user@example.contoso.com, or domain\user name.
SAMIN\Administrator
Domain: SAMIN
Please enter a user name and password.
OK
Cancel
Cancel



Check “Certification Authority”:



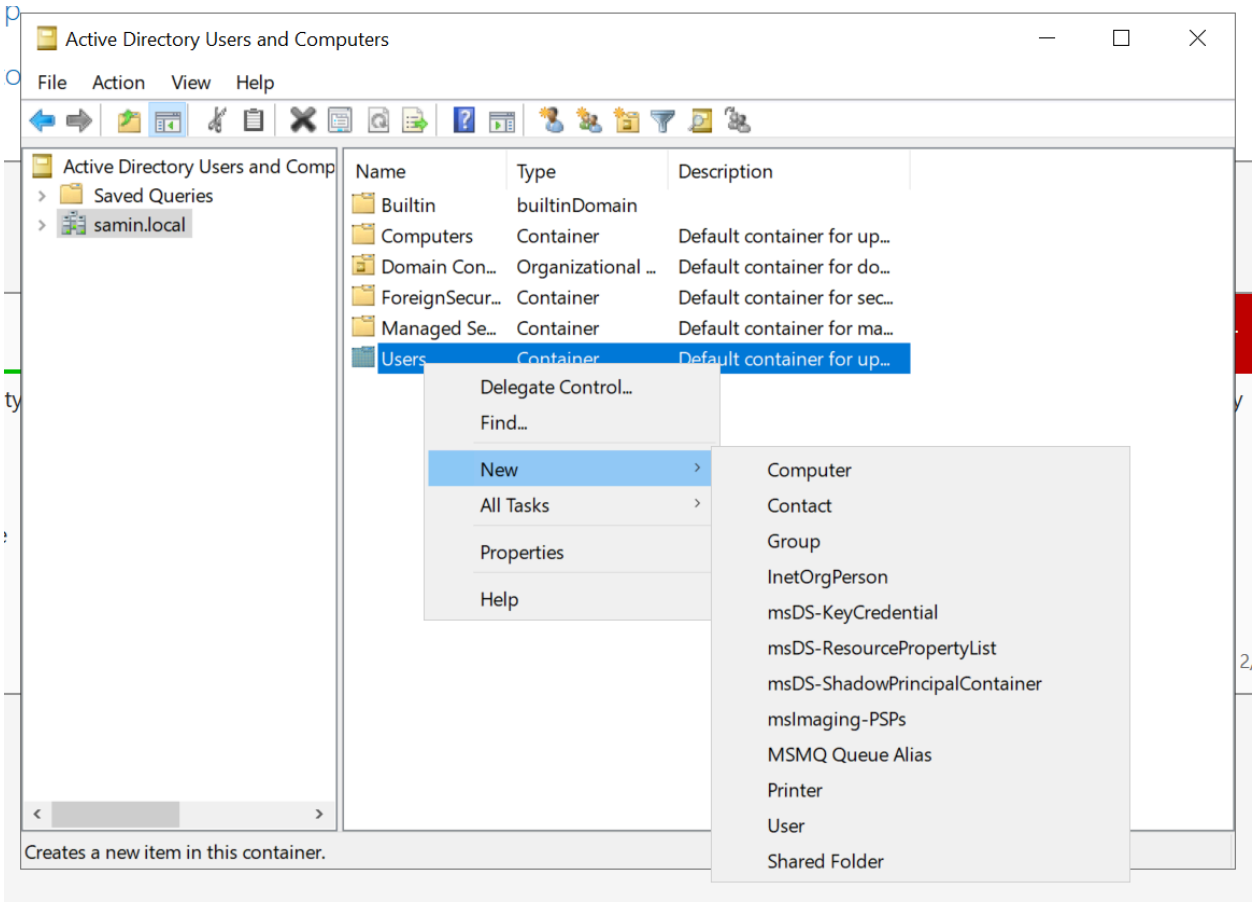
Hit “Next” until you are able to click “Configure”:



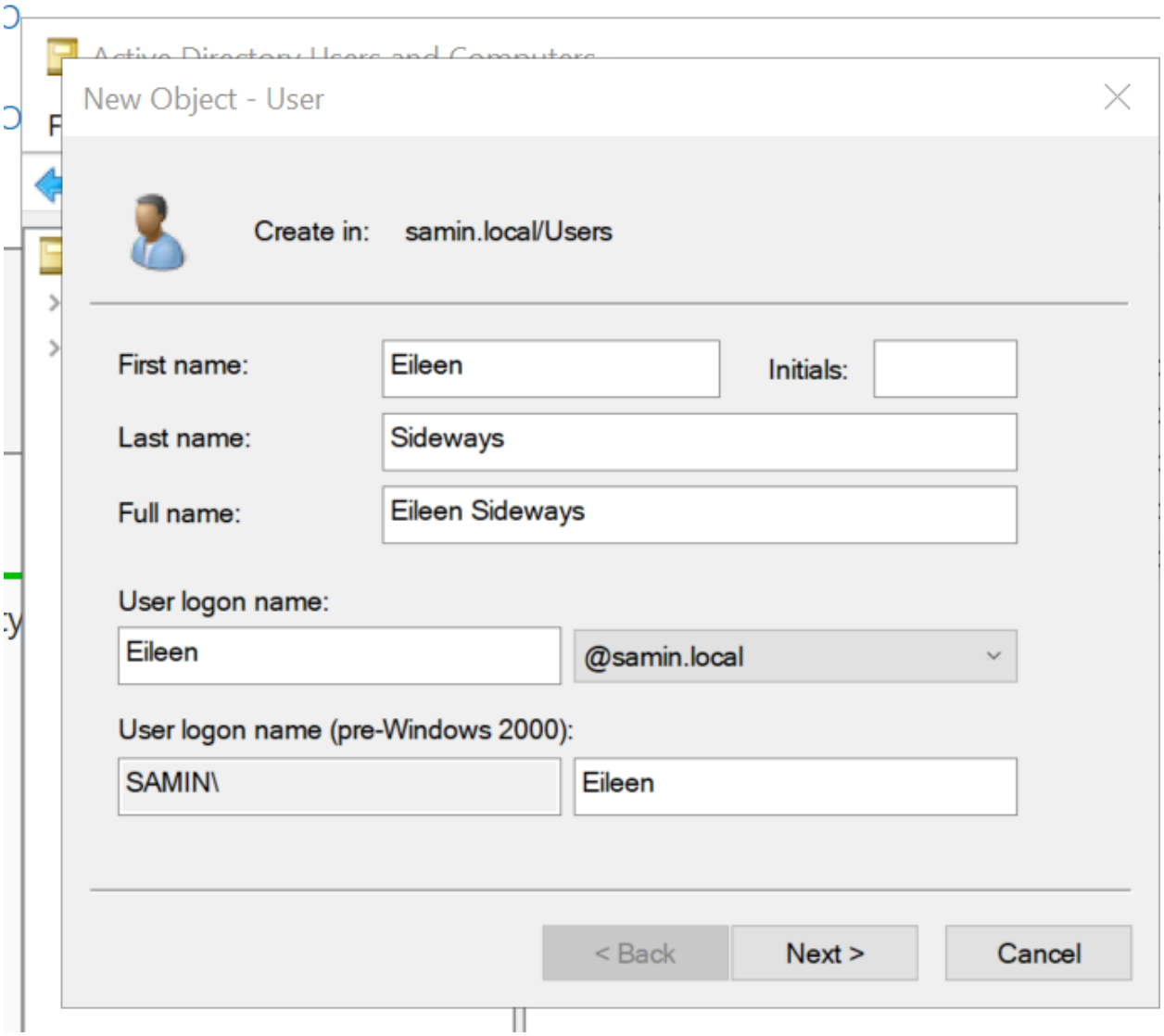
Once done, manually restart the machine if it did not do so automatically.

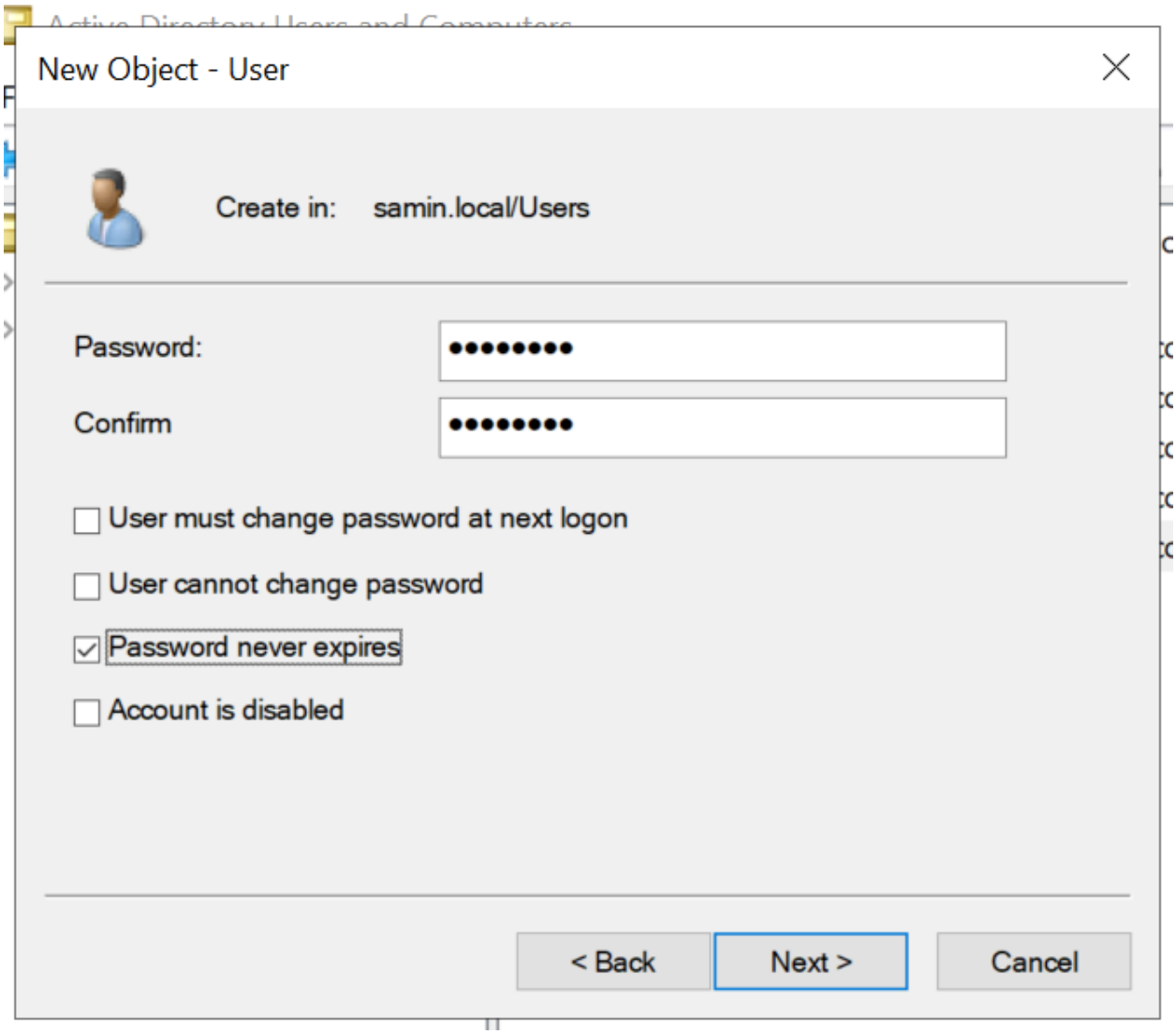
To add users, click “Active Directory Users and Computers” under “Tools”

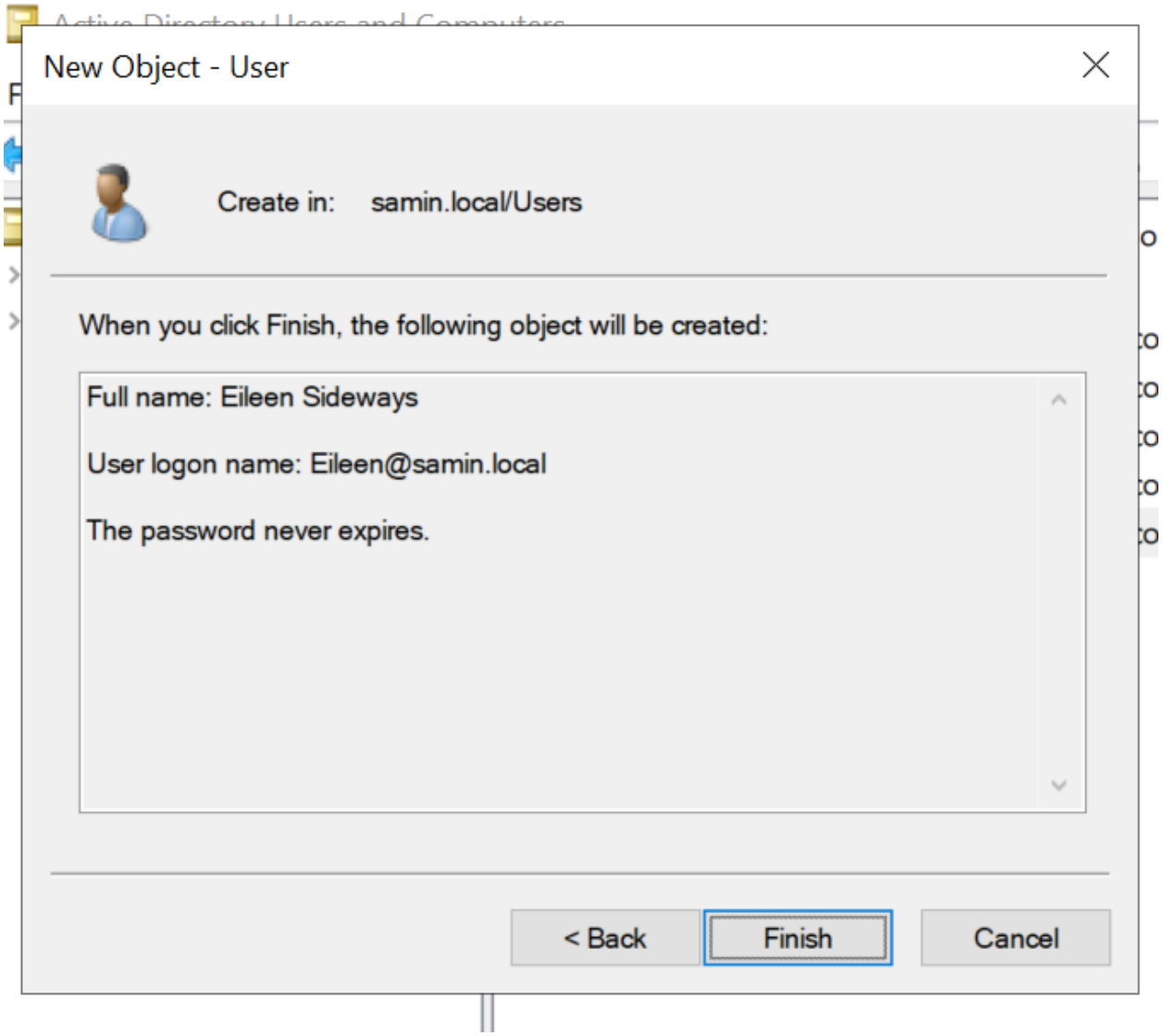
Click the local domain and right click on the “Users” file and click “User” under “New”:



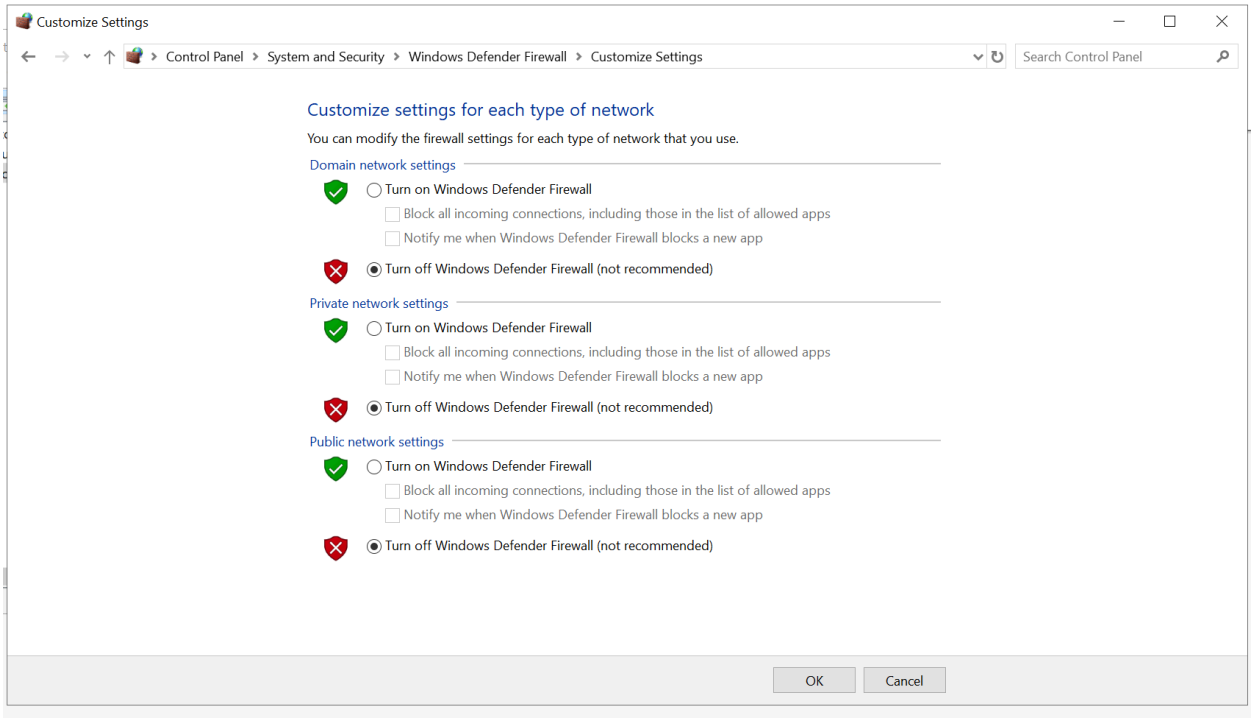
Create the user, ensuring to uncheck the changing password option and check the “Password never expires” option:


New Object - User
Create in: samin.local/Users
First name:
Eileen
Initials:
Last name:
Sideways
Full name:
Eileen Sideways
User logon name:
Eileen
@samin.local
User logon name (pre-Windows 2000):
SAMIN\
Eileen
< Back
Next >
Cancel

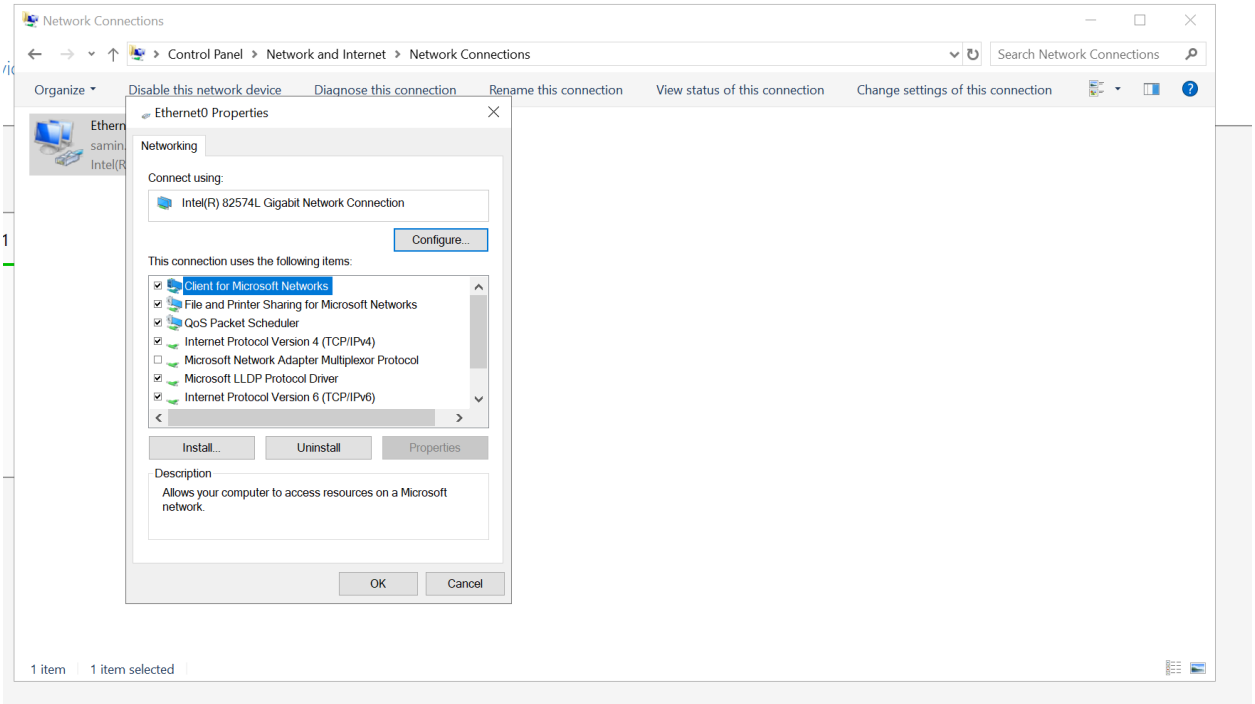

New Object - User
Create in: samin.local/Users
Password:
Confirm
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
< Back
Next >
Cancel



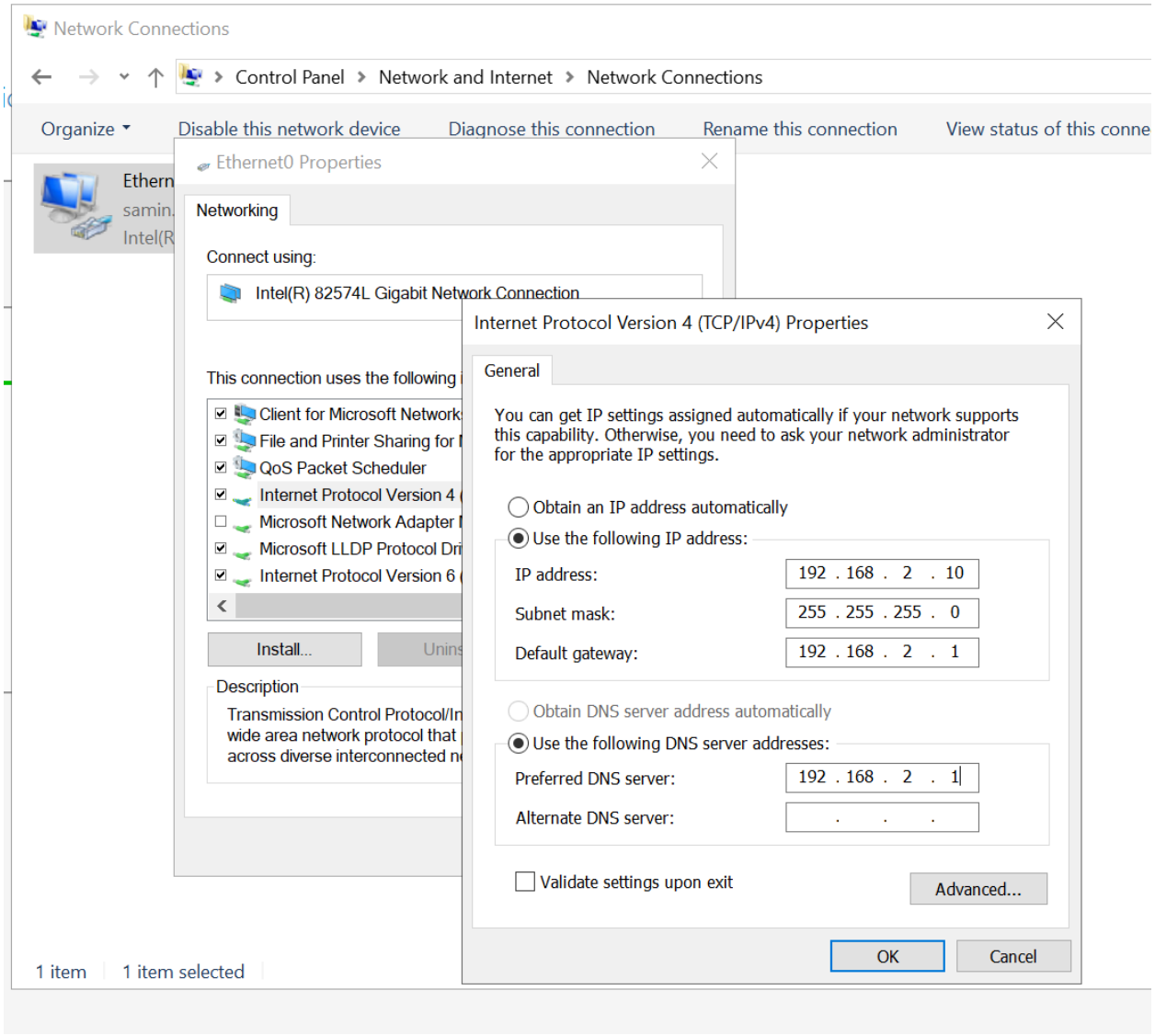
After clicking finish and adding the user, search up Windows Defender Firewall on Windows and turn them all off:



Now, open up Control Panel and navigate to “Network Connections” under “Network and Internet” before right-clicking on the Ethernet connection and selecting “Properties”:



Click on the IPv4 line and enter the following configurations:



Configuring Windows 10 Desktop

Log into the Kali machine and navigate to the pfSense website

Under the victim network in Services - DHCP Server, add “192.168.2.10” to the DNS servers and the domain name created for the windows server to the “Domain Name” field:

Services / DHCP Server / VICTIMNETWORK

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend.

