

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](#)

[Configuring Security Onion](#)

[Configure the Security Onion Analyst Machine](#)

[Configuring Kali as the Attack Box](#)

[Configuring pfSense Interface and Firewall Rules](#)

[Configuring Windows Server as a Domain Controller](#)

[Configuring Windows 10 Desktop](#)

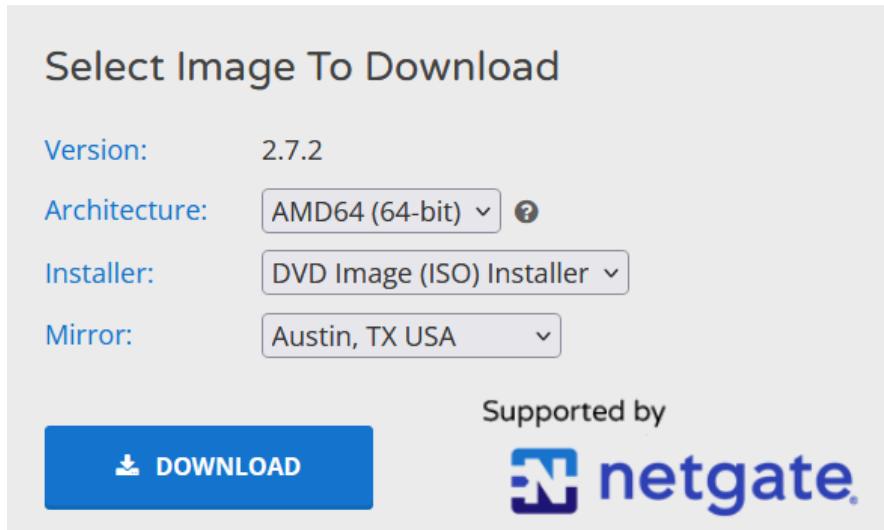
[Configuring Splunk](#)

[Configuring a Universal Forwarder on a Windows Server](#)

Configuring pfSense as a Firewall

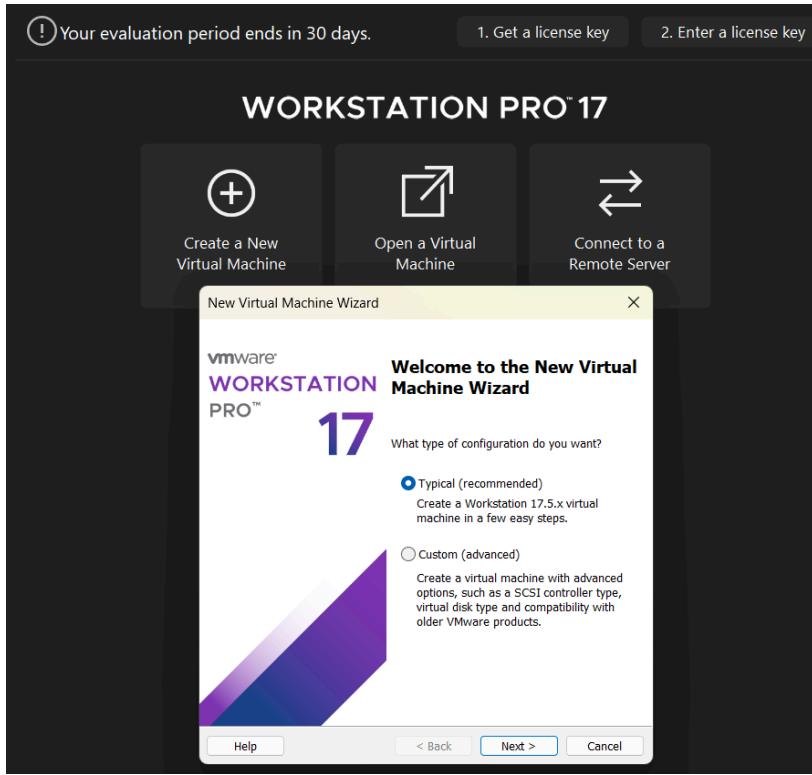
To create the pfSense firewall, we first need to download the ISO file, available on their [website](#).

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

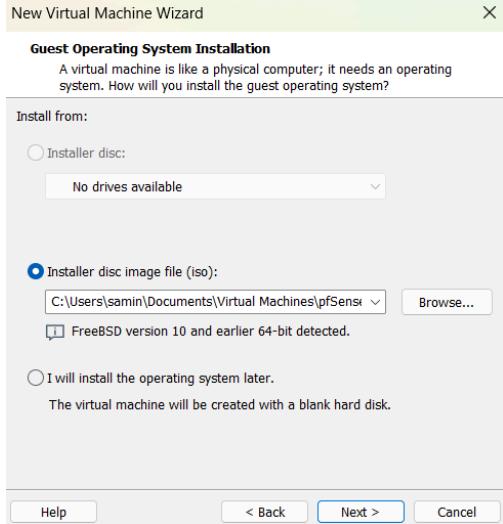


Extracting the downloaded file using the Windows Extractor gave an error, so I used 7zip instead

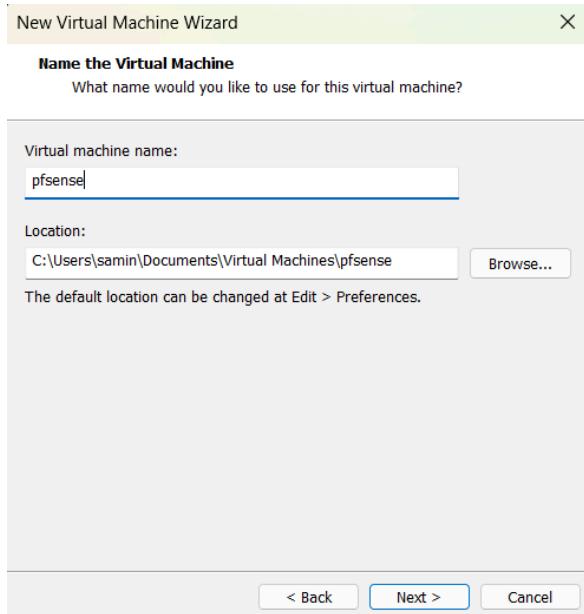
Open up VMWare and click “Create a New Virtual Machine” - ensure the “Typical” is selected before clicking “Next”:



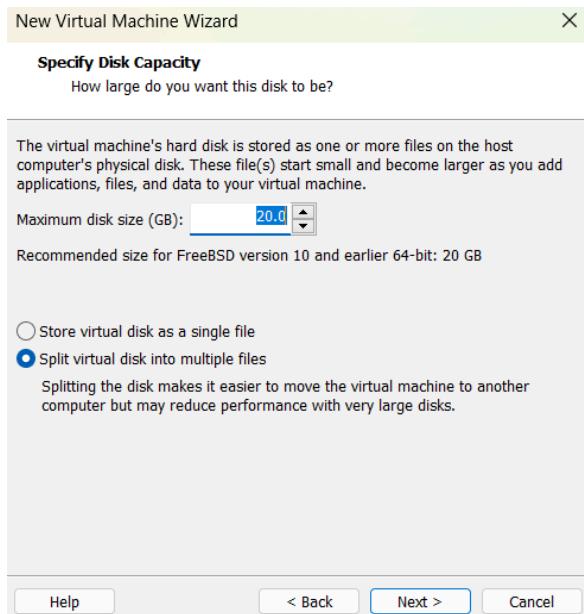
Select the ISO file by clicking “Browse” and browsing to where the file is located before clicking “Next”:



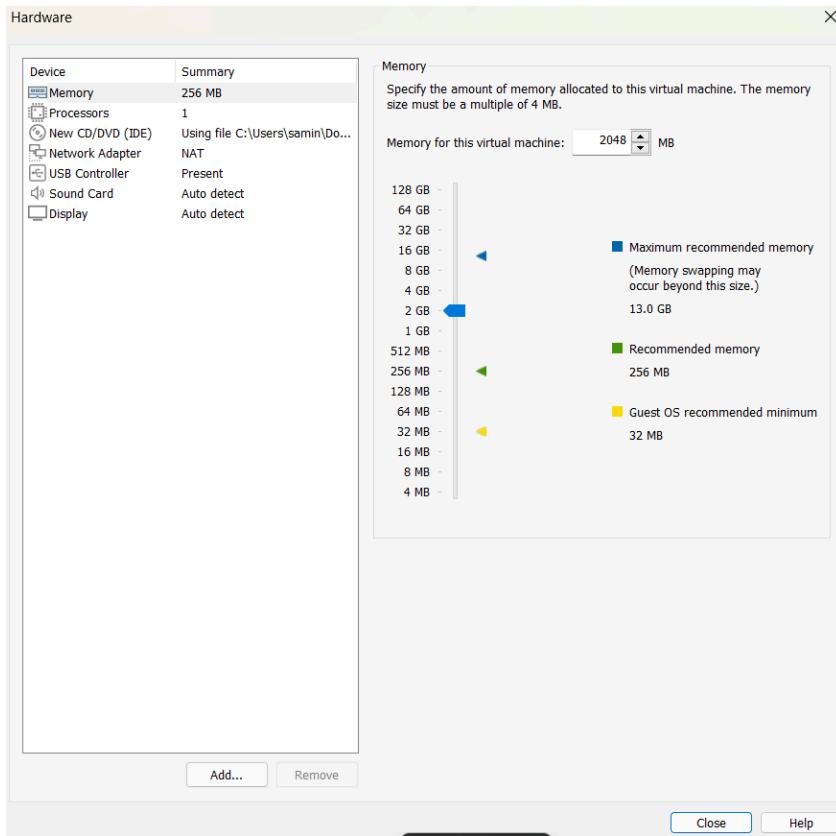
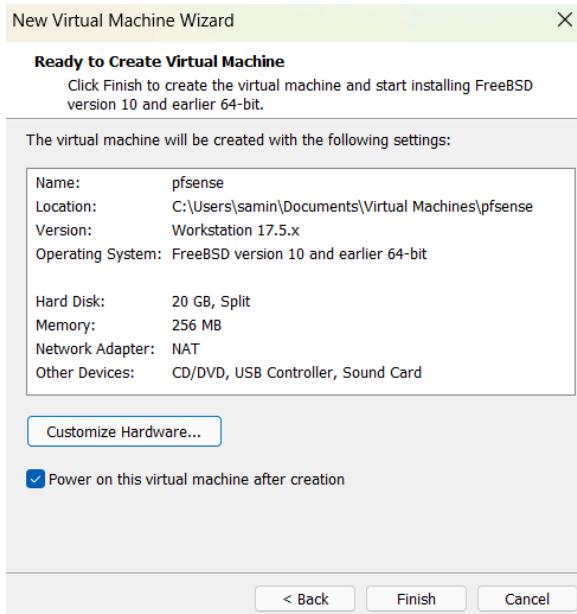
Give your virtual machine a name and a location before clicking next:



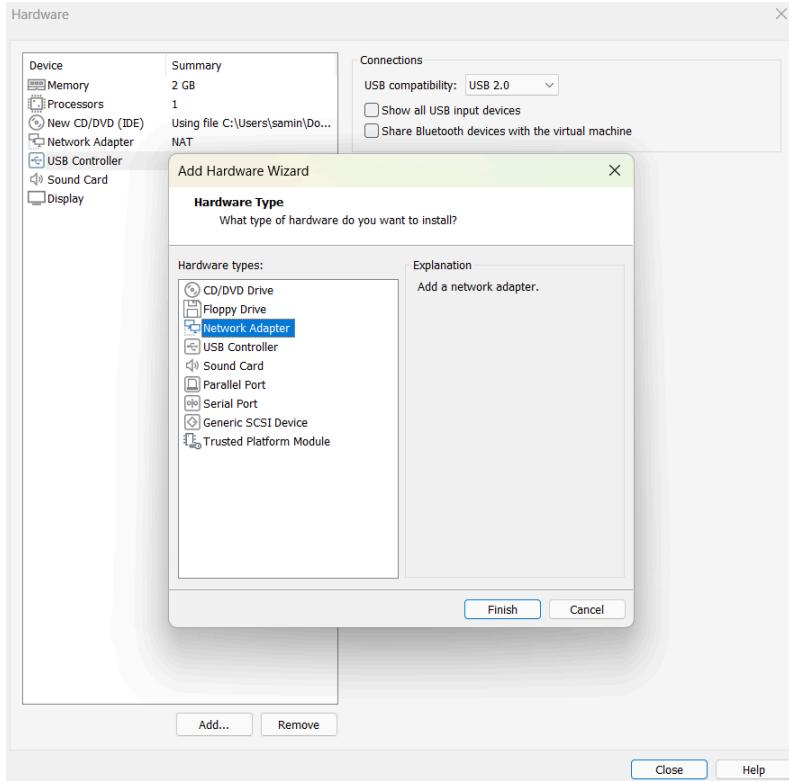
Keep the preselected options and click “Next”:



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



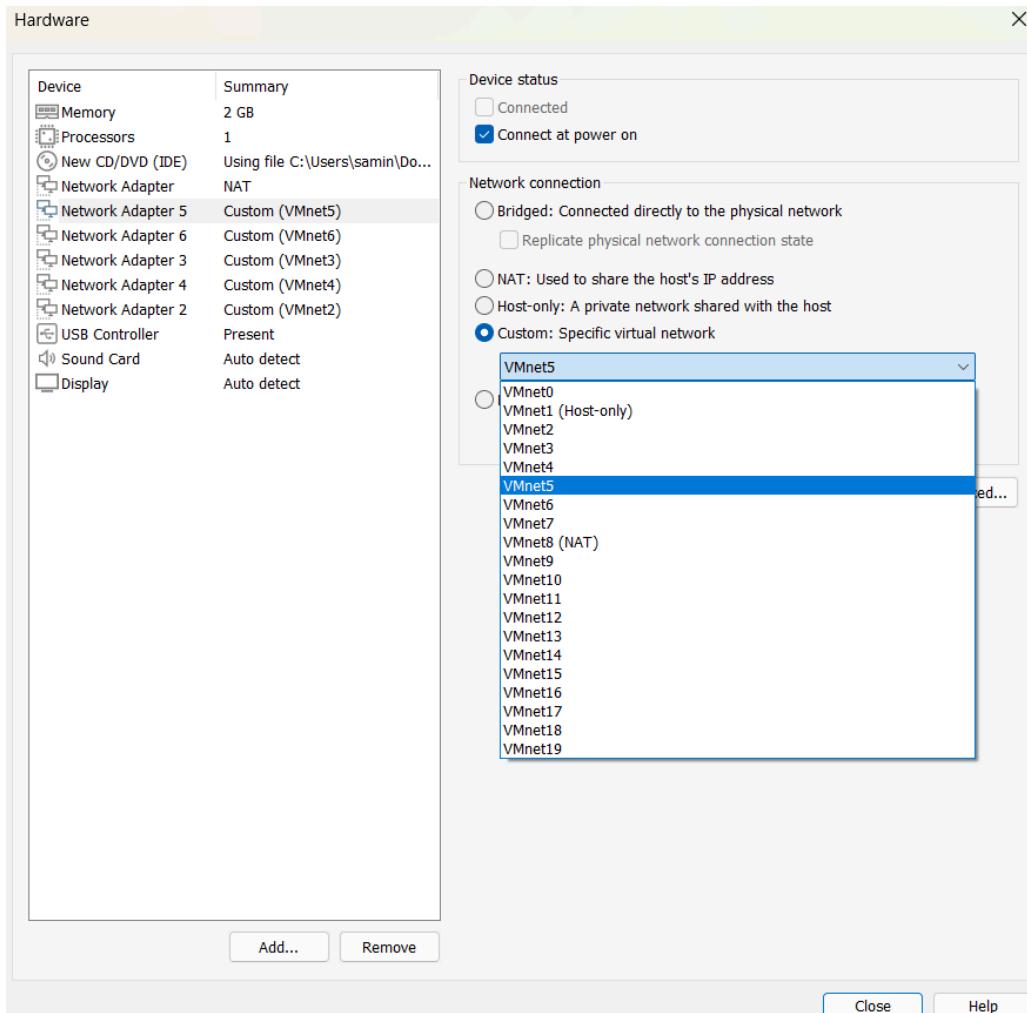
Add a network adapter by clicking "Add", selecting "Network Adapter" and clicking "Finish":



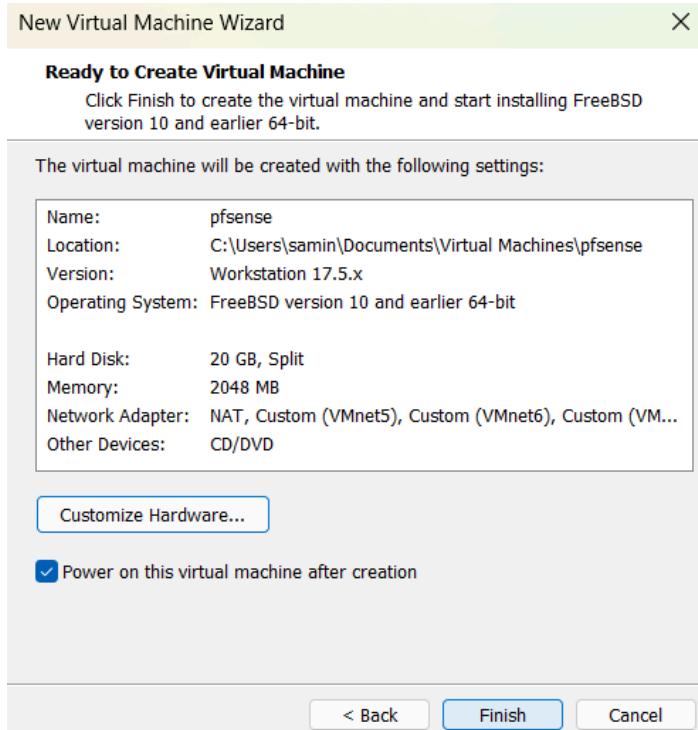
Repeat this 4 more times so that you have 6 network adapters total:

Device	Summary
Memory	2 GB
Processors	1
New CD/DVD (IDE)	Using file C:\Users\samin\Do...
Network Adapter	NAT
Network Adapter 5	NAT
Network Adapter 6	NAT
Network Adapter 3	NAT
Network Adapter 4	NAT
Network Adapter 2	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

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":

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: a5f4f379625442d6778b

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.112.128/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

 0) Logout (SSH only)          9) pfTop
 1) Assign Interfaces          10) Filter Logs
 2) Set interface(s) IP address 11) Restart webConfigurator
 3) Reset webConfigurator password 12) PHP shell + pfSense tools
 4) Reset to factory defaults   13) Update from console
 5) Reboot system               14) Enable Secure Shell (sshd)
 6) Halt system                 15) Restore recent configuration
 7) Ping host                   16) Restart PHP-FPM
 8) Shell

Enter an option: 1
```

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

```
Enter an option: 1

Valid interfaces are:

em0      00:0c:29:34:b1:09    (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:34:b1:13    (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em2      00:0c:29:34:b1:1d    (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em3      00:0c:29:34:b1:27    (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em4      00:0c:29:34:b1:31    (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em5      00:0c:29:34:b1:3b    (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em4 em5 or a): ■
```

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

```
Enter an option: 1

Valid interfaces are:

em0      00:0c:29:34:b1:09    (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1      00:0c:29:34:b1:13    (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em2      00:0c:29:34:b1:1d    (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em3      00:0c:29:34:b1:27    (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em4      00:0c:29:34:b1:31    (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em5      00:0c:29:34:b1:3b    (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\!n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em4 em5 or a): em0■
```

```
NOTE: this enables full Firewalling/NAT mode.  
(em1 em2 em3 em4 em5 a or nothing if finished): em1  
  
Enter the Optional 1 interface name or 'a' for auto-detection  
(em2 em3 em4 em5 a or nothing if finished): em2  
  
Enter the Optional 2 interface name or 'a' for auto-detection  
(em3 em4 em5 a or nothing if finished): em3  
  
Enter the Optional 3 interface name or 'a' for auto-detection  
(em4 em5 a or nothing if finished): em4  
  
Enter the Optional 4 interface name or 'a' for auto-detection  
(em5 a or nothing if finished): em5  
  
The interfaces will be assigned as follows:  
  
WAN -> em0  
LAN -> em1  
OPT1 -> em2  
OPT2 -> em3  
OPT3 -> em4  
OPT4 -> em5  
  
Do you want to proceed [y\?n]? █
```

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

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

```
Writing configuration...done.  
One moment while the settings are reloading... done!  
VMware Virtual Machine - Netgate Device ID: a5f4f379625442d6778b  
  
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.112.128/24  
LAN (lan)      -> em1      -> v4: 192.168.1.1/24  
OPT1 (opt1)    -> em2      ->  
OPT2 (opt2)    -> em3      ->  
OPT3 (opt3)    -> em4      ->  
OPT4 (opt4)    -> em5      ->  
  
0) Logout (SSH only)          9) pfTop  
1) Assign Interfaces          10) Filter Logs  
2) Set interface(s) IP address 11) Restart webConfigurator  
3) Reset webConfigurator password 12) PHP shell + pfSense tools  
4) Reset to factory defaults 13) Update from console  
5) Reboot system              14) Enable Secure Shell (sshd)  
6) Halt system                15) Restore recent configuration  
7) Ping host                  16) Restart PHP-FPM  
8) Shell  
  
Enter an option: 2 █
```

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):

```
Enter an option: 2

Available interfaces:

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

Enter the number of the interface you wish to configure: 2

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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.1.1

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 LAN IPv4 subnet bit count (1 to 32):
> ■
```

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

```
> 192.168.1.1

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 LAN IPv4 subnet bit count (1 to 32):
> 24

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

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

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

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.1.11
Enter the end address of the IPv4 client address range: 192.168.1.200
Disabling IPv6 DHCPD...

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

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:

```

VMWare Virtual Machine - Netgate Device ID: a5f4f379625442d6778b

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.112.128/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2          -> v4: 192.168.2.1/24
OPT2 (opt2)    -> em3          -> v4: 192.168.3.1/24
OPT3 (opt3)    -> em4          ->
OPT4 (opt4)    -> em5          -> v4: 192.168.4.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■

```

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)

2.3.280-20231128 ISO image built on 2023/11/28

Download and Verify

2.3.280-20231128 ISO image:

<https://download.securityonion.net/file/securityonion/securityonion-2.3.280-20231128.iso>

MD5: 0BC68BD73547B7E2FBA6F53BEC174590

SHA1: 1D33C565D37772FE7A3C3FE3ECB05FC1AC1EBFF1

SHA256: ADBD9DC9E1B266B18EOFDBDF084073EF926C565041858060D283CDAEF021EE11

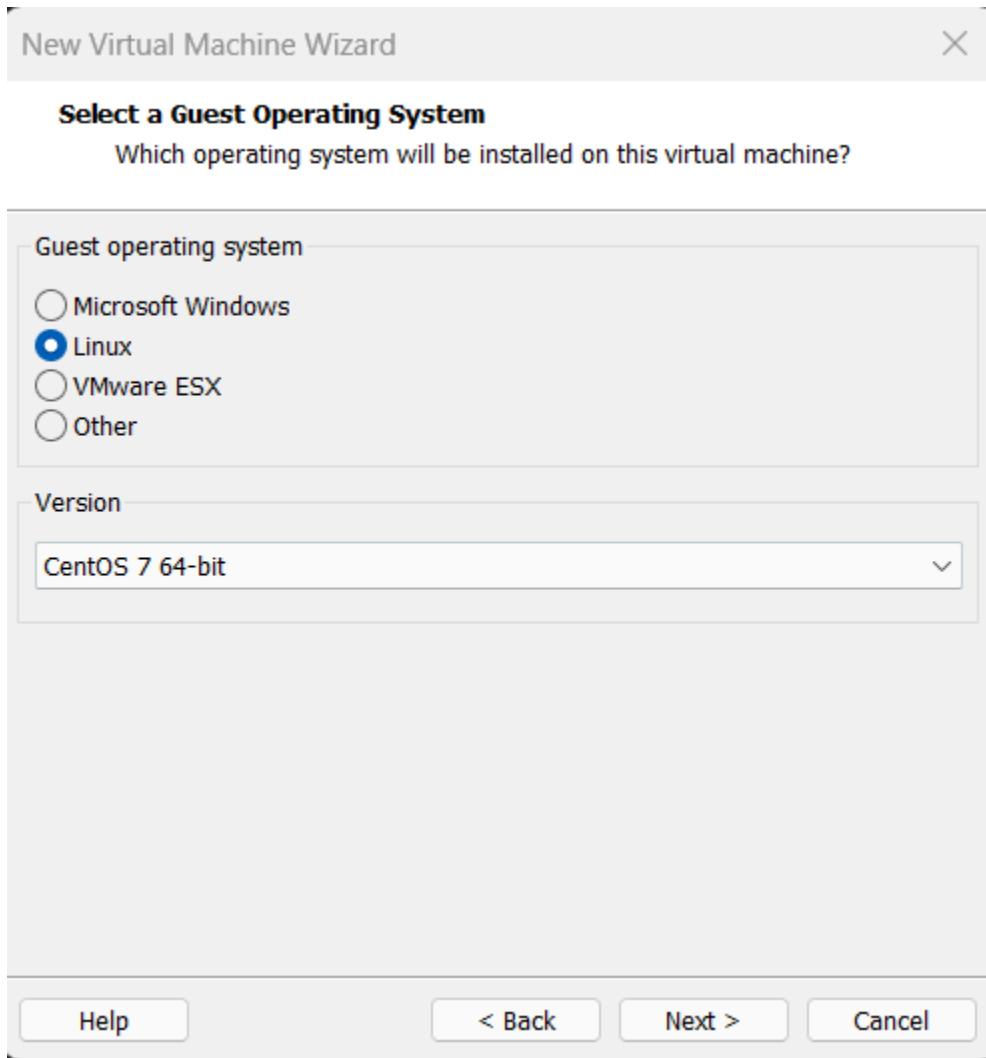
Signature for ISO image:

<https://github.com/Security-Onion-Solutions/securityonion/raw/master/sigs/securityonion-2.3.280-20231128.iso.sig>

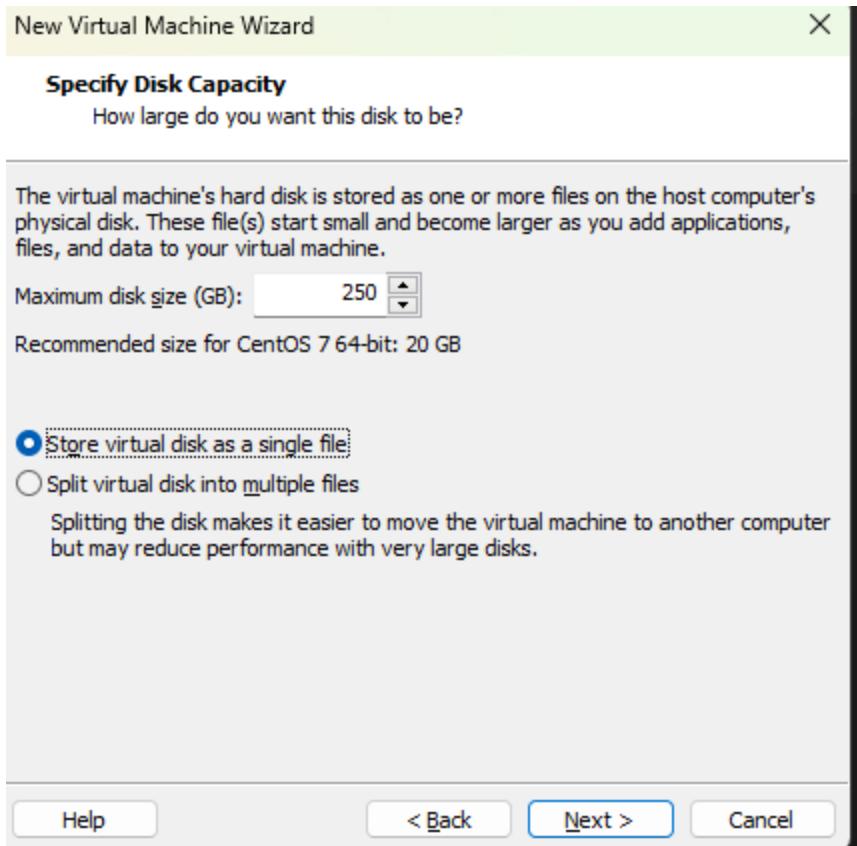
Signing key:

<https://raw.githubusercontent.com/Security-Onion-Solutions/securityonion/master/KEYS>

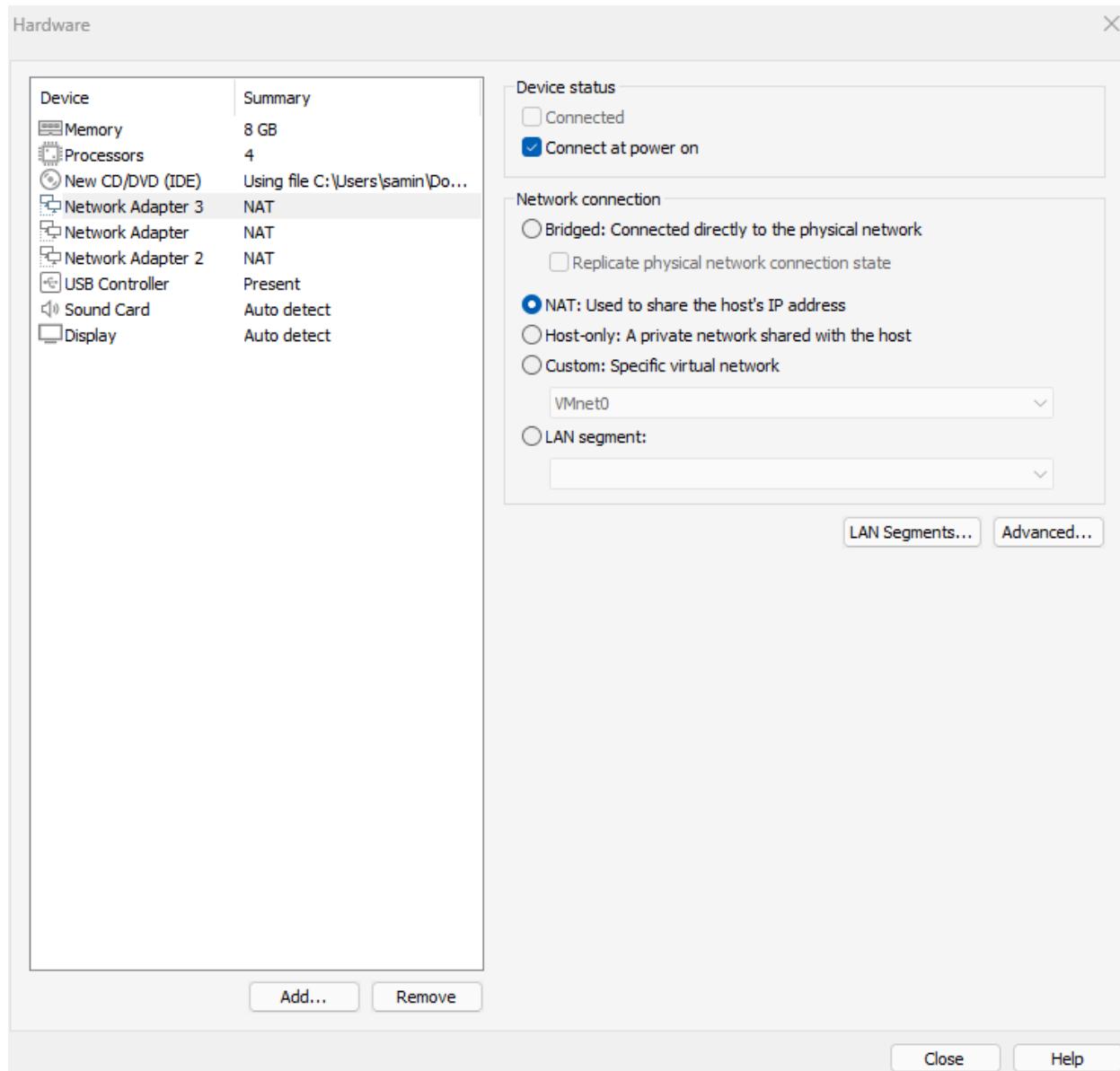
Set up a new virtual machine in VMWare as done above (with pfSense) with “Typical” selected on the first screen, and then select the disc image from where you downloaded it. When it asks to select a guest operating system, use the configuration below:



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:

Device	Summary
Memory	8 GB
Processors	4
New CD/DVD (IDE)	Using file C:\Users\samin\Do...
Network Adapter 3	Custom (VMnet5)
Network Adapter	NAT
Network Adapter 2	Custom (VMnet4)
Display	Auto detect

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.

```
#####
##      ** W A R N I N G **      ##
##      _____      ##
##      Installing the Security Onion ISO      ##
## on this device will DESTROY ALL DATA      ##
##      and partitions!      ##
##      ##      ##
##      ** ALL DATA WILL BE LOST **      ##
#####
Do you wish to continue? (Type the entire word 'yes' to proceed.) yes

A new administrative user will be created. This user will be used for setting up and administering S
ecurity Onion.

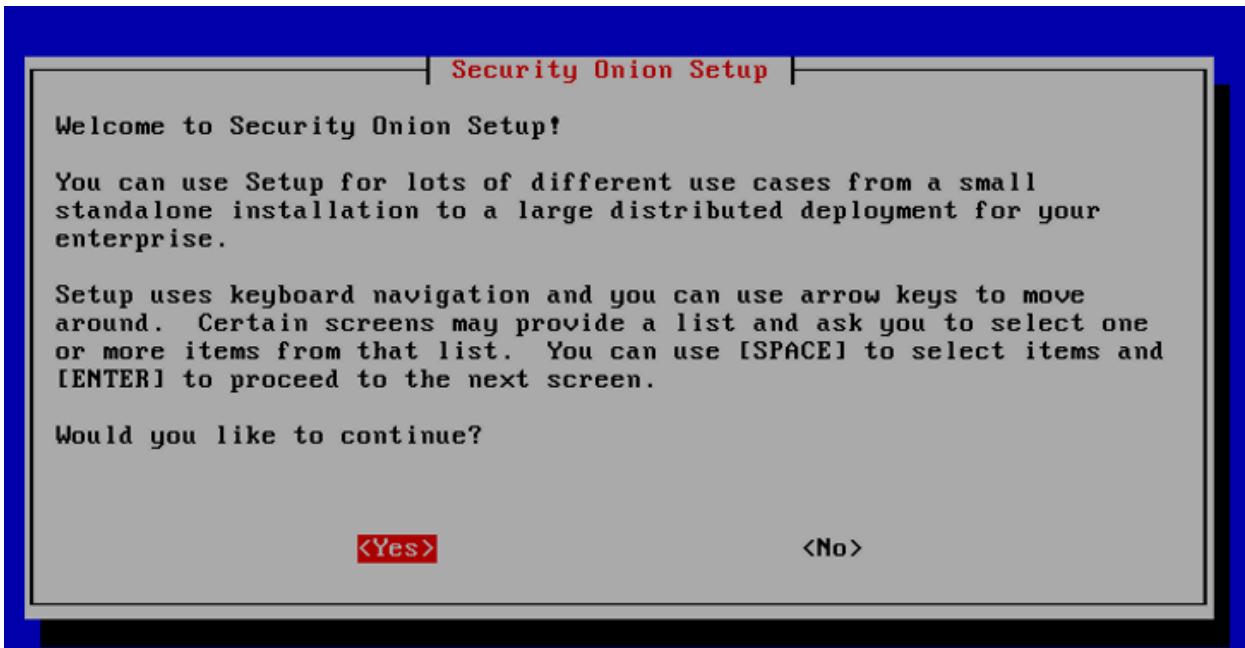
Enter an administrative username: samin

Let's set a password for the samin user:

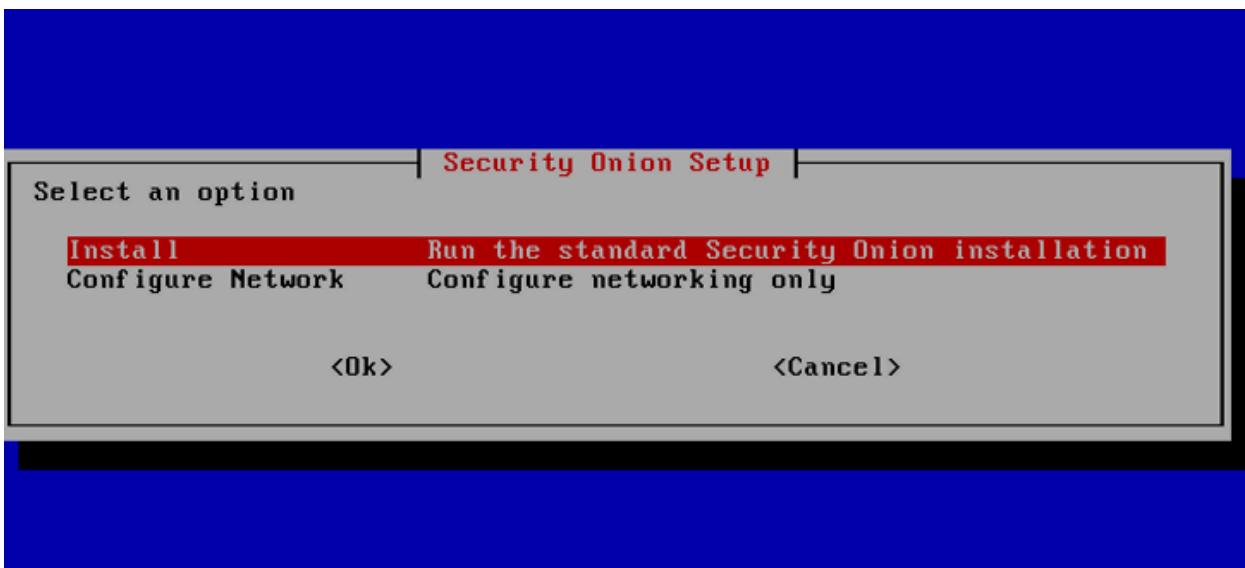
Enter a password:
Re-enter the password: _
```

