



# 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.*

---

<b>Overview</b> .....	<b>2</b>
<b>Tools and Capabilities</b> .....	<b>4</b>
<b>Architecture</b> .....	<b>5</b>
Standalone.....	5
Distributed.....	6
<b>Security Onion Installation</b> .....	<b>7</b>
Troubleshooting SecOnion Browser: ERR_SSL_Key.....	22
<b>Configuring the Security Onion Firewall</b> .....	<b>23</b>
Deploying the Elastic Agent.....	25
For Shop/Testing use:.....	26
For Customer use:.....	26
Enabling Alerts in Elastic.....	28
Enabling Playbook Alerts in Security Onion.....	31
Adding Integrations.....	32
<b>Security Onion Baselineing</b> .....	<b>33</b>

---



## 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.

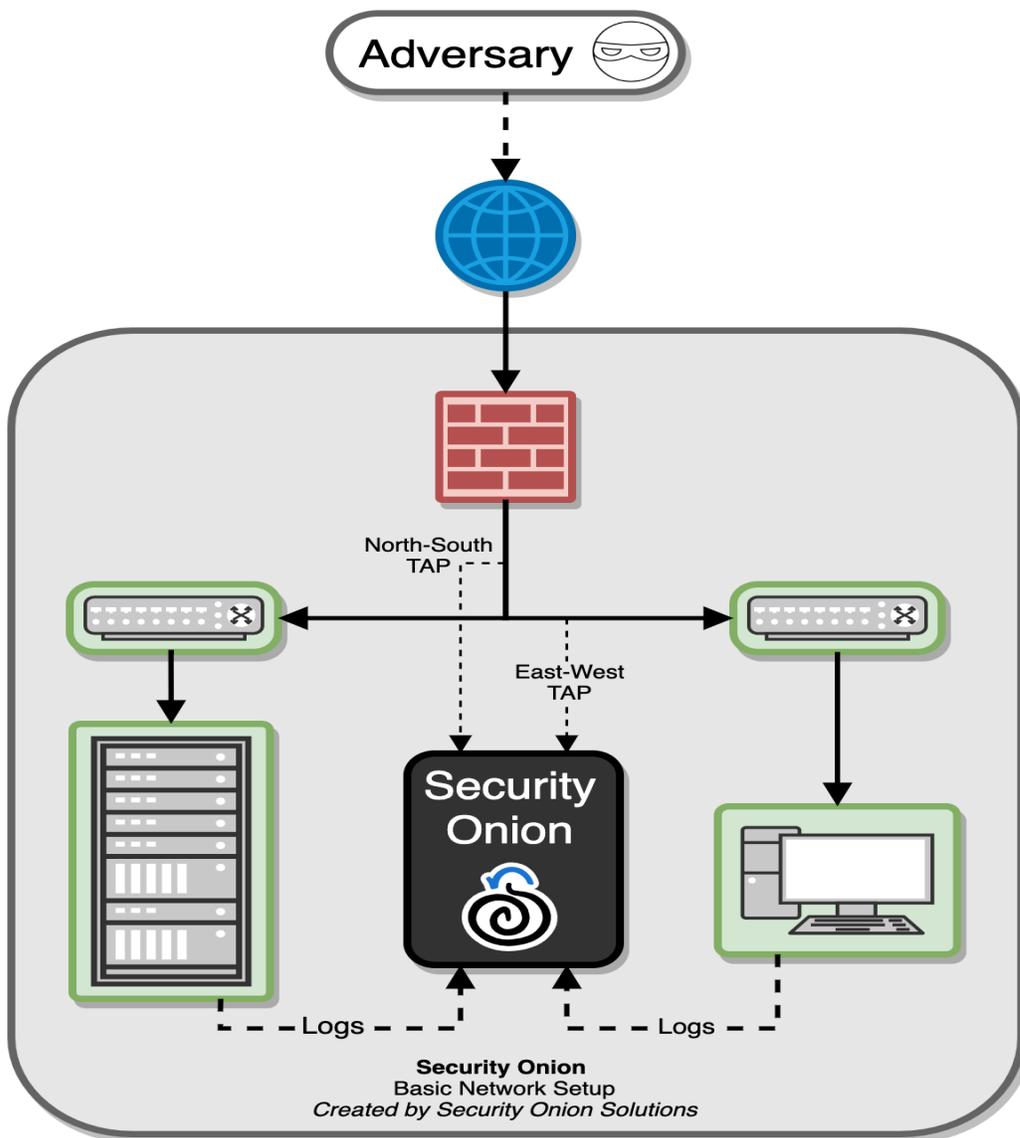
The “Downloads” tab on the homepage of the website redirects to a Github portal containing the most current version of the SO .ISO file (Version 2.4 at the time this guide was written).

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](https://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

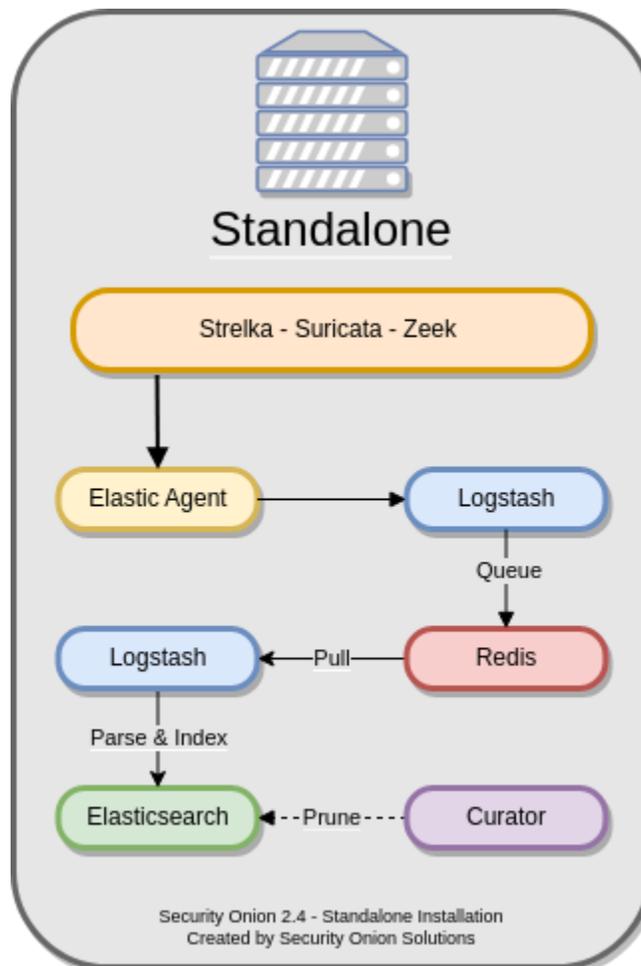
**OpenCanary** - Intrusion detection honeypots



# Architecture

## Standalone

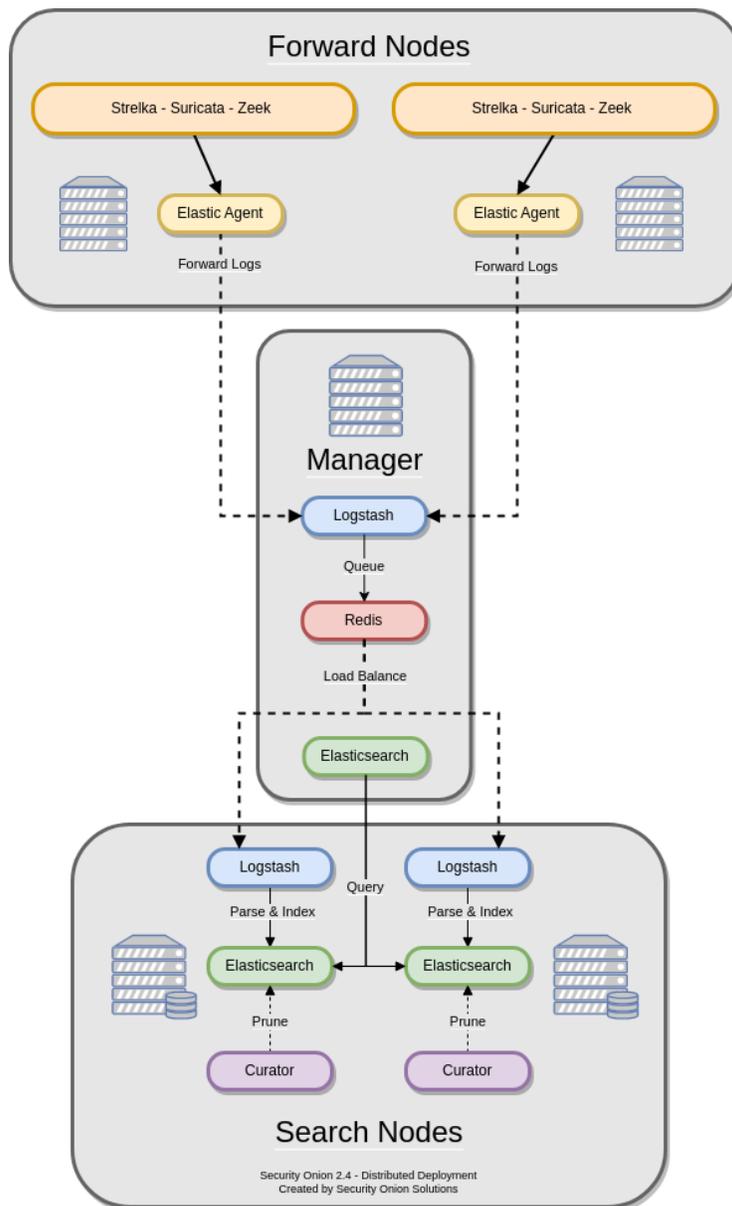
Standalone runs all components on one box. However, instead of Elastic agents sending logs directly to Elasticsearch, it sends them to Logstash, which sends them to Redis for queuing. A second logstash pipeline pulls the logs out of Redis and sends them to Elasticsearch, where they are parsed and indexed. 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

The screenshot shows the VMware vSphere 'New virtual machine' wizard. The title bar reads 'New virtual machine'. On the left, a progress indicator shows five steps: 1. Select creation type (highlighted with a green checkmark), 2. Select a name and guest OS, 3. Select storage, 4. Customize settings, and 5. Ready to complete. The main content area is titled 'Select creation type' and asks 'How would you like to create a Virtual Machine?'. There are two radio button options: 'Create a new virtual machine' (selected) and 'Deploy a virtual machine from an OVF or OVA file'. Below the 'Create a new virtual machine' option, there are two sub-options: 'Deploy a virtual machine from an OVF or OVA file' and 'Register an existing virtual machine'. To the right of these options, a text box explains: 'This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.' At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'. The VMware logo is visible in the bottom left corner of the wizard window.

## Step 2:

Name: SecOnion

Compatibility: ESXi 7.0 U2 Virtual Machine

Guest OS Family: Linux

Guest OS Version: Oracle 9

The screenshot shows the VMware vSphere 'New virtual machine' wizard at Step 2: 'Select a name and guest OS'. The title bar reads 'New virtual machine - SecOnion (ESXi 7.0 U2 virtual machine)'. The progress indicator on the left shows step 2 highlighted with a green checkmark. The main content area is titled 'Select a name and guest OS' and asks 'Specify a unique name and OS'. There is a text input field for 'Name' containing 'SecOnion'. Below this, a note states: 'Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.' Another note says: 'Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.' There are three dropdown menus: 'Compatibility' set to 'ESXi 7.0 U2 virtual machine', 'Guest OS family' set to 'Linux', and 'Guest OS version' set to 'Oracle Linux 9 (64-bit)'. At the bottom right, there are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'. The VMware logo is visible in the bottom left corner of the wizard window.



