Security Onion

Sgt Uptmor,Connor,SSgt Caban,Richard
Sgt Camp,Derrick

This document will serve as the guide to Security Onion installation and usage for operations.

Overview

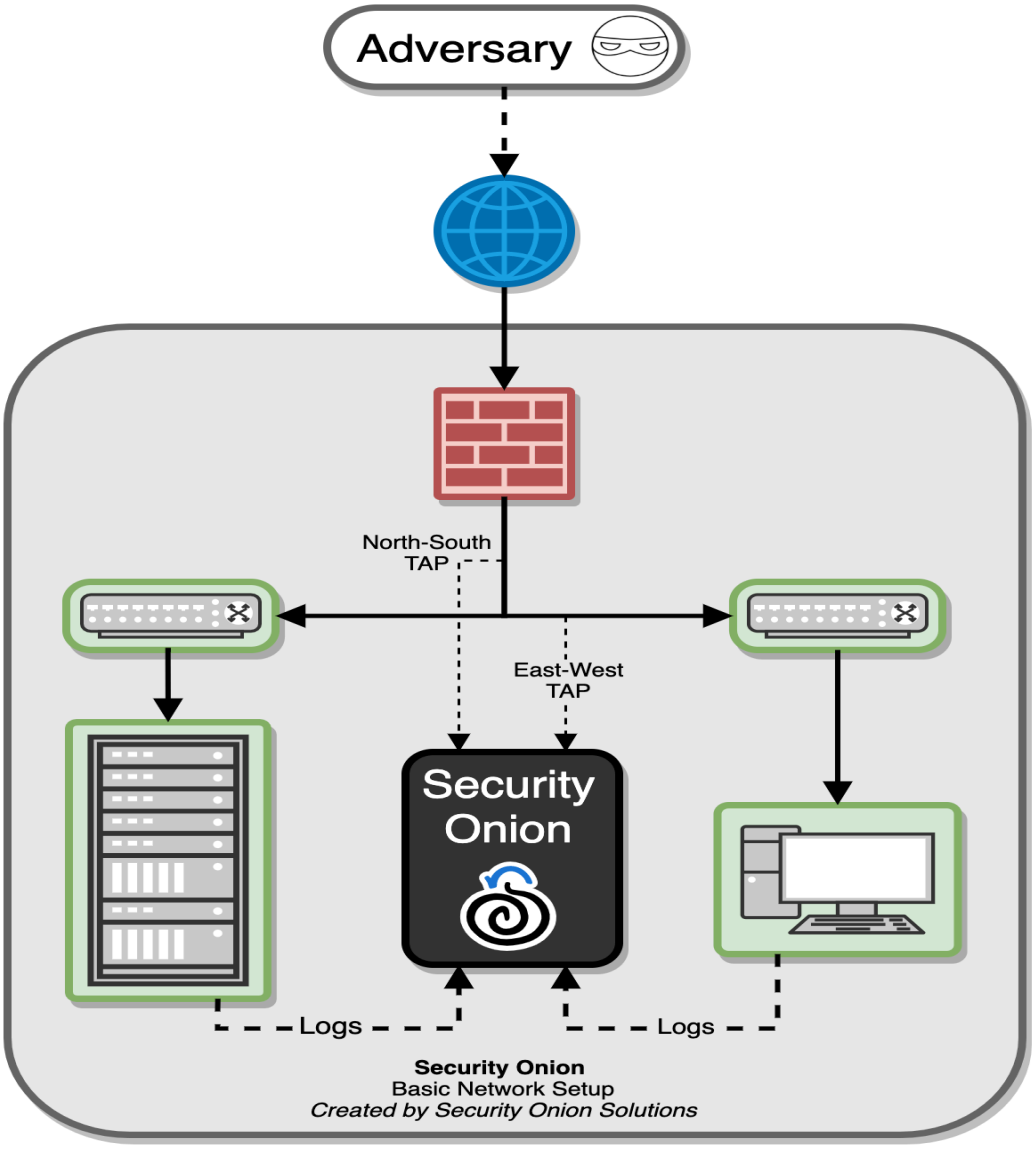
Security Onion is a free and open platform built by defenders for defenders. It includes network visibility, host visibility, intrusion detection, honeypots, log management, and case management. Security Onion has been downloaded over 2 million times and is being used by security teams around the world to monitor and defend their enterprises.

https://Securityonion.net is the primary source for Security Onion media and online documentation.
The “Downloads” tab on the homepage of the website redirects to a Github portal containing the most current version of the SO .ISO file (Version 2.4 at the time this guide was written).

The ISO. file should be downloaded and verified on local media prior to any live application. An external hard drive containing this file, as well as any additional tools required by the team, is recommended bearing in mind that all tools and media will need to be replicated across both NIPR and SIPR enclaves. Additionally, forward deployed networks and many target environments will be operating on minimal bandwidth without access to a standard white-line. Attempting to update currently running services in these environments is not recommended and all steps should be taken to ensure that all software taken to the target environment is already configured with any and all recent changes.

For any questions about Security Onion, please refer to: “ docs.securityonion.net/en/latest “.

In the diagram below, we see Security Onion in a traditional enterprise network with a firewall, workstations, and servers. You can use Security Onion to monitor north/south traffic to detect an adversary entering an environment, establishing command-and-control (C2), or perhaps data exfiltration. You'll probably also want to monitor east/west traffic to detect lateral movement. As more and more of our network traffic becomes encrypted, it's important to fill in those blind spots with additional visibility in the form of endpoint telemetry. Security Onion can consume logs from your servers and workstations so that you can then hunt across all of your network and host logs at the same time.



Tools and Capabilities

ATT&CK - Visualize defensive coverage

CyberChef - Compress and decompress data

Suricata - Signature based detections

Suricata - Rich protocol metadata file extractor

Zeek - Rich protocol metadata file extractor

Stenographer - Full packet capture

Strelka - File analysis

Elastic Agent - Host visibility

OSquery - Live queries

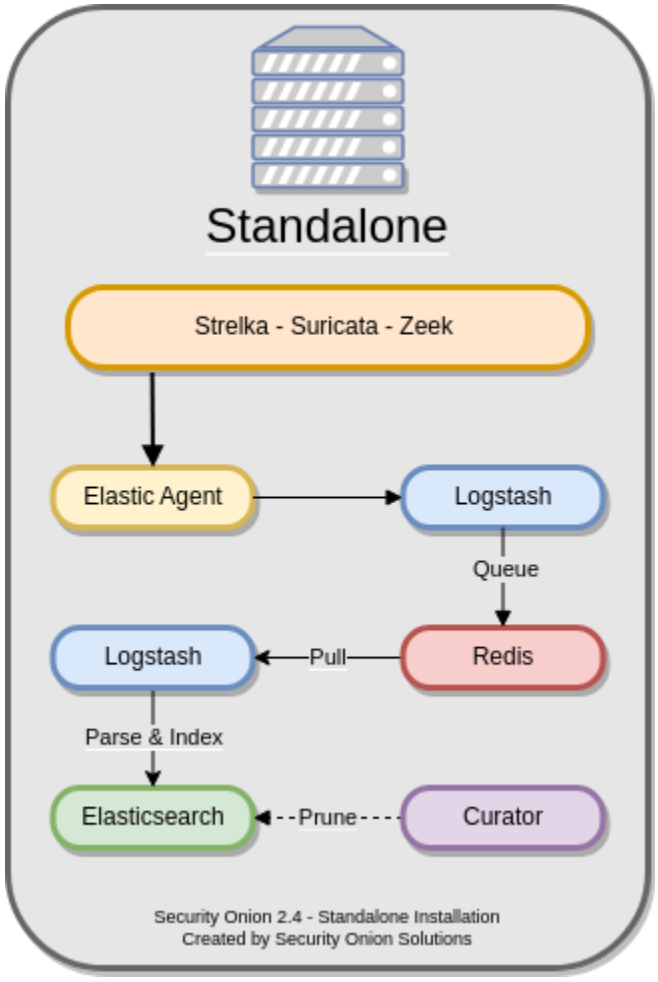
Elastic Fleet - Centralized Management

OpenCanary - Intrusion detection honeypots

Architecture

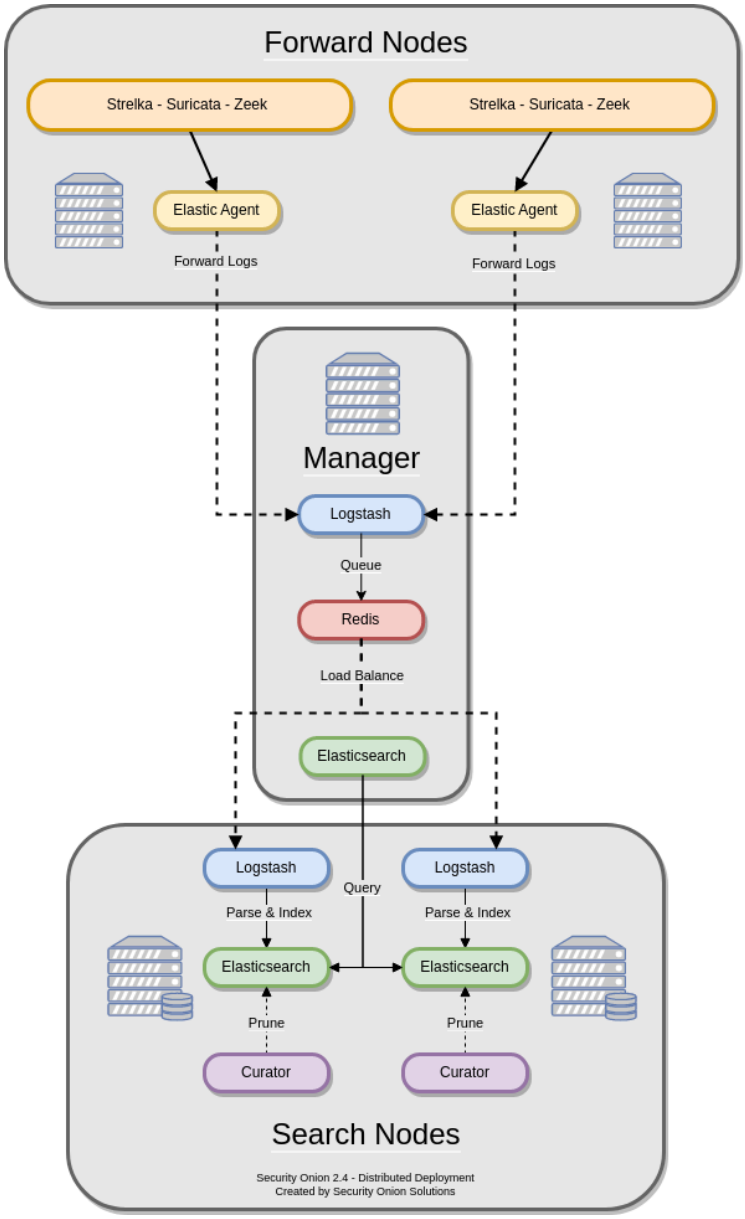
Standalone

Standalone runs all components run on one box. However, instead of Elastic agents sending logs directly to Elasticsearch, it sends them to Logstash, which sends them to Redis for queuing. A second logstash pipeline pulls the logs out of Redis and sends them to ElasticSearch, where they are parsed and indexed. This type of deployment is best used for low throughput environments and is not as scalable as a distributed deployment.



Distributed

Standard distributed deployment includes a manager node, and one or more forward nodes running network sensor components, and one or more search nodes running Elastic search components. This architecture may cost more upfront, but it provides for greater scalability and performance, as you can simply add more nodes to handle more traffic or log sources.

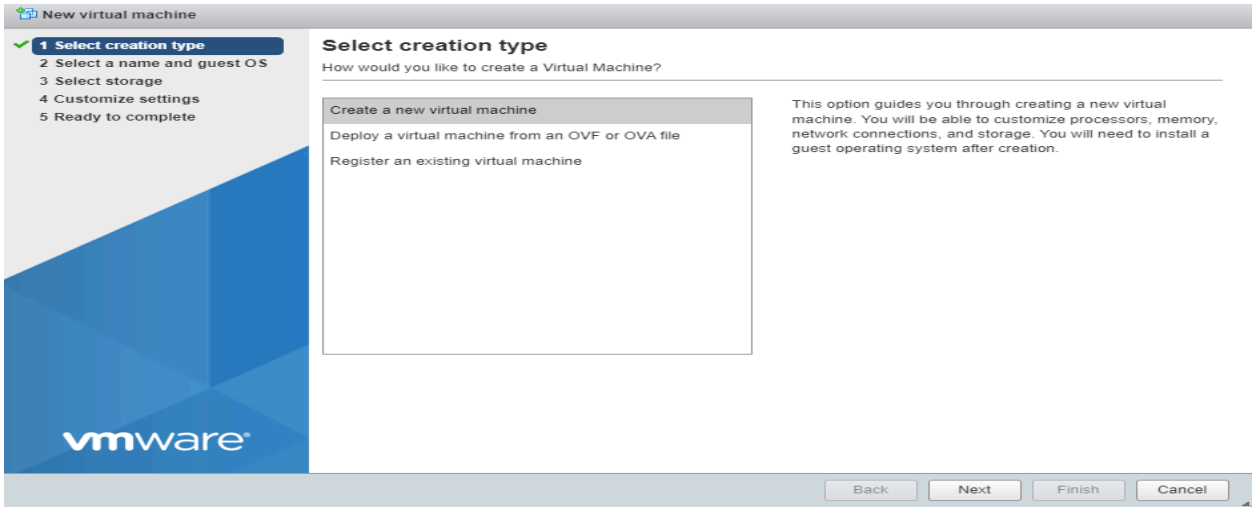


Security Onion Installation

By: Sgt Camp, Derrick
3rd PLT DCO-IDM
LU: 20231101

Step 1:

Create a new Virtual Machine



Step 2:

Name: SecOnion

Compatibility: ESXi 7.0 U2 Virtual Machine

Guest OS Family: Linux

Guest OS Version: Oracle 9

Step 3:

Select Storage: Minirax Datastore 1 -> Next

Customize settings :

- CPU : 10
- Memory : 120GB
- Hard disk 1 : 2.5T

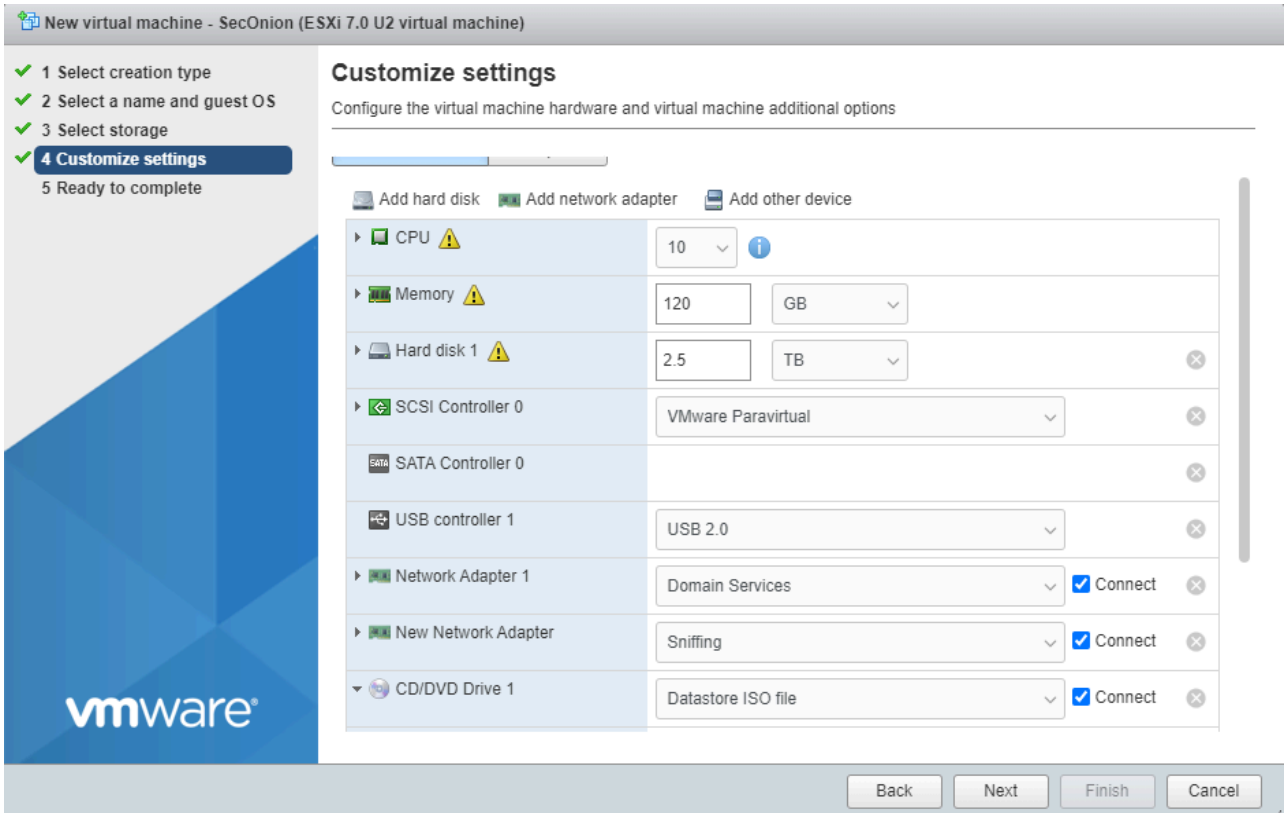
*Click hard disk drop down and make it thin provision *

Add network adapter

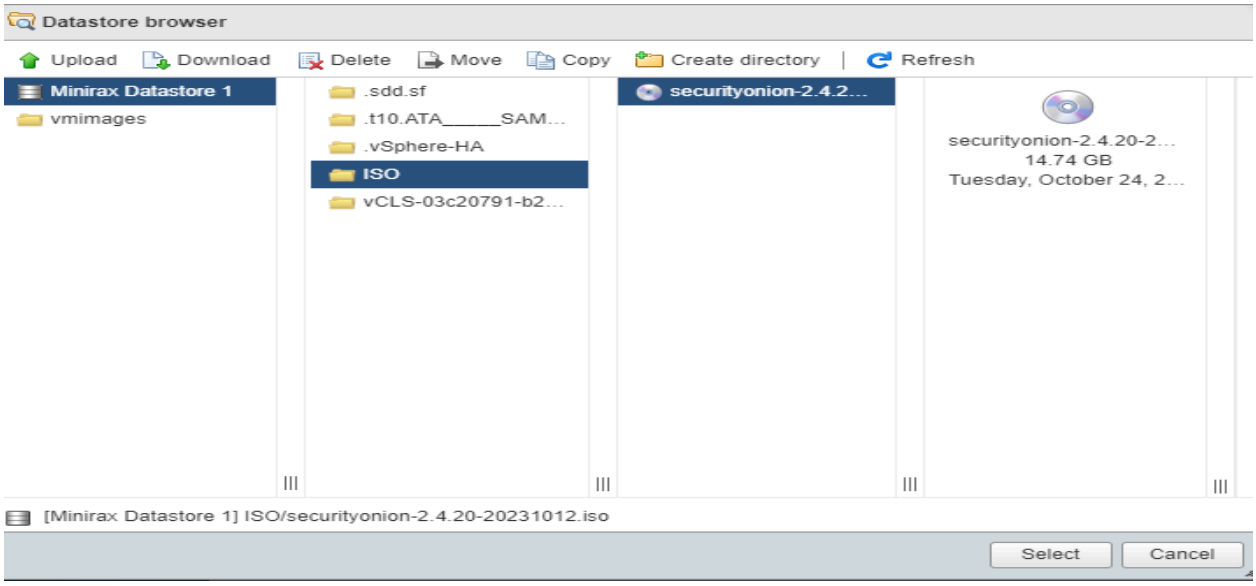
Scroll down to “New network Adapter”

- Select dropdown

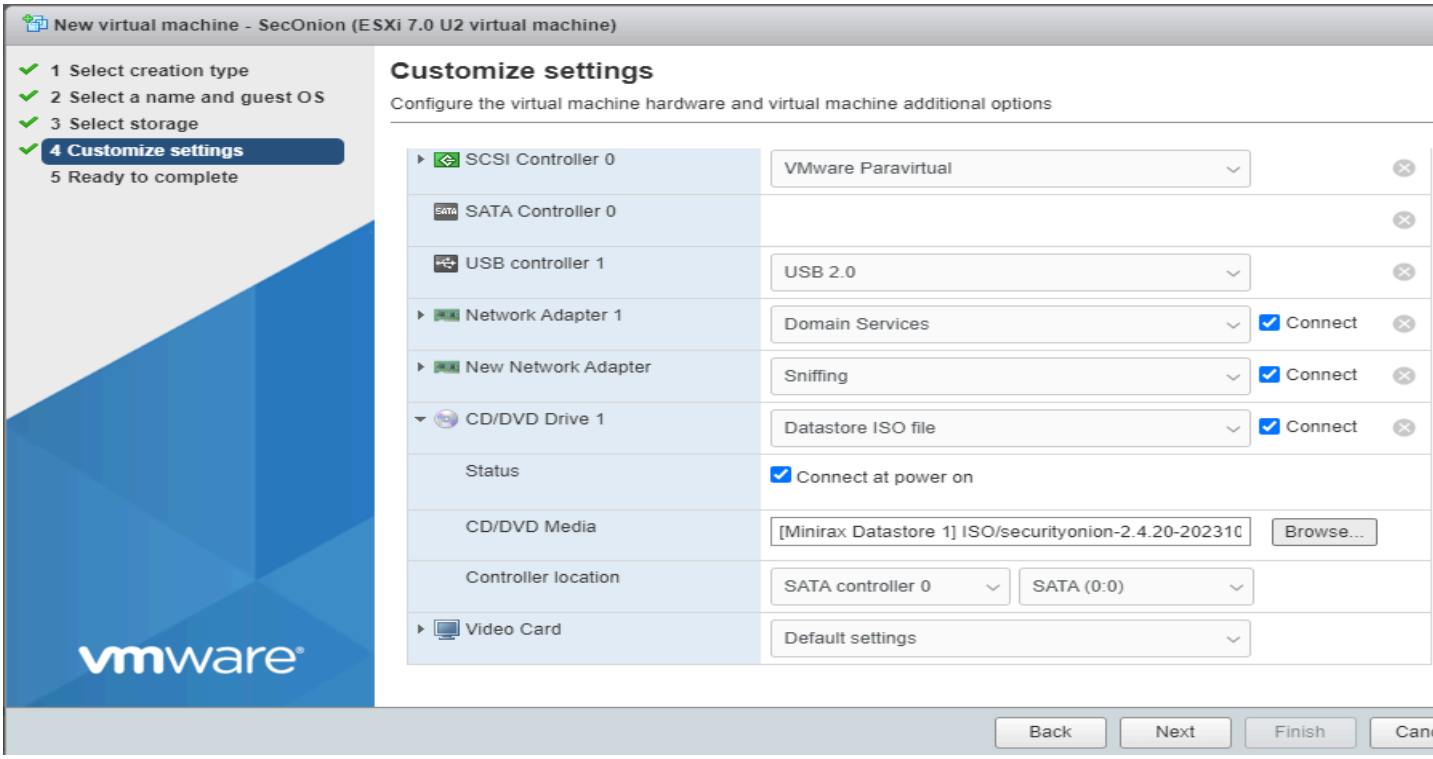
Select “sniffing”