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

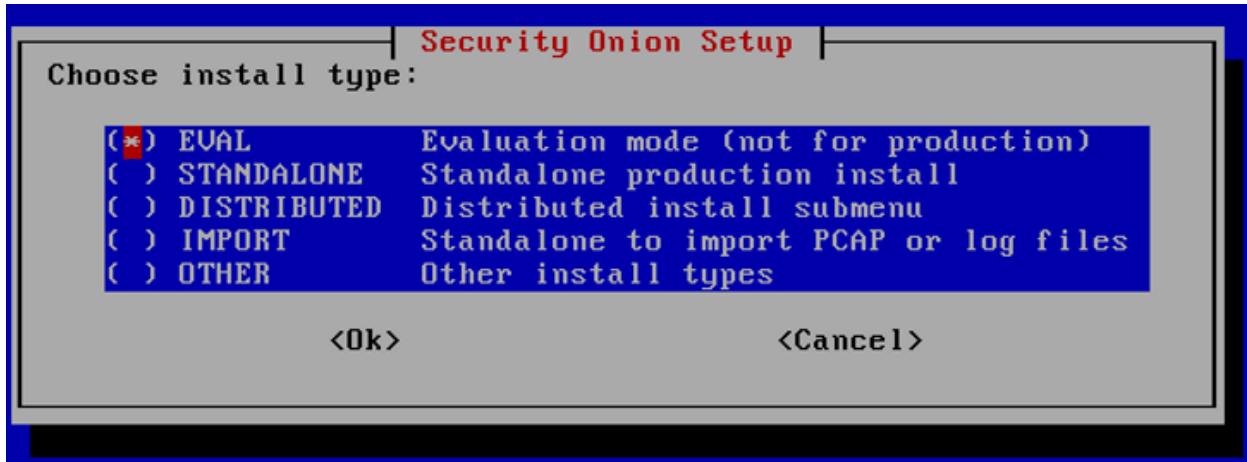
Select “Yes” by pressing enter on the next screen:



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



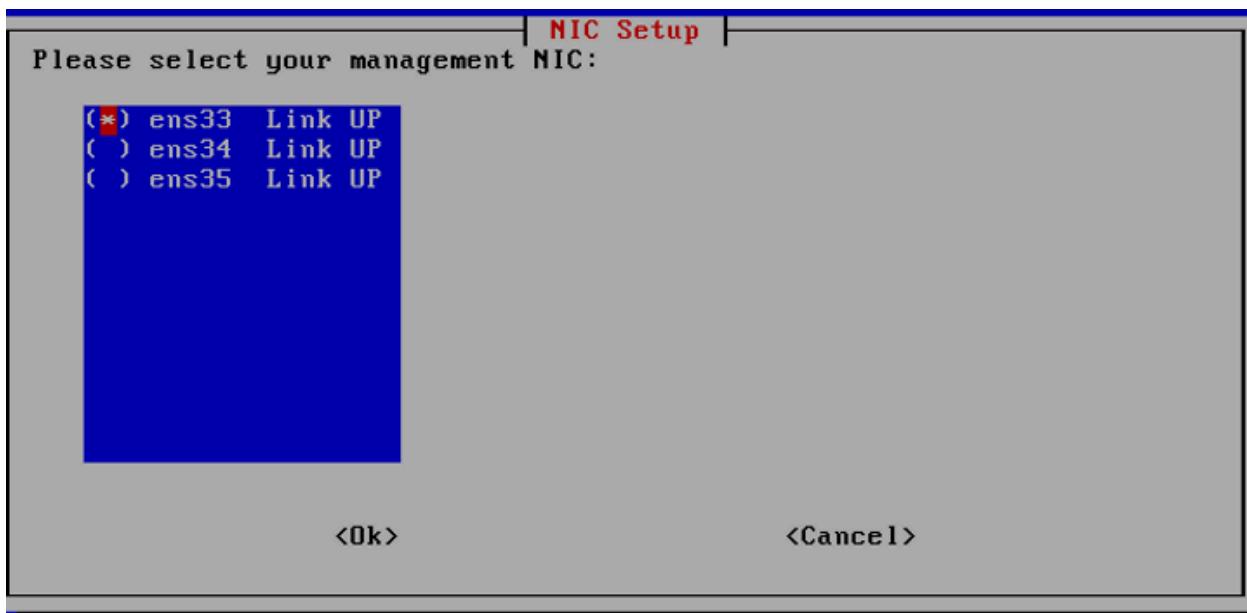
Ensure the “EVAL” option is selected before pressing enter on the screen after:



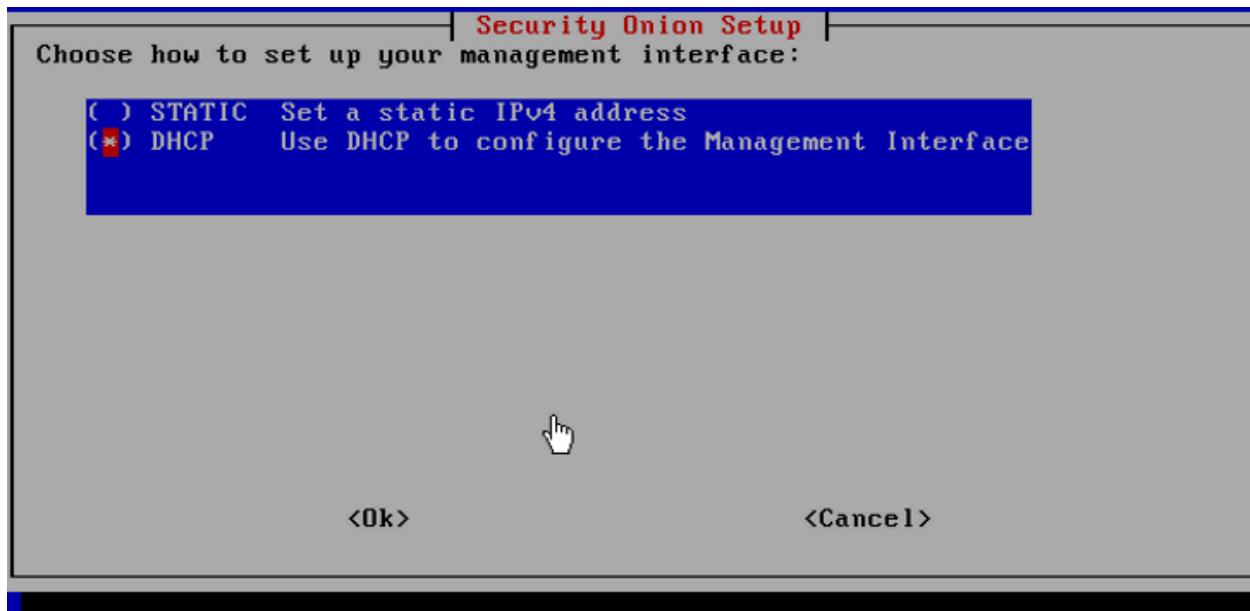
Type out "AGREE" when prompted. Select "Standard" on the next screen:



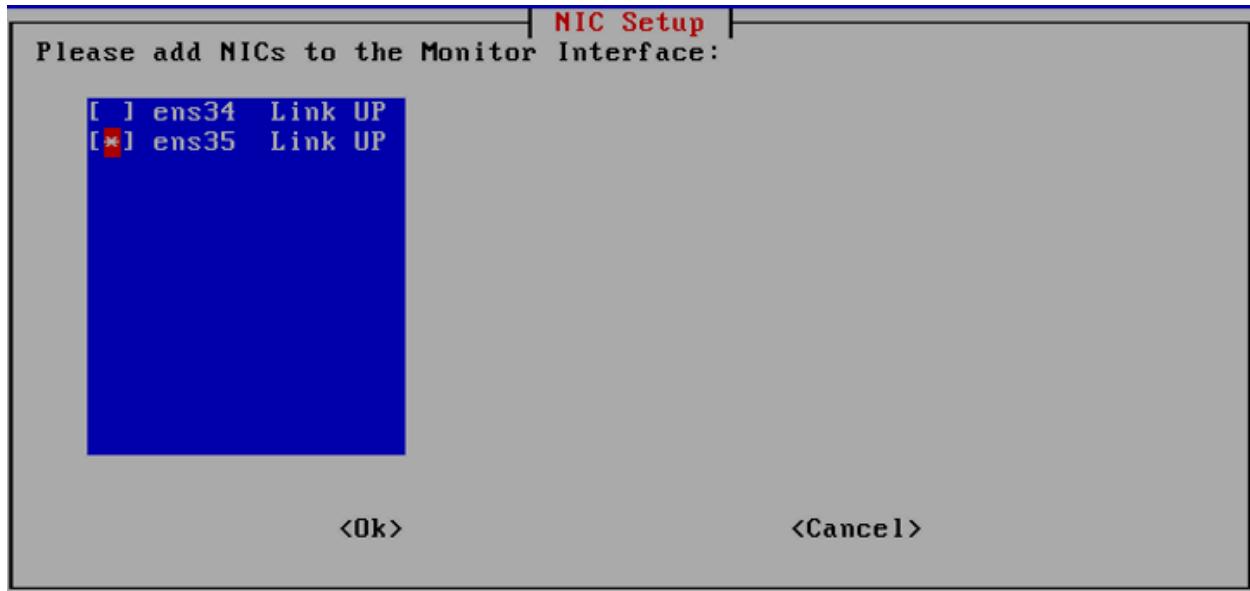
Create a hostname when asked. Select "ens33" on the next screen:



Select “DHCP” on the next screen:

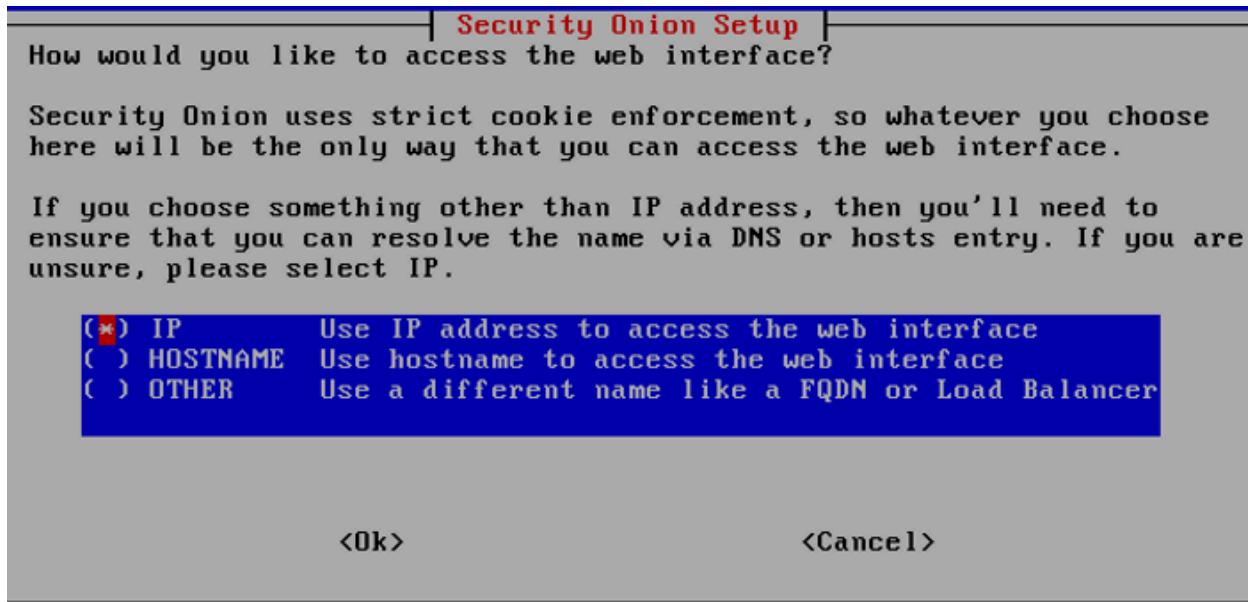


Select “YES”, “OK”, and then “Direct” for the next 3 prompts. Then select “ens35” at the next prompt:



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](#):

Ubuntu 22.04.3 LTS

The latest [LTS](#) version of Ubuntu, for desktop PCs and laptops. LTS stands for long-term support — which means five years of free security and maintenance updates, guaranteed until April 2027.

[Ubuntu 22.04 LTS release notes](#)

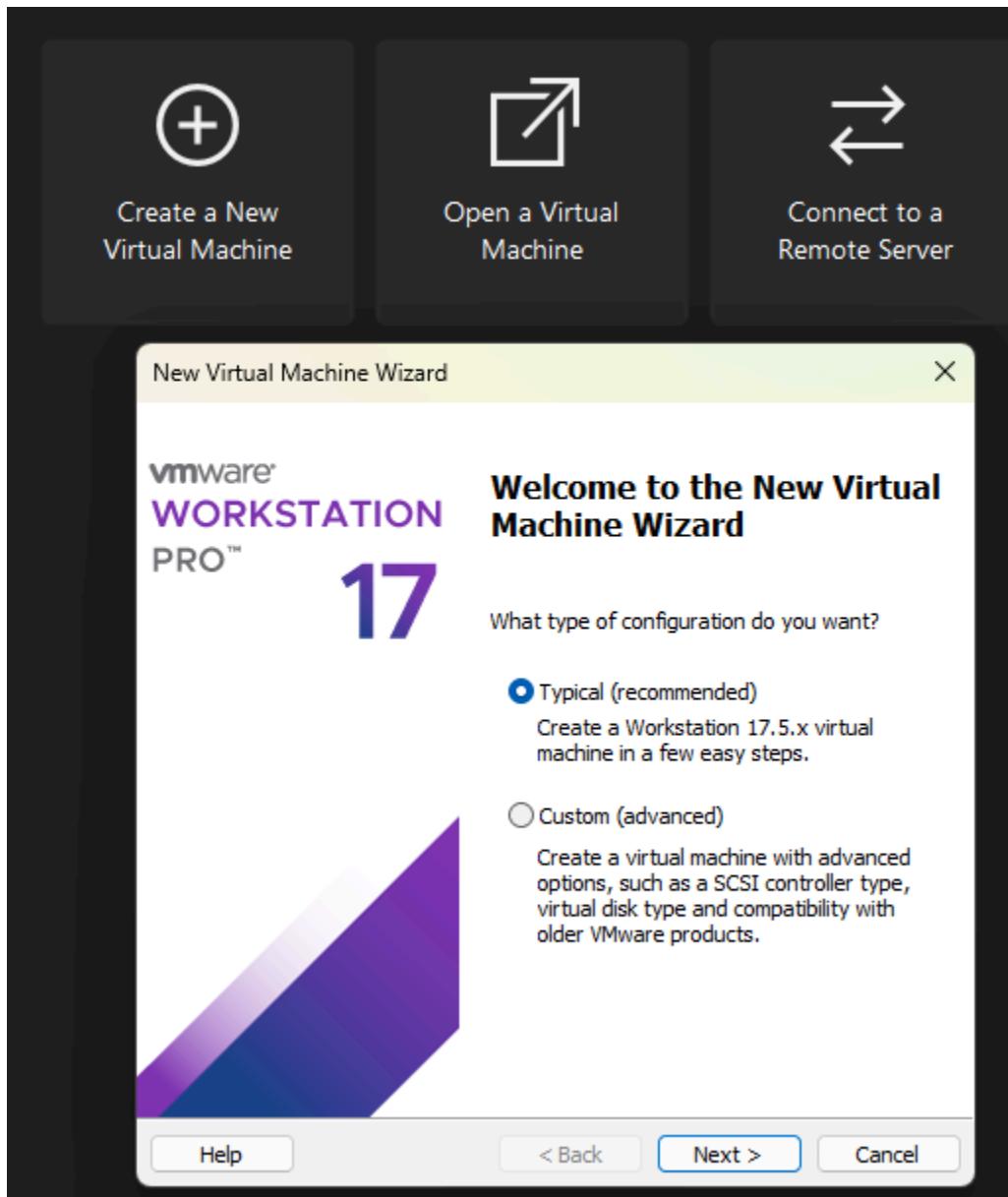
Recommended system requirements:

⦿ 2 GHz dual-core processor or better	⦿ Internet access is helpful
⦿ 4 GB system memory	⦿ Either a DVD drive or a USB port for the installer media
⦿ 25 GB of free hard drive space	

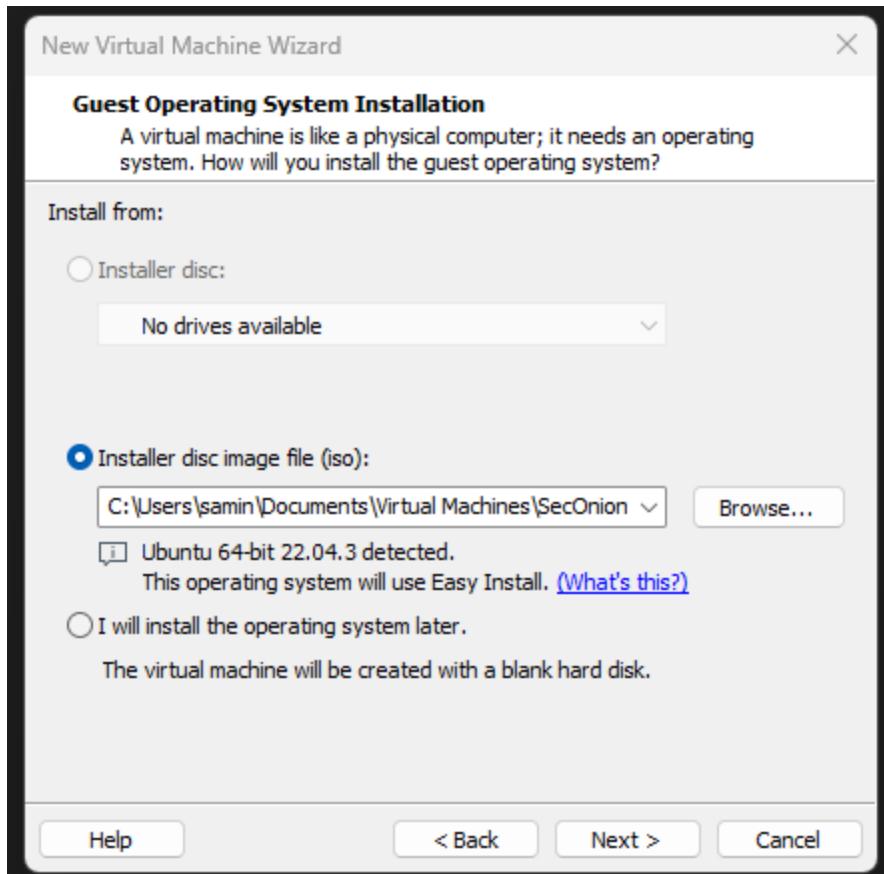
[Download 22.04.3](#)

For other versions of Ubuntu Desktop including torrents, the network installer, a list of local mirrors and past releases see our [alternative downloads](#).

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”:

New Virtual Machine Wizard

X

Easy Install Information

This is used to install Ubuntu 64-bit.

Personalize Linux

Full name: SecOnionMgmt

User name: samin

Password: *****

Confirm: *****|

Help

< Back

Next >

Cancel

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

New Virtual Machine Wizard

X

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:

SecOnionMgmt

Location:

C:\Users\samin\Documents\Virtual Machines\SecOnion Ubuntu

[Browse...](#)

The default location can be changed at [Edit > Preferences](#).

[< Back](#)

[Next >](#)

[Cancel](#)

The next two screens you can leave at the defaults:

New Virtual Machine Wizard

X

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): 

Recommended size for Ubuntu 64-bit: 20 GB

Store virtual disk as a single file

Split virtual disk into multiple files

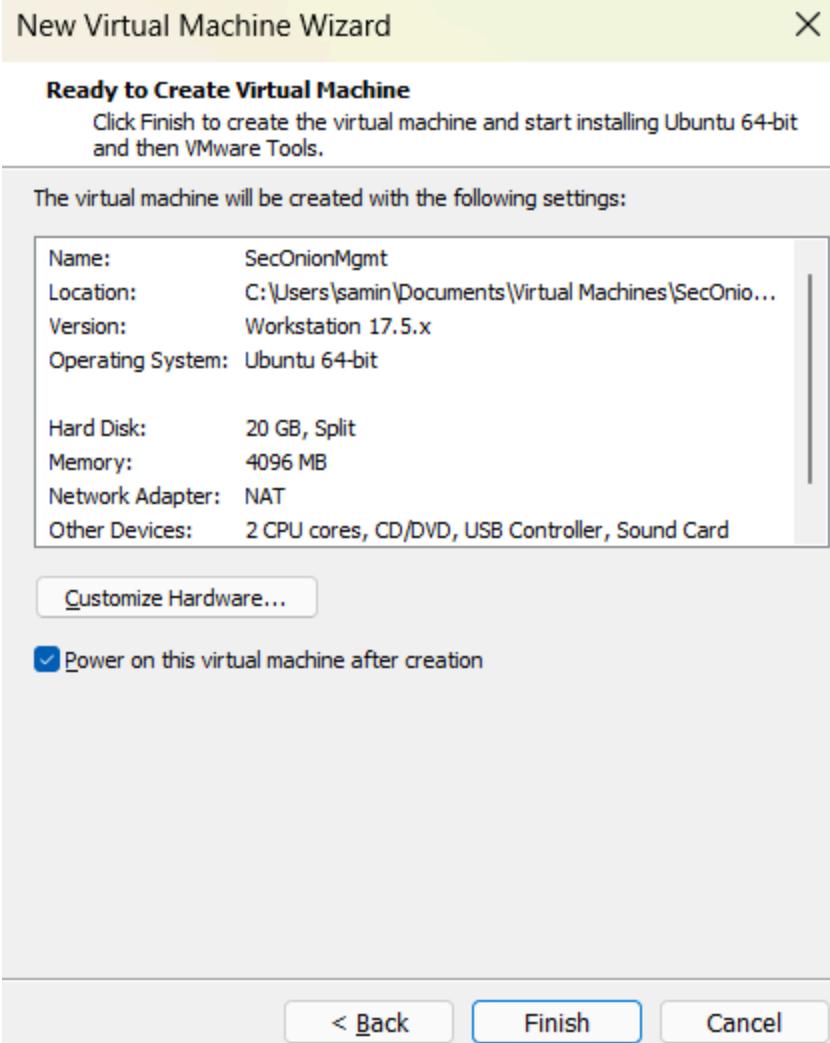
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

[Help](#)

[< Back](#)

[Next >](#)

[Cancel](#)

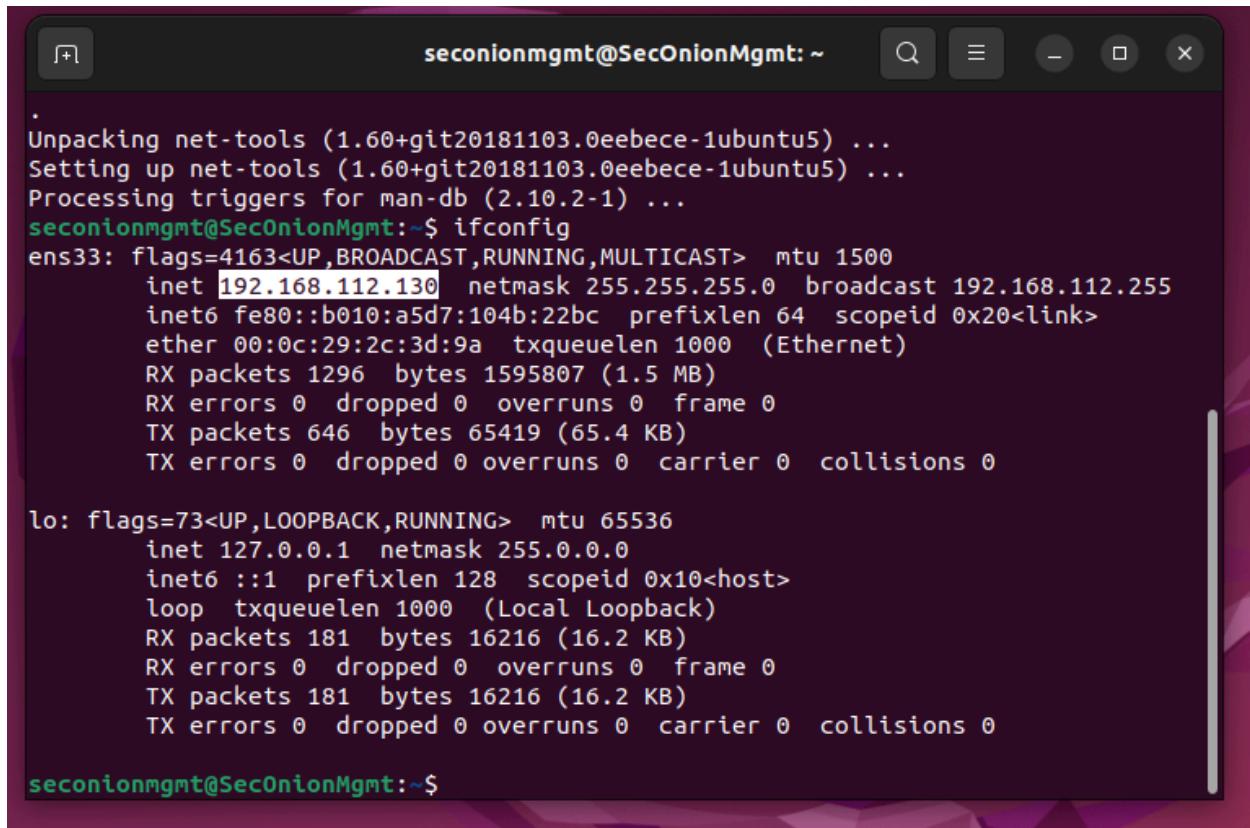


Load up the virtual machine and configure it as you wish; for this lab, all the default options were used (ignore any warnings about overwriting the defaults). Once you are able to log into the machine, open up a terminal and enter “`sudo apt install net-tools`”:

```
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:



A terminal window titled "seconionmgmt@SecOnionMgmt: ~" displaying the output of the "ifconfig" command. The window shows network interface details for ens33 (Ethernet) and lo (Loopback). The ens33 interface has an IP address of 192.168.112.130. The lo interface has an IP address of 127.0.0.1. Both interfaces show standard statistics like RX/TX bytes, errors, and collisions.

```
.  
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:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
      inet 192.168.112.130 netmask 255.255.255.0 broadcast 192.168.112.255  
        inet6 fe80::b010:a5d7:104b:22bc prefixlen 64 scopeid 0x20<link>  
          ether 00:0c:29:2c:3d:9a txqueuelen 1000 (Ethernet)  
            RX packets 1296 bytes 1595807 (1.5 MB)  
            RX errors 0 dropped 0 overruns 0 frame 0  
            TX packets 646 bytes 65419 (65.4 KB)  
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
      inet 127.0.0.1 netmask 255.0.0.0  
        inet6 ::1 prefixlen 128 scopeid 0x10<host>  
          loop txqueuelen 1000 (Local Loopback)  
            RX packets 181 bytes 16216 (16.2 KB)  
            RX errors 0 dropped 0 overruns 0 frame 0  
            TX packets 181 bytes 16216 (16.2 KB)  
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
seconionmgmt@SecOnionMgmt:~$
```

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.105.1.el7.x86_64 on an x86_64

seconion login: samin
Password:
Last login: Wed Jan 24 21:15:33 on tty1

Access the Security Onion web interface at https://192.168.112.129
(You may need to run so-allow first if you haven't yet)

[samin@seconion ~]$ sudo so-allow

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for samin:

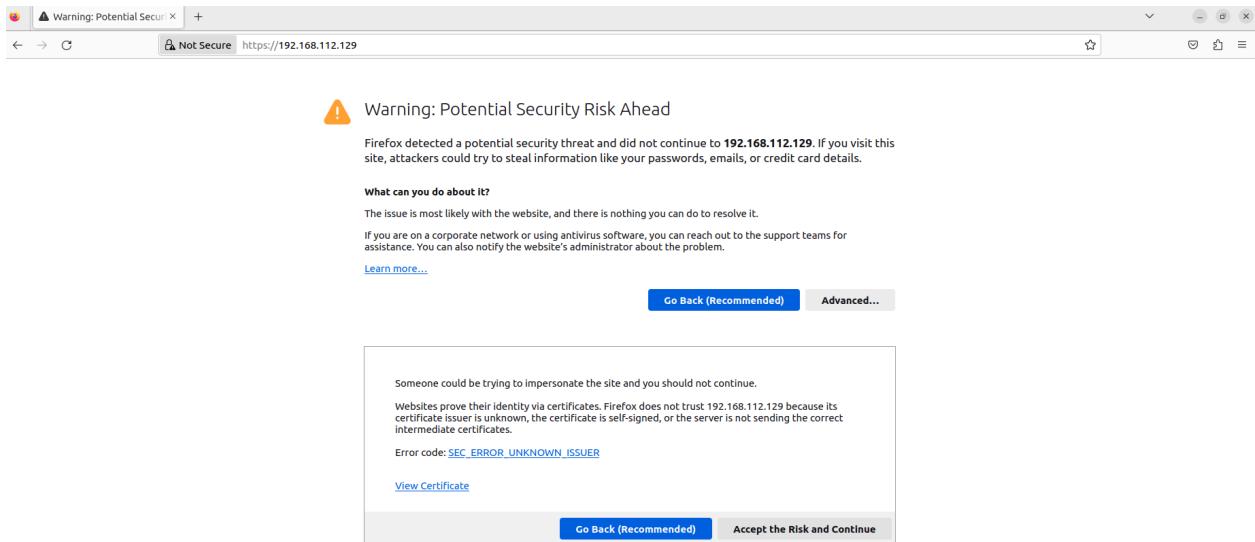
Choose the role for the IP or Range you would like to allow

[a] - Analyst - 80/tcp, 443/tcp
[b] - Logstash Beat - 5044/tcp
[e] - Elasticsearch REST API - 9200/tcp
[f] - Strelka frontend - 57314/tcp
[o] - Osquery endpoint - 8890/tcp
[s] - Syslog device - 514/tcp/udp
[w] - Wazuh agent - 1514/tcp/udp
[p] - Wazuh API - 55000/tcp
[r] - Wazuh registration service - 1515/tcp

Please enter your selection: 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

Alerts

Total Found: 18

Group By Name, Module

Last 24 hours

REFRESH

Fetch Limit: 500

Click the clock icon to change to absolute time

Count rules.name event.module event.severity_label

rules.name	event.module	event.severity_label
System Audit event.	ossec	low
PAM: Login session opened.	ossec	low
Ossec server started.	ossec	low
Listened ports status (netstat) changed (new port opened or closed).	ossec	low
Successful sudo to ROOT executed.	ossec	low
CyberChef	ossec	low
PAM: Login session closed.	ossec	low
Ossec agent started.	ossec	low
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

Filter your data using KQL syntax

Last 24 hours

Logs Over Time

Count: 1,819

Logs Over Time (Count vs timestamp per 30 minutes)

Security Onion - Data Overview

host (red), database (blue), network (green)

Security Onion - Dataset

Dataset	Count
syscollector	742
access	308
elasticsearch.server	243
ossec	199
kibana.log	157
application	77
audit	63

Security Onion - Modules

Module	Count
ossec	967
kratos	448
elasticsearch	243
kibana	157
zeek	4

Security Onion - Log Count By Node

Node	Count
seconion	4

Home > Dashboards > Dashboards > Security Onion Grid Overview

Node All Role All Docker Containers All Disk All

Last 3 hours

Overview

System Uptime

Container Uptime Current

CPU Usage

Name Max Mean Last *

seconion eval so-playbook 19.9 min

seconion eval so-wazuh 19.9 min

seconion eval so-socotpus 20.0 min

seconion eval so-fleet 20.0 min

seconion eval so-redis 20.1 min

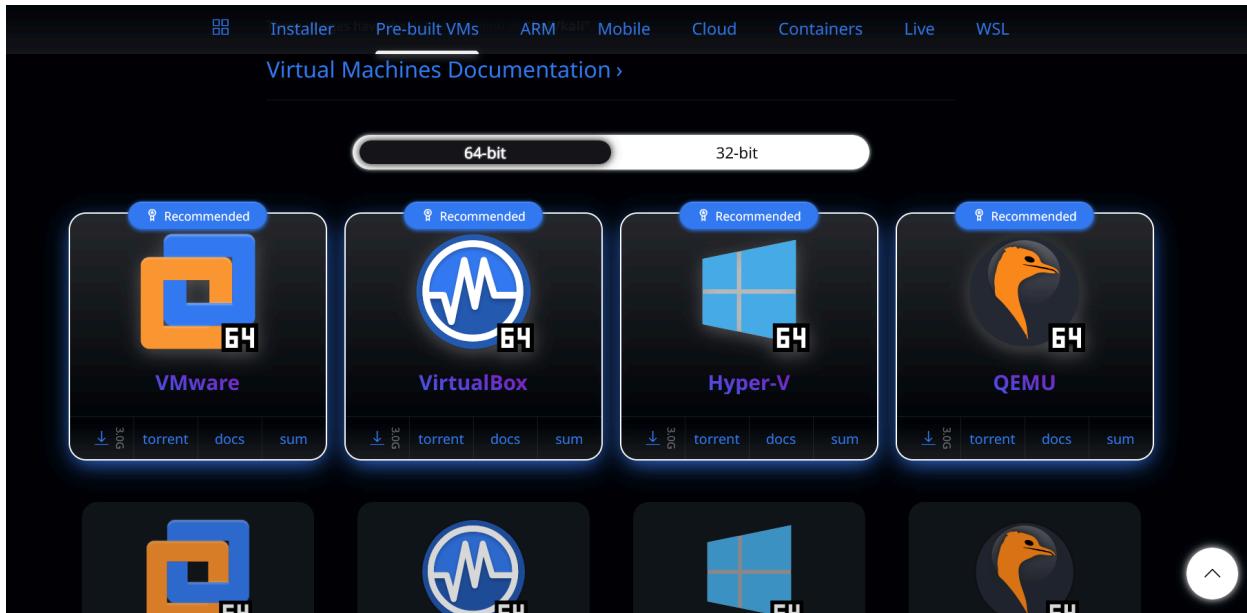
seconion eval so-elastalert 20.2 min

seconion eval so-curator 20.2 min

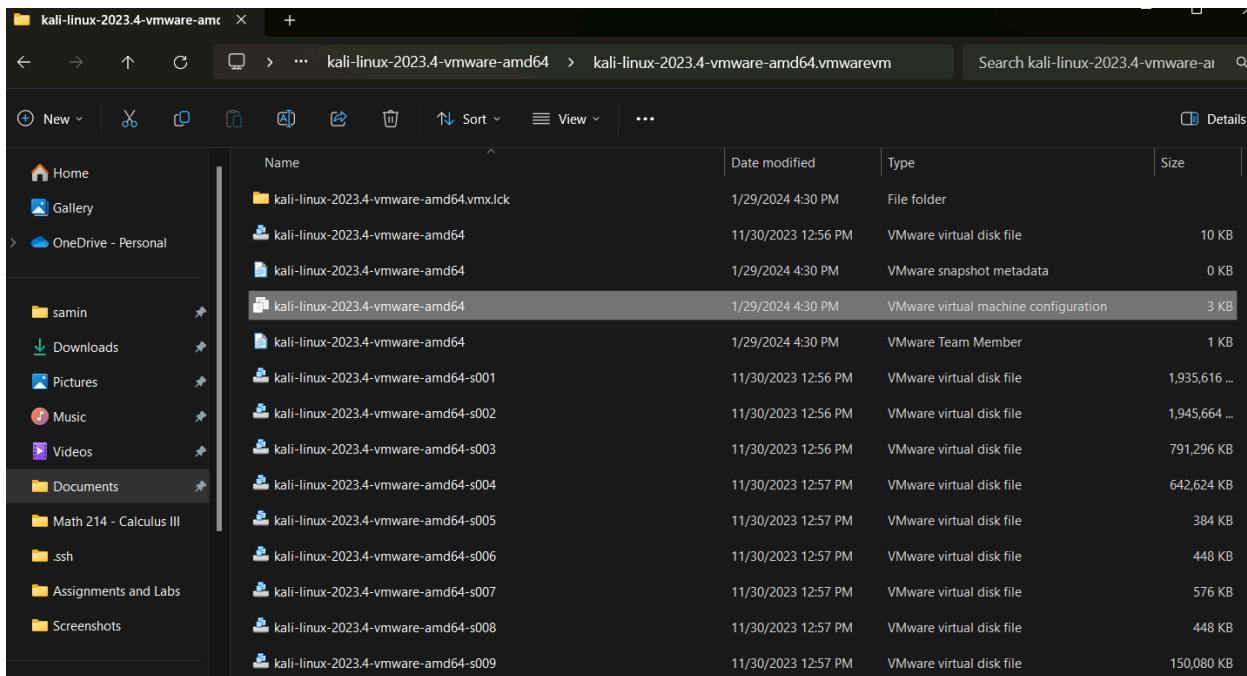
seconion eval so-filebeat 21.2 min

Configuring Kali as the Attack Box

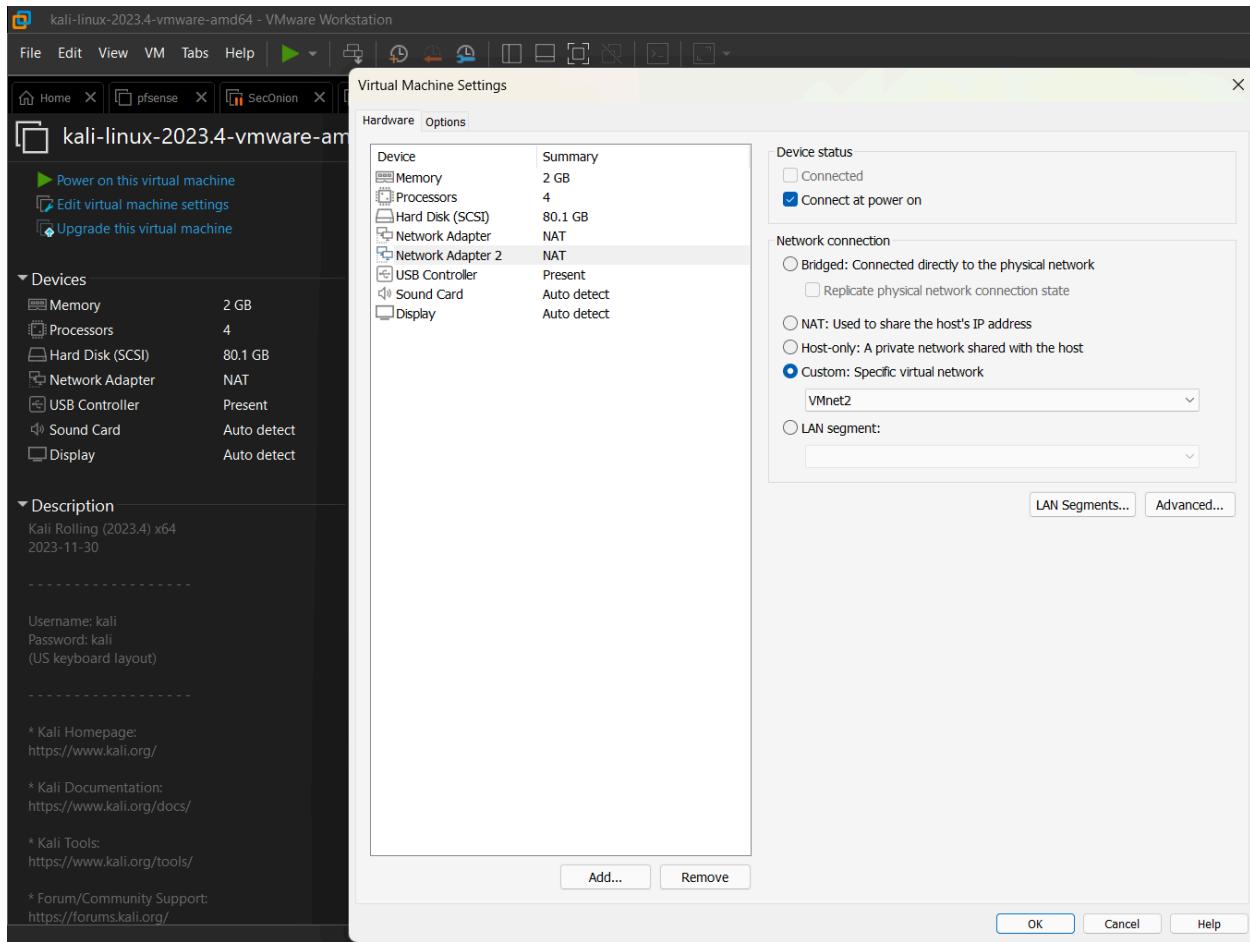
First we will need to download the Kali image, which can be found on their [website](#). For this lab, we will be downloading the VMware 64 bit version:



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



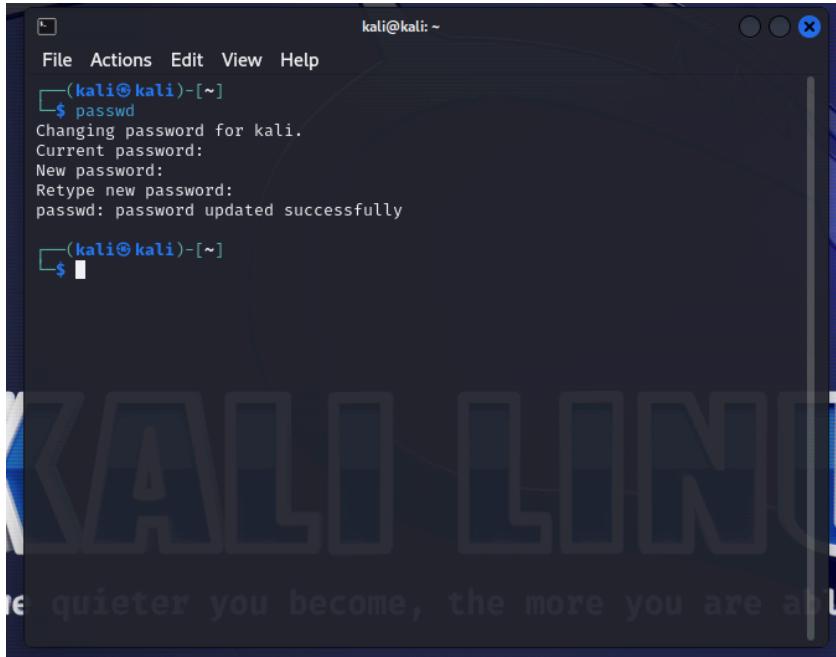
Edit the virtual machine settings to add another Network Adapter and map it to VMnet2:



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:



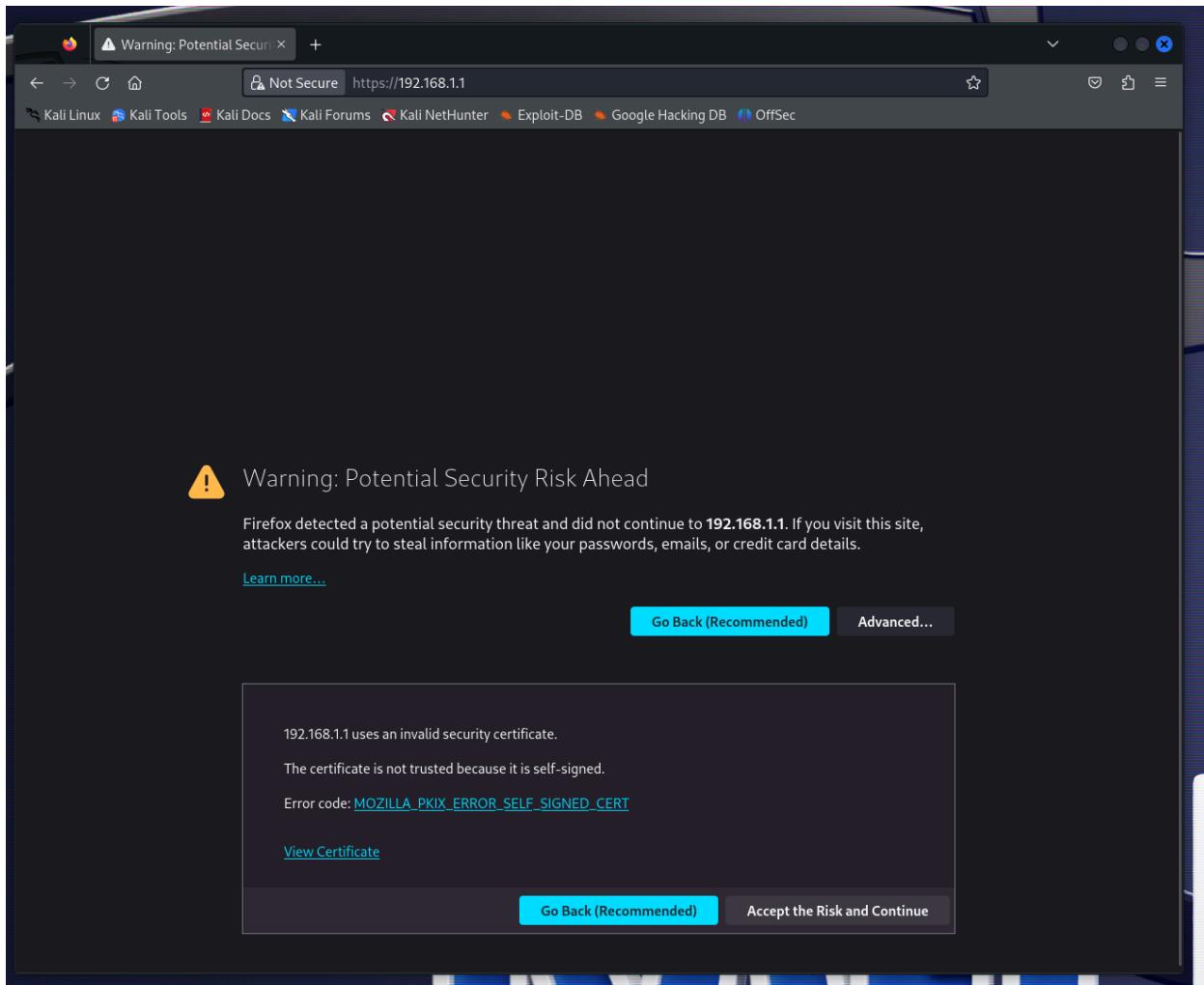
A screenshot of a terminal window titled "kali@kali: ~". The window shows the command \$ passwd being run, followed by prompts for the current password, new password, and retype new password. The output indicates that the password was updated successfully. The background of the terminal window features a large, semi-transparent watermark of the word "KALI-LINUX" and the quote "the quieter you become, the more you are able".