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”

Device	Configuration	Connect	Remove
CPU	10		
Memory	120 GB		
Hard disk 1	2.5 TB		
SCSI Controller 0	VMware Paravirtual		
SATA Controller 0			
USB controller 1	USB 2.0		
Network Adapter 1	Domain Services	<input checked="" type="checkbox"/>	
New Network Adapter	Sniffing	<input checked="" type="checkbox"/>	
CD/DVD Drive 1	Datastore ISO file	<input checked="" type="checkbox"/>	

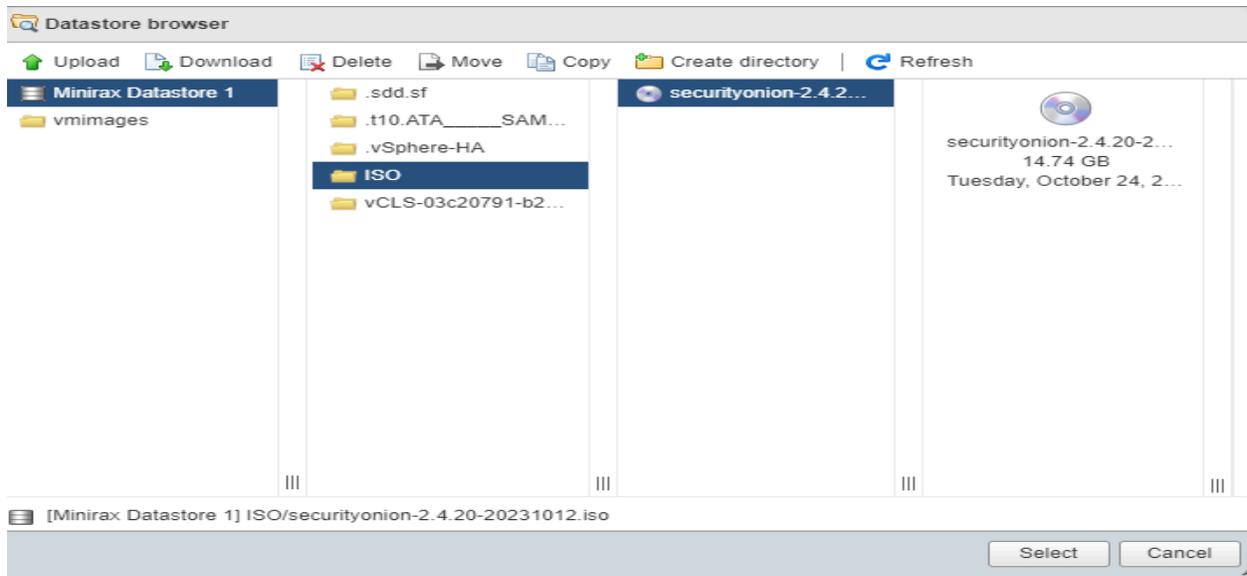


Step 4:

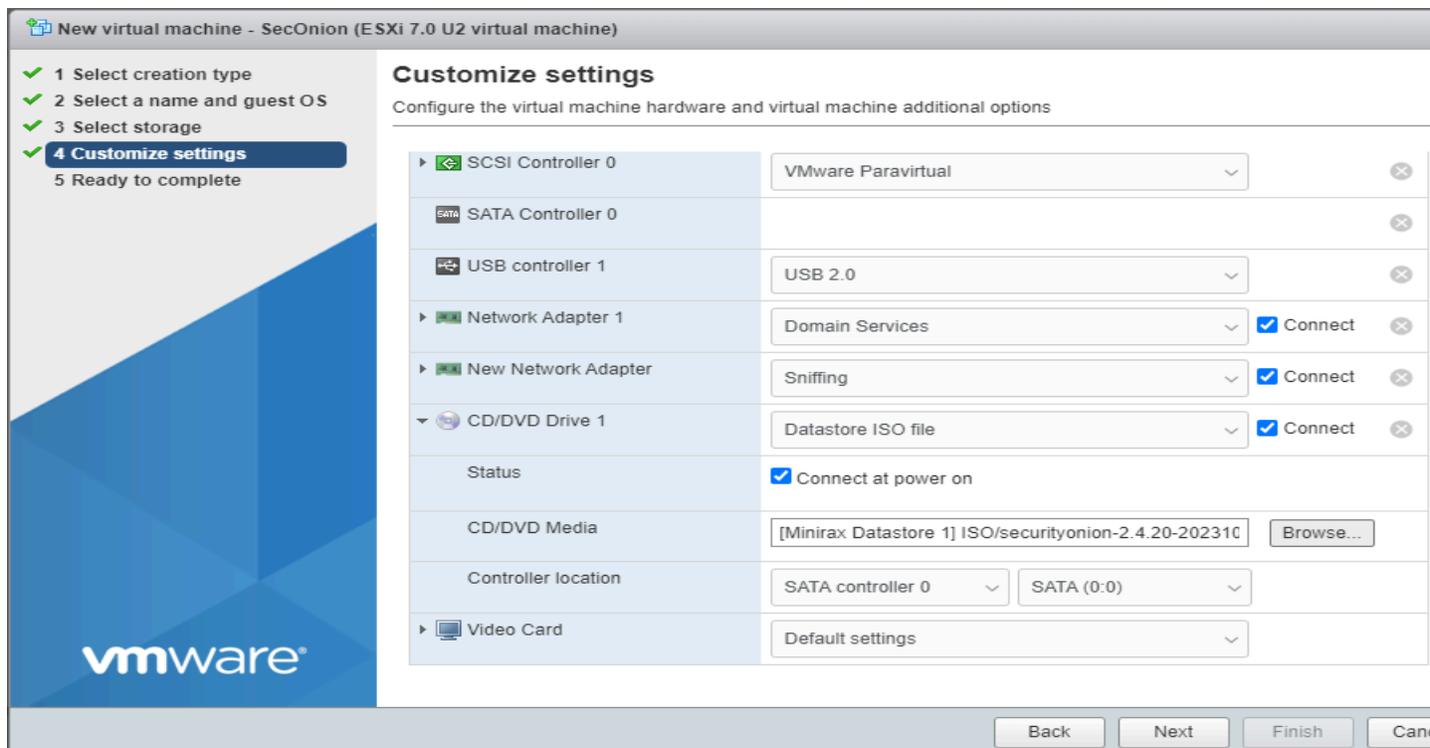
Select CD/DVD Drive dropdown

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

**New virtual machine - SecOnion (ESXi 7.0 U2 virtual machine)**

- 1 Select creation type
- 2 Select a name and guest OS
- 3 Select storage
- 4 Customize settings
- 5 Ready to complete

Property	Value
Name	SecOnion
Datastore	Minirax Datastore 1
Guest OS name	Oracle Linux 9 (64-bit)
Compatibility	ESXi 7.0 U2 virtual machine
vCPUs	10
Memory	120 GB
Network adapters	2
Network adapter 1 network	Domain Services
Network adapter 1 type	VMXNET 3
Network adapter 2 network	Sniffing
Network adapter 2 type	VMXNET 3
IDE controller 0	IDE 0
IDE controller 1	IDE 1
SCSI controller 0	VMware Paravirtual
SATA controller 0	New SATA controller
Hard disk 1	
Capacity	2.5TB
Datastore	[Minirax Datastore 1] SecOnion/
Mode	Dependent

Buttons: Back, Next, Finish, Cancel

Step 7:  
Click Finish

**Provisioning**: Thick provisioned, lazily zeroed

**Controller**: SCSI controller 0 : 0

**CD/DVD drive 1**

**Backing**: [Minirax Datastore 1] ISO/securityonion-2.4.20-20231012.iso

**Connected**: Yes

**USB controller 1**: USB 2.0

Buttons: Back, Next, Finish, Cancel

Virtual machine SecOnion was successfully created - dismiss

Virtual machine	Status	Used space	Guest OS	Host name	Host CPU	Host memory
vCLS-03c20701-4297-4c34-95a7-c52bad4e3ab	Normal	484.01 MB	Other 3.x or later Linux (64-bit)	None	5 MHz	157 MB
SecOnion	Normal	0 B	Oracle Linux 9 (64-bit)	Unknown	0 MHz	0 MB

Quick filters: 2 items

**Complete!!!**

Task	Target	Initiator	Queued	Started	Result	Completed
Destroy	SecOnion	root	10/25/2023 07:10:14	10/25/2023 07:10:14	Completed successfully	10/25/2023 07:10:14
Shutdown Guest	SecOnion	root	10/25/2023 07:10:01	10/25/2023 07:10:01	Completed successfully	10/25/2023 07:10:02
Create VM	SecOnion	root	10/25/2023 07:28:22	10/25/2023 07:28:22	Completed successfully	10/25/2023 07:28:23

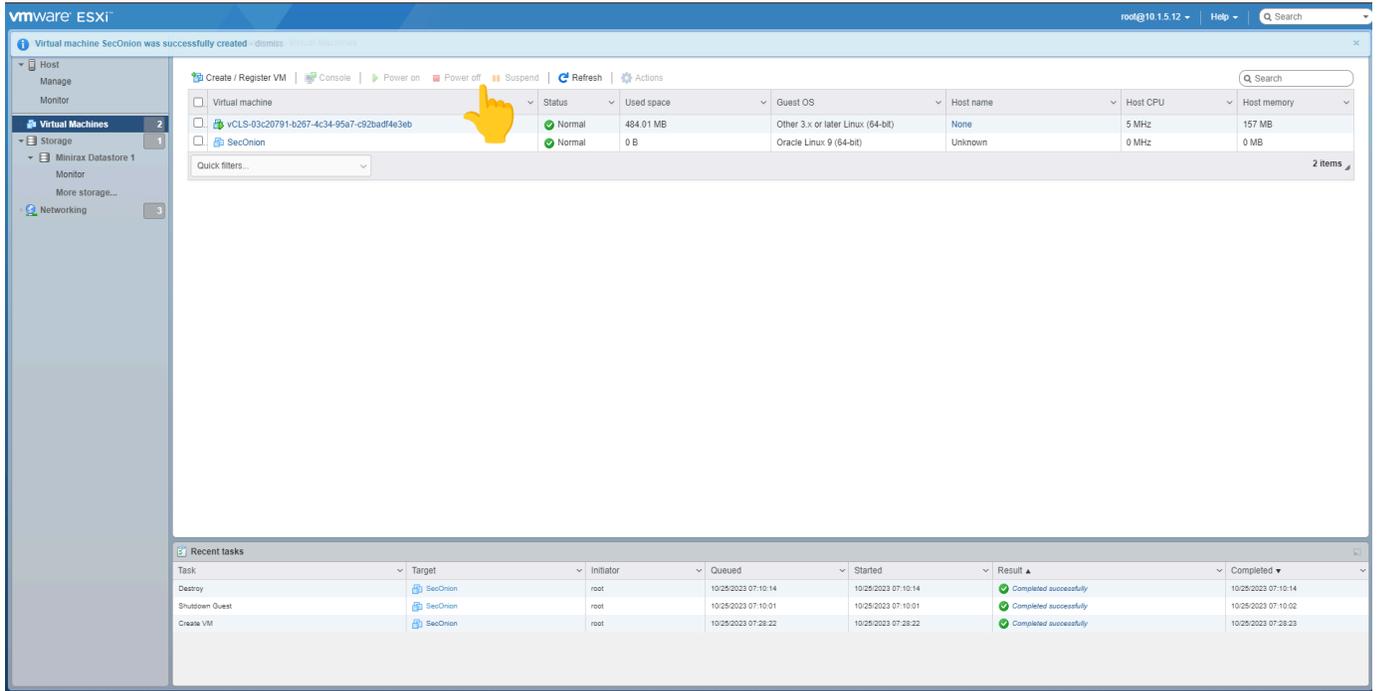


# Security Onion Configuration

Step 1:

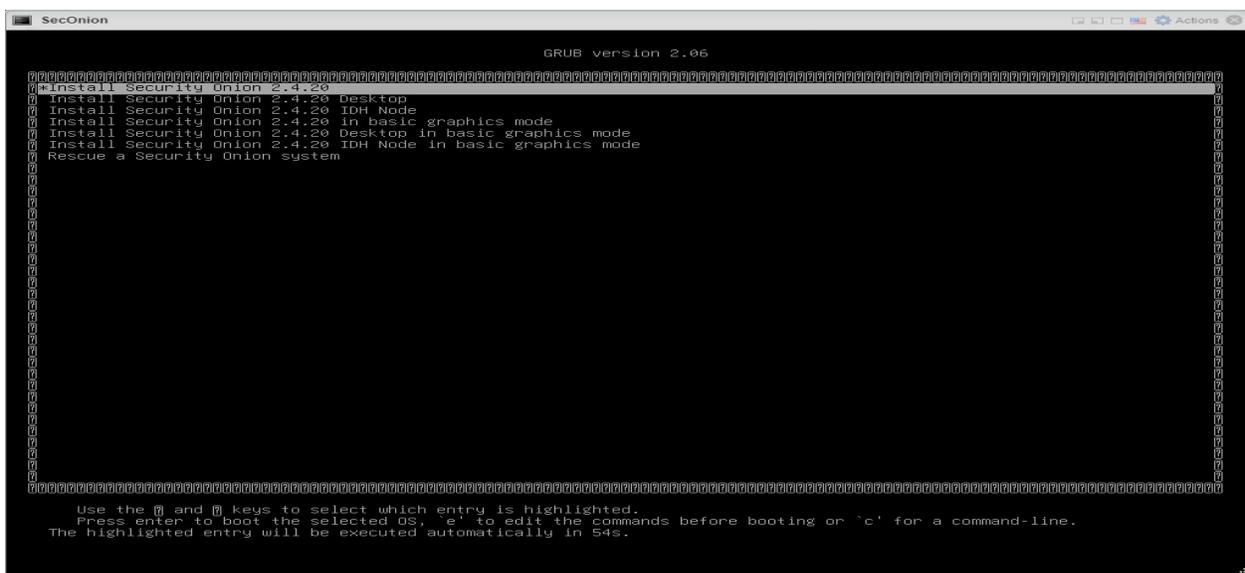
Power On Virtual Machine “Security Onion”