Step 4:
Select CD/DVD Drive dropdown
Select Datastore ISO file
Click ISO in datastore browser



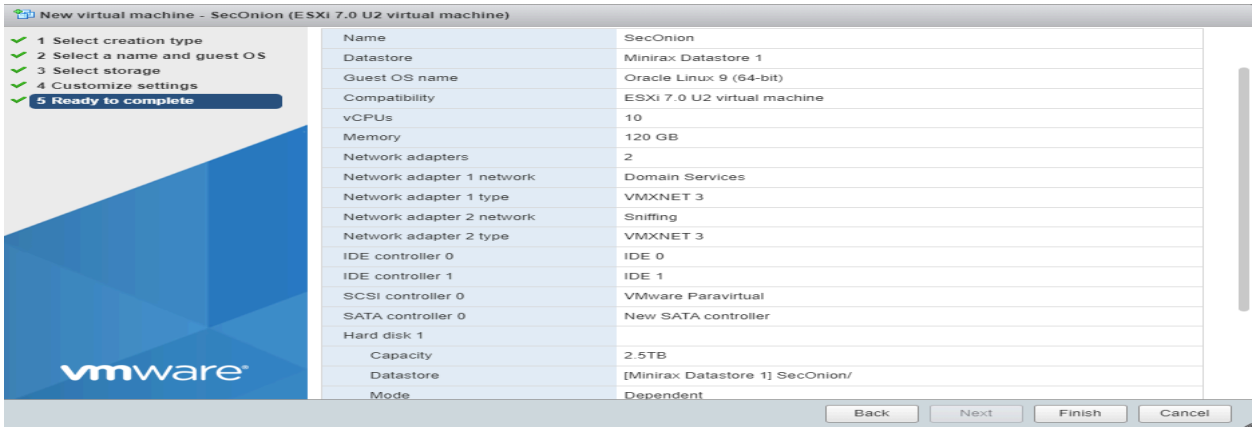
Step 5: SecurityOnion-2.4.2 (or most up to date)



Step 6:

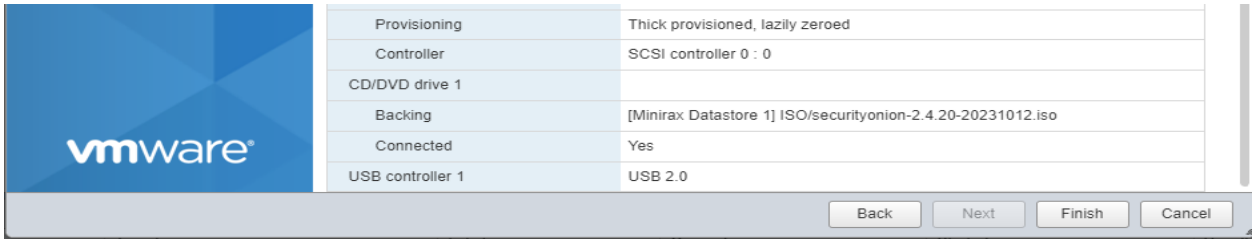
Select Next

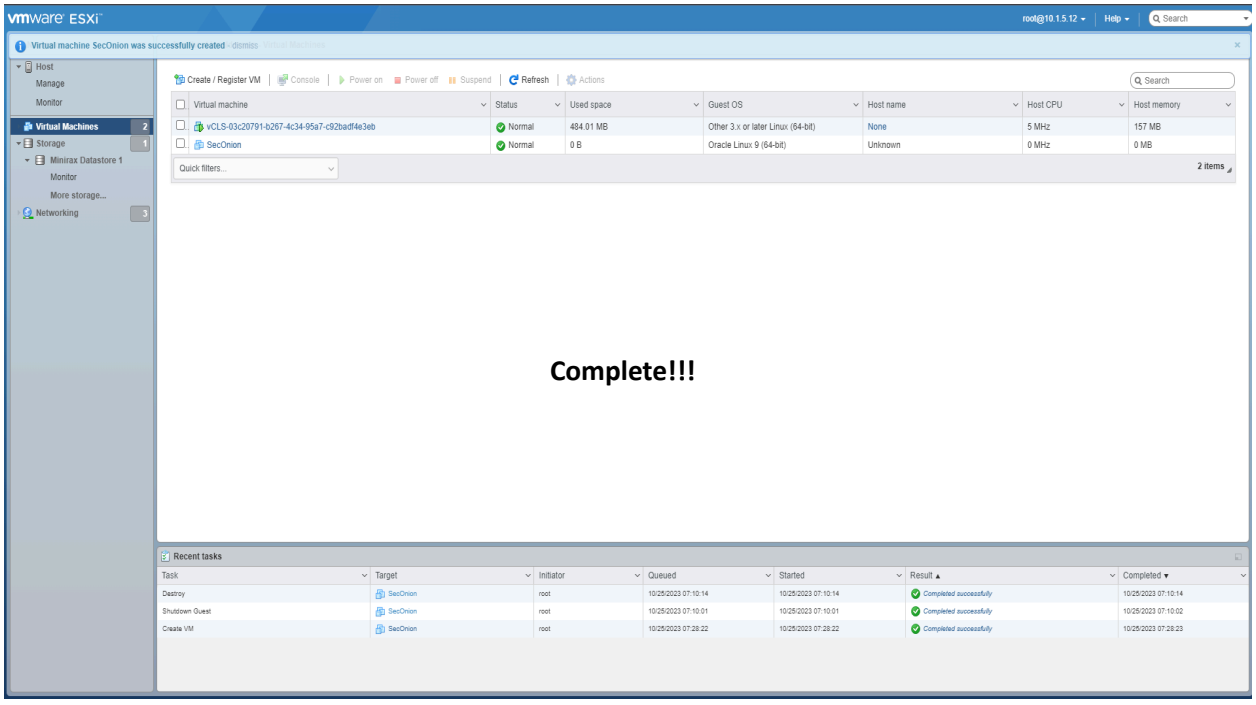
Review All Configurations



Step 7:

Click Finish





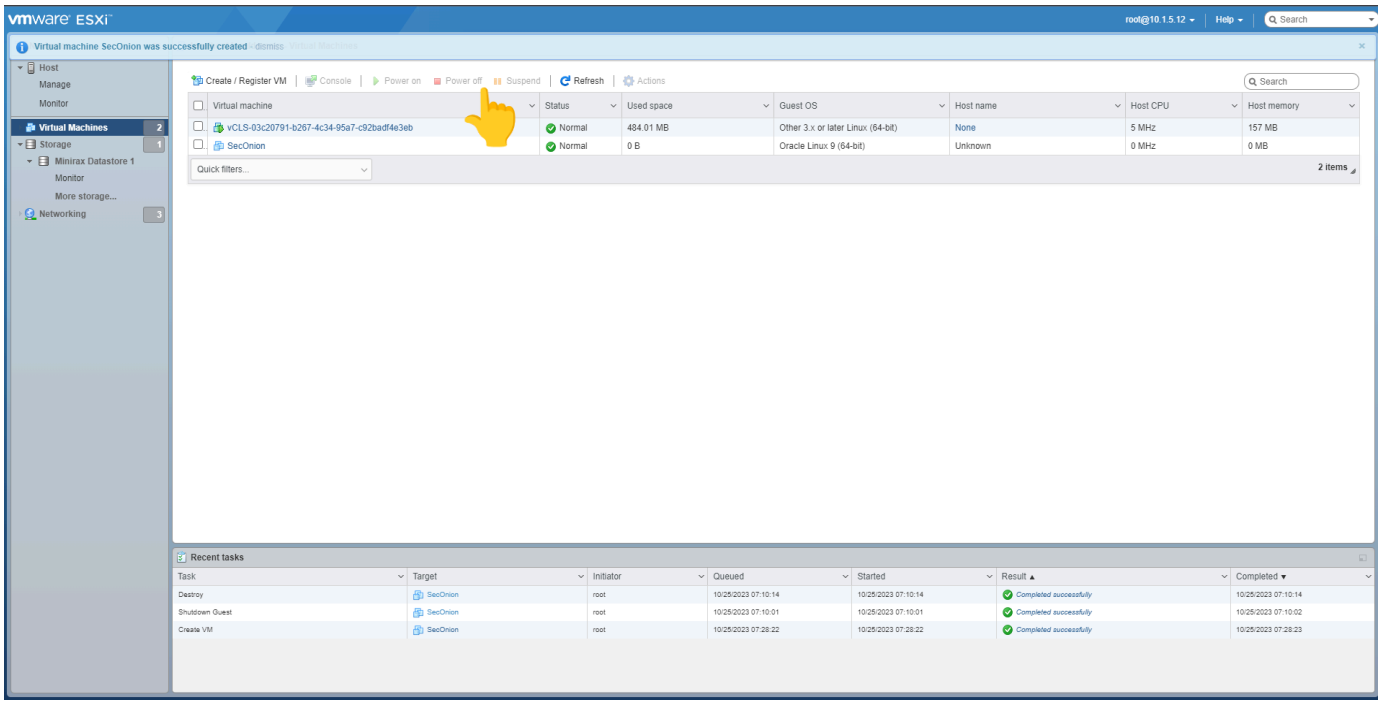
Complete!!!

Security Onion Configuration

Step 1:

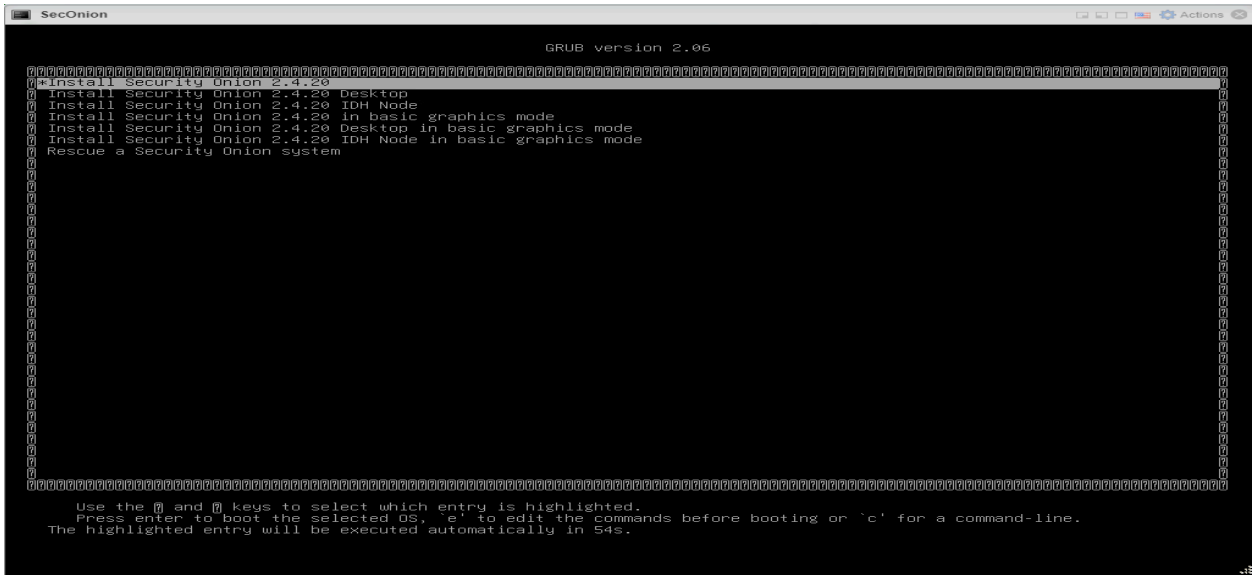
Power On Virtual Machine “Security Onion”

-Click Power On

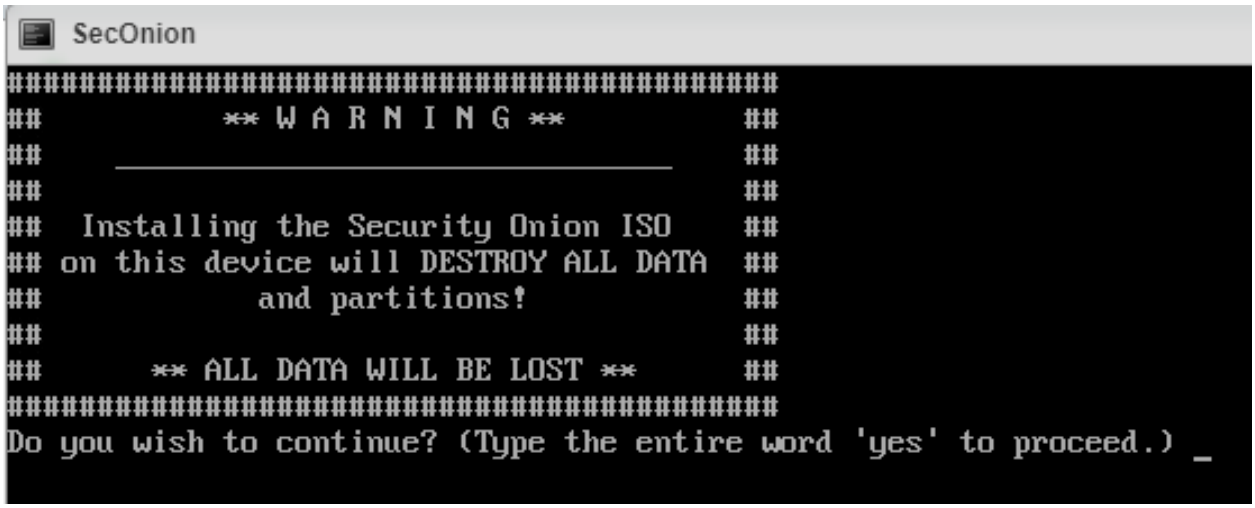


Step 2:

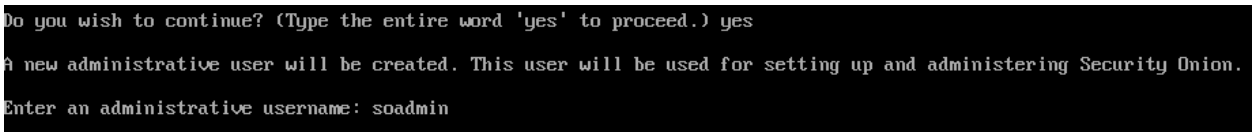
Select “Install Security Onion”



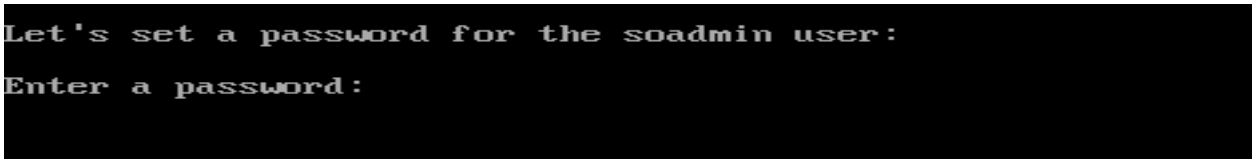
Step 3:
Select “Yes” to proceed
Hit Enter on keyboard



Step 4:
Enter an administrator username: “ soadmin “
Hit Enter on keyboard

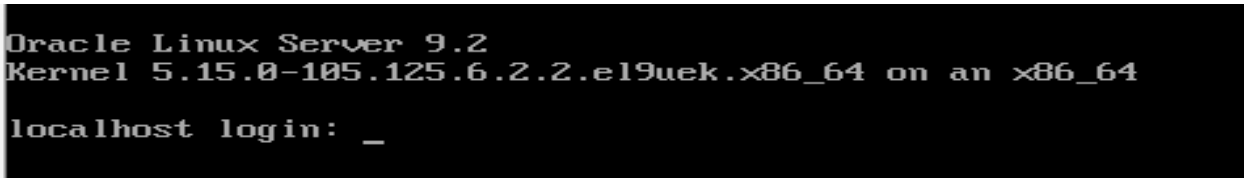


Step 5:
set password to standard
Re-Enter Password

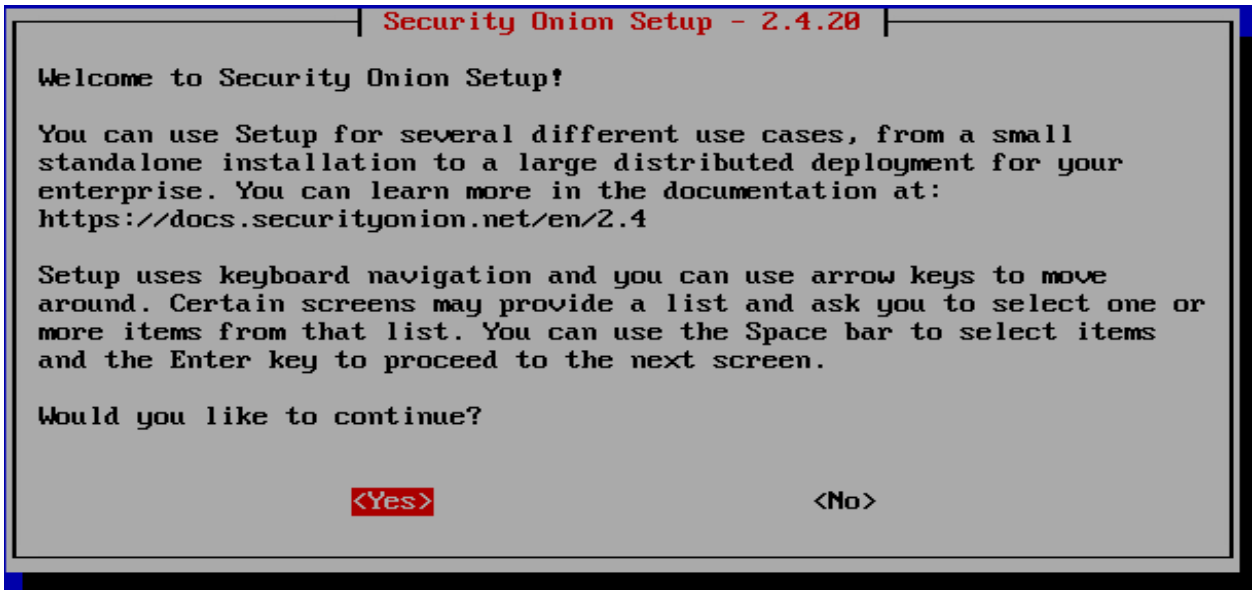


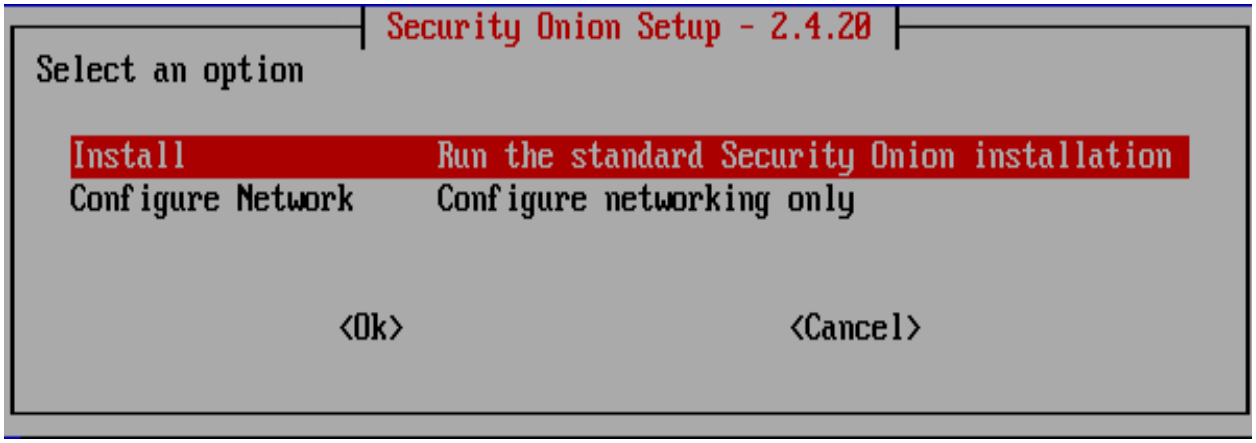
Step 6:
Hit the enter key
Wait for installation to begin
Takes a long time
Hit the enter key to reboot

Step 7:
Login

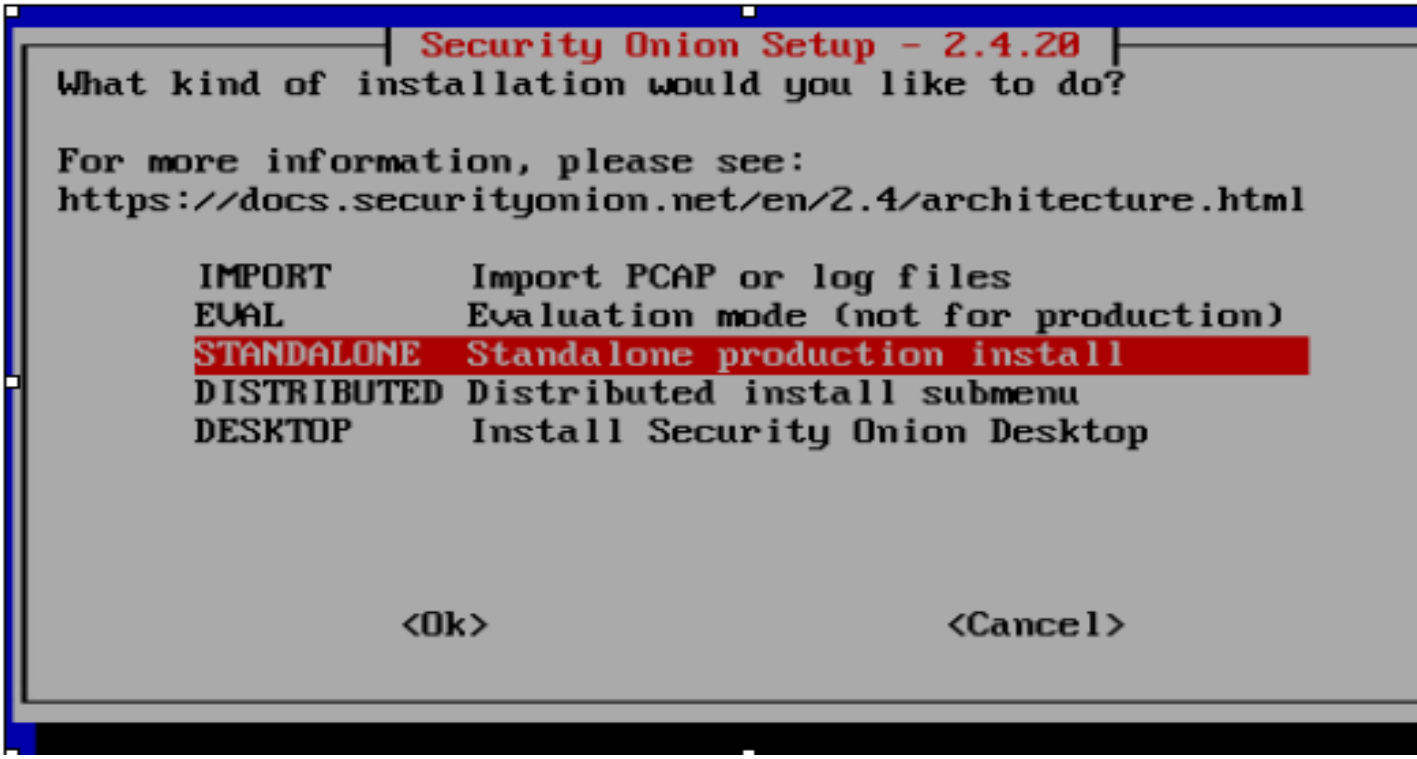


Step 8:
Select Install to run the standard installation
Press the enter key to continue