KALI | VICTIMNETWORK | SECONION | SPLUNK

General DHCP Options

DHCP Backend ISC DHCP

Enable ☐ Enable DHCP server on VICTIMNETWORK interface

BOOTP ☐ Ignore BOOTP queries

Deny Unknown Clients Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on ***any*** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

Ignore Denied Clients ☐ Ignore denied clients rather than reject

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore Client Identifiers ☐ Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet 192.168.2.0/24

Subnet Range 192.168.2.1 - 192.168.2.254

Address Pool Range From To

The specified range for this pool must not be within the range configured on any other address pool for this interface.

Additional Pools + Add Address Pool

If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.

Server Options

WINS Servers WINS Server 1

WINS Server 2

DNS Servers 192.168.2.10

DNS Server 2

DNS Server 3

DNS Server 4

OMAPI

OMAPI Port OMAPI Port

Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable.Only the first OMAPI configuration is used.

OMAPI Key OMAPI Key

Enter a key matching the selected algorithm to secure connections to the OMAPI endpoint.

☐ Generate New Key

Generate a new key based on the selected algorithm.

Key Algorithm HMAC-SHA256 (current bind9 default)

Set the algorithm that OMAPI key will use.

Other DHCP Options

Gateway 192.168.2.1

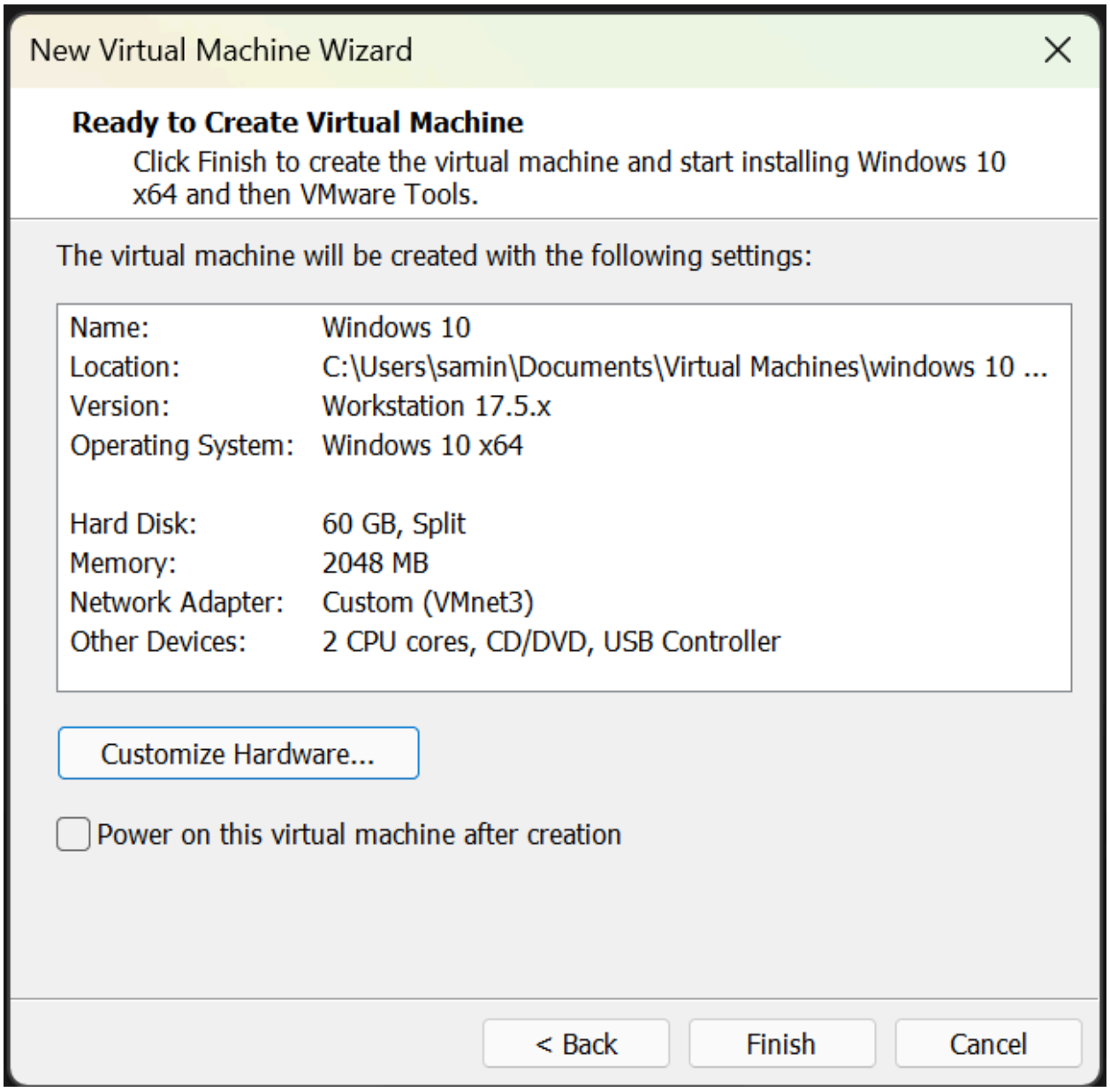
The default is to use the IP address of this firewall interface as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Enter "none" for no gateway assignment.

Domain Name samin.local

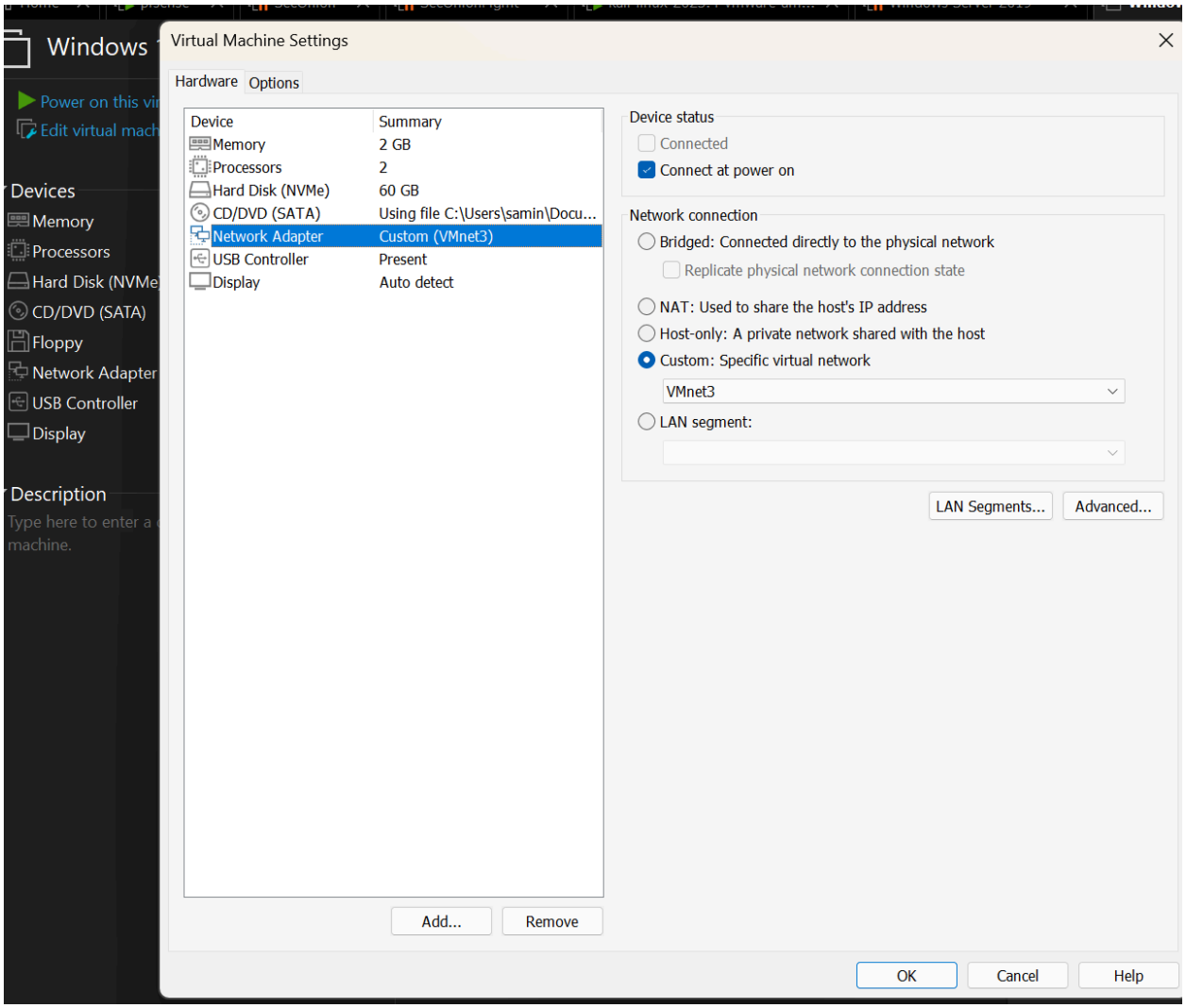
Save and apply the changes

Now, create a new virtual machine using the Windows 10 ISO file downloaded from their website

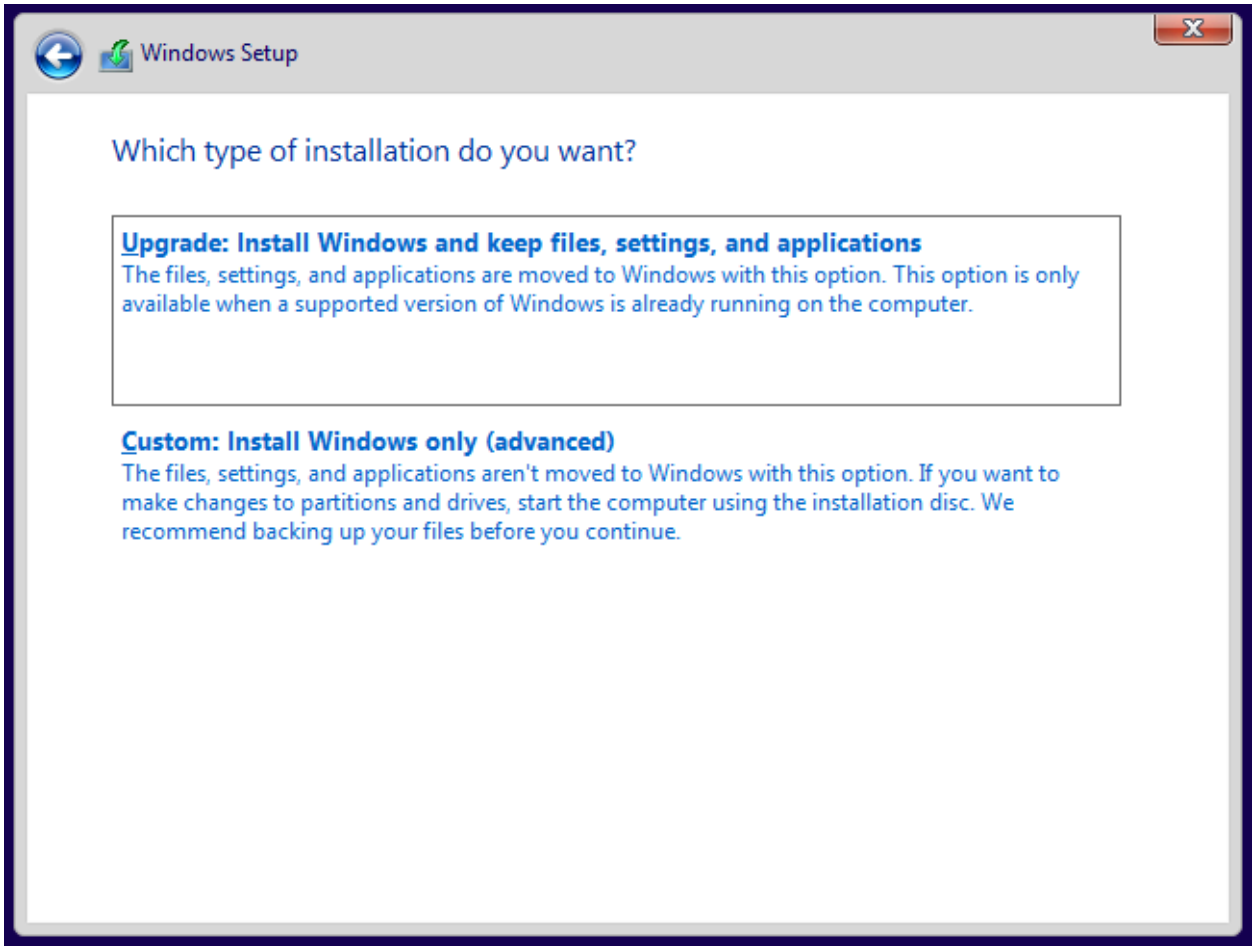
Using this ISO file, configure a new virtual machine, similar to the Windows Server machine configured earlier. Ensure that the Network Adapter is changed to Vmnet3 and “Power on this virtual machine after creation” is unchecked:



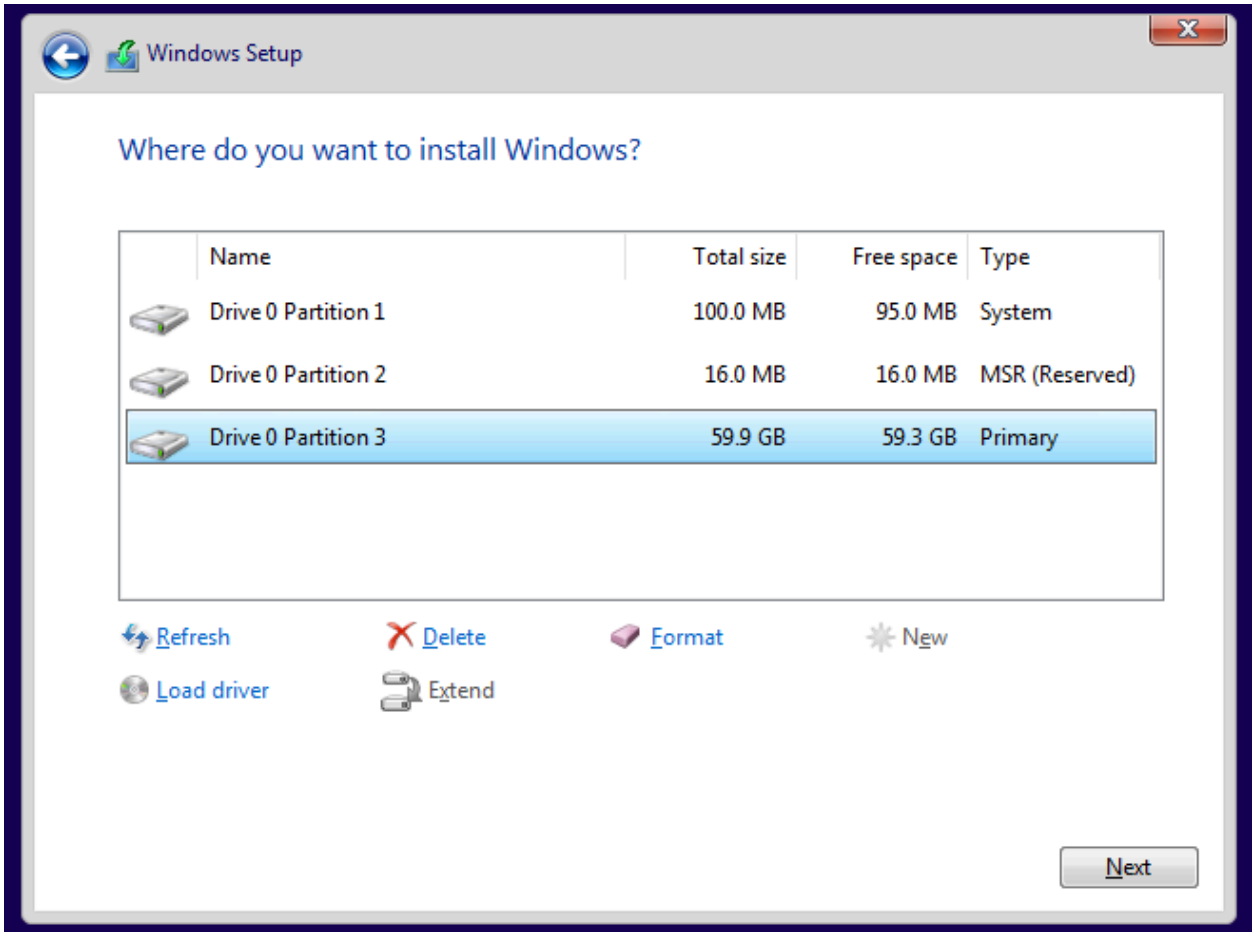
Click “Finish”, and before powering on the machine edit the settings again to remove the Floppy drive:



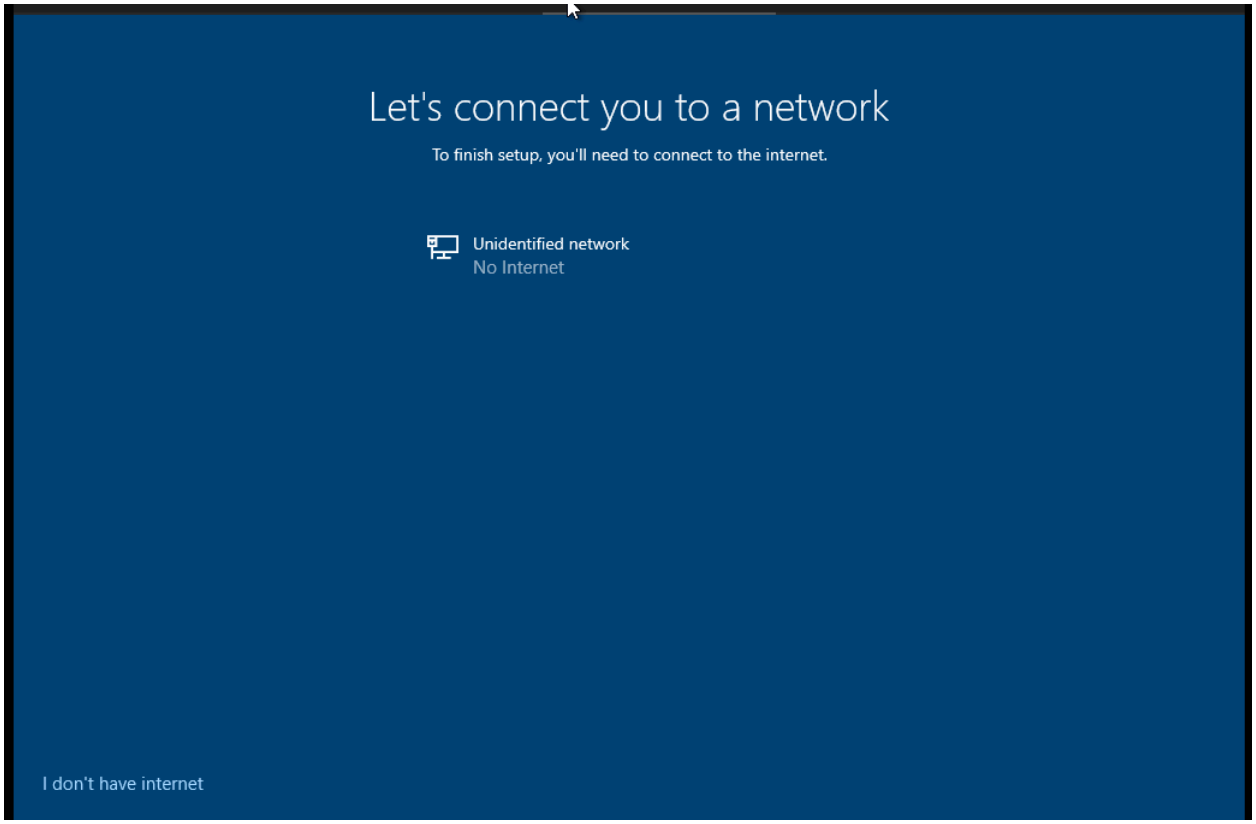
Configure as you wish once starting the machine up. Once you get to the following screen, select “Custom”:



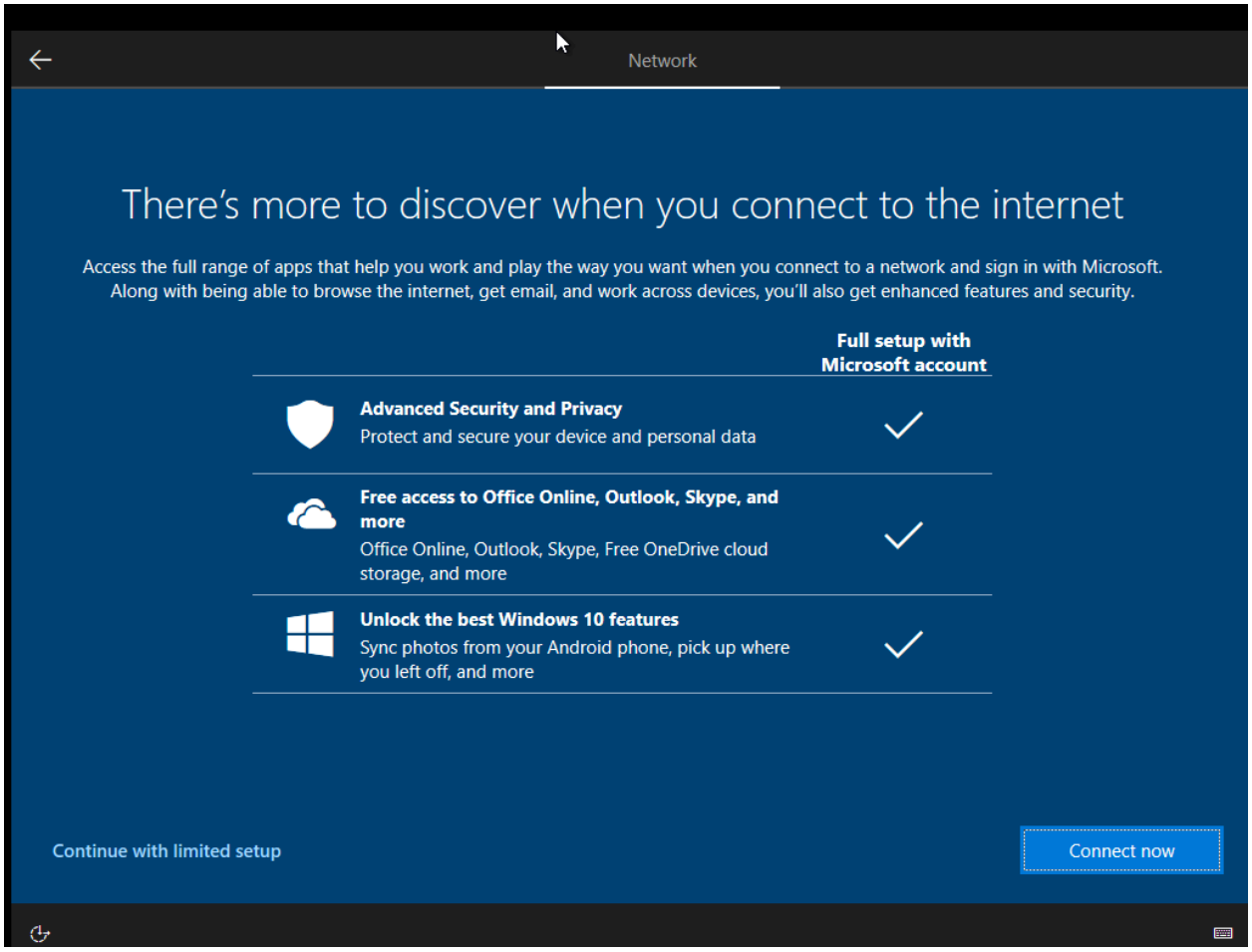
Click “Next” on the following screen:



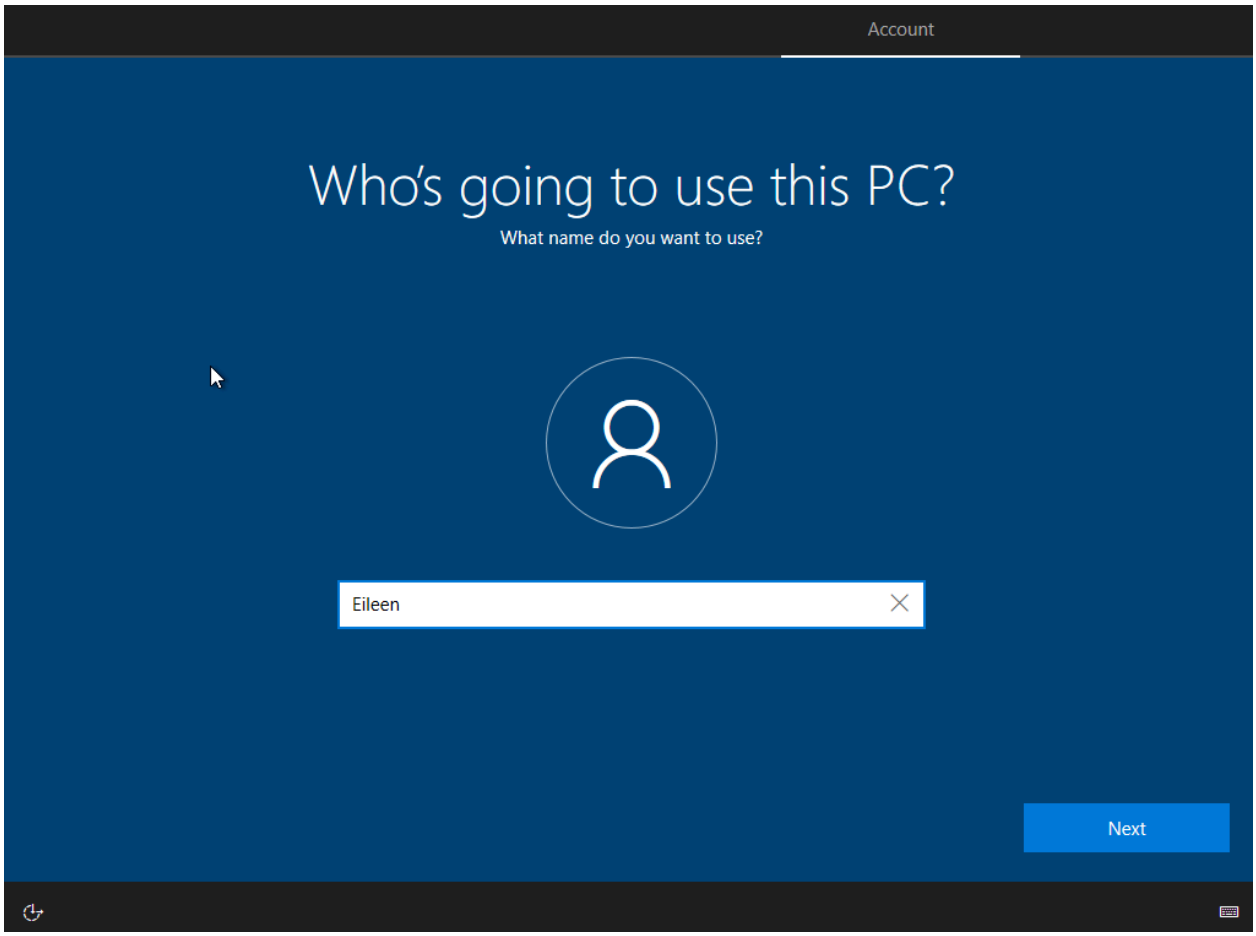
Continue configuring as you wish. Once you get to the following screen, select “I don’t have internet”:



Select “Continue with limited setup”:



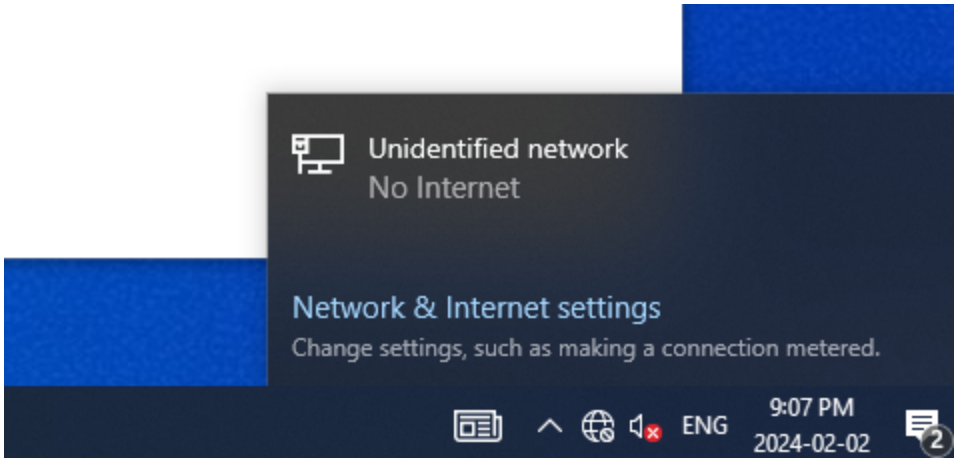
Set a name and password:



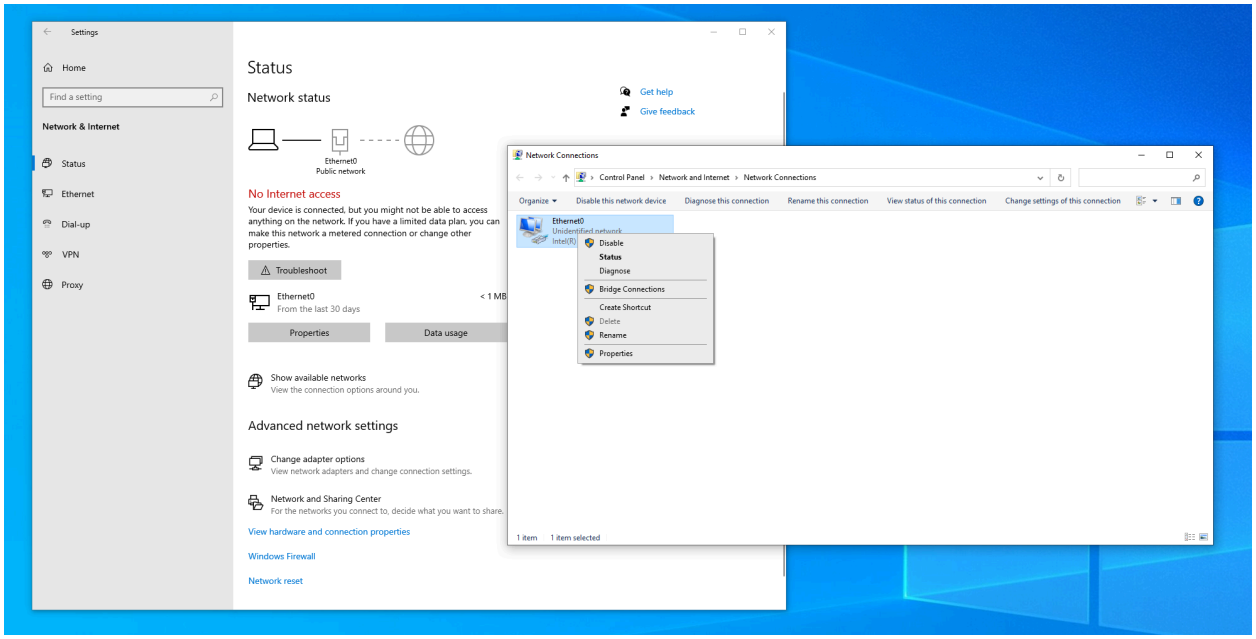
You can set the security questions to be whatever you want. For the rest of the configurations, select “No” whenever it is the option and don’t share the optional data.

Once you can log in, change the name of the machine so it reflects the ‘user’ that will be using it; you can do this by searching for “PC name” in the Windows search bar and changing it. You will need to restart the machine so that the change is applied.

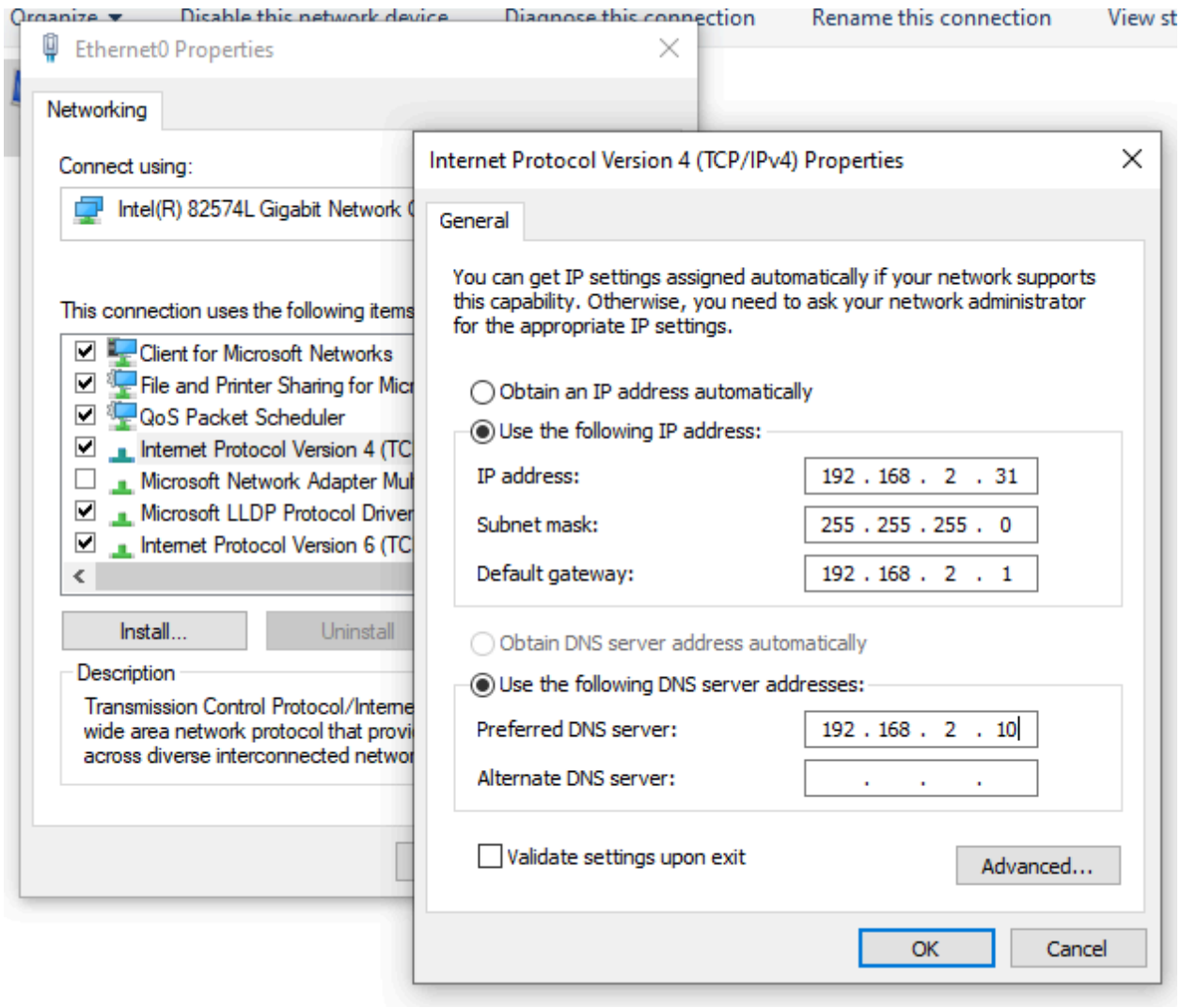
After logging in again, open up the network and internet settings from the bottom right hand corner:



Press “Change adapter options” and then right click the Ethernet network and click “Properties”:



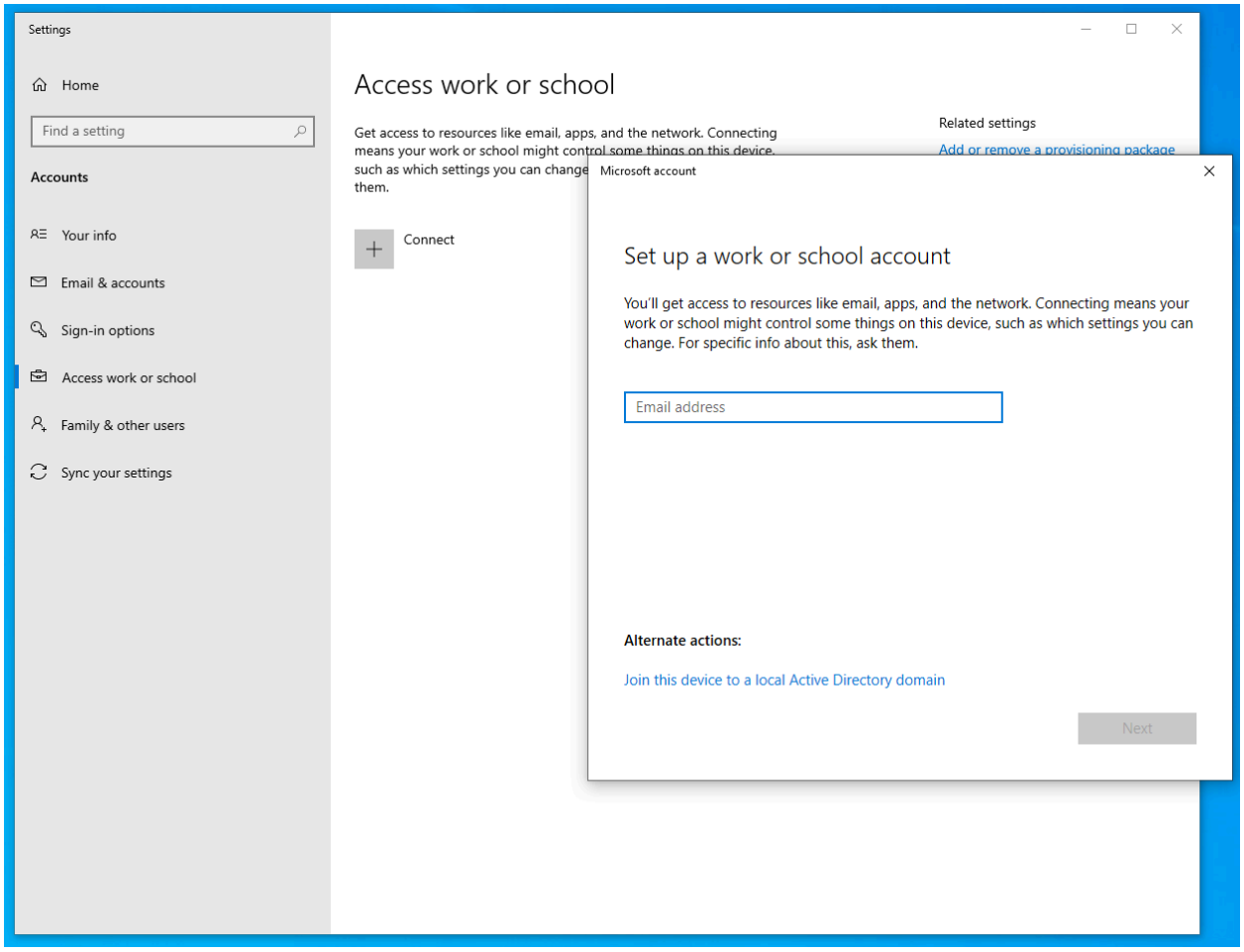
Click on the IPv4 line and configure as follows:



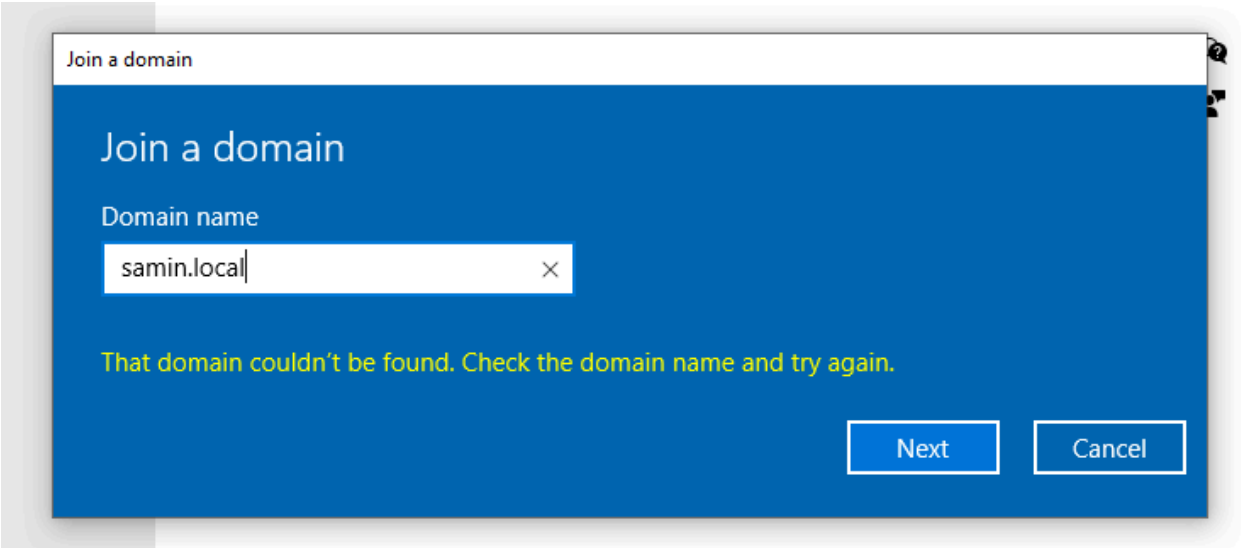
Click “OK” to exit out of the pop-ups and close everything else opened

Search for “Access work or school” in the Windows search box and click “Connect” once it’s opened up.

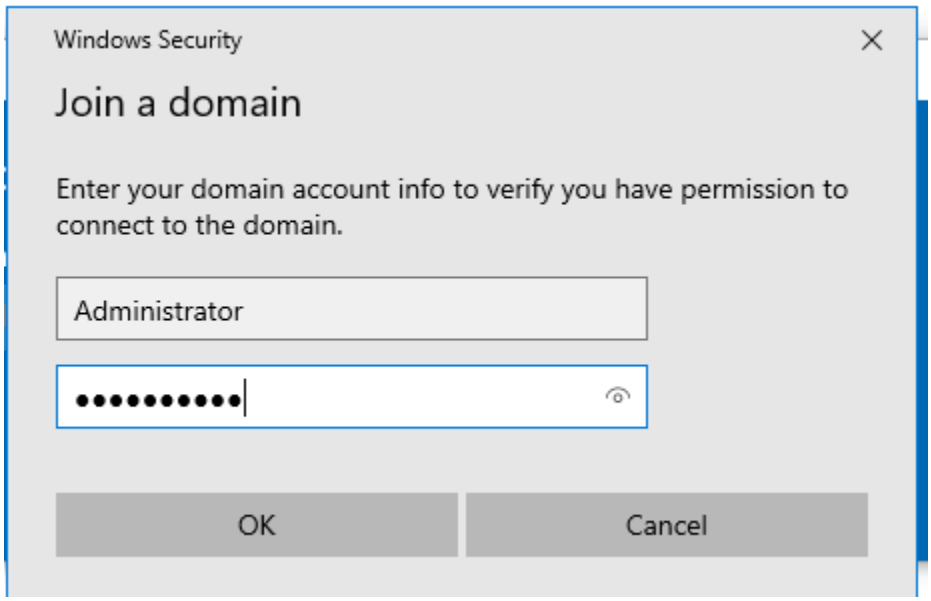
Select “Join this device to local Active Directory Domain”:



Enter the domain name; ensure that the pfSense machine and Windows Server machines are both running to avoid the error below:

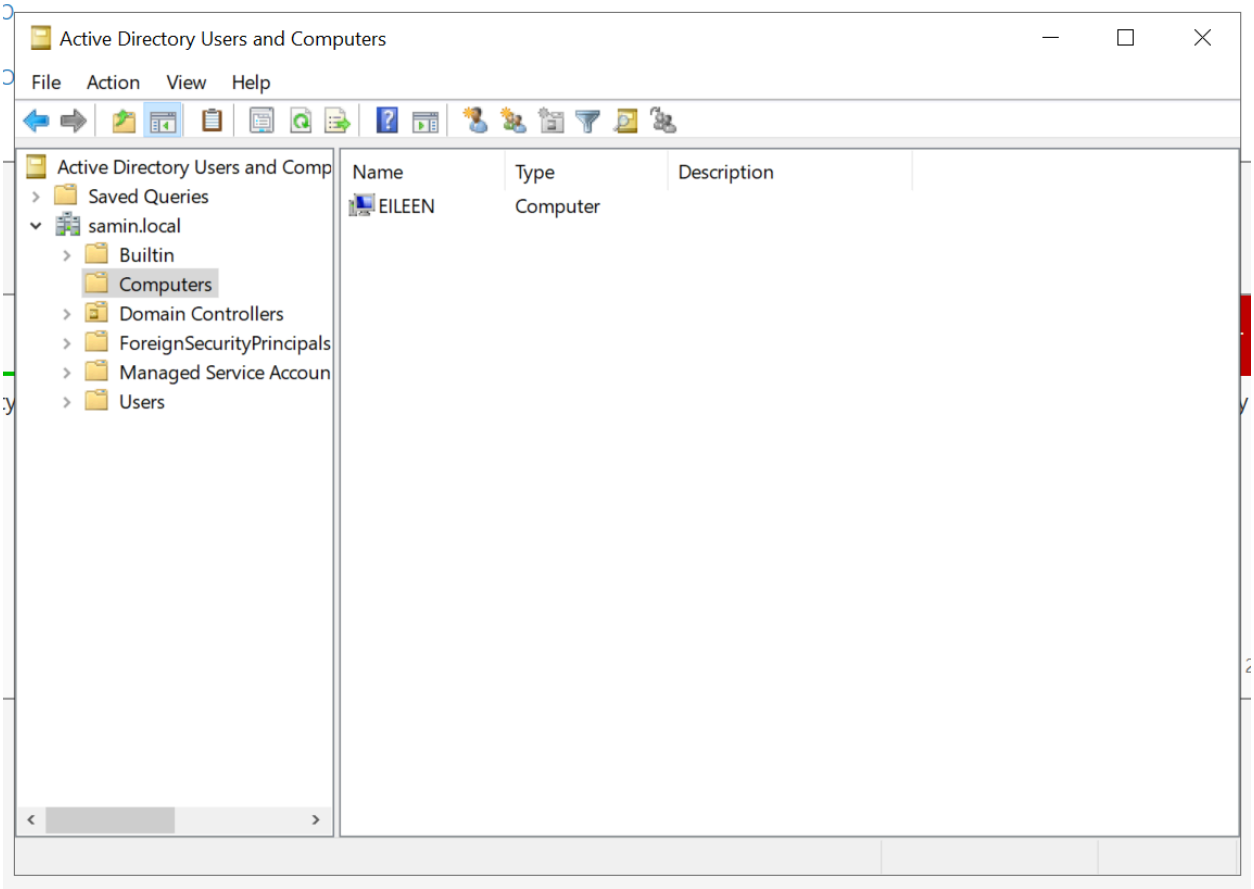


Enter in the username and password:



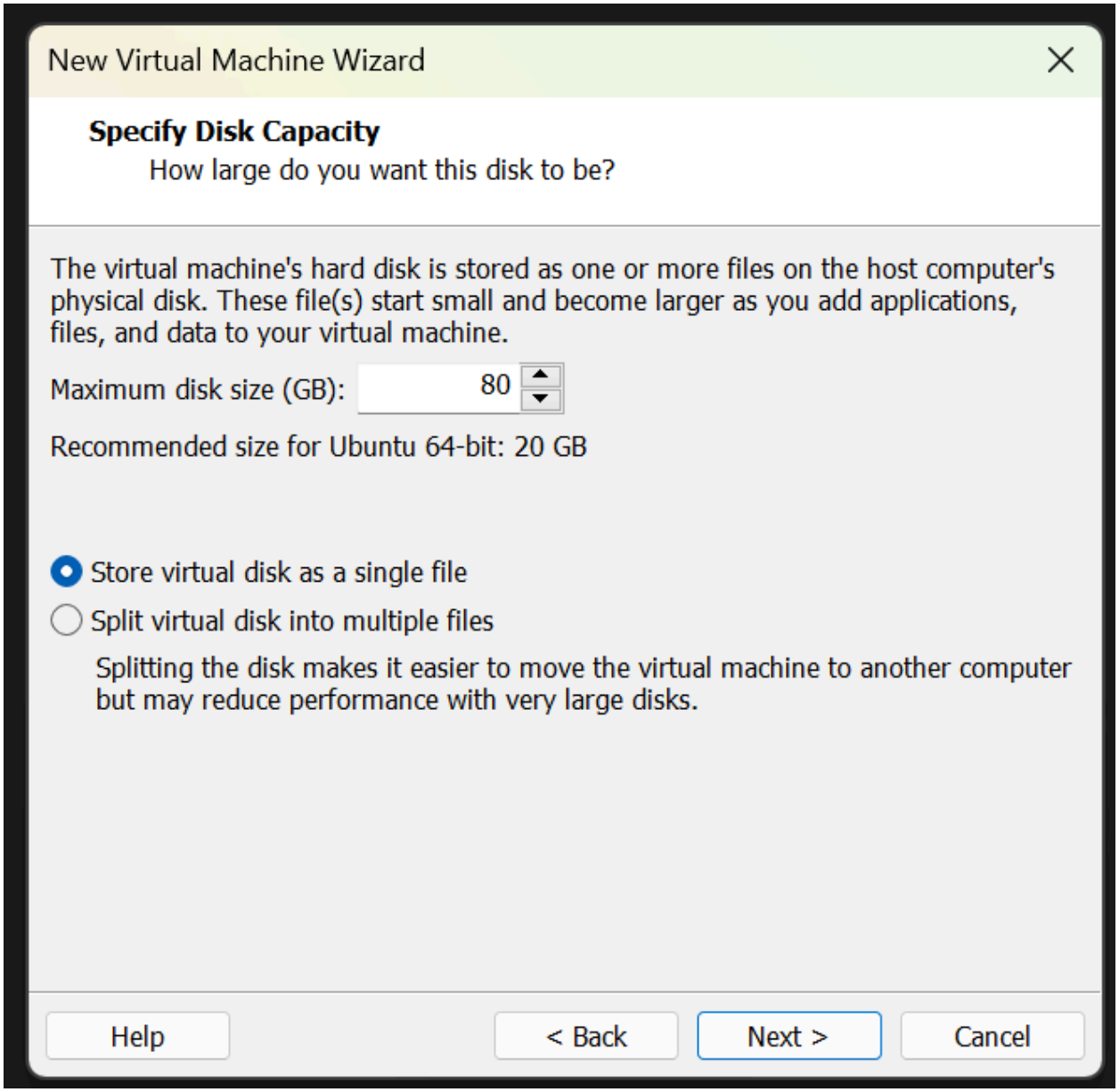
Click “Skip” and then restart the device when prompted