-Click Power On



Step 2:

Select “Install Security Onion”





Step 3:  
Select "Yes" to proceed  
Hit Enter on keyboard

```
SecOnion
#####
##          ** 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.) _
```

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

```
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 Security Onion.
Enter an administrative username: soadmin
```

Step 5:  
set password to standard  
Re-Enter Password

```
Let's set a password for the soadmin user:
Enter a password:
```

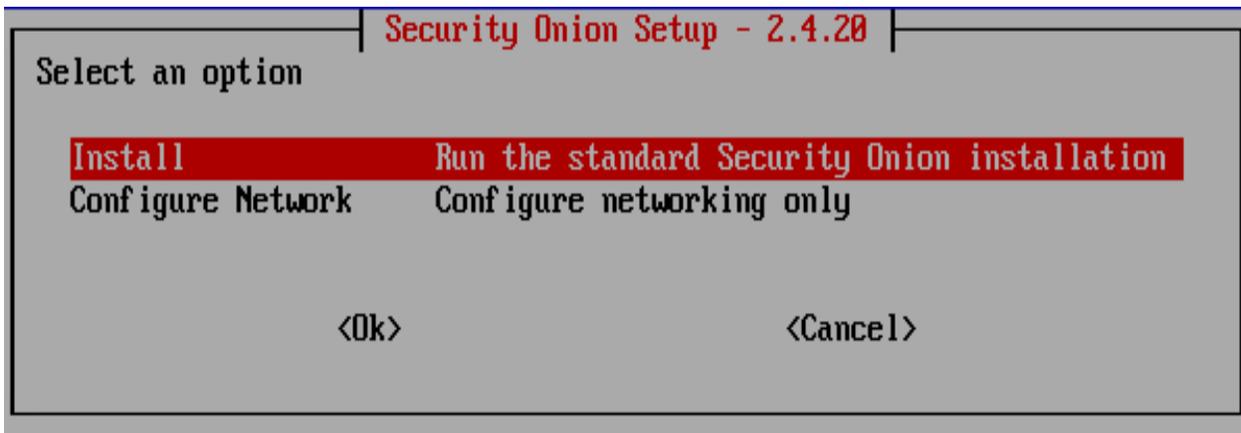
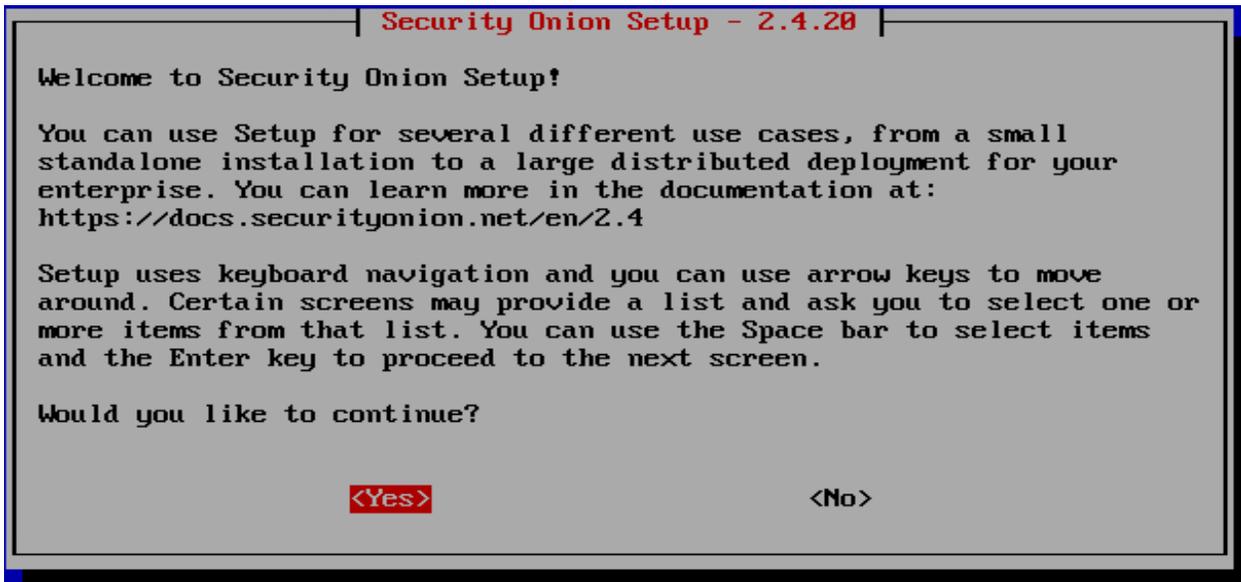
Step 6:  
Hit the enter key  
Wait for installation to begin  
**Takes a long time**  
Hit the enter key to reboot

Step 7:  
Login



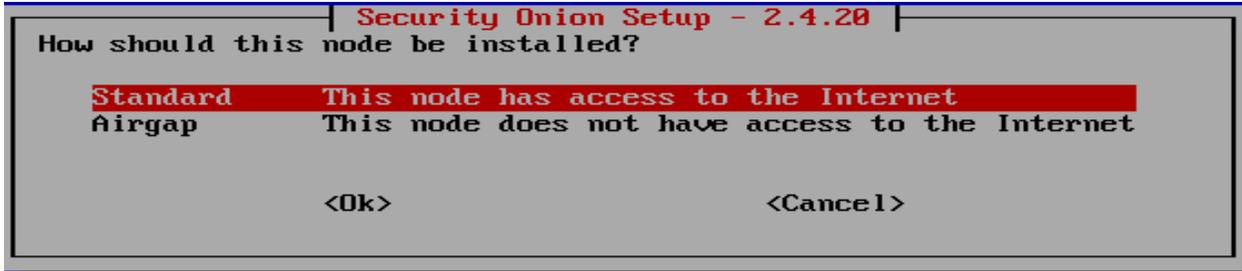
```
Oracle Linux Server 9.2
Kernel 5.15.0-105.125.6.2.2.el9uek.x86_64 on an x86_64
localhost login: _
```

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

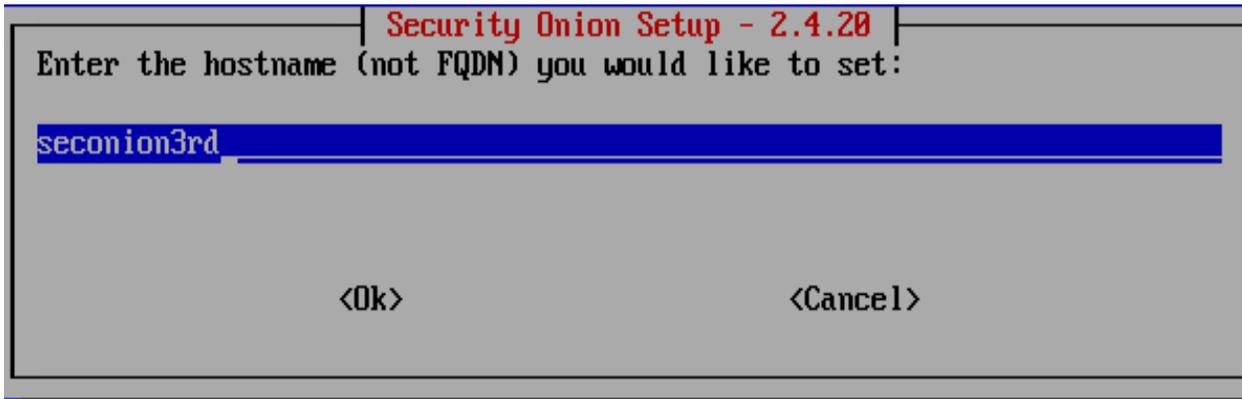


Step 9:  
\*This is now considered the beginning of the configuration of Security Onion\*  
Select the type of installation you would like to do  
Standalone for this instance

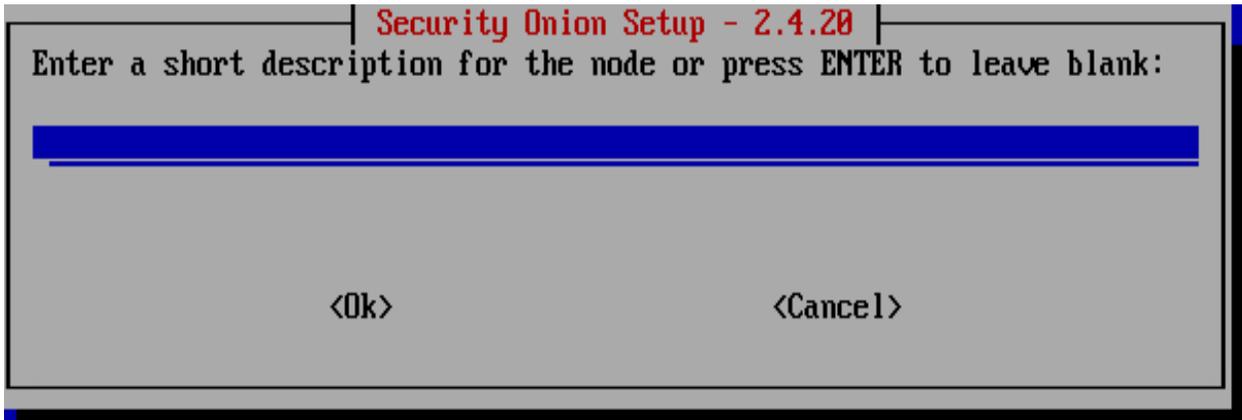




Step 12:  
Enter Hostname:  
" Seconion3rd "  
Press the Enter Key



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



```
Security Onion Setup - 2.4.20
Please select the NIC you would like to use for management.

ens192 00:0c:29:a1:62:32 Link UP
ens224 00:0c:29:a1:62:3c Link UP
```

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

```
Security Onion Setup - 2.4.20
Choose how to set up your management interface:

STATIC Set a static IPv4 address
DHCP Use DHCP to configure the Management Interface
```

```
Security Onion Setup - 2.4.20
What IPv4 address would you like to assign to this
Security Onion installation?

Please enter the IPv4 address with CIDR mask
(e.g. 192.168.1.2/24):

10.1.10.22/24

<Ok> <Cancel>
```



Step 16

Gateway IPv4 address:

10.1.10.1

A screenshot of a terminal window titled "Security Onion Setup - 2.4.20". The prompt is "Enter your gateway's IPv4 address:". The input field contains "10.1.10.1". At the bottom, there are two buttons: "<Ok>" and "<Cancel>".

```
Security Onion Setup - 2.4.20
Enter your gateway's IPv4 address:
10.1.10.1
<Ok> <Cancel>
```

Step 17:

Enter your DNS servers separated by commas. 10.1.10.14,10.1.10.15

A screenshot of a terminal window titled "Security Onion Setup - 2.4.20". The prompt is "Enter your DNS servers separated by commas:". The input field contains "10.1.10.14,10.1.10.15". At the bottom, there are two buttons: "<Ok>" and "<Cancel>".

```
Security Onion Setup - 2.4.20
Enter your DNS servers separated by commas:
10.1.10.14,10.1.10.15
<Ok> <Cancel>
```

Step 18:

Enter your dns search domain : 3rdplt.dco.mil

(editor's note: use direct after step 18)

A screenshot of a terminal window titled "Security Onion Setup - 2.4.20". The prompt is "Enter your DNS search domain:". The input field contains "3rdplt.dco.mil". At the bottom, there are two buttons: "<Ok>" and "<Cancel>".

```
Security Onion Setup - 2.4.20
Enter your DNS search domain:
3rdplt.dco.mil
<Ok> <Cancel>
```