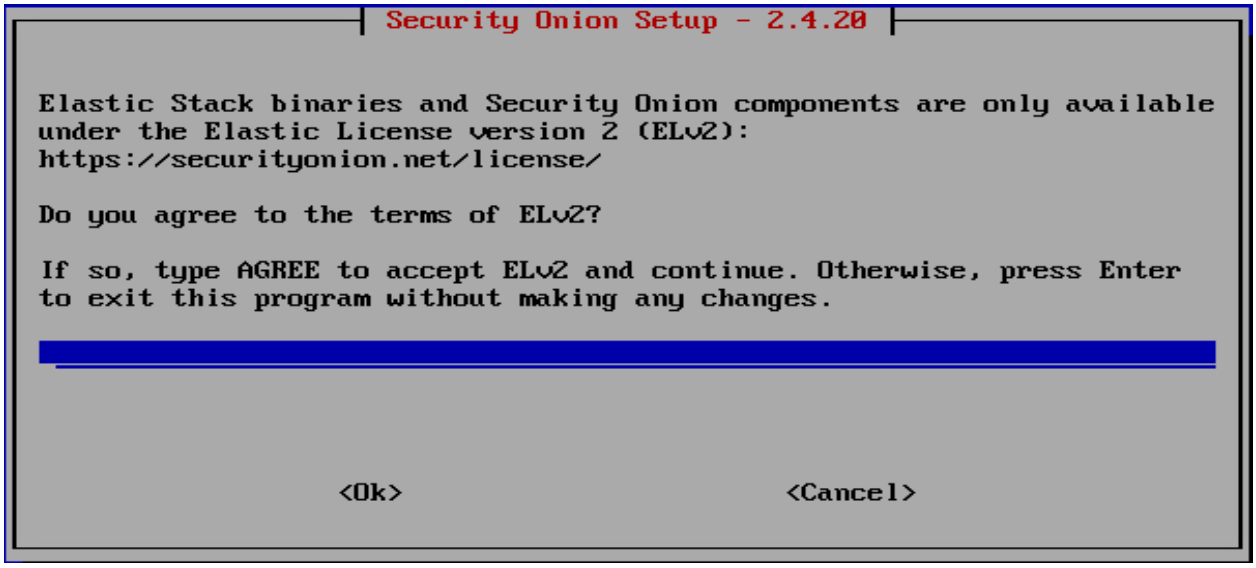




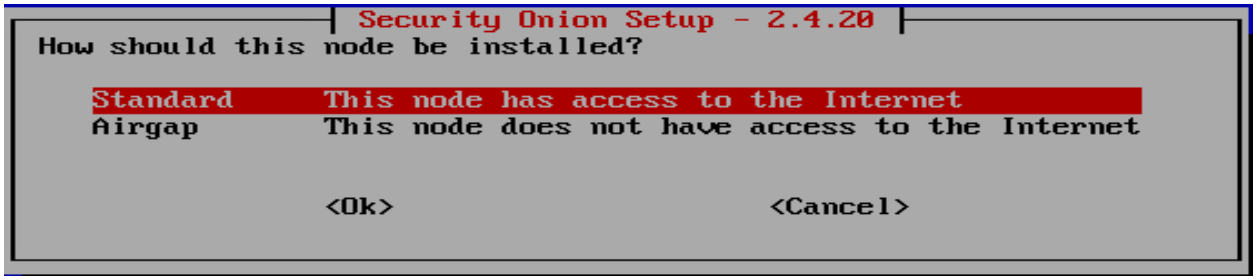
Step 9:
This is now considered the beginning of the configuration of Security Onion
Select the type of installation you would like to do
Standalone for this instance



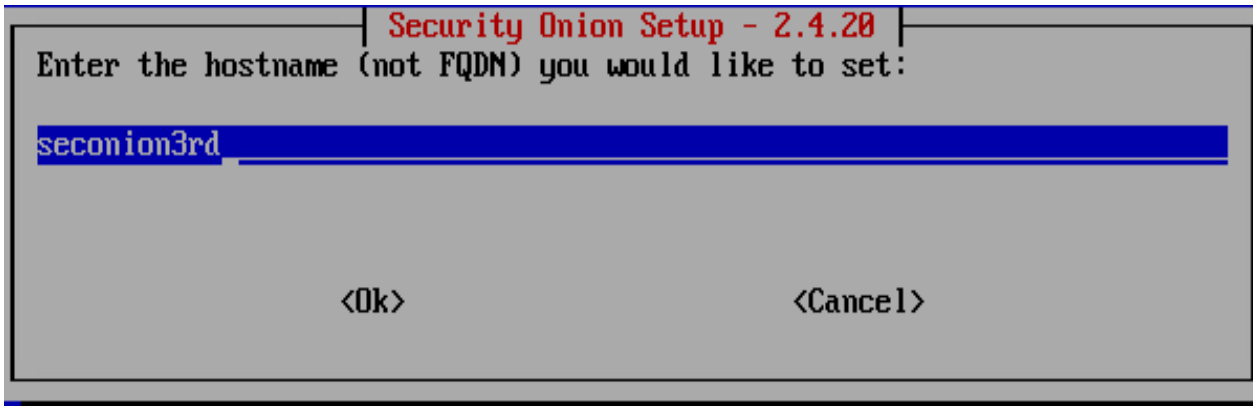
Step 10:
Type “ AGREE “ and press the ENTER key



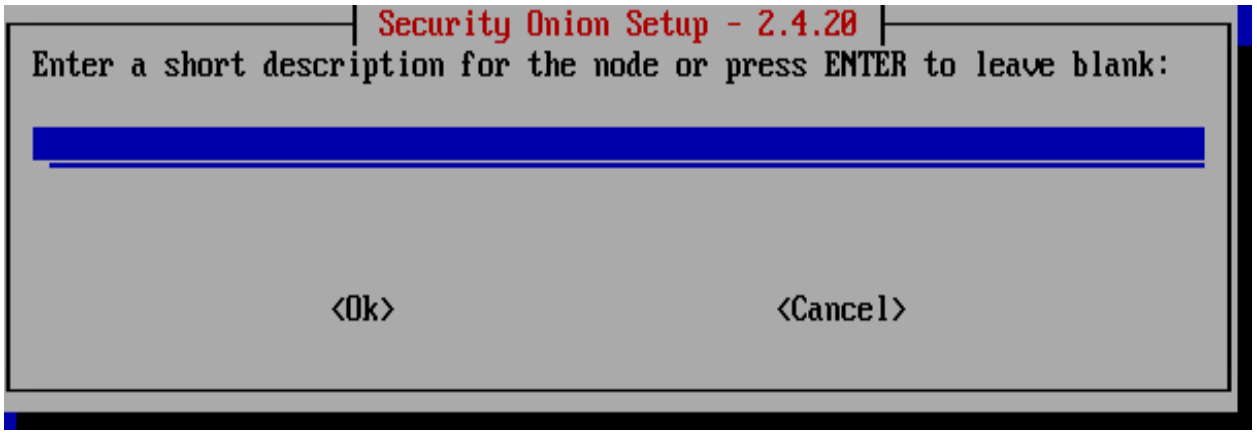
Step 11:
Select AIRGAP (THIS MODE DOES NOT HAVE ACCESS TO THE INTERNET)



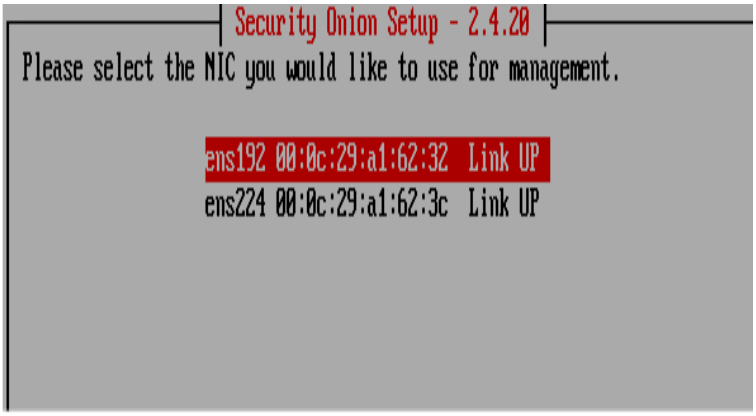
Step 12:
Enter Hostname:
“ Seconion3rd “
Press the Enter Key



Step 13:
Not required.
You’ll have the option to add a description for this Security Onion build



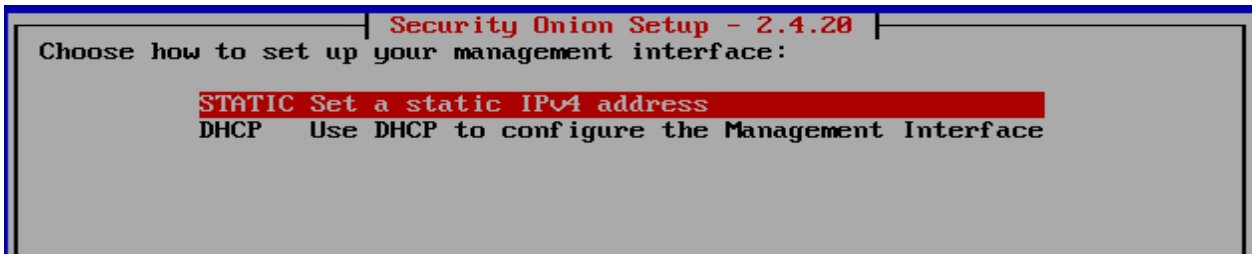
Step 14:
The first Network Interface Card should be the **Management** interface
Press the ENTER key

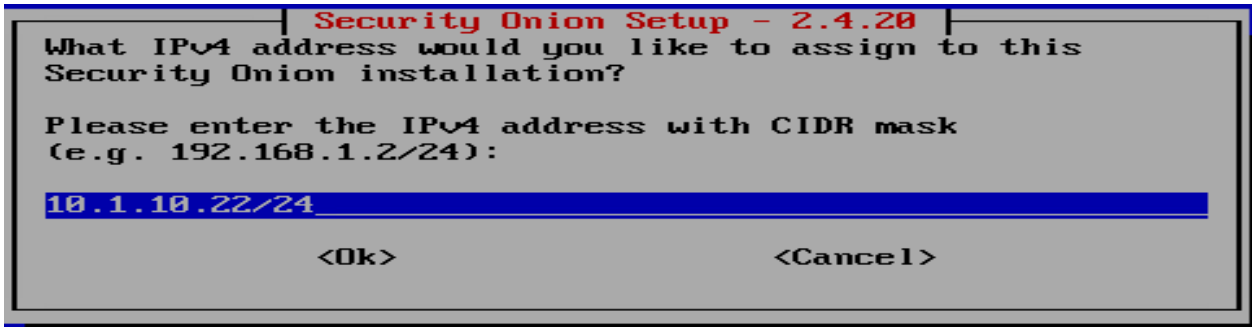


Step 15:

Depending on your internal network environment. You have the option to set-up your management interface.

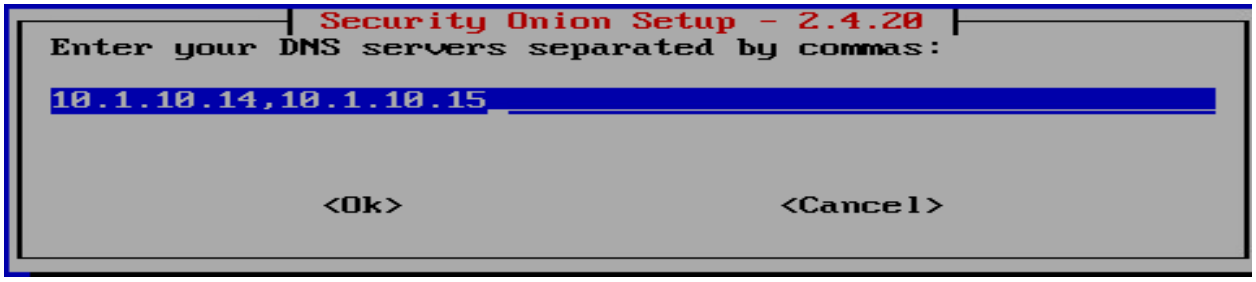
- Select Static
- Enter an IPv4 address with CIDR 10.1.10.22/24
- Press ENTER





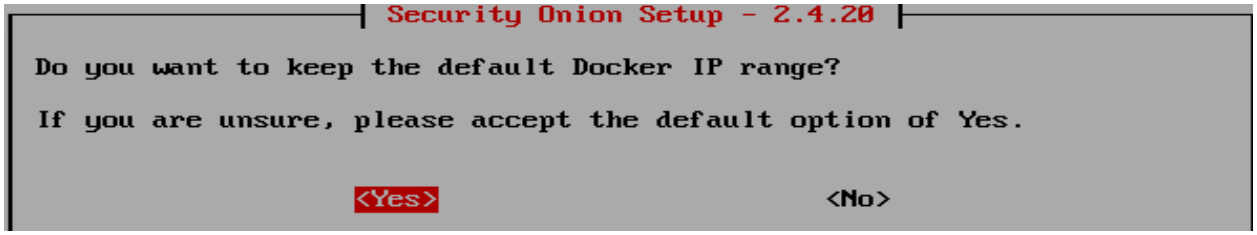
Step 16
Gateway IPv4 address:
10.1.10.1

Step 17:
Enter your DNS servers separated by commas. 10.1.10.14,10.1.10.15

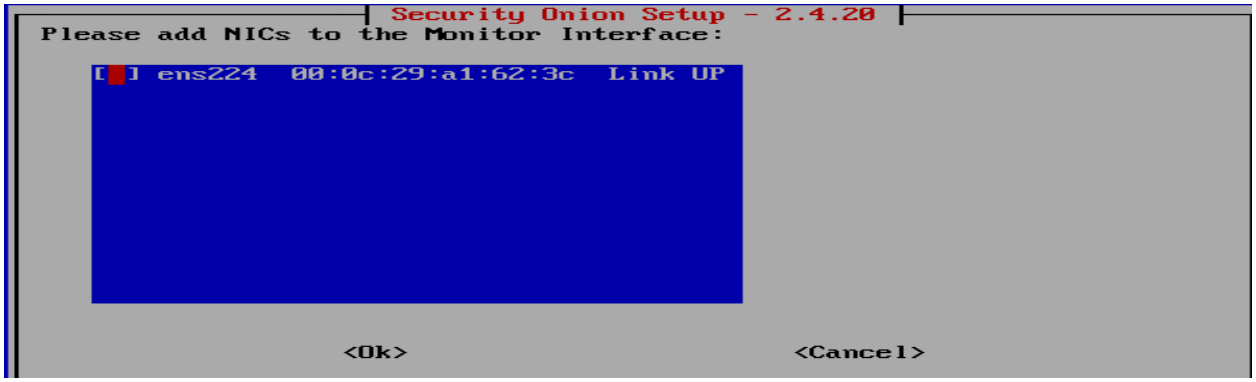


Step 18:
Enter your dns search domain : 3rdplt.dco.mil
(editor's note: use direct after step 18)

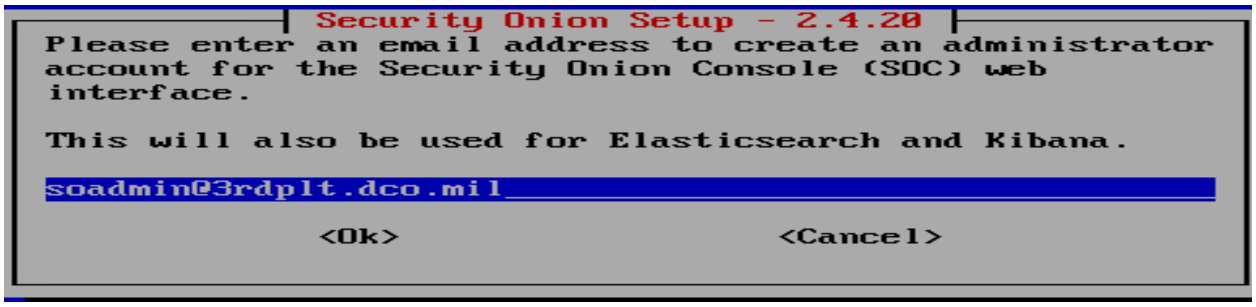
Step 19:



Step 20:
Press the spacebar to select the monitor interface

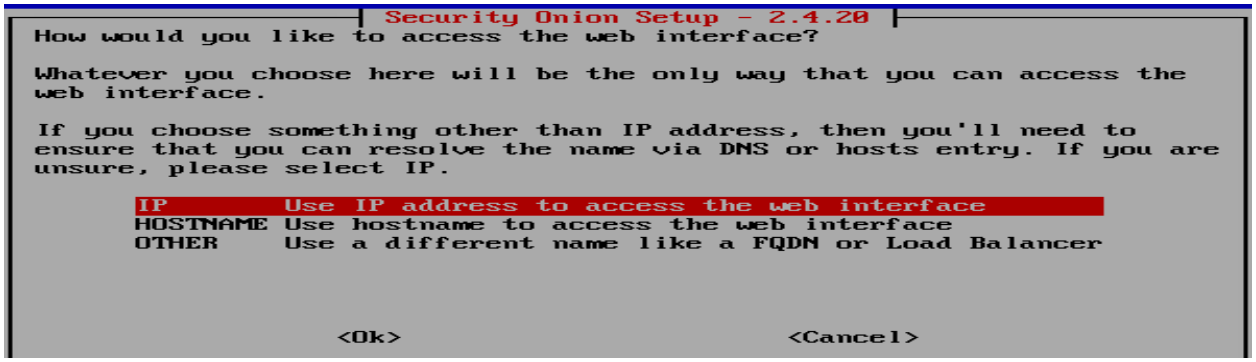


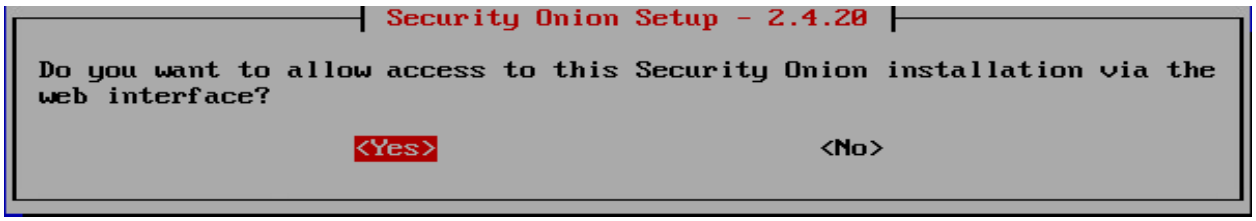
Step 21:
Enter an email address to create an administrator account for the web interface
soadmin@3rdplt.dco.mil

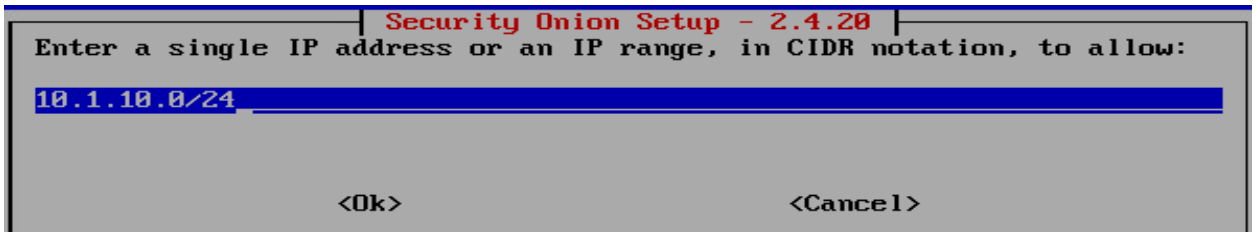


Step 22:
Standard password

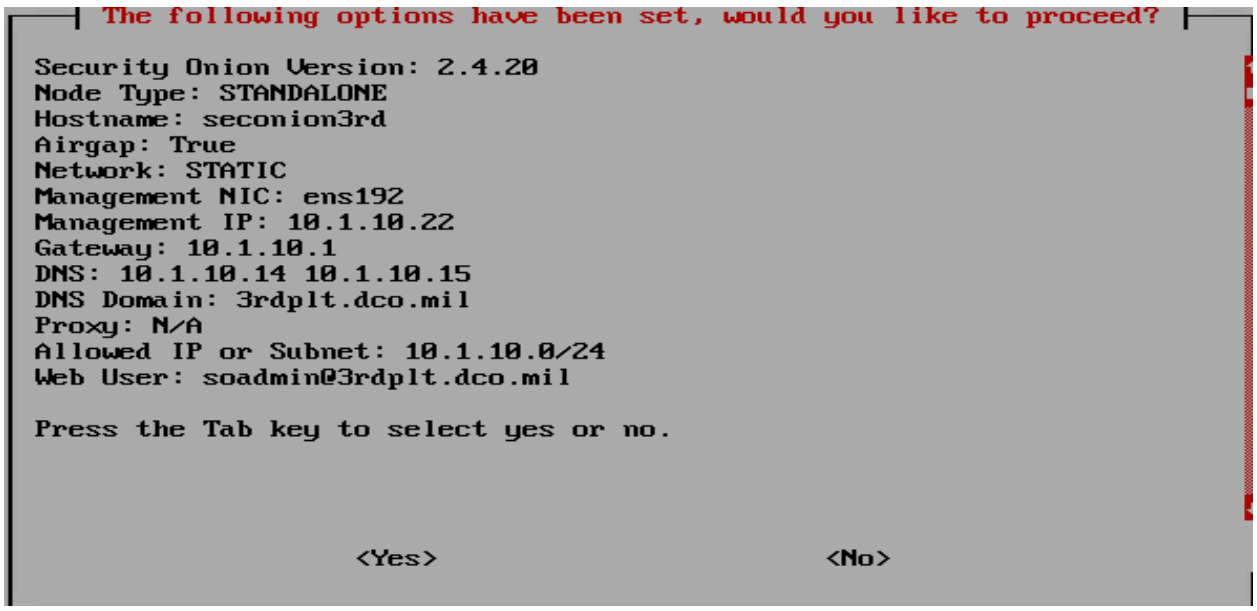
Step 23:
Select how you would like to reach the web interface.
We prefer IP.
Select Yes by using the TAB key
Enter a single IP Address or an IP range to allow : 10.1.10.0/24

