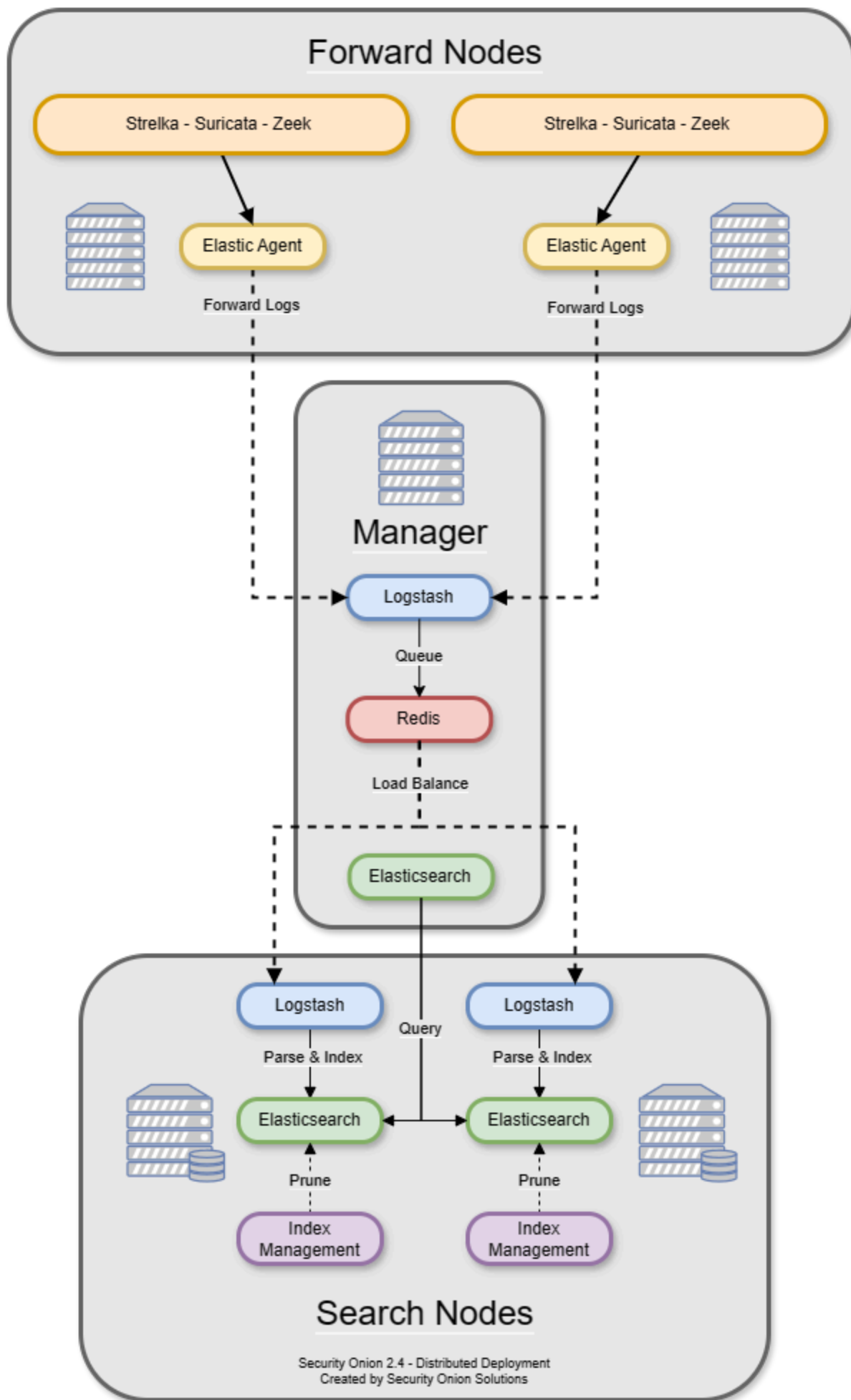


# Manager - Security Onion Distributed Installation

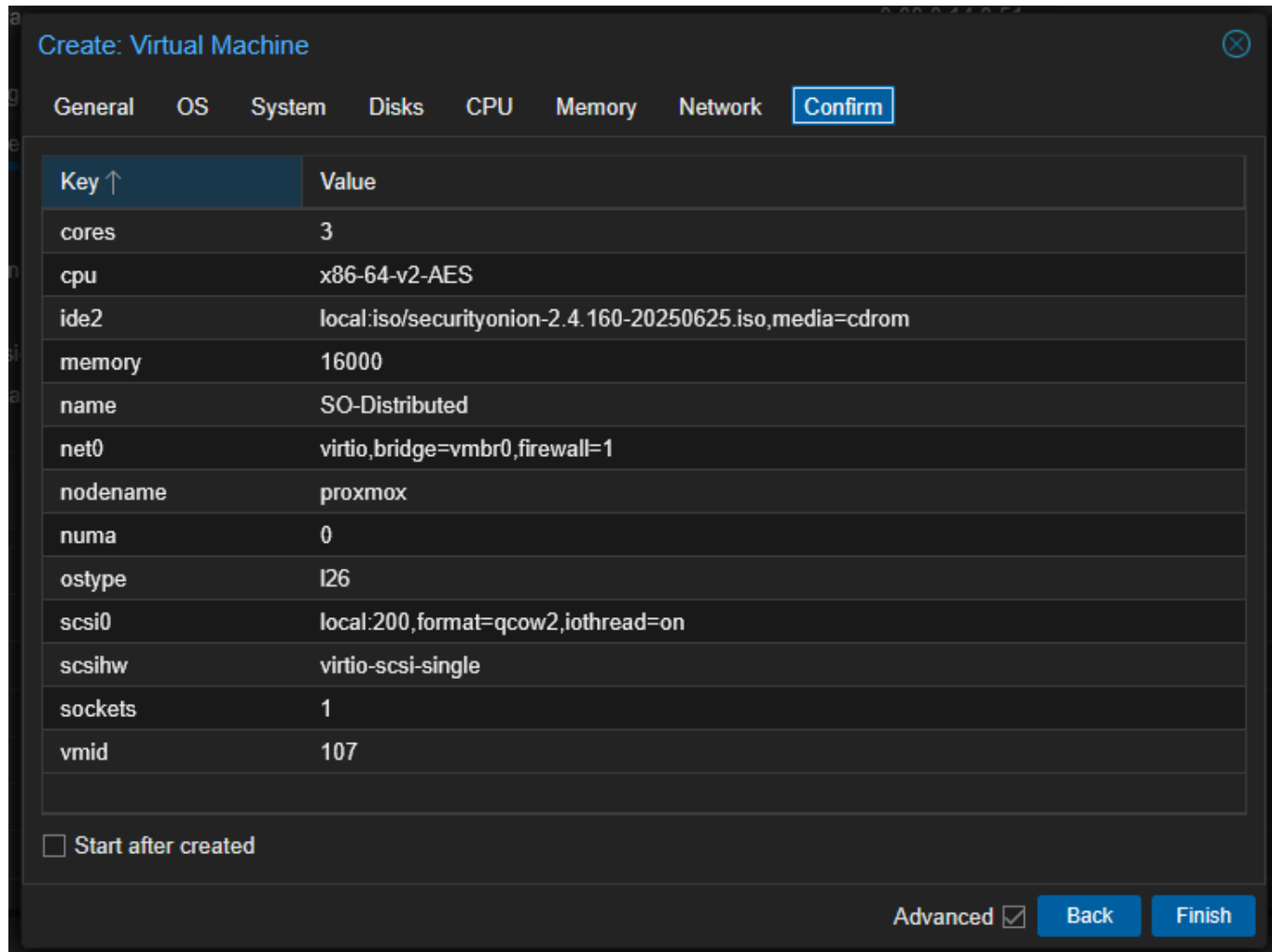
8/1/2025 - *Security Onion 2.4.160*

I am going to be walking you through the steps of deploying Security Onion Distributed architecture, this is a awesome way to deploy Security Onion as the way we did it previously was "standalone" which is all on one machine, this is a issue though in terms of high availability because if something was to happen to that machine the whole system would be effected, by doing distributed we are spreading out the resources and required applications across multiple servers. If your interested in the installation for the standalone [Security Onion Installation Guide](#)



## Step 1: Creating The Node VM

Create your VM using the Security Onion ISO, here [Machine Requirements](#) is a photo of the required resources needed per application, since the first step to deploying the distributed architecture is the manager node we are going to give this VM 3 cores (I don't have 4 cores to spare, & 16GB of ram.)



Key ↑	Value
cores	3
cpu	x86-64-v2-AES
ide2	local:iso/securityonion-2.4.160-20250625.iso,media=cdrom
memory	16000
name	SO-Distributed
net0	virtio,bridge=vbr0,firewall=1
nodename	proxmox
numa	0
ostype	l26
scsi0	local:200,format=qcow2,ioread=on
scsihw	virtio-scsi-single
sockets	1
vmid	107