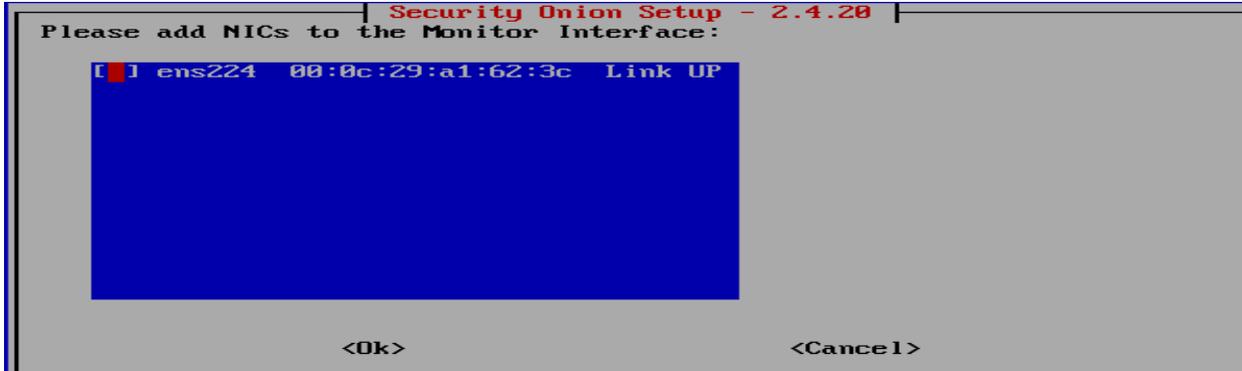
Step 19:

A screenshot of a terminal window titled "Security Onion Setup - 2.4.20". The text reads: "Do you want to keep the default Docker IP range? If you are unsure, please accept the default option of Yes." At the bottom, there are two buttons: "<Yes>" and "<No>".

```
Security Onion Setup - 2.4.20
Do you want to keep the default Docker IP range?
If you are unsure, please accept the default option of Yes.
<Yes> <No>
```

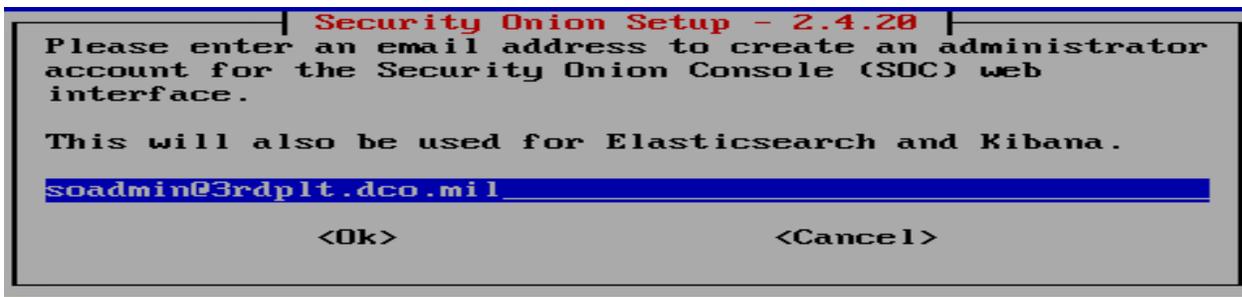
Step 20:

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



```
Security Onion Setup - 2.4.20
How would you like to access the web interface?

Whatever you choose here will be the only way that you can access the
web interface.

If you choose something other than IP address, then you'll need to
ensure that you can resolve the name via DNS or hosts entry. If you are
unsure, please select IP.

IP      Use IP address to access the web interface
HOSTNAME Use hostname to access the web interface
OTHER   Use a different name like a FQDN or Load Balancer

<Ok>                                <Cancel>
```

```
Security Onion Setup - 2.4.20
Do you want to allow access to this Security Onion installation via the
web interface?

<Yes>                                <No>
```

```
Security Onion Setup - 2.4.20
Enter a single IP address or an IP range, in CIDR notation, to allow:
10.1.10.0/24

<Ok>                                <Cancel>
```

Step 24:  
Hit TAB to select yes  
Hit ENTER

```
The following options have been set, would you like to proceed?

Security Onion Version: 2.4.20
Node Type: STANDALONE
Hostname: seconion3rd
Airgap: True
Network: STATIC
Management NIC: ens192
Management IP: 10.1.10.22
Gateway: 10.1.10.1
DNS: 10.1.10.14 10.1.10.15
DNS Domain: 3rdplt.dco.mil
Proxy: N/A
Allowed IP or Subnet: 10.1.10.0/24
Web User: soadmin@3rdplt.dco.mil

Press the Tab key to select yes or no.

<Yes>                                <No>
```



**Security Onion Setup - 2.4.20**

STANDALONE setup is now complete!

Access the Security Onion Console (SOC) web interface by navigating to:  
<https://10.1.10.22>

Then login with the following username and password.

SOC Username: soadmin@3rdplt.dco.mil  
 SOC Password: Use the password that was entered during setup

Press TAB and then the ENTER key to exit this screen.

Hit TAB to select okay

Hit ENTER

Step 25:

ON ESXi

Go to the Networking tab

Under Port Groups

Name	Active ports	VLAN ID	Type	vSwitch	VMs
VM Network	0	0	Standard port group	vSwitch0	0
Management Network	1	4095	Standard port group	vSwitch0	N/A
Domain Services	1	4095	Standard port group	Domain Services	1
Sniffing	1	4095	Standard port group	Sniffing	1

-Virtual Switches

- Select Domain Services

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

Domain Services

Type: Standard vSwitch  
 Port groups: 1  
 Uplinks: 1

**Warning:** This virtual switch has no uplink redundancy. You should add another uplink adapter.

vSwitch Details	
MTU	1500
Ports	3840 (3822 available)
Link-discovery	Listen / Cisco discovery protocol (CDP)
Attached VMs	1 (1 active)
Beacon interval	1

NIC teaming policy	
Notify switches	Yes
Policy	Route based on originating port ID
Reverse policy	Yes
Failback	Yes

Security policy	
Allow promiscuous mode	Yes
Allow forged transmits	Yes
Allow MAC changes	Yes

vSwitch topology

Domain Services  
 VLAN ID: 4095  
 Virtual Machines (1)  
 SecOnion  
 MAC Address 00:0c:29:a1:62:32

Physical adapters  
 vmnic2, 1000 Mbps, Full

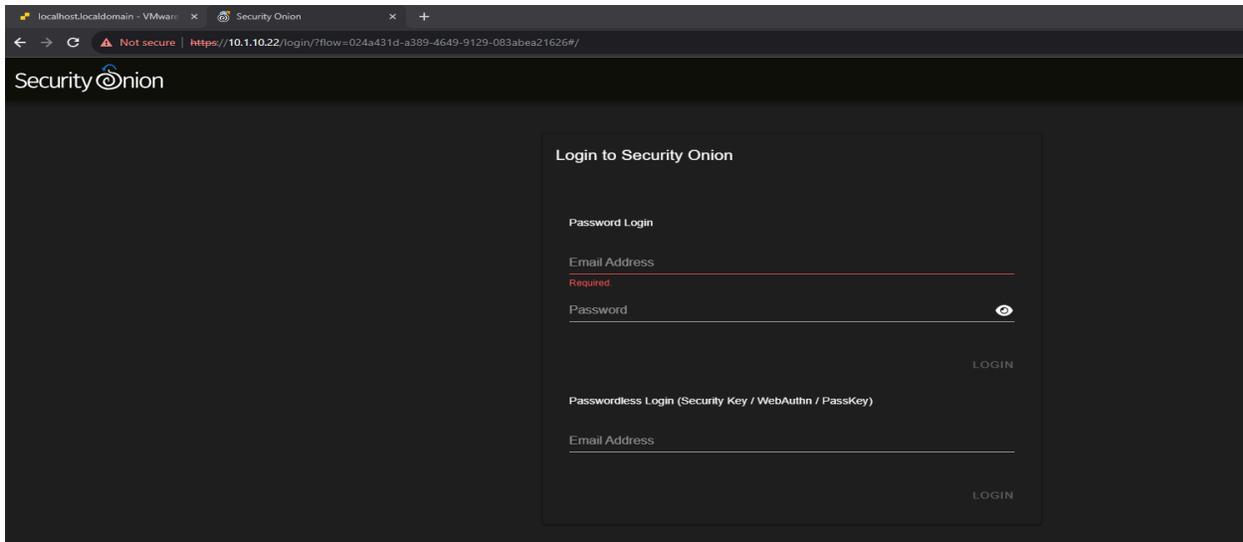


Step 26:

Log in with the WEB IP assigned

10.1.10.22

\*\*If trouble reaching SecOnion occurs, refer to troubleshooting section about RSA keys

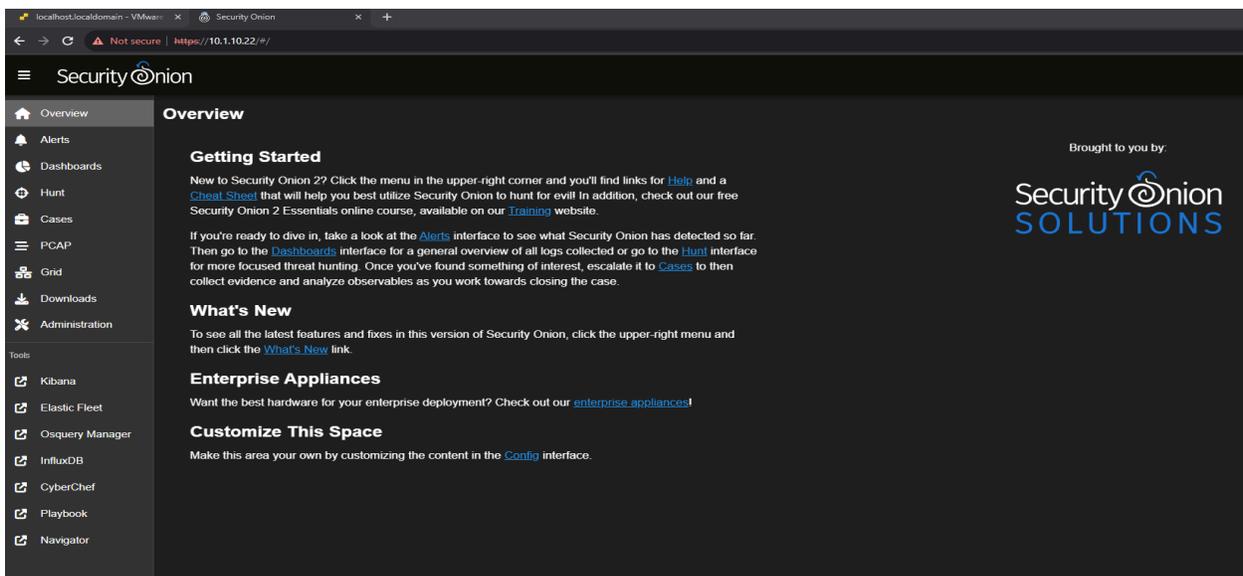


Step 27:

Credentials

soadmin@3rdpltdco.mil

Standard

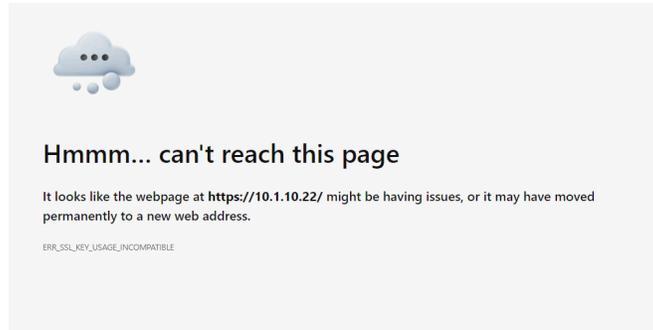




## Troubleshooting SecOnion Browser: *ERR\_SSL\_Key*

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*'



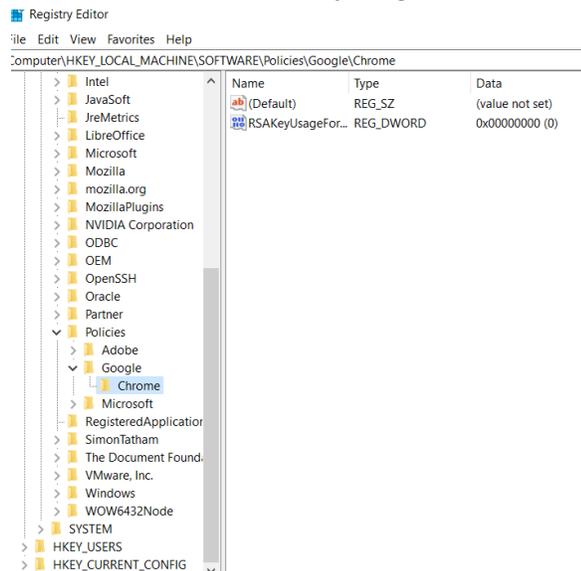
- ❖ Attempt navigating to the WEB IP on Google Chrome