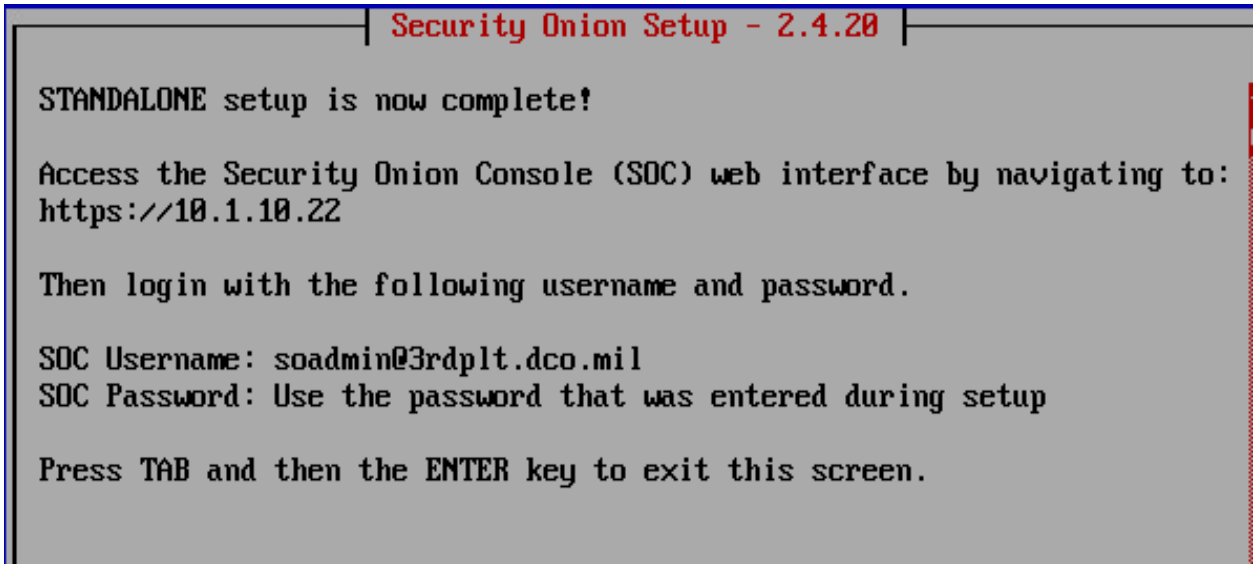






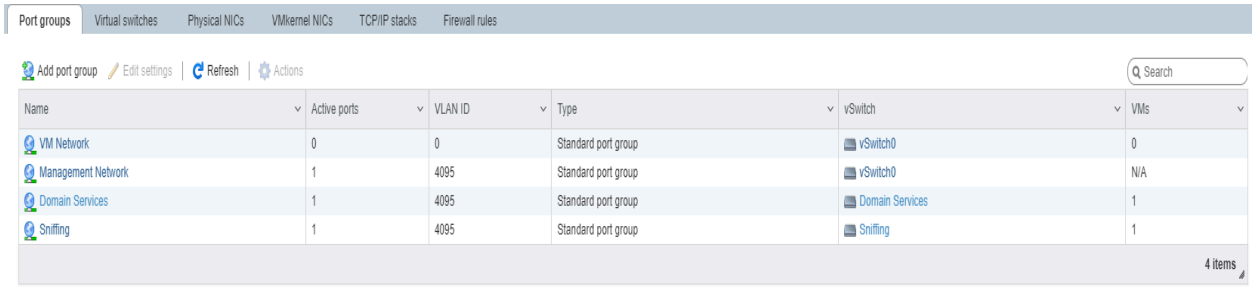
Step 24:
Hit TAB to select yes
Hit ENTER





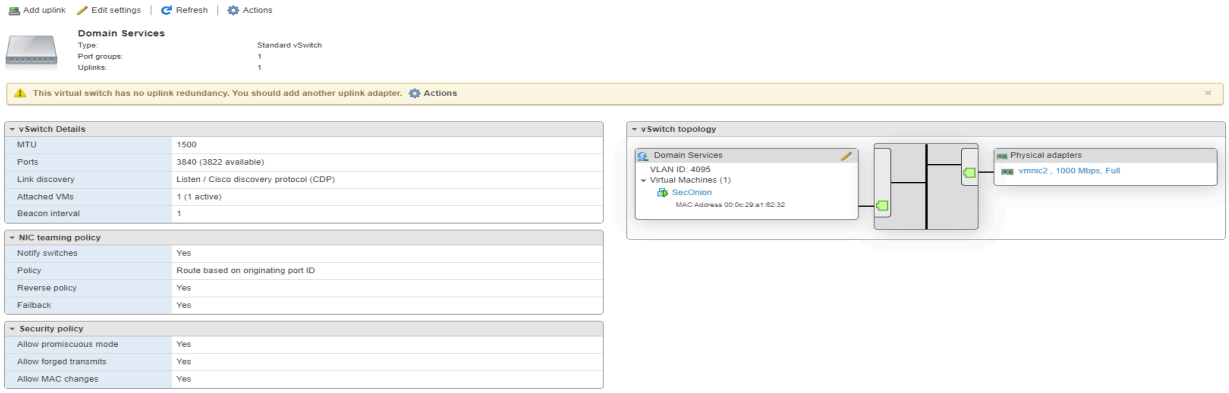
Hit TAB to select okay
Hit ENTER

Step 25:
ON ESXi
Go to the Networking tab
Under Port Groups

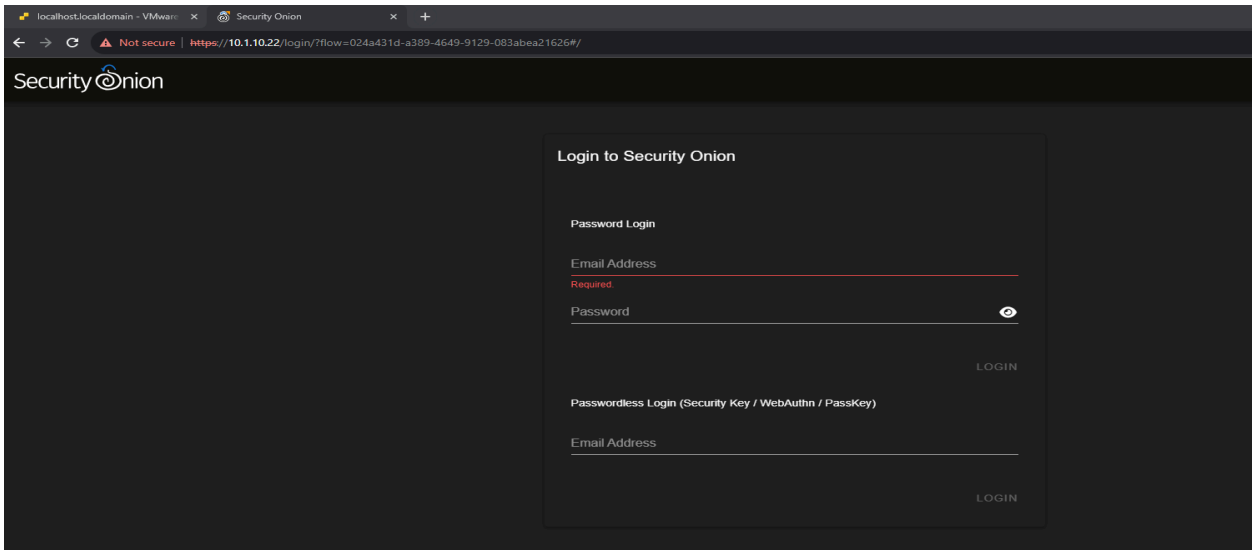


-Virtual Switches
- Select Domain Services

To reach the web interfaces you must have to GREEN connections on your switch topology

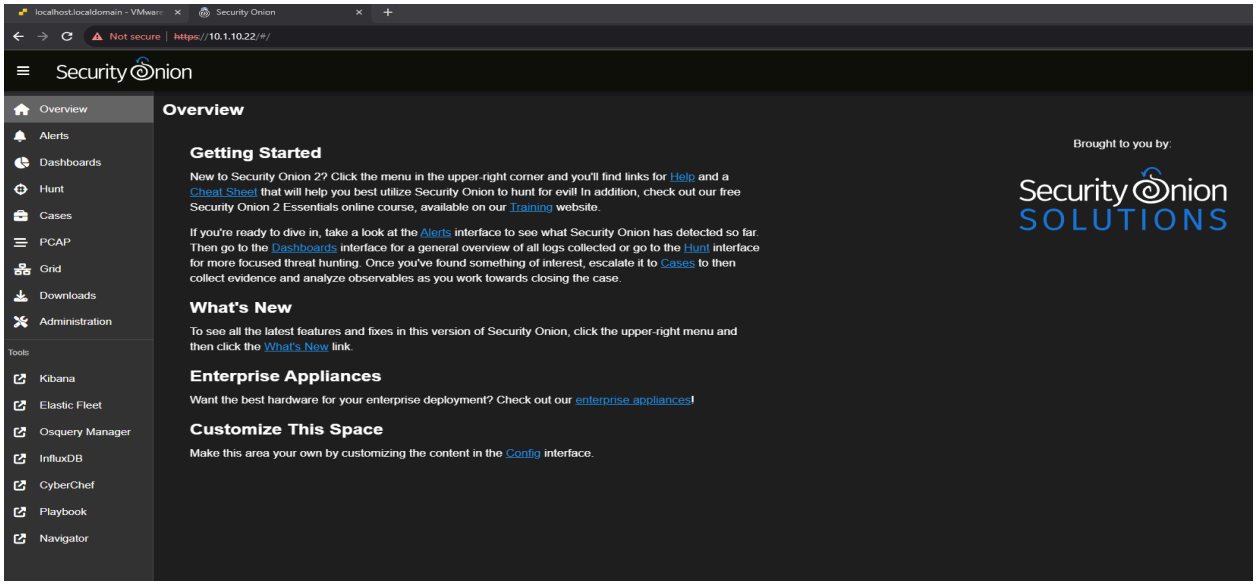


Step 26:
Log in with the WEB IP assigned
10.1.10.22
**If trouble reaching SecOnion occurs, refer to troubleshooting section about RSA keys



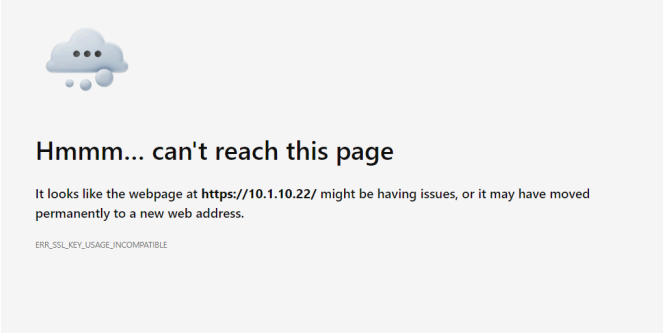
Step 27:
Credentials

soadmin@3rdplt.dco.mil
Standard



Troubleshooting SecOnion Browser: *ERR_SSL_Key*

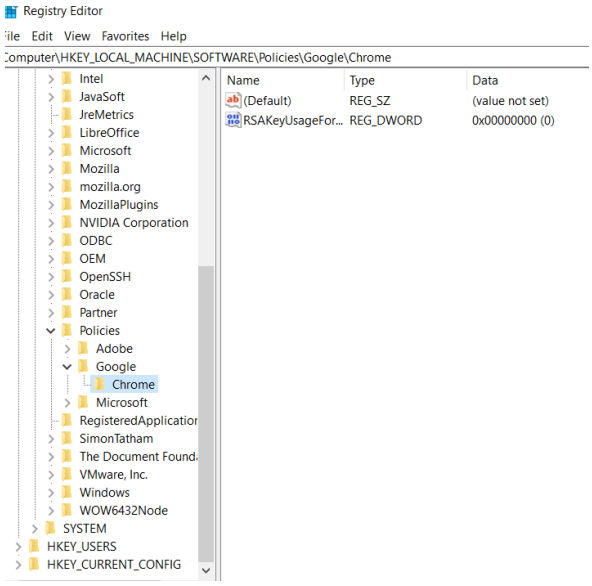
When navigating to the WEB IP, browser displays the Error Page:
'The webpage at **https://[SecOnion_IP]/** might be having issues, or it may have moved permanently to a new web address. *ERR_SSL_KEY_USAGE_INCOMPATIBLE*'



- Attempt navigating to the WEB IP on Google Chrome

If error persists:
This error displays because the workstation Registry is missing the necessary key to access the page.
Add it with the steps below:

- On DCO Workstation, Open Regedit
- Navigate to HKLM/SOFTWARE/Policies
- Right-Click Policies
  - New -> Key -> Name it 'Google'
- Right-Click Google
  - New -> Key -> Name it 'Chrome'
- Right-Click Chrome
  - New -> DWORD -> 'RSAKeyUsageForLocalAnchorEnabled'



- Open Chrome Web Browser
- Clear All browsing history
- Close and Reopen Chrome
- Navigate to assigned WEB IP
- Enter SecOnion Credentials

Configuring the Security Onion Firewall.

By: Cpl Uptmor, Connor J.
3rd PLT DCO-IDM
LU: 20231010

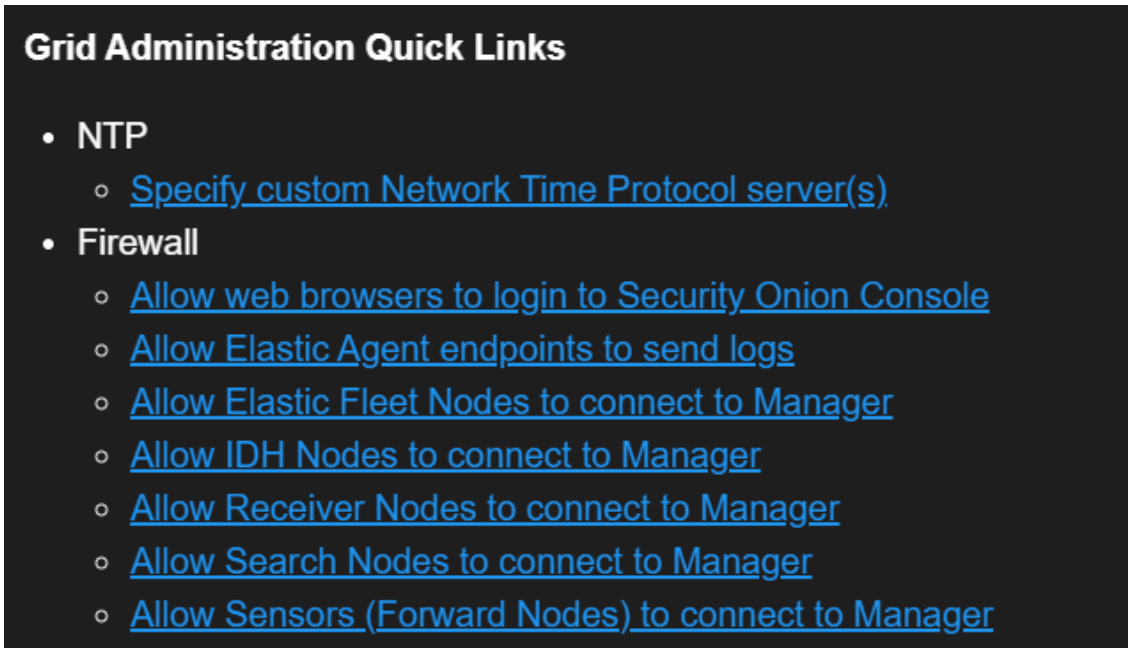
This document will serve as the guide to configuring your security onion standalone manager after you have already successfully installed your SOM on either your ESXi hypervisor or on a bare metal server.

You will need to allow 3 things through the firewall on security onion

1. Your internal IP space.
2. Your external firewall IP address.
3. Your customer's IP space.

How to get there:

Navigate to the Security Onions home page.
Then go to
>> Administration
>> Configuration
>> Firewall
>>hostgroups
>> elastic_agent_endpoint



You can also navigate to it via the hyperlink and it will take you directly to it.

Configuring your REAL firewall.

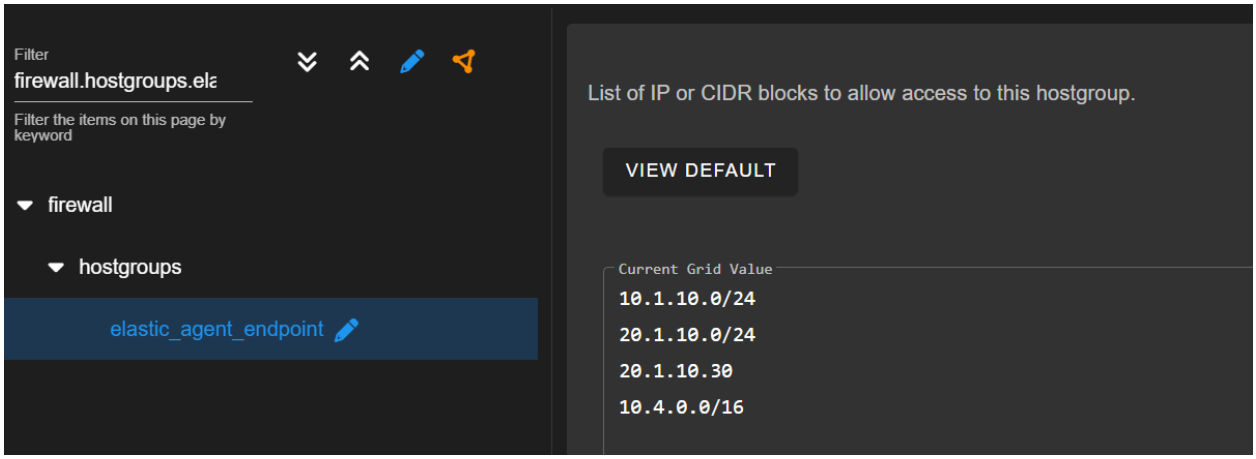
(a more detailed guide of how to configure this on the palo alto firewall will be included in the Palo Alto firewall S.O.P.)

In your firewall you need to allow the customer network to send logs through it to the security onion.

This means allowing through the ports that the endpoint agent ships logs over and also the port that it connects over to initiate the initial connection to the SOM.

Default Ports allowed on Palo Alto:
8220
5055
5044
8443

These ports need to be allowed because those ports are what the Elastic Agent uses to forward its traffic to the Security Onion Manager.
*** Only add the top ip in current grid value ***



Deploying the Elastic Agent

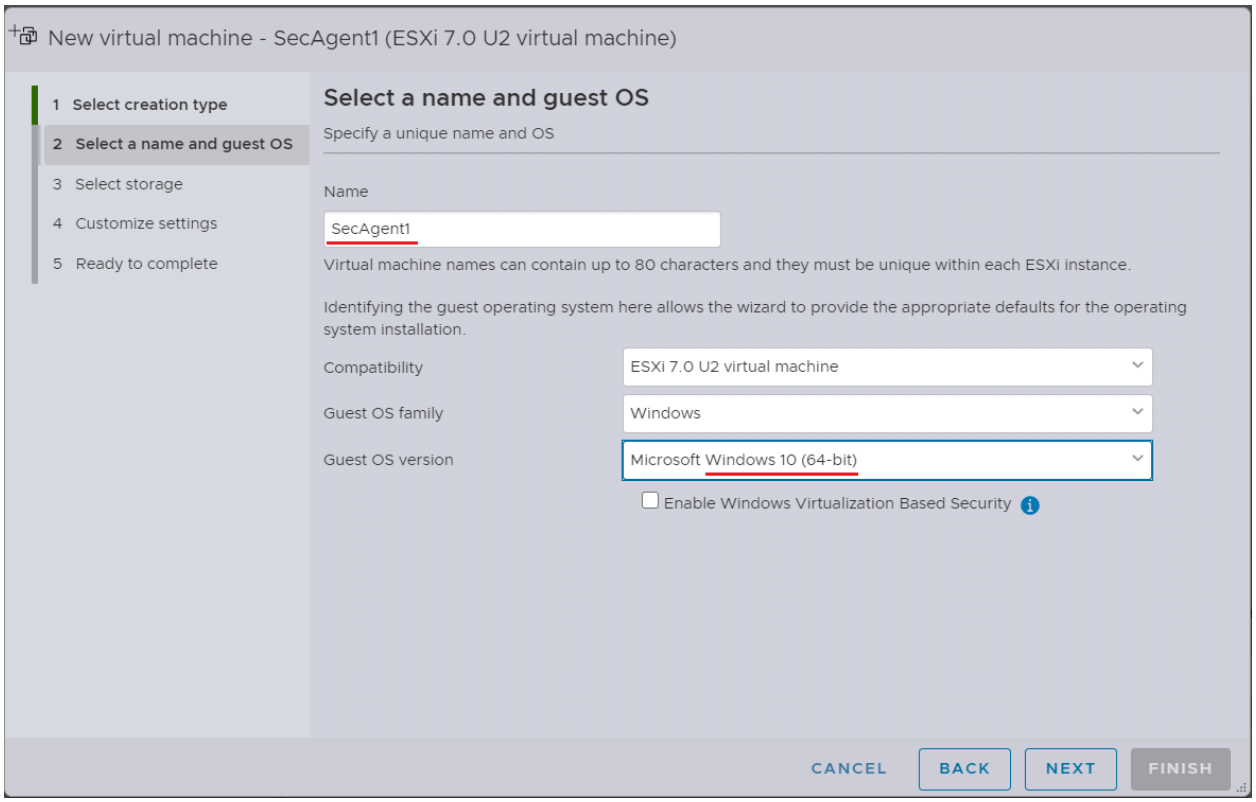
LCpl Klippel, LCpl Stephens

Deploying the elastic agent on the customers machines requires two things. A short powershell one liner and the elastic_agent_package which is a folder of contents that is needed to install the elastic agent. There is a different elastic_agent_package for windows and linux.

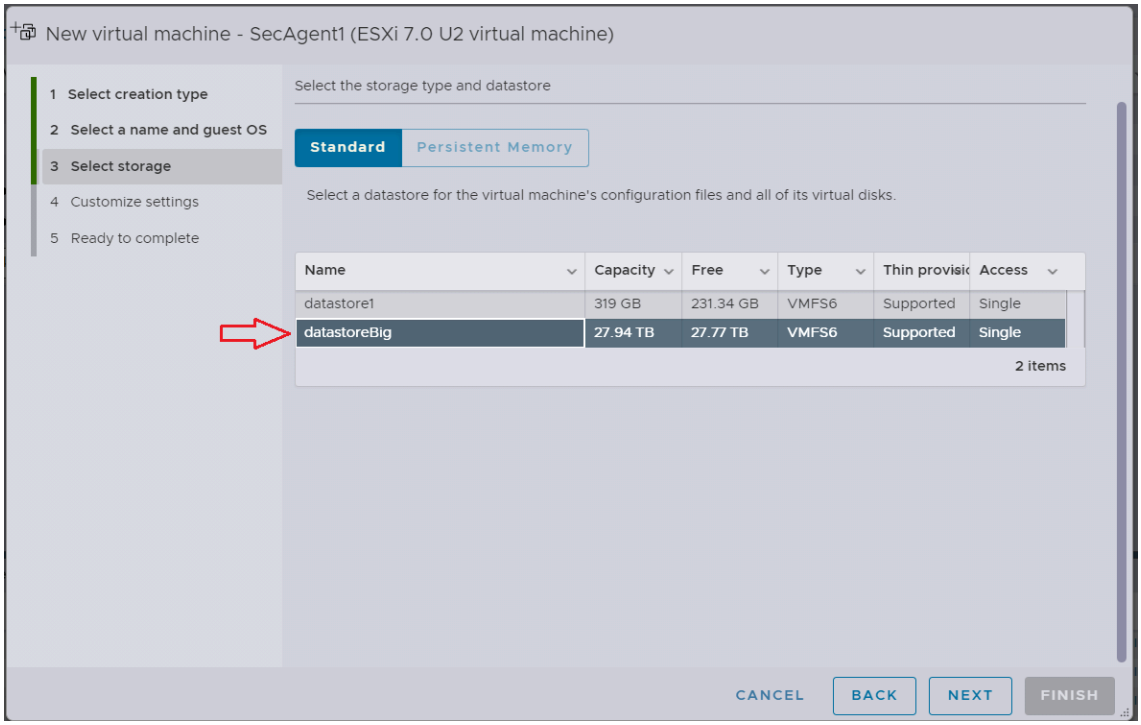
The whole package which includes the powershell script and the folder is already created but should be updated as you update your security onion over time.