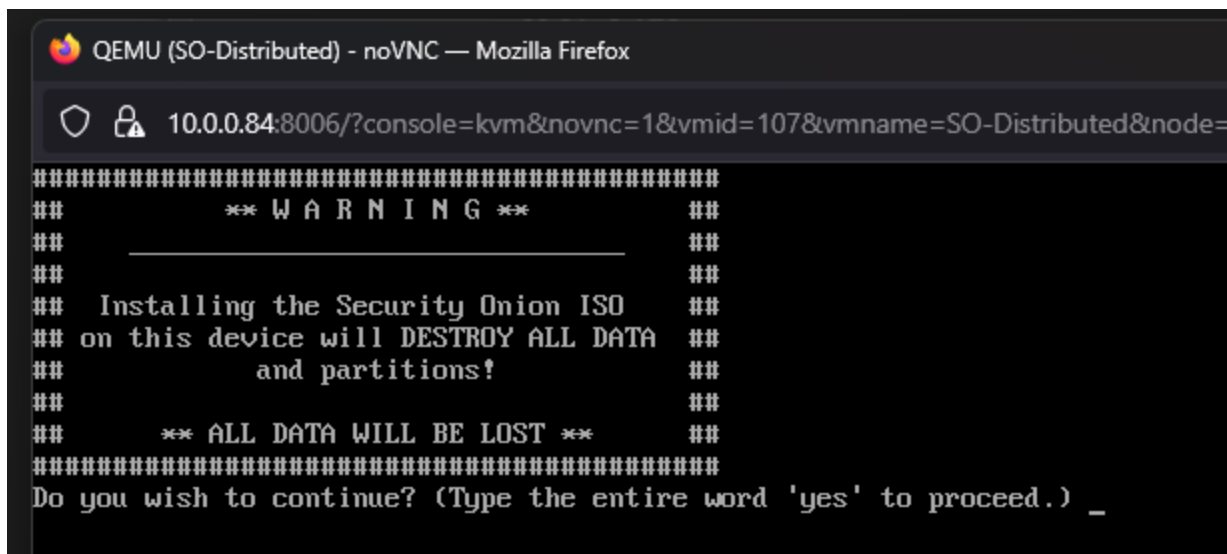
☐ Start after created

Advanced ☒ Back Finish

After the VM is created ensure you start the VM so obviously we can connect to the machine,

## Step 2: Installation/Configuration Of The Manager Node

Once the VM is started, connect to the console and let the ISO do it's initialization required, once it's done with what it needs to do you will be prompted with;

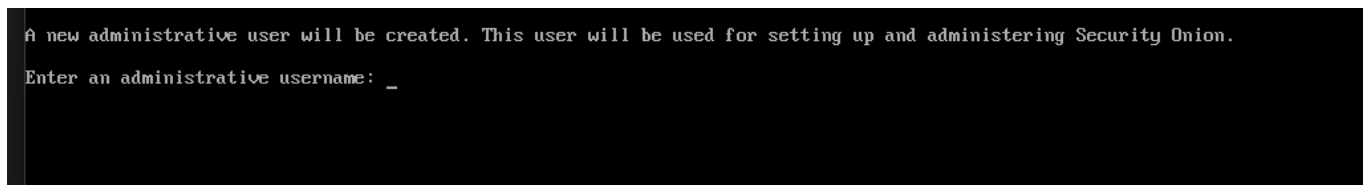


```
QEMU (SO-Distributed) - noVNC — Mozilla Firefox
10.0.0.84:8006/?console=kvm&novnc=1&vmid=107&vmname=SO-Distributed&node=
#####
##          *** W A R N I N G ***          ##
##          _____                    ##
##  Installing the Security Onion ISO      ##
## on this device will DESTROY ALL DATA  ##
##          and partitions!                ##
##          *** ALL DATA WILL BE LOST *** ##
#####
Do you wish to continue? (Type the entire word 'yes' to proceed.) _
```

Since this is a fresh machine, we know we aren't going to be losing any data, so I am going to proceed by typing 'yes'

After proceeding you will be required to enter a administrator username & pass, for the sake of the lab I am going to keep it very simple and provide the username & pass

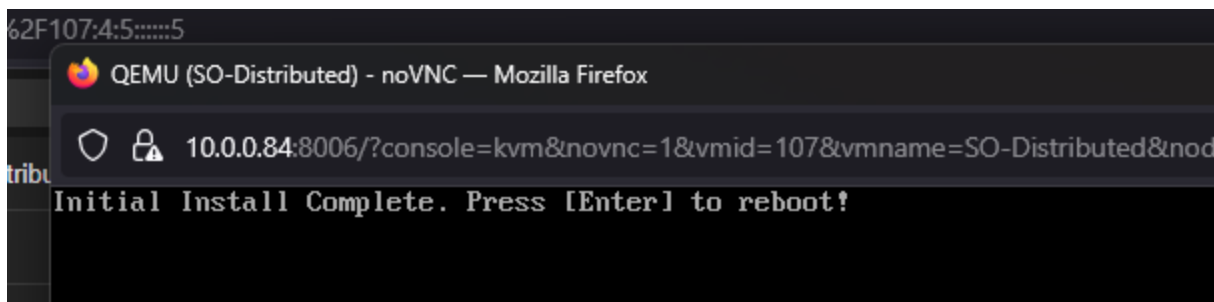
***securityonion:securityonion***



```
A new administrative user will be created. This user will be used for setting up and administering Security Onion.
Enter an administrative username: _
```

After that is done it is going to run through a few more startup things, be patient it can take some time.