```
(kali㉿kali)-[~]
$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
passwd: password updated successfully

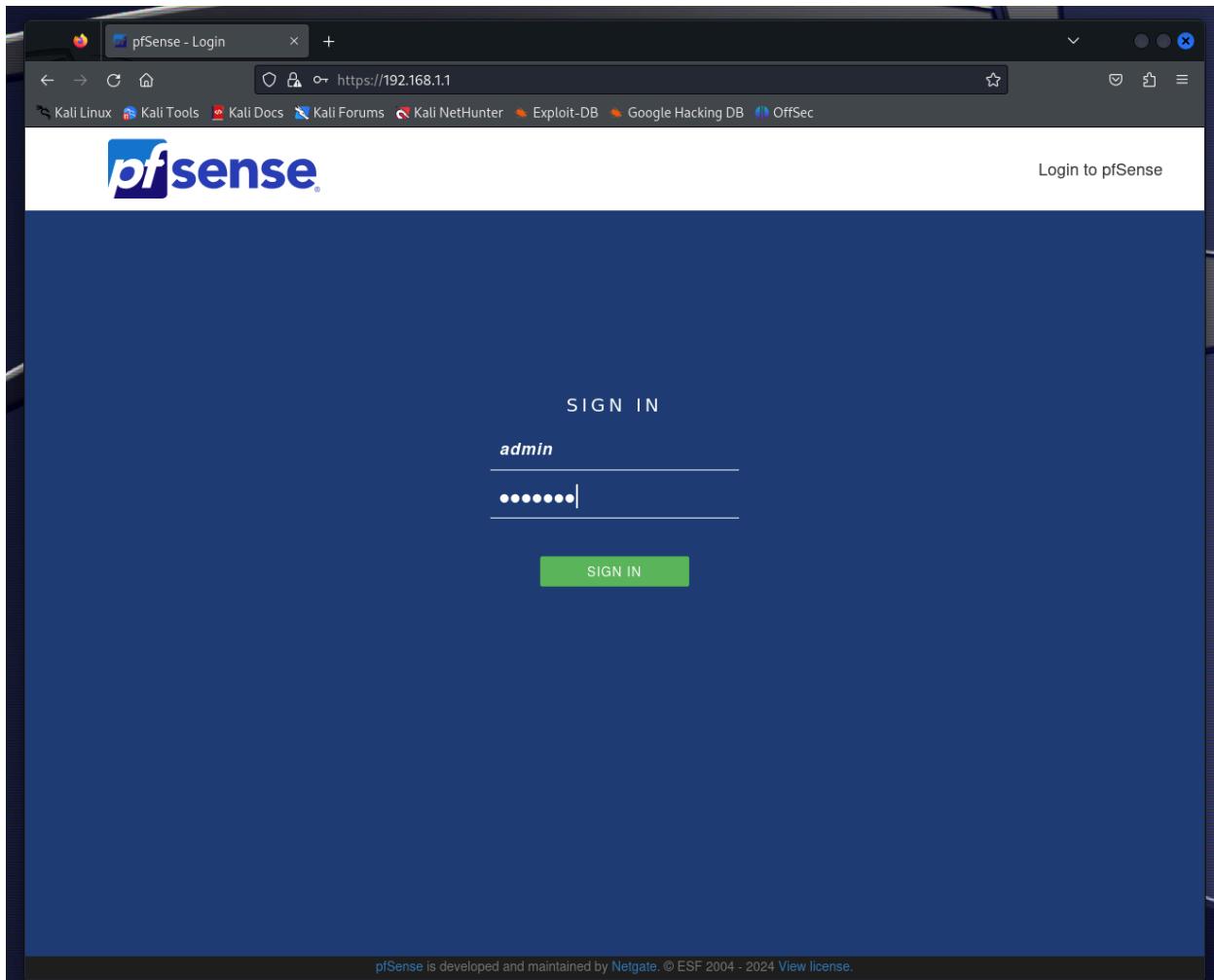
(kali㉿kali)-[~]
$
```

Configuring pfSense Interface and Firewall Rules

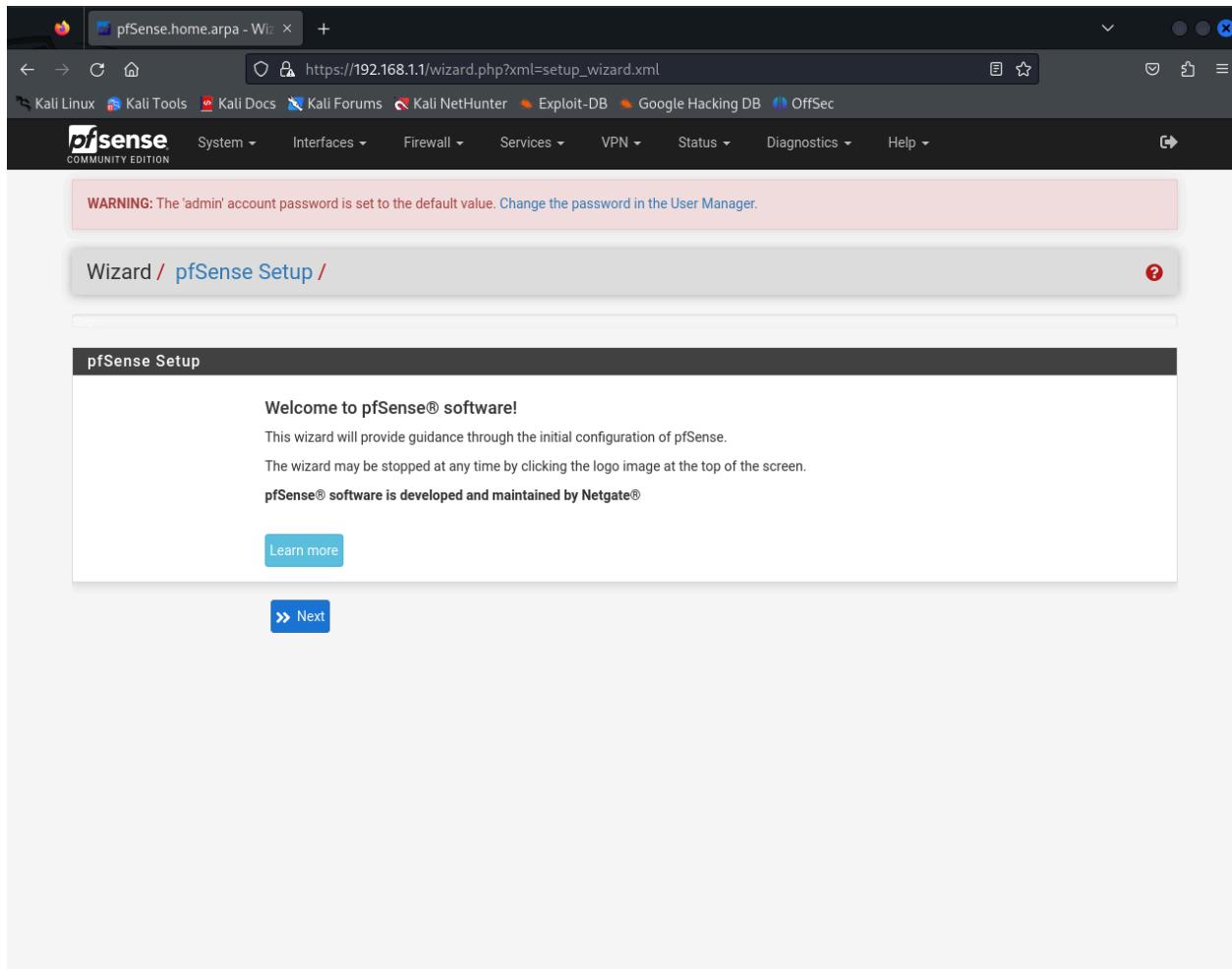
Log into the Kali machine and open up a web browser and navigate to 192.168.1.1. You will be warned about potential security risks, but you can accept and continue:



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



Click “Next” on the first two screens:



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Netgate® Global Support is available 24/7



Step 1 of 9

Netgate® Global Support is available 24/7

Our 24/7 worldwide team of support engineers are the most qualified to diagnose your issue and resolve it quickly, from branch office to enterprise – on premises to cloud.

We offer several support subscription plans tailored to fit different environment sizes and requirements. Many companies around the world choose Netgate support because:

- Support is available 24 hours a day, seven days a week, including holidays.
- Support engineers are located around the world, ensuring that no support call is missed.
- Our support engineers hold many prestigious network engineer certificates and have years of hands-on experience with networking.

[Learn more](#)

[» Next](#)

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

Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname pfSense
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain home.arpa
Domain name for the firewall.
Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server 8.8.8.8

Secondary DNS Server 4.4.4.4

Override DNS Allow DNS servers to be overridden by DHCP/PPP on WAN

>> Next

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

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname 2.pfsense.pool.ntp.org
Enter the hostname (FQDN) of the time server.

Timezone Canada/Mountain

>> 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:

PPTP configuration

PPTP Username	<input type="text"/>
PPTP Password	<input type="password"/>
Show PPTP password	<input type="checkbox"/> Reveal password characters
PPTP Local IP Address	<input type="text"/>
pptplocalsubnet	32
PPTP Remote IP Address	<input type="text"/>
PPTP Dial on demand	<input type="checkbox"/> Enable Dial-On-Demand mode This option causes the interface to operate in dial-on-demand mode, allowing a virtual full time connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.
PPTP Idle timeout	<input type="text"/>
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.	

RFC1918 Networks

Block RFC1918 Private Networks	<input type="checkbox"/> Block private networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.
--------------------------------	---

Block bogon networks

Block bogon networks	<input type="checkbox"/> Block non-Internet routed networks from entering via WAN When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.
----------------------	--

>> Next

The next screen you should just click “Next”:

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address	<input type="text" value="192.168.1.1"/> Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask	24

>> Next

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

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password: (REDACTED)

Admin Password AGAIN: (REDACTED)

>> 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:

Wizard / pfSense Setup / Wizard completed.

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

Check for updates

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

Finish

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:

<p>If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.</p>	
DNS Resolution Behavior	<input type="button" value="Use local DNS (127.0.0.1), fall back to remote DNS Servers (Default)"/>
<p>By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.</p>	
Localization	
Timezone	<input type="button" value="Canada/Mountain"/> Select a geographic region name (Continent/Location) to determine the timezone for the firewall. Choose a special or "Etc" zone only in cases where the geographic zones do not properly handle the clock offset required for this firewall.
Timeservers	<input type="button" value="2.pfsense.pool.ntp.org"/> Use a space to separate multiple hosts (only one required). Remember to set up at least one DNS server if a host name is entered here!
Language	<input type="button" value="English"/> Choose a language for the webConfigurator
webConfigurator	
Theme	<input type="button" value="pfSense-dark"/> Choose an alternative css file (if installed) to change the appearance of the webConfigurator. css files are located in /usr/local/www/css/
Top Navigation	<input type="button" value="Scrolls with page"/> The fixed option is intended for large screens only.
Hostname in Menu	<input type="button" value="Default (No hostname)"/> Replaces the Help menu title in the Navbar with the system hostname or FQDN.
Dashboard Columns	<input type="button" value="2"/>
Interfaces Sort	<input type="checkbox"/> Sort Alphabetically If selected, lists of interfaces will be sorted by description, otherwise they are listed wan,lan,optn...
Associated Panels	<input type="checkbox"/> Available Widgets <input type="checkbox"/> Log Filter <input type="checkbox"/> Manage Log <input type="checkbox"/> Monitoring Settings Show/Hide Show the Available Widgets panel on the Dashboard. Show the Log Filter panel in System Logs. Show the Manage Log panel in System Logs. Show the Settings panel in Status Monitoring.

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

pfSense COMMUNITY EDITION

Interfaces / LAN (em1)

General Configuration

Enable **Enable interface**

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xxxx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a **WAN type interface**.
Gateways can be managed by [clicking here](#).

Reserved Networks

Block private networks and loopback addresses
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

[!\[\]\(03d7b8ce621d443287c24386c477802a_img.jpg\) Save](#)

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

The Kali configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

Apply Changes

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	Kali Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	XX:XX:XX:XX:XX:XX This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx or leave blank.
MTU	
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.	
MSS	
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.	
Speed and Duplex	Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.	

Static IPv4 Configuration

IPv4 Address	192.168.1.1	/ 24
IPv4 Upstream gateway	None	<input type="button" value="Add a new gateway"/>
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface . Gateways can be managed by clicking here .		

Reserved Networks

Block private networks and loopback addresses	<input type="checkbox"/>	Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.
Block bogon networks	<input type="checkbox"/>	Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received. This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic. Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

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

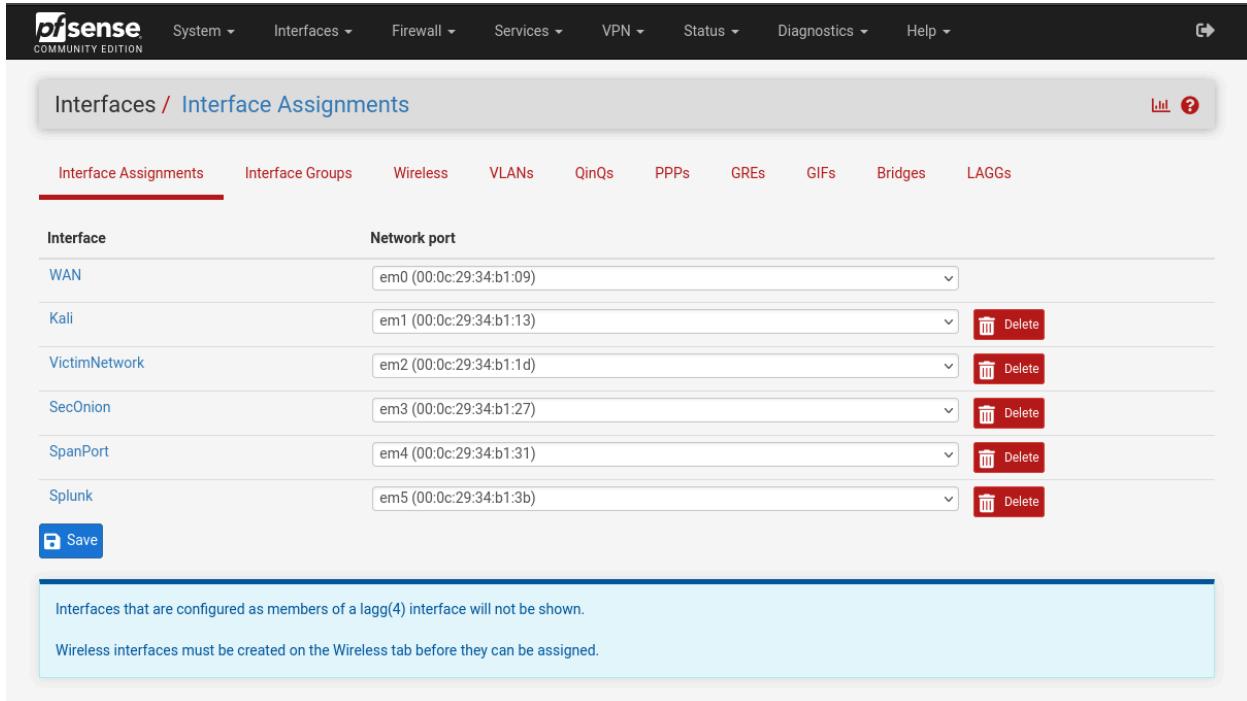
OPT1 will be for the victim network

OPT2 will be for Security Onion

OPT3 will be for the span port

OPT4 will be for Splunk

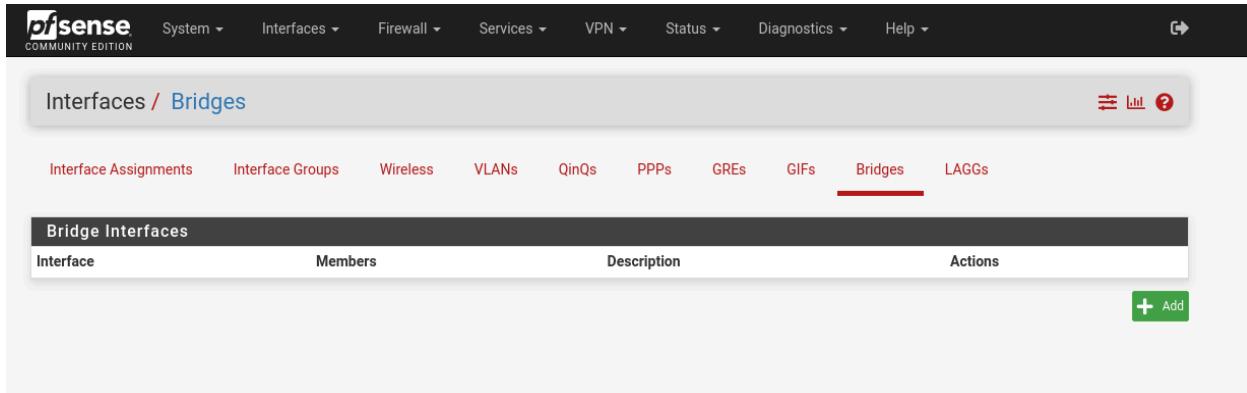
Make sure to check that “Enable interface” is checked for all of them, particularly OPT3. After you apply all changes, you should see the changes reflected under interface assignments:



The screenshot shows the pfSense web interface under the 'Interfaces' tab, specifically the 'Interface Assignments' section. It lists six interfaces (WAN, Kali, VictimNetwork, SecOnion, SpanPort, Splunk) and their corresponding network ports (em0 through em5). Each entry includes a dropdown menu and a red 'Delete' button. A 'Save' button is at the bottom left, and a note at the bottom states: 'Interfaces that are configured as members of a lagg(4) interface will not be shown.' and 'Wireless interfaces must be created on the Wireless tab before they can be assigned.'

Interface	Network port
WAN	em0 (00:0c:29:34:b1:09)
Kali	em1 (00:0c:29:34:b1:13)
VictimNetwork	em2 (00:0c:29:34:b1:1d)
SecOnion	em3 (00:0c:29:34:b1:27)
SpanPort	em4 (00:0c:29:34:b1:31)
Splunk	em5 (00:0c:29:34:b1:3b)

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



The screenshot shows the pfSense web interface under the 'Interfaces' tab, specifically the 'Bridges' section. It displays an empty table for 'Bridge Interfaces' with columns for 'Interface', 'Members', 'Description', and 'Actions'. A green 'Add' button is located at the bottom right.

Bridge Interfaces			
Interface	Members	Description	Actions
			+ Add

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

Interfaces / Bridges / Edit

Bridge Configuration

Member Interfaces	<input type="checkbox"/> WAN <input type="checkbox"/> KALI <input checked="" type="checkbox"/> VICTIMNETWORK <input type="checkbox"/> SECONION
Interfaces participating in the bridge.	
Description	<input type="text"/>
Advanced Options	<input type="button" value="Hide Advanced"/>

Advanced Configuration

Cache Size	<input type="text"/>
Set the size of the bridge address cache. The default is 2000 entries.	
Cache expire time	<input type="text"/>
Set the timeout of address cache entries to this number of seconds. If seconds is zero, then address cache entries will not be expired. The default is 1200 seconds.	
Span Port	<input type="checkbox"/> VICTIMNETWORK <input type="checkbox"/> SECONION <input type="checkbox"/> SPANPORT <input type="checkbox"/> SPLUNK
Add the interface named by interface as a span port on the bridge. Span ports transmit a copy of every frame received by the bridge. This is most useful for snooping a bridged network passively on another host connected to one of the span ports of the bridge. The span interface cannot be part of the bridge member interfaces.	
Edge Ports	<input type="checkbox"/> WAN <input type="checkbox"/> KALI <input type="checkbox"/> VICTIMNETWORK <input type="checkbox"/> SECONION
Set interface as an edge port. An edge port connects directly to end stations and cannot create bridging loops in the network; this allows it to transition straight to forwarding.	
Auto Edge Ports	<input type="checkbox"/> WAN <input type="checkbox"/> KALI <input type="checkbox"/> VICTIMNETWORK <input type="checkbox"/> SECONION

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

Interfaces / Bridges

Interface Assignments	Interface Groups	Wireless	VLANs	QinQs	PPPs	GREs	GIFs	Bridges	LAGGs
-----------------------	------------------	----------	-------	-------	------	------	------	----------------	-------

Bridge Interfaces

Interface	Members	Description	Actions
BRIDGE0	VICTIMNETWORK		<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Add

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:

The screenshot shows the pfSense Firewall / Rules / WAN interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation is a breadcrumb trail: Firewall / Rules / WAN. A toolbar with icons for List, Grid, and Help is located at the top right. Below the toolbar, tabs for Floating, WAN, KALI, VICTIMNETWORK, SECONION, SPANPORT, and SPLUNK are present, with WAN selected. A header bar titled "Rules (Drag to Change Order)" contains columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. A message box states: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule." At the bottom are buttons for Add (up and down arrows), Delete, Toggle, Copy, Save, and Separator.

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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match	Any	Source Address	/	
--------	---------------------------------------	-----	----------------	---	--

Destination

Destination	<input type="checkbox"/> Invert match	Any	Destination Address	/	
-------------	---------------------------------------	-----	---------------------	---	--

Extra Options

Log	<input type="checkbox"/> 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	<input type="text"/>
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	

Firewall / Rules / WAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Floating	WAN	KALI	VICTIMNETWORK	SECONION	SPANPORT	SPLUNK					
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4 *	*	*	*	*	*	none			
Add Add Delete Toggle Copy Save											

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

* Company size

* Job role

* Phone

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:



New Virtual Machine Wizard

X

Guest Operating System Installation

A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?

Install from:

Installer disc:

No drives available

Installer disc image file (iso):

C:\Users\samin\Documents\Virtual Machines\windows s

[Browse...](#)

i Windows Server 2019 detected.

This operating system will use Easy Install. ([What's this?](#))

I will install the operating system later.

The virtual machine will be created with a blank hard disk.

[Help](#)

[< Back](#)

[Next >](#)

[Cancel](#)

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

New Virtual Machine Wizard X

Easy Install Information
This is used to install Windows Server 2019.

Windows product key

Version of Windows to install
 ▾

Personalize Windows

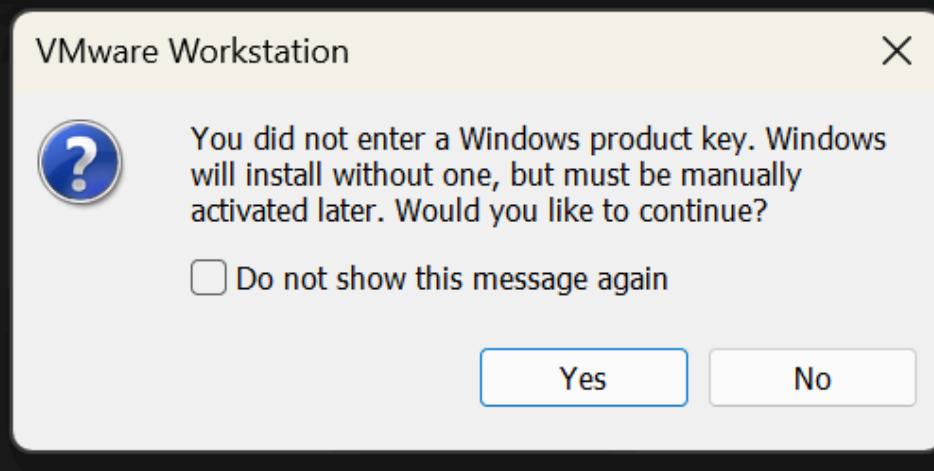
Full name:

Password: (optional)

Confirm:

Log on automatically (requires a password)

Help < Back Next > Cancel



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

New Virtual Machine Wizard X

Name the Virtual Machine

What name would you like to use for this virtual machine?

Virtual machine name:
Windows Server 2019

Location:
C:\Users\samin\OneDrive\Documents\Virtual Machines\Windows Browse...

The default location can be changed at Edit > Preferences.

[< Back](#) [Next >](#) [Cancel](#)

You can keep the default selections for the disk:

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): 

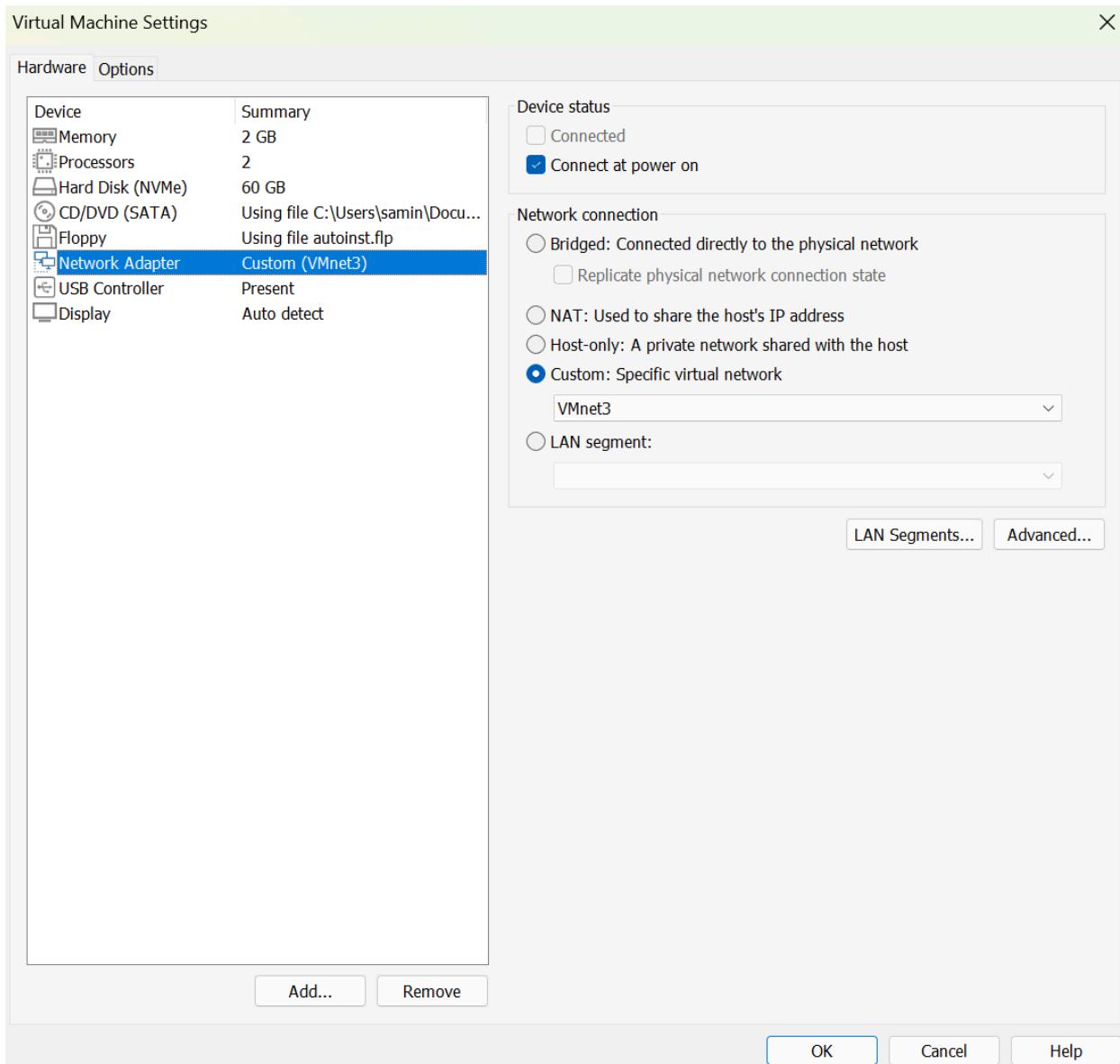
Recommended size for Windows Server 2019: 60 GB

- Store virtual disk as a single file
- Split virtual disk into multiple files

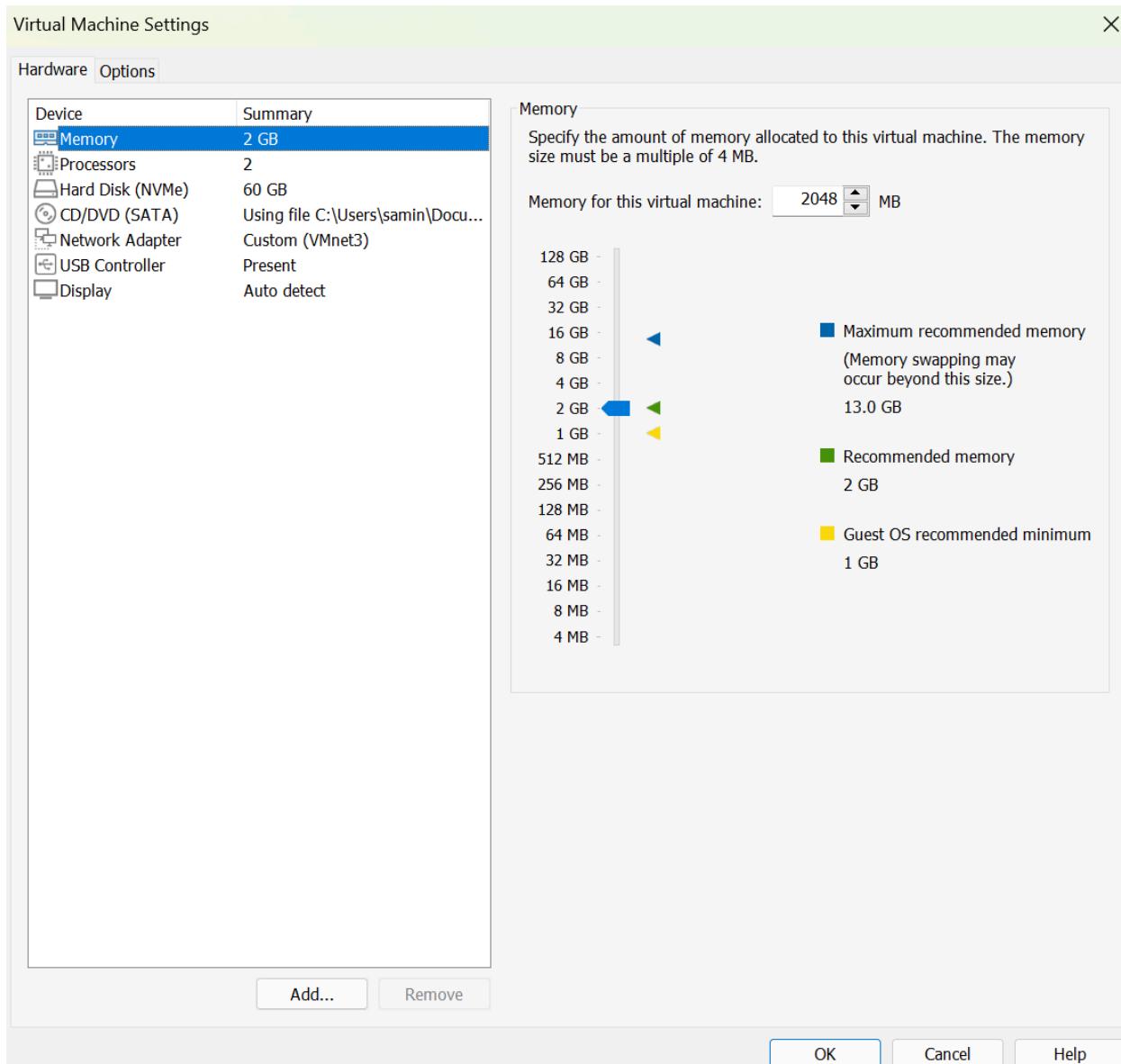
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

[Help](#)[< Back](#)[Next >](#)[Cancel](#)

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

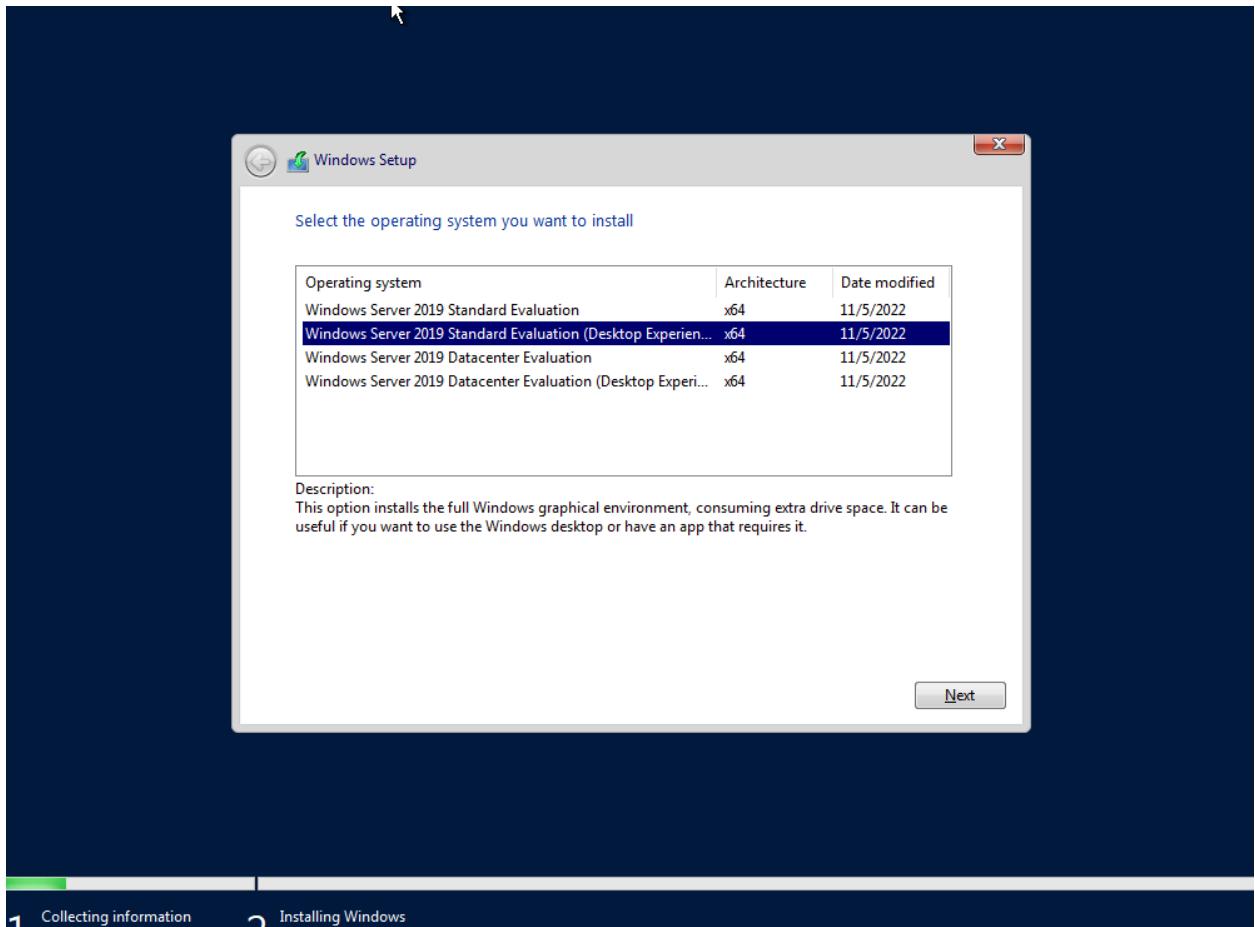


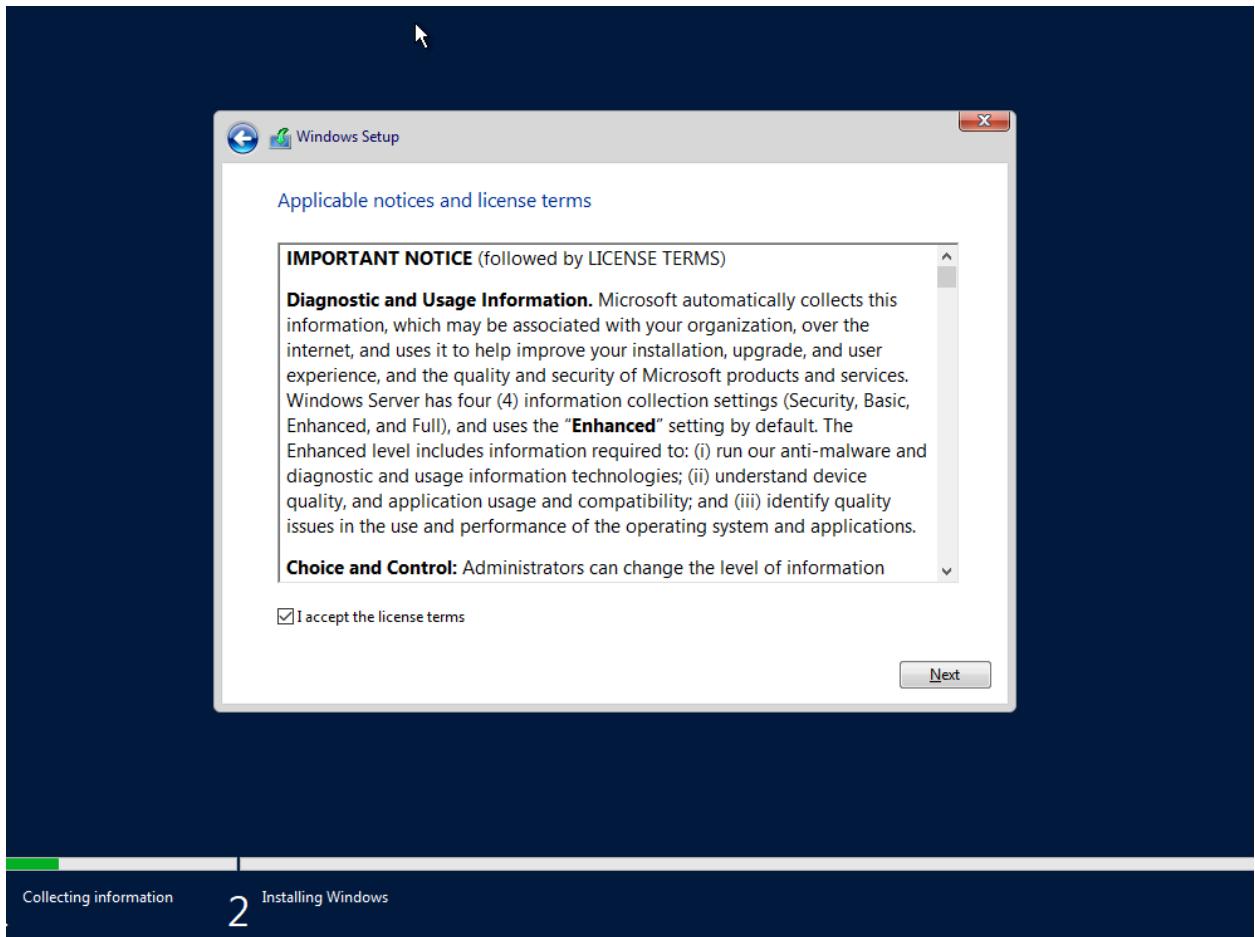
Remove the floppy drive:



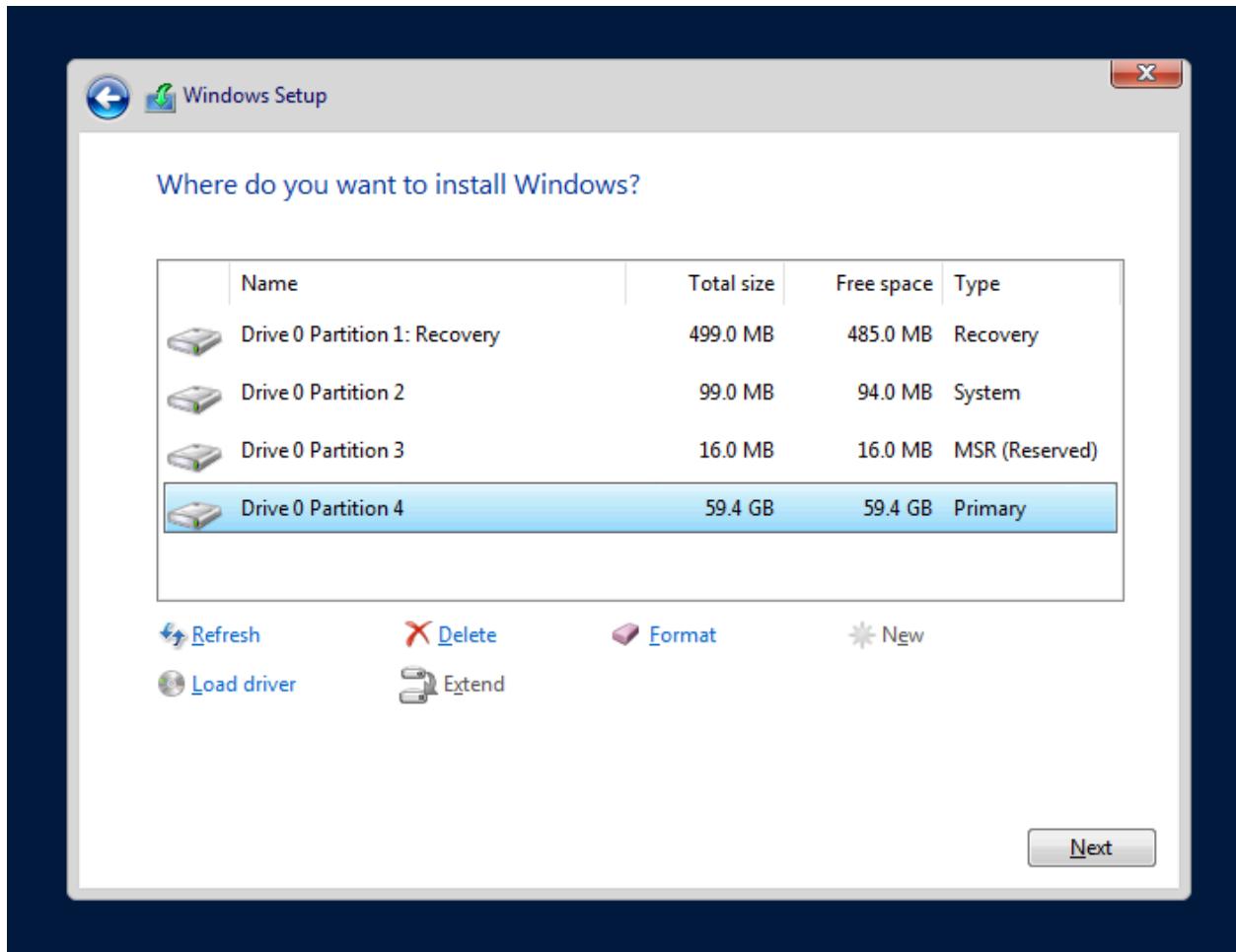
Power the machine on and press a key very quickly (otherwise it will time out). Click “Next” and then “Install Now”.

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

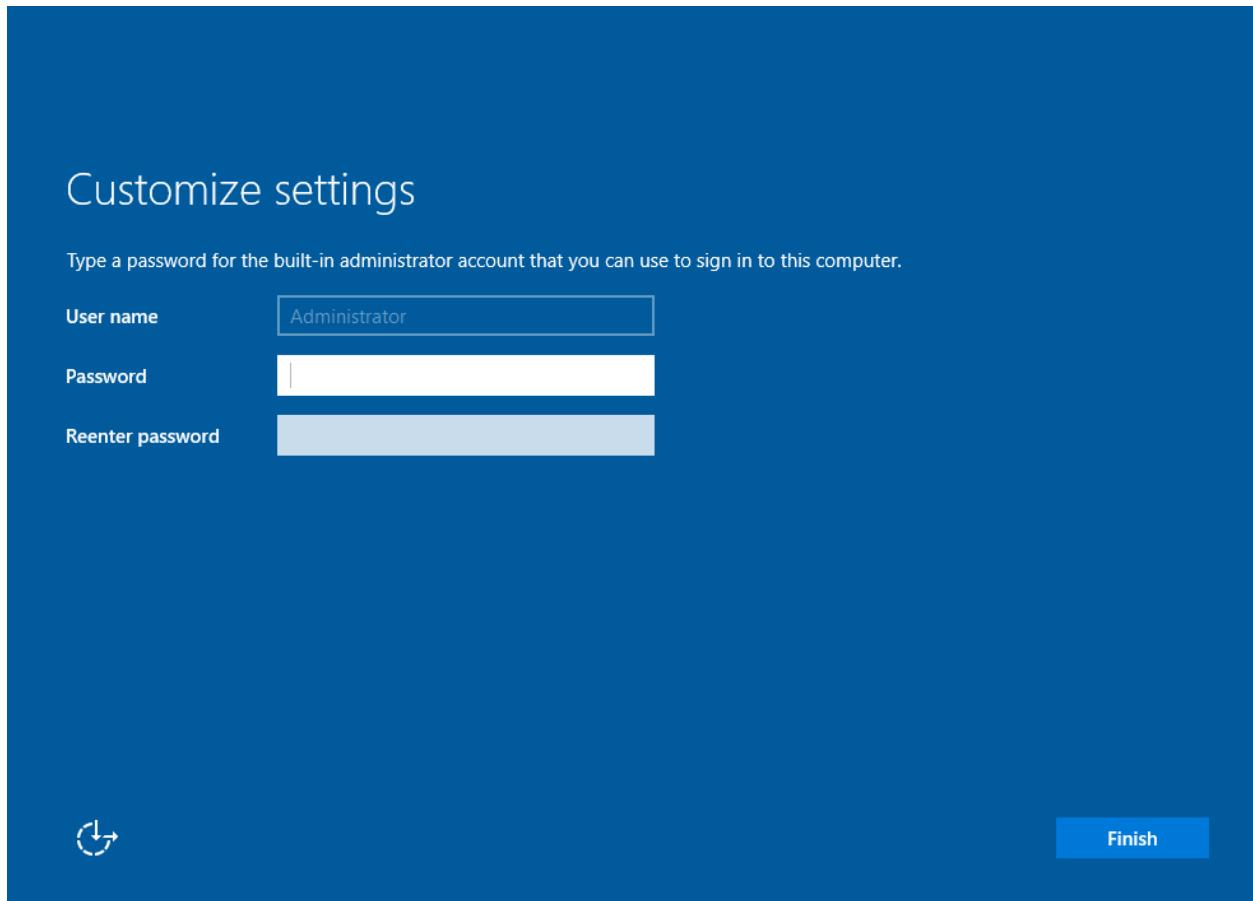




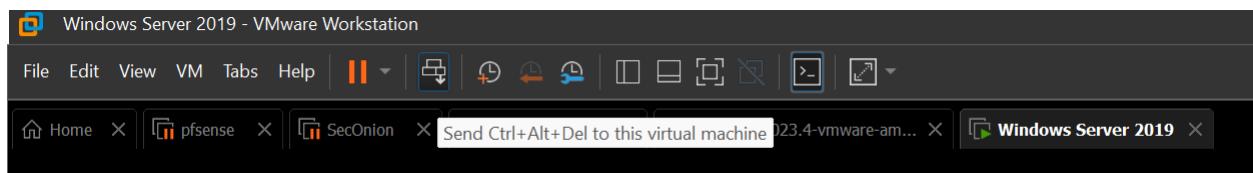
Click “New”, then “Apply”, and then “Ok” before clicking “Next”:



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

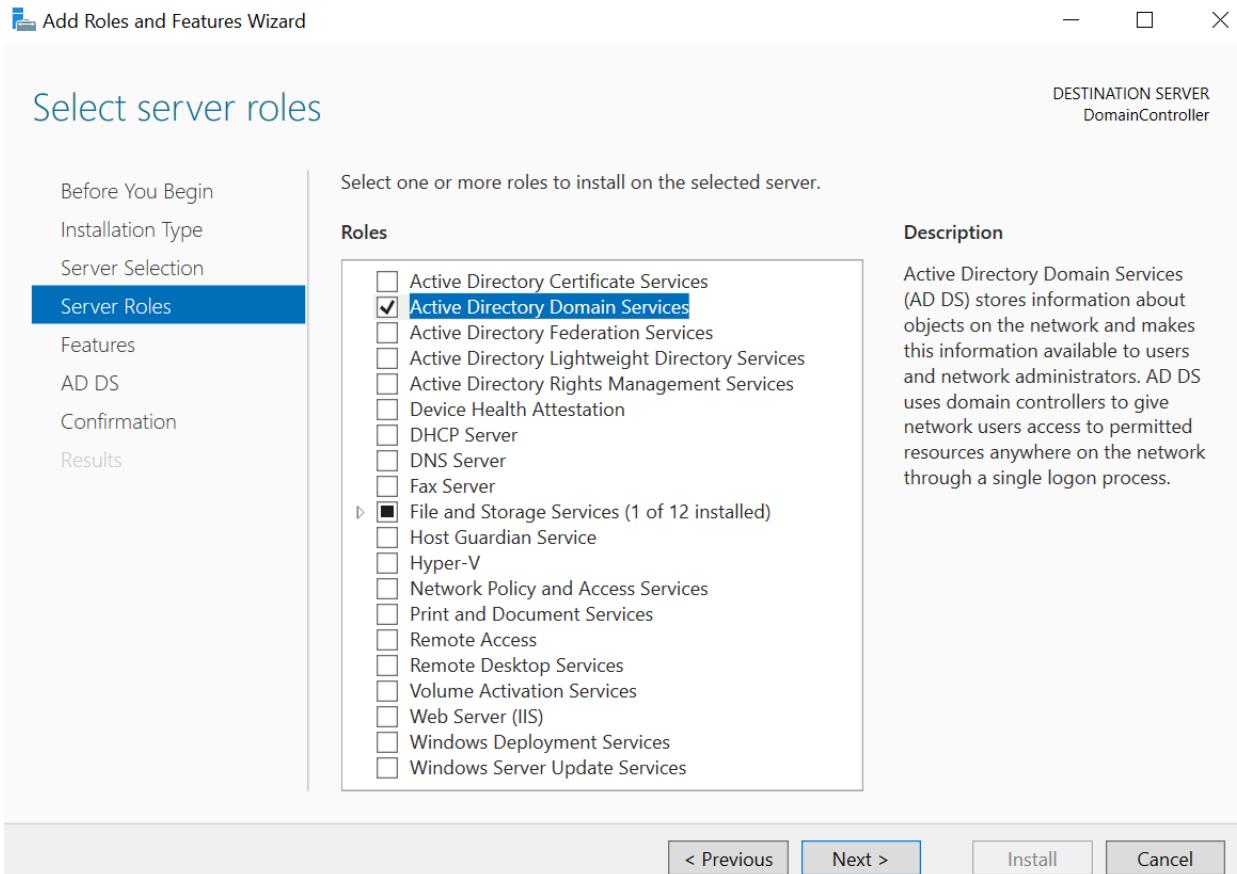


To log in, send CTRL-ALT-DELETE to the machine:

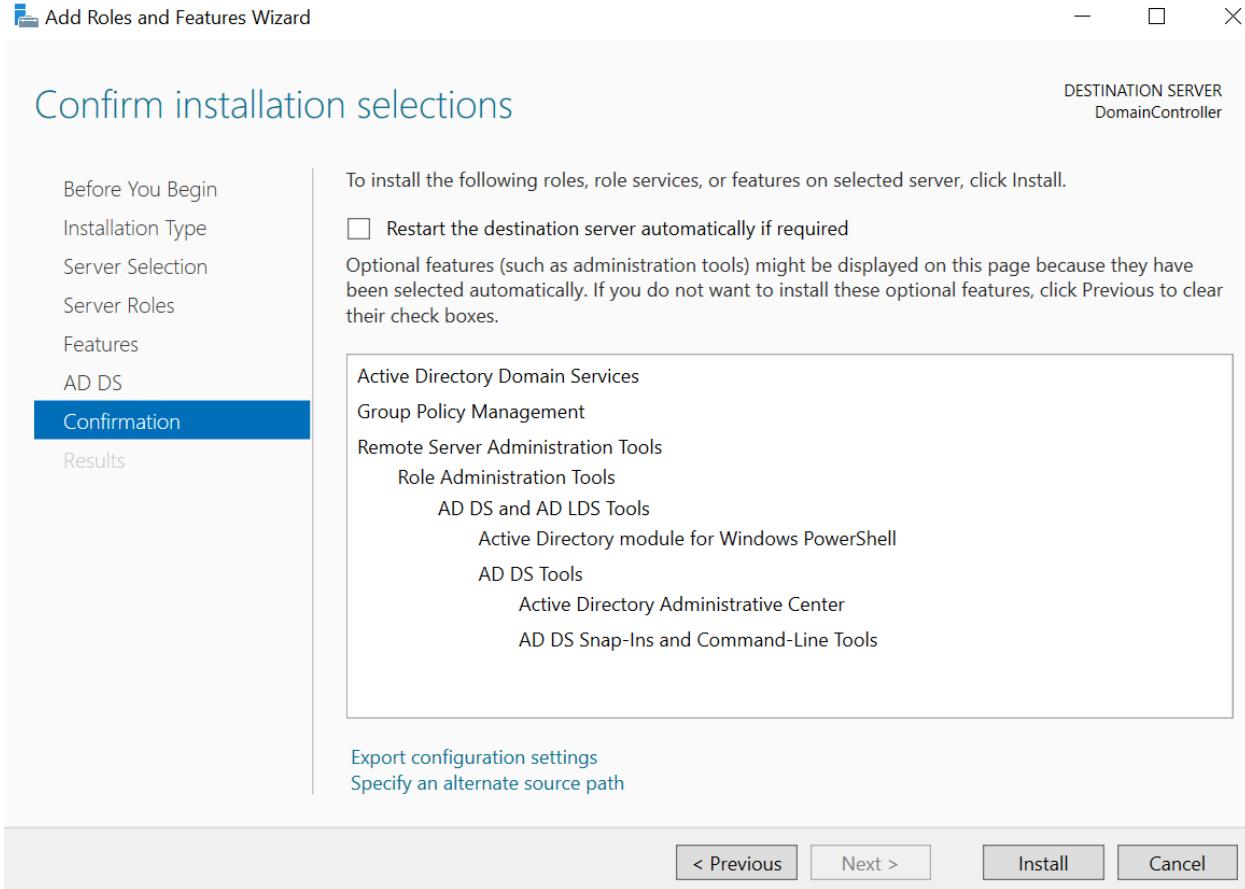


Once the Server Manager Dashboard loads up, Click “Add Roles and Features” under “Manage”

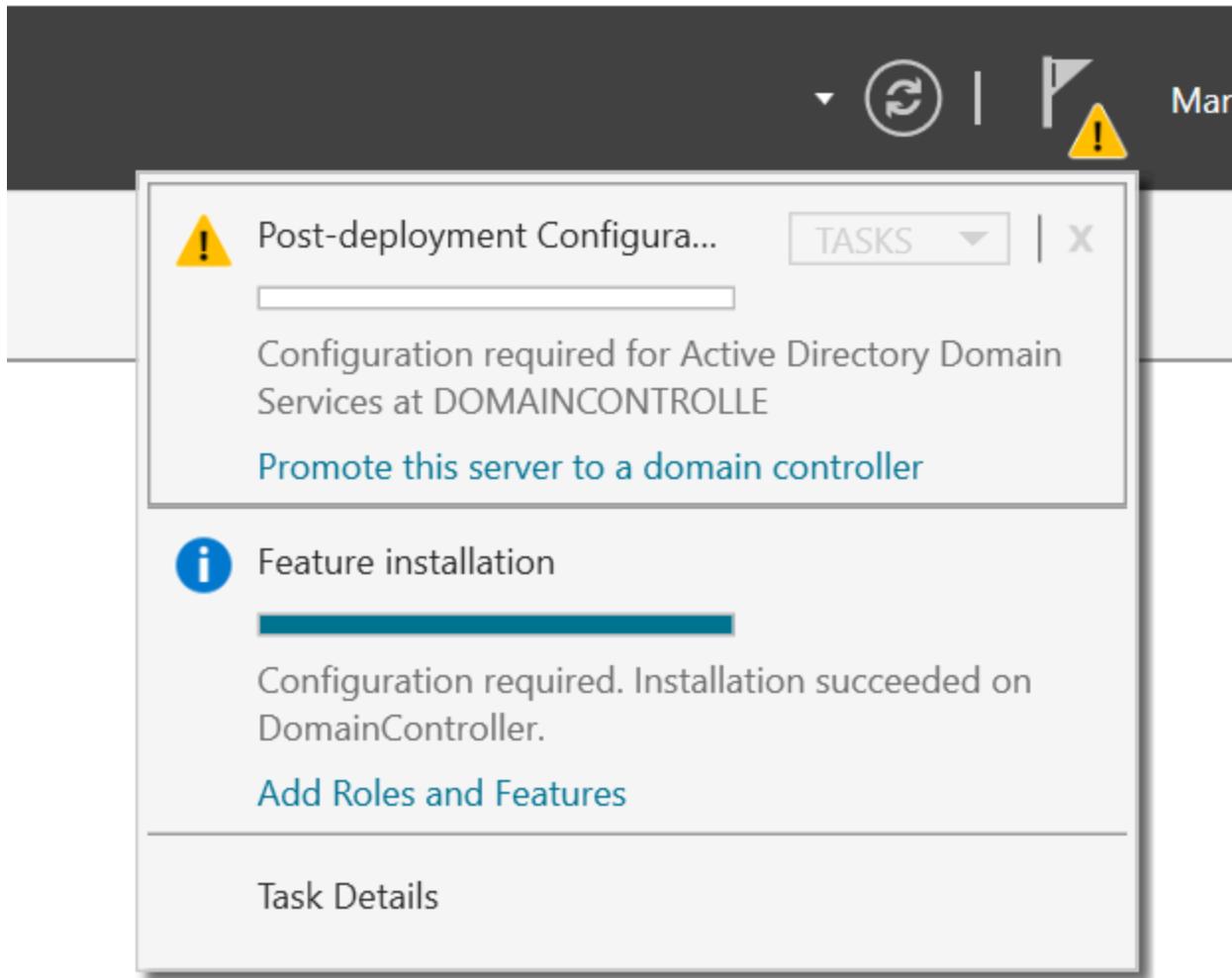
Click “Next” until you get to the following screen, where you can check the “Active Directory Domain Services” and then click “Add Features“:



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”:

TARGET SERVER
DomainController

Deployment Configuration

- Deployment Configuration
- Domain Controller Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Root domain name:

samin.local

[More about deployment configurations](#)

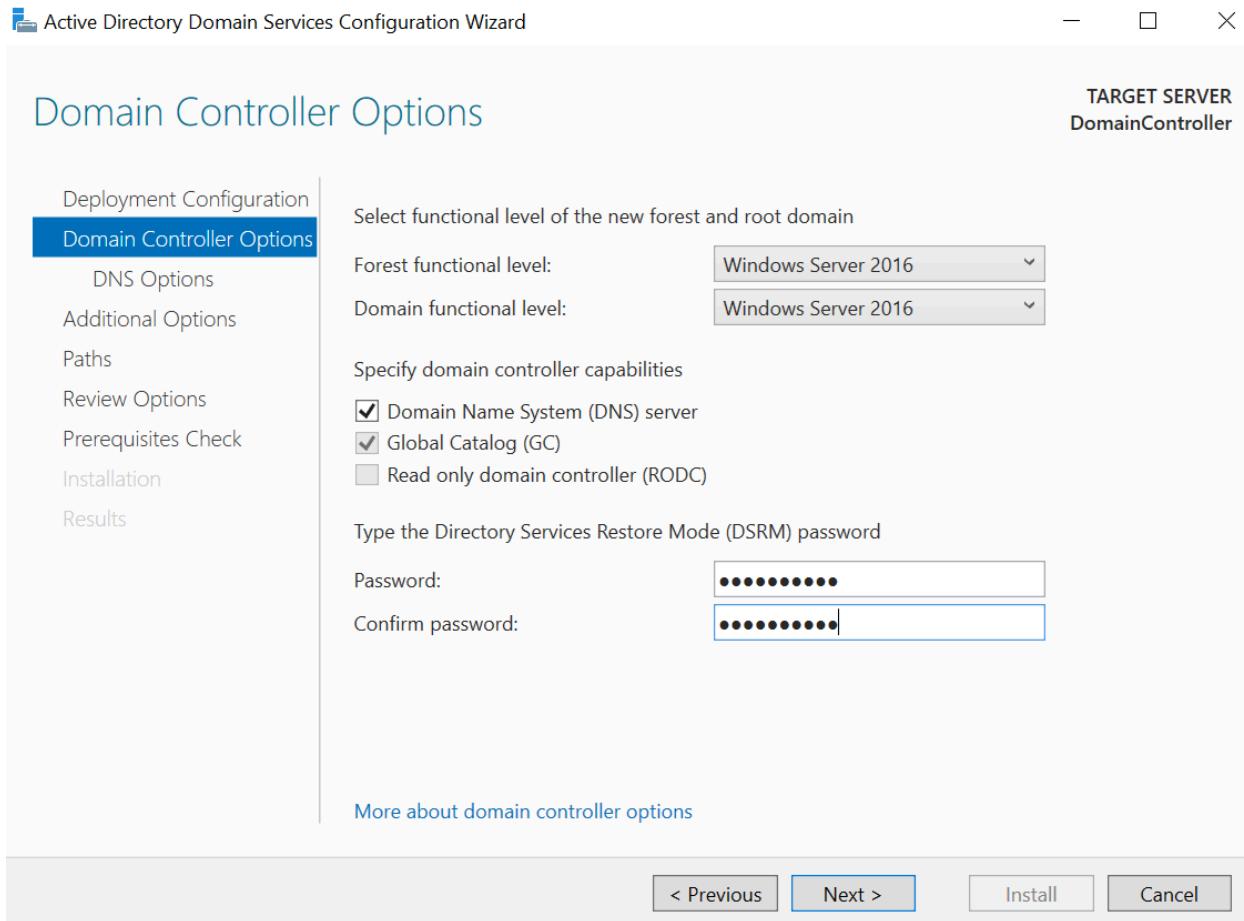
< Previous

Next >

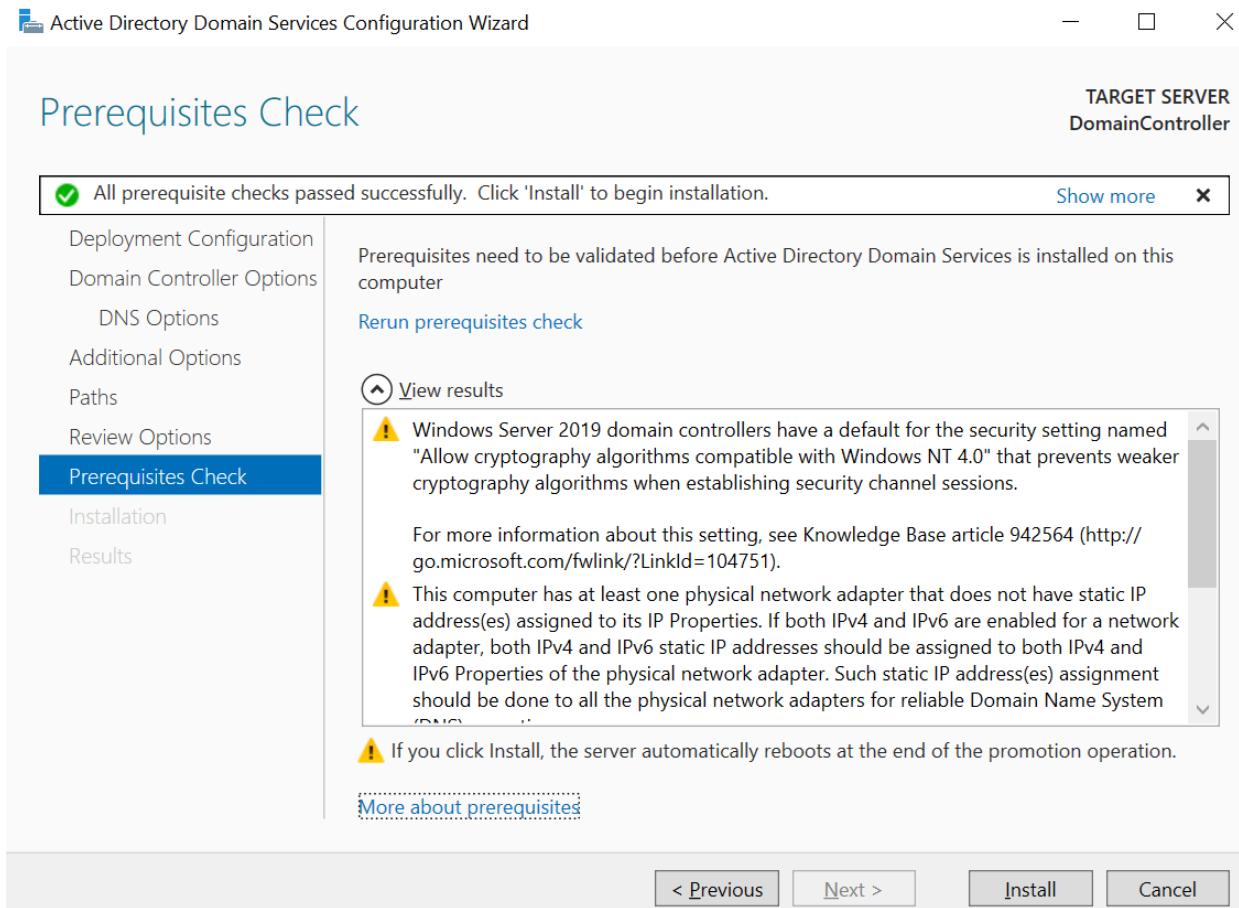
Install

Cancel

Set a password:



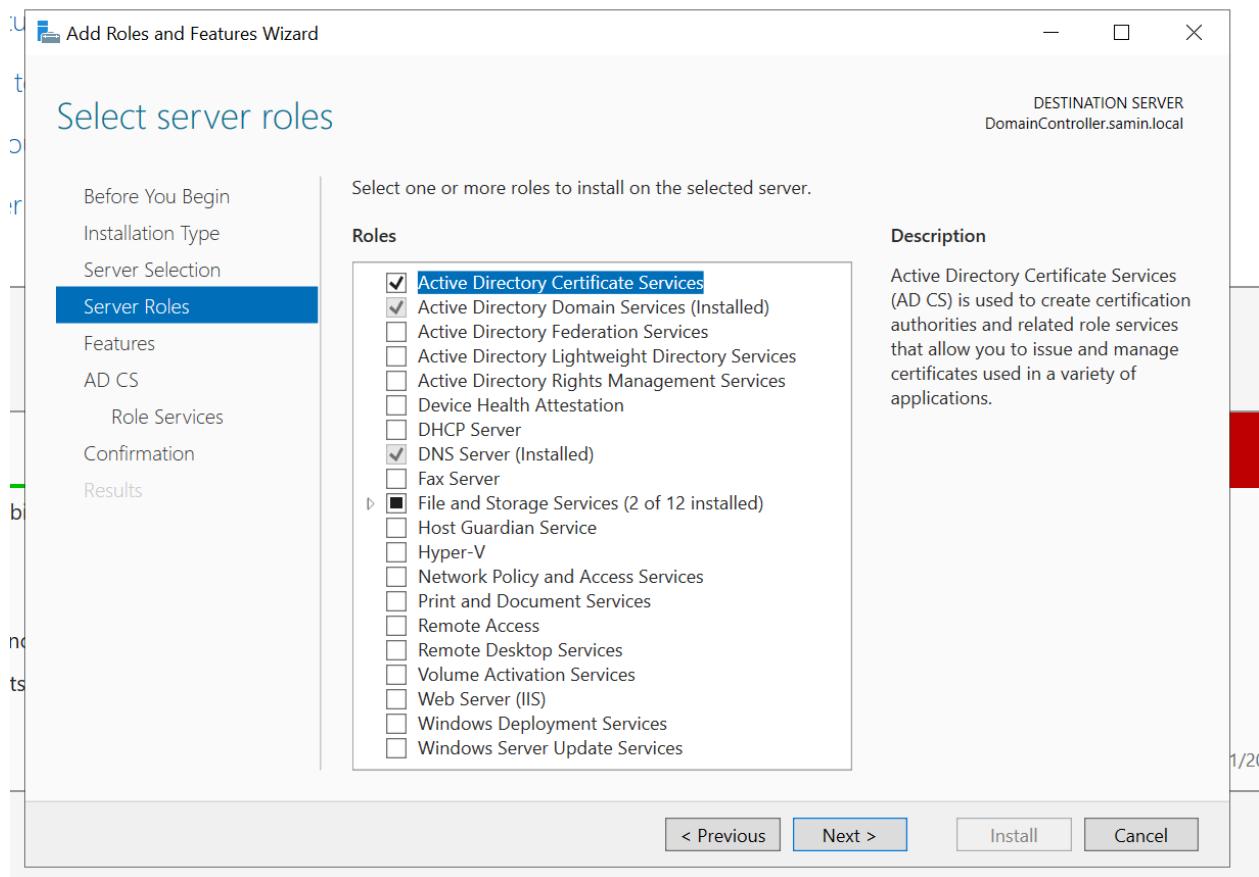
Click “Next” until you can click “Install”:



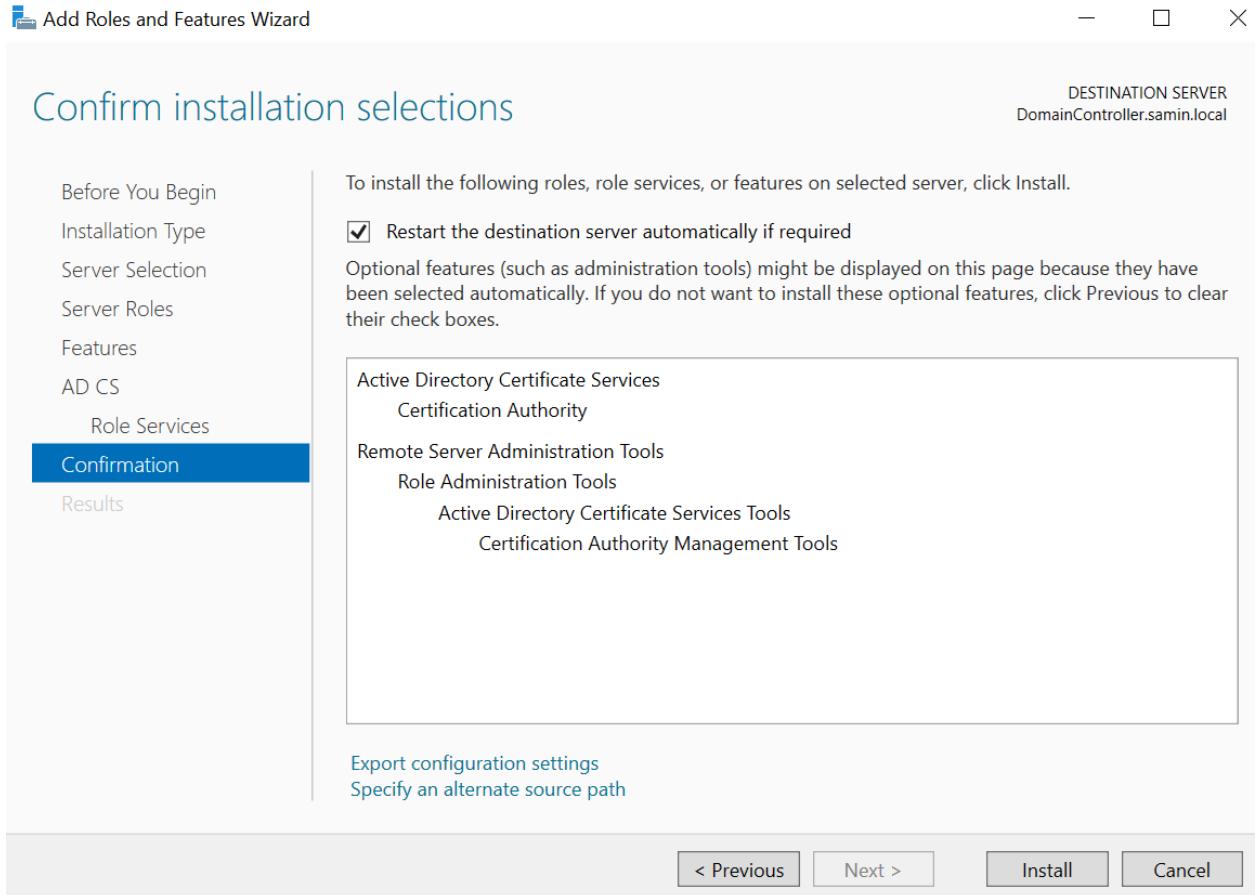
Click “Install”, then wait for the machine to reboot and log back in.

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

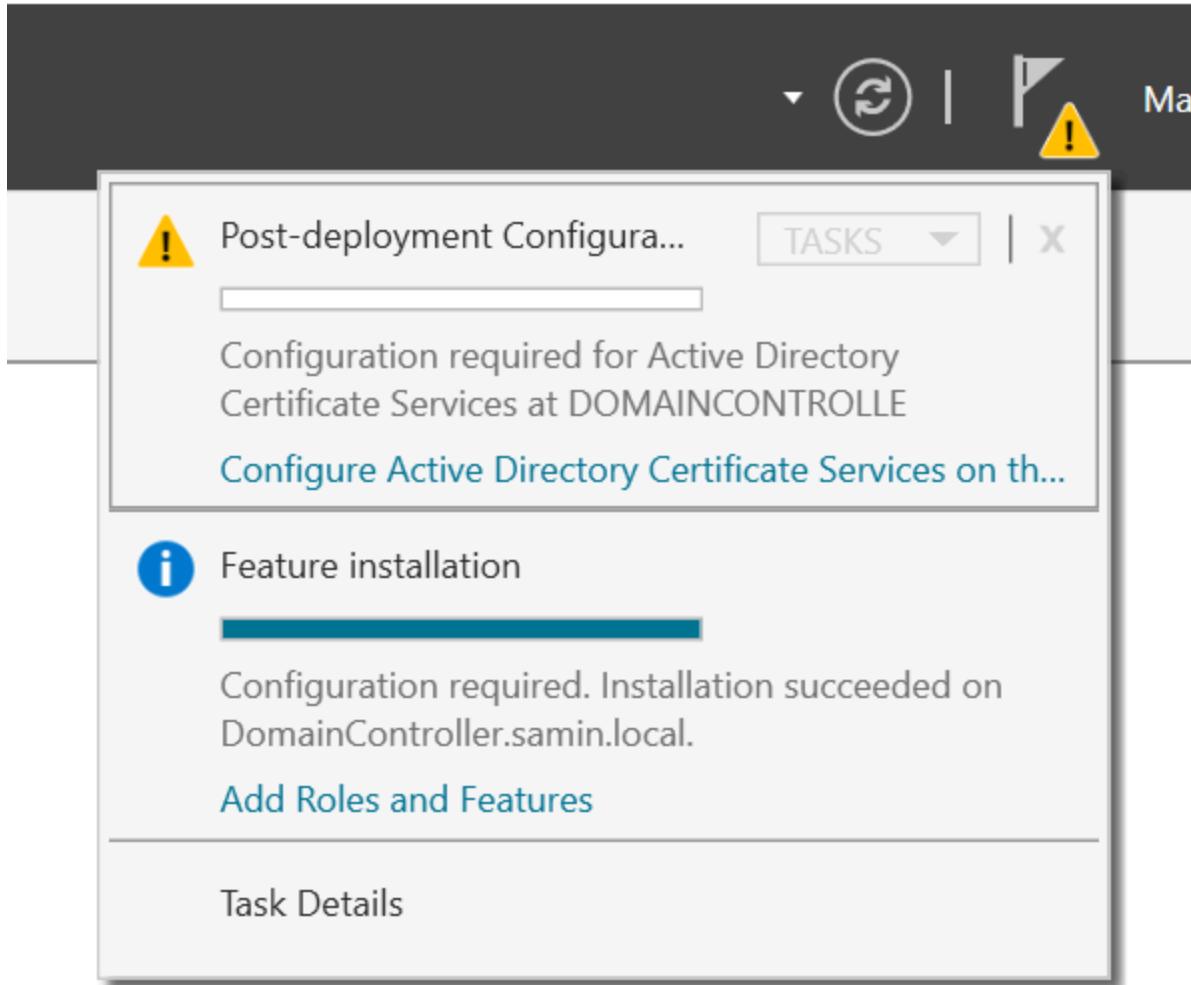
Click “Next” until you get to the screen below. Here, check off “Active Directory Certificate Services” and click “Add Features” before clicking “Next”:



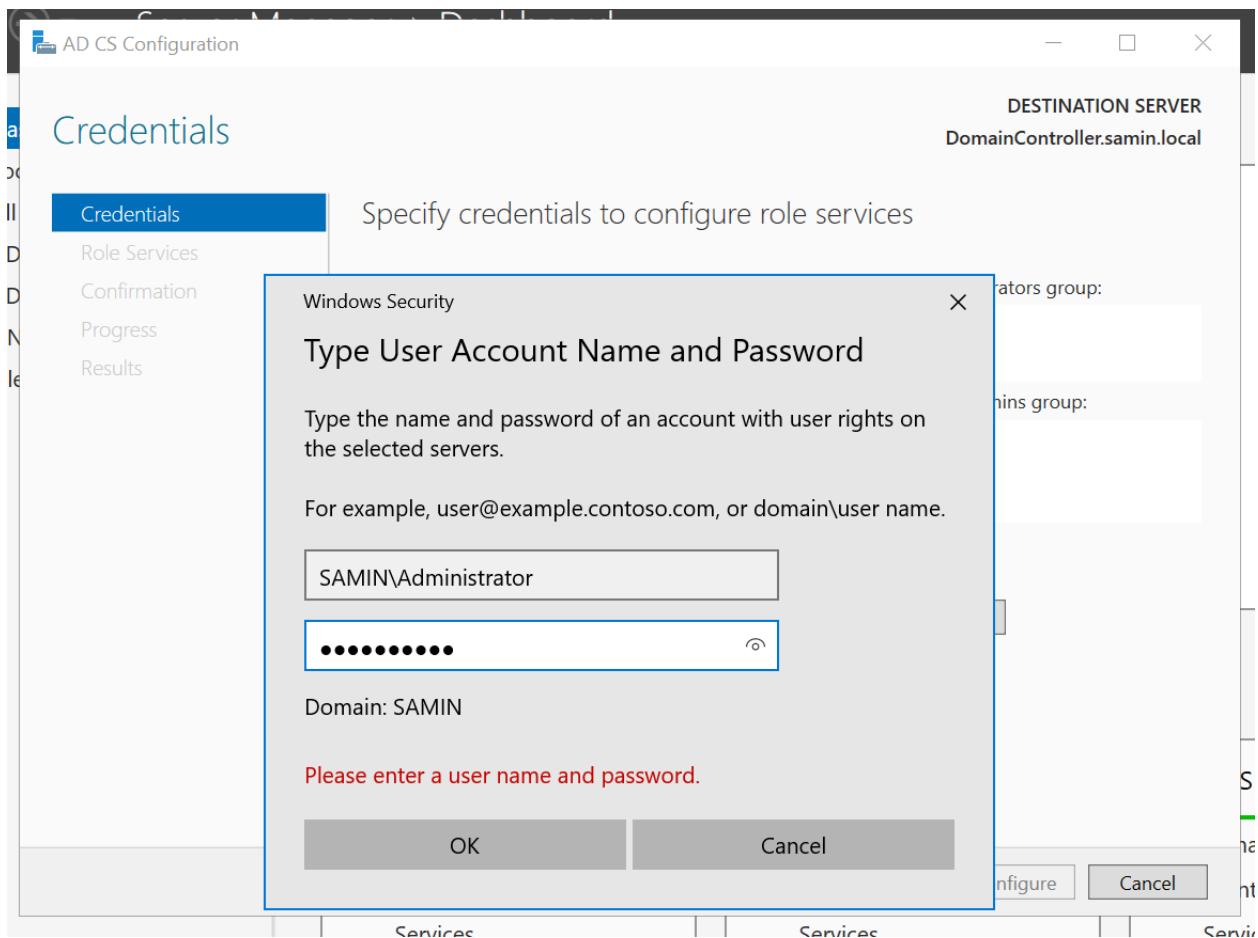
Click “Next” until you reach the screen with the install button. Here, check the box that says “Restart the destination server automatically if required” and click “Yes” before pressing the “Install” button:

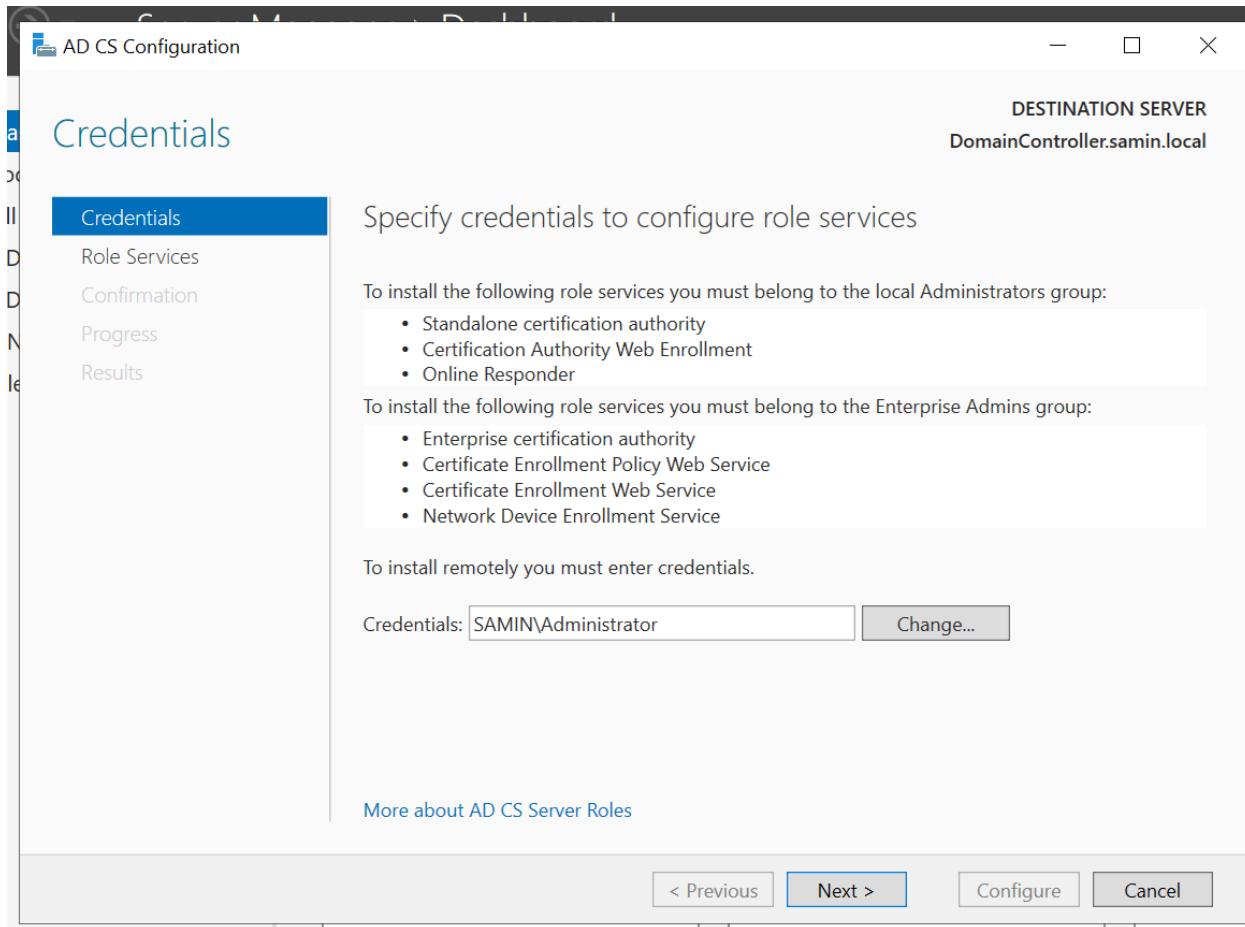


Click on the flag with the yellow triangle and click “Configure Active Directory Certificate Services on the destination server”:

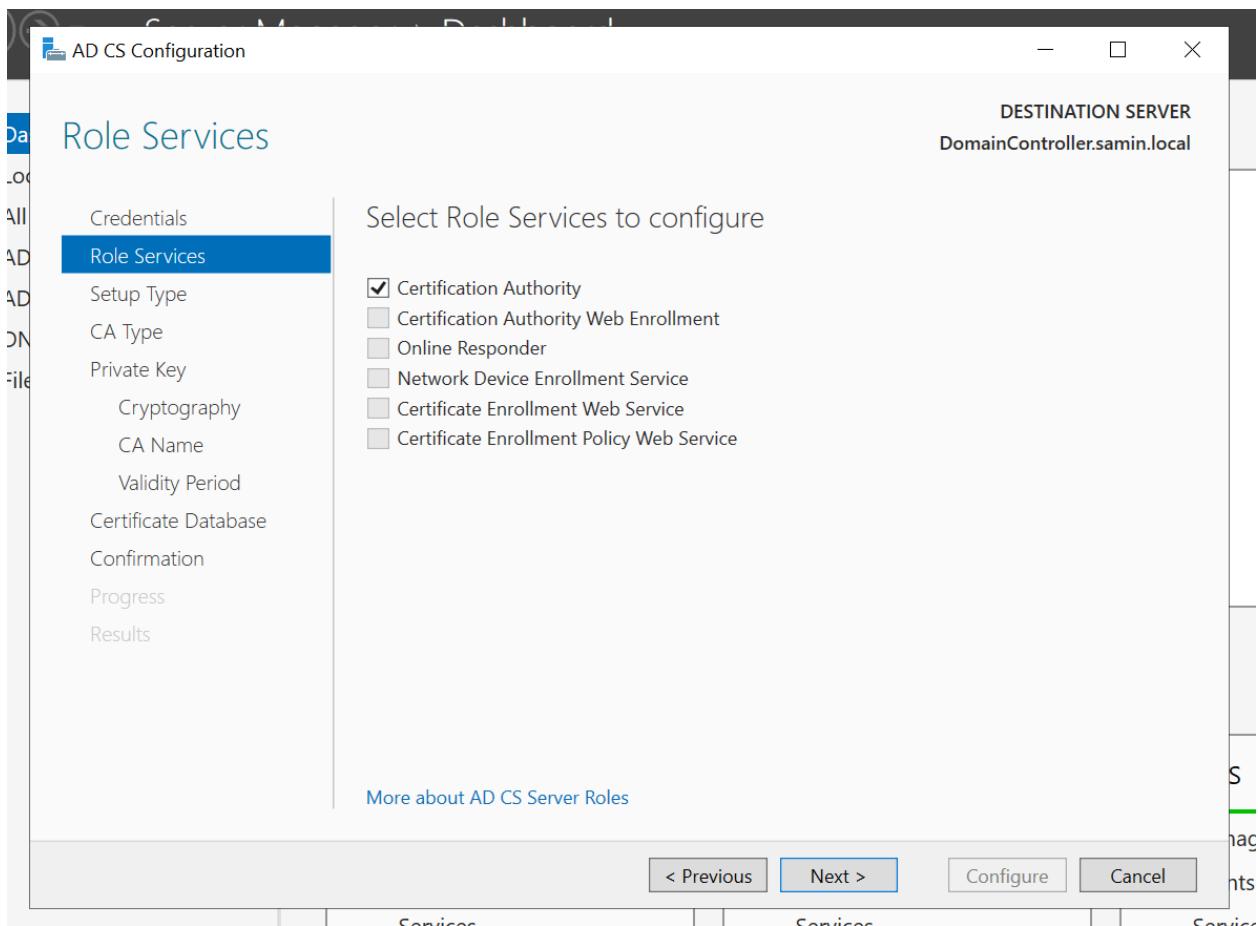


Enter your credentials before clicking next:

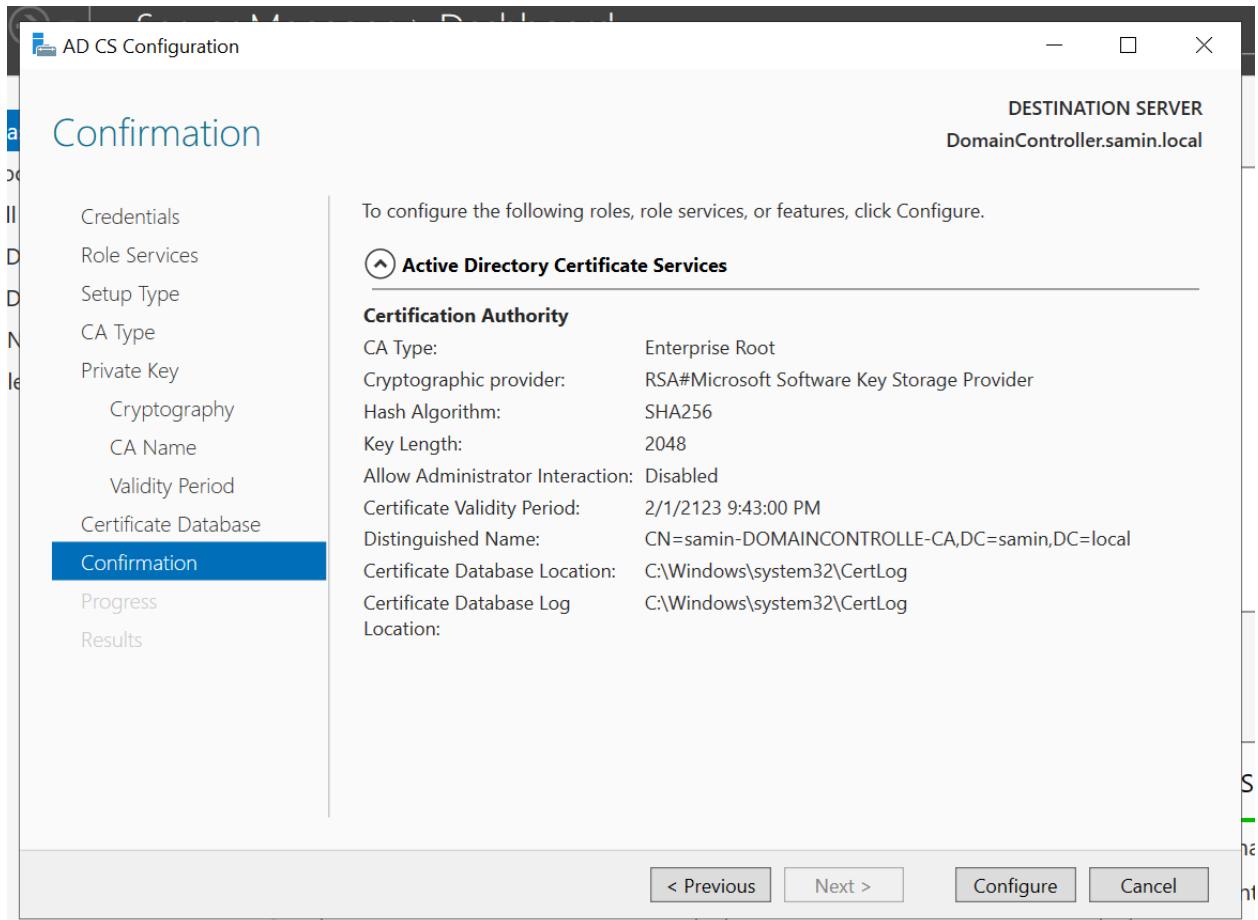




Check “Certification Authority”:



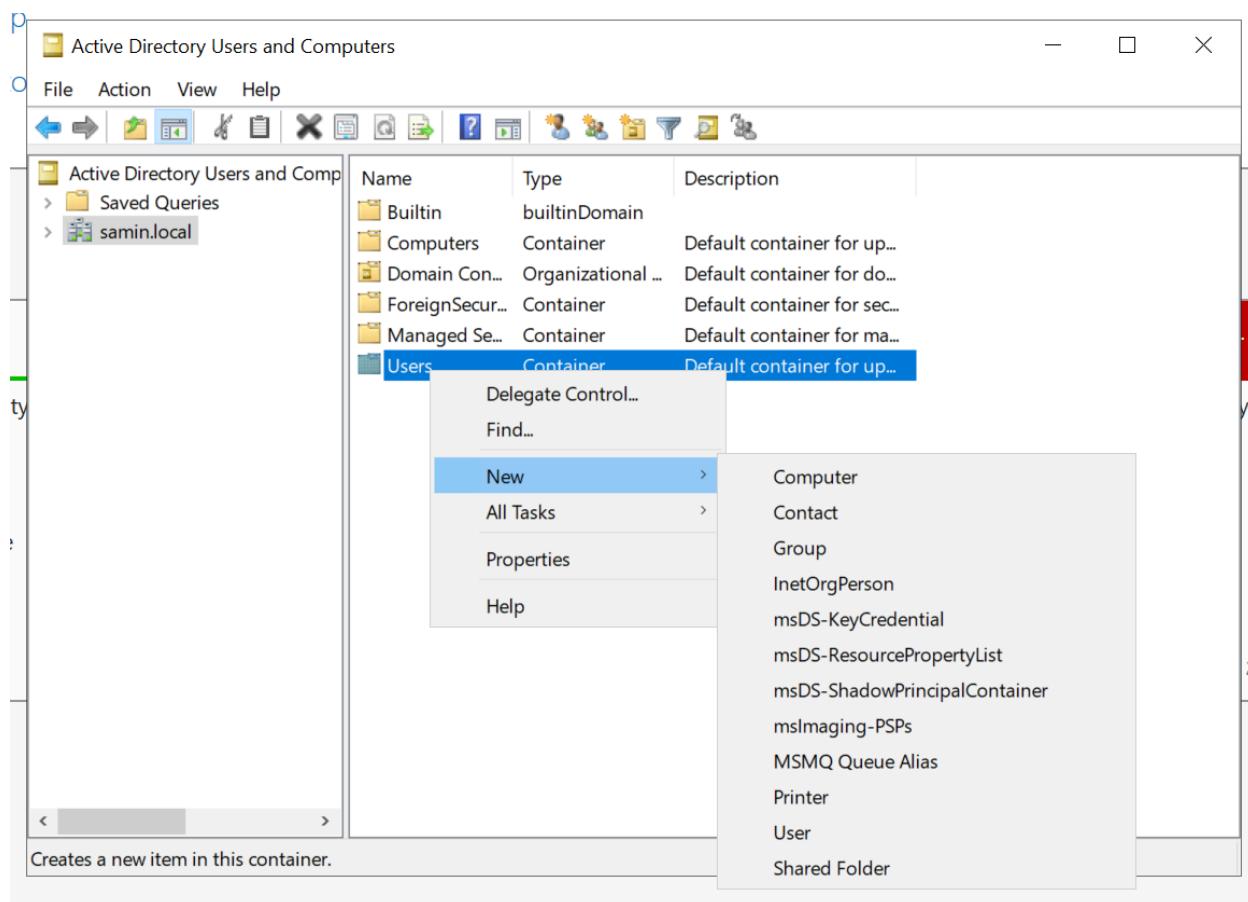
Hit “Next” until you are able to click “Configure”:



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

X



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

Active Directory Users and Computers

New Object - User

Create in: samin.local/Users

>Password: ······

Confirm ······

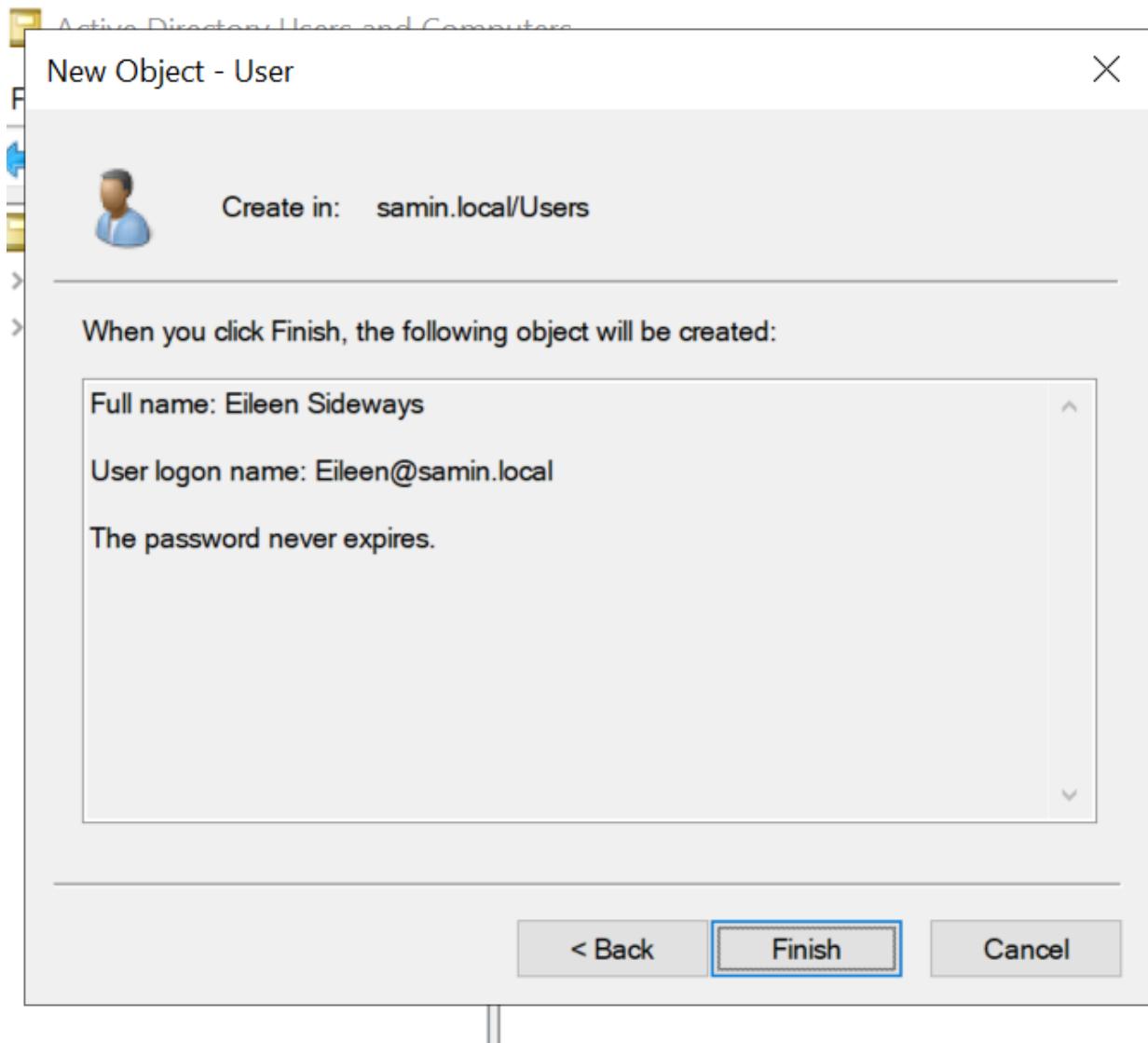
User must change password at next logon

User cannot change password

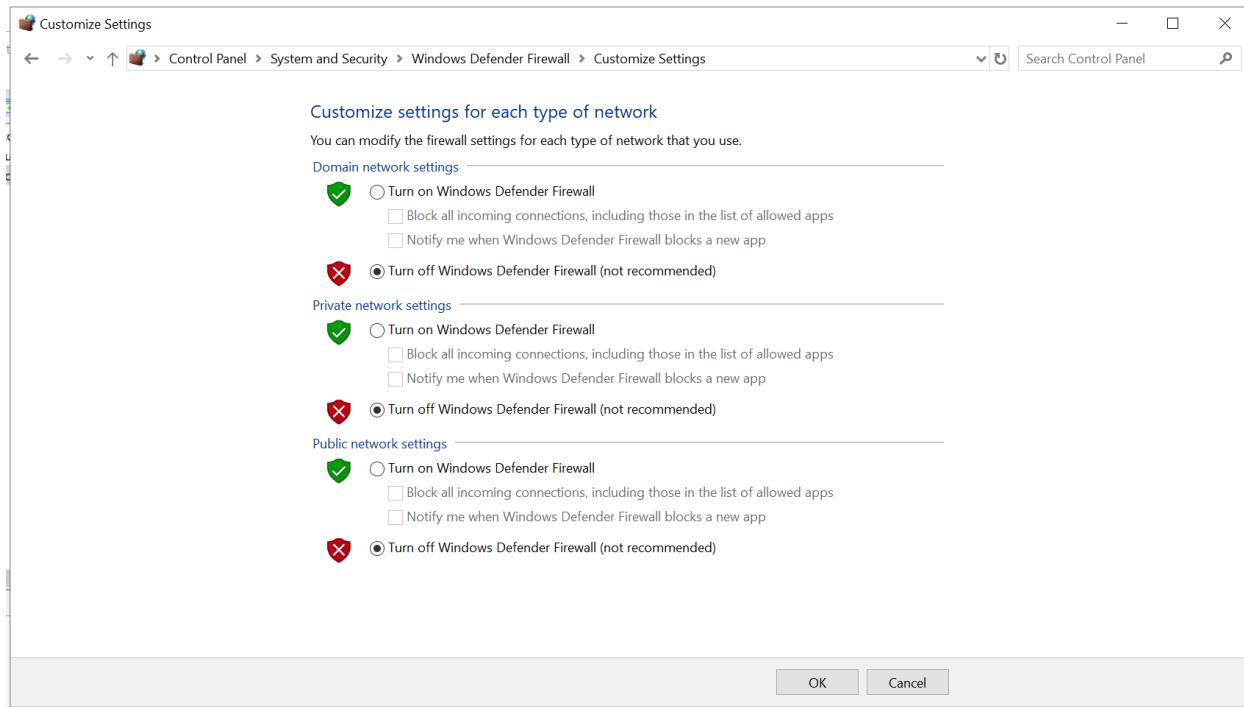
Password never expires

Account is disabled

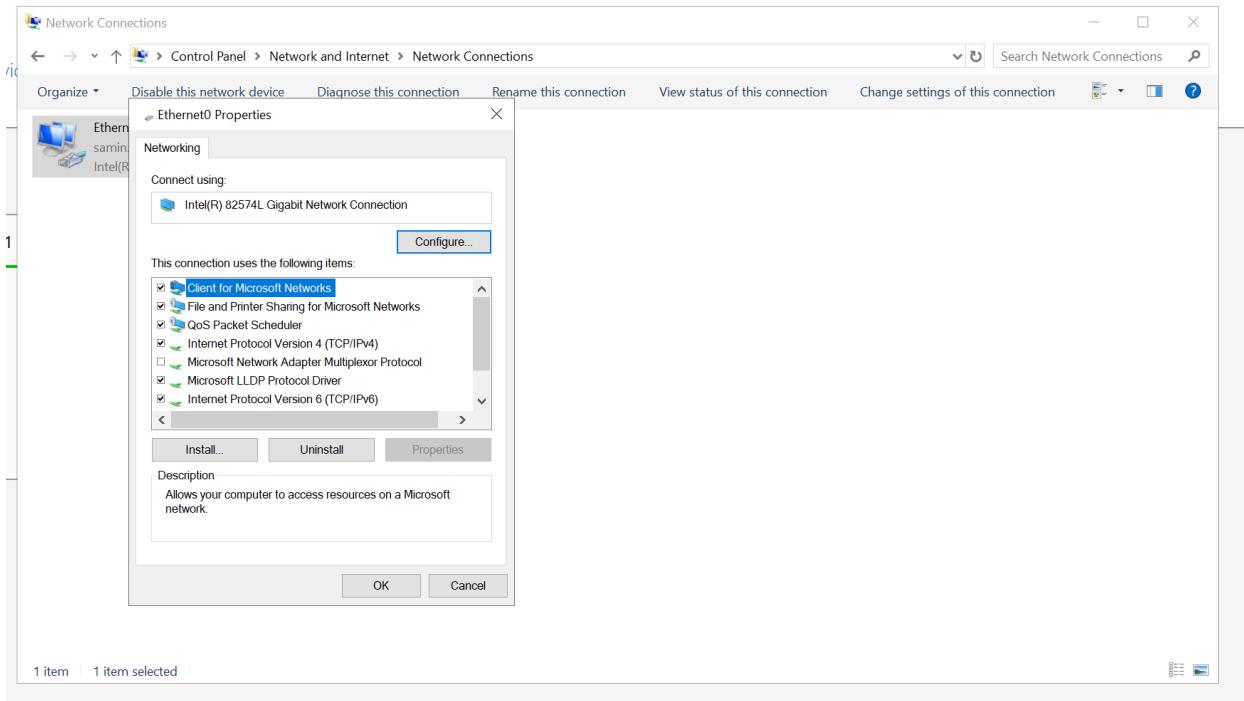
< Back Next > Cancel



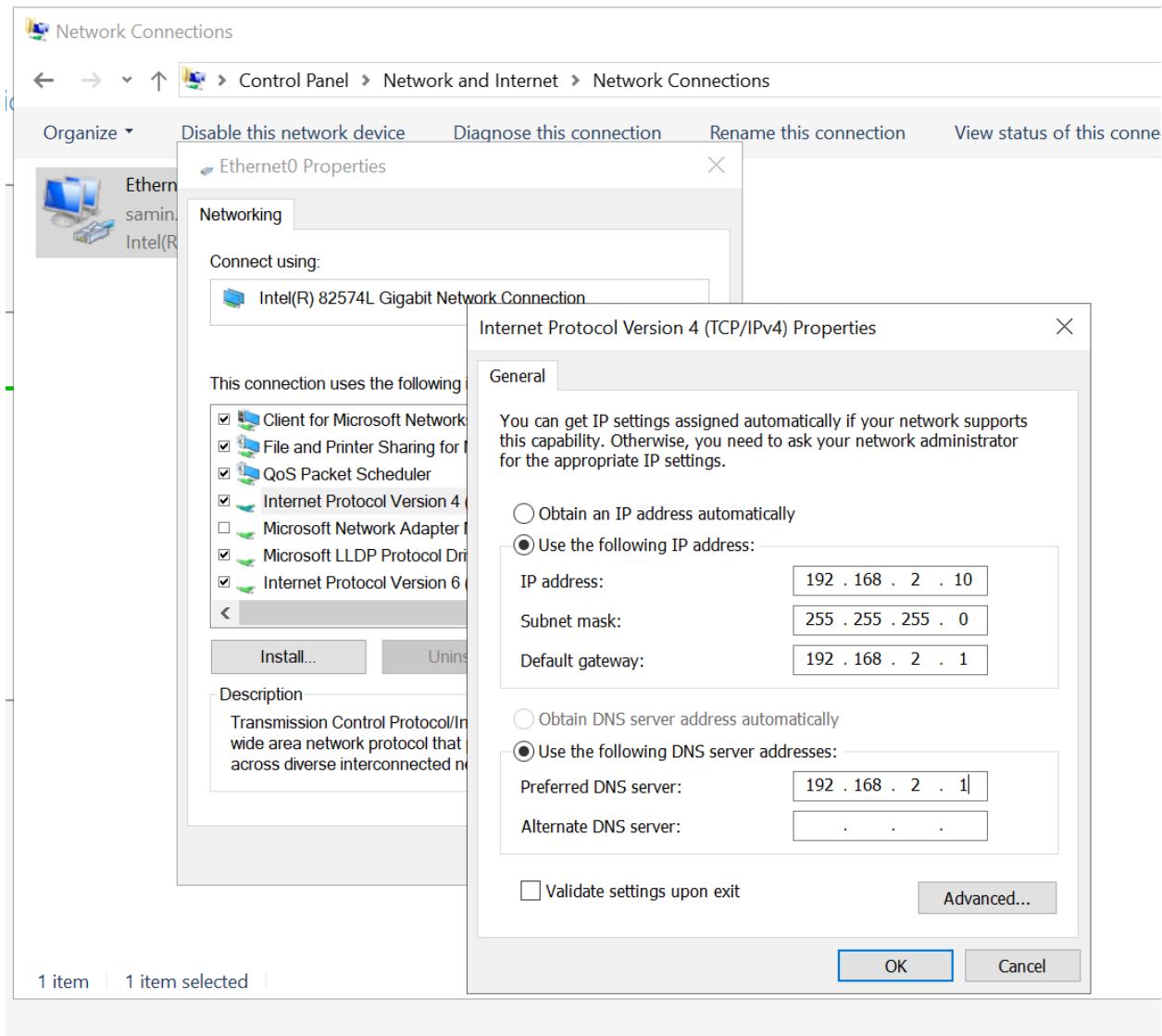
After clicking finish and adding the user, search up Windows Defender Firewall on Windows and turn them all off:



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:

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	<input type="checkbox"/> Enable DHCP server on VICTIMNETWORK interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<input type="button" value="Allow all clients"/> <small>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.</small>
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject <small>This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.</small>
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request <small>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.</small>

Primary Address Pool

Subnet	192.168.2.0/24
Subnet Range	192.168.2.1 - 192.168.2.254
Address Pool Range	<input type="text" value="From"/> <input type="text" value="To"/> <small>The specified range for this pool must not be within the range configured on any other address pool for this interface.</small>
Additional Pools	<input type="button" value="+ Add Address Pool"/>
<small>If additional pools of addresses are needed inside of this subnet outside the above range, they may be specified here.</small>	

Server Options

WINS Servers	<input type="text" value="WINS Server 1"/> <input type="text" value="WINS Server 2"/>
DNS Servers	<input type="text" value="192.168.2.10"/> <input type="text" value="DNS Server 2"/> <input type="text" value="DNS Server 3"/> <input type="text" value="DNS Server 4"/>

OMAPI

OMAPI Port	<input type="text" value="OMAPI Port"/>
<small>Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable. Only the first OMAPI configuration is used.</small>	
OMAPI Key	<input type="text" value="OMAPI Key"/> <div style="display: flex; justify-content: space-between;"> <input type="checkbox"/> Generate New Key <small>Generate a new key based on the selected algorithm.</small> </div>
Key Algorithm	<input type="button" value="HMAC-SHA256 (current bind9 default)"/> <small>Set the algorithm that OMAPI key will use.</small>

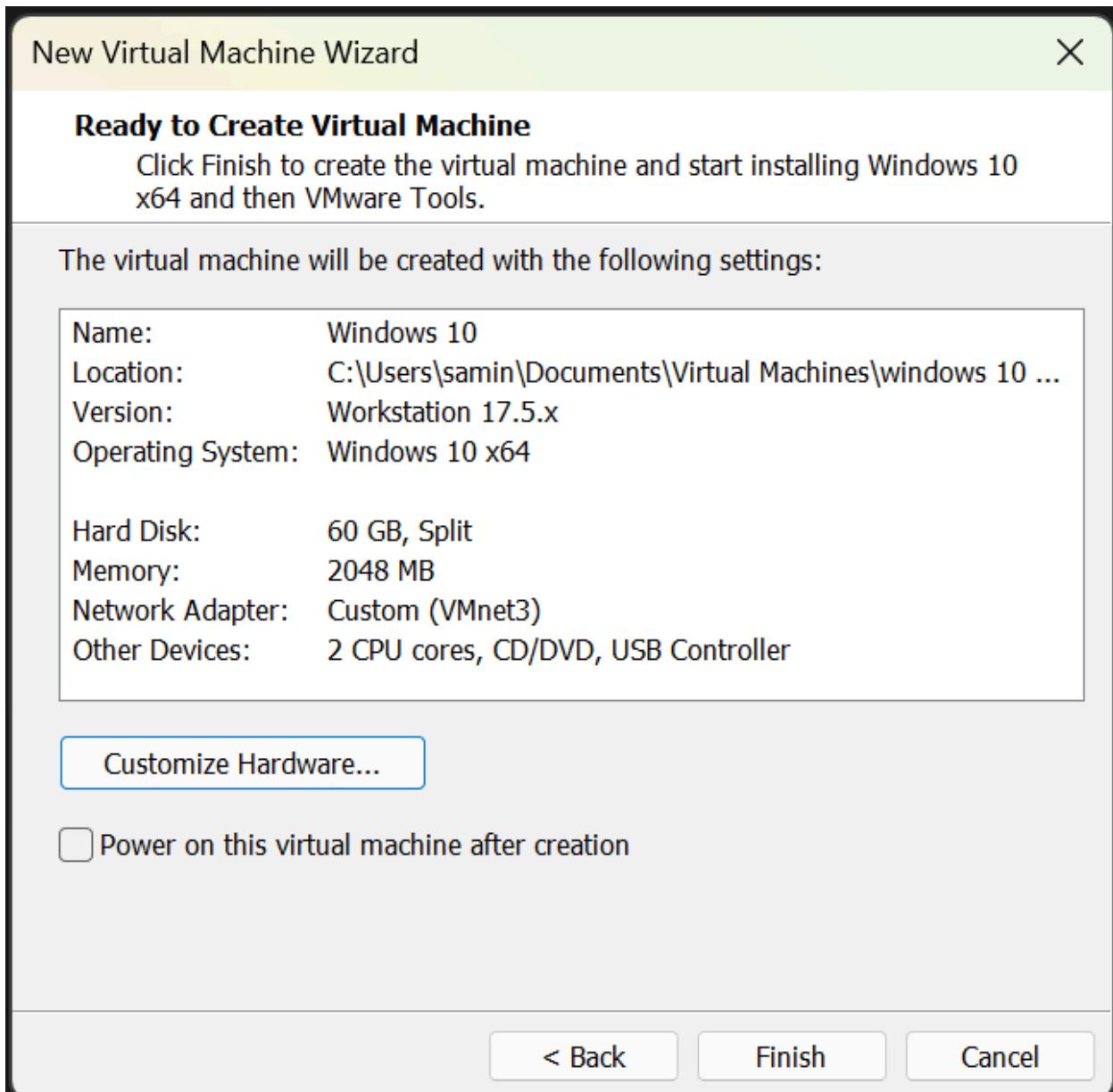
Other DHCP Options

Gateway	<input type="text" value="192.168.2.1"/>
<small>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.</small>	
Domain Name	<input type="text" value="samin.local"/>

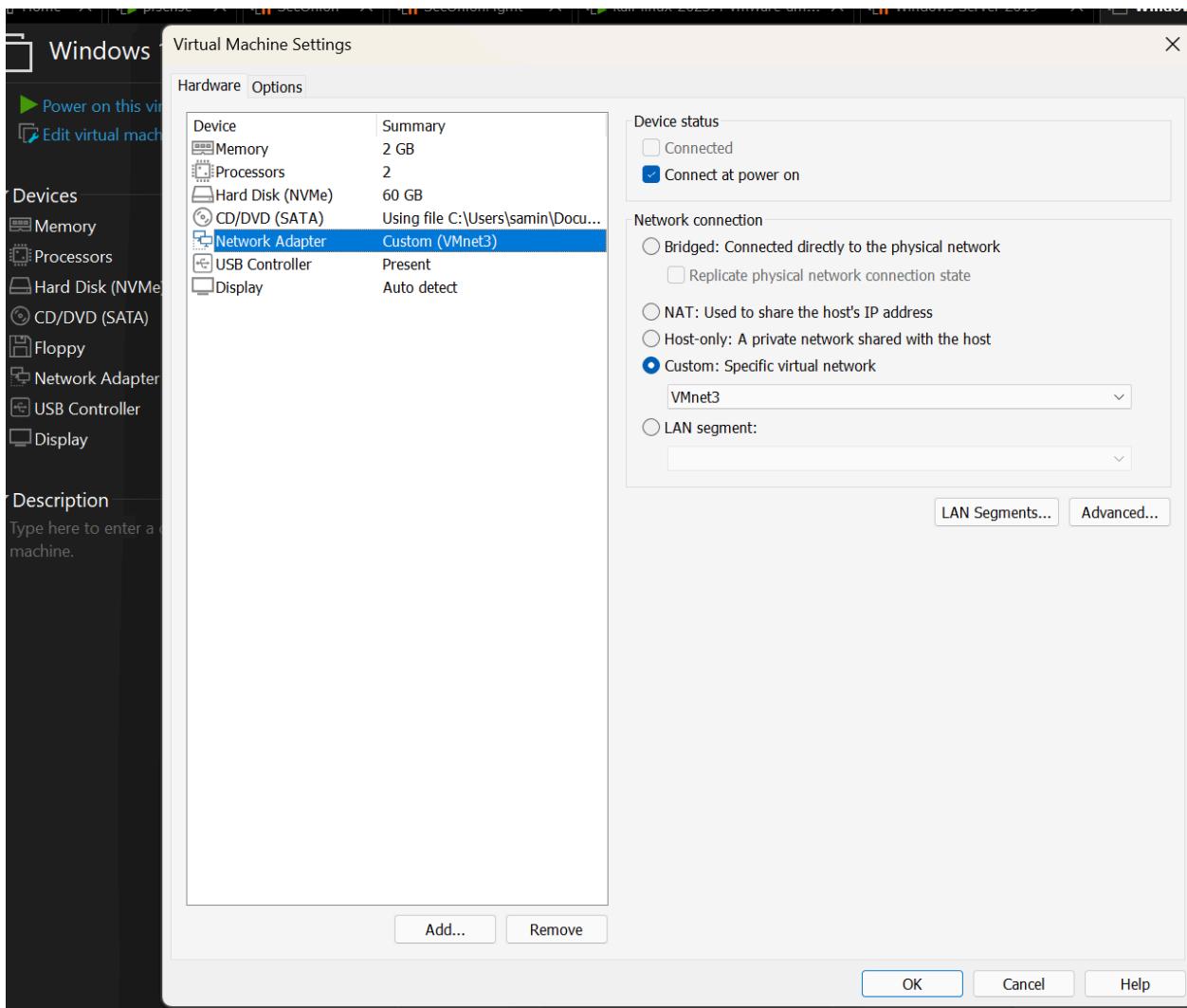
Save and apply the changes

Now, create a new virtual machine using the Windows 10 ISO file downloaded from their [website](#)

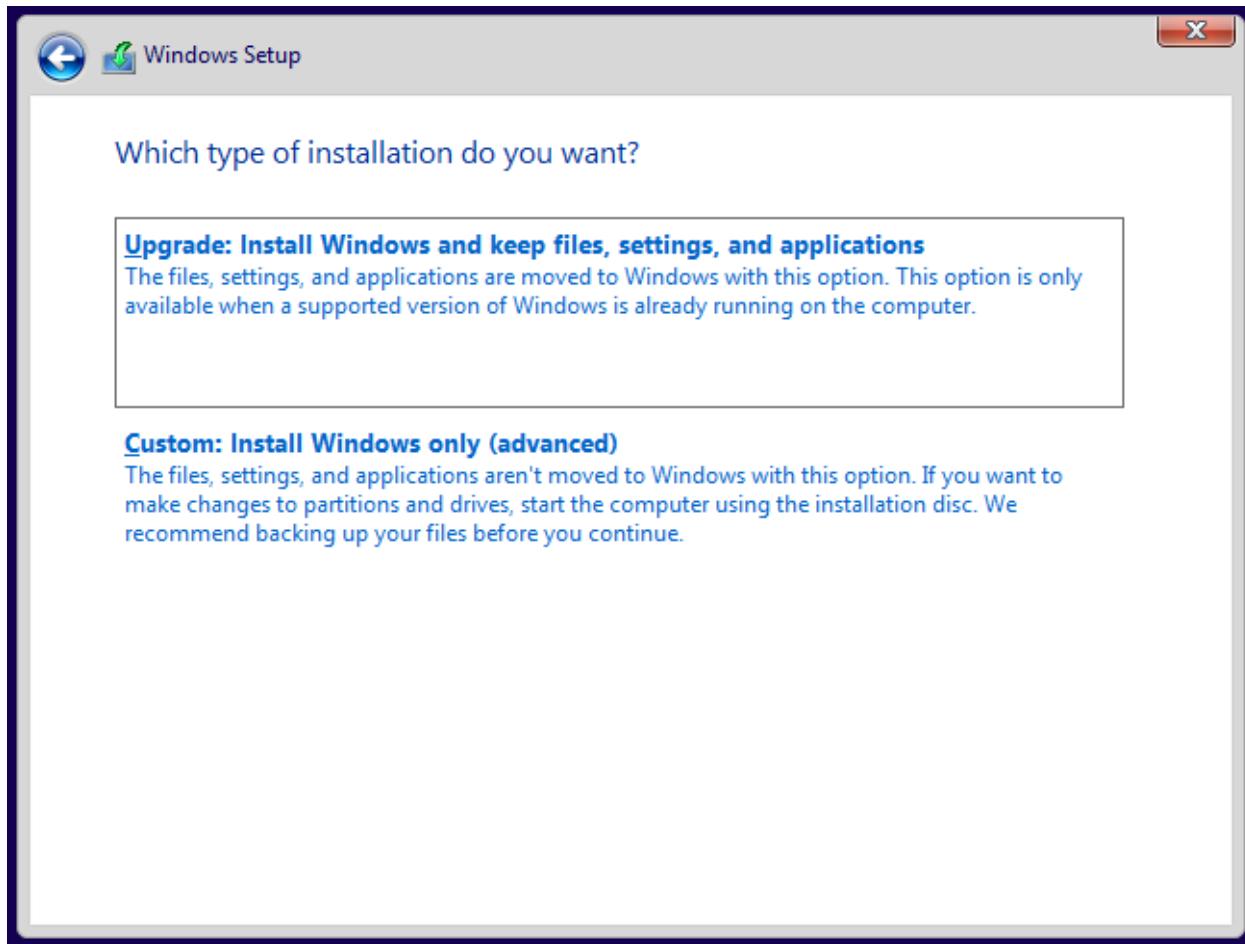
Using this ISO file, configure a new virtual machine, similar to the Windows Server machine configured earlier. Ensure that the Network Adapter is changed to Vmnet3 and “Power on this virtual machine after creation” is unchecked:



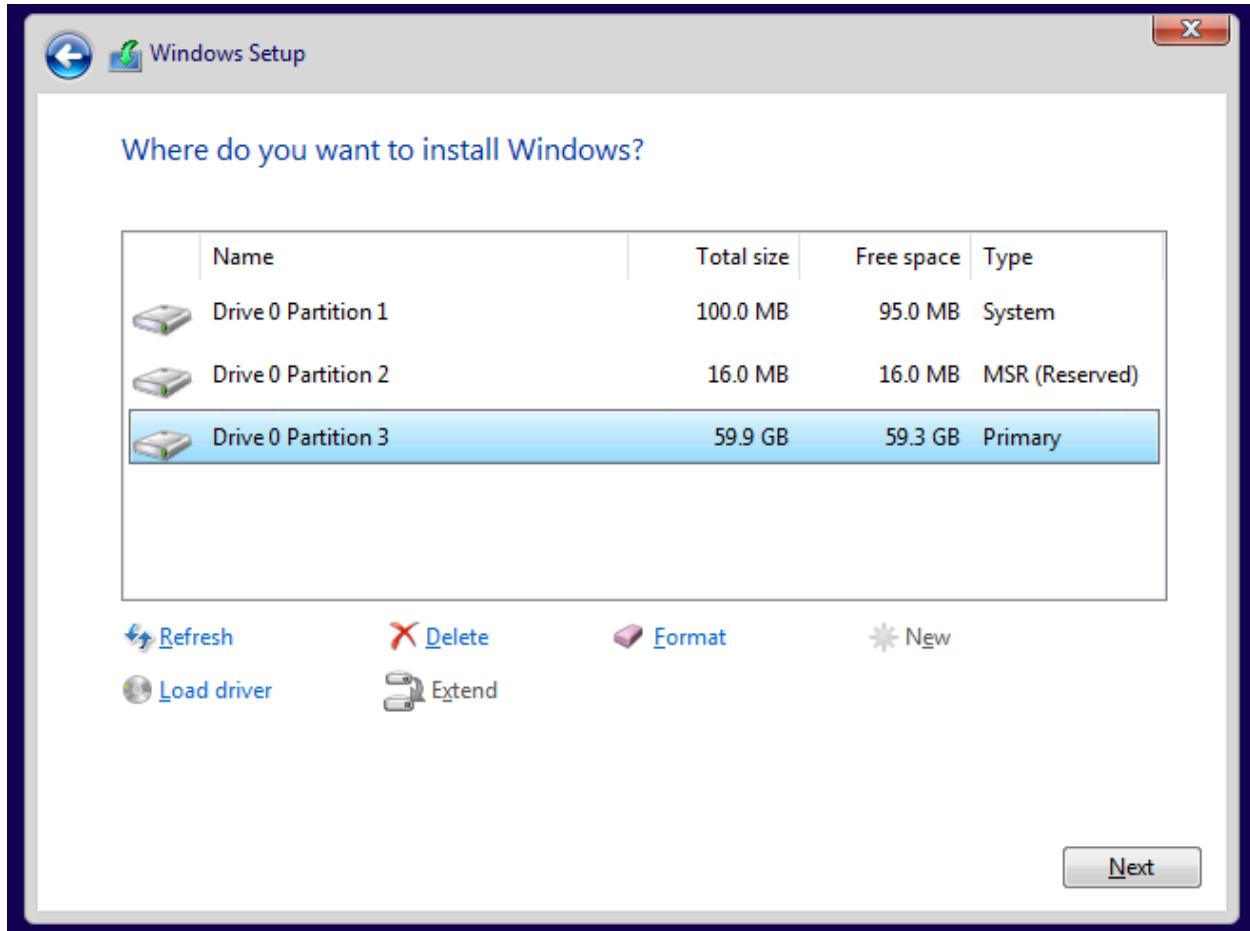
Click “Finish”, and before powering on the machine edit the settings again to remove the Floppy drive:



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”:

Let's connect you to a network

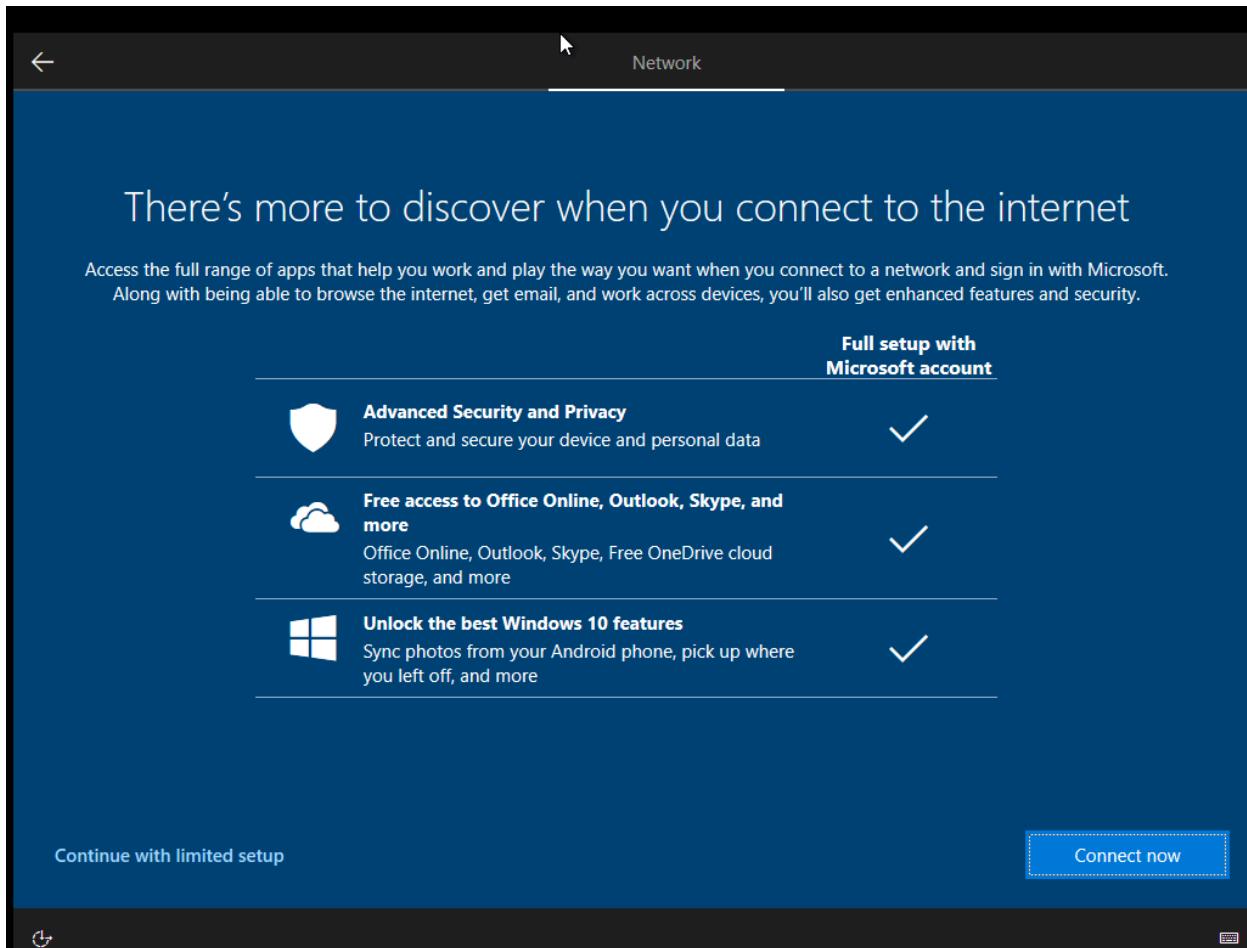
To finish setup, you'll need to connect to the internet.



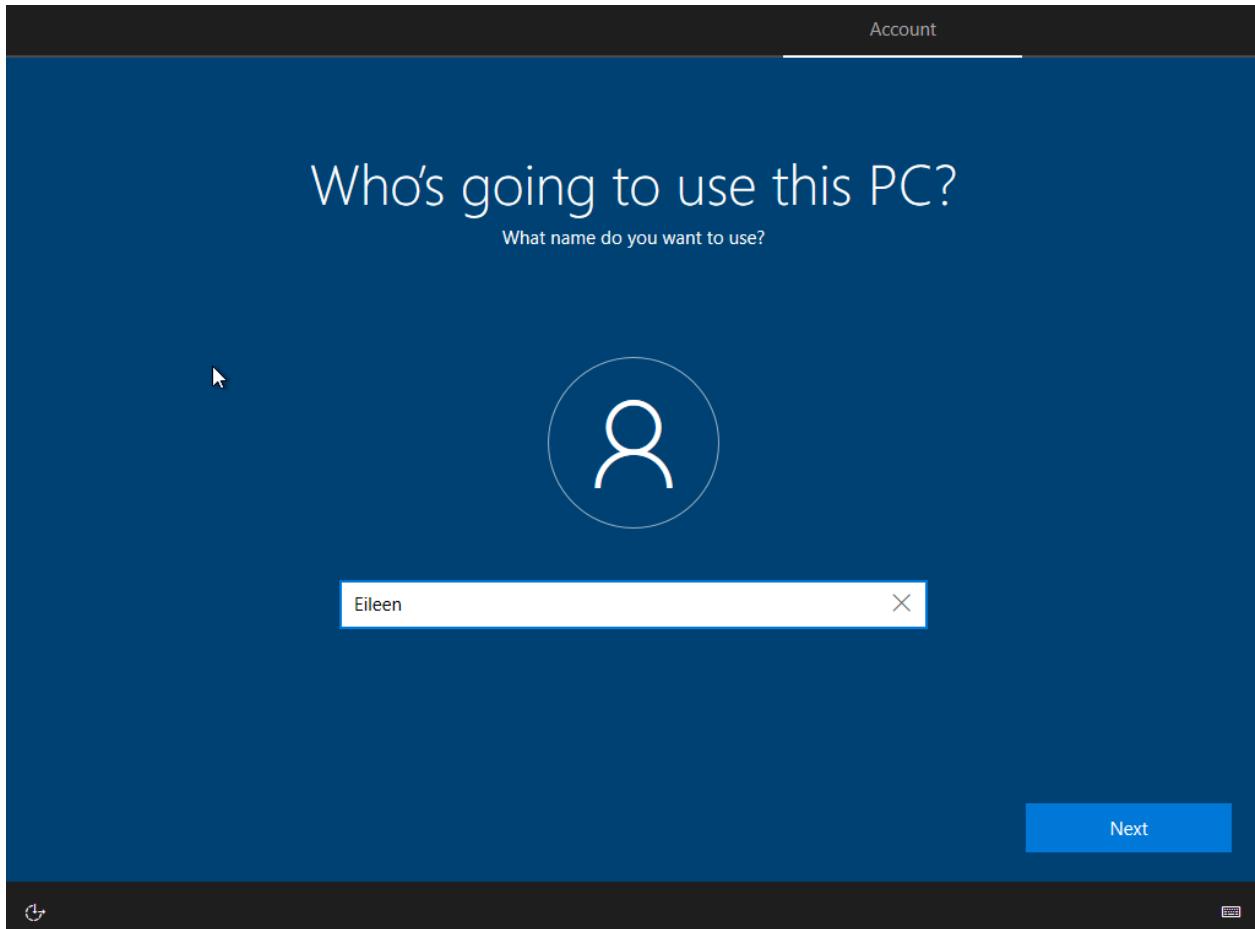
Unidentified network
No Internet

I don't have internet

Select “Continue with limited setup”:



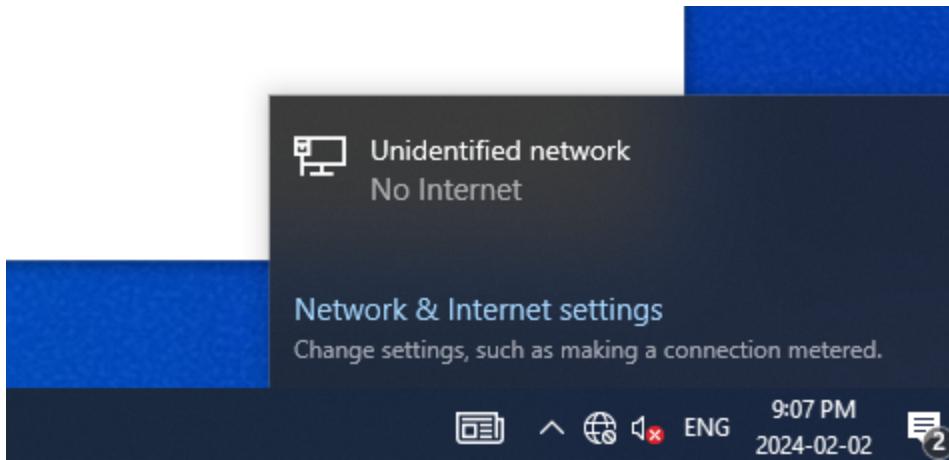
Set a name and password:



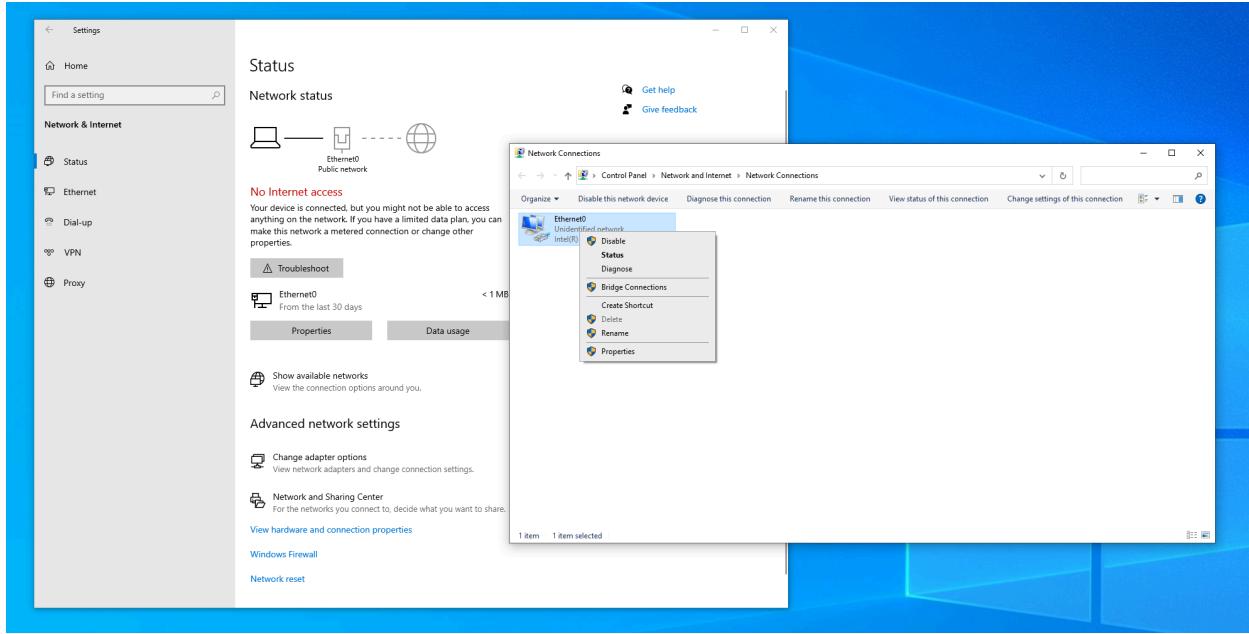
You can set the security questions to be whatever you want. For the rest of the configurations, select “No” whenever it is the option and don’t share the optional data.

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.

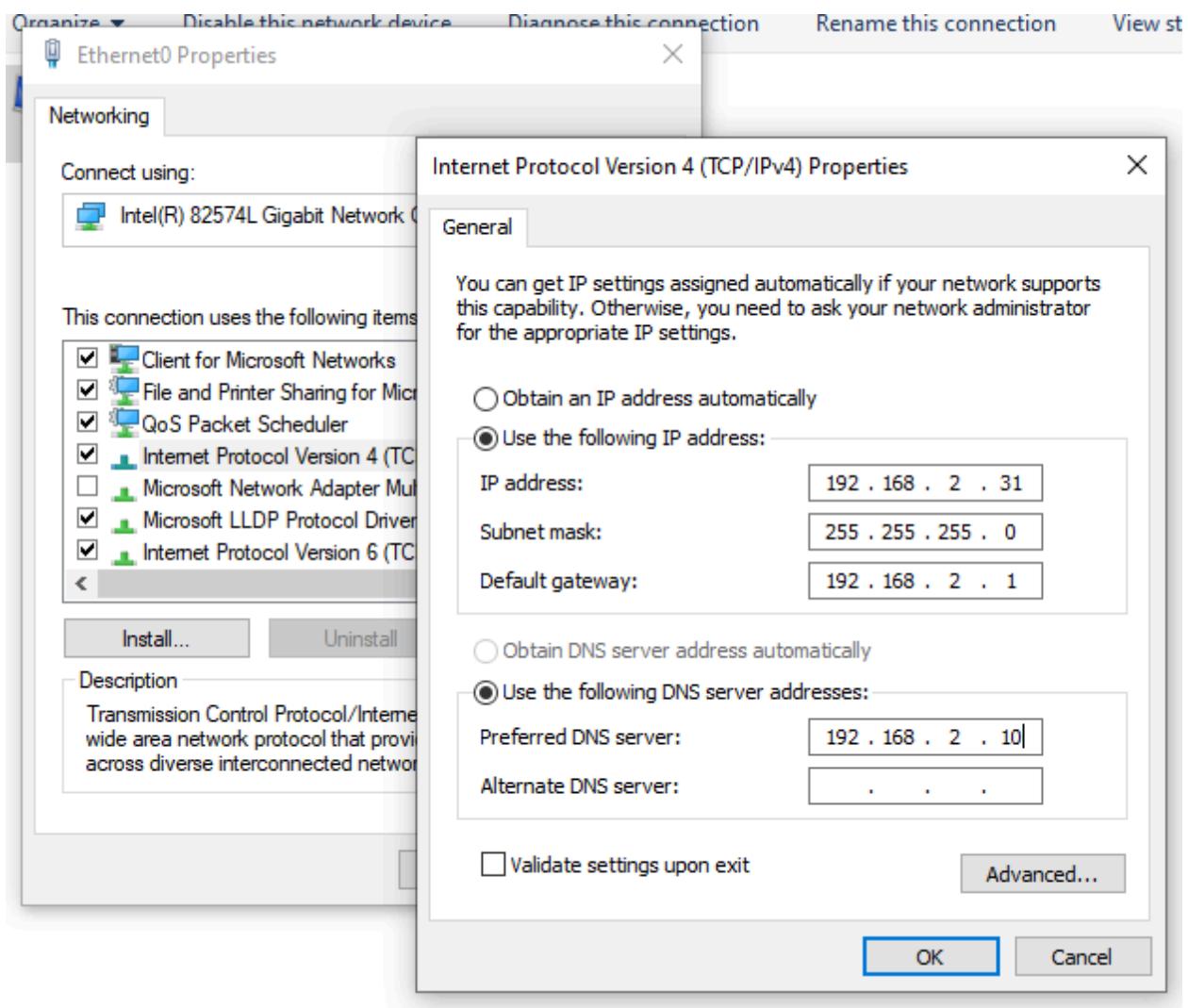
After logging in again, open up the network and internet settings from the bottom right hand corner:



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



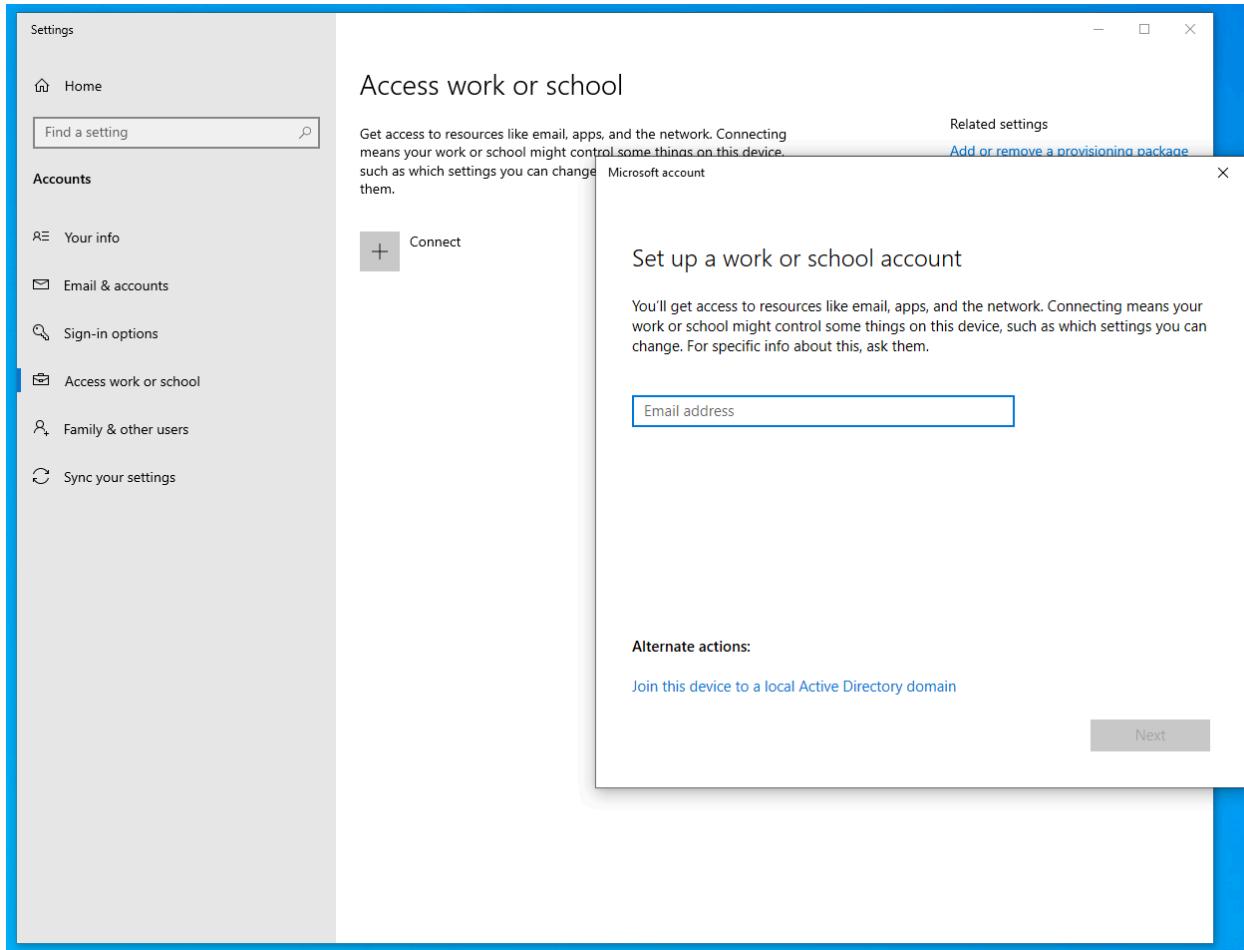
Click on the IPv4 line and configure as follows:



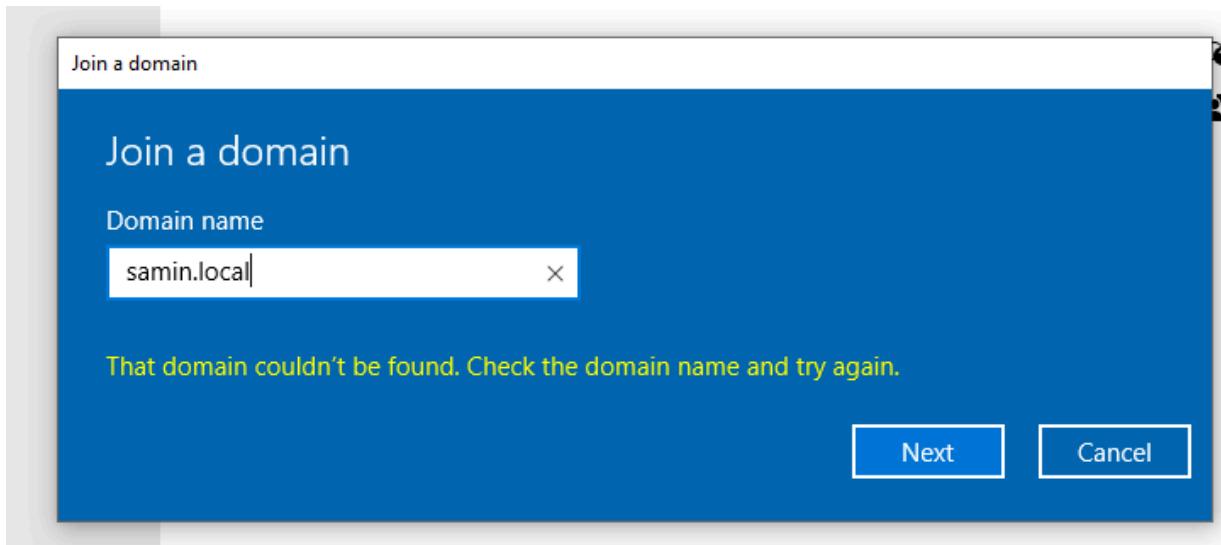
Click “OK” to exit out of the pop-ups and close everything else opened

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

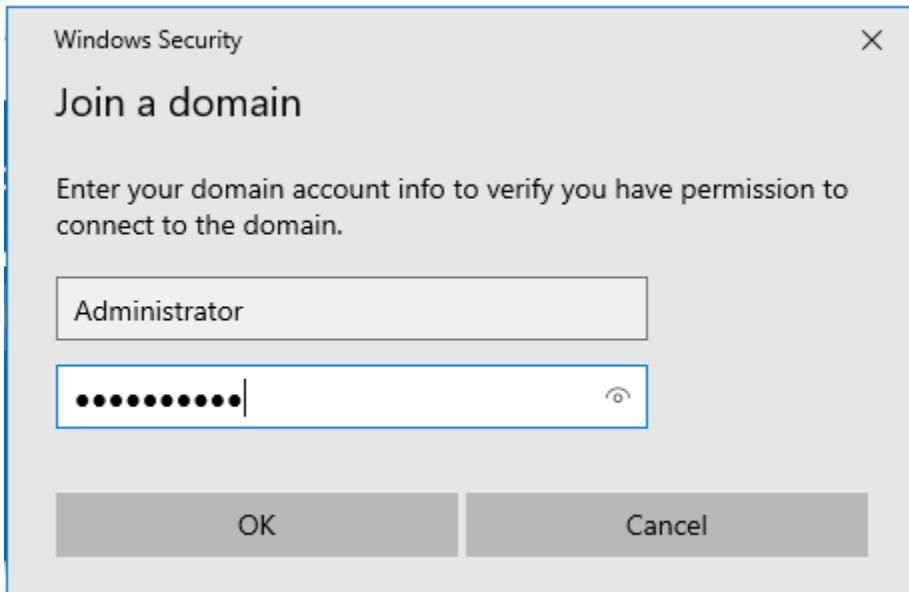
Select “Join this device to local Active Directory Domain”:



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

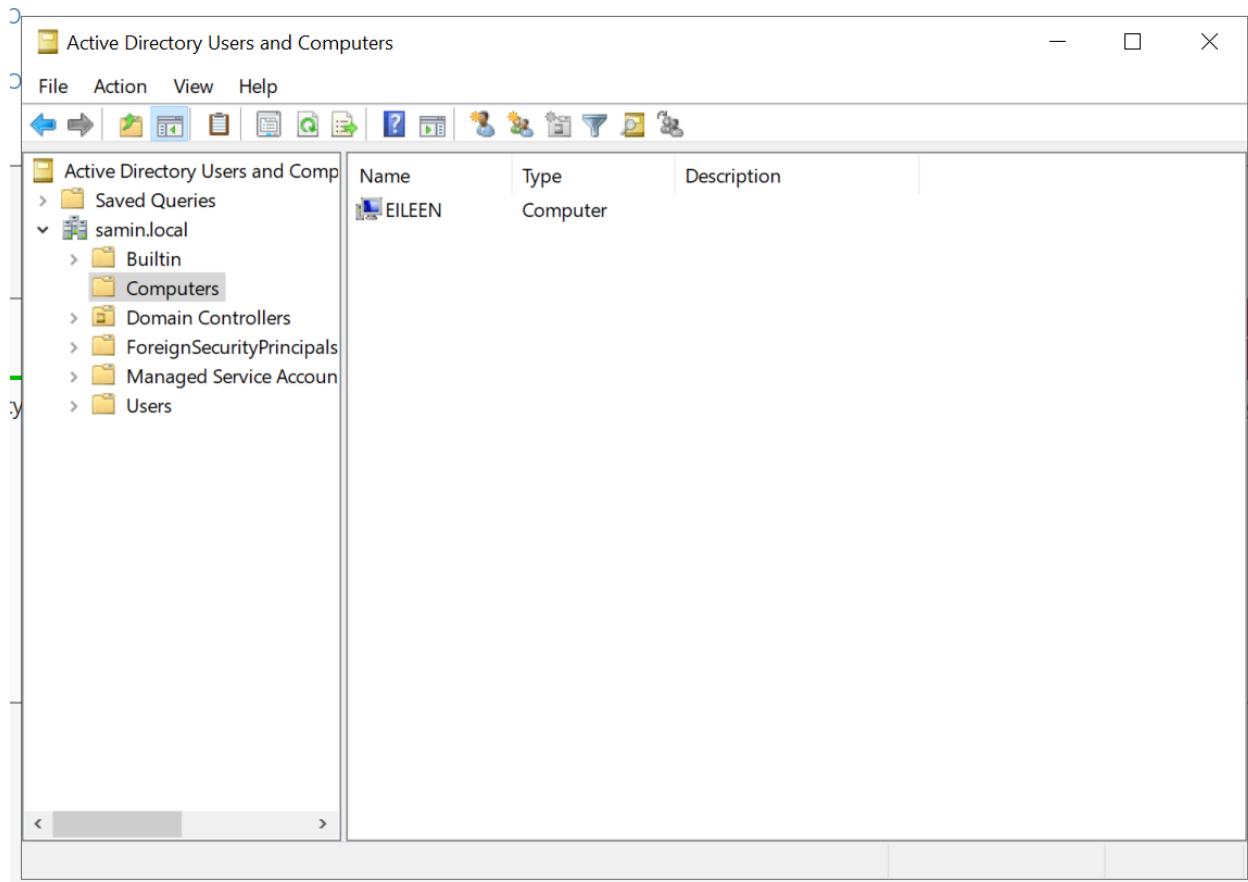


Enter in the username and password:



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):

Recommended size for Ubuntu 64-bit: 20 GB

- Store virtual disk as a single file
- Split virtual disk into multiple files

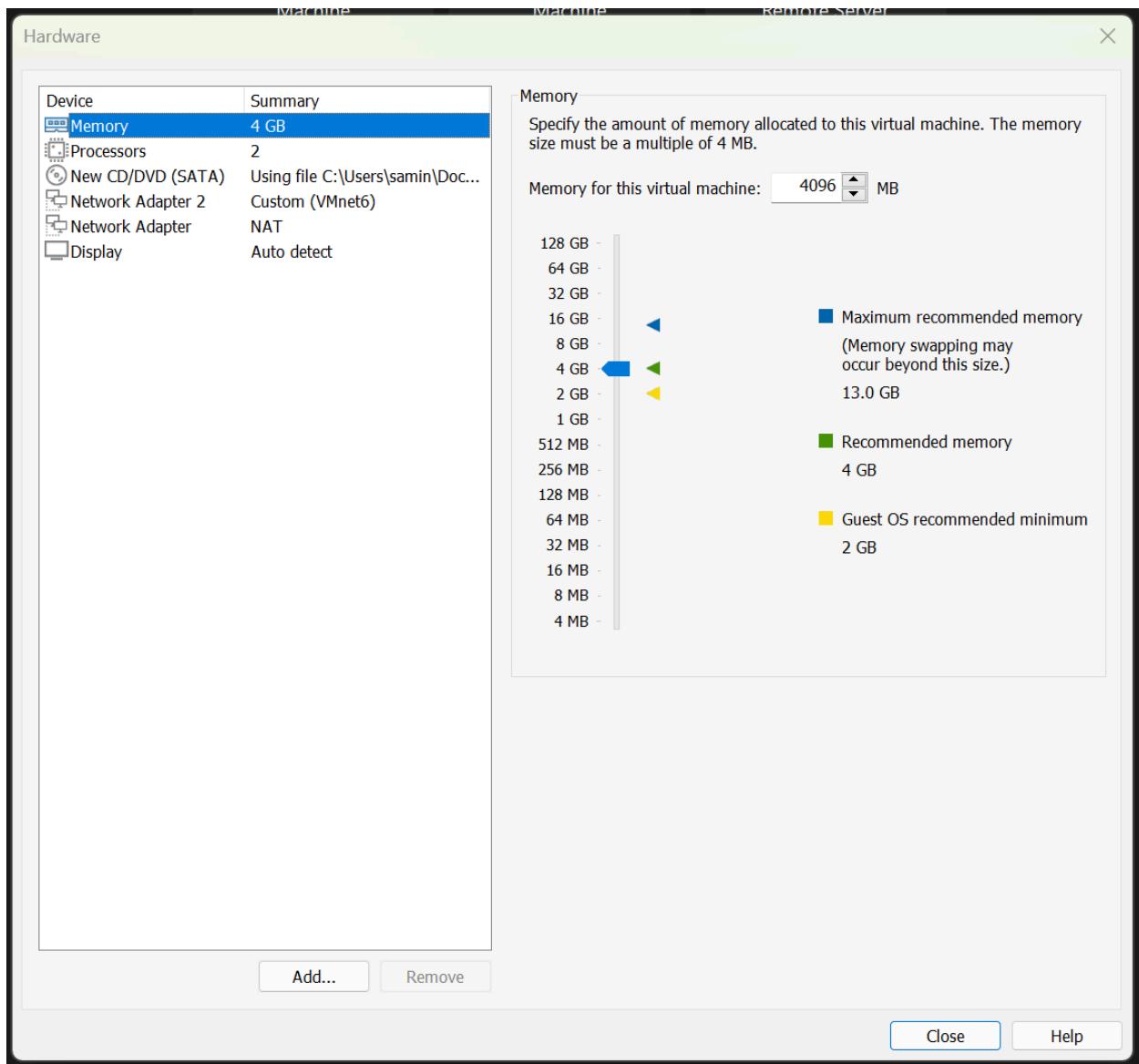
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.

Help

< Back

Next >

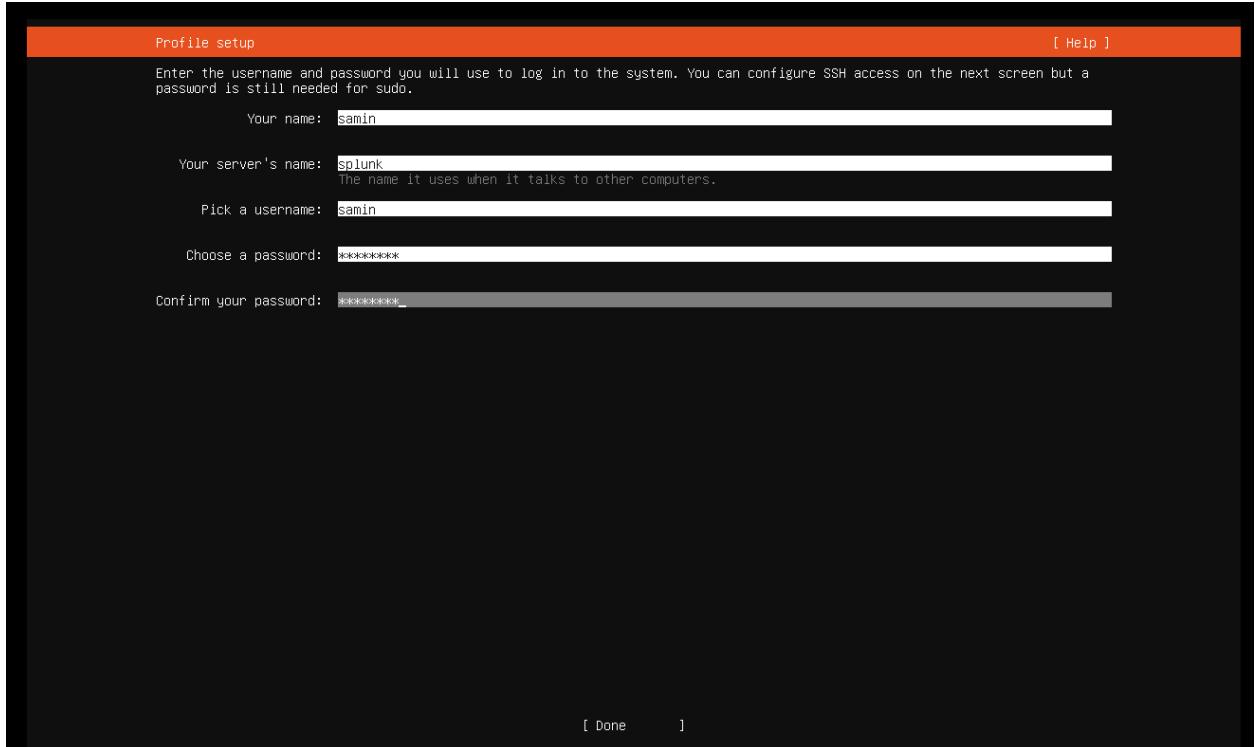
Cancel



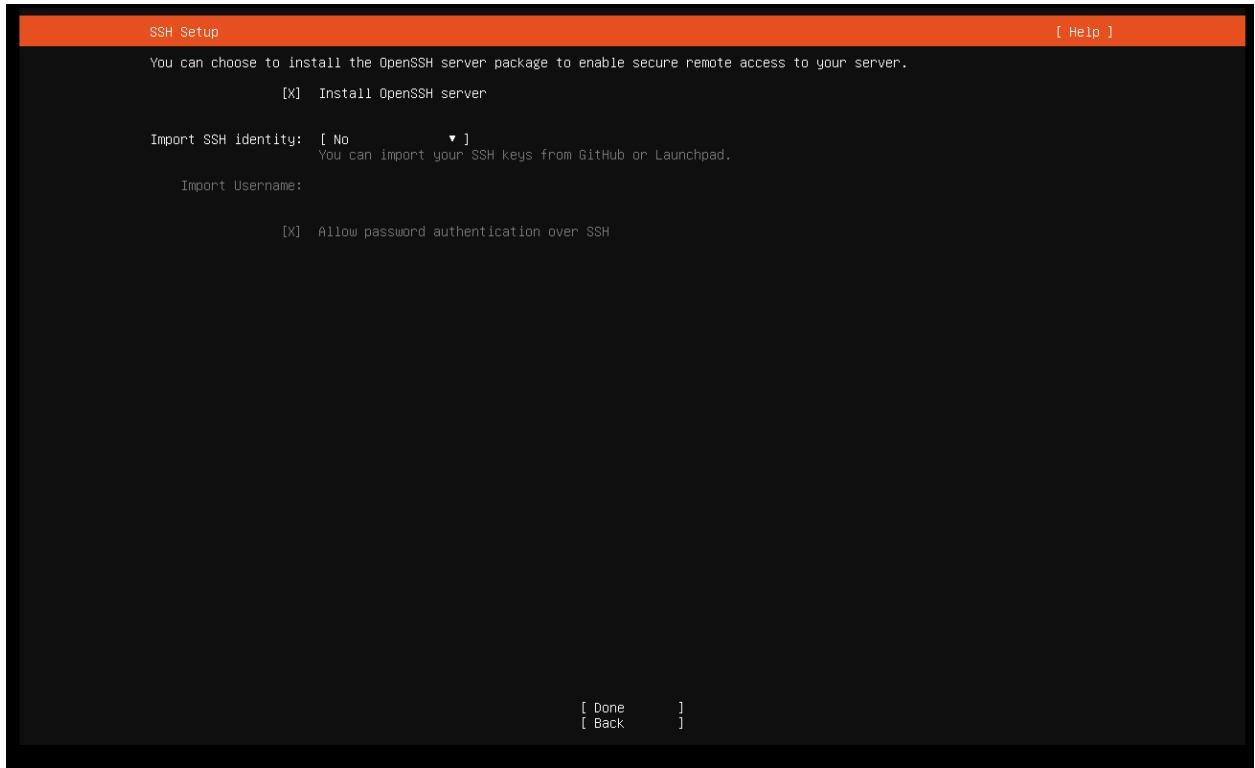
Try and install ubuntu

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:

```
Installing system [ Help ]  
subiquity/Late/apply_autoinstall_config  
configuring apt  
    curtin command in-target  
installing system  
executing curtin install initial step  
executing curtin install partitioning step  
    curtin command install  
    configuring storage  
        running 'curtin block-meta simple'  
        curtin command block-meta  
        removing previous storage devices  
        configuring disk: disk-sda  
        configuring partition: partition-0  
        configuring partition: partition-1  
        configuring format: format-0  
        configuring partition: partition-2  
        configuring lvm_volumegroup: lvm_volumegroup-0  
        configuring lvm_partition: lvm_partition-0  
        configuring format: format-1  
        configuring mount: mount-1  
        configuring mount: mount-0  
executing curtin install extract step  
    curtin command install  
        writing install sources to disk  
        running 'curtin extract'  
        curtin command extract  
            acquiring and extracting image from cp:///tmp/tmpypppe6q7n/mount  
executing curtin install curthooks step  
    curtin command install  
        configuring installed system  
        running 'curtin in-target -- setupcon --save-only'  
        curtin command in-target  
        running 'curtin curthooks'  
        curtin command curthooks  
            configuring apt  
            configuring apt  
            installing missing packages  
            configuring iscsi service  
            configuring raid (mdadm) service  
            installing Kernel \  
[ View full log ]
```

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