As an example or for testing purposes:

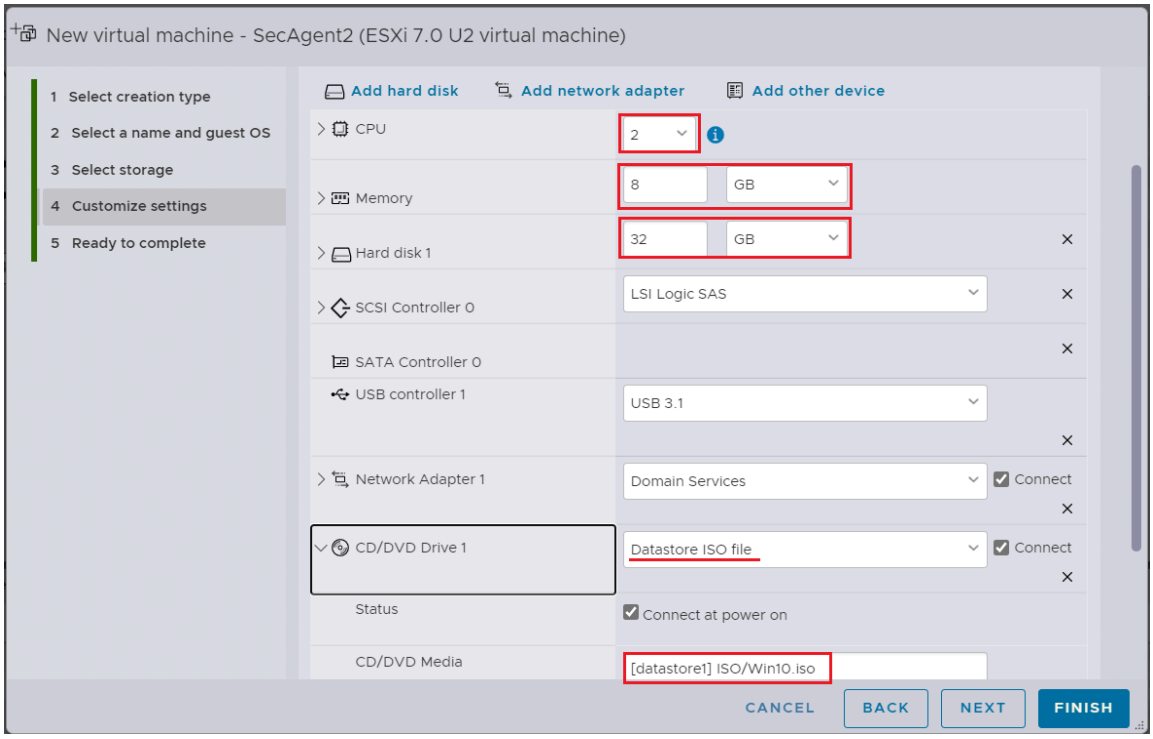
- Create 2 VMs with Windows 10
  - SecAgent1 and SecAgent2
  - Windows - Windows 10 (64-bit)



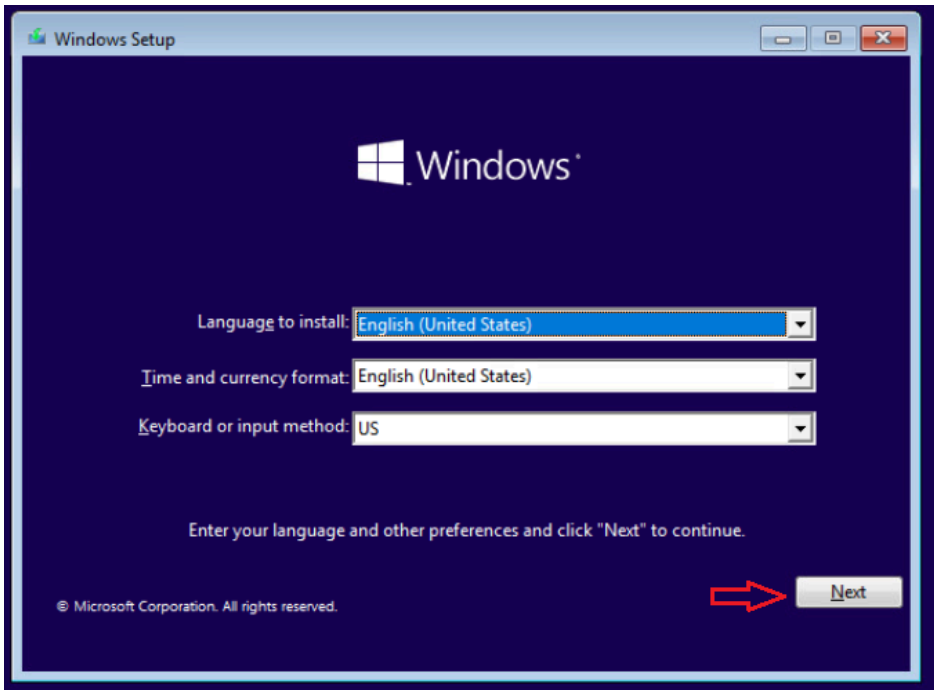
- Save in largest datastore



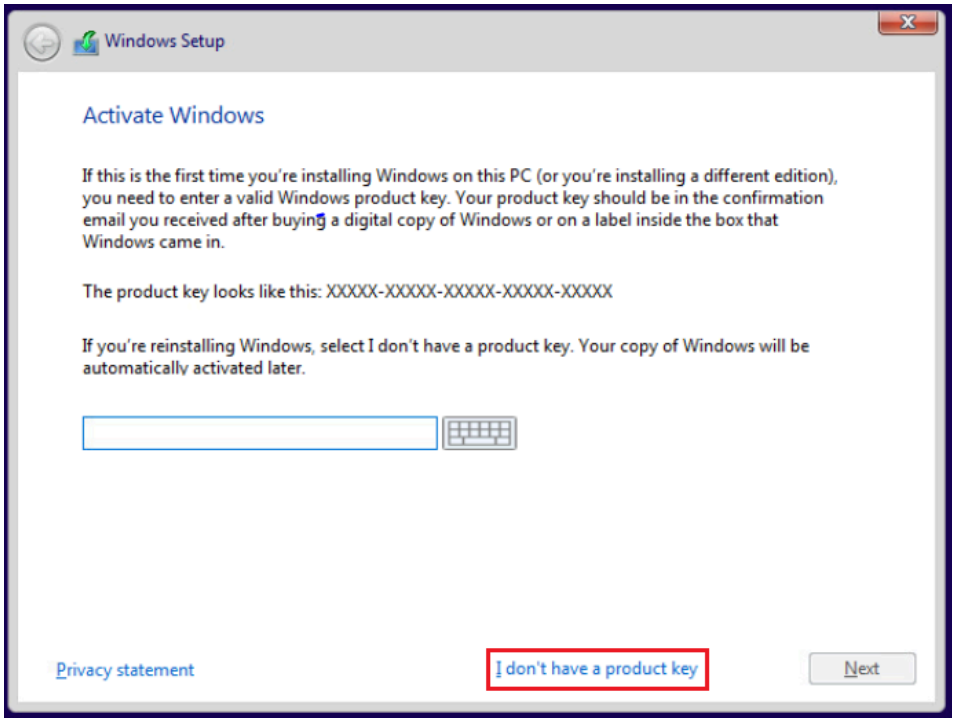
- 2 CPUs
- 8GB Memory
- 32GB Storage, thin-provisioned
- Win10.iso



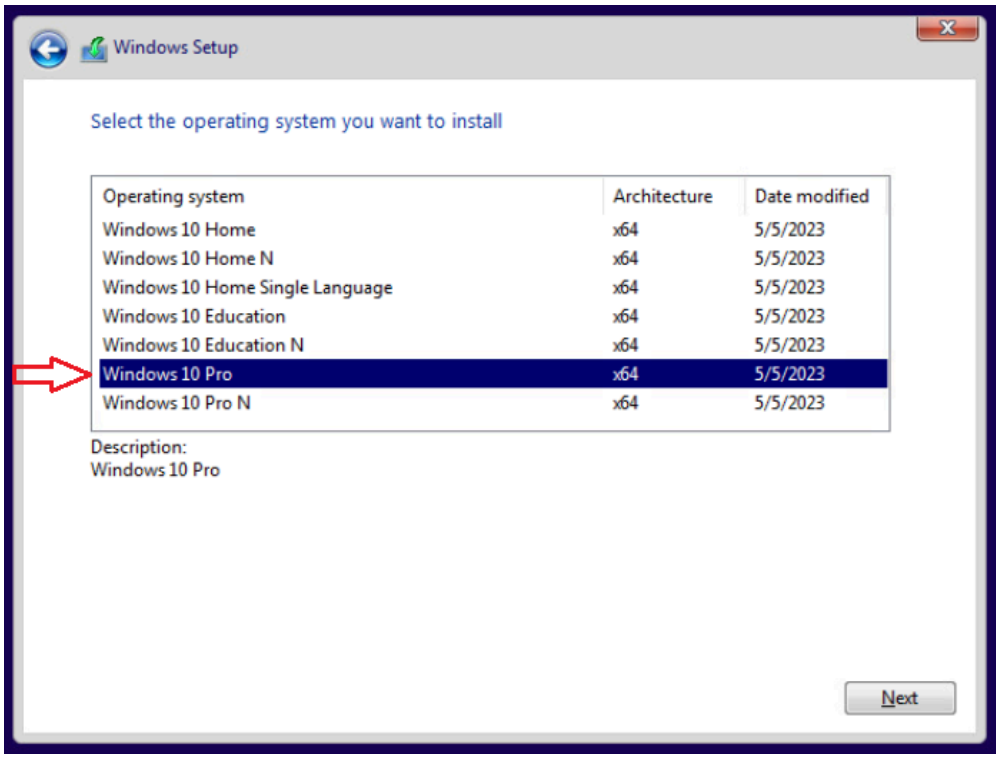
- Power On
  - (press ENTER if required to “boot normally”)
- Set language/time currency to ‘English’ -> Next



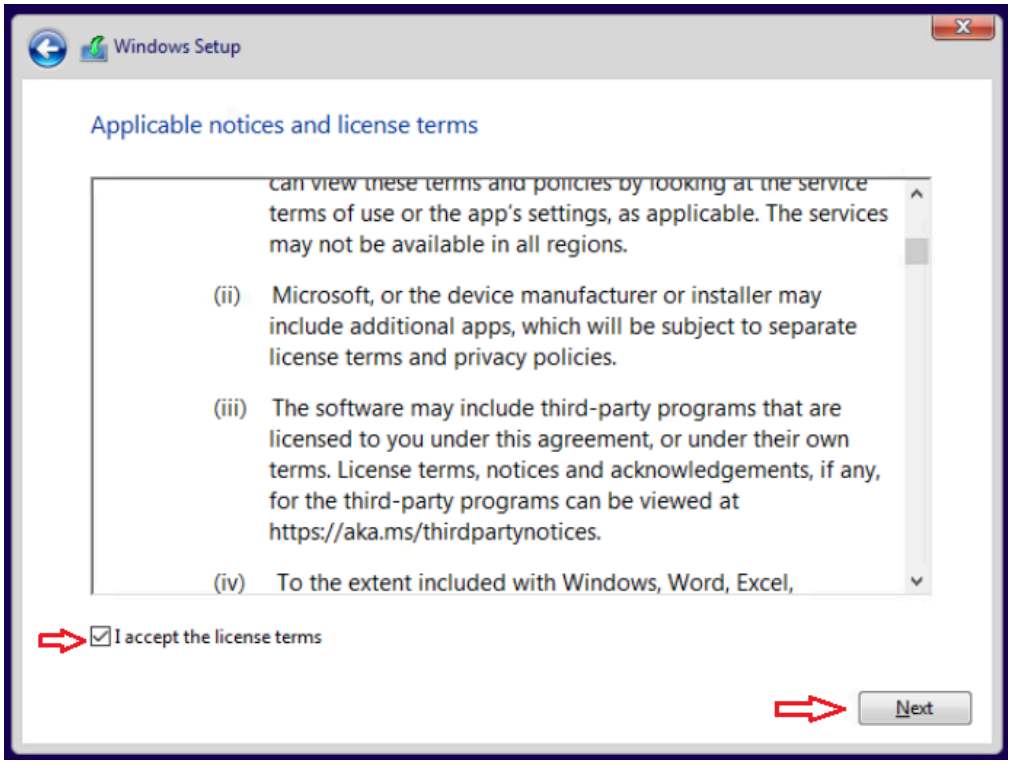
- Install Now
- ‘I don’t have a product key’



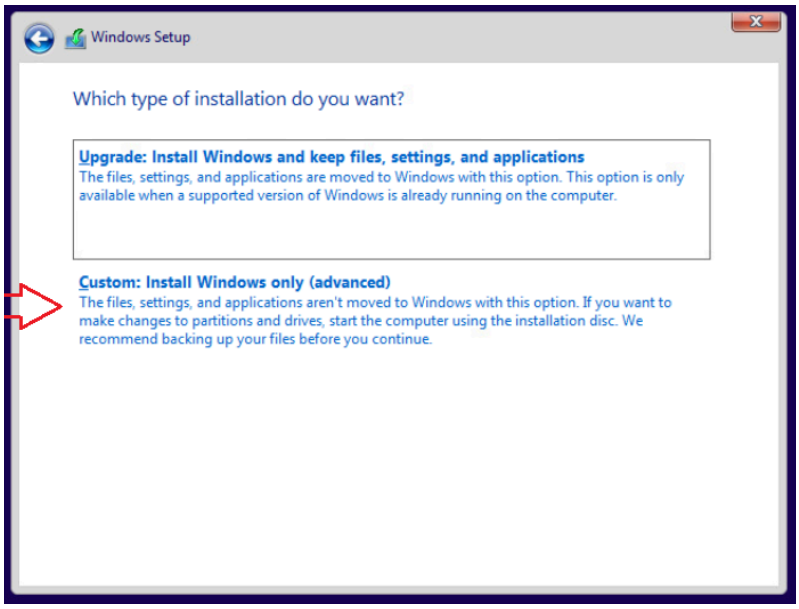
- Windows 10 Pro -> Next

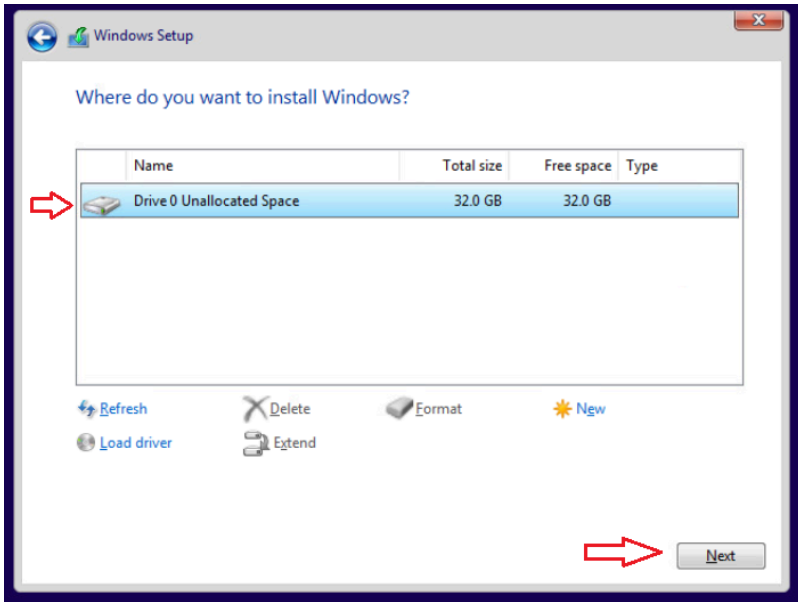


- Accept license terms -> Next



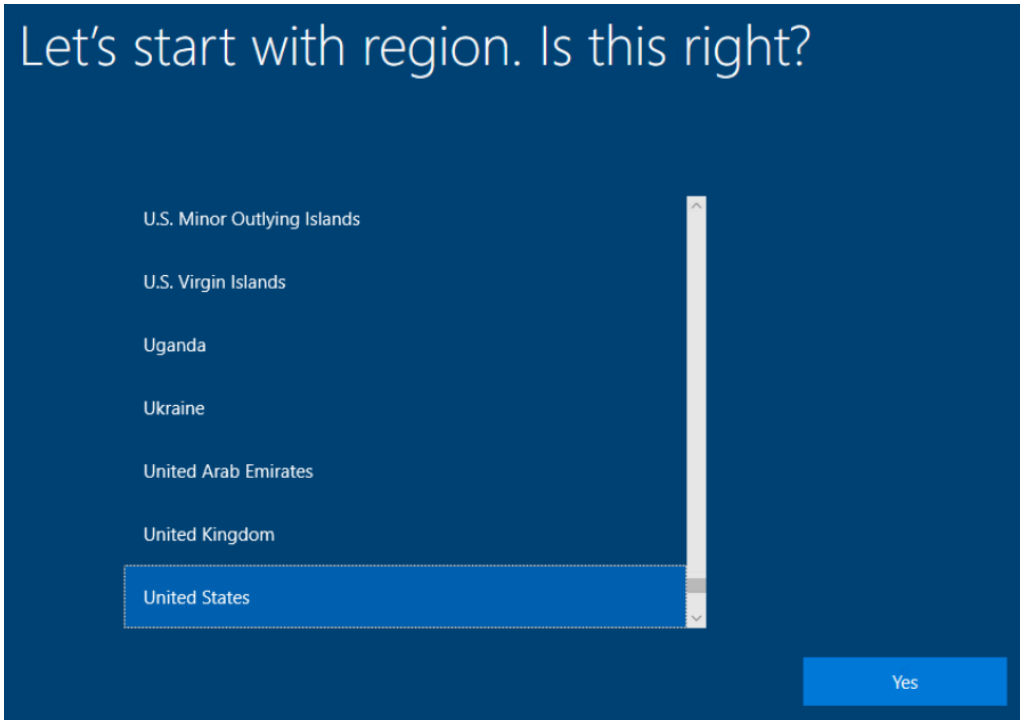
- Custom Install -> Drive0 -> Next

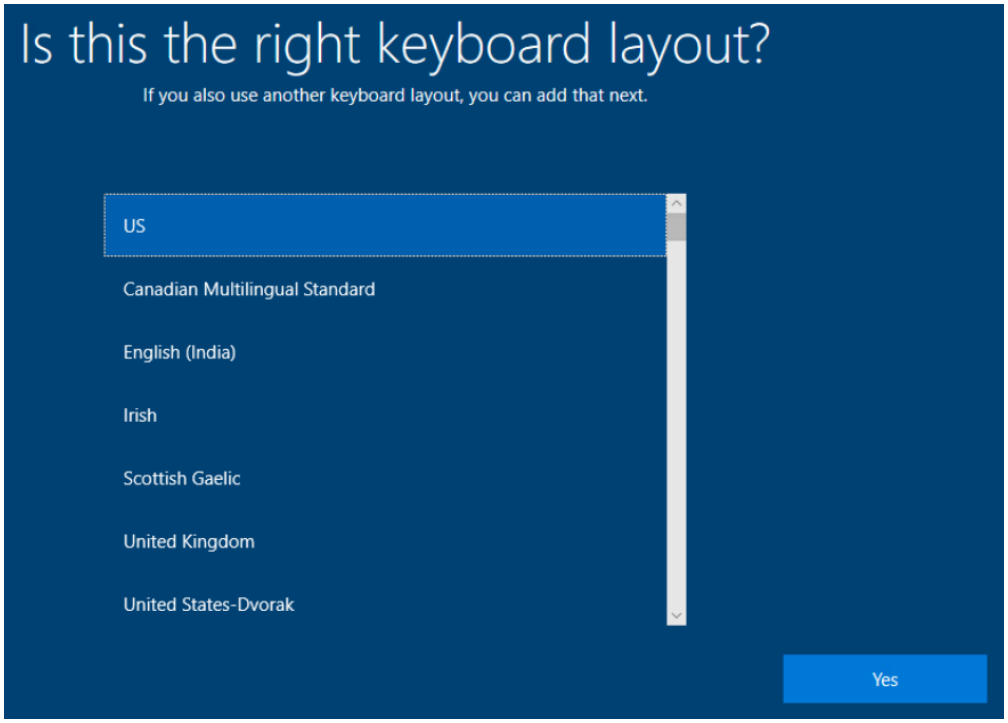




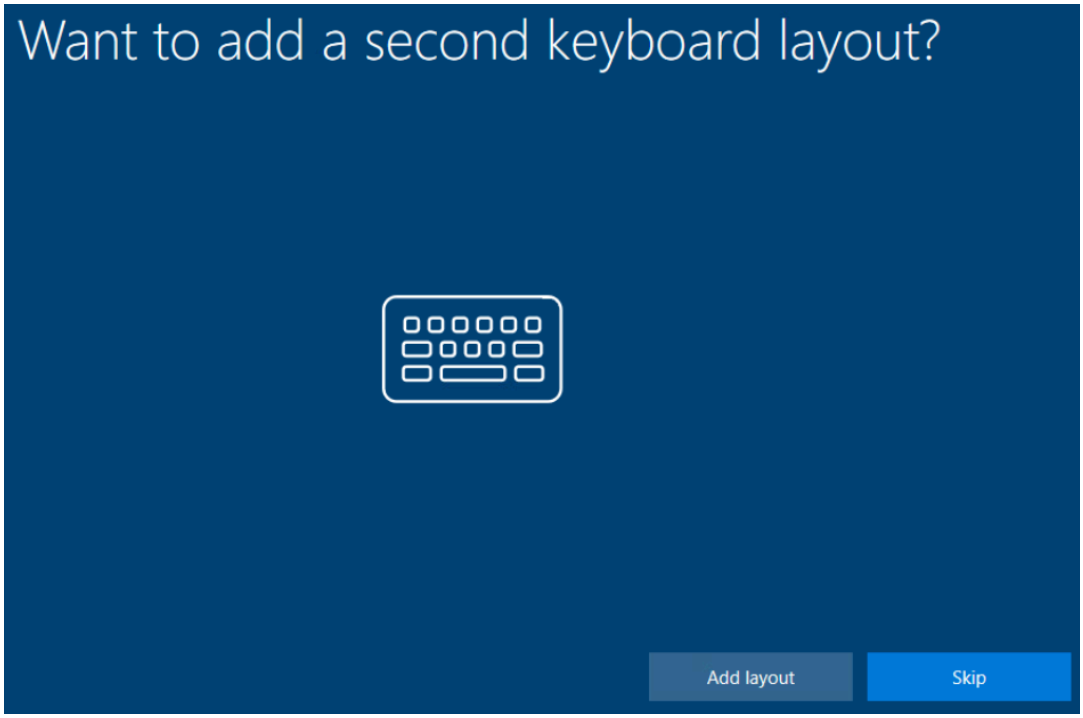
- Allow time for install
- VM should restart automatically / If not, restart manually