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

### **Grid Administration Quick Links**

- NTP
  - [Specify custom Network Time Protocol server\(s\)](#)
- Firewall
  - [Allow web browsers to login to Security Onion Console](#)
  - [Allow Elastic Agent endpoints to send logs](#)
  - [Allow Elastic Fleet Nodes to connect to Manager](#)
  - [Allow IDH Nodes to connect to Manager](#)
  - [Allow Receiver Nodes to connect to Manager](#)
  - [Allow Search Nodes to connect to Manager](#)
  - [Allow Sensors \(Forward Nodes\) to connect to Manager](#)

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 \*\*\*

The screenshot shows the Palo Alto Networks firewall configuration interface. On the left, a sidebar menu is visible with the following structure:

- Filter: firewall.hostgroups.elc
- Filter the items on this page by keyword
- firewall
  - hostgroups
    - elastic\_agent\_endpoint

The main content area displays the configuration for the 'elastic\_agent\_endpoint' hostgroup. It includes a 'VIEW DEFAULT' button and a list of IP or CIDR blocks to allow access to this hostgroup. The list is titled 'Current Grid Value' and contains the following entries:

- 10.1.10.0/24
- 20.1.10.0/24
- 20.1.10.30
- 10.4.0.0/16



# 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)

New virtual machine - SecAgent1 (ESXi 7.0 U2 virtual machine)

1 Select creation type

2 Select a name and guest OS

3 Select storage

4 Customize settings

5 Ready to complete

### Select a name and guest OS

Specify a unique name and OS

Name

SecAgent1

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Compatibility: ESXi 7.0 U2 virtual machine

Guest OS family: Windows

Guest OS version: Microsoft Windows 10 (64-bit)

Enable Windows Virtualization Based Security

CANCEL BACK NEXT FINISH



## ➤ Save in largest datastore

New virtual machine - SecAgent1 (ESXi 7.0 U2 virtual machine)

1 Select creation type  
2 Select a name and guest OS  
3 Select storage  
4 Customize settings  
5 Ready to complete

Select the storage type and datastore

**Standard** Persistent Memory

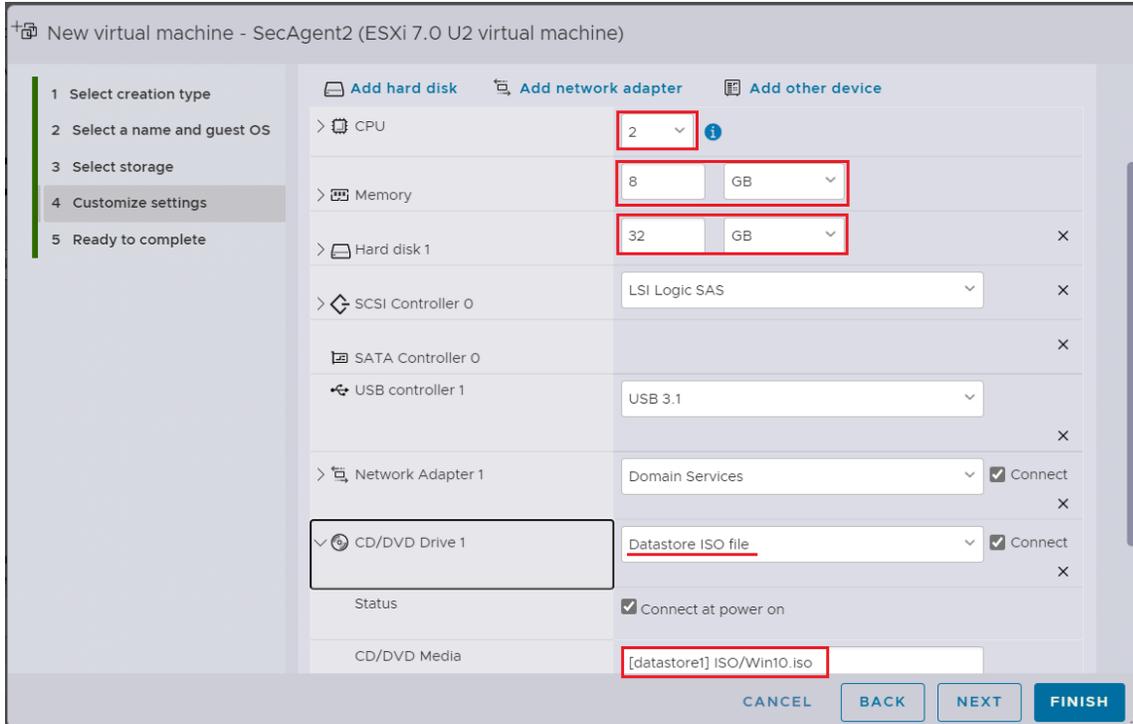
Select a datastore for the virtual machine's configuration files and all of its virtual disks.

Name	Capacity	Free	Type	Thin provision	Access
datastore1	319 GB	231.34 GB	VMFS6	Supported	Single
datastoreBig	27.94 TB	27.77 TB	VMFS6	Supported	Single

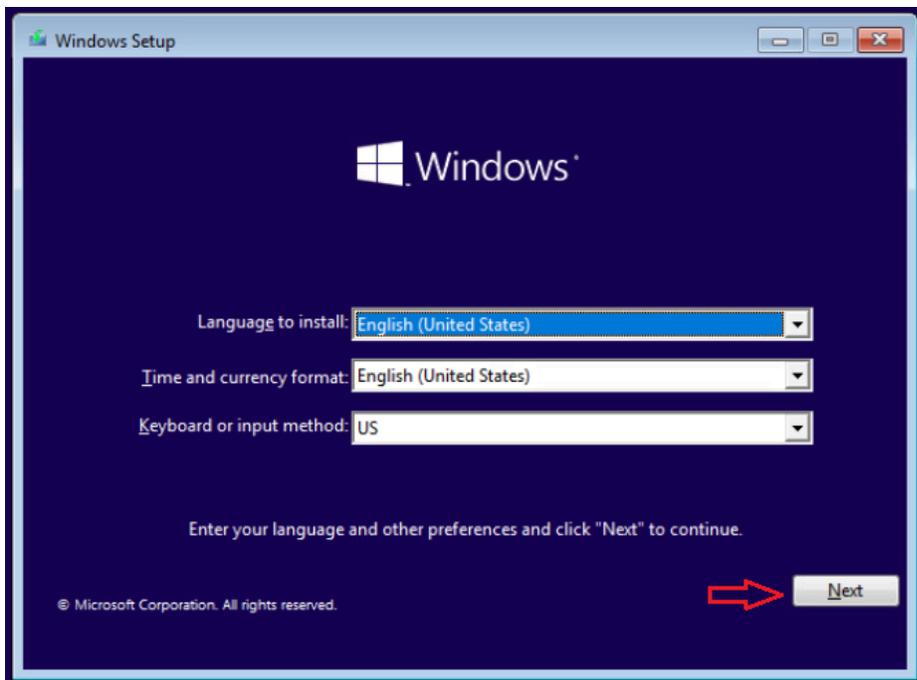
2 items

CANCEL BACK NEXT FINISH

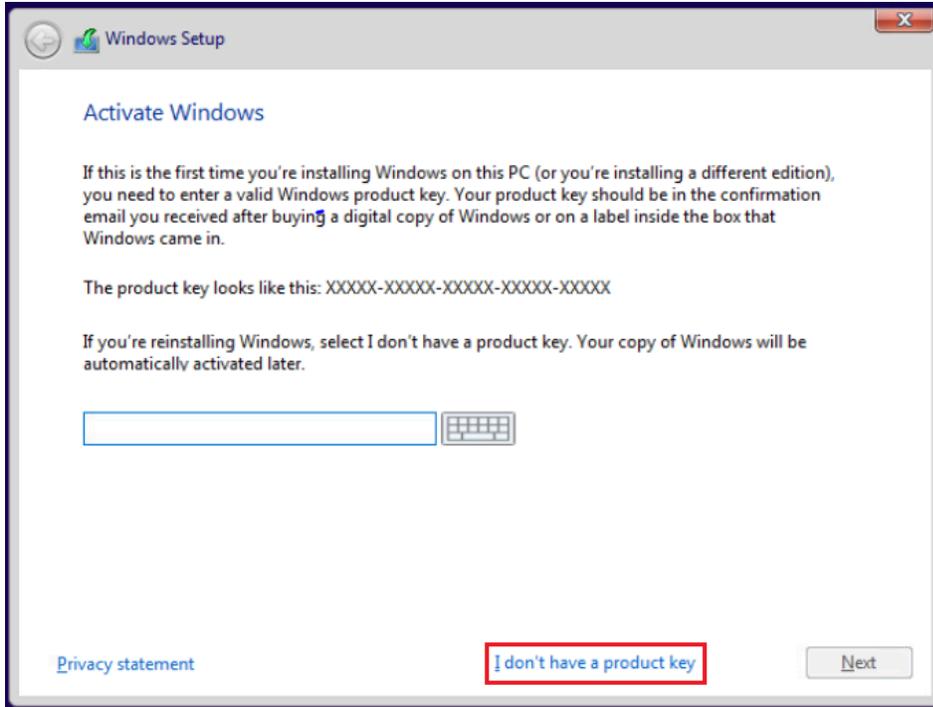
- 2 CPUs
- 8GB Memory
- 32GB Storage, thin-provisioned
- Win10.iso



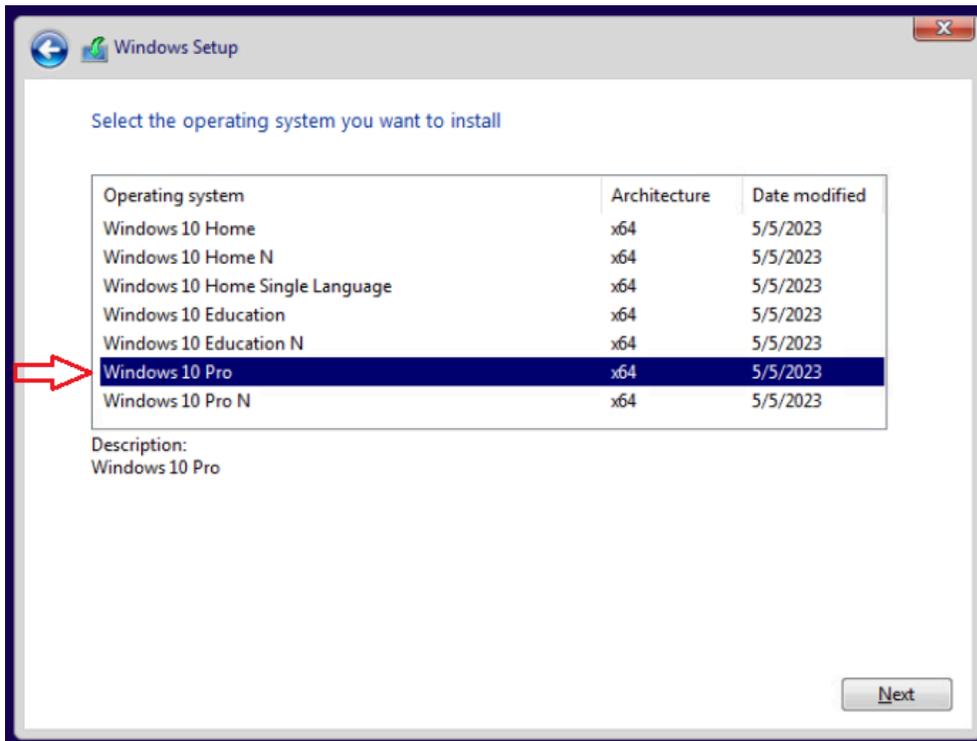
- ❖ Power On
  - (press ENTER if required to “boot normally”)
- ❖ Set language/time currency to ‘English’ -> Next