```
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%
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:~$
```

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

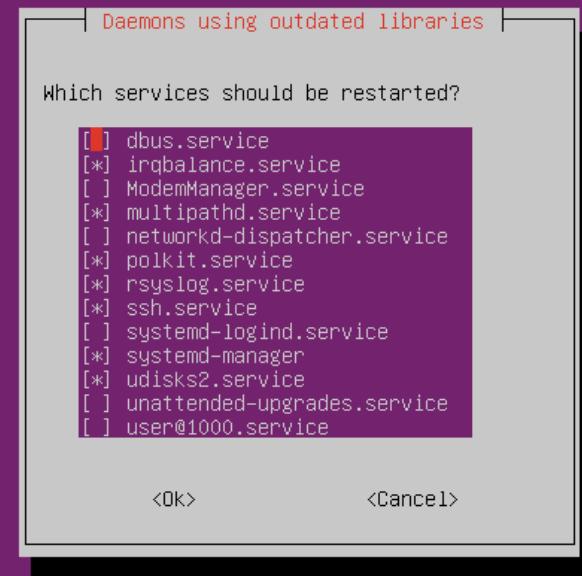
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

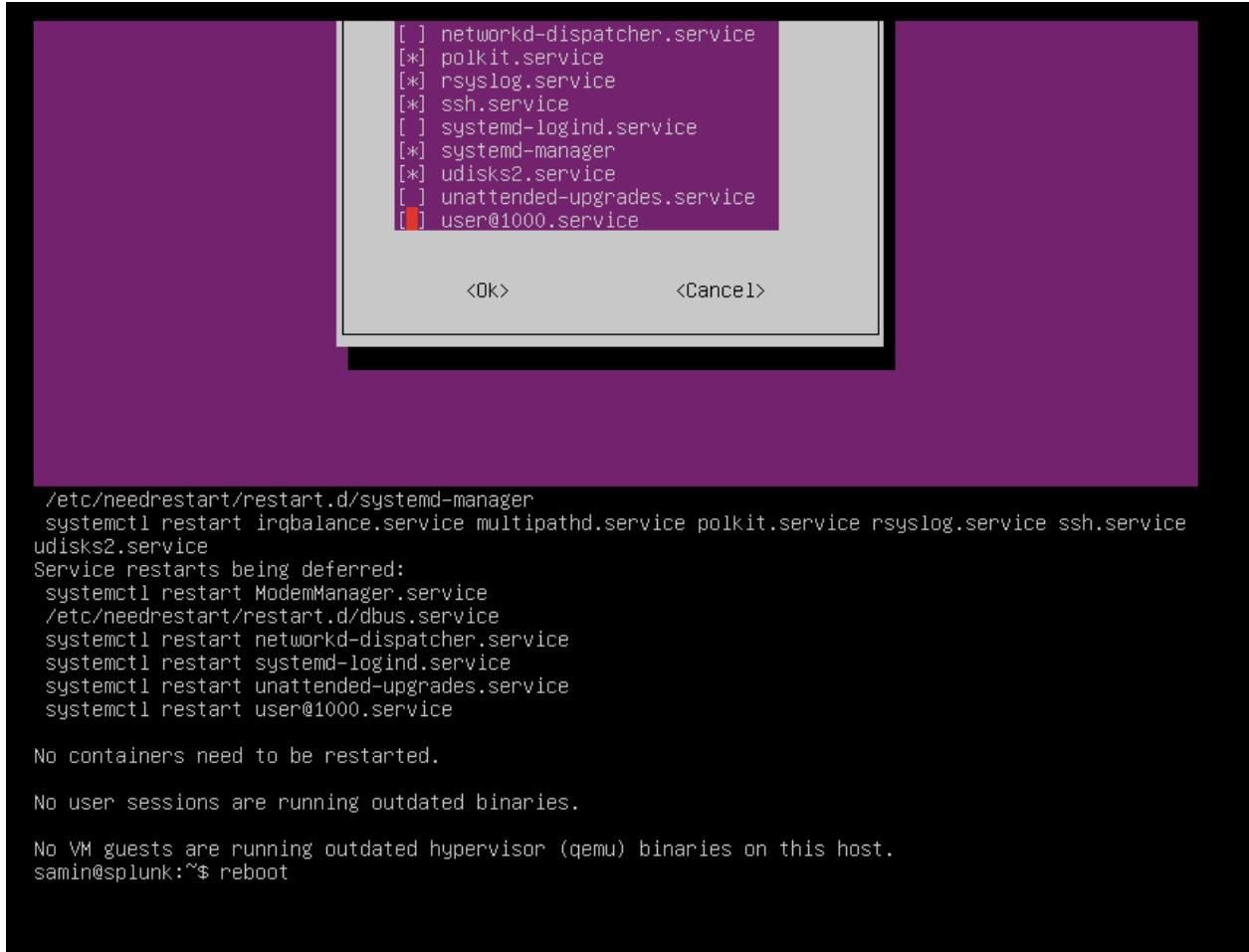
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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





The terminal window displays a list of services with their status (active or inactive). A service named 'user@1000.service' is highlighted in red, indicating it is active. Below the list are two buttons: '<OK>' and '<Cancel>'.