- Select ‘US’ keyboard layout -> Next

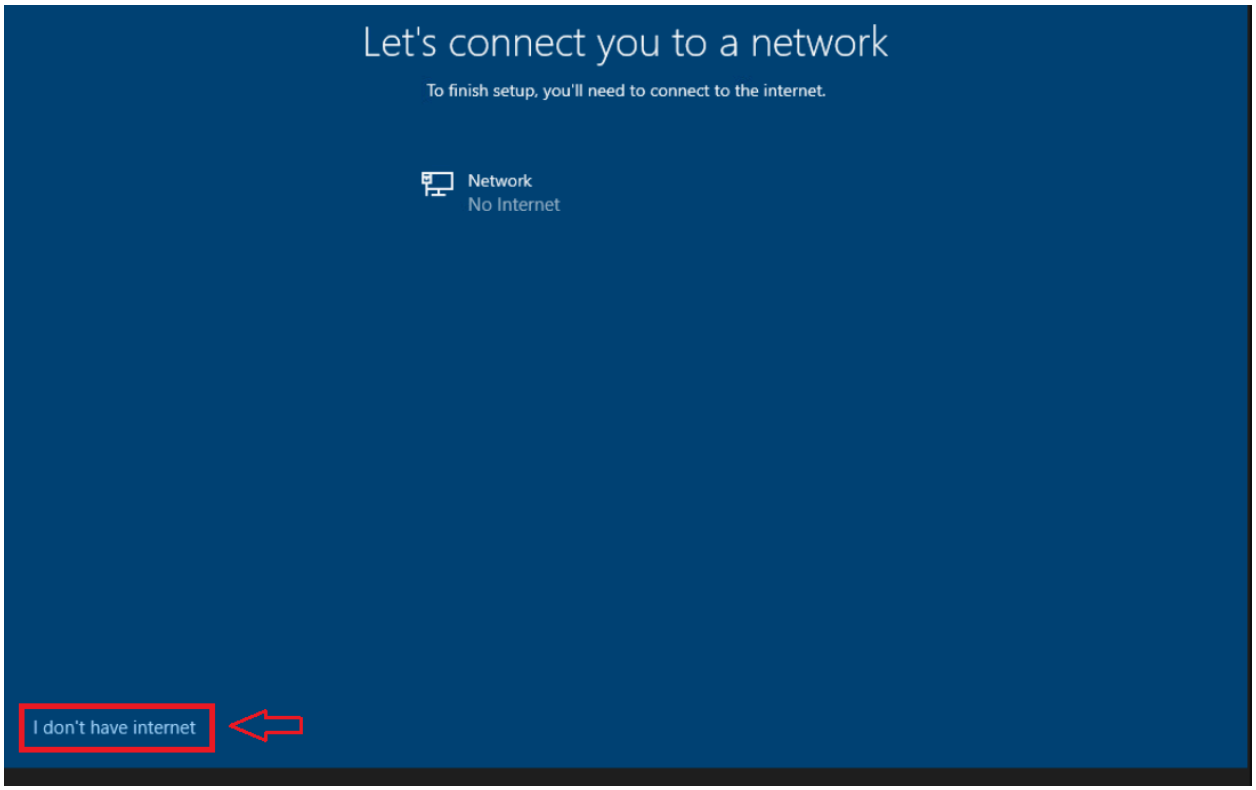




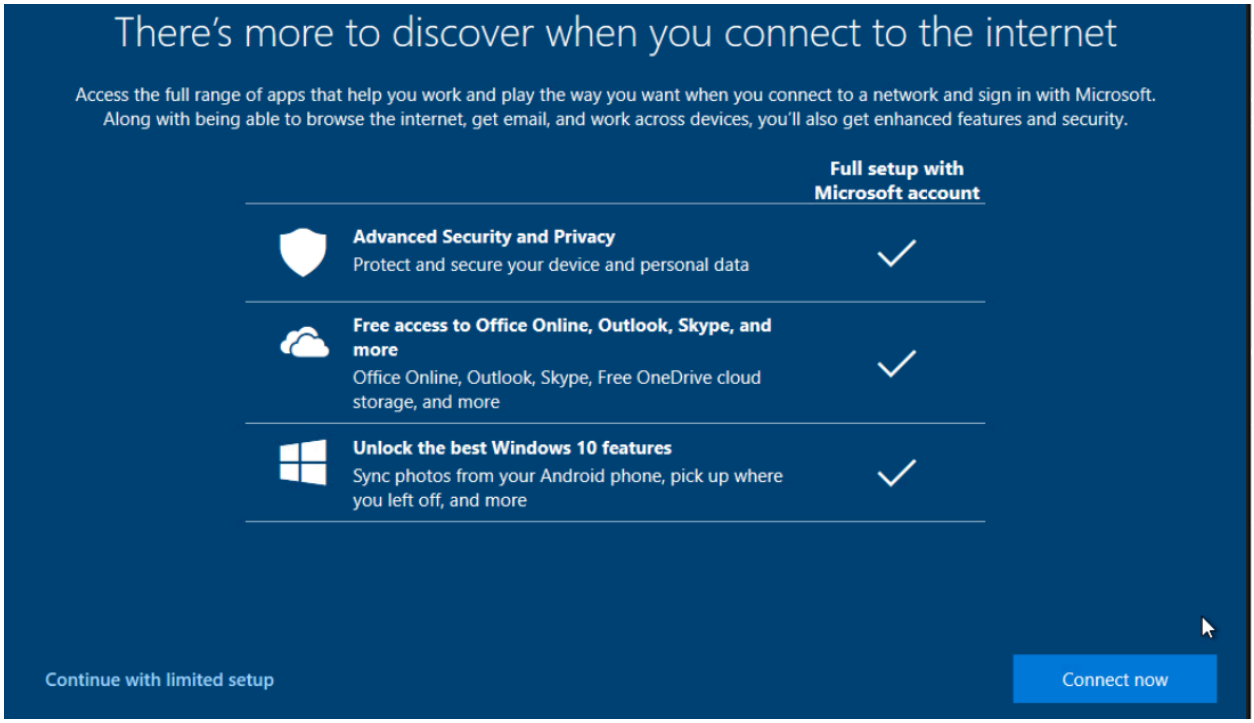
- Skip second keyboard layout



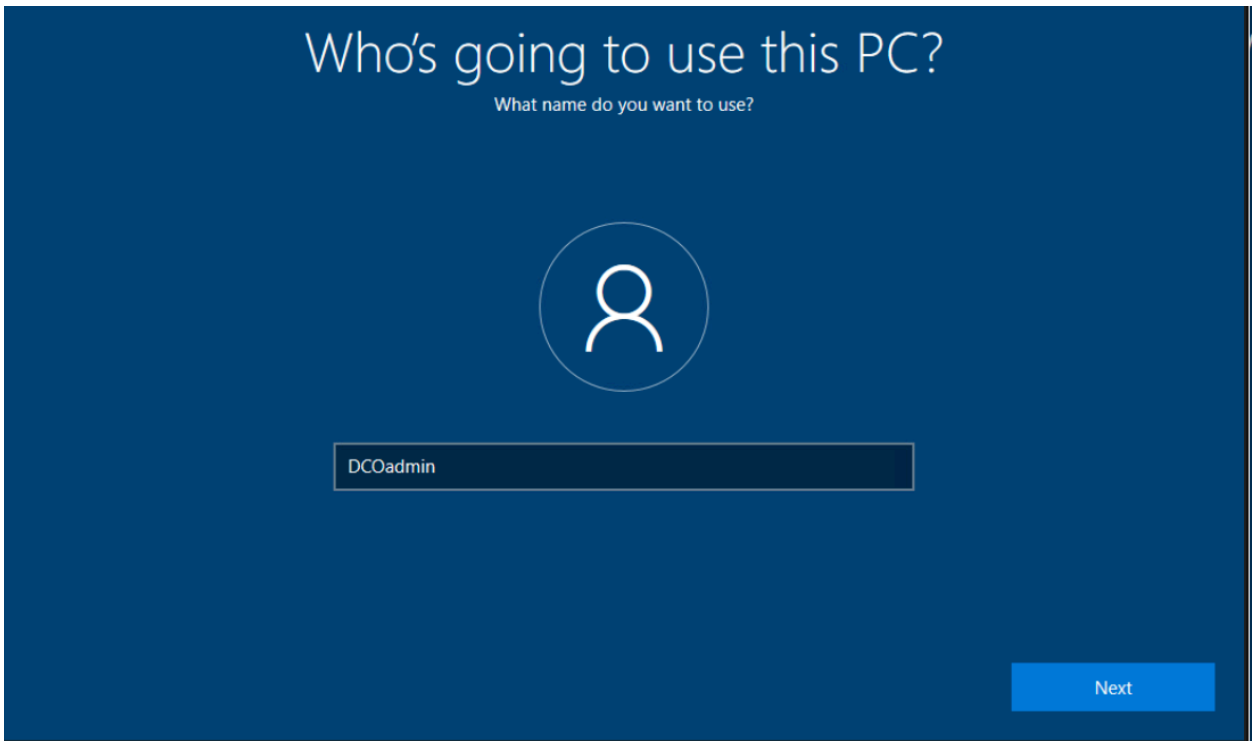
- ‘I don’t have network’



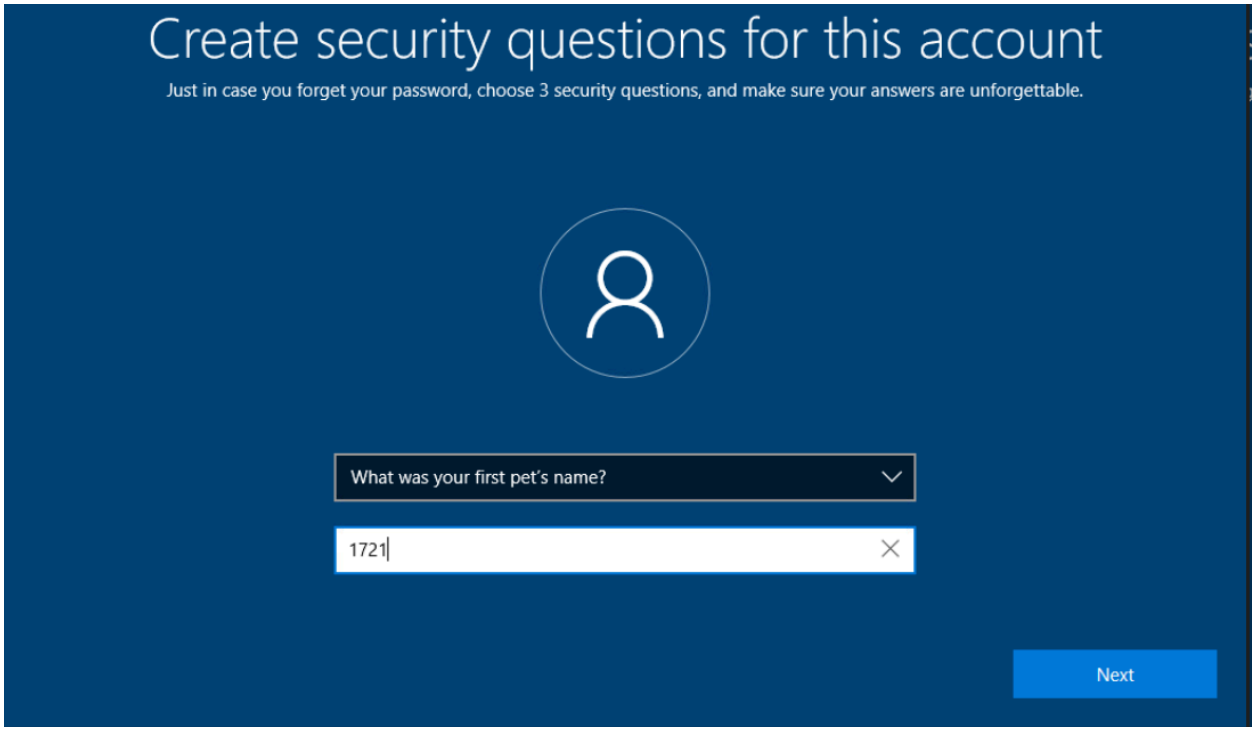
- ‘Continue with limited setup’



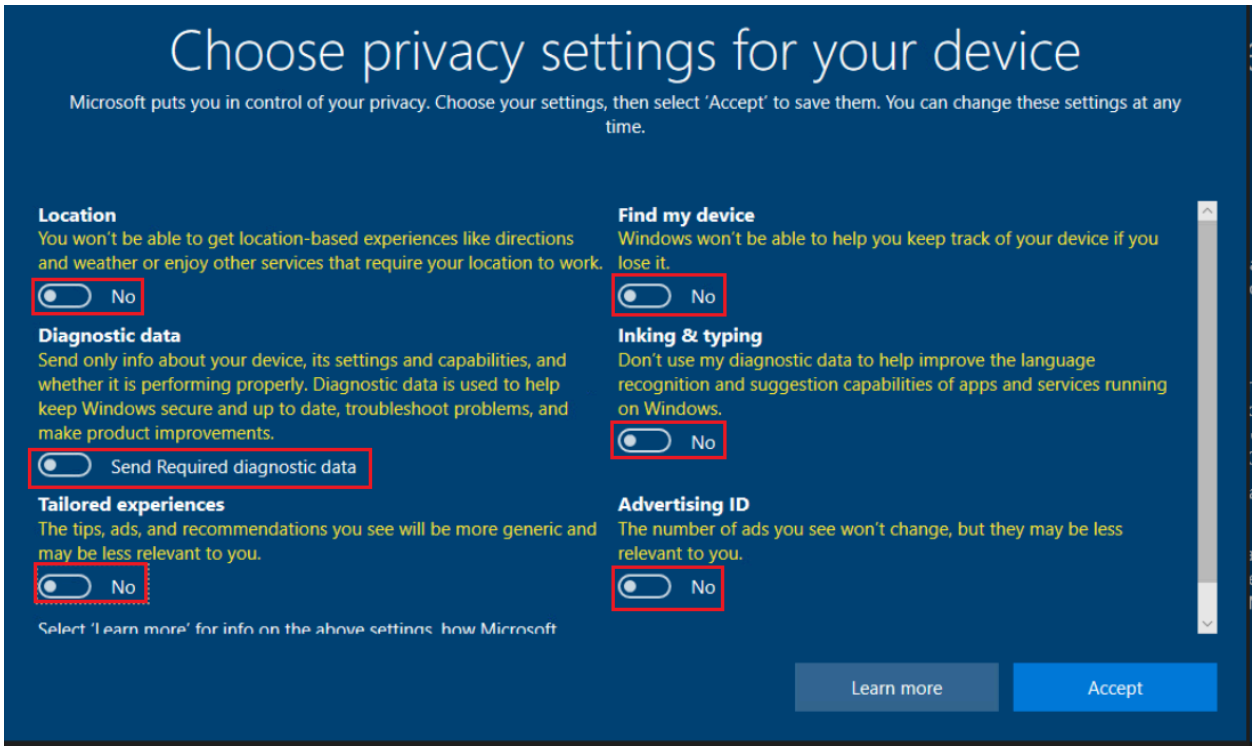
- Create ‘DCOadmin’ account -> Next
- Shop standard password -> Next -> Confirm Password -> Next



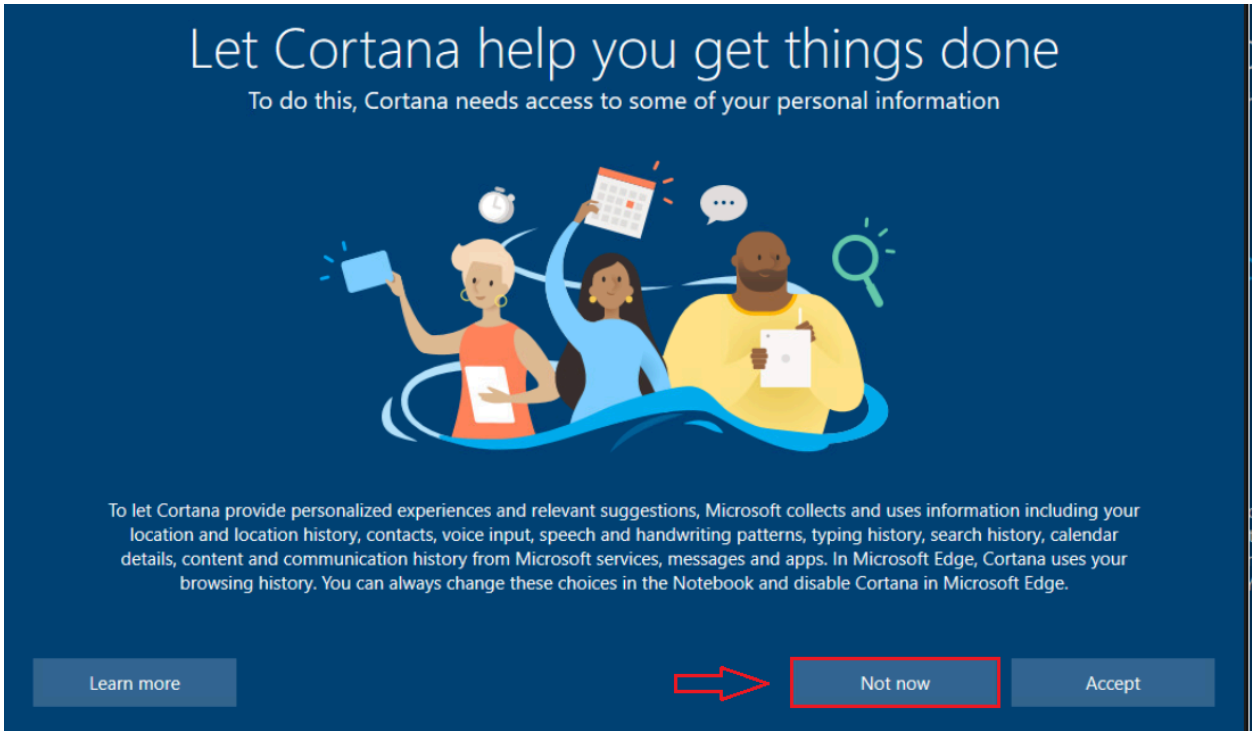
- Select security questions -> Answer: 1721



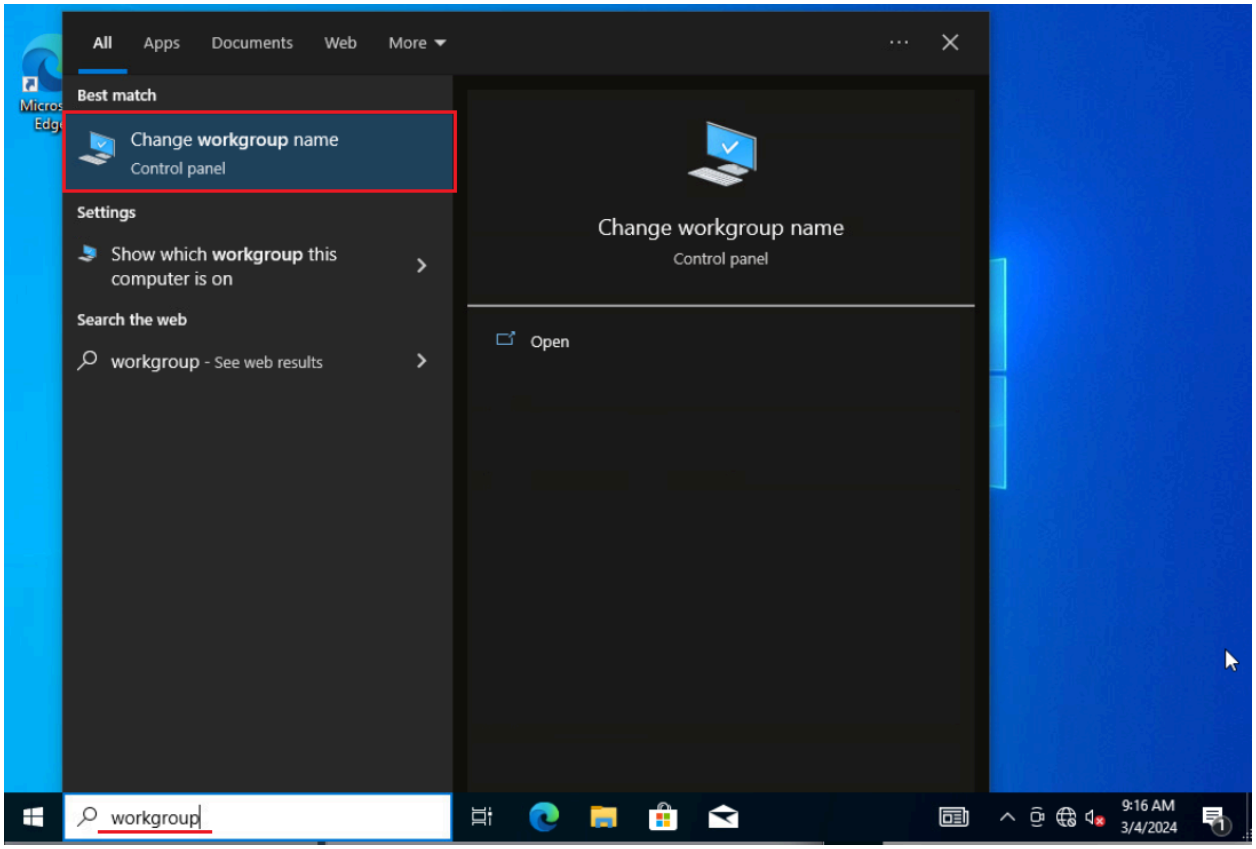
- Check 'No' for all options -> Accept



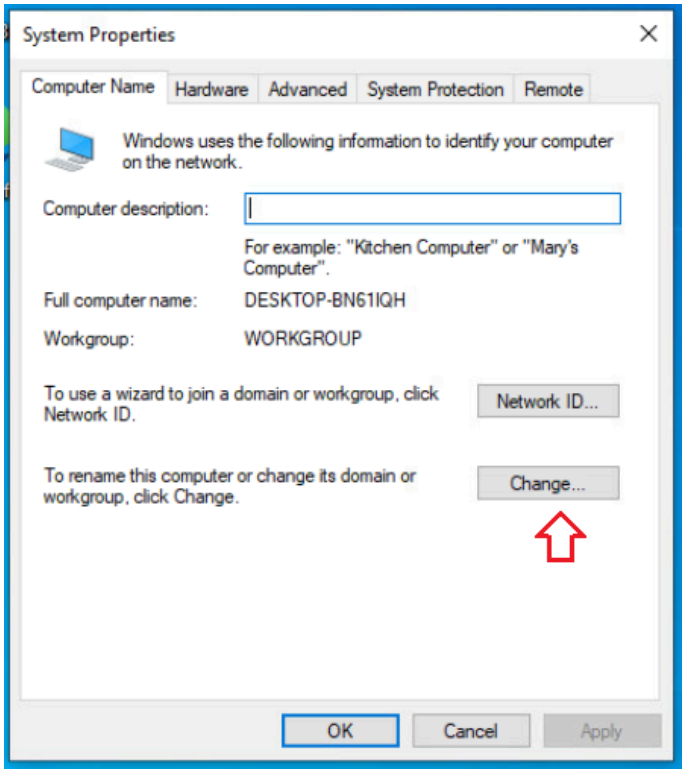
- ‘Not Now’