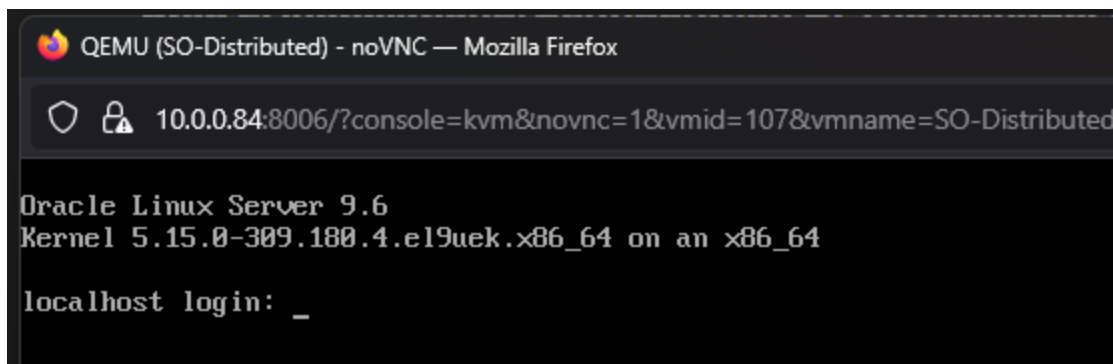
Once it's done what it needs to do you'll see a message similar to this requesting you hit enter to reboot;



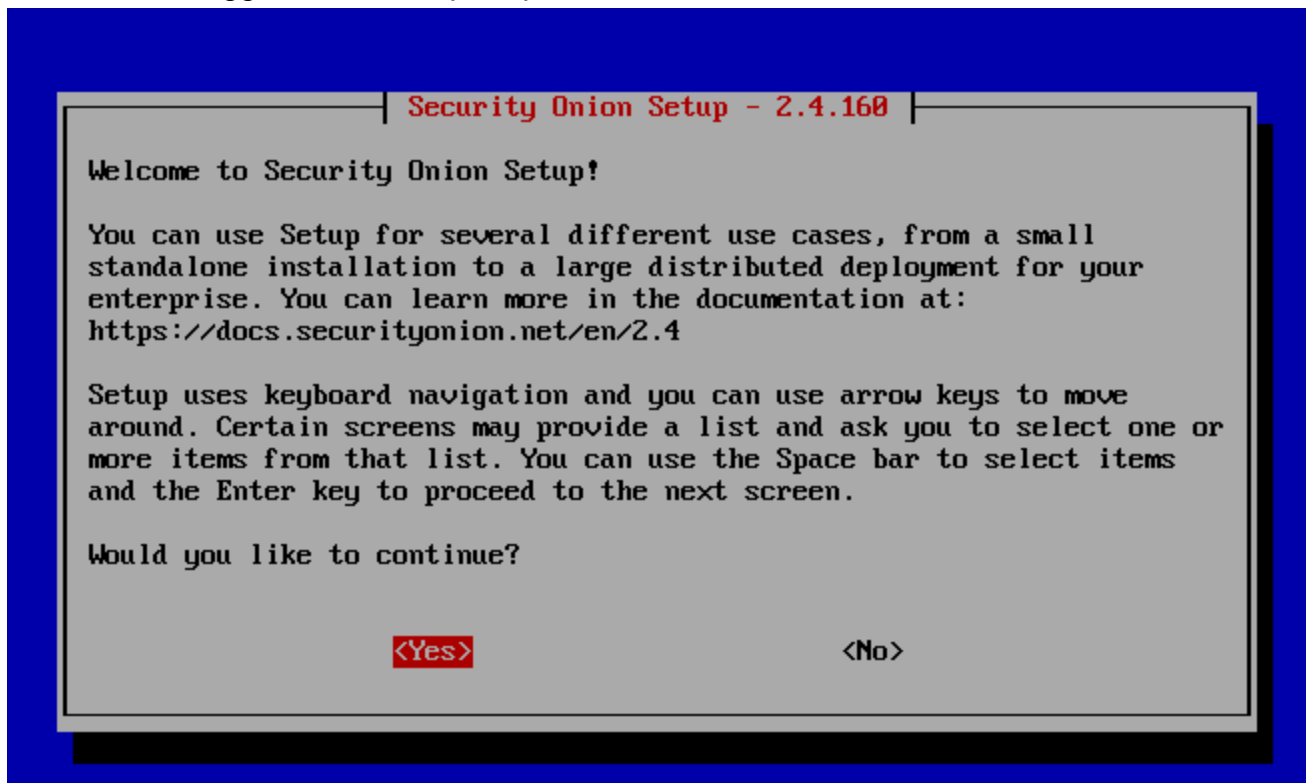
```
62F107:4:5:::5
QEMU (SO-Distributed) - noVNC — Mozilla Firefox
10.0.0.84:8006/?console=kvm&novnc=1&vmid=107&vmname=SO-Distributed&node=
Initial Install Complete. Press [Enter] to reboot!
```

So hit enter and carry on with the installation;

Once it's rebooted, you'll be prompted to login with the credentials we previously created above, so log in and move to the next step;