```
[ ] networkd-dispatcher.service
[*] polkit.service
[*] rsyslog.service
[*] ssh.service
[ ] systemd-logind.service
[*] systemd-manager
[*] udisks2.service
[ ] unattended-upgrades.service
[!] user@1000.service

<OK> <Cancel>
```

The terminal session continues with the following commands and output:

```
/etc/needrestart/restart.d/systemd-manager
systemctl restart irqbalance.service multipathd.service polkit.service rsyslog.service ssh.service
udisks2.service
Service restarts being deferred:
systemctl restart ModemManager.service
/etc/needrestart/restart.d/dbus.service
systemctl restart networkd-dispatcher.service
systemctl restart systemd-logind.service
systemctl restart unattended-upgrades.service
systemctl restart user@1000.service

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:~$ reboot
```

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 Downloads

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](#)

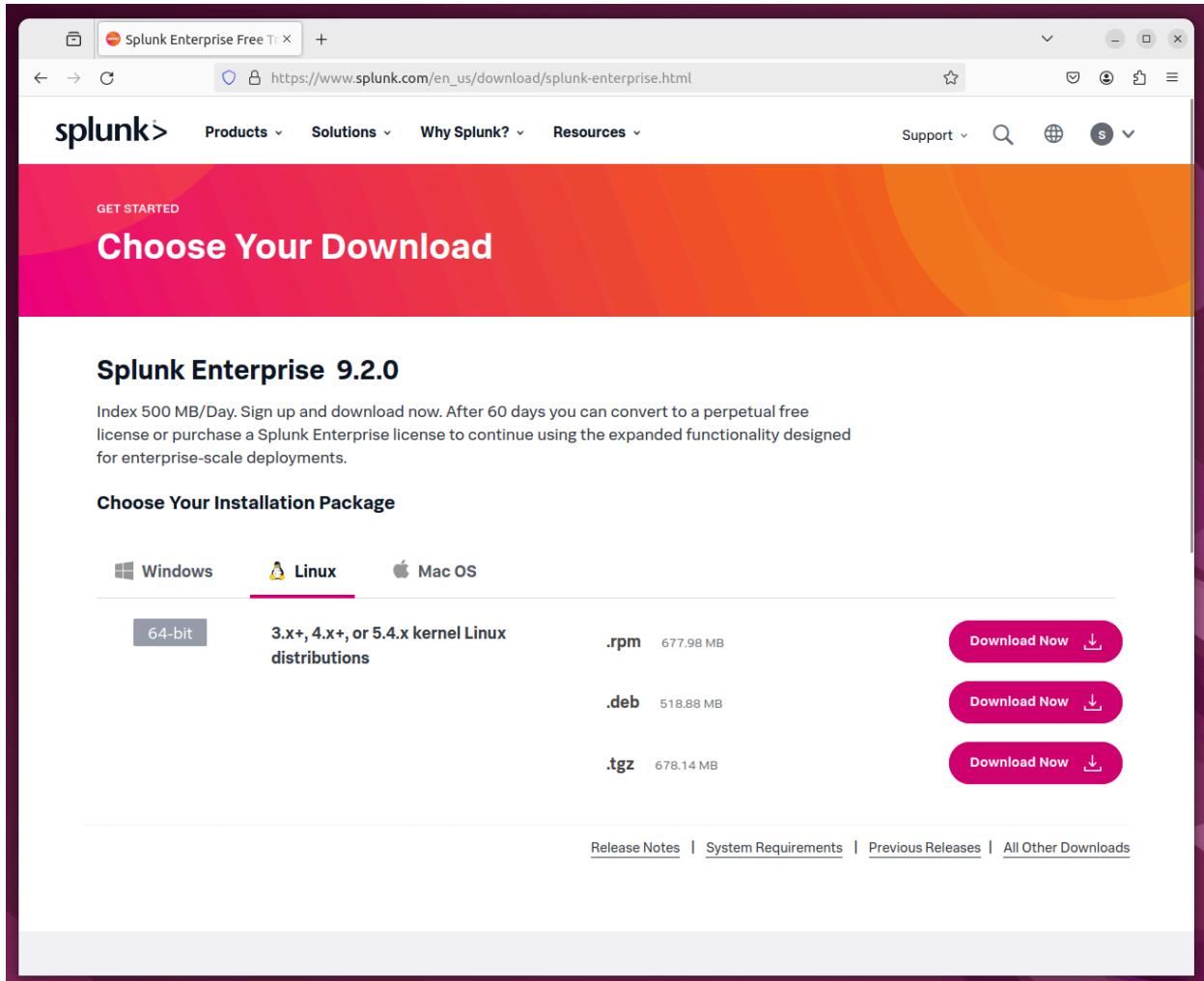


Splunk Enterprise

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](#)





The screenshot shows a web browser displaying the Splunk website at https://www.splunk.com/en_us/download/splunk-enterprise.html. The page is titled "Choose Your Download" and features a prominent "Splunk Enterprise 9.2.0" section. It provides a brief overview: "Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments." Below this, there's a "Choose Your Installation Package" section with tabs for Windows, Linux (selected), and Mac OS. Under the Linux tab, the "64-bit" option is selected. It lists three download links: ".rpm" (677.98 MB), ".deb" (518.88 MB), and ".tgz" (678.14 MB), each accompanied by a "Download Now" button.

GET STARTED

Choose Your Download

Splunk Enterprise 9.2.0

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

Windows **Linux** Mac OS

64-bit

3.x+, 4.x+, or 5.4.x kernel Linux distributions

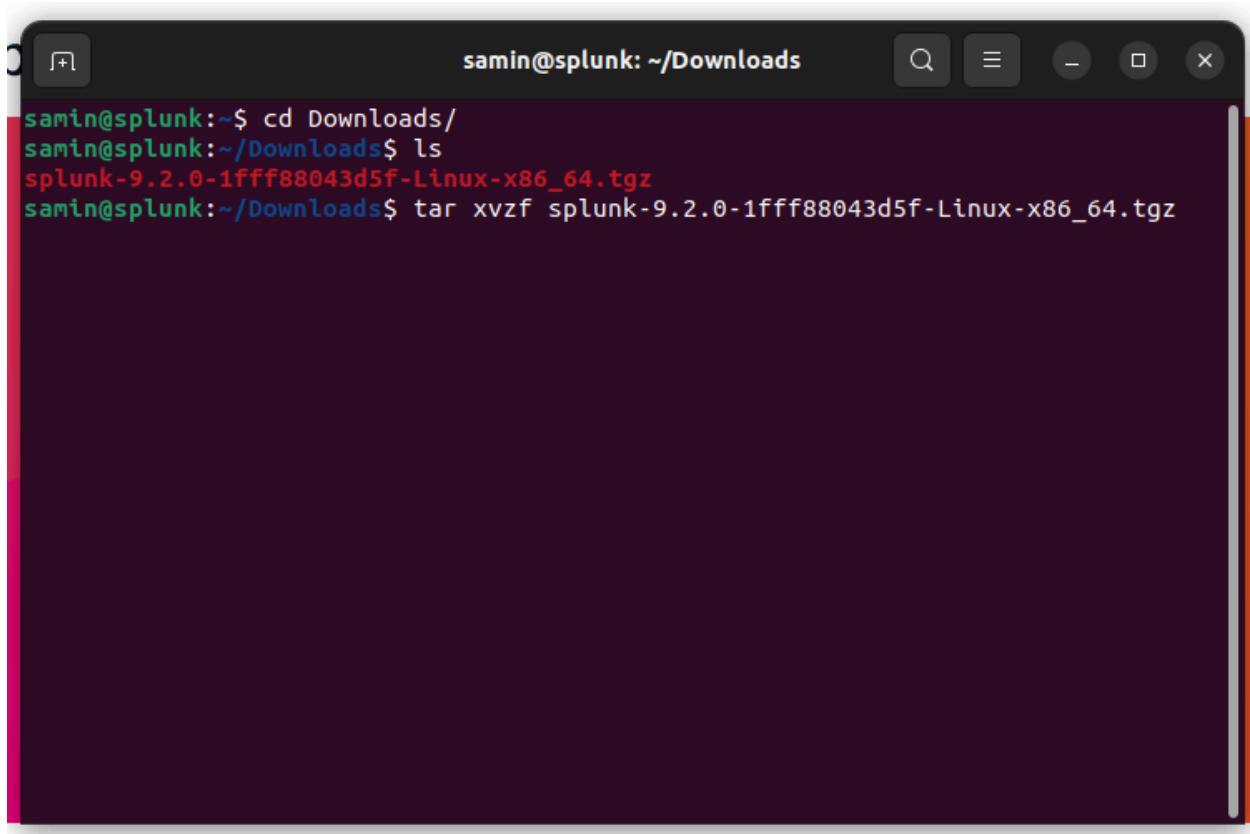
.rpm 677.98 MB [Download Now](#)

.deb 518.88 MB [Download Now](#)

.tgz 678.14 MB [Download Now](#)

[Release Notes](#) | [System Requirements](#) | [Previous Releases](#) | [All Other Downloads](#)

Open up a terminal and unzip the file:



A screenshot of a terminal window titled "samin@splunk: ~/Downloads". The terminal shows the following command sequence:

```
samin@splunk:~$ cd Downloads/  
samin@splunk:~/Downloads$ ls  
splunk-9.2.0-1fff88043d5f-Linux-x86_64.tgz  
samin@splunk:~/Downloads$ tar xvzf splunk-9.2.0-1fff88043d5f-Linux-x86_64.tgz
```

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

Agree with the license and set a username and password

```
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
```

```
"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: █
```

```
samin@splunk: ~/Downloads/splunk/bin
```

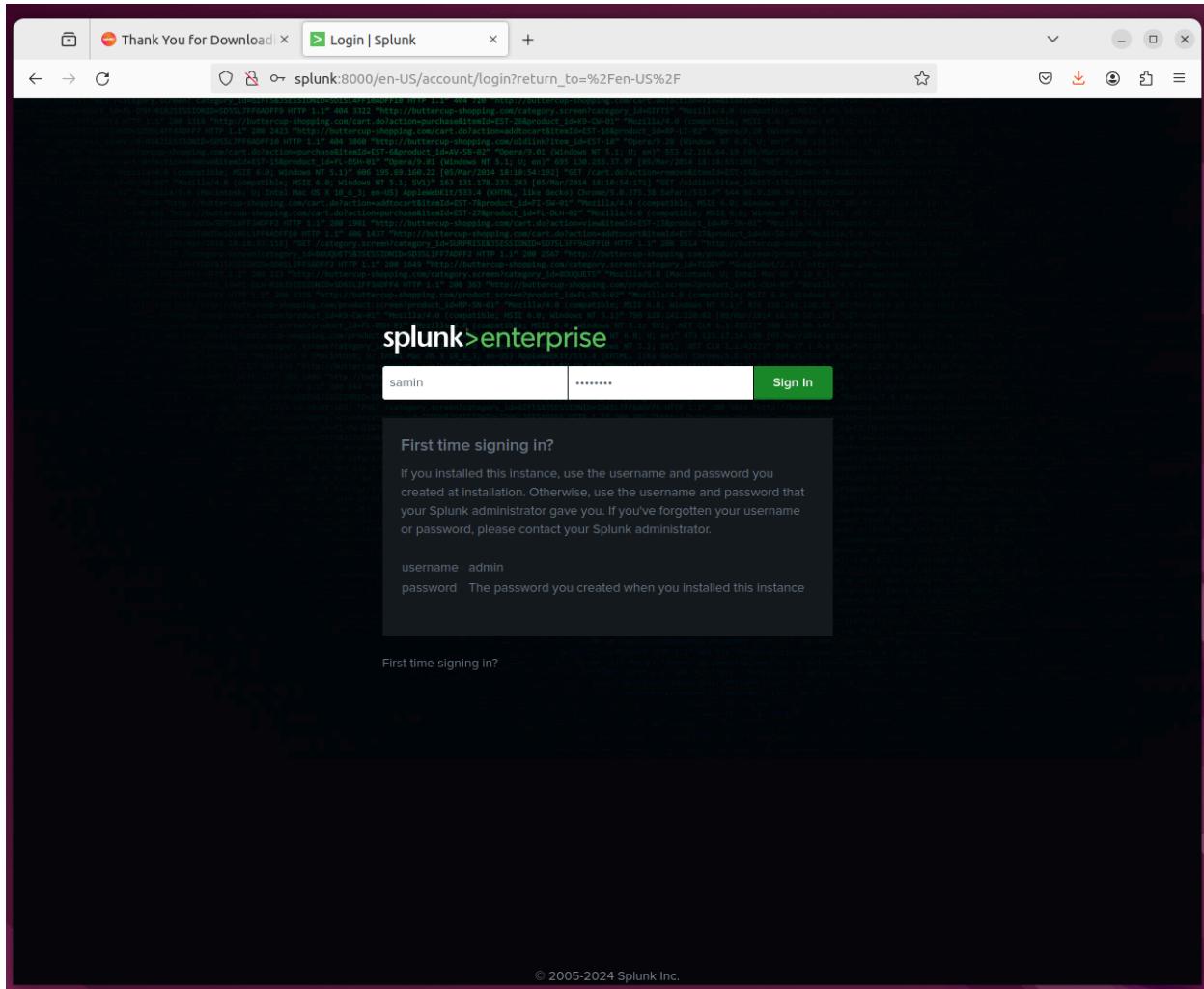
```
.....+++++
.....+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=splunk/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done

Waiting for web server at http://127.0.0.1:8000 to be available.....
Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://splunk:8000
samin@splunk:~/Downloads/splunk/bin$
```

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



The screenshot shows the Splunk Enterprise Home page. At the top, there's a navigation bar with tabs for 'splunk>enterprise' and 'Apps'. Below the navigation is a search bar and a 'Hello, Administrator' greeting. A 'Quick links' section includes links for 'Dashboard', 'Recently viewed', 'Created by you', and 'Shared with you'. To the left, there's a sidebar titled 'Apps' with a search bar and a list of available apps: 'Search & Reporting', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. Below the sidebar is a link to 'Find more apps'. The main content area is divided into sections: 'Common tasks' (with links for 'Add data', 'Search your data', 'Visualize your data', 'Add team members', 'Manage permissions', and 'Configure mobile devices'), 'Learning and resources' (with links for 'Product tours', 'Learn more with Splunk Docs', 'Get help from Splunk experts', 'Extend your capabilities', 'Join the Splunk Community', and 'See how others use Splunk'), and a 'Thank You for Download!' message.

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 Downloading!

splunk:8000/en-US/app/launcher/home

Administrator Messages Settings Activity Help Find

Hello, Administrator

Apps Manage

Search apps by name...

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.

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.
- Get help from Splunk experts** Actionable guidance on the Splunk Lantern Customer Success Center.
- Join the Splunk Community** Learn, get inspired, and share knowledge.
- Learn more with Splunk Docs** Deploy, manage, and use Splunk software with comprehensive guidance.
- Extend your capabilities** Browse thousands of apps on Splunkbase.
- See how others use Splunk** Browse real customer stories.

The screenshot shows the Splunk Settings interface for managing data forwarding and receiving. The top navigation bar includes tabs for 'splunk>enterprise' and 'Apps', along with links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. The main content area is titled 'Forwarding and receiving'.

Forward data

Set up forwarding between two or more Splunk instances.

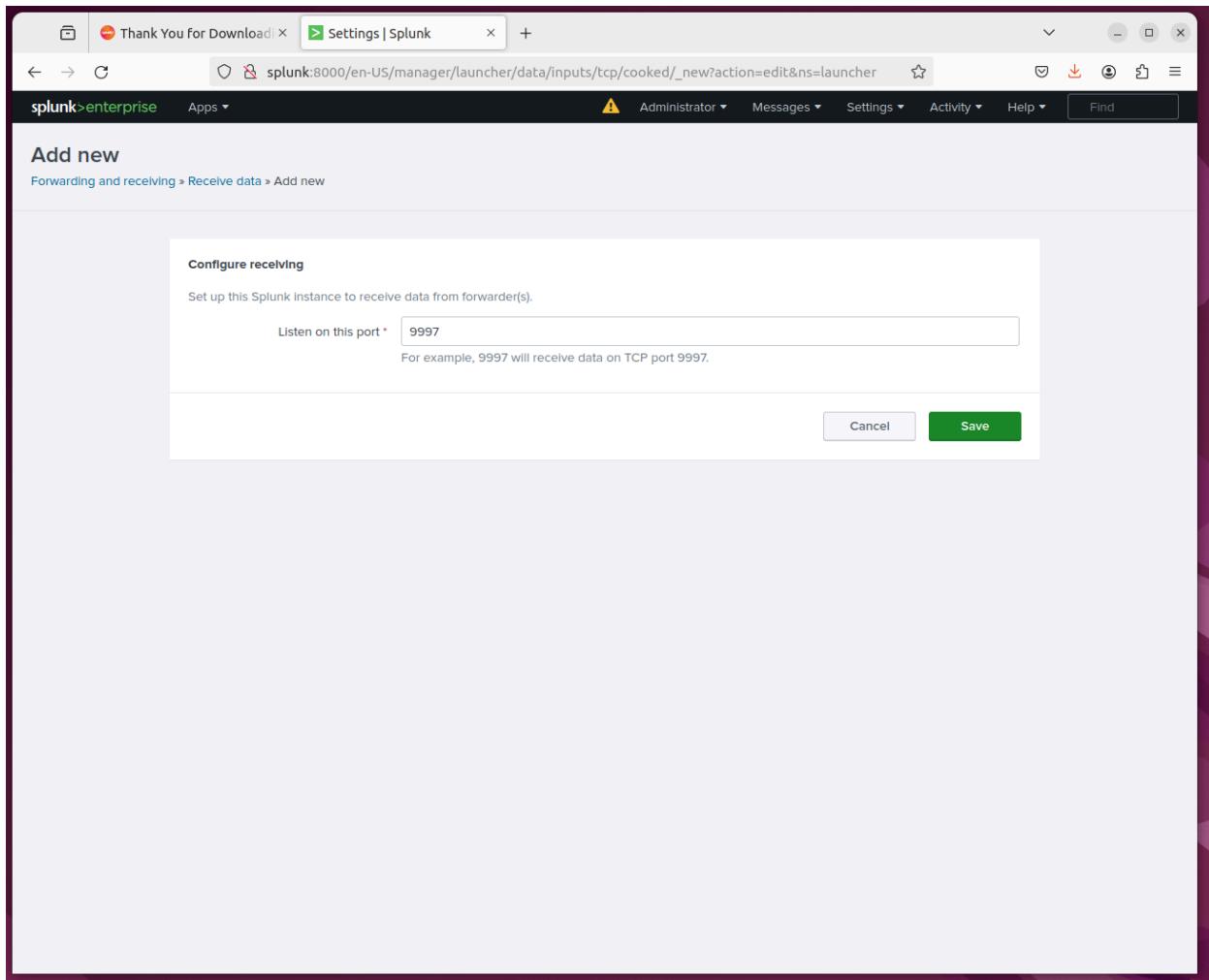
Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data

Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

Listen on port 9997 and save:



The screenshot shows the Splunk Settings interface with the title 'Settings | Splunk'. The URL in the address bar is 'splunk:8000/en-US/manager/launcher/data/inputs/tcp/cooked?msgid=6895650.065424534163099'. The top navigation bar includes links for 'splunk>enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. A green button labeled 'New Receiving Port' is visible on the right.

The main content area is titled 'Receive data' and shows the path 'Forwarding and receiving > Receive data'. A success message 'Successfully saved "9997"' is displayed. Below it, a table lists one item:

Listen on this port	Status	Actions
9997	Enabled Disable	Delete

There are filters and a search icon at the top of the table, and a '25 per page' dropdown menu on the right.

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

The screenshot shows the Splunk Enterprise interface with the following details:

- Title Bar:** Shows 'splunk>enterprise' and the current page as 'Manage Indexes | Splunk'.
- Left Sidebar:** Labeled 'Indexes' with a sub-header 'A repository for data in Splunk Enterprise'. It lists 15 indexes: '_audit', '_configtrack', '_dsappevent', '_dsclient', '_dsphonehome', '_internal', '_introspection', '_metrics', '_metrics_rollup', and '_telemetry'. Each entry has 'Edit' and 'Delete' buttons.
- Central Content:**
 - New Index Modal:** Titled 'New Index'.
 - General Settings:**
 - Index Name:** wineventlog
 - Index Data Type:** Events (selected)
 - Home Path:** optional
 - Cold Path:** optional
 - Thawed Path:** optional
 - Data Integrity Check:** Options: Enable (selected) or Disable.
 - Max Size of Entire Index:** 500 GB
 - Max Size of Hot/Warm/Cold Bucket:** auto
 - Frozen Path:** optional
 - App:** Search & Reporting
- Bottom Status Bar:** Shows '_thefishbuck' with Edit, Delete, Disable buttons, and file system information: Events (1 MB), system (488.28 GB), and 0.
- Right Panel:** Shows a list of existing indexes with their respective Home and Frozen paths, all marked as 'N/A'.

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):

Edit Firewall Rule

Action	<input type="button" value="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	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.				
Interface	<input type="button" value="VICTIMNETWORK"/>	Choose the interface from which packets must come to match this rule.				
Address Family	<input type="button" value="IPv4"/>	Select the Internet Protocol version this rule applies to.				
Protocol	<input type="button" value="Any"/>	Choose which IP protocol this rule should match.				
Source						
Source	<input type="checkbox"/> Invert match	<input type="button" value="Any"/>	Source Address	/	<input type="button" value="▼"/>	
Destination						
Destination	<input type="checkbox"/> Invert match	<input type="button" value="Any"/>	Destination Address	/	<input type="button" value="▼"/>	
Extra Options						
Log	<input type="checkbox"/> 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	<input type="text"/>					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	<input type="button" value="Display Advanced"/>					
<input type="button" value="Save"/>						

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

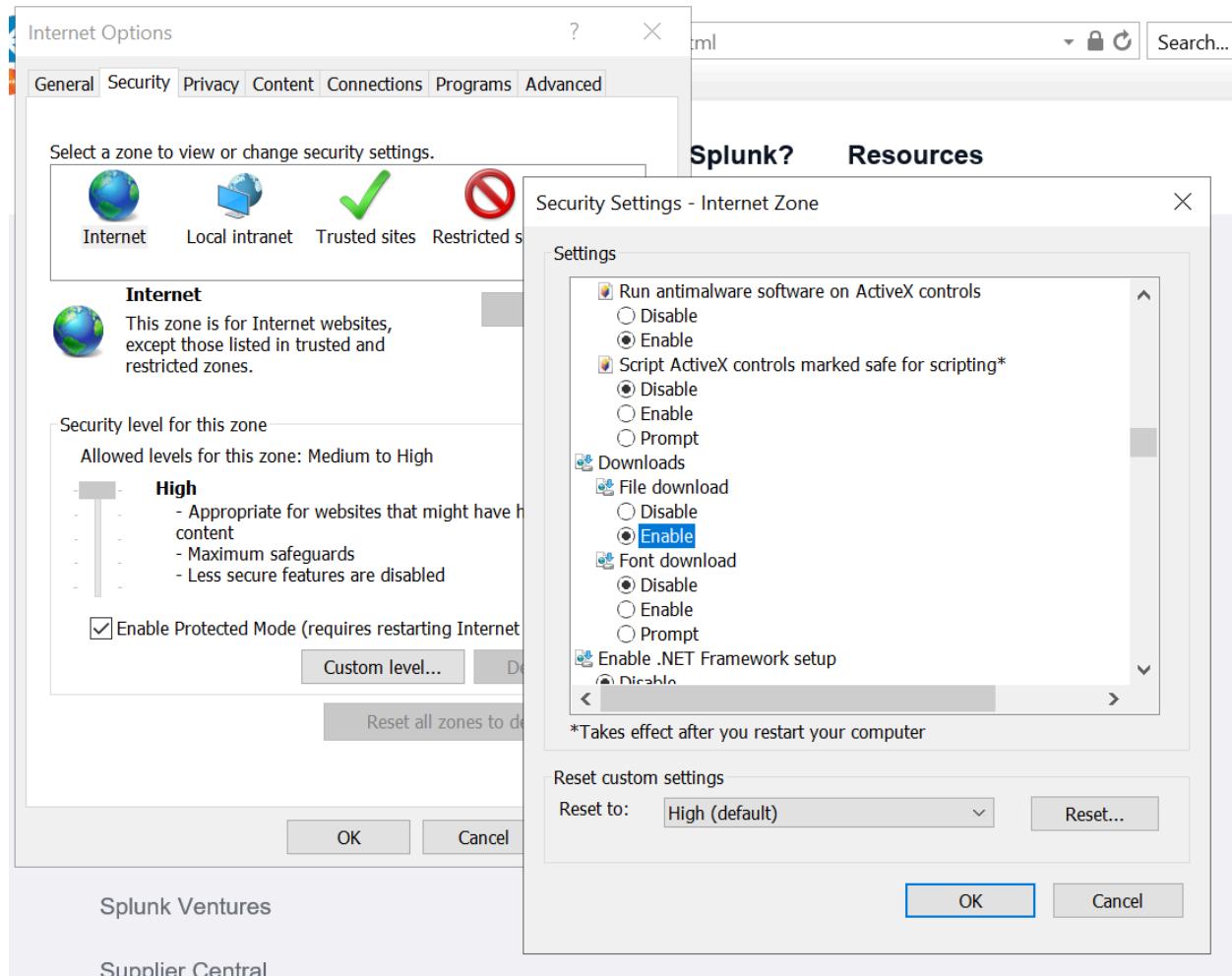
 Apply Changes
[Floating](#) [WAN](#) [KALI](#) [VICTIMNETWORK](#) [SECONION](#) [SPANPORT](#) [SPLUNK](#)
Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 *	*	*	*	*	*	none			



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:

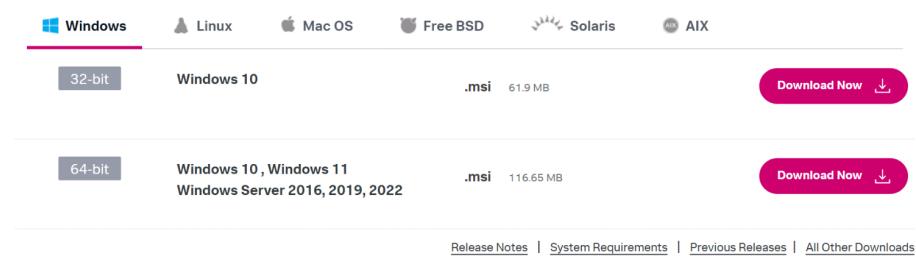
GET STARTED

Choose Your Download

Splunk Universal Forwarder 9.2.0

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package



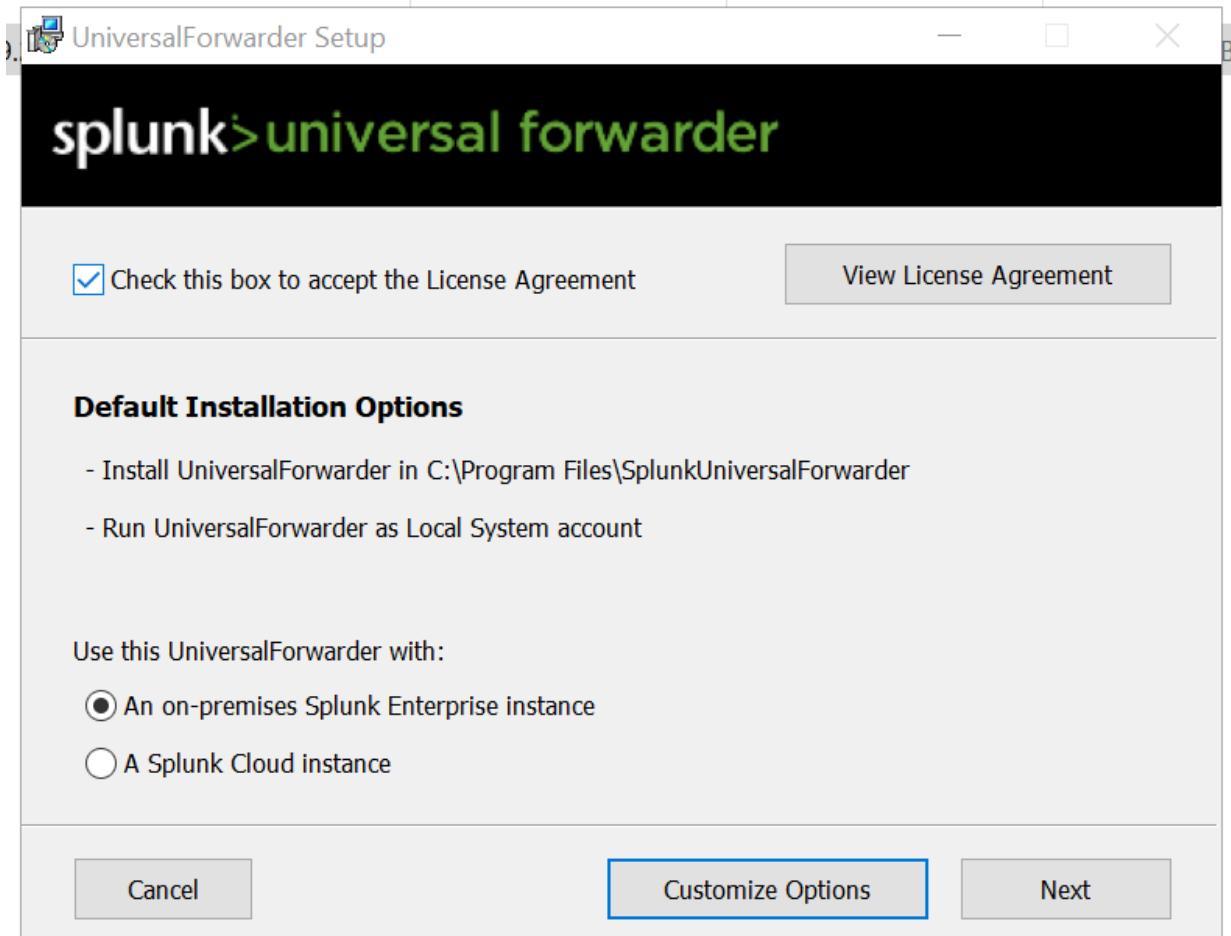
The screenshot shows the download page for Splunk Universal Forwarder 9.2.0. At the top, there are tabs for Windows (selected), Linux, Mac OS, FreeBSD, Solaris, and AIX. Under the Windows tab, there are two sections: one for 32-bit (Windows 10) and one for 64-bit (Windows 10, 11, Server 2016, 2019, 2022). Each section includes a download link labeled "Download Now". Below these sections, there are links for Release Notes, System Requirements, Previous Releases, and All Other Downloads.

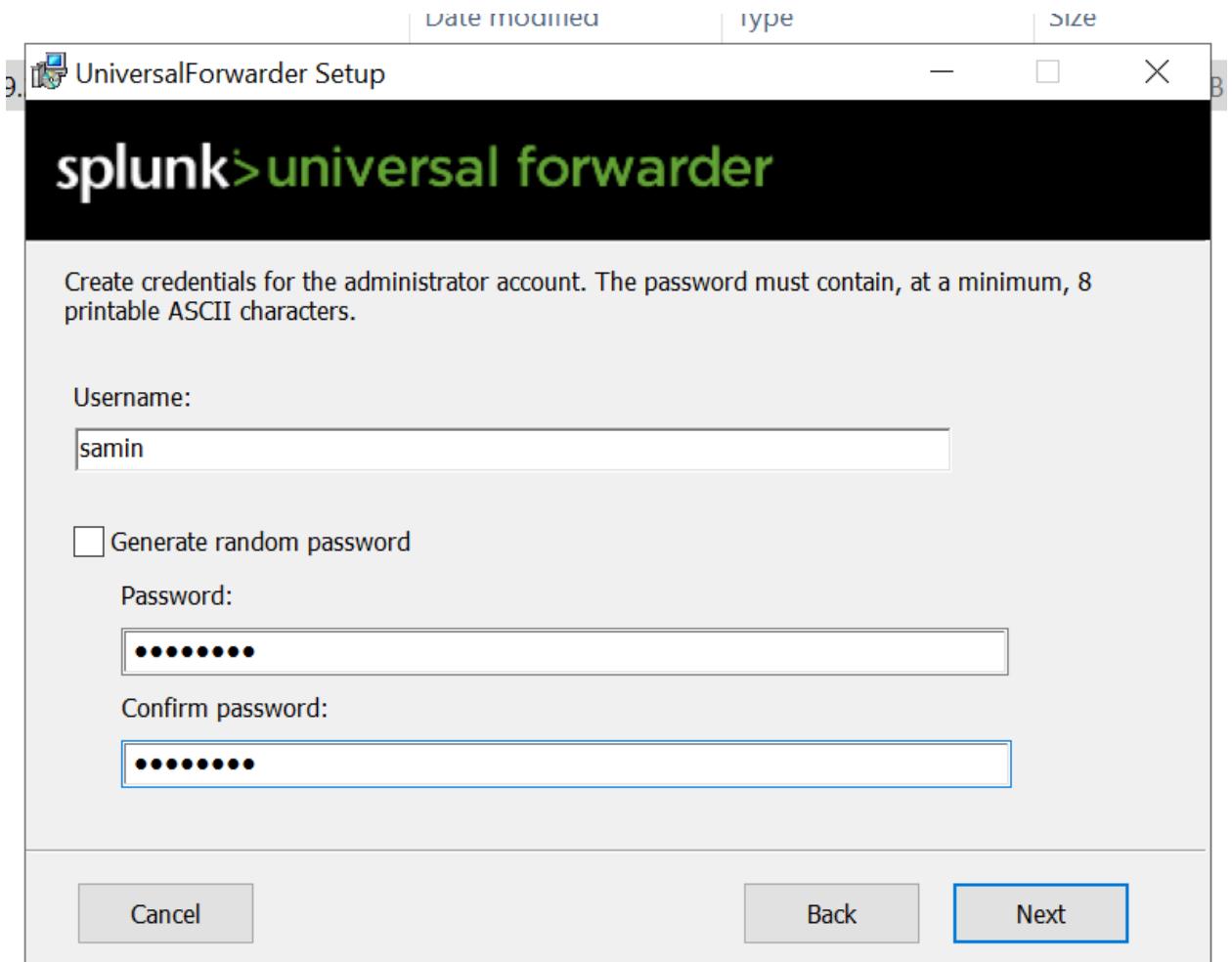
Platform	Version	File Type	Size	Action
Windows	32-bit	.msi	61.9 MB	Download Now
Windows	64-bit	.msi	116.65 MB	Download Now

[Release Notes](#) | [System Requirements](#) | [Previous Releases](#) | [All Other Downloads](#)

Run the installer.

Accept the License Agreement and set a username and password:

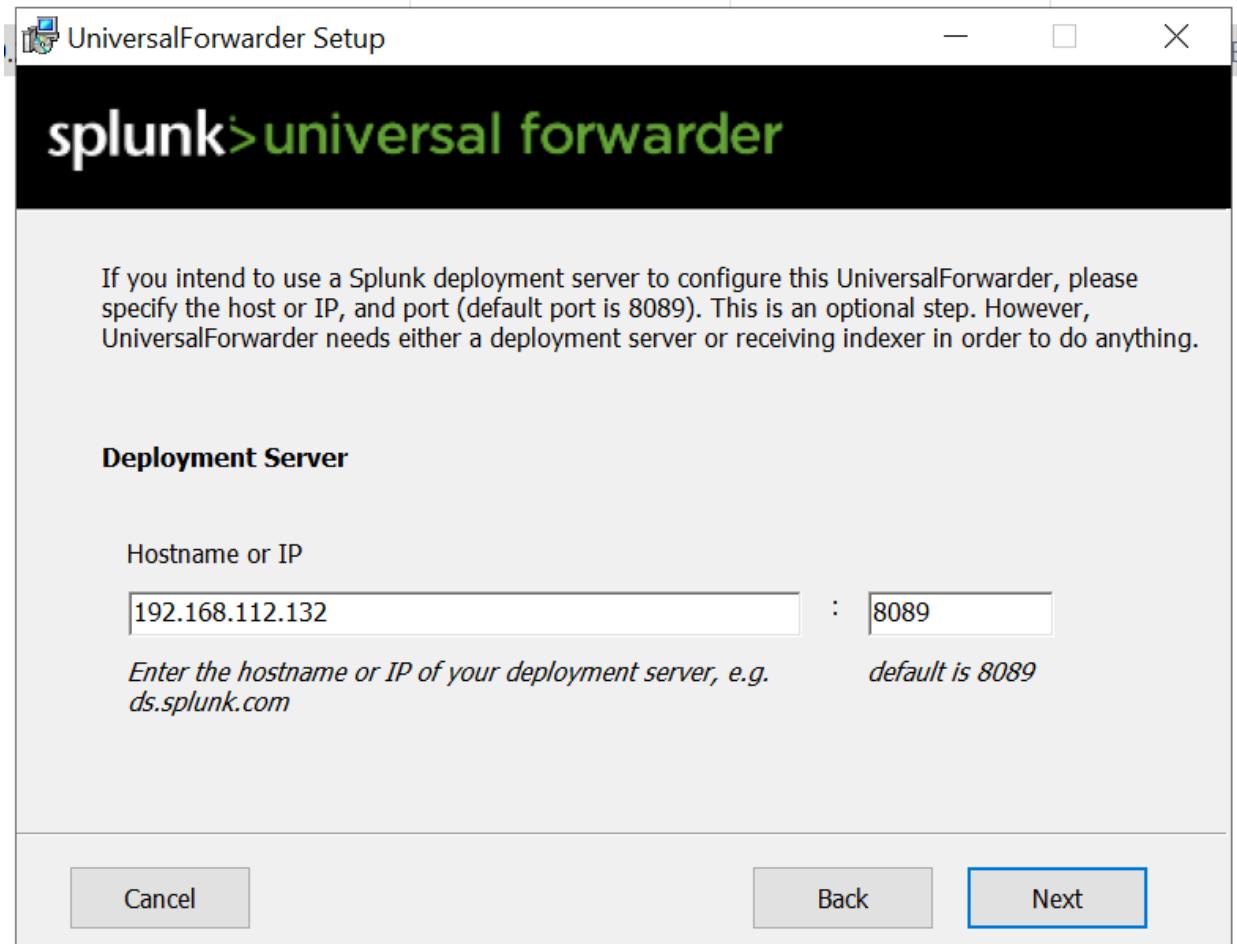


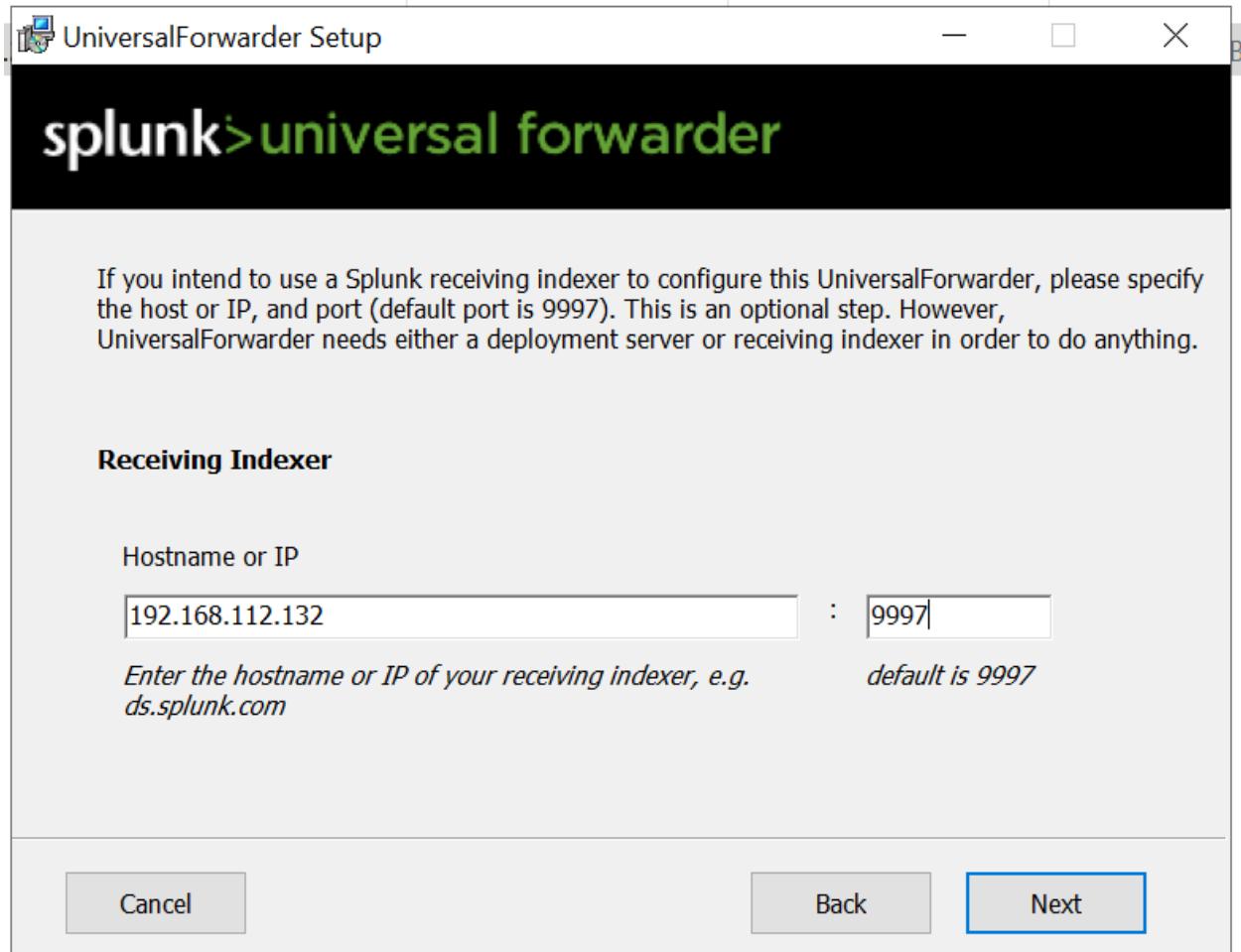


Find the IP address of the Splunk machine and use it to fill in the IP fields for the next 2 screens, using the default ports 8089 and 9997:

```
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:fed:e807a 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:fed:e8084 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)
```





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

The screenshot shows a web browser window with the URL `splunk:8000/en-US/manager/search/adddata`. The page title is "What data do you want to send to the Splunk platform?". It features a search bar and four categories: Cloud computing (10 data sources), Networking (2 data sources), Operating System (1 data source), and Security (3 data sources). Below these, it says "4 data sources in total". Under the heading "Or get data in with the following methods", there are three options: "Upload" (files from my computer, including Local log files, Local structured files (e.g. CSV), and a "Tutorial for adding data" link), "Monitor" (files and ports on this Splunk platform instance, including Files - HTTP - WMI - TCP/UDP - Scripts and Modular inputs for external data sources), and "Forward" (data from a Splunk forwarder, including Files - TCP/UDP - Scripts).

What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources

Cloud computing (10 data sources)

Networking (2 data sources)

Operating System (1 data source)

Security (3 data sources)

4 data sources in total

Or get data in with the following methods

Upload files from my computer

Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)

Monitor files and ports on this Splunk platform instance

Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

Forward data from a Splunk forwarder

Files - TCP/UDP - Scripts

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

The screenshot shows the 'Add Data - Select Forwarders' page in the Splunk web interface. The URL is <splunk:8000/en-US/manager/search/adddatamethods/selectforwarders>. The top navigation bar includes links for 'Manage Indexes | Splunk', 'Add Data - Select Forwarders', and other system navigation.

The main content area has a title 'Select Forwarders' and a sub-instruction: 'Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.' Below this, a note says: 'To enable forwarding of data from deployment clients to this Instance, set the output configurations on your forwarders. [Learn More](#)'.

A horizontal navigation bar at the top of the form shows the steps: 'Add Data' (highlighted), 'Select Forwarders', 'Select Source', 'Input Settings', 'Review', and 'Done'. Buttons for '[Next >](#)' and '[< Back](#)' are also present.

The 'Select Server Class' section contains two tabs: 'New' (selected) and 'Existing'. Under 'Available host(s)', there is a list box containing 'WINDOWS DomainController'. An 'add all' button is next to it. Under 'Selected host(s)', there is a list box containing 'WINDOWS DomainController'. A '< remove all' button is next to it.

A 'New Server Class Name' input field contains the value 'Domain Controller'.

At the bottom left, there is a 'FAQ' section with several expandable questions:

- How do I create source types for data originating from Forwarders?
- What is a deployment server?
- What are deployment clients?
- What are server classes?
- How do I make changes to the deployment server configuration?
- How do I manage deployment clients?
- How many deployment clients are supported by this instance?
- How do I add data from forwarders in distributed Splunk environments?

Select which Local Event Logs to keep track of:

Add Data < Back Next >

Local Event Logs
Collect event logs from this machine.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Scripts
Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier
Assigns a random identifier to every node

Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.

Configure selected Splunk Universal Forwarders to monitor local Windows event log channels, which contain log data published by installed applications, services, and system processes. The event log monitor runs once for every event log input defined in the Splunk platform. [Learn More](#)

Select Event Logs Available item(s) [add all >](#)

Application
ForwardedEvents
Security
Setup
Custom

Select the Windows Event Logs you want to index from the list.

FAQ

- › What event logs does this Splunk platform instance have access to?
- › What is the best method for monitoring event logs of remote Windows machines?

Choose the “wineventlog” as the Index:

Add Data < Back Review >

Input Settings
Optionally set additional input parameters for this data input as follows:

Index

The Splunk platform stores incoming data as events in the selected Index. Consider using a “sandbox” index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index Create a new index

FAQ

- › How do indexes work?
- › How do I know when to create or use multiple indexes?

Click “Review” and then “Submit”