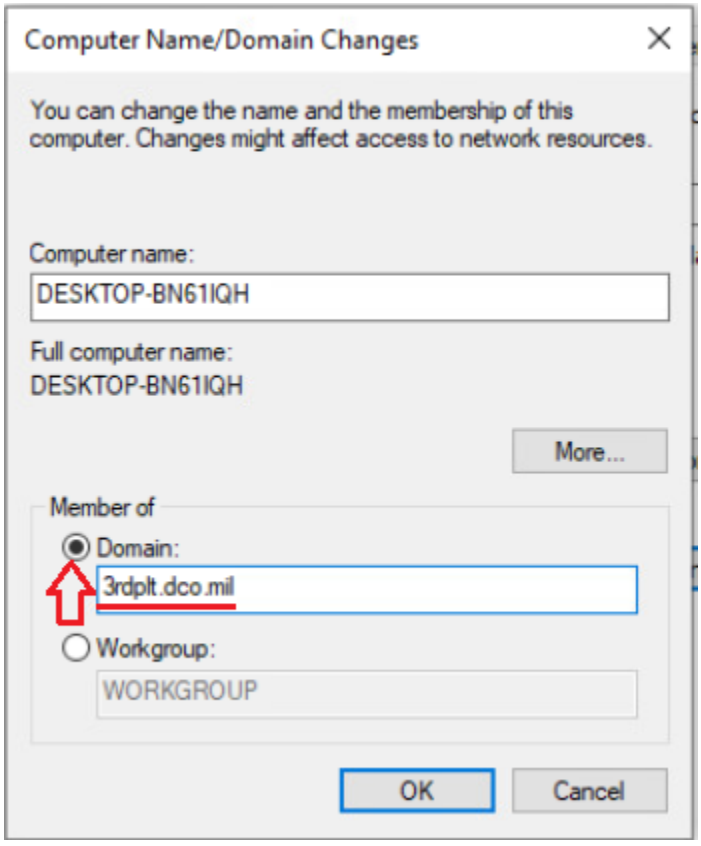


- Allow time for configuration
- Navigate to ‘Change Workgroup Name’

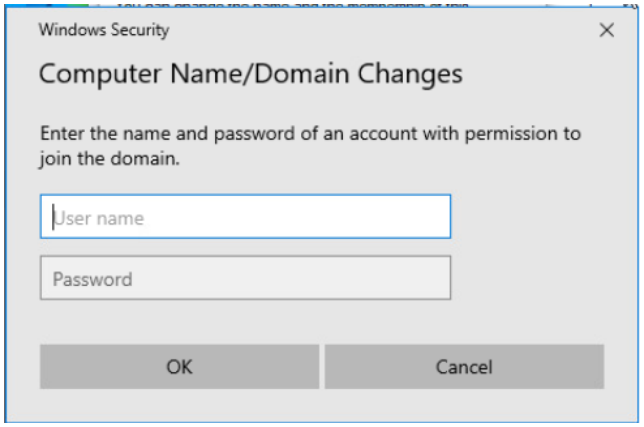


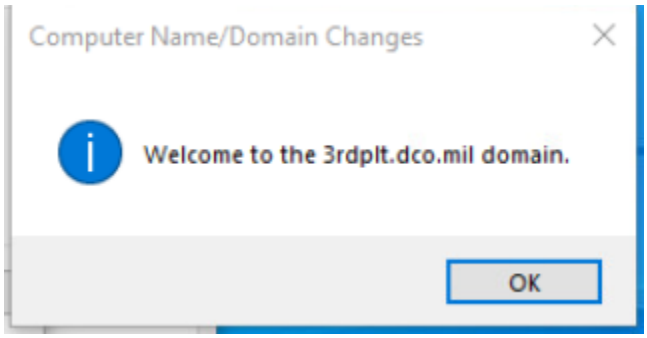
- Add VM to 3rdplt.dco.mil





- Enter ‘Administrator’ credentials



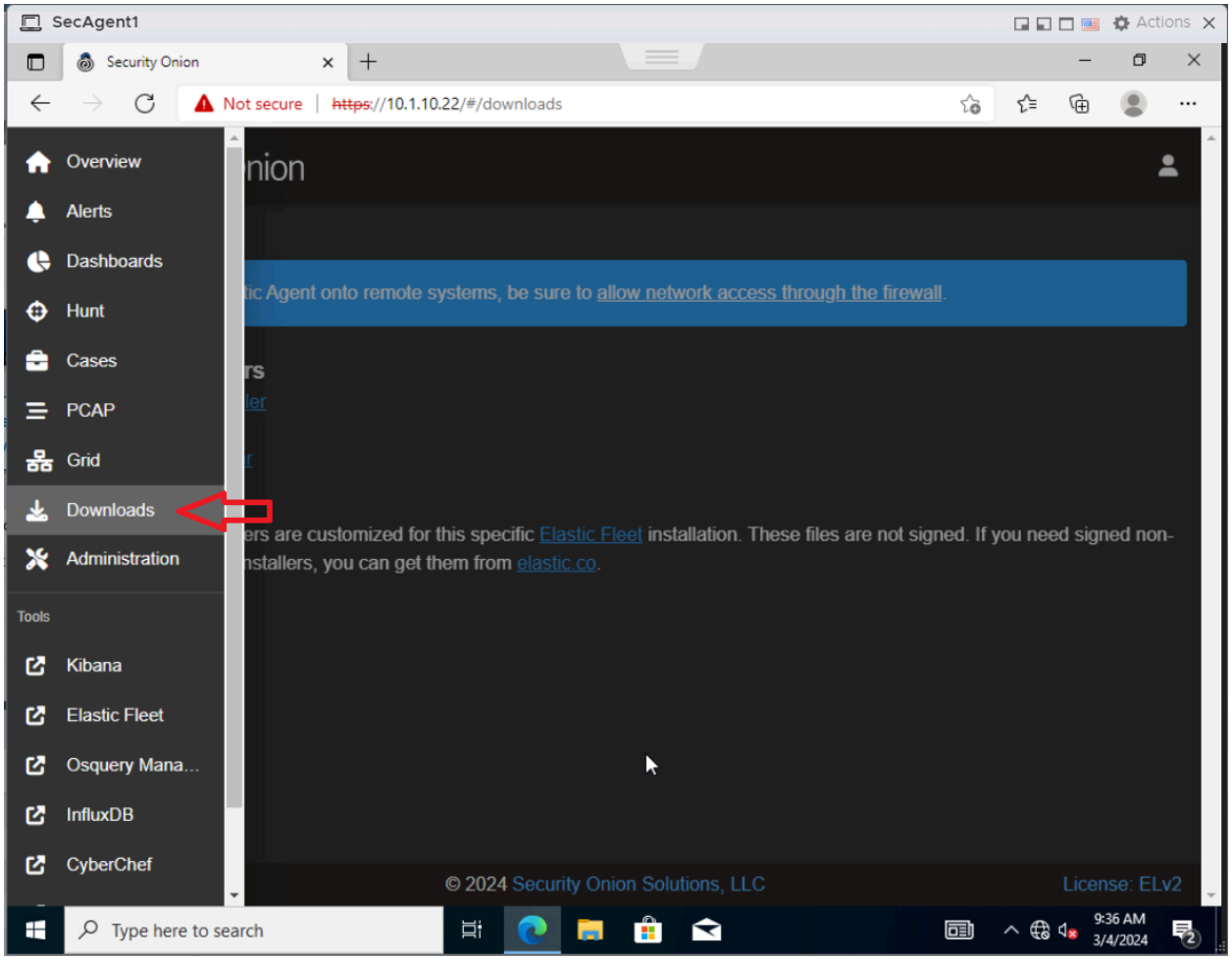


- Restart agent VMs

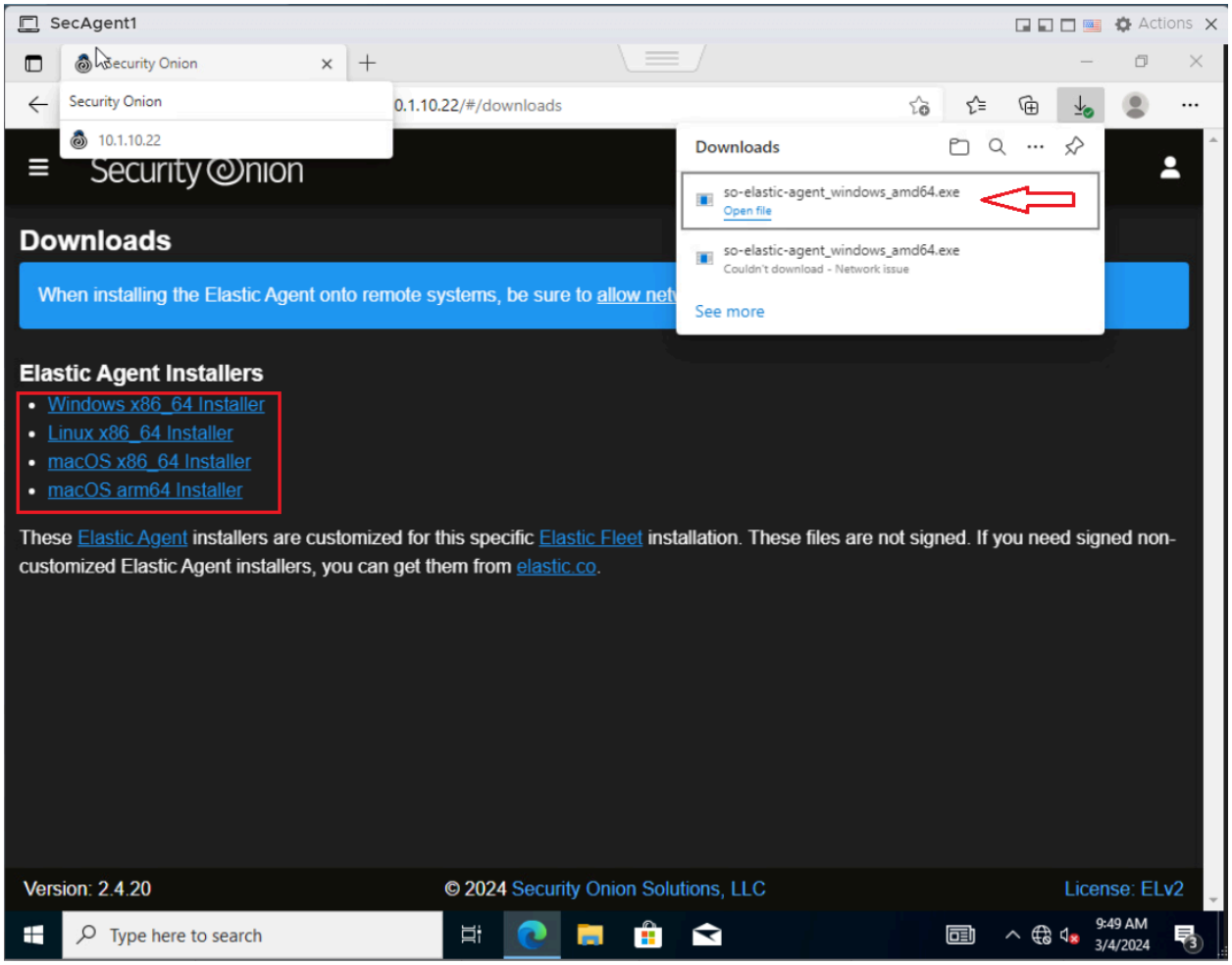
For Shop/Testing use:

- On VM, open a web browser and navigate to SecOnion
  - ➢ If prompted for Microsoft Edge, select ‘complete setup’ and close prompt
- Sign in to SecOnion with soadmin credentials

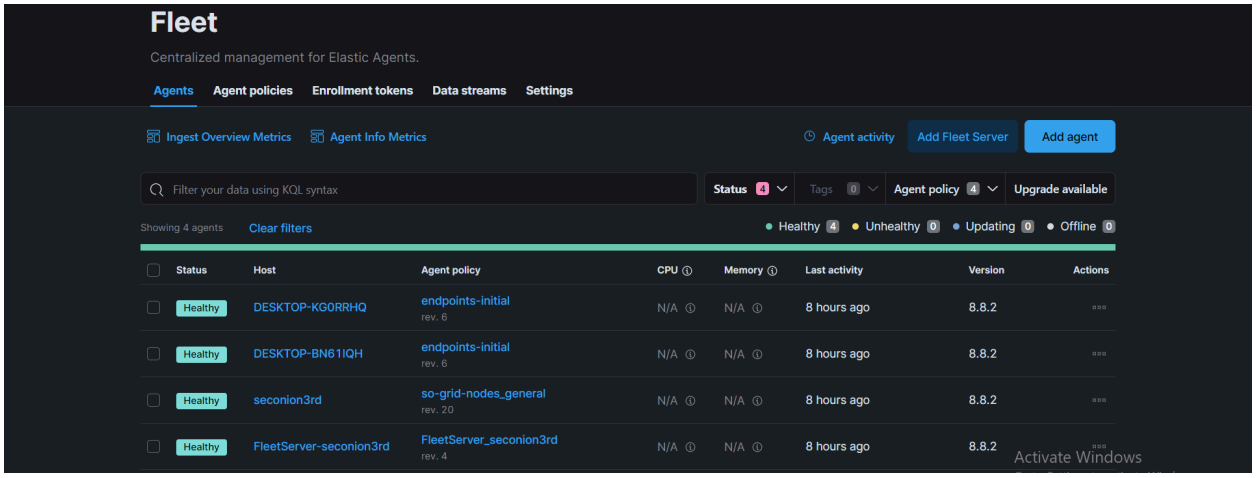
- Navigate to Downloads



- Select ‘Windows x86_64 installer’
  - ➢ Do not open file
  - ➢ If denied for maliciousness, select ‘Keep’ under the download drop down

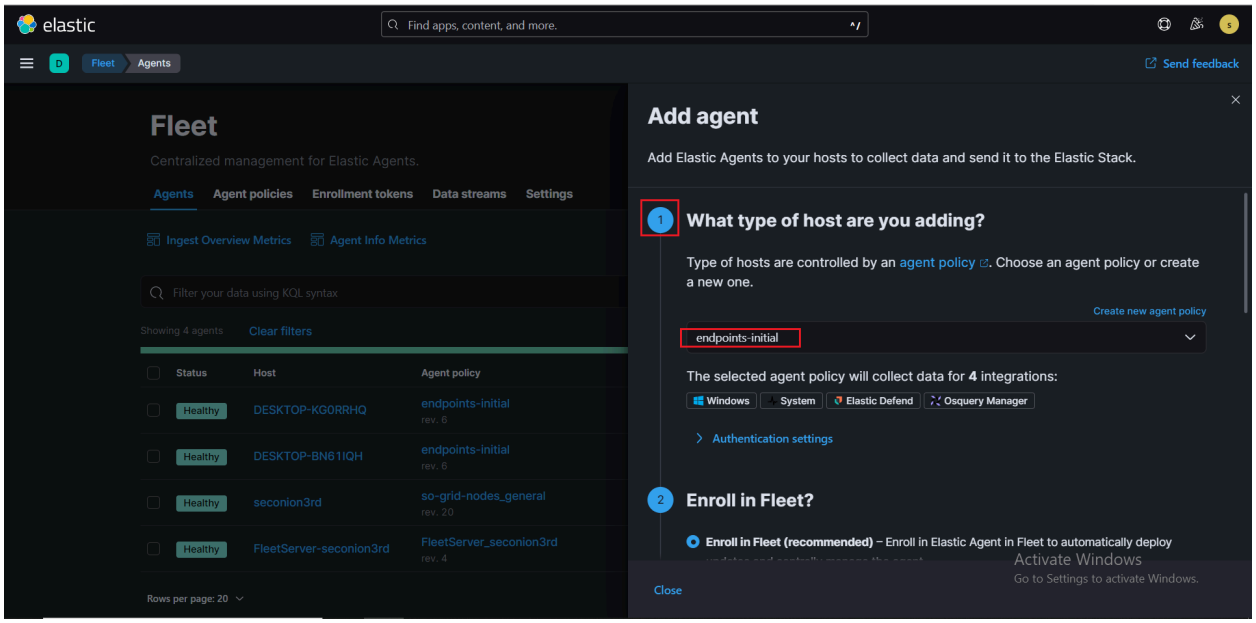


- From File Explorer -> Downloads, run package as Administrator
  - When prompted for changes, select Allow
  - If SmartScreen prompt appears, select ‘Run’
- On workstation, Navigate to Elastic Fleet via Security Onion and verify agent installation

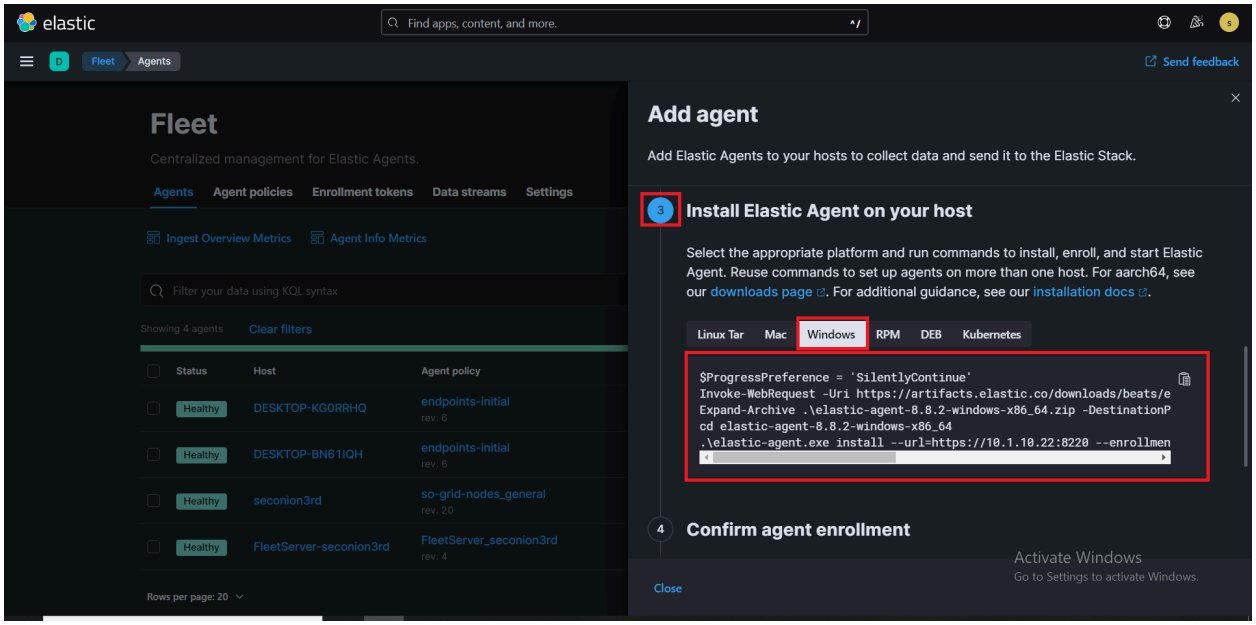


For Customer use:

- On Workstation, navigate to: Security Onion -> Elastic -> Add Agent
- Under ‘1’ Select ‘endpoints-initial’



- Scroll down to ‘3’ and select Windows
- Copy the given script to the clipboard



- Open 2 notepad files -> Named *pulldown.ps1* and *customerdeployment* -> Save to Desktop -> SecOnion_Deployment
- Paste into the first file (pulldown.ps1)
- Cut from ‘cd elastic’ to ‘--enrollment-token=[enrollment-token]==’
- Paste into second file (customerdeployment)
- On *pulldown.ps1*:
  - Between ‘http://’ and ‘artifacts’, insert ‘[seconion_ip]:8443/’
- On *customerdeployment:*
  - Insert ‘--insecure’ before ‘--url=https**:[customer_ip]**’
  - ***Note:*** Enrollment token must match the running version of Security Onion. Each Security Onion instance will create its own unique token.

pulldown.ps1 - Notepad

File Edit Format View Help

```
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri http://10.1.10.22:8443/artifacts/beats/elastic-agent/elastic-agent-8.8.2-windows-x86_64.zip -OutFile elastic-agent-8.8.2-windows-x86_64.zip
Expand-Archive .\elastic-agent-8.8.2-windows-x86_64.zip -DestinationPath .
```

customerdeployment - Notepad

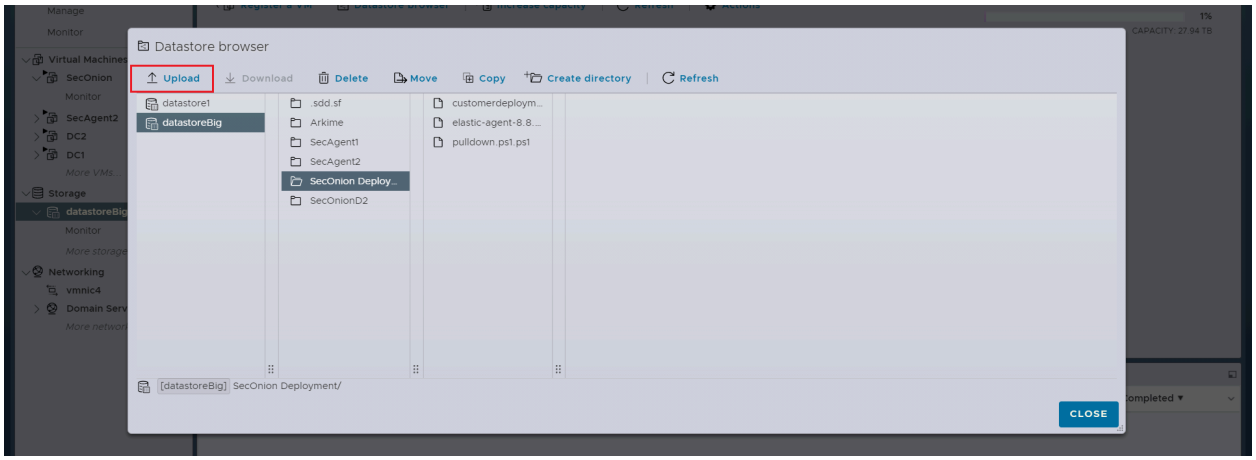
File Edit Format View Help

```
cd elastic-agent-8.8.2-windows-x86_64
.\elastic-agent.exe install --insecure --url=https://10.1.10.22:8220 --enrollment-token=VkxUcmhJMEJnY21CSnp1VnBBbzE6NU5mVTg3cHVRcUdsMjRwQkJEd3RmUQ==
```