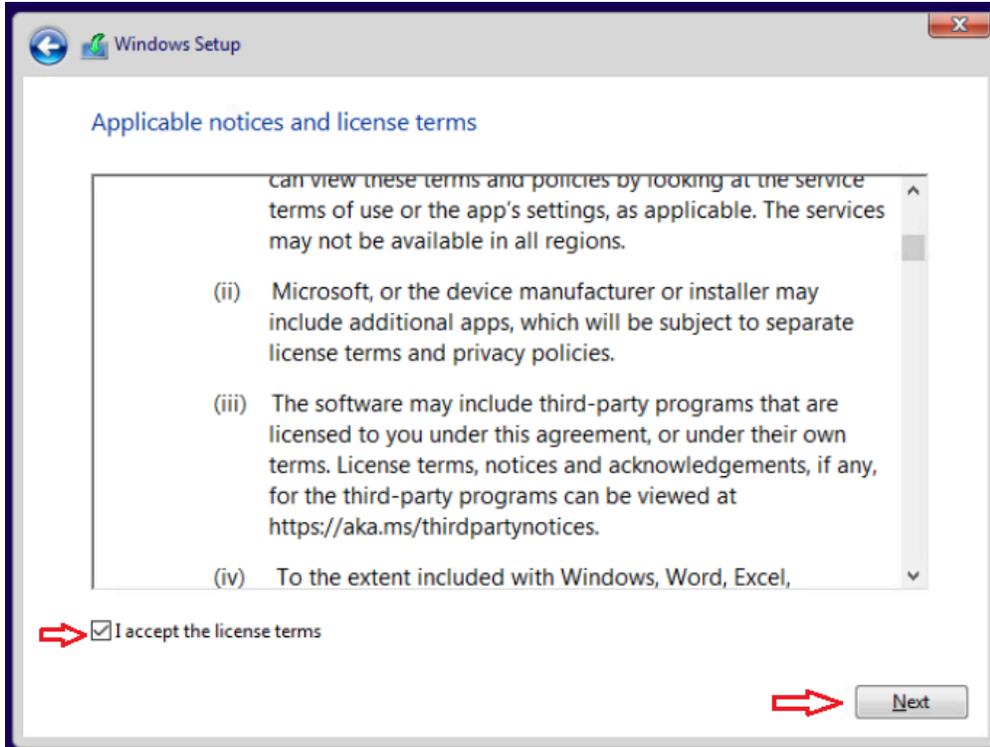
- ❖ Install Now
- ❖ ‘I don’t have a product key’



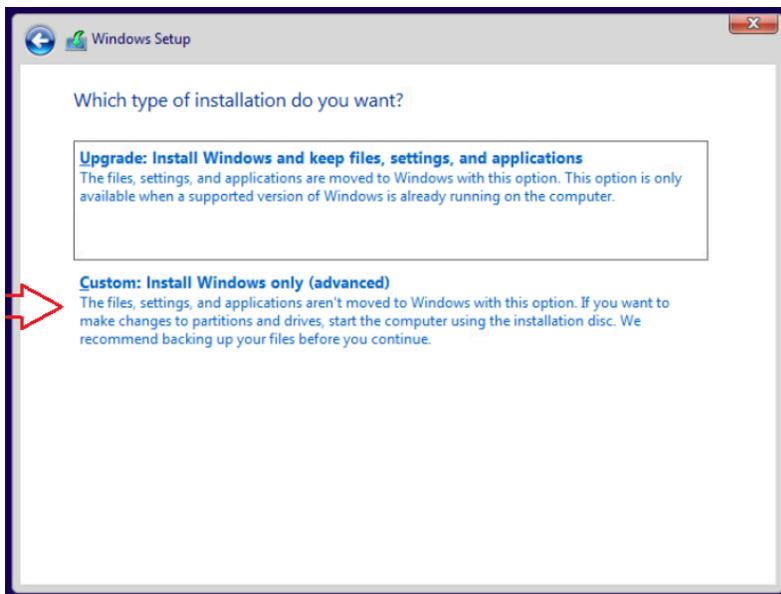
❖ Windows 10 Pro -> Next

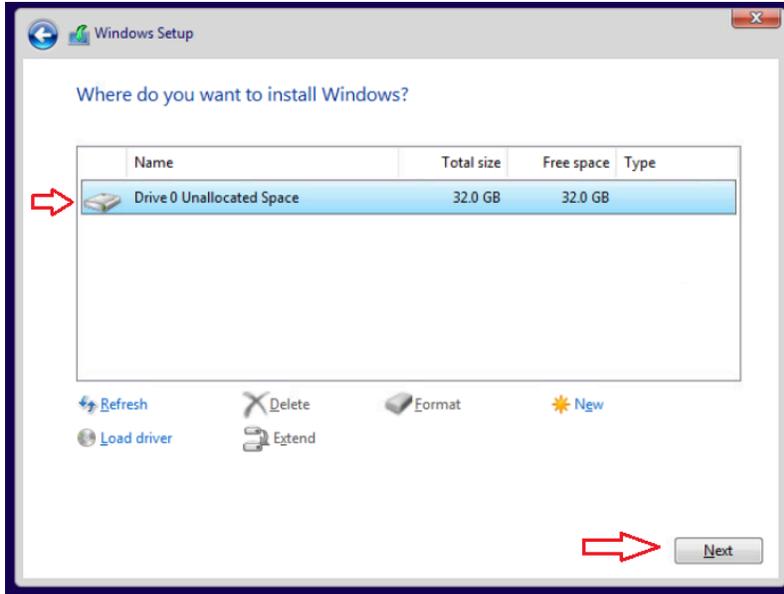


❖ Accept license terms -> Next



#### ❖ Custom Install -> Drive0 -> Next





- ❖ Allow time for install
- ❖ VM should restart automatically / If not, restart manually
- ❖ Select 'US' keyboard layout -> Next



## Let's start with region. Is this right?

U.S. Minor Outlying Islands

U.S. Virgin Islands

Uganda

Ukraine

United Arab Emirates

United Kingdom

United States

Yes

## Is this the right keyboard layout?

If you also use another keyboard layout, you can add that next.

US

Canadian Multilingual Standard

English (India)

Irish

Scottish Gaelic

United Kingdom

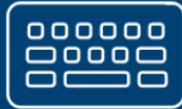
United States-Dvorak

Yes

❖ Skip second keyboard layout



Want to add a second keyboard layout?



Add layout

Skip

❖ 'I don't have network'

Let's connect you to a network

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

 Network  
No Internet

I don't have internet





❖ 'Continue with limited setup'

## There's more to discover when you connect to the internet

Access the full range of apps that help you work and play the way you want when you connect to a network and sign in with Microsoft. Along with being able to browse the internet, get email, and work across devices, you'll also get enhanced features and security.

	Full setup with Microsoft account
 <b>Advanced Security and Privacy</b> Protect and secure your device and personal data	✓
 <b>Free access to Office Online, Outlook, Skype, and more</b> Office Online, Outlook, Skype, Free OneDrive cloud storage, and more	✓
 <b>Unlock the best Windows 10 features</b> Sync photos from your Android phone, pick up where you left off, and more	✓

[Continue with limited setup](#) [Connect now](#)

❖ Create 'DCOadmin' account -> Next

❖ Shop standard password -> Next -> Confirm Password -> Next

## Who's going to use this PC?

What name do you want to use?

[Next](#)



❖ Select security questions -> Answer: 1721

## Create security questions for this account

Just in case you forget your password, choose 3 security questions, and make sure your answers are unforgettable.



What was your first pet's name? ▼

 ×[Next](#)

❖ Check 'No' for all options -> Accept

## Choose privacy settings for your device

Microsoft puts you in control of your privacy. Choose your settings, then select 'Accept' to save them. You can change these settings at any time.

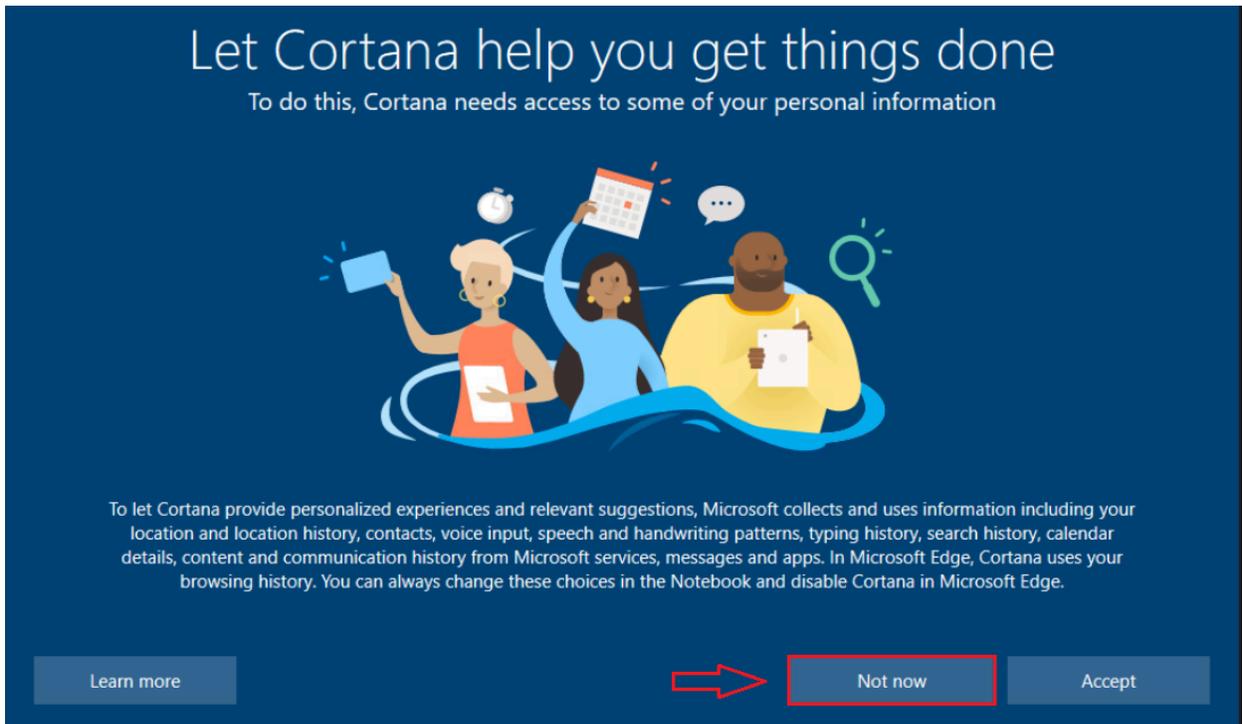
<b>Location</b> You won't be able to get location-based experiences like directions and weather or enjoy other services that require your location to work. <input checked="" type="checkbox"/> No	<b>Find my device</b> Windows won't be able to help you keep track of your device if you lose it. <input checked="" type="checkbox"/> No
<b>Diagnostic data</b> Send only info about your device, its settings and capabilities, and whether it is performing properly. Diagnostic data is used to help keep Windows secure and up to date, troubleshoot problems, and make product improvements. <input checked="" type="checkbox"/> Send Required diagnostic data	<b>Inking &amp; typing</b> Don't use my diagnostic data to help improve the language recognition and suggestion capabilities of apps and services running on Windows. <input checked="" type="checkbox"/> No
<b>Tailored experiences</b> The tips, ads, and recommendations you see will be more generic and may be less relevant to you. <input checked="" type="checkbox"/> No	<b>Advertising ID</b> The number of ads you see won't change, but they may be less relevant to you. <input checked="" type="checkbox"/> No

Select 'Learn more' for info on the above settings, how Microsoft

[Learn more](#) [Accept](#)



❖ 'Not Now'