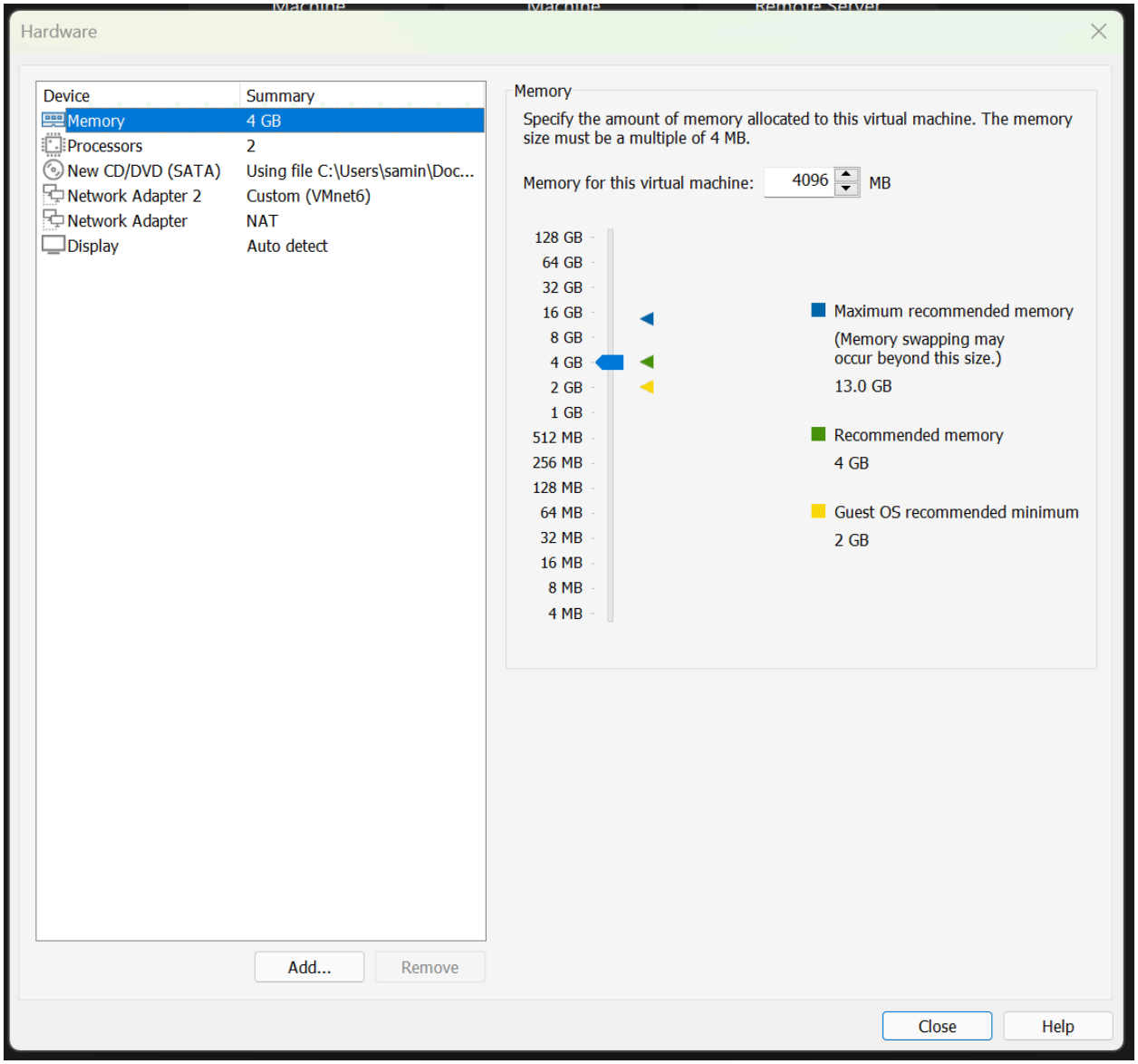
If you check on the Windows server machine, this computer will now appear in the Active Directory computers:



Configuring Splunk

Download the Ubuntu server ISO: https://ubuntu.com/download/server

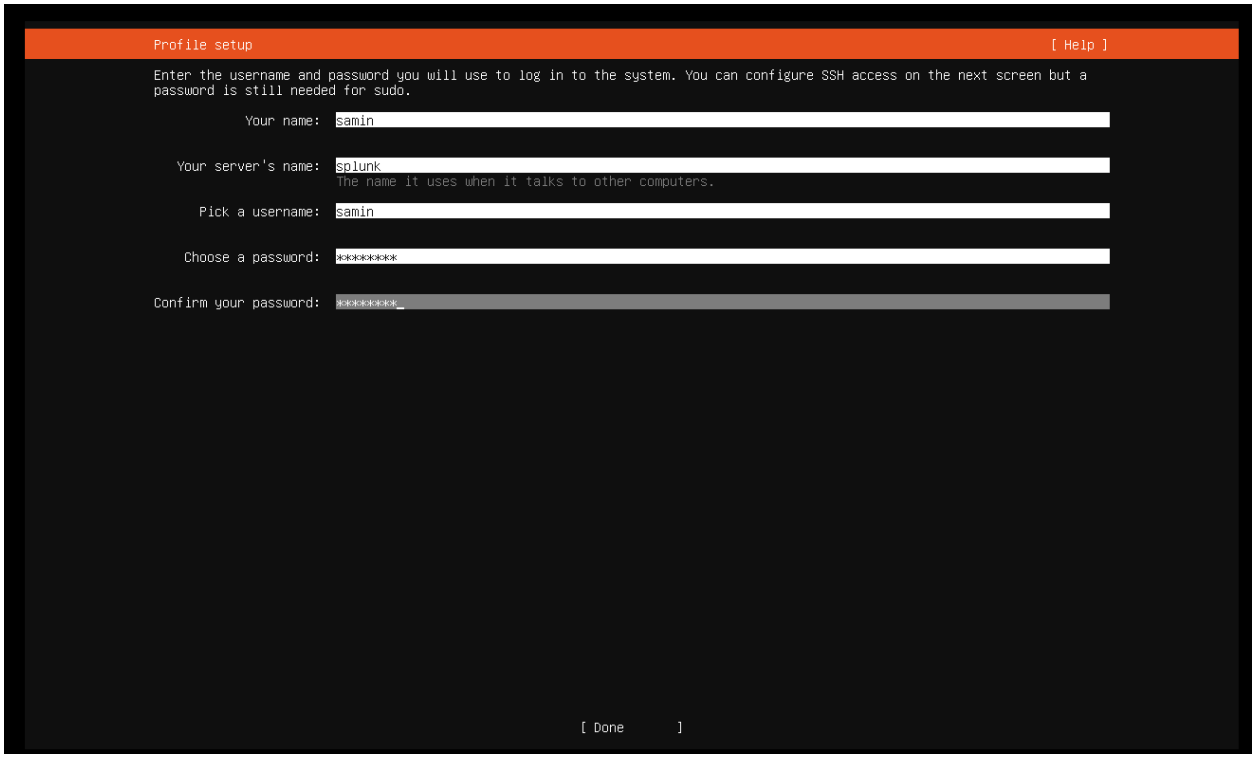

New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.
Maximum disk size (GB):
80
Recommended size for Ubuntu 64-bit: 20 GB
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel



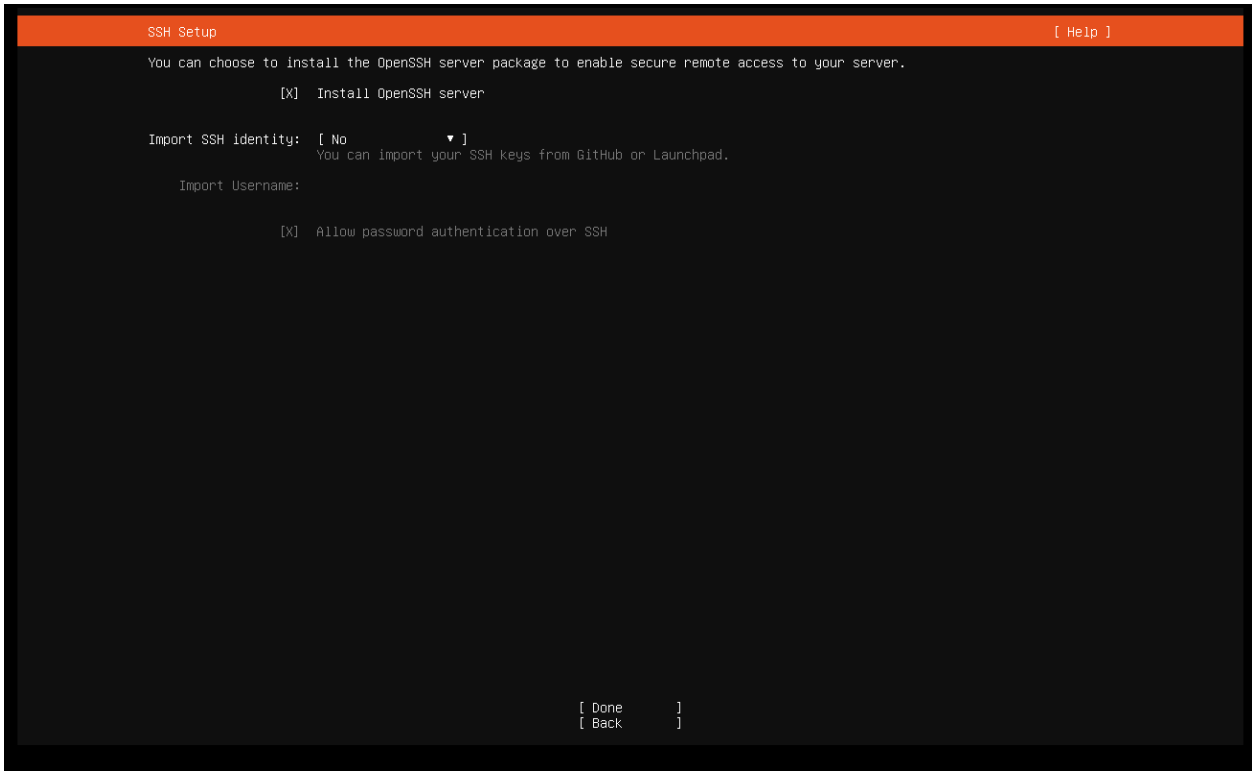
Try and install ubuntu

Press “Enter” while having “Done” highlighted and select all the default selections until you are asked for a name and password

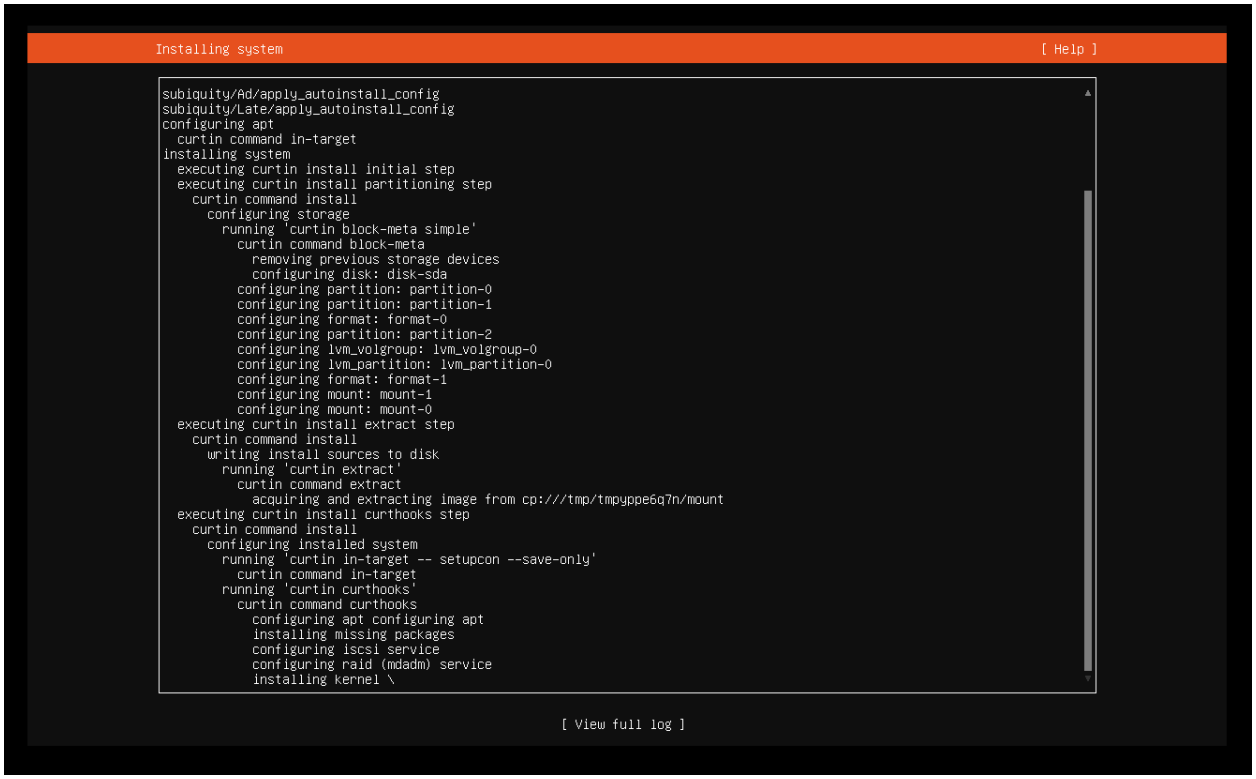
Fill in the fields as you wish



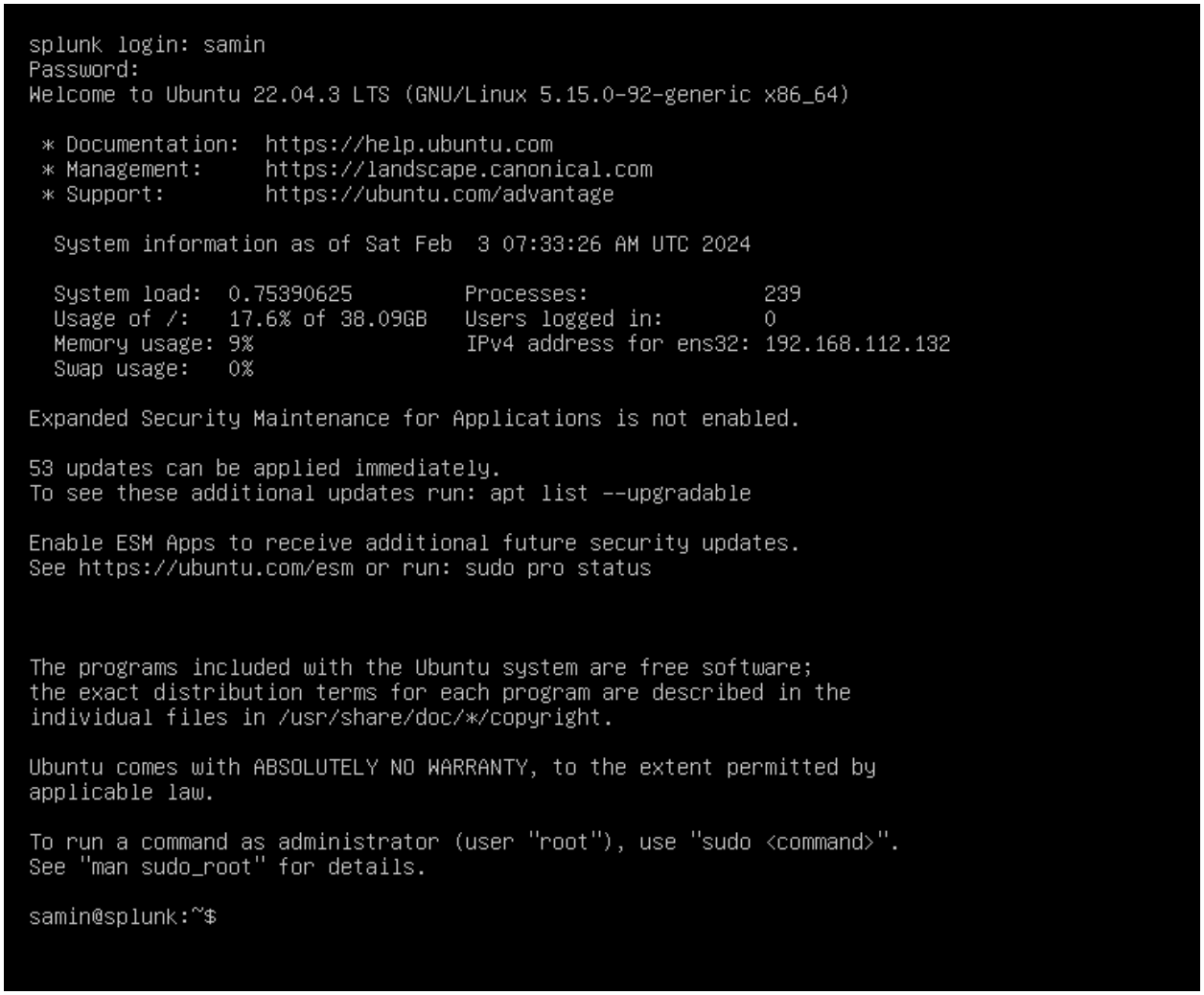
Press “Enter” to select the “Install OpenSSH server” option before moving on by selecting “Done”:



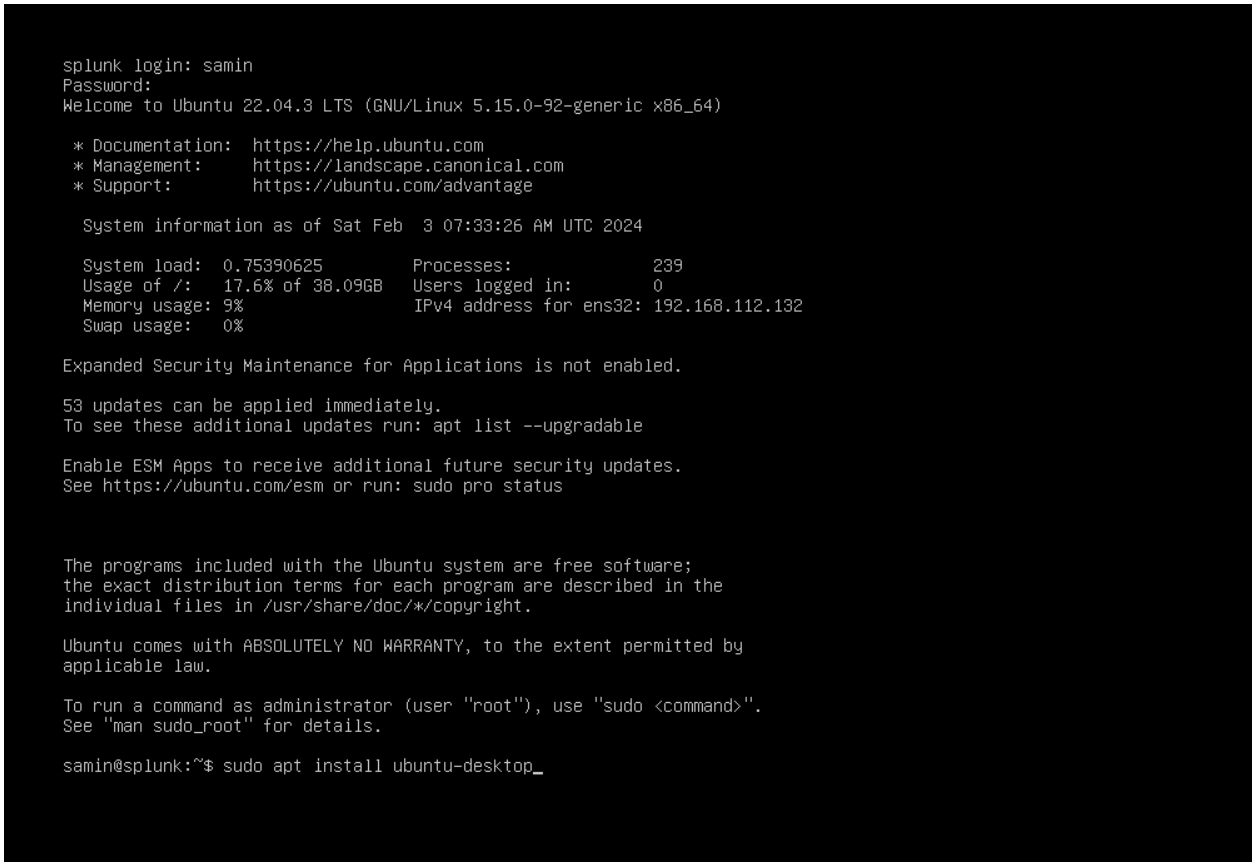
Keep the default selections for the next screens and then wait for the install to finish:

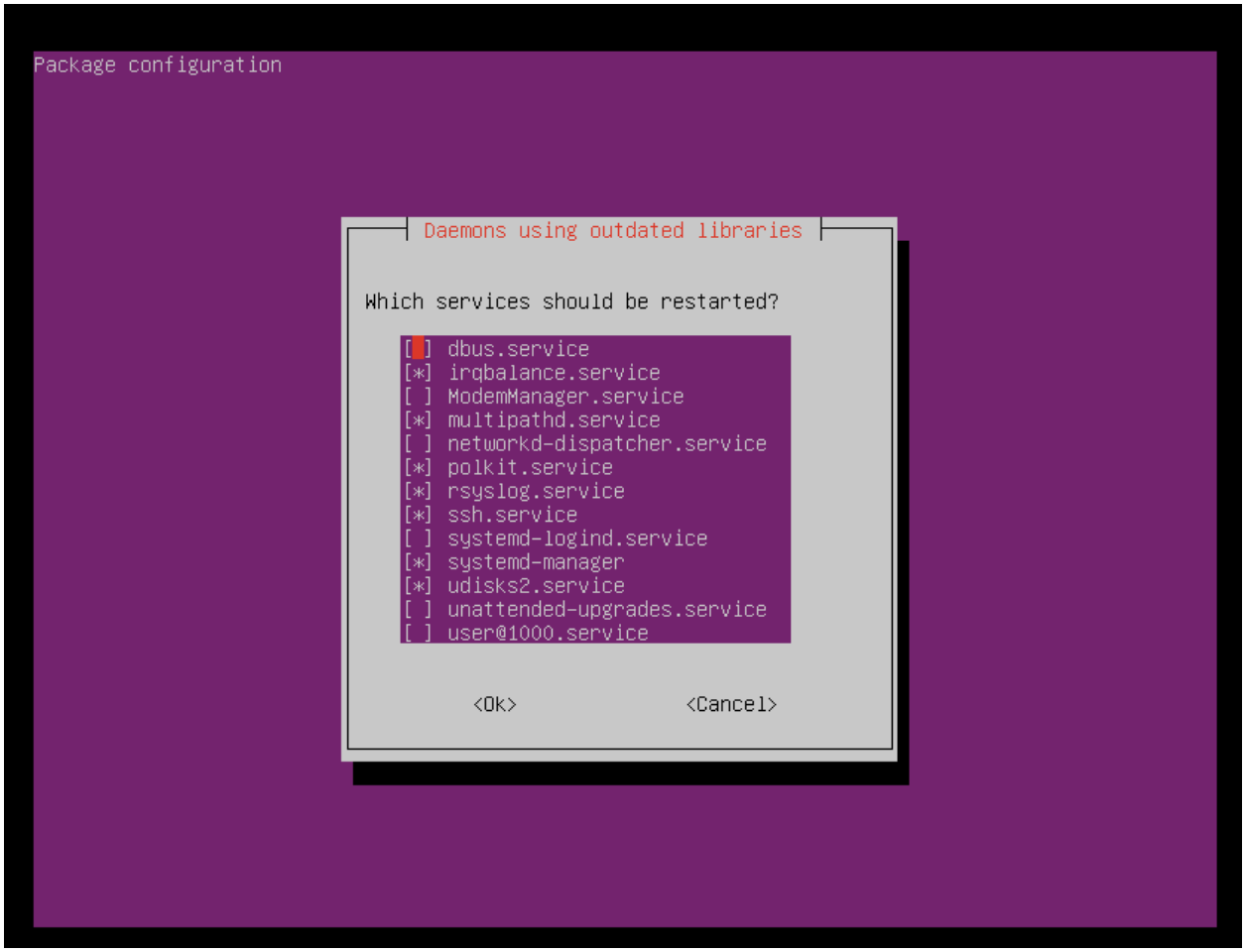


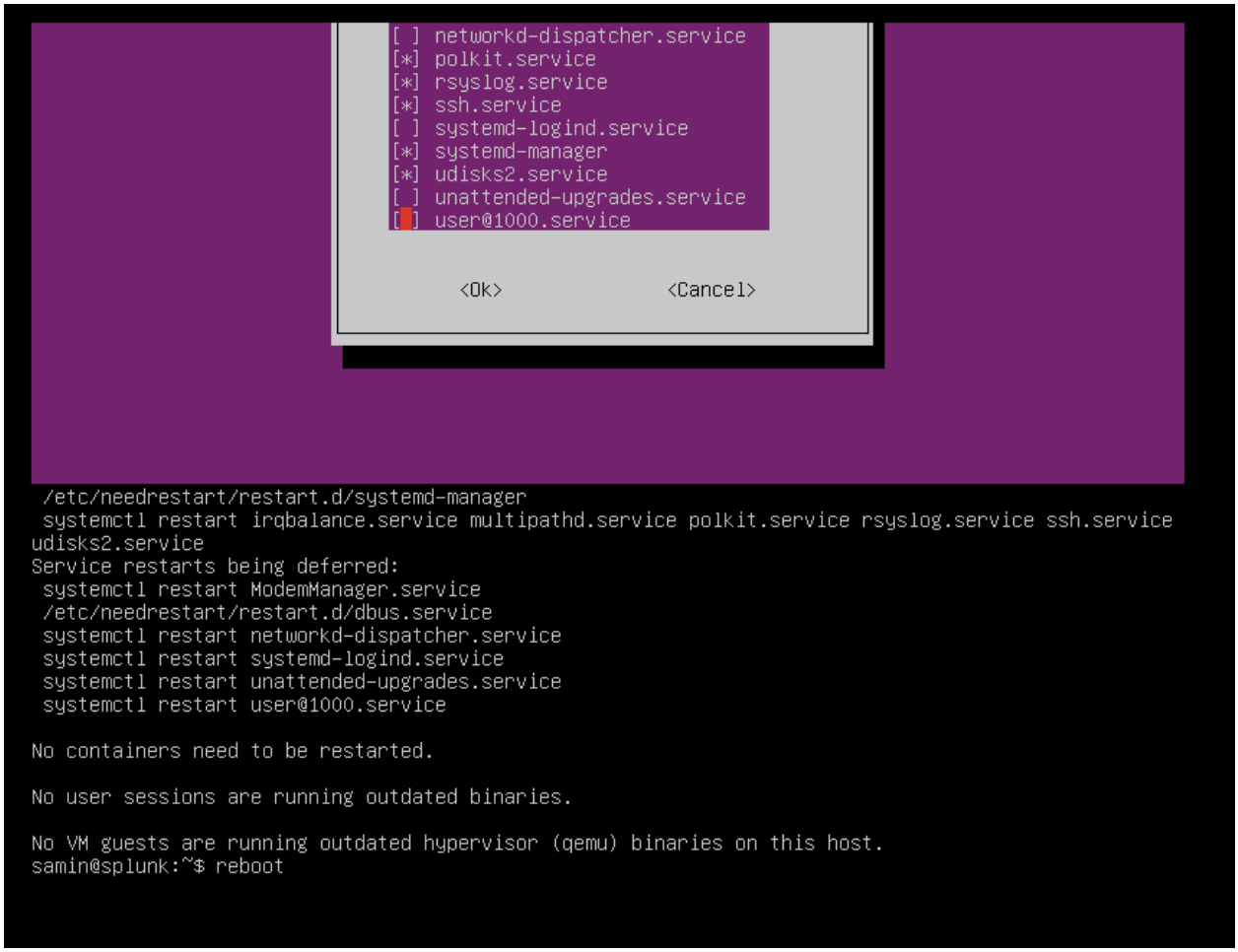
Once you are able, reboot the machine and log in:



Run the command “sudo apt install ubuntu-desktop” to get a GUI

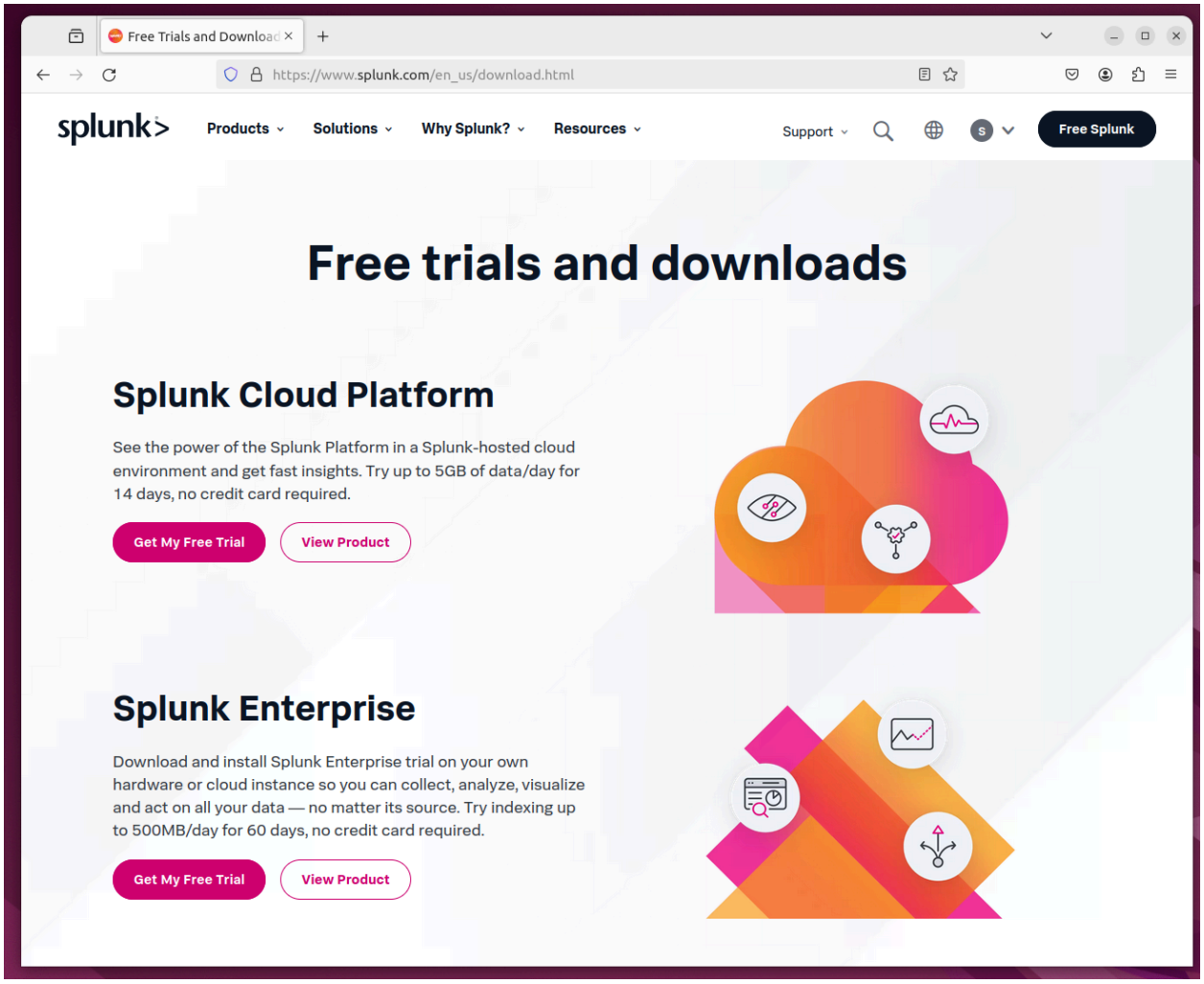

splunk login: samin
Password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 5.15.0-92-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Sat Feb 3 07:33:26 AM UTC 2024
System load: 0.75390625 Processes: 239
Usage of /: 17.6% of 38.09GB Users logged in: 0
Memory usage: 9% IPv4 address for ens32: 192.168.112.132
Swap usage: 0%
Expanded Security Maintenance for Applications is not enabled.
53 updates can be applied immediately.
To see these additional updates run: apt list --upgradable
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
samin@splunk:~$ sudo apt install ubuntu-desktop_

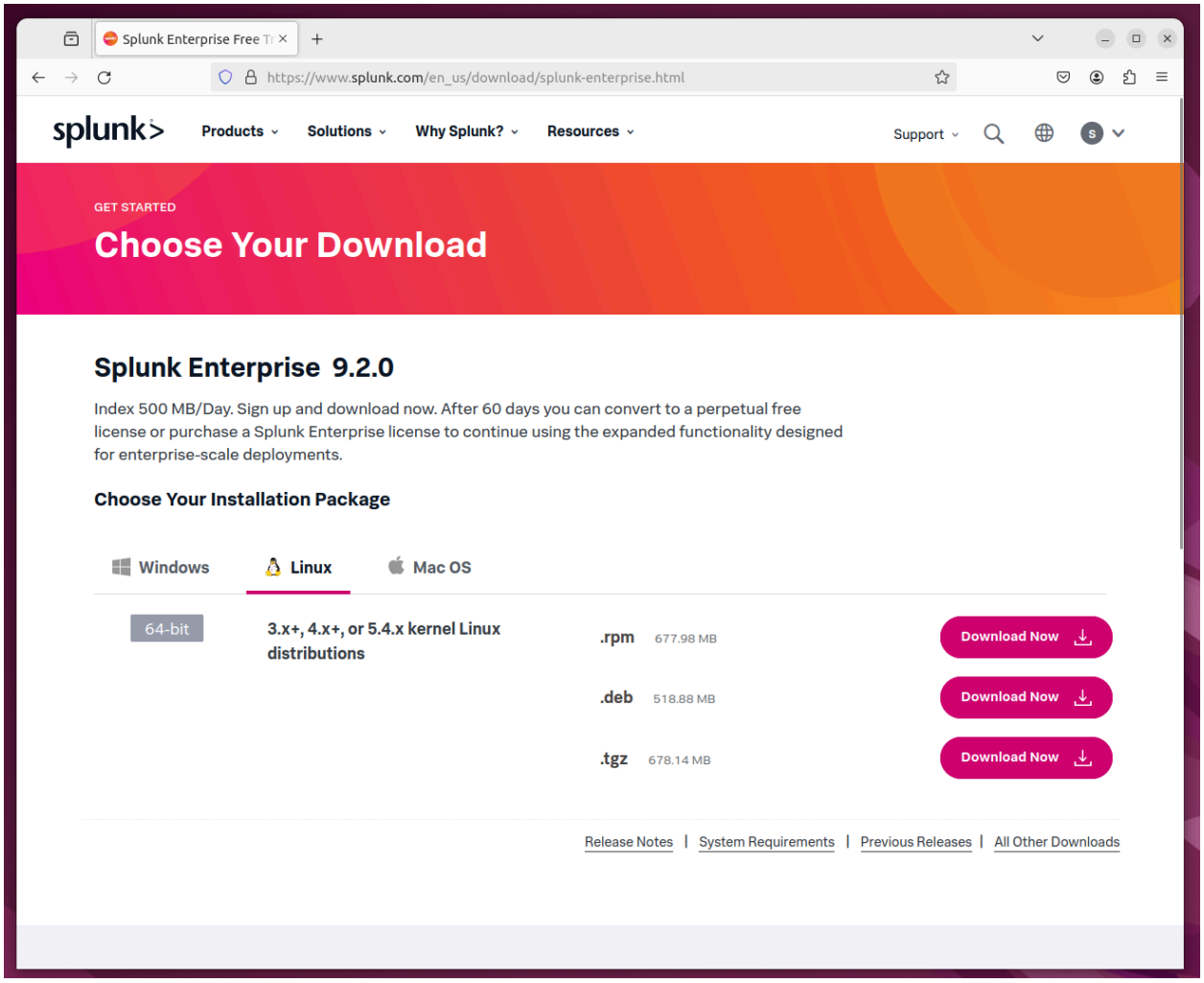

Package configuration
Daemons using outdated libraries
Which services should be restarted?
[ ] dbus.service
[*] irqbalance.service
[ ] ModemManager.service
[*] multipathd.service
[ ] networkd-dispatcher.service
[*] polkit.service
[*] rsyslog.service
[*] ssh.service
[ ] systemd-logind.service
[*] systemd-manager
[*] udisks2.service
[ ] unattended-upgrades.service
[ ] user@1000.service
<Ok>
<Cancel>



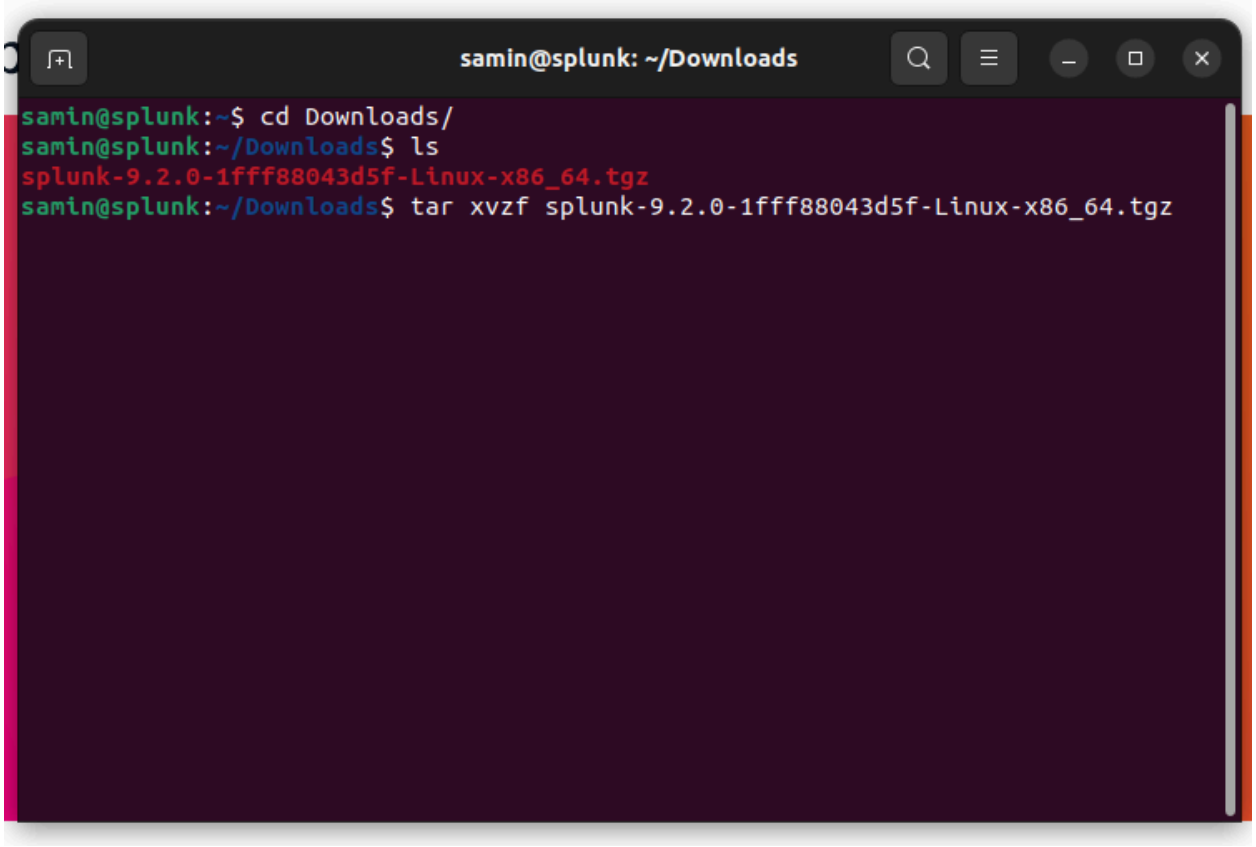
Once the machine is rebooted, open up Firefox and log into the Splunk website website; if you do not have an account, create one account.

Click “Get My Free Trial” of Splunk Enterprise and download the linux .tgz file:


Free Trials and Downloa
https://www.splunk.com/en_us/download.html
splunk>
Products
Solutions
Why Splunk?
Resources
Support
Free Splunk
Free trials and downloads
Splunk Cloud Platform
See the power of the Splunk Platform in a Splunk-hosted cloud environment and get fast insights. Try up to 5GB of data/day for 14 days, no credit card required.
Get My Free Trial
View Product
Splunk Enterprise
Download and install Splunk Enterprise trial on your own hardware or cloud instance so you can collect, analyze, visualize and act on all your data — no matter its source. Try indexing up to 500MB/day for 60 days, no credit card required.
Get My Free Trial
View Product

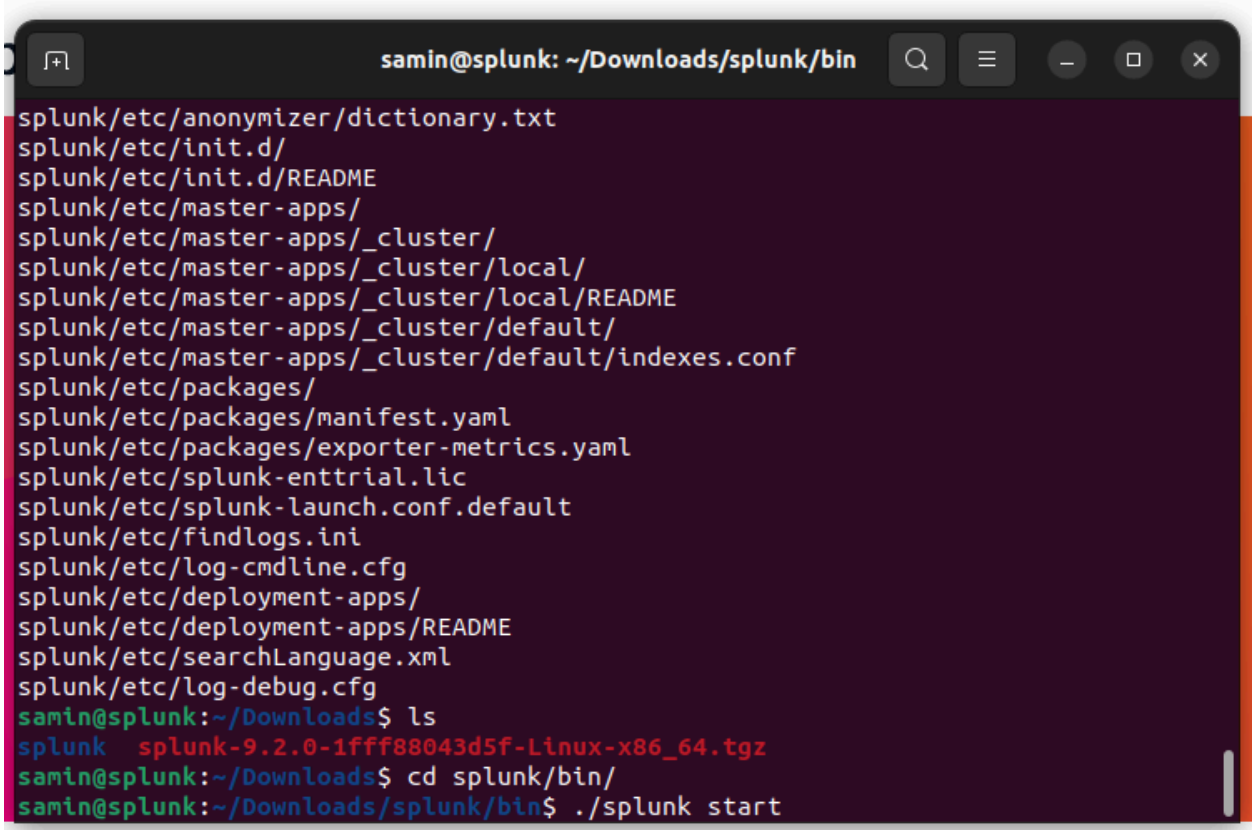


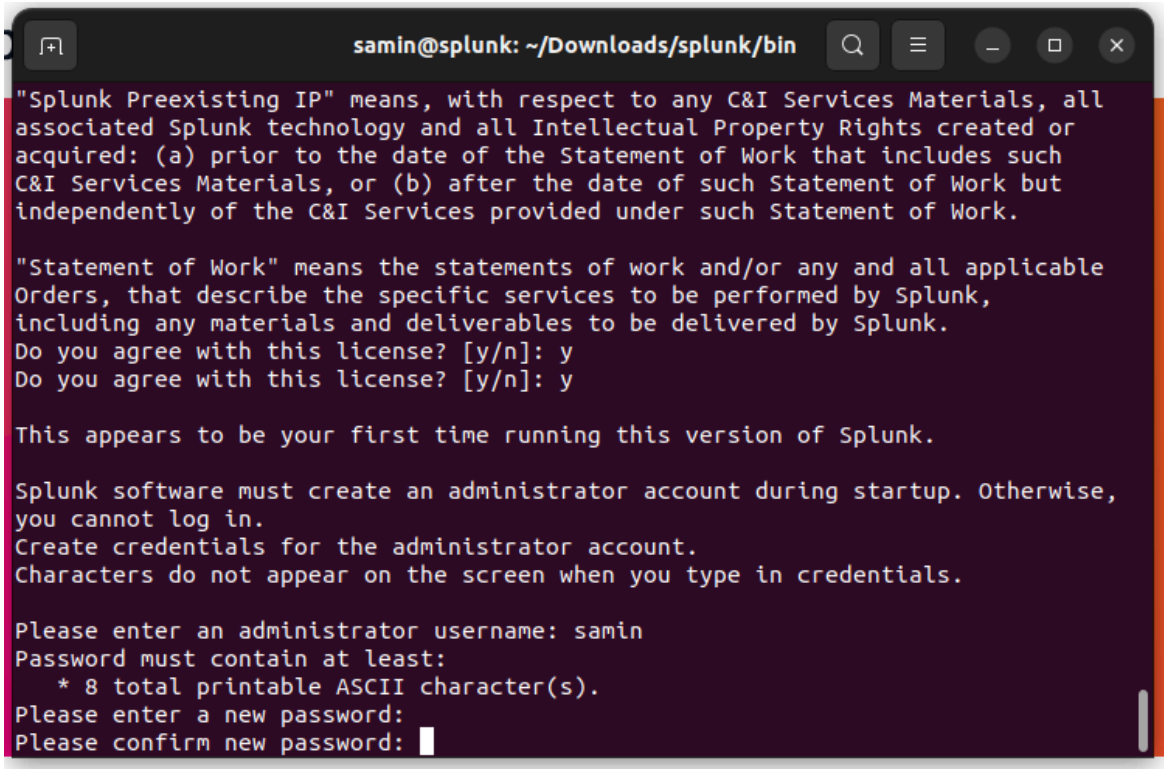
Open up a terminal and unzip the file:

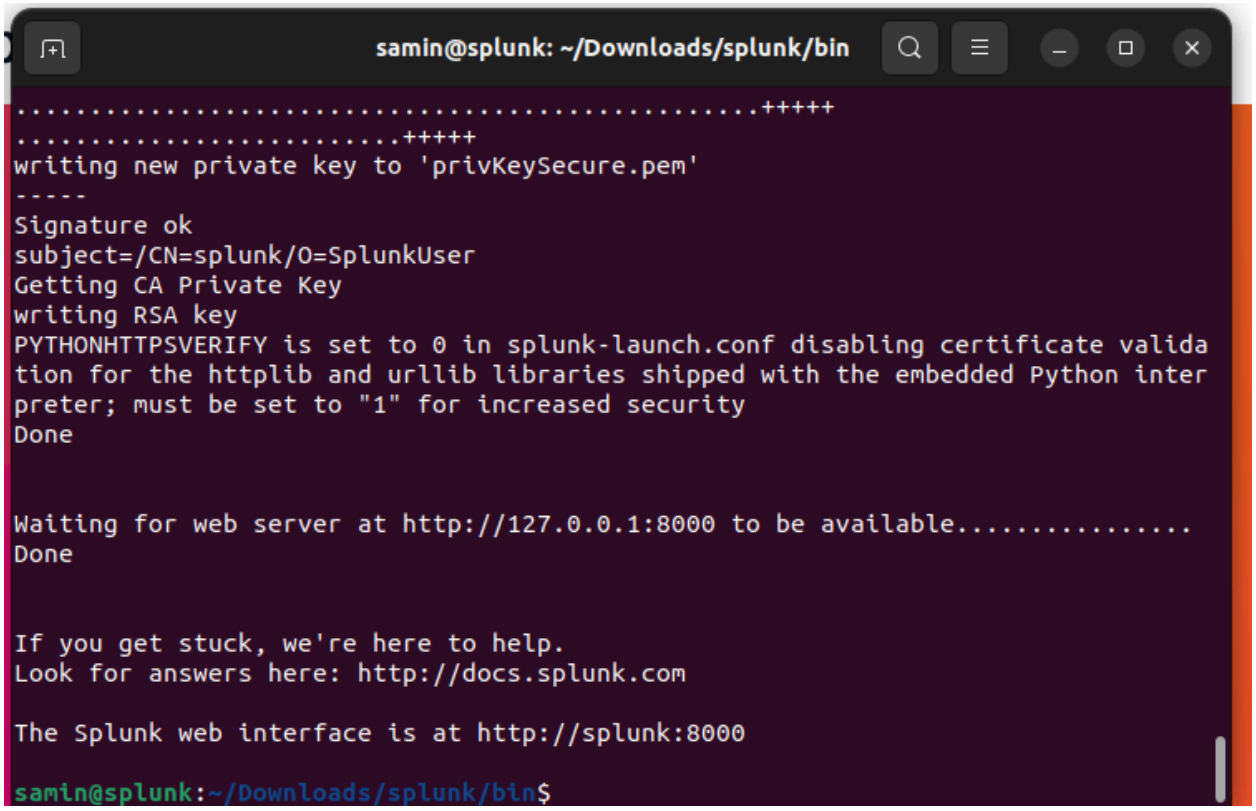


Move to the splunk/bin directory and run “./splunk start”