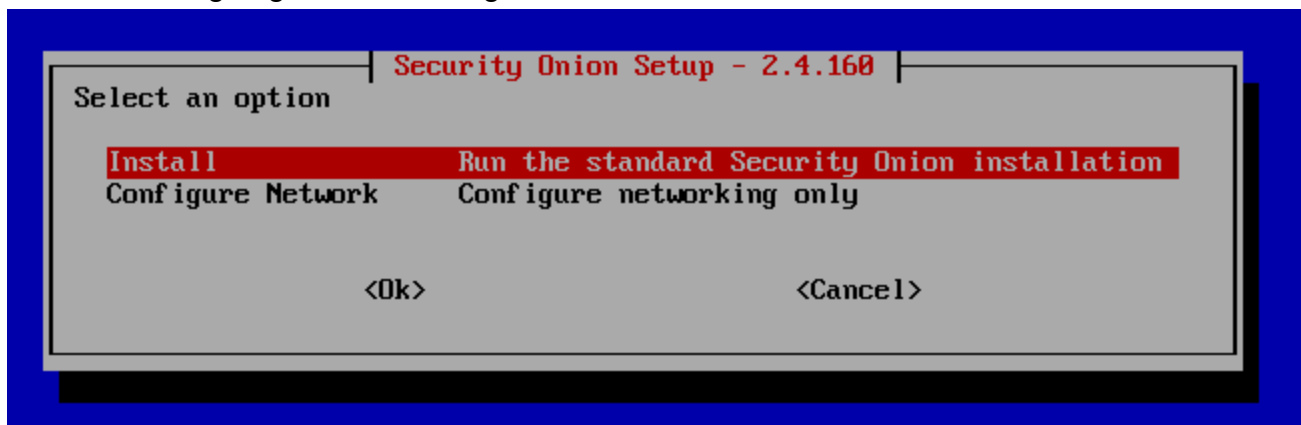


Once we are logged in, we are prompted with the Welcome screen



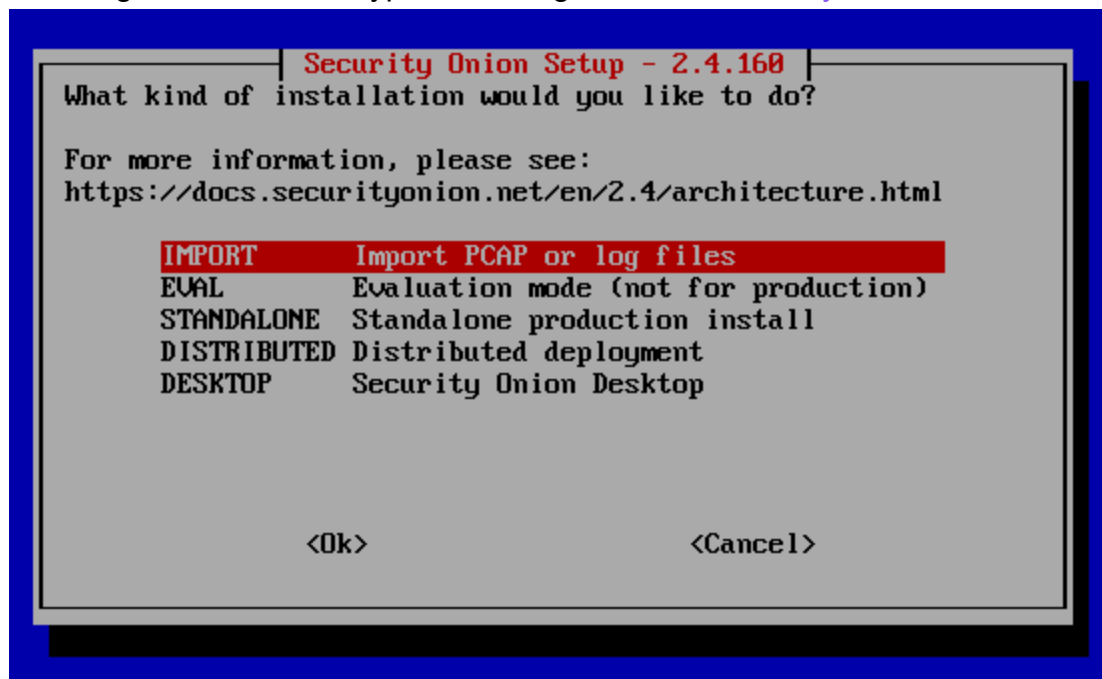
Select yes to carry on.

After selecting yes, we will be prompted with 2 options, install security onion, or configure the network; I am going to be selecting Install;