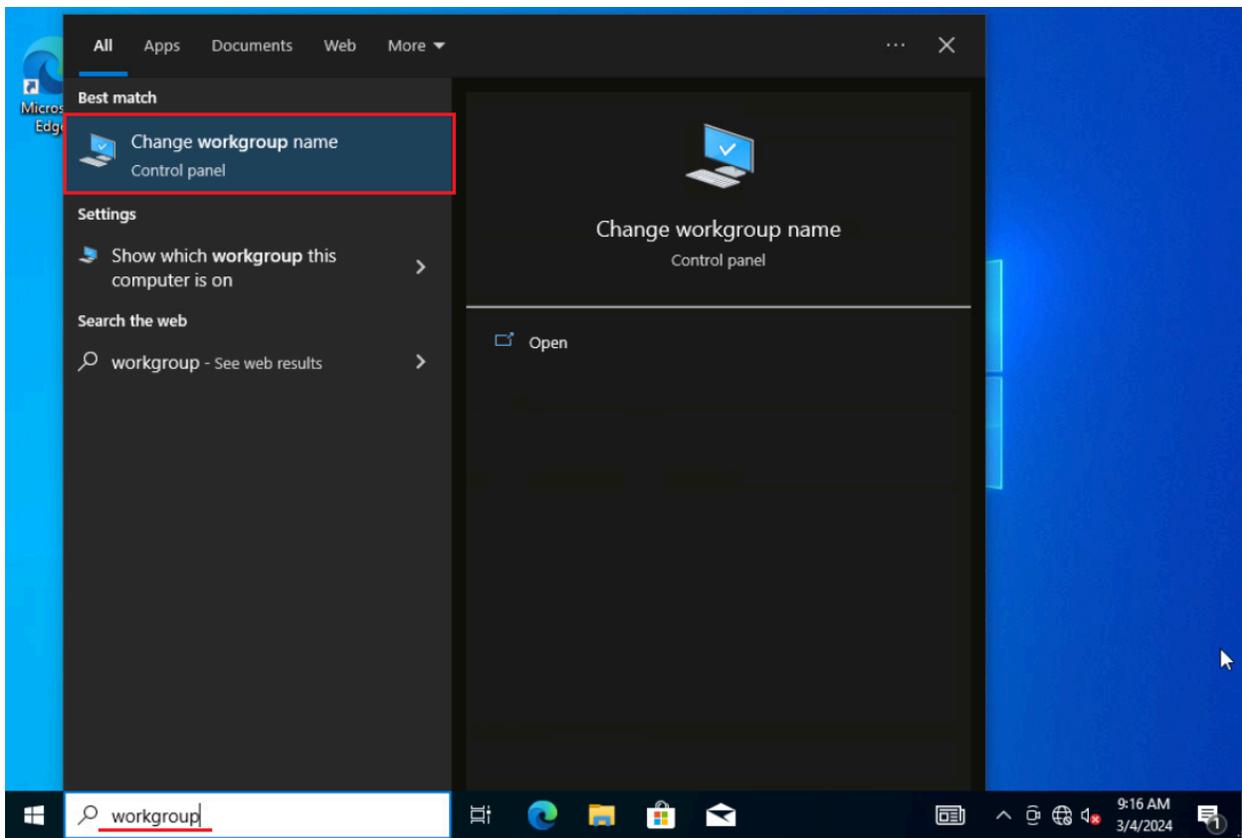


Let Cortana help you get things done  
To do this, Cortana needs access to some of your personal information

To let Cortana provide personalized experiences and relevant suggestions, Microsoft collects and uses information including your location and location history, contacts, voice input, speech and handwriting patterns, typing history, search history, calendar details, content and communication history from Microsoft services, messages and apps. In Microsoft Edge, Cortana uses your browsing history. You can always change these choices in the Notebook and disable Cortana in Microsoft Edge.

Learn more Not now Accept

- ❖ Allow time for configuration
- ❖ Navigate to 'Change Workgroup Name'



Windows search interface showing results for 'workgroup'. The search bar contains 'workgroup'. The search results are displayed in a dark theme. The 'Best match' section shows 'Change workgroup name' (Control panel) with a red box around it. The 'Settings' section shows 'Show which workgroup this computer is on'. The 'Search the web' section shows 'workgroup - See web results'. The taskbar at the bottom shows the search bar with 'workgroup' entered, and the system tray shows the time as 9:16 AM on 3/4/2024.



❖ Add VM to 3rdplt.dco.mil

System Properties

Computer Name Hardware Advanced System Protection Remote

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: DESKTOP-BN61IQH

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:

Full computer name: DESKTOP-BN61IQH

Member of

Domain:

Workgroup:



❖ Enter 'Administrator' credentials

Windows Security

### Computer Name/Domain Changes

Enter the name and password of an account with permission to join the domain.

User name

Password

OK Cancel

### Computer Name/Domain Changes

**i** Welcome to the 3rdpdt.dco.mil domain.

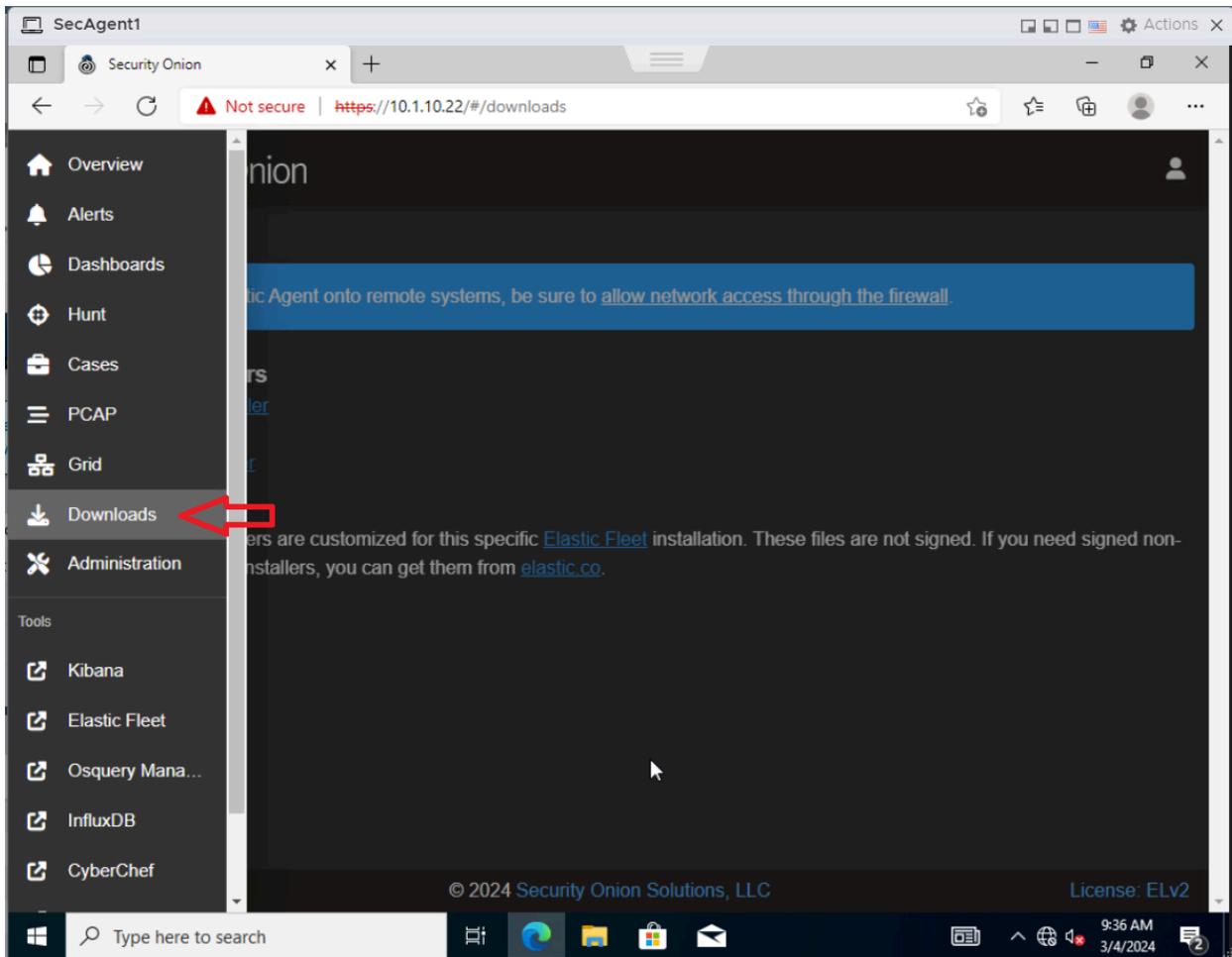
OK

❖ 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'

The screenshot shows the Elastic Fleet interface with the 'Add agent' dialog open. The 'What type of host are you adding?' step is highlighted with a red box. The 'endpoints-initial' policy is selected. Below the policy selection, it states that the policy will collect data for 4 integrations: Windows, System, Elastic Defend, and Osquery Manager. The 'Enroll in Fleet?' step is also visible, with the 'Enroll in Fleet (recommended)' option selected.

- ❖ Scroll down to '3' and select Windows
- ❖ Copy the given script to the clipboard

The screenshot shows the Elastic Fleet interface with the 'Add agent' dialog open. The 'Install Elastic Agent on your host' step is highlighted with a red box. The 'Windows' platform is selected. A terminal window displays the following installation script:

```
$ProgressPreference = 'SilentlyContinue'  
Invoke-WebRequest -Uri https://artifacts.elastic.co/downloads/beats/e  
Expand-Archive .\elastic-agent-8.8.2-windows-x86_64.zip -DestinationP  
cd elastic-agent-8.8.2-windows-x86_64  
.\elastic-agent.exe install --url=https://10.1.10.22:8220 --enrollmen
```



- ❖ 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.

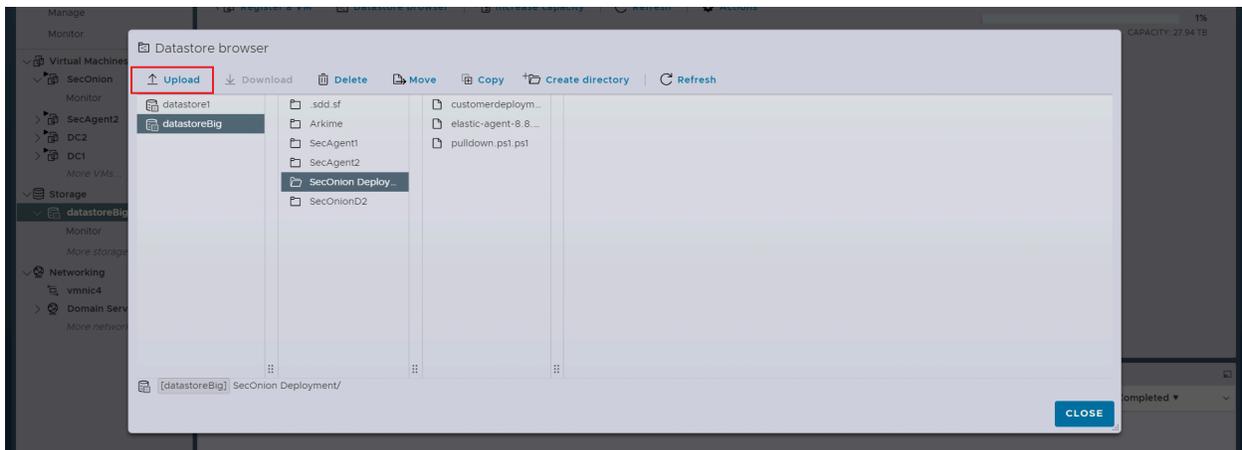
```
pulldown.ps1 - Notepad
File Edit Format View Help
$ProgressPreference = 'SilentlyContinue'
Invoke-WebRequest -Uri http://10.1.10.22:8443/artifacts/beats/elastic-agent/elastic-agent-8.8.2-windows-x86_64.zip -OutFile elastic-agent-8.8.2-windows-x86_64.zip
Expand-Archive .\elastic-agent-8.8.2-windows-x86_64.zip -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=VxUcmhJME3nY21CSnp1VnBBbzE6NU5mVTg3cHVRcUdsMjRwQkJEEd3RmUQ==
```