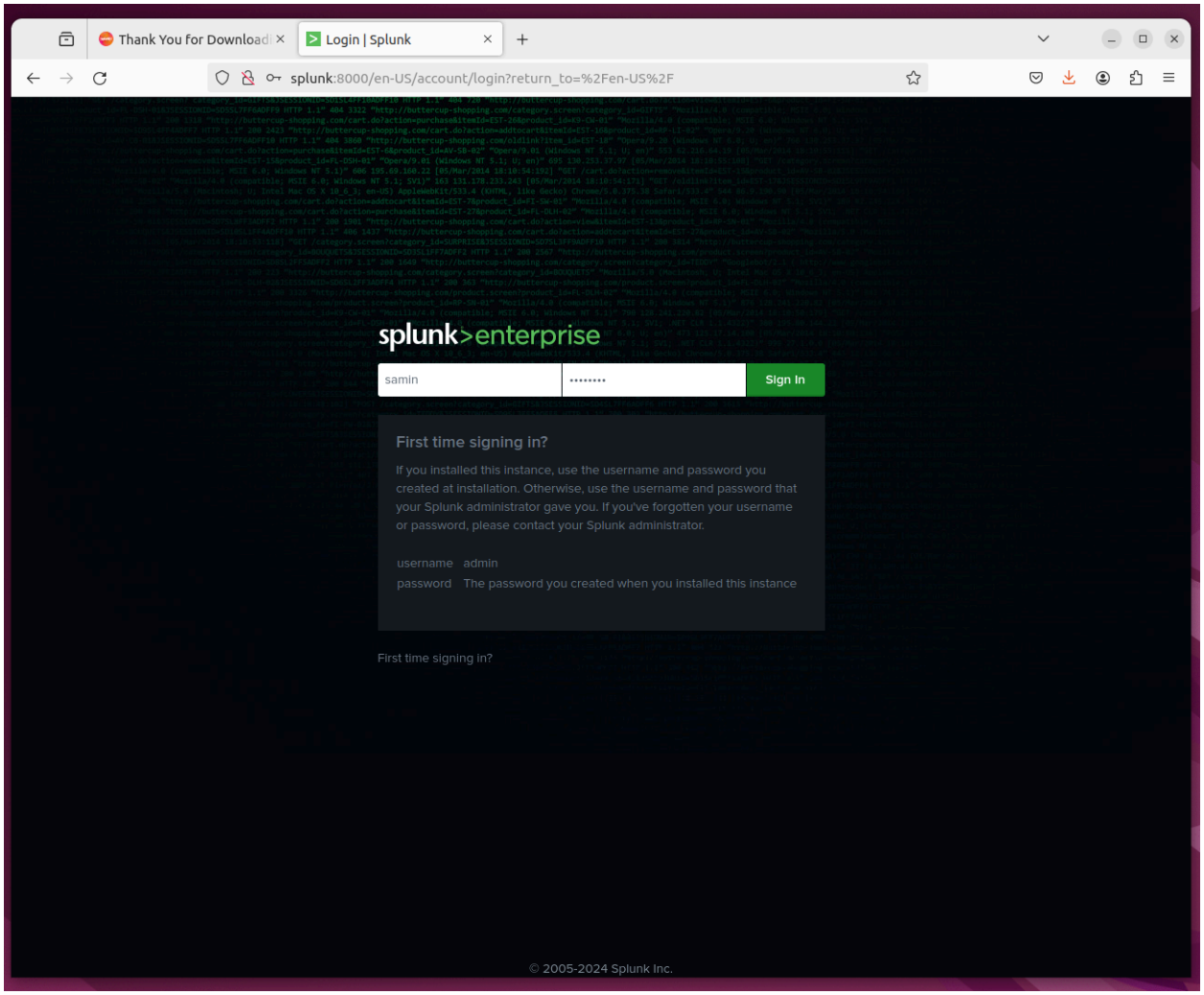
Agree with the license and set a username and password

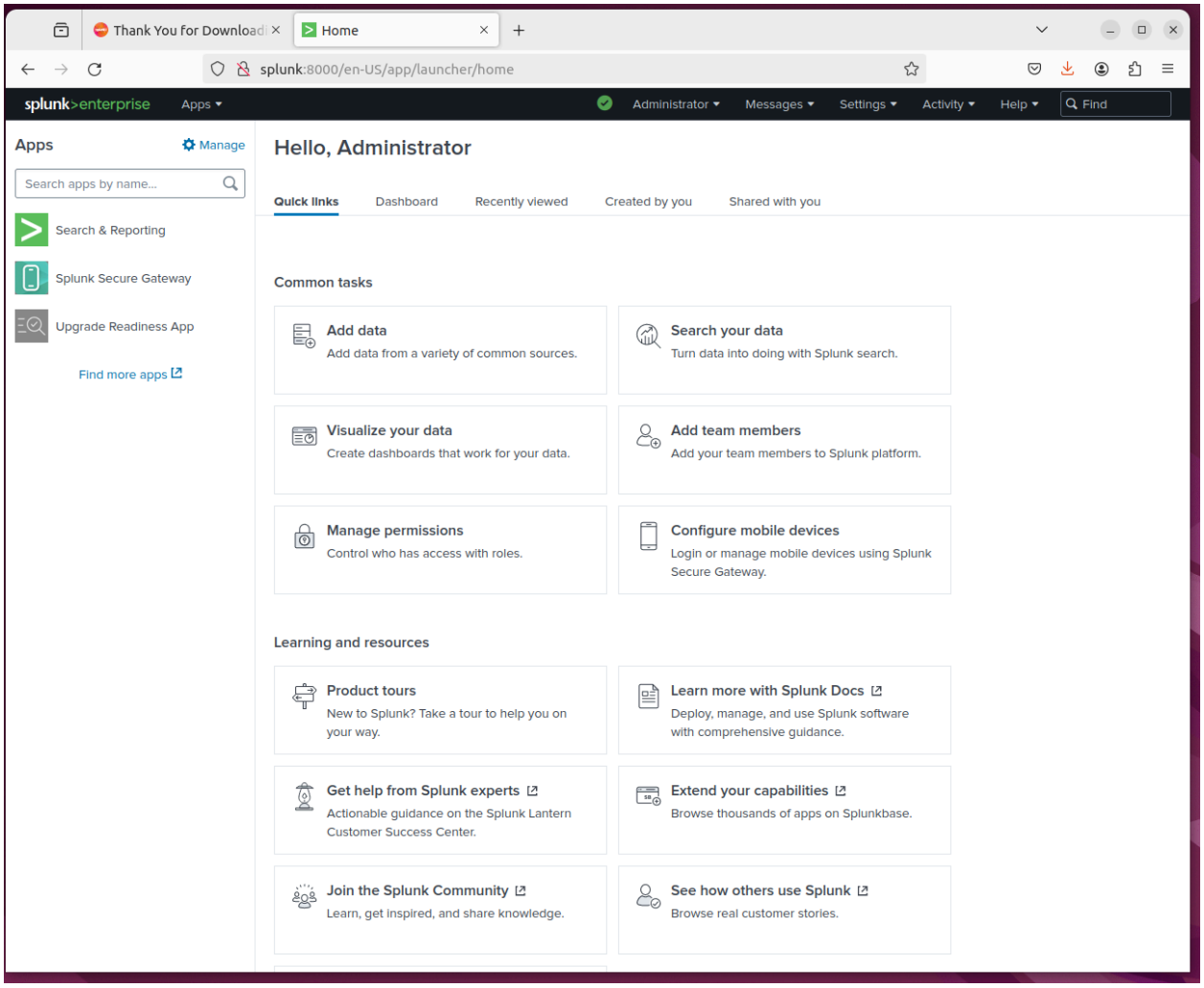

samin@splunk: ~/Downloads/splunk/bin
splunk/etc/anonymizer/dictionary.txt
splunk/etc/init.d/
splunk/etc/init.d/README
splunk/etc/master-apps/
splunk/etc/master-apps/_cluster/
splunk/etc/master-apps/_cluster/local/
splunk/etc/master-apps/_cluster/local/README
splunk/etc/master-apps/_cluster/default/
splunk/etc/master-apps/_cluster/default/indexes.conf
splunk/etc/packages/
splunk/etc/packages/manifest.yaml
splunk/etc/packages/exporter-metrics.yaml
splunk/etc/splunk-enttrial.lic
splunk/etc/splunk-launch.conf.default
splunk/etc/findlogs.ini
splunk/etc/log-cmdline.cfg
splunk/etc/deployment-apps/
splunk/etc/deployment-apps/README
splunk/etc/searchLanguage.xml
splunk/etc/log-debug.cfg
samin@splunk:~/Downloads$ ls
splunk splunk-9.2.0-1fff88043d5f-Linux-x86_64.tgz
samin@splunk:~/Downloads$ cd splunk/bin/
samin@splunk:~/Downloads/splunk/bin$ ./splunk start


samin@splunk: ~/Downloads/splunk/bin
"Splunk Preexisting IP" means, with respect to any C&I Services Materials, all
associated Splunk technology and all Intellectual Property Rights created or
acquired: (a) prior to the date of the Statement of Work that includes such
C&I Services Materials, or (b) after the date of such Statement of Work but
independently of the C&I Services provided under such Statement of Work.
"Statement of Work" means the statements of work and/or any and all applicable
Orders, that describe the specific services to be performed by Splunk,
including any materials and deliverables to be delivered by Splunk.
Do you agree with this license? [y/n]: y
Do you agree with this license? [y/n]: y
This appears to be your first time running this version of Splunk.
Splunk software must create an administrator account during startup. Otherwise,
you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.
Please enter an administrator username: samin
Password must contain at least:
* 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:



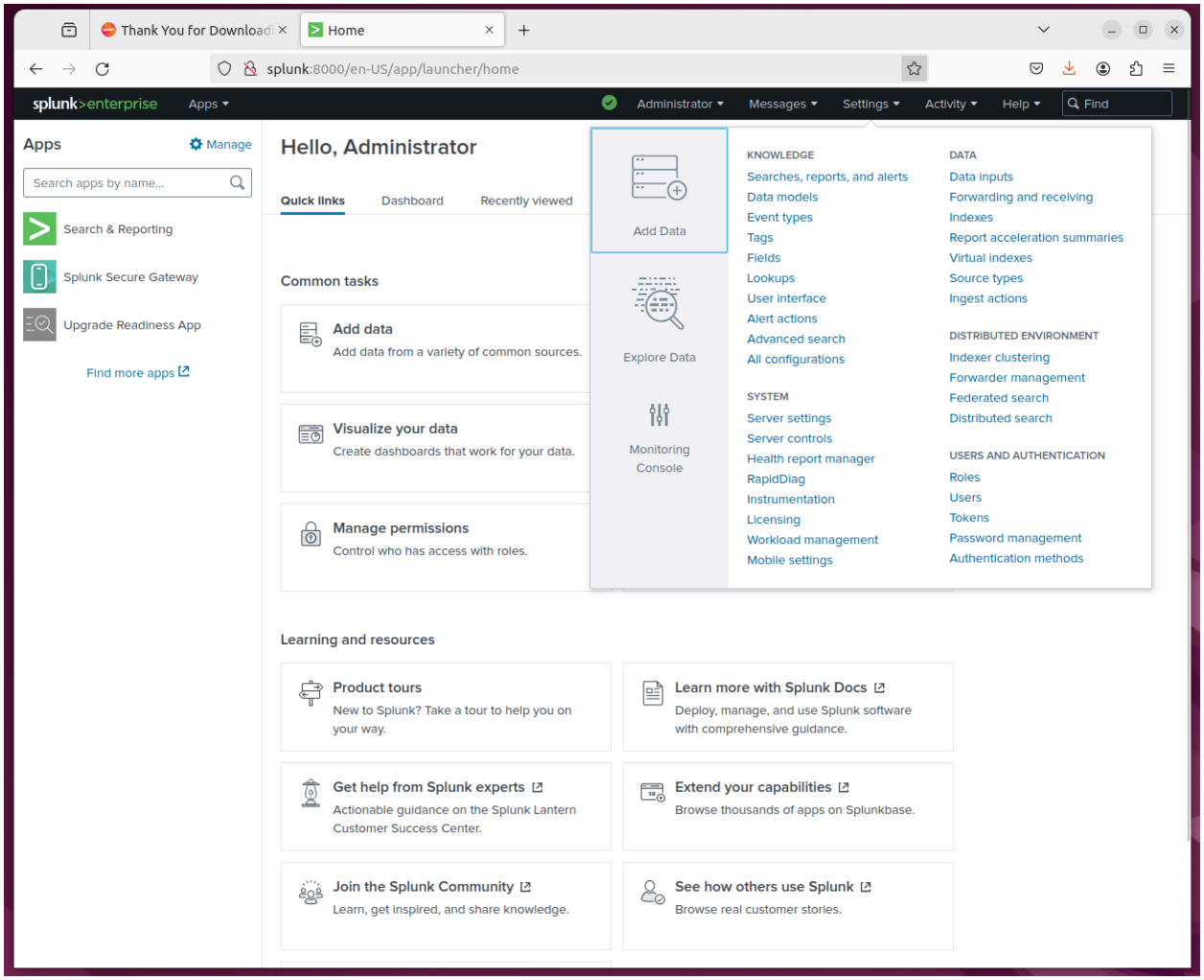
You can now log in at “http://splunk:8000”

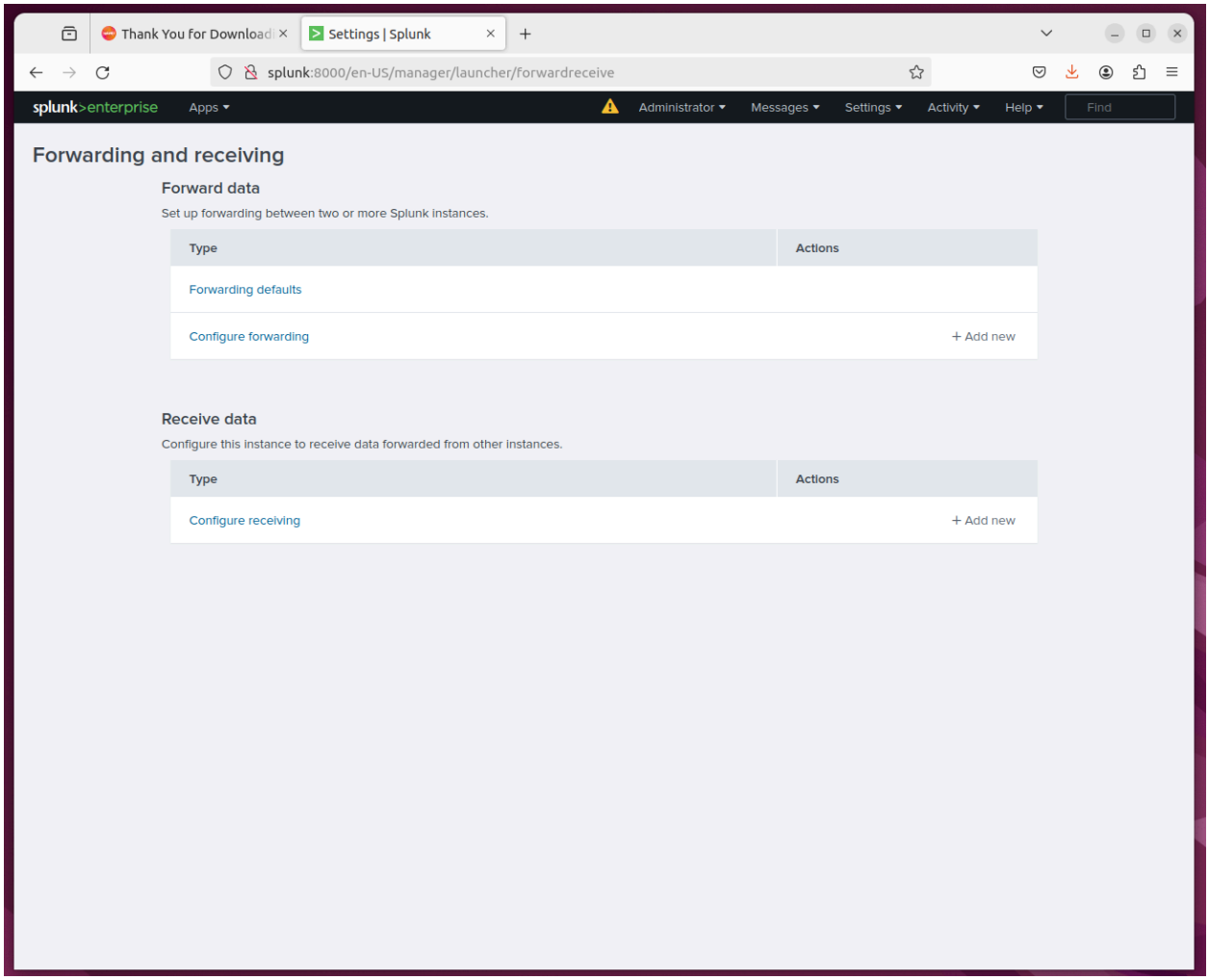

Thank You for Downloadi
Login | Splunk
splunk:8000/en-US/account/login?return_to=%2Fen-US%2F
splunk>enterprise
samin
Sign In
First time signing in?
If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.
username admin
password The password you created when you installed this instance
First time signing in?
© 2005-2024 Splunk Inc.



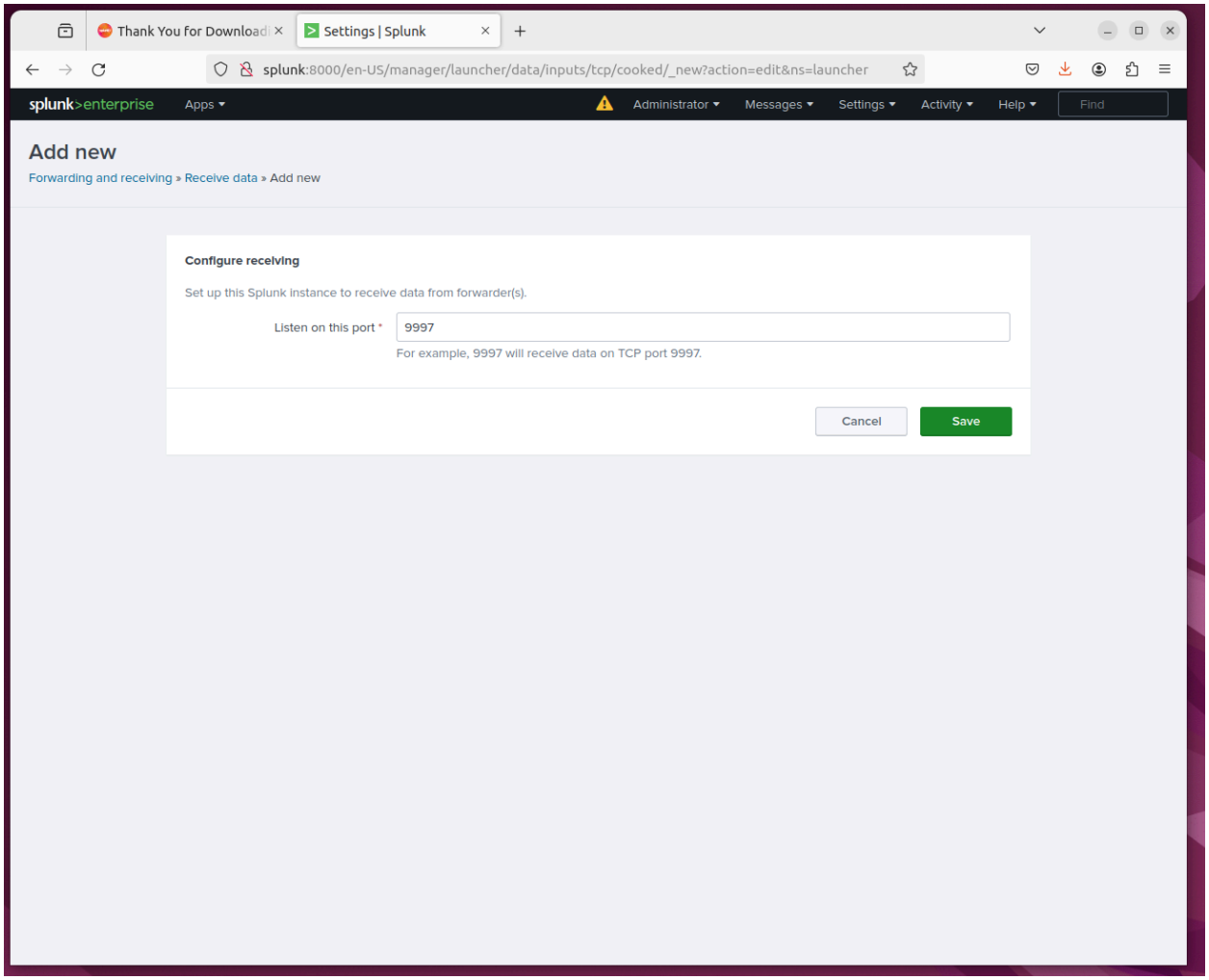
Configuring a Universal Forwarder on a Windows Server

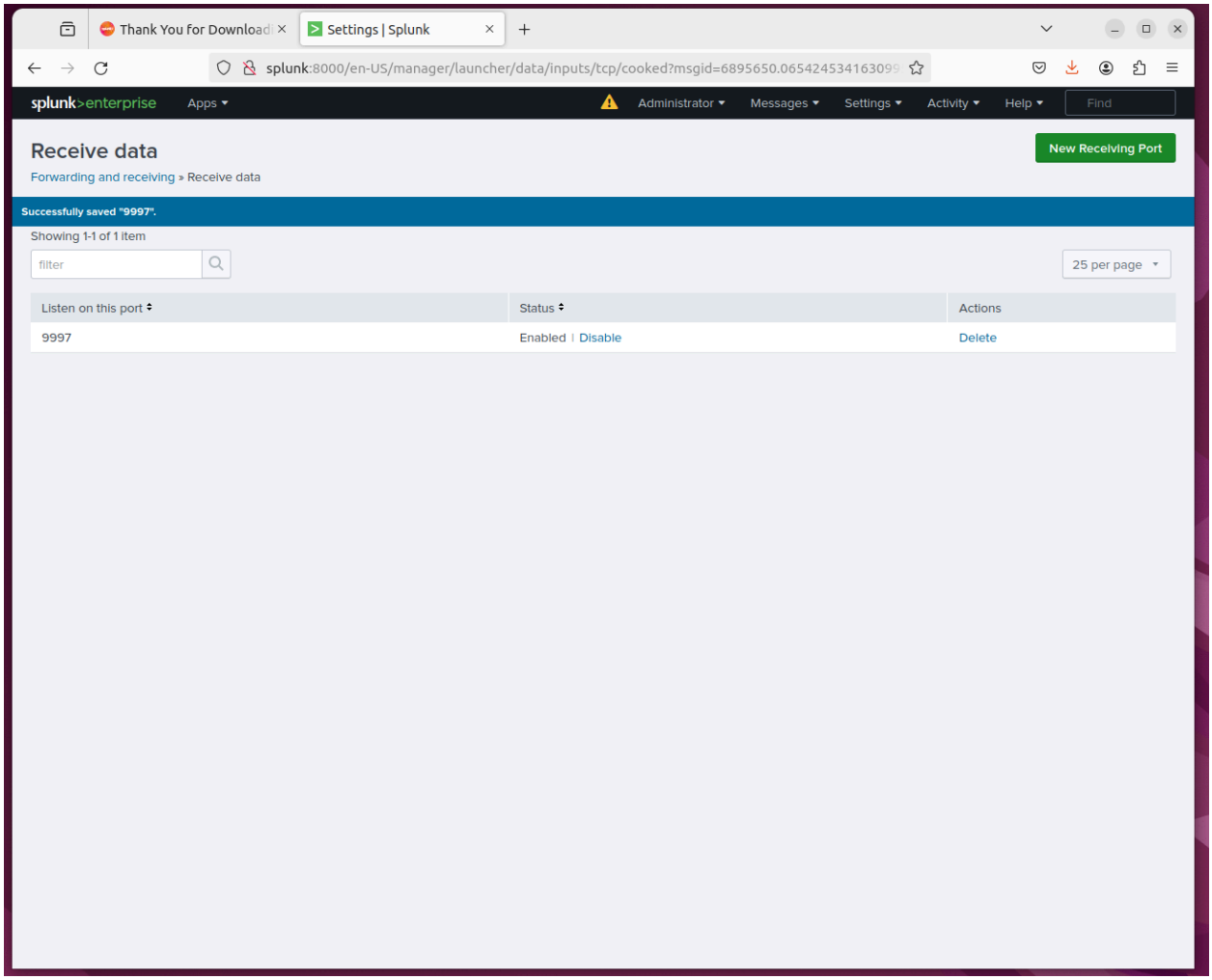
Navigate to http://splunk:8000 on the Ubuntu server and go to
Settings >> Forwarding and Receiving >> Add new


Thank You for Download
Home
splunk:8000/en-US/app/launcher/home
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Manage
Search apps by name...
Search & Reporting
Splunk Secure Gateway
Upgrade Readiness App
Find more apps
Hello, Administrator
Quick links
Dashboard
Recently viewed
Common tasks
Add data
Add data from a variety of common sources.
Visualize your data
Create dashboards that work for your data.
Manage permissions
Control who has access with roles.
Add Data
Explore Data
Monitoring Console
KNOWLEDGE
Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations
SYSTEM
Server settings
Server controls
Health report manager
RapidDiag
Instrumentation
Licensing
Workload management
Mobile settings
DATA
Data inputs
Forwarding and receiving
Indexes
Report acceleration summaries
Virtual indexes
Source types
Ingest actions
DISTRIBUTED ENVIRONMENT
Indexer clustering
Forwarder management
Federated search
Distributed search
USERS AND AUTHENTICATION
Roles
Users
Tokens
Password management
Authentication methods
Learning and resources
Product tours
New to Splunk? Take a tour to help you on your way.
Learn more with Splunk Docs
Deploy, manage, and use Splunk software with comprehensive guidance.
Get help from Splunk experts
Actionable guidance on the Splunk Lantern Customer Success Center.
Extend your capabilities
Browse thousands of apps on Splunkbase.
Join the Splunk Community
Learn, get inspired, and share knowledge.
See how others use Splunk
Browse real customer stories.