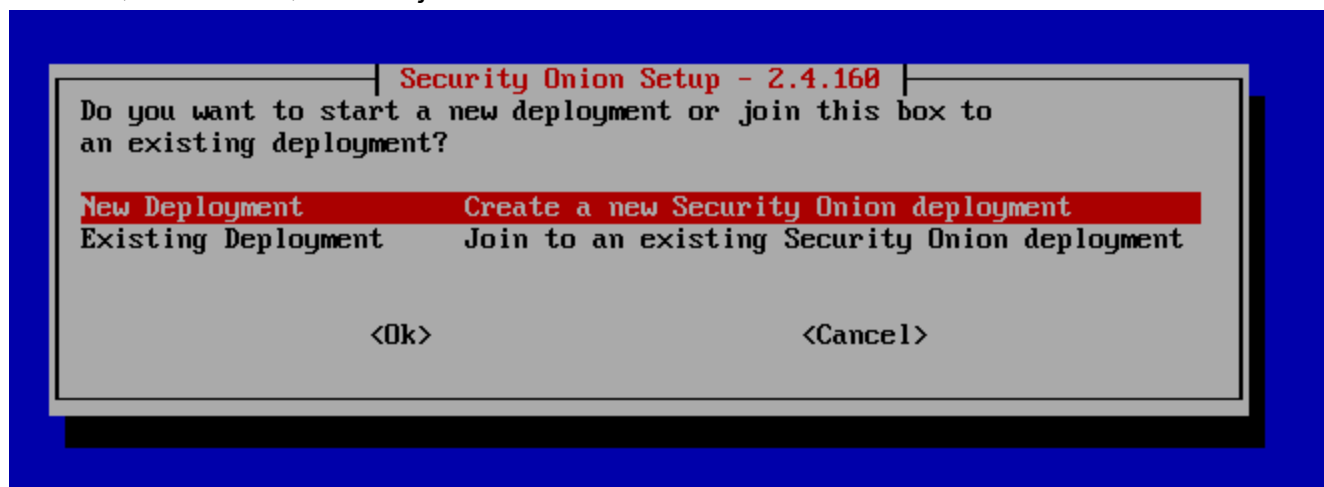


After selecting install we are prompted with what kind of install we would like to do, since we are doing a lab with the distributed type, I am going to select distributed, if your interested in

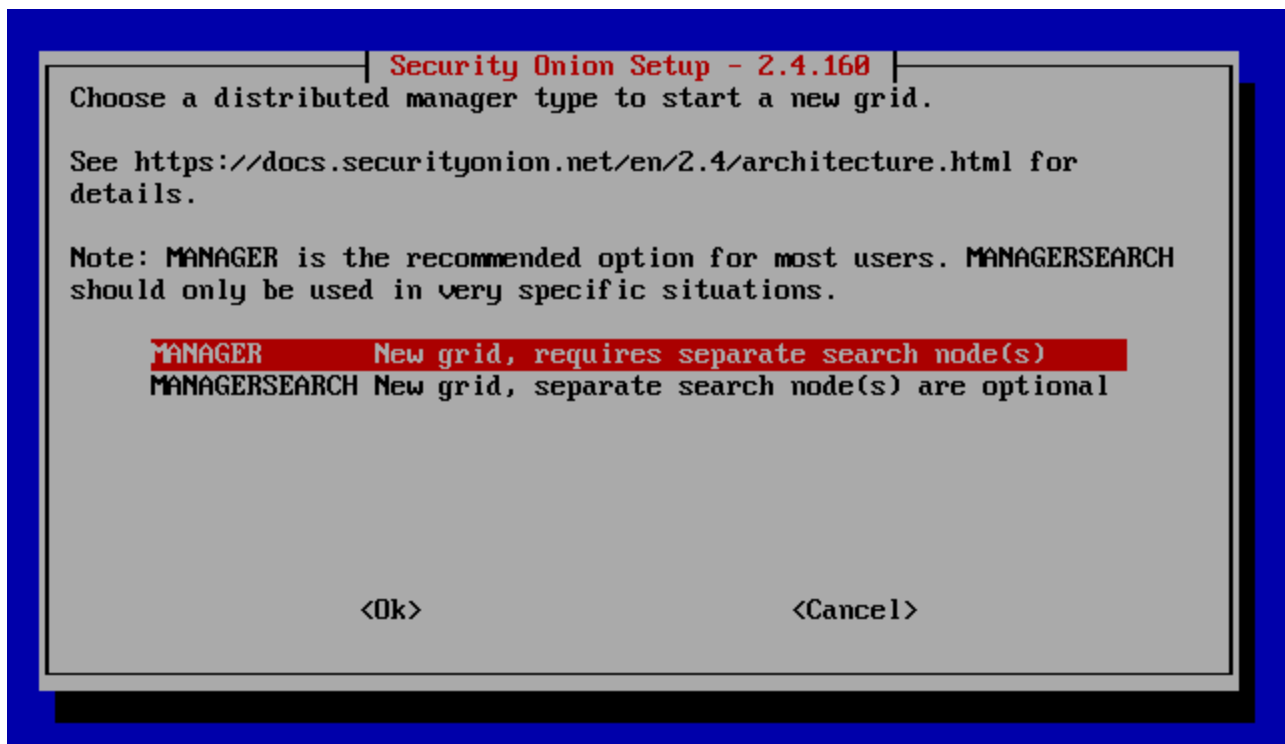
installing the standalone type I have a guide here; [Security Onion Installation Guide](https://docs.securityonion.net/en/2.4/architecture.html)