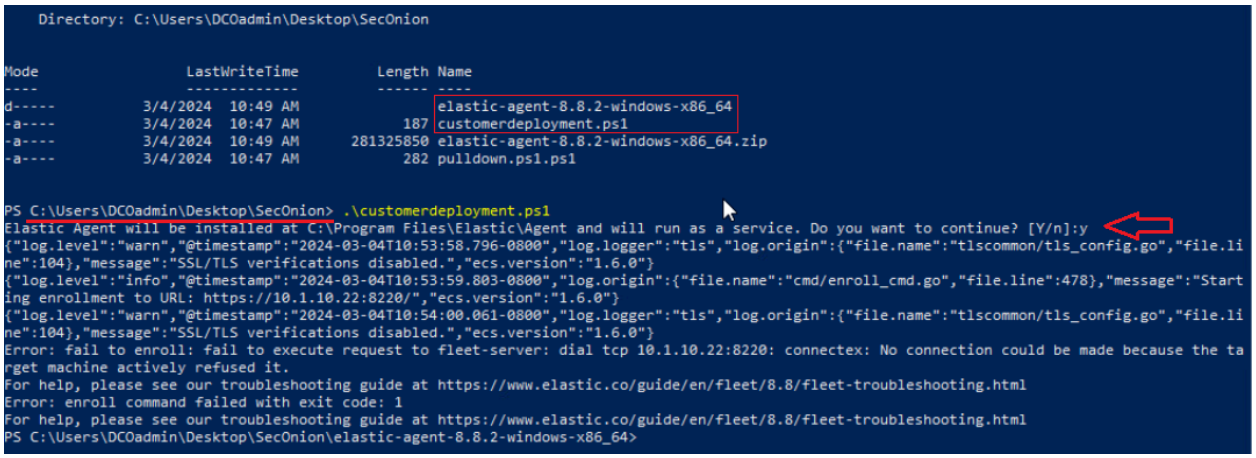
- On Workstation, Run Powershell as administrator
  - Cd C:\Desktop\SecOnion_Deployment
  - Set-ExecutionPolicy Bypass
  - .\pulldown.ps1
  - **Note:** running this script will produce two files, one zipped and one unzipped

```
Set-ExecutionPolicy bypass
.\pulldown.ps1
```

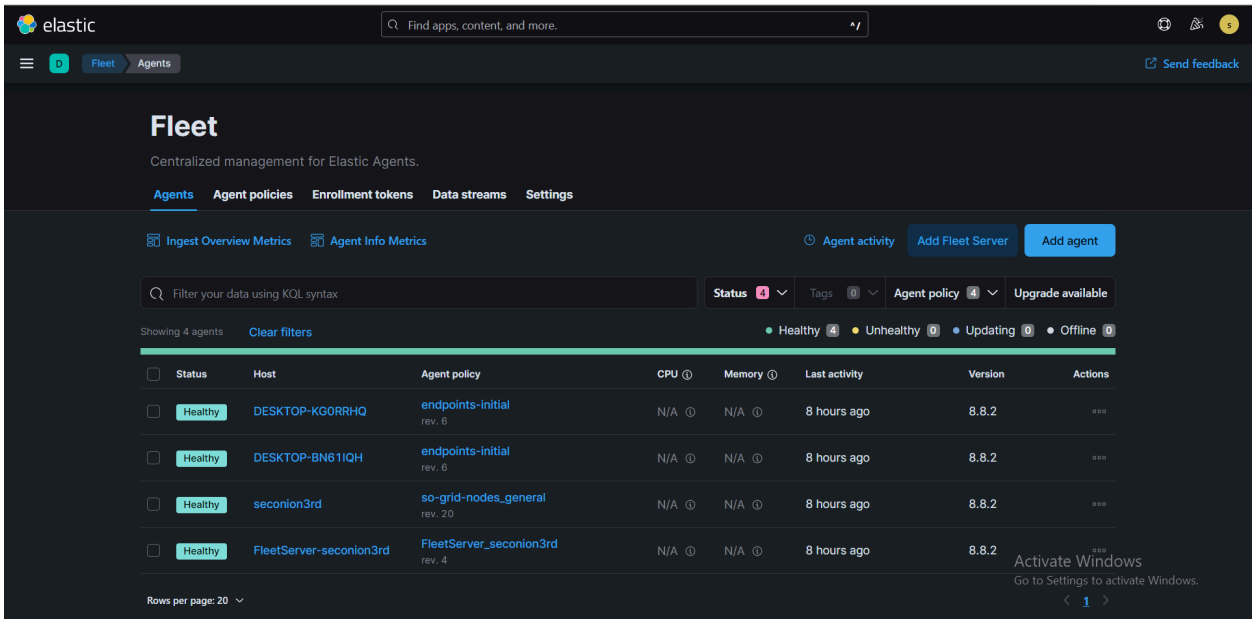
- On ESXI, add *customerdeployment* and both produced files to the datastore



- On VM, open a Web Browser and navigate to ESXI
  - Download both files from the datastore to Desktop\SecOnion
  - Run Powershell as administrator
  - Set-ExecutionPolicy Bypass
  - .\customerdeployment
    - When prompted to continue, enter y for yes



- On Workstation, navigate to Elastic Fleet via Security Onion and verify agent installation

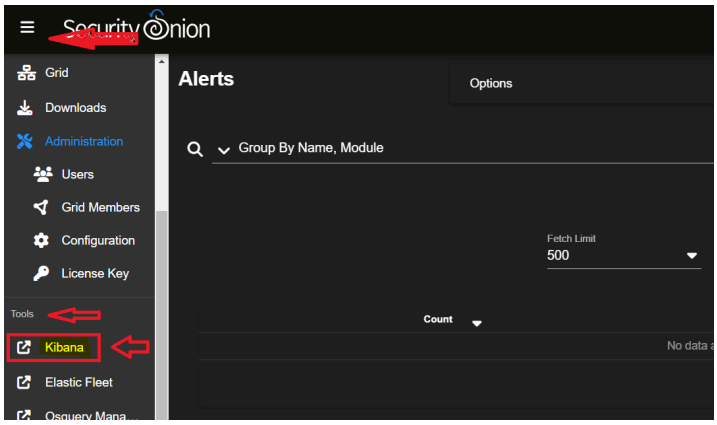


NOTE
in the powershell script the ip address of your elastic host needs to be changed to the external ip address of your firewall (if you are re-creating the elastic_package at anytime)

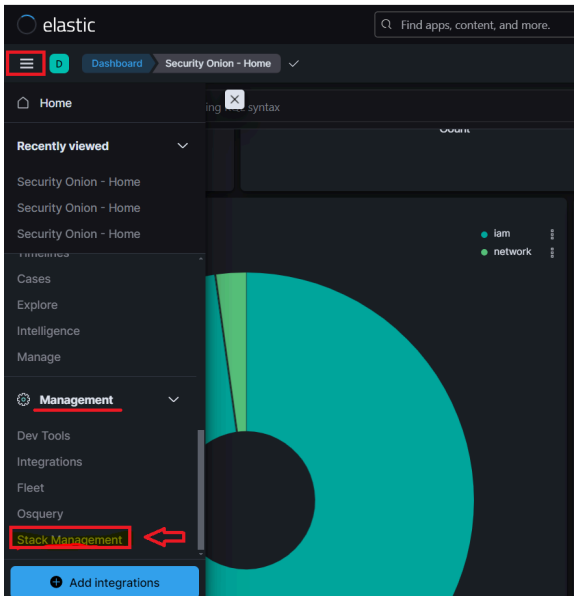
Enabling Alerts in Elastic

In the security tab in Kibana there is a link for alerts. In this page you will be able to manage the rules that trigger and alert. Enable all of the rules to alert that has an integration capable of triggering that rule.

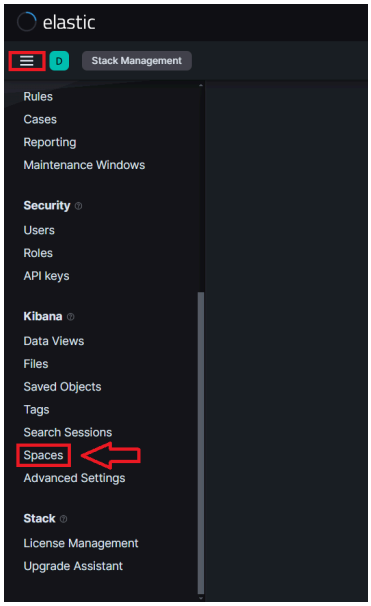
- Navigate to Security Onion. Under Tools, select Kibana.



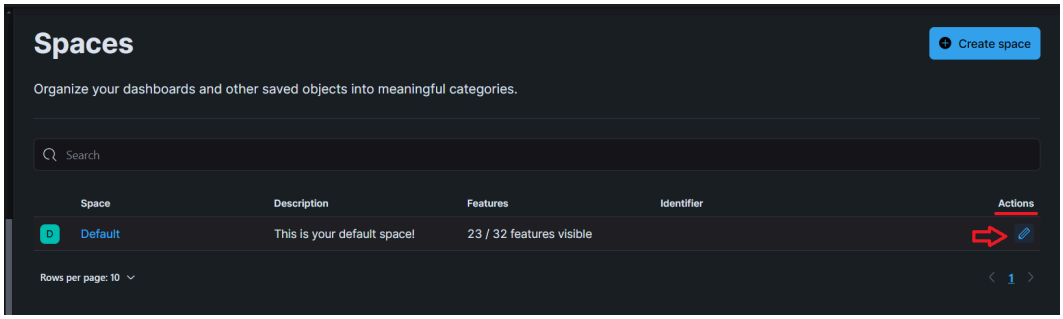
- Navigate to Management and select Stack Management.



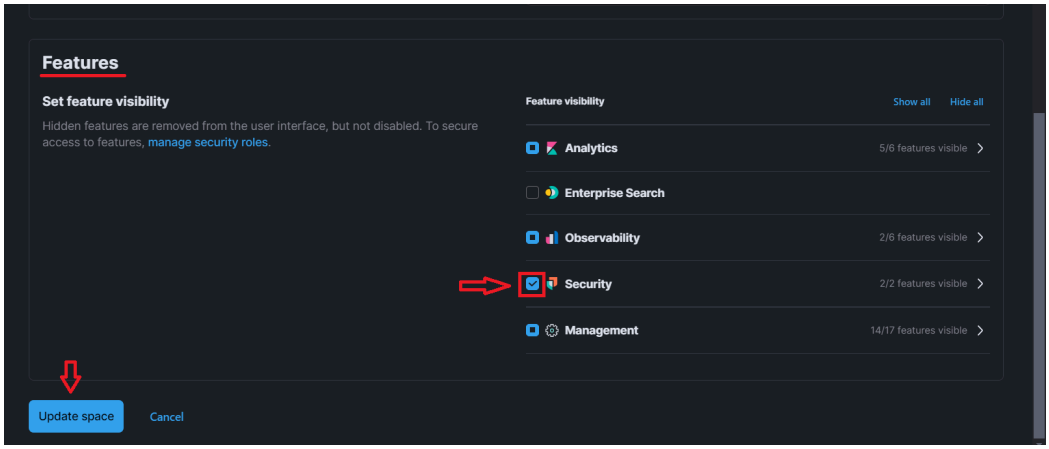
- In the drop down on the left, scroll down and select Spaces.



❖ Select ‘Edit’ (pencil icon) under Actions.



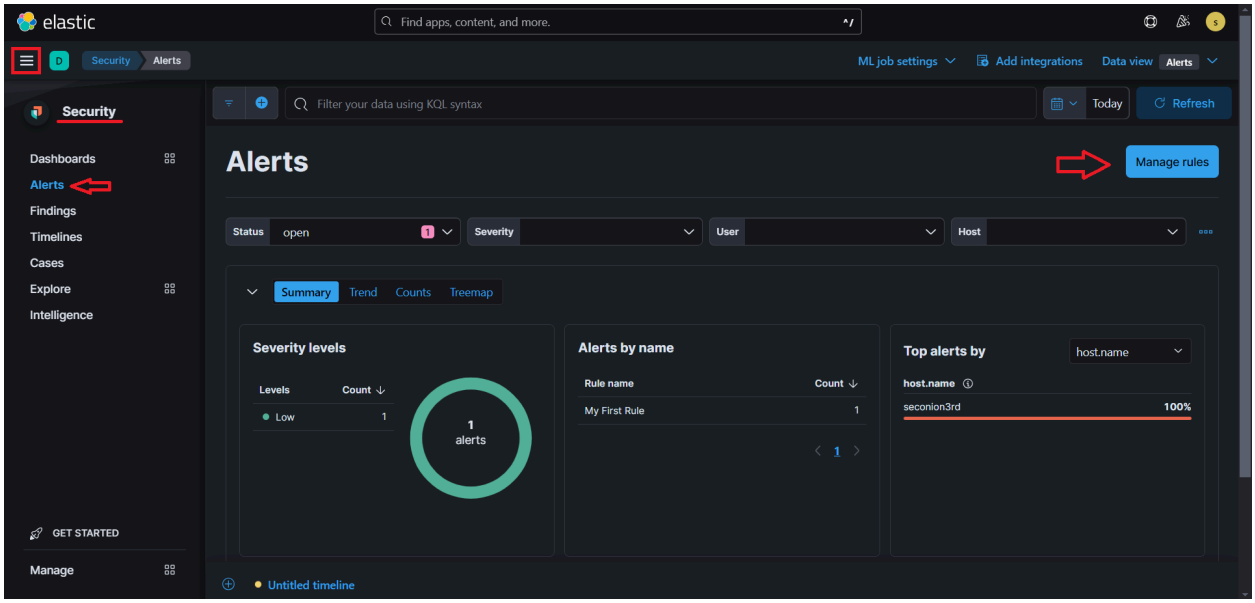
❖ Navigate to Features and checkmark Security



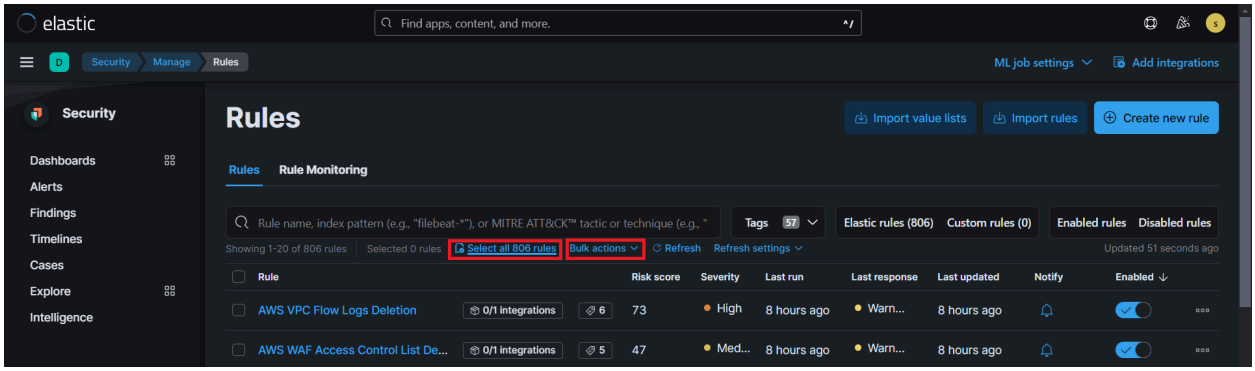
- Update Space and confirm.

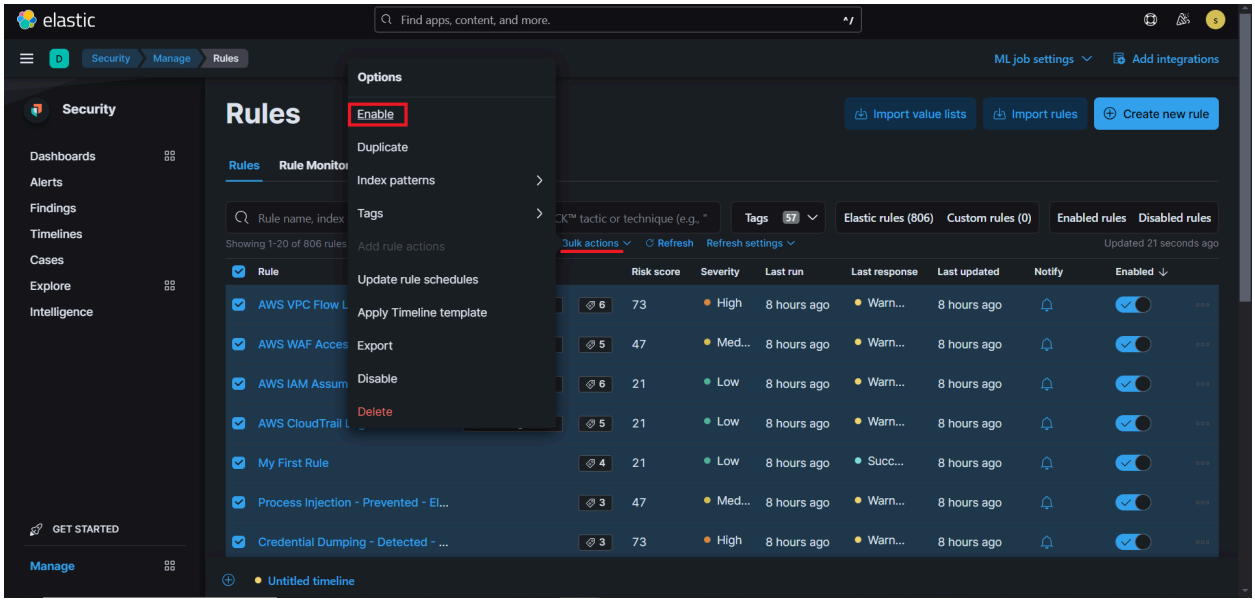
- Open a second Kibana tab from Security Onion.
- Navigate to Security and select Alerts.

- Select Manage Rules.



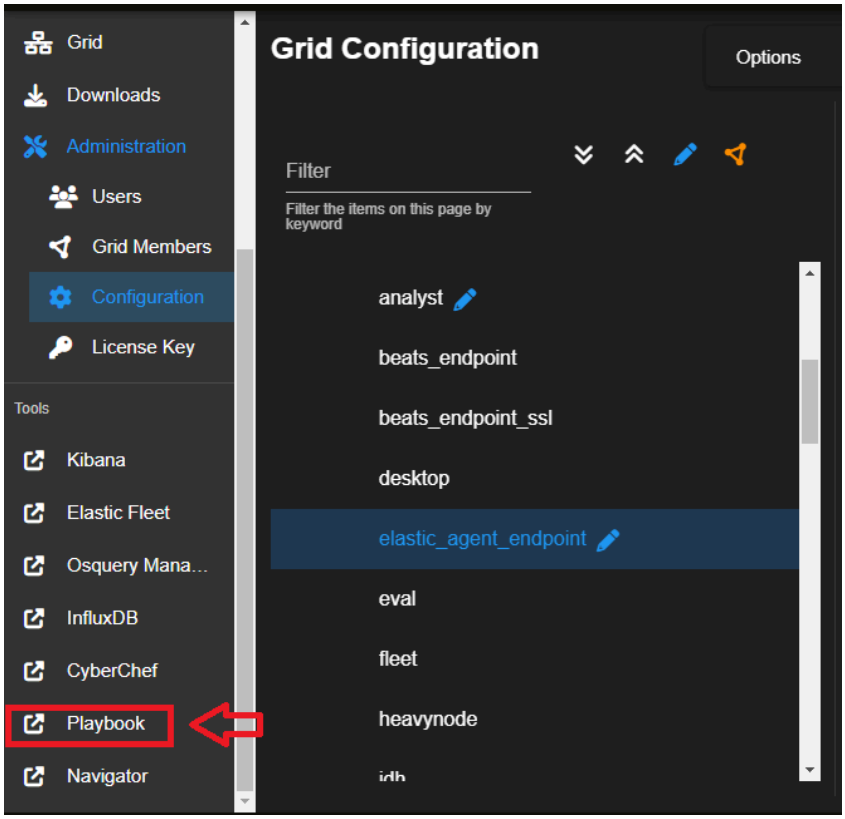
- Load prebuilt rules
- Click on Select All [#] rules
  - Select Bulk Actions and click enable from the pop up.
  - *after it loads there should be 47 rules that have errors, this is normal*



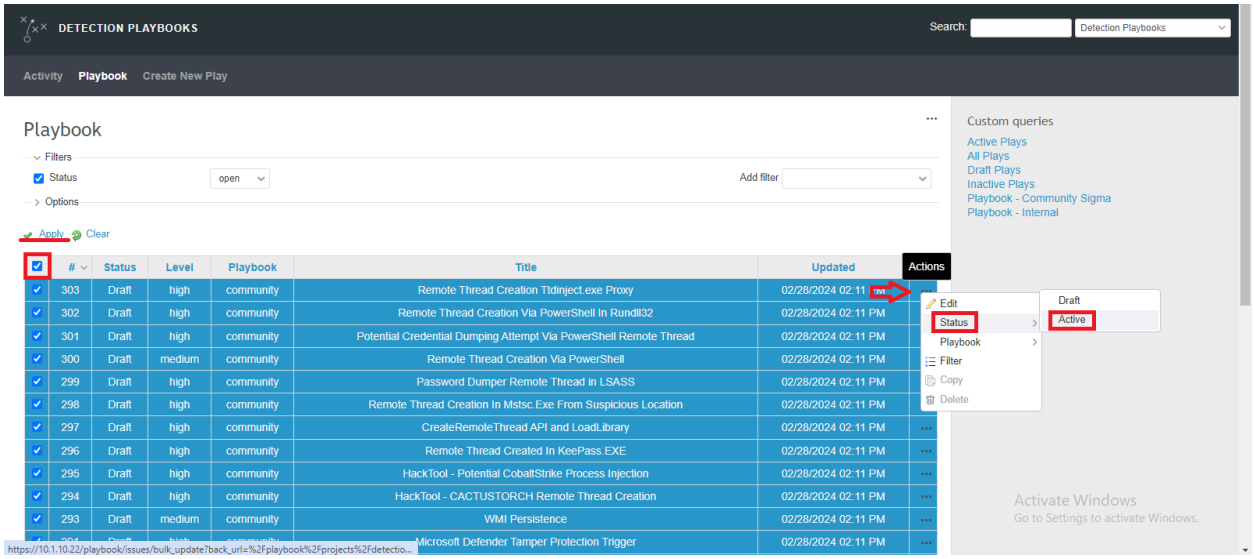


Enabling Playbook Alerts in Security Onion

- From the security onion homepage navigate to the Playbook link on the left hand side of the page



- Once you are in the detection playbook, select the “select all box” at top of chart.
- Click on 3 dots under “Actions” to set “Status” to “Active”.
  - *A few will stay as Draft status which is normal*



It will bring you to a new tab for the play book. From here you are going to click on “All Plays” and select all of them that you can on the page. Then click the three dots and select “active” and will enable all of those rules. Yes you have to manually do this for each page of alerts and it is tedious.

Adding Integrations

In the elastic stack within security onion you can add integrations to your elastic endpoint agent dynamically without having to reinstall the endpoint on each device after adding the integration.

To access the integrations page you will navigate to Kibana, then on the left hand side scroll all the way down and click on the integrations link. This will bring you the page with all of the integrations that are available to add.

Security Onion Baselining

Initial baselines give a control point as a reference. Comparing and knowing what normal logs and/or traffic look like is necessary to finding malicious traffic

- Collecting live OS-Queries
  - security onion application -> tools (bottom left corner) -> OS-query Manager
  - OS-query Manager -> new live query -> input platform and pack you want to run
  - Add to case (clipboard) -> create case -> name the case based on query being ran -> add a brief description ->create description

There are pre-loaded packs that will pull various os information on selected agents, the baseline will give a control sample on what the network looks like prior to any adversary action.

- View created cases
  - go to https://10.x.x.x(Security Onion IP)/kibana/app/observability/cases

Once malicious activity has been detected within the network, these cases can be monitored for detection alerts.