- ❖ 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





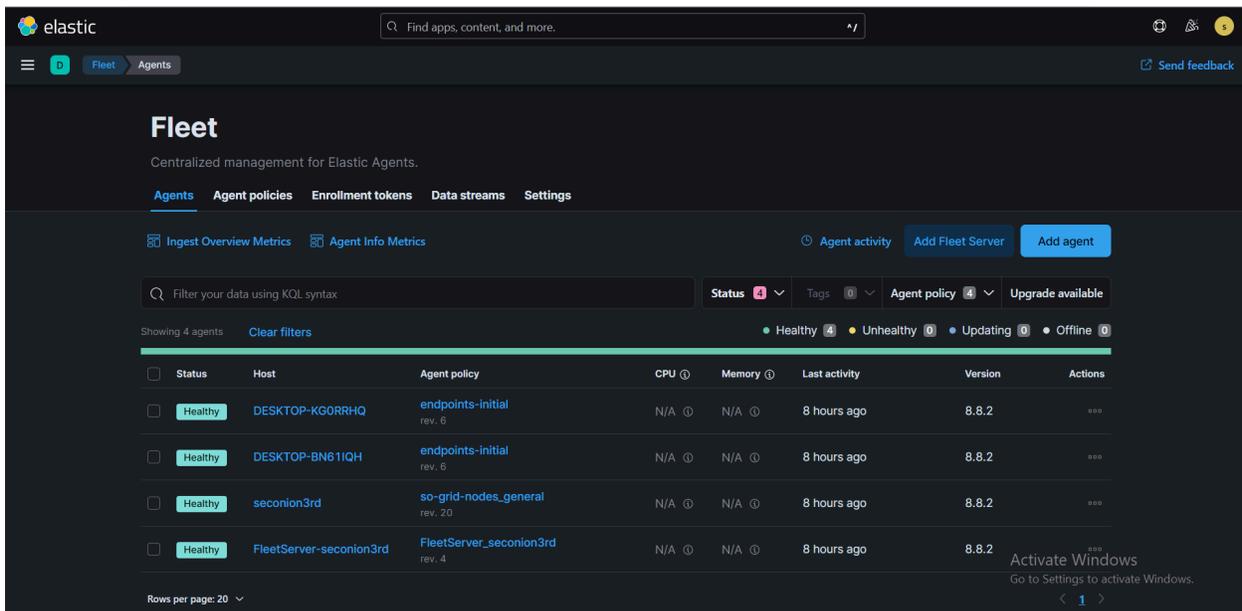
- ❖ On VM, open a Web Browser and navigate to ESXI
  - Download both files from the datastore to Desktop\SecOnion
  - Run Powershell as administrator
  - Set-ExecutionPolicy Bypass
  - .\customerdeployment
  - When prompted to continue, enter y for yes

```
Directory: C:\Users\DCOadmin\Desktop\SecOnion

Mode                LastWriteTime         Length Name
----                -
d-----          3/4/2024 10:49 AM             elastic-agent-8.8.2-windows-x86_64
-a----          3/4/2024 10:47 AM              187 customerdeployment.ps1
-a----          3/4/2024 10:49 AM     281325850 elastic-agent-8.8.2-windows-x86_64.zip
-a----          3/4/2024 10:47 AM              282 pulldown.ps1.ps1

PS C:\Users\DCOadmin\Desktop\SecOnion> .\customerdeployment.ps1
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:y
{"log.level":"warn","@timestamp":"2024-03-04T10:53:58.796-0800","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.go","file.line":104},"message":"SSL/TLS verifications disabled.","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2024-03-04T10:53:59.803-0800","log.origin":{"file.name":"cmd/enroll_cmd.go","file.line":478},"message":"Starting enrollment to URL: https://10.1.10.22:8220/","ecs.version":"1.6.0"}
{"log.level":"warn","@timestamp":"2024-03-04T10:54:00.061-0800","log.logger":"tls","log.origin":{"file.name":"tlscommon/tls_config.go","file.line":104},"message":"SSL/TLS verifications disabled.","ecs.version":"1.6.0"}
Error: fail to enroll: fail to execute request to fleet-server: dial tcp 10.1.10.22:8220: connectex: No connection could be made because the target machine actively refused it.
For help, please see our troubleshooting guide at https://www.elastic.co/guide/en/fleet/8.8/fleet-troubleshooting.html
Error: enroll command failed with exit code: 1
For help, please see our troubleshooting guide at https://www.elastic.co/guide/en/fleet/8.8/fleet-troubleshooting.html
PS C:\Users\DCOadmin\Desktop\SecOnion\elastic-agent-8.8.2-windows-x86_64>
```

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



**\*\*NOTE\*\***

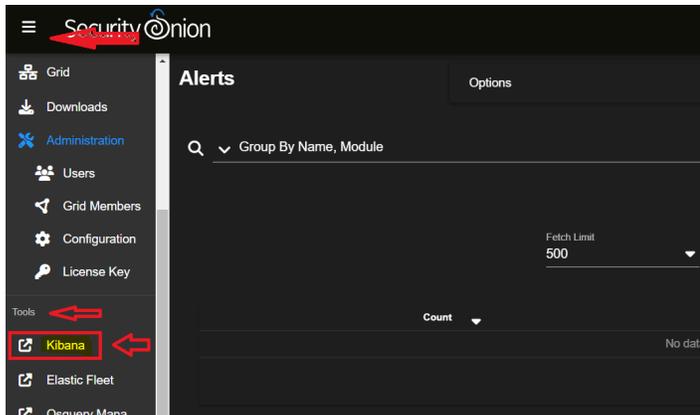
in the powershell script the ip address of your elastic host needs to be changed to the external ip address of your firewall (if you are re-creating the elastic\_package at anytime)



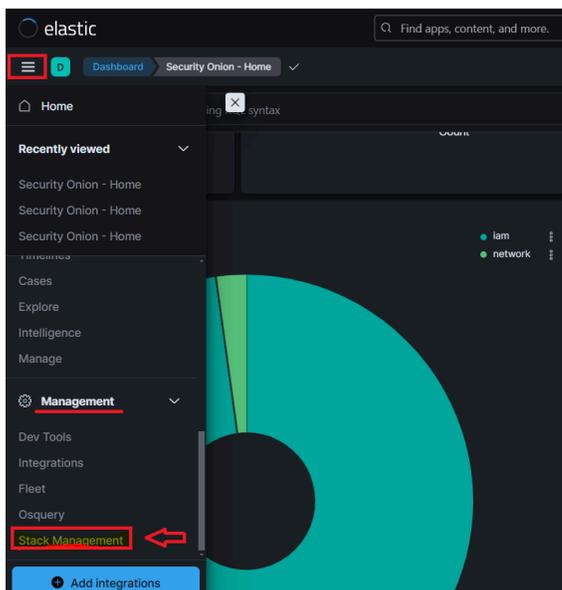
## Enabling Alerts in Elastic

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.

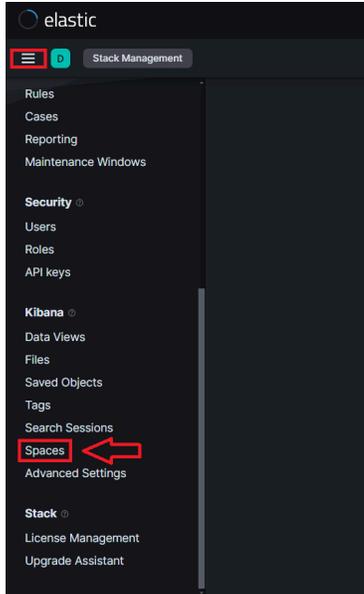
- ❖ Navigate to Security Onion. Under Tools, select Kibana.



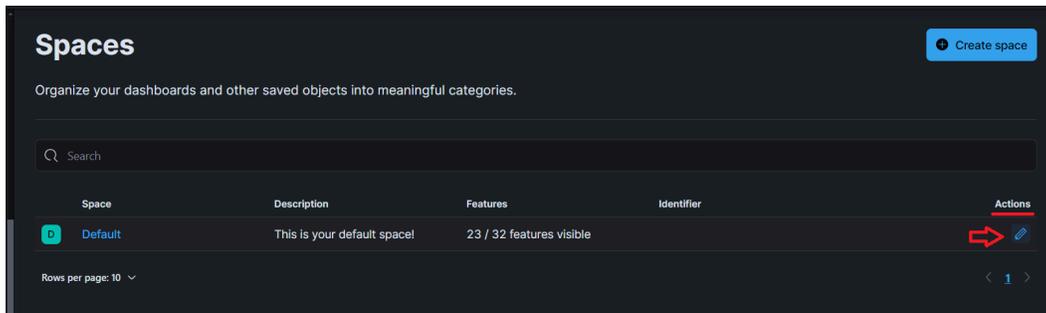
- ❖ Navigate to Management and select Stack Management.



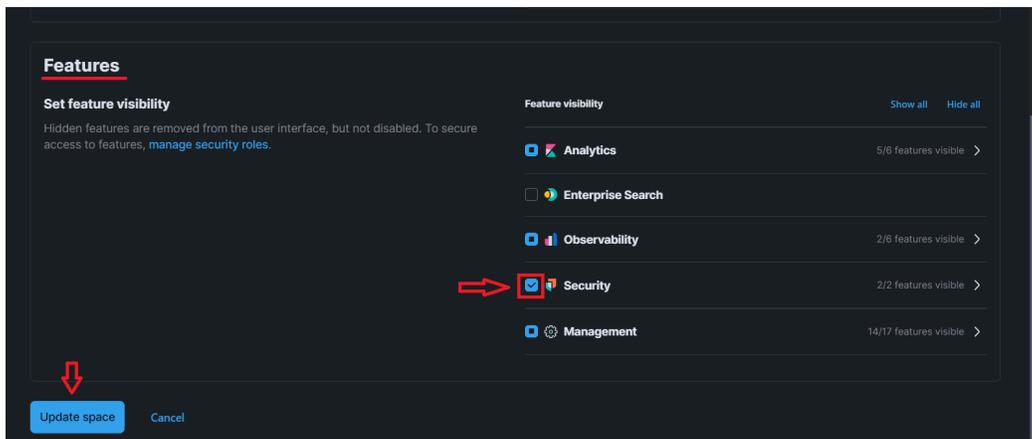
- ❖ In the drop down on the left, scroll down and select Spaces.



❖ 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.

The screenshot shows the Elastic Security Alerts page. The left sidebar has 'Security' selected, and 'Alerts' is highlighted. The main content area shows 'Alerts' with a 'Manage rules' button highlighted by a red arrow. Below the button are filters for Status (open), Severity, User, and Host. There are three charts: 'Severity levels' showing 1 Low alert, 'Alerts by name' showing 'My First Rule' with 1 alert, and 'Top alerts by' showing 'seconion3rd' with 100% of alerts.

- ❖ 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\*

The screenshot shows the Elastic Security Rules page. The left sidebar has 'Security' selected, and 'Manage' and 'Rules' are highlighted. The main content area shows 'Rules' with 'Import value lists', 'Import rules', and 'Create new rule' buttons. Below are filters for Rule name, index pattern, and tags. A table shows rules with columns for Rule, Risk score, Severity, Last run, Last response, Last updated, Notify, and Enabled. Two rules are visible: 'AWS VPC Flow Logs Deletion' and 'AWS WAF Access Control List De...'. The 'Select all 806 rules' and 'Bulk actions' buttons are highlighted with red boxes.



Rule	Risk score	Severity	Last run	Last response	Last updated	Notify	Enabled
AWS VPC Flow L...	6	73	High	8 hours ago	Warn...	8 hours ago	Enabled
AWS WAF Acces...	5	47	Med...	8 hours ago	Warn...	8 hours ago	Enabled
AWS IAM Assum...	6	21	Low	8 hours ago	Warn...	8 hours ago	Enabled
AWS CloudTrail L...	5	21	Low	8 hours ago	Warn...	8 hours ago	Enabled
My First Rule	4	21	Low	8 hours ago	Succ...	8 hours ago	Enabled
Process Injection - Prevented - El...	3	47	Med...	8 hours ago	Warn...	8 hours ago	Enabled
Credential Dumping - Detected - ...	3	73	High	8 hours ago	Warn...	8 hours ago	Enabled

## Enabling Playbook Alerts in Security Onion

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

**Grid Configuration**

Filter: analyst, beats\_endpoint, beats\_endpoint\_ssl, desktop, elastic\_agent\_endpoint, eval, fleet, heavynode, irth



- ❖ 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\*

The screenshot shows the 'DETECTION PLAYBOOKS' interface. At the top, there is a search bar and a dropdown menu set to 'Detection Playbooks'. Below this, there are tabs for 'Activity', 'Playbook', and 'Create New Play'. The main area displays a table of playbooks with columns for '#', 'Status', 'Level', 'Playbook', 'Title', 'Updated', and 'Actions'. The first row is selected, and a dropdown menu is open under the 'Actions' column, showing options like 'Edit', 'Status', 'Playbook', 'Filter', 'Copy', and 'Delete'. The 'Status' option is highlighted, and a sub-menu is visible with 'Draft' and 'Active' options. The 'Active' option is selected.

#	Status	Level	Playbook	Title	Updated	Actions
303	Draft	high	community	Remote Thread Creation Tldirjct.exe Proxy	02/28/2024 02:11 PM	...
302	Draft	high	community	Remote Thread Creation Via PowerShell In Rundll32	02/28/2024 02:11 PM	...
301	Draft	high	community	Potential Credential Dumping Attempt Via PowerShell Remote Thread	02/28/2024 02:11 PM	...
300	Draft	medium	community	Remote Thread Creation Via PowerShell	02/28/2024 02:11 PM	...
299	Draft	high	community	Password Dumper Remote Thread in LSASS	02/28/2024 02:11 PM	...
298	Draft	high	community	Remote Thread Creation In Mstsc.Exe From Suspicious Location	02/28/2024 02:11 PM	...
297	Draft	high	community	CreateRemoteThread API and LoadLibrary	02/28/2024 02:11 PM	...
296	Draft	high	community	Remote Thread Created In KeePass EXE	02/28/2024 02:11 PM	...
295	Draft	high	community	HackTool - Potential CobaltStrike Process Injection	02/28/2024 02:11 PM	...
294	Draft	high	community	HackTool - CACTUSTORCH Remote Thread Creation	02/28/2024 02:11 PM	...
293	Draft	medium	community	WMI Persistence	02/28/2024 02:11 PM	...
292	Draft	high	community	Microsoft Defender Tamper Protection Trigger	02/28/2024 02:11 PM	...

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 Baseline

*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](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.