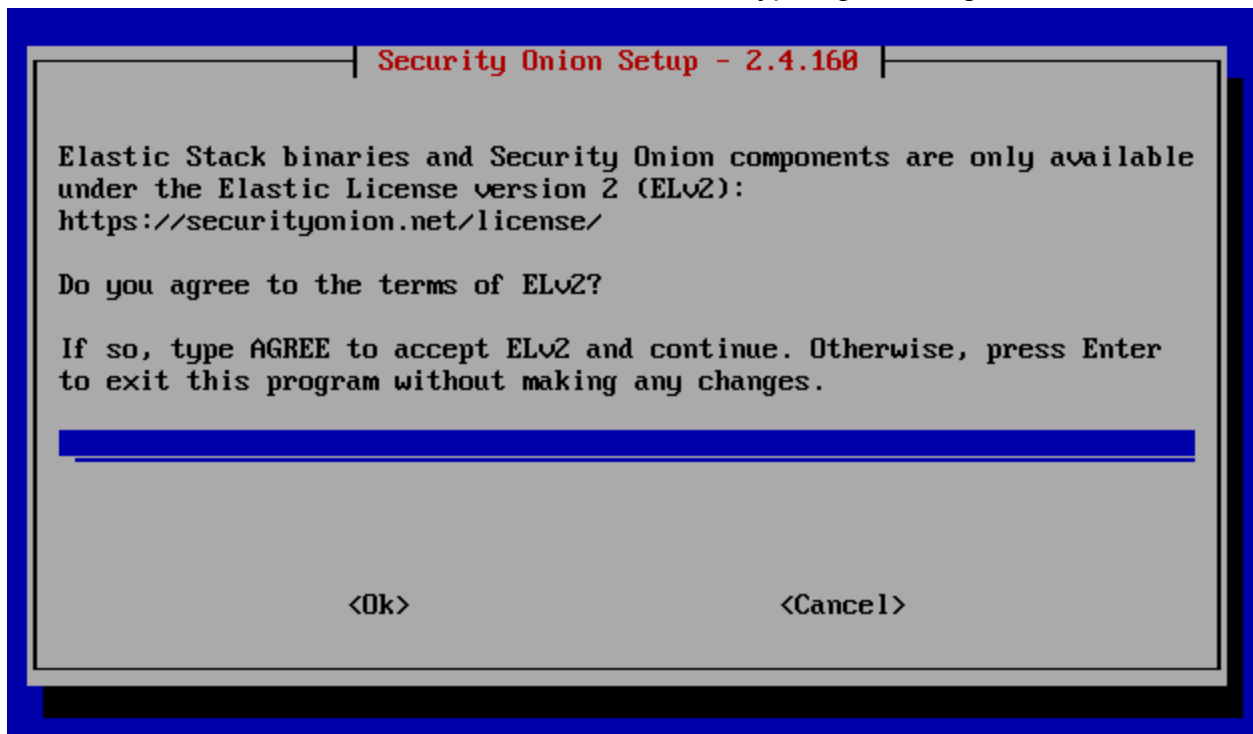
After selecting distributed, we are prompted with 2 options, since we have no other nodes setup or configured yet, we need to do a new deployment so the rest of the nodes we deploy like sensors, forwarders, etc can join to this node.



After proceeding with New deployment we are prompted to select the type of manager, I am going to be using the "MANAGER" option as it is recommend for most users.

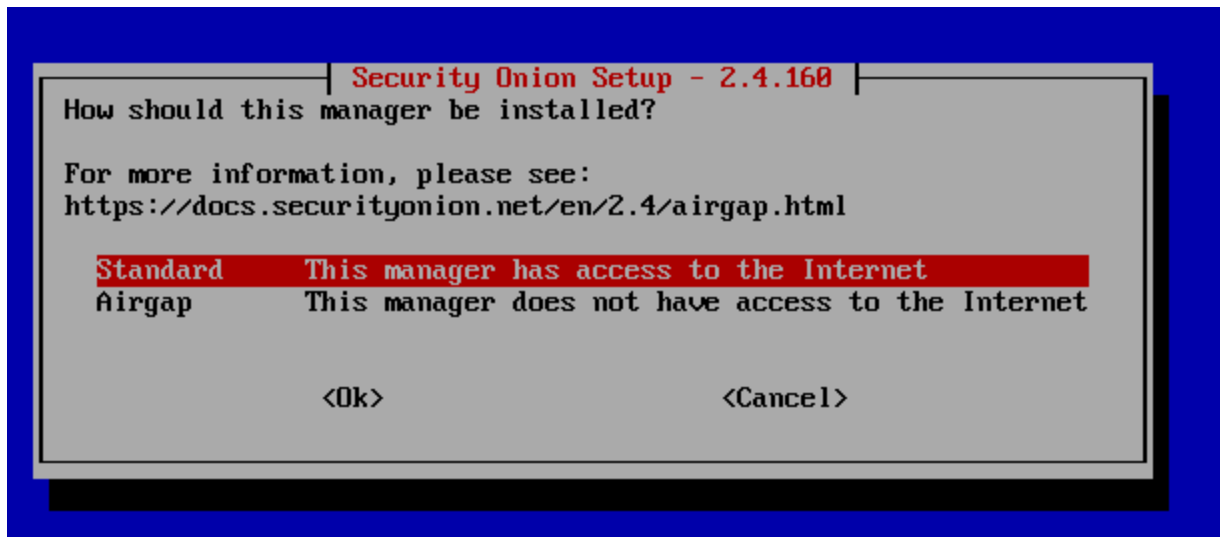


After that we will be hit with a box where we have to type agree to agree to the terms;