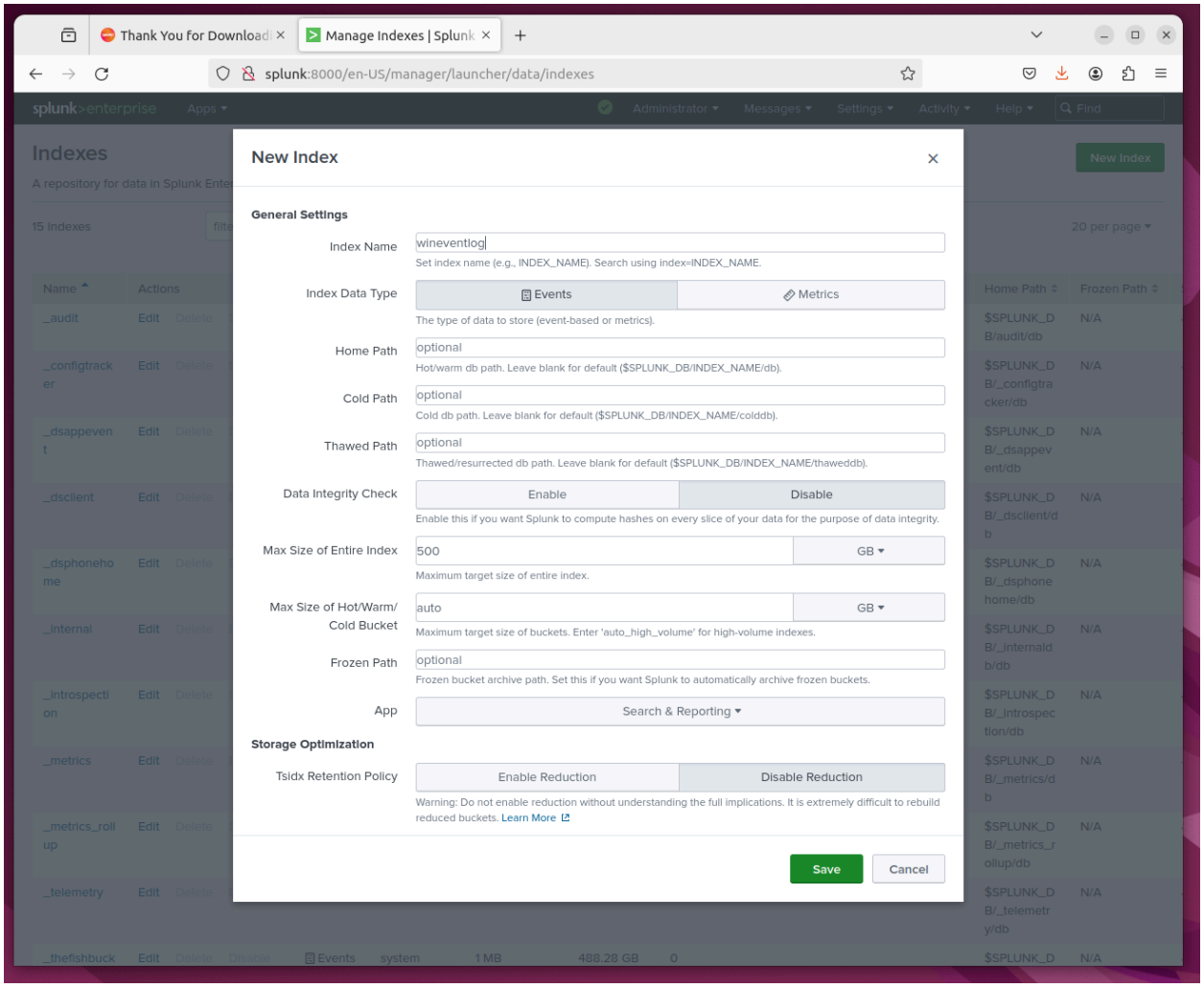


Listen on port 9997 and save:

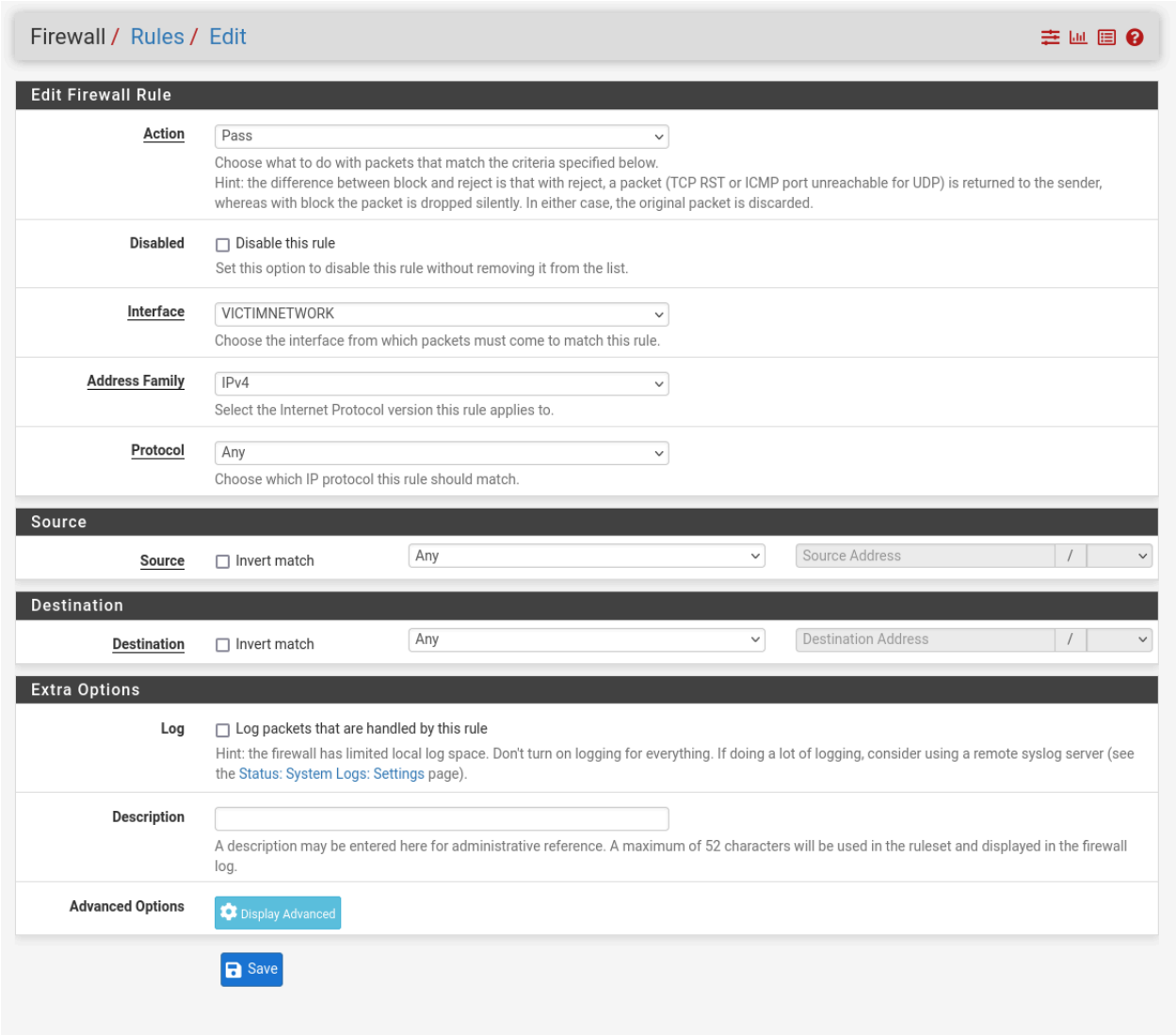

Thank You for Downloadi
Settings | Splunk
splunk:8000/en-US/manager/launcher/data/inputs/tcp/cooked/_new?action=edit&ns=launcher
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Add new
Forwarding and receiving » Receive data » Add new
Configure receiving
Set up this Splunk instance to receive data from forwarder(s).
Listen on this port *
9997
For example, 9997 will receive data on TCP port 9997.
Cancel
Save

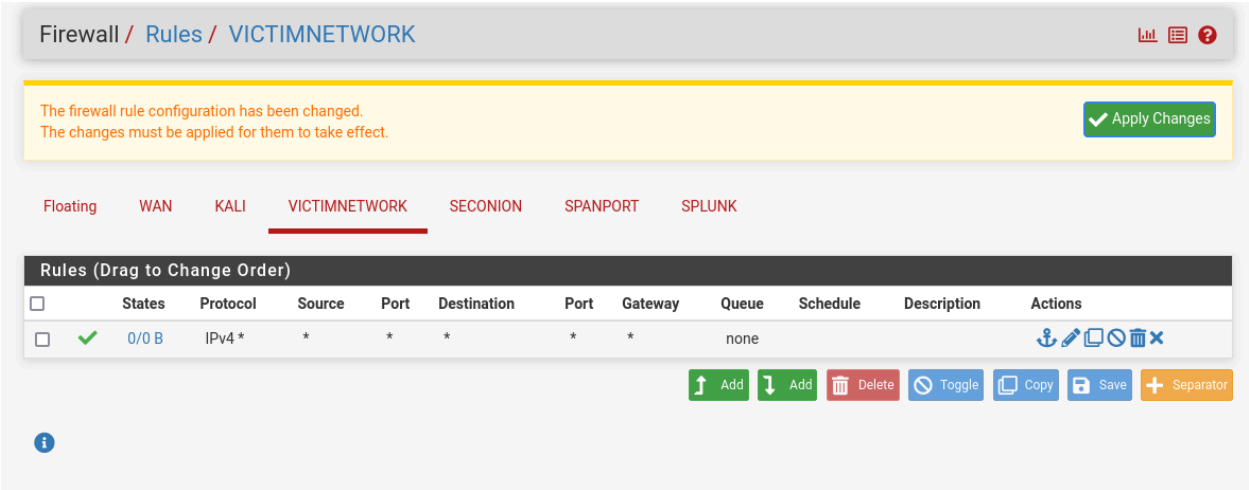


Next, go to **Settings >> Indexes >> New index** and set the name “wineventlog” before saving (keep all the other options as default):



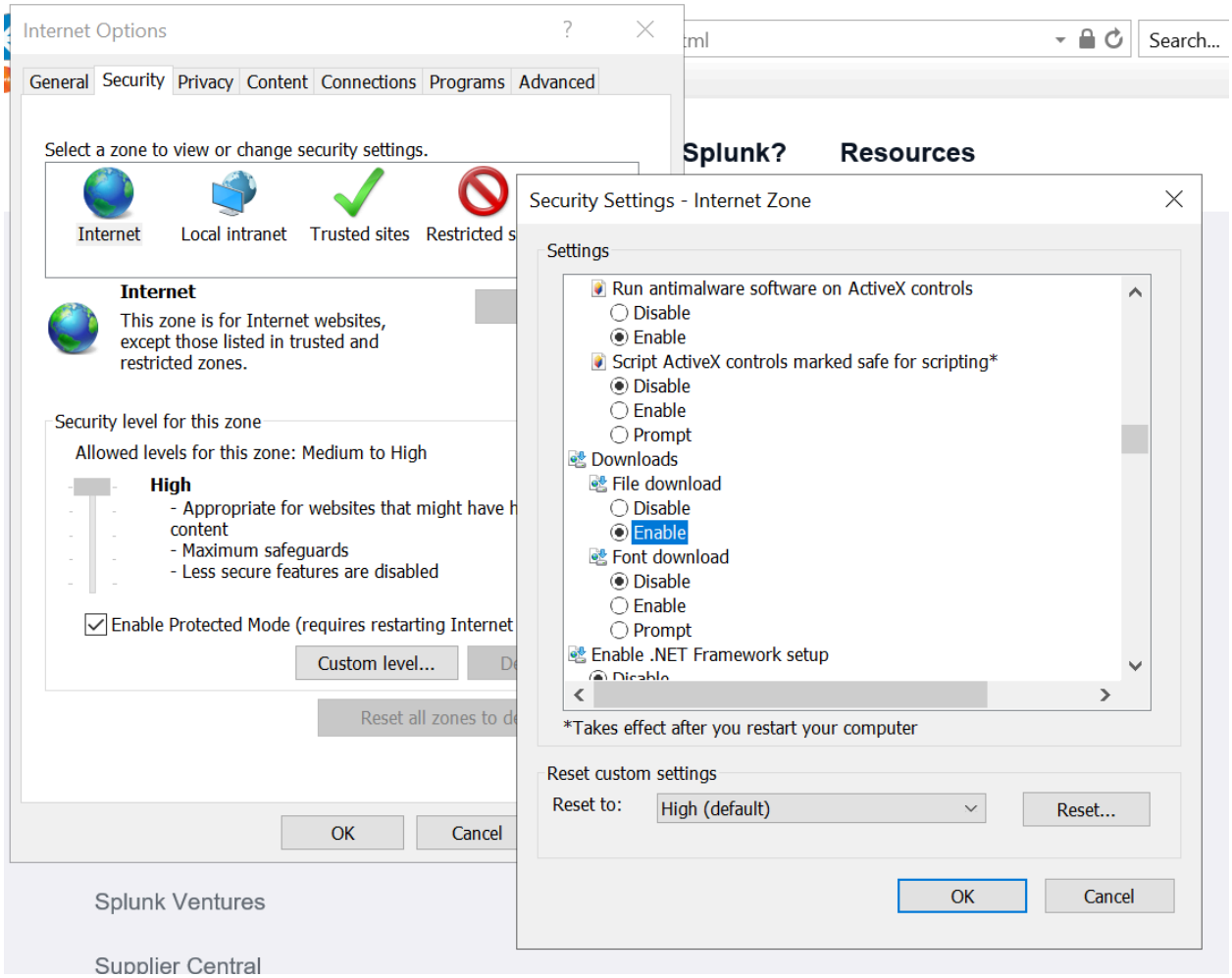
Now, access the pfSense interface from the Kali machine and go to **Firewall >> Rules >> Edit** and use the following configurations (make sure you are on the Victim Network):





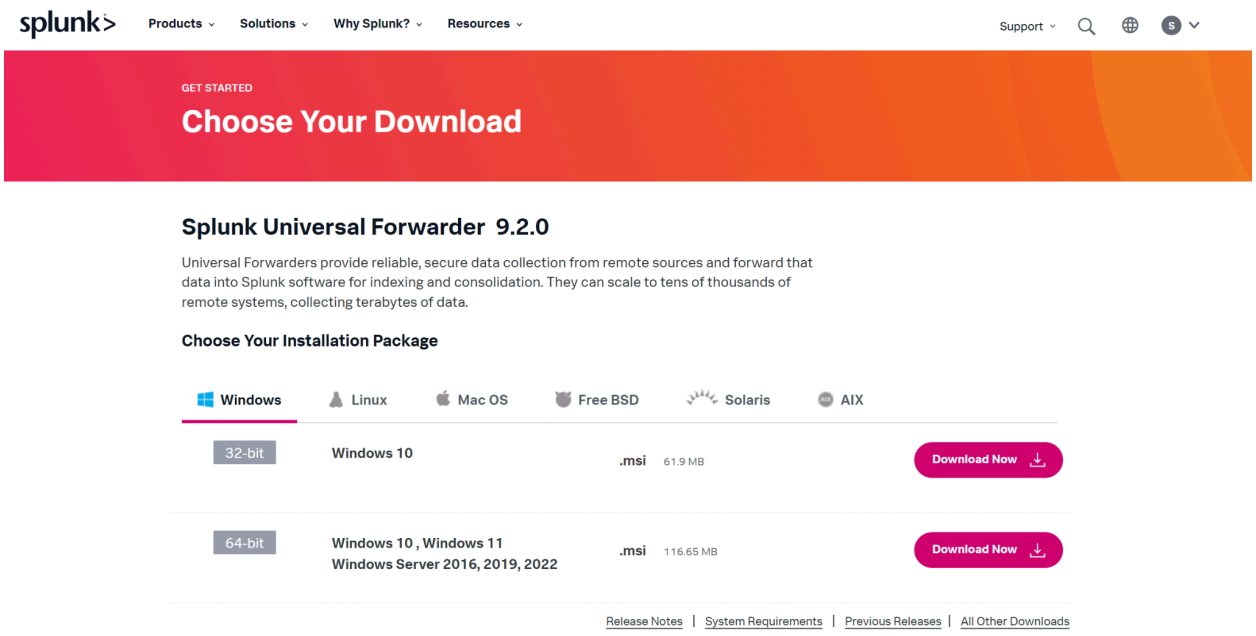
You should now be able to access the internet from the domain controller (Windows Server)

Make the following changes under **Settings>>Internet Options** in Internet Explorer:



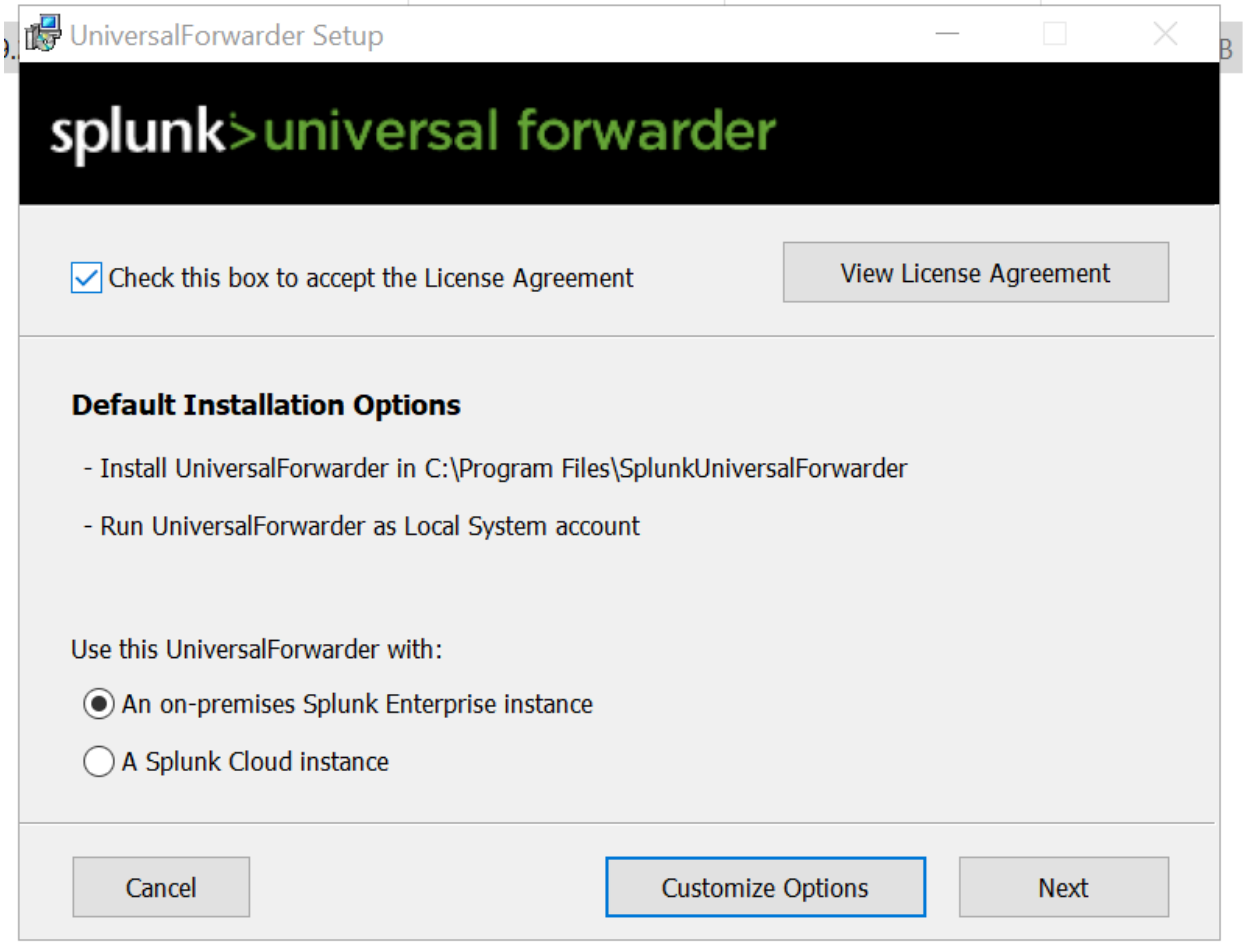
Restart the machine so the change can take effect.

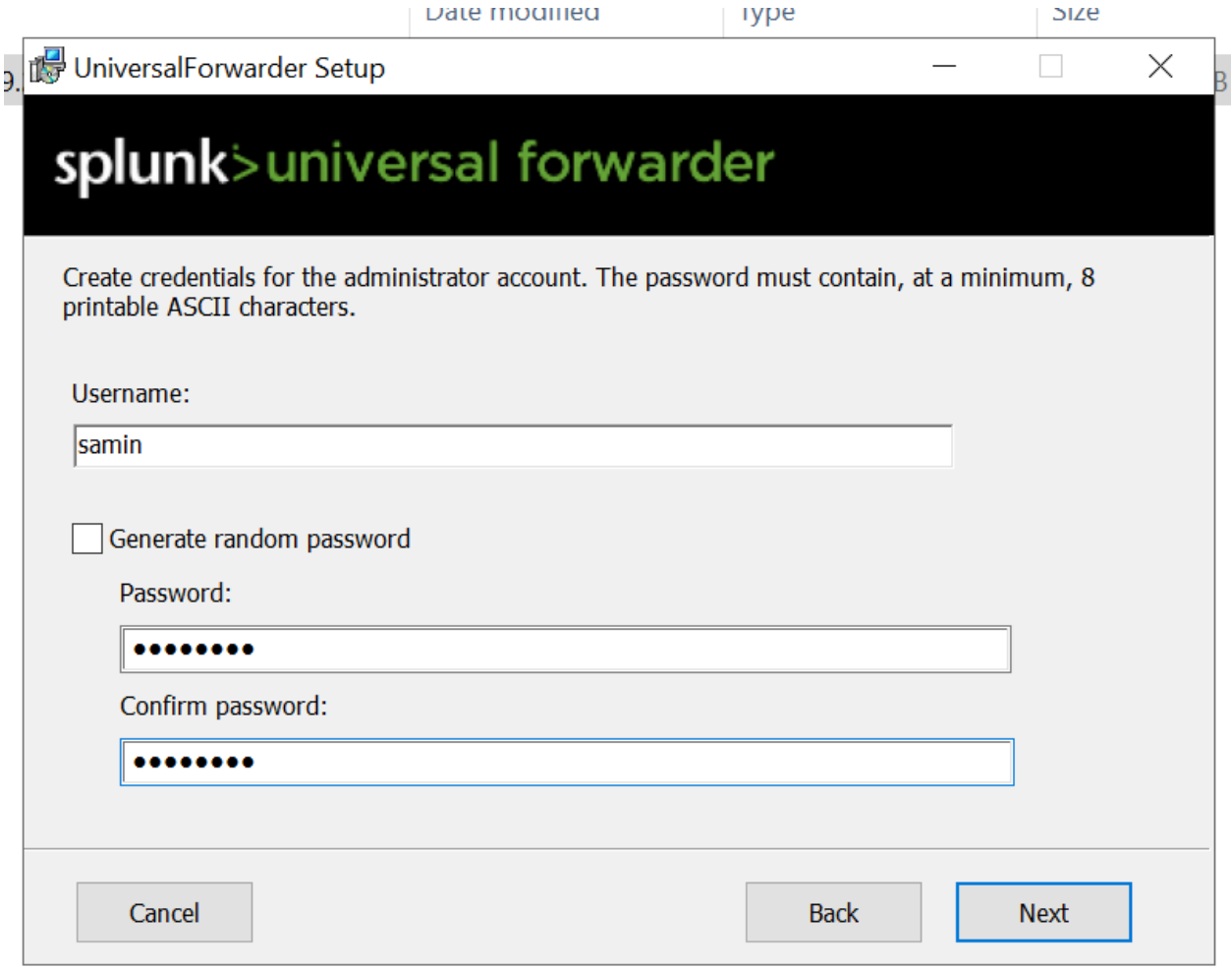
Download the Universal Forwarder, 64 bit version:



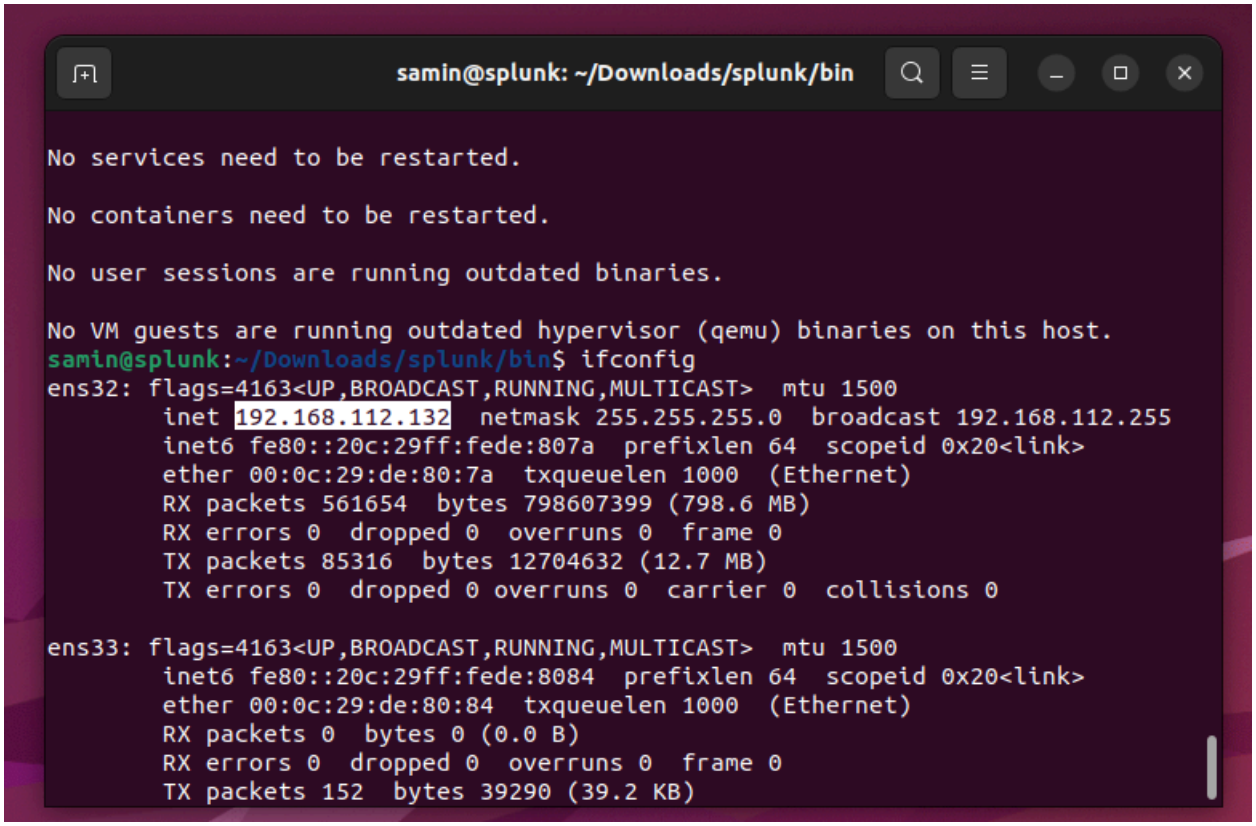
Run the installer.

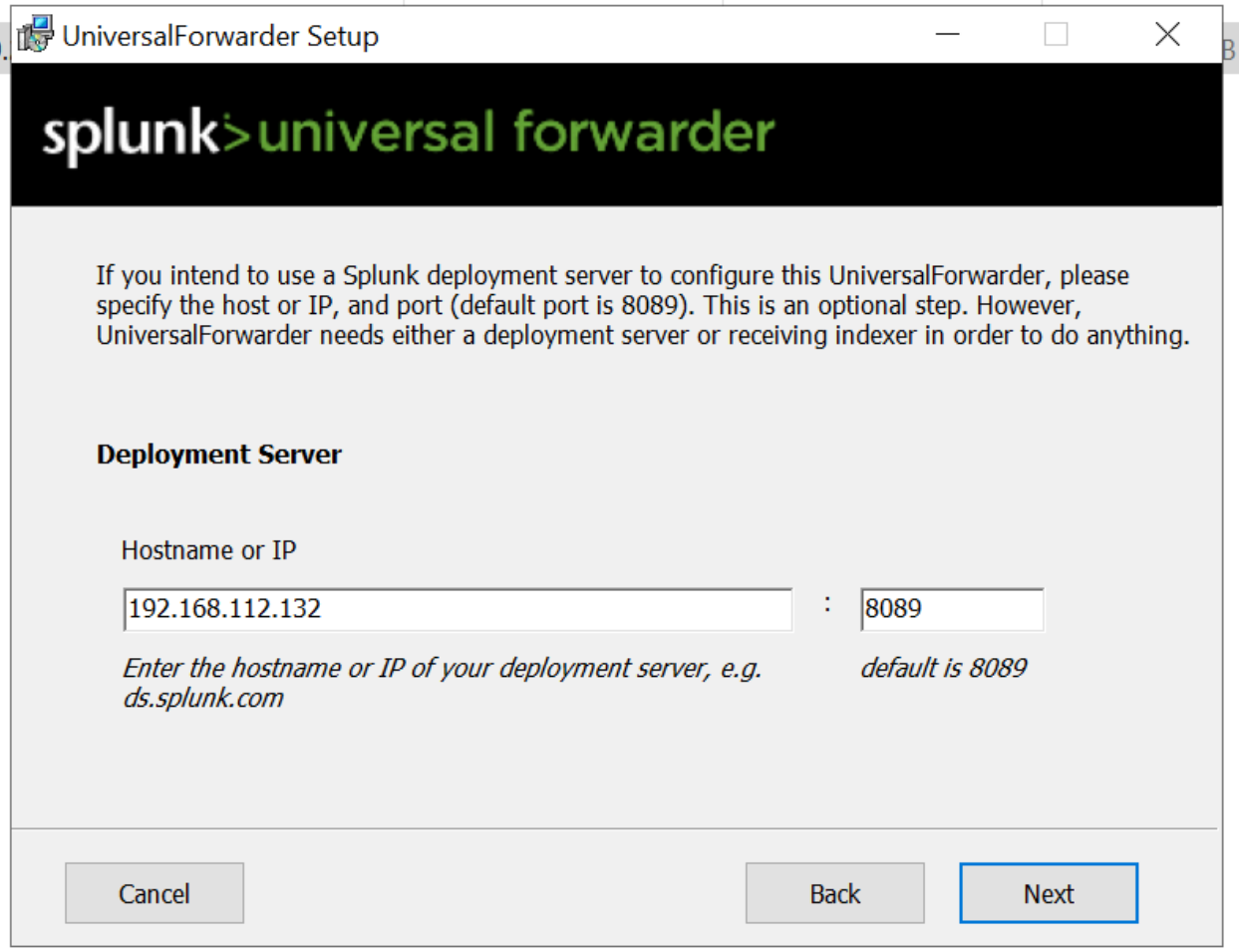
Accept the License Agreement and set a username and password:

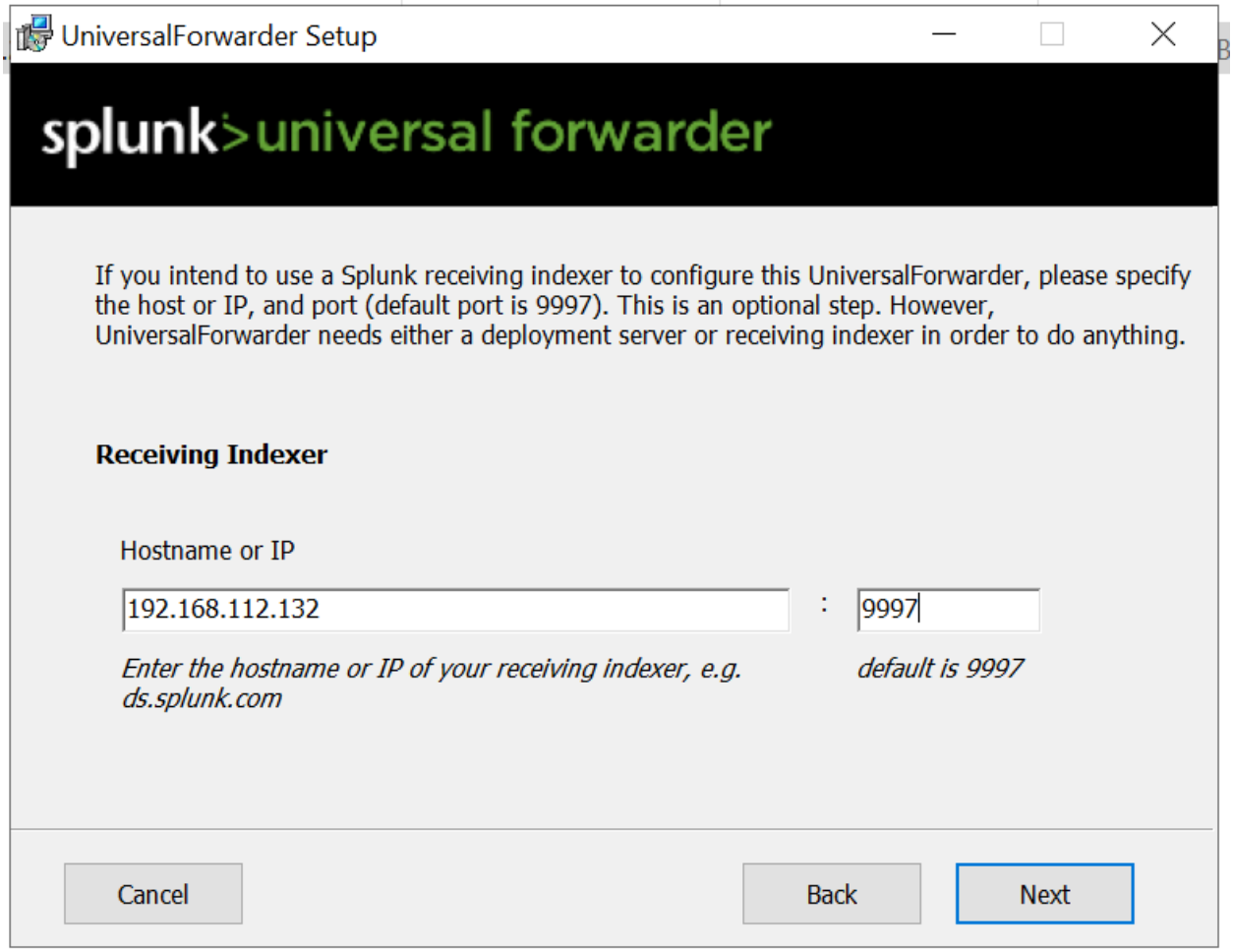

UniversalForwarder Setup
splunk>universal forwarder
Check this box to accept the License Agreement
View License Agreement
Default Installation Options
- Install UniversalForwarder in C:\Program Files\SplunkUniversalForwarder
- Run UniversalForwarder as Local System account
Use this UniversalForwarder with:
An on-premises Splunk Enterprise instance
A Splunk Cloud instance
Cancel
Customize Options
Next



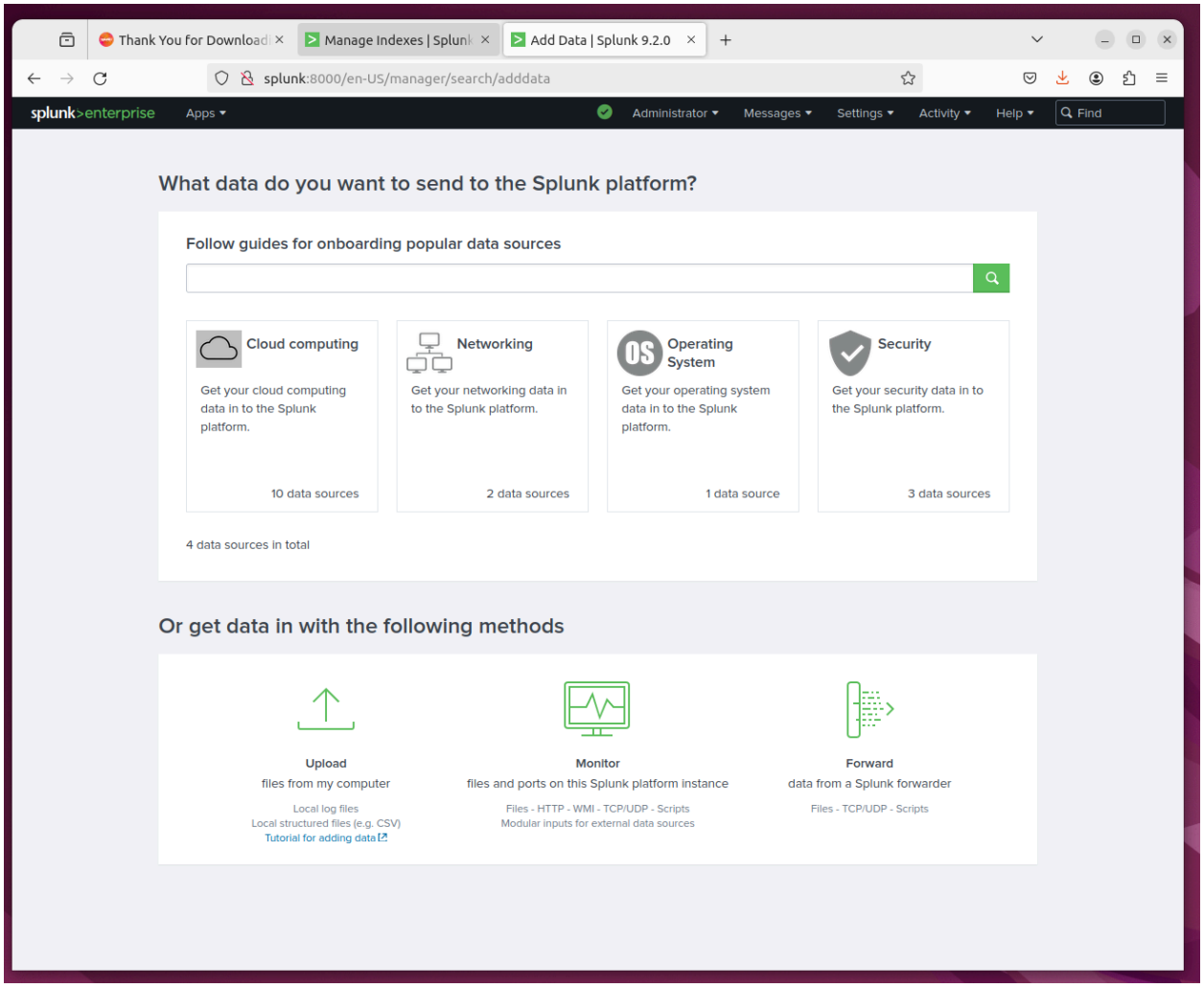
Find the IP address of the Splunk machine and use it to fill in the IP fields for the next 2 screens, using the default ports 8089 and 9997:


samin@splunk: ~/Downloads/splunk/bin
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
samin@splunk:~/Downloads/splunk/bin$ ifconfig
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.112.132 netmask 255.255.255.0 broadcast 192.168.112.255
inet6 fe80::20c:29ff:fede:807a prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:de:80:7a txqueuelen 1000 (Ethernet)
RX packets 561654 bytes 798607399 (798.6 MB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 85316 bytes 12704632 (12.7 MB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet6 fe80::20c:29ff:fede:8084 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:de:80:84 txqueuelen 1000 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 152 bytes 39290 (39.2 KB)

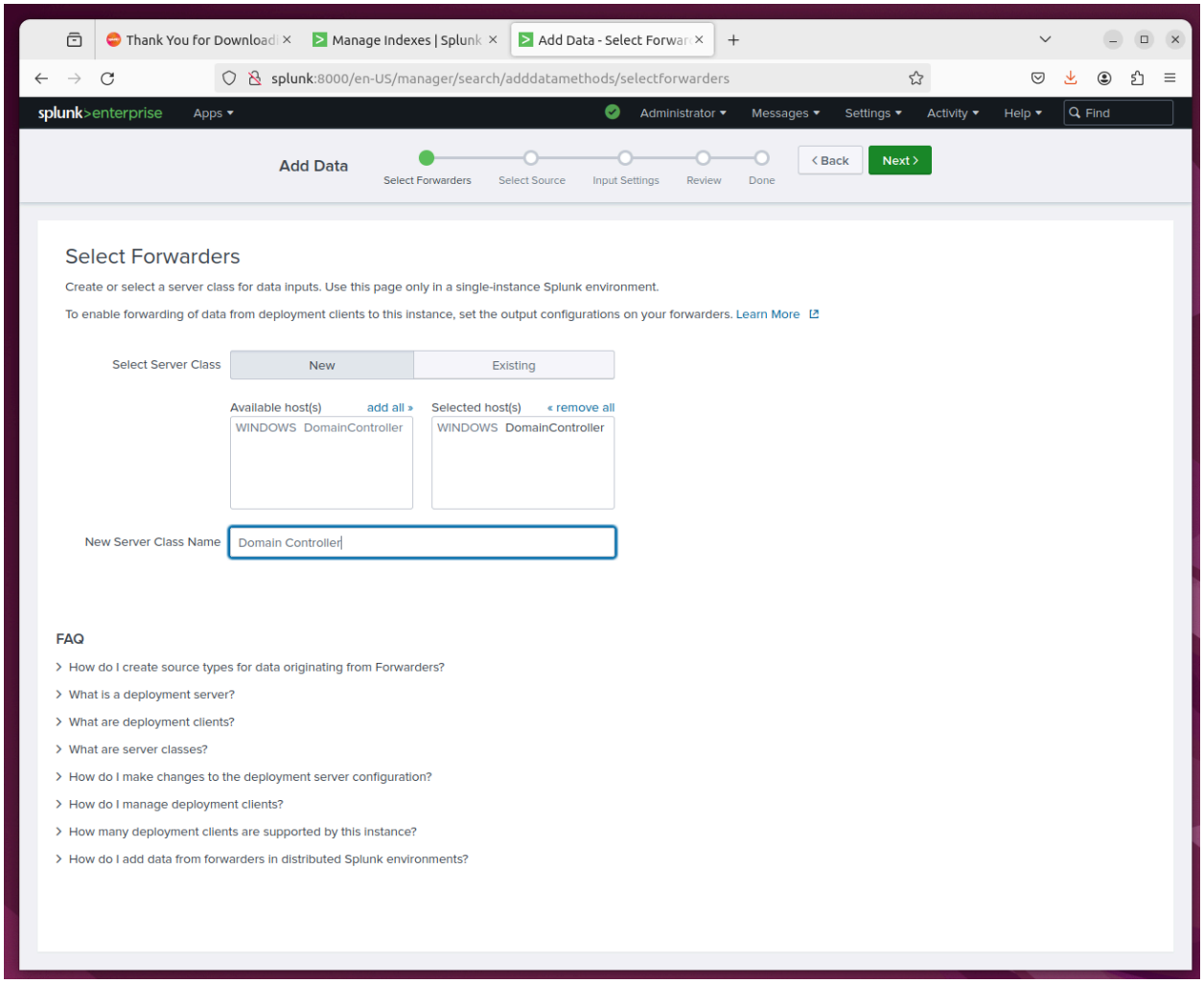

UniversalForwarder Setup
splunk>universal forwarder
If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.
Deployment Server
Hostname or IP
192.168.112.132
:
8089
Enter the hostname or IP of your deployment server, e.g. ds.splunk.com
default is 8089
Cancel
Back
Next



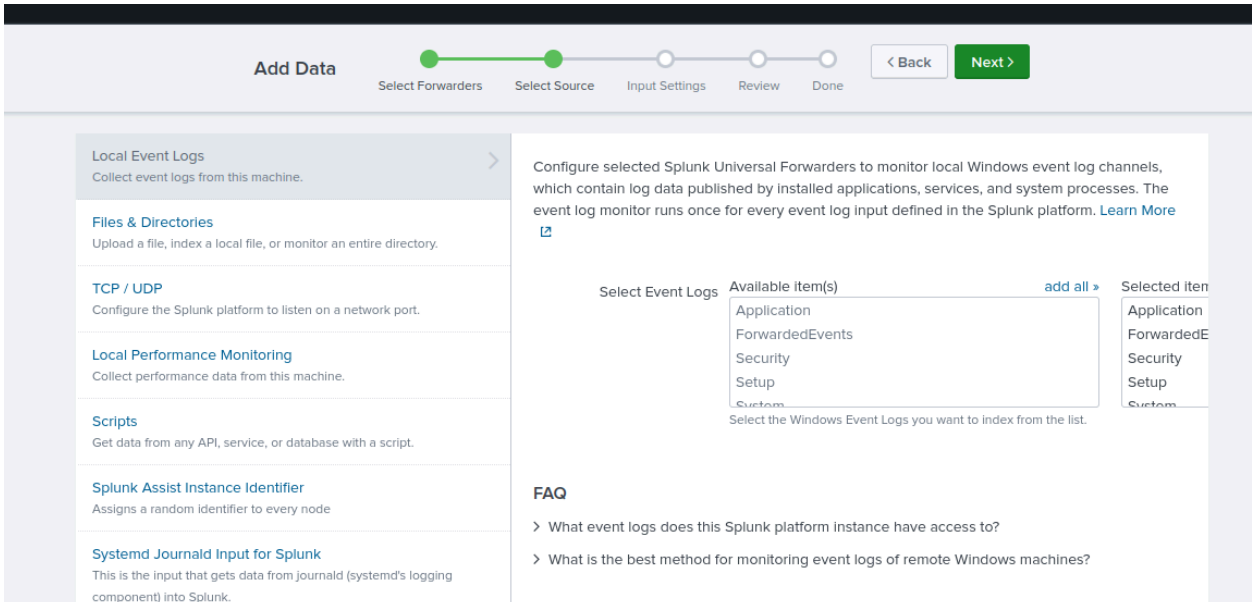
Press “Next” and install. Once completed, go to the **Splunk Instance >> Settings >> Add Data**:



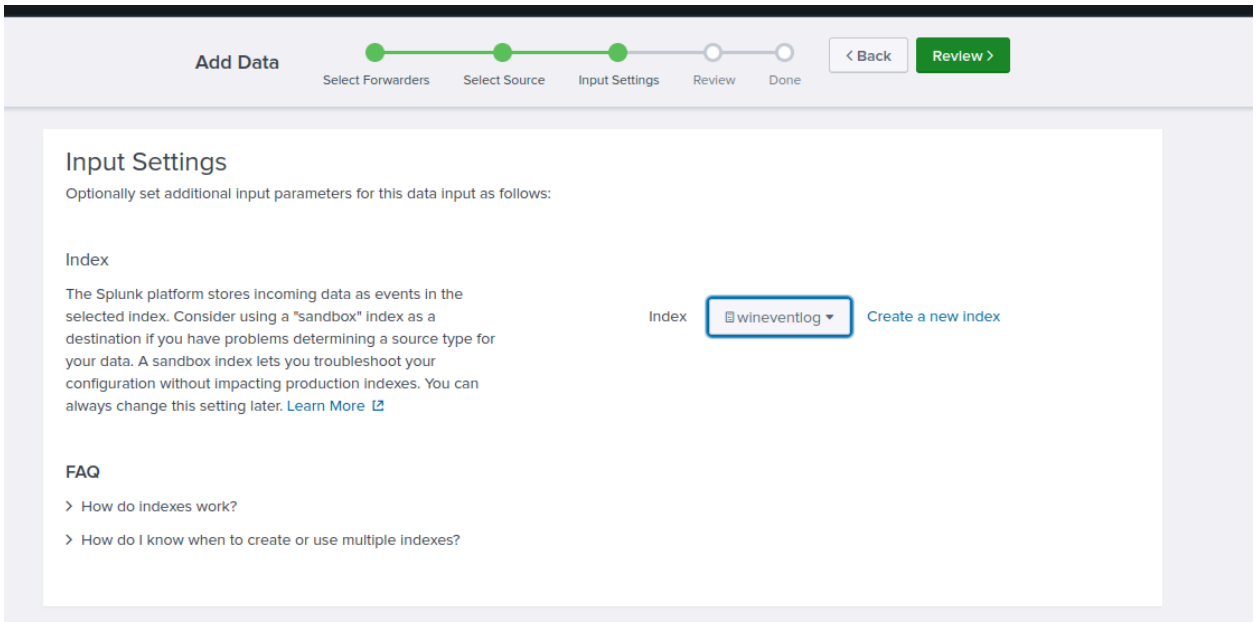
Click “Forward” and select the domain controller and enter a name:



Select which Local Event Logs to keep track of:



Choose the “wineventlog” as the Index:



Click “Review” and then “Submit”