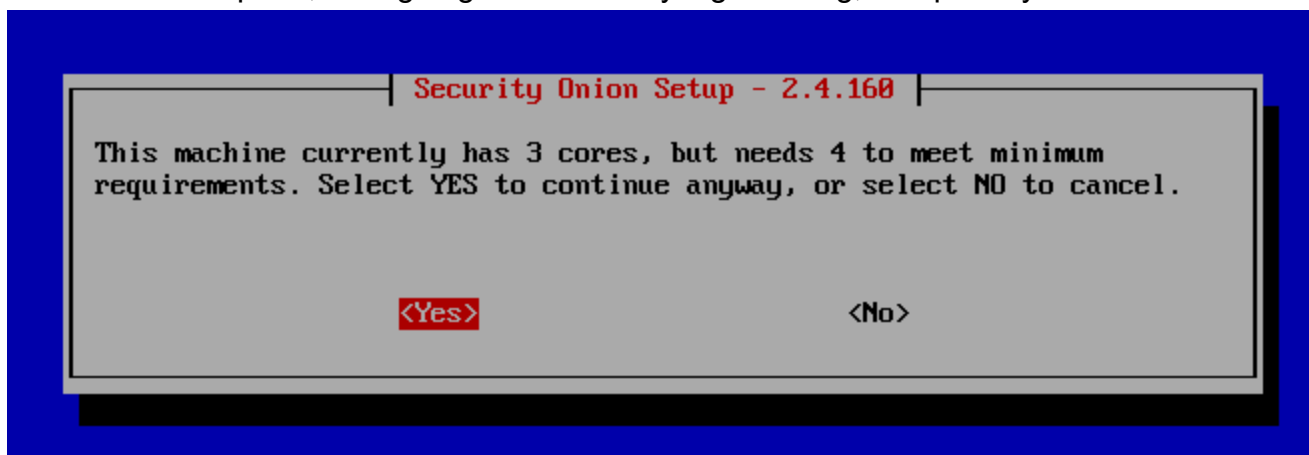


After agreeing to the license we need to choose if this machine is airgapped, or standard (Can be accessed from the internet), so the sake of this lab and because it's on my home network I am going to do airgap, but if you we're doing this in a organization setting you would wanna look into standard since your manager should be in the DMZ between your agents (who are at

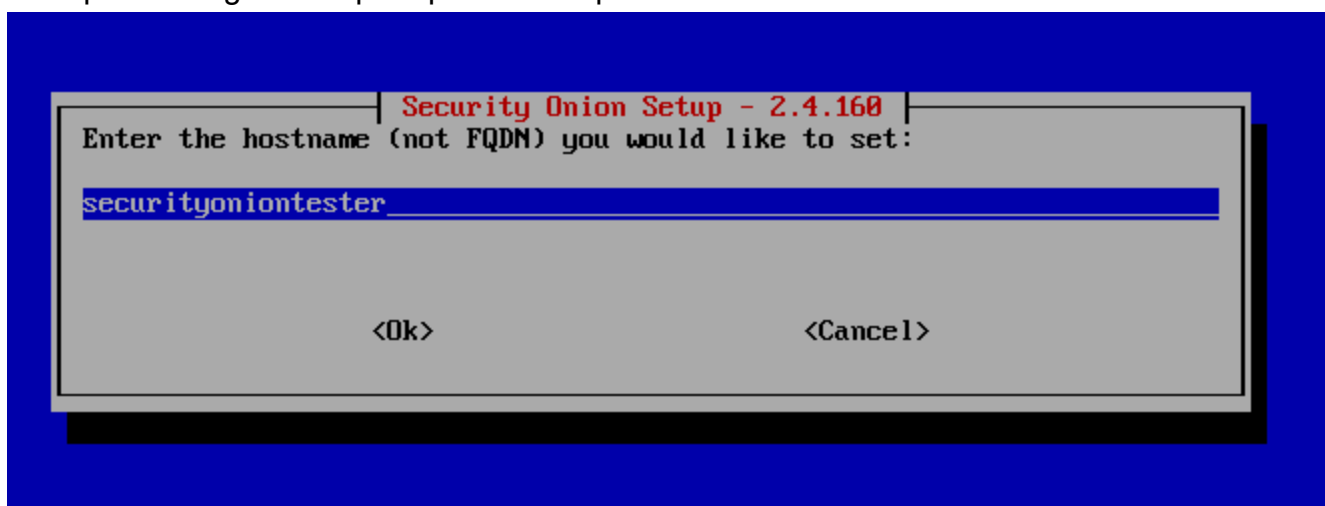
home, or not in office) and the elasticsearch storage instances behind the scenes



After proceeding, we are hit with a warning telling us we are missing a core, since my machine isn't a nasa computer, I am going to do the only logical thing, and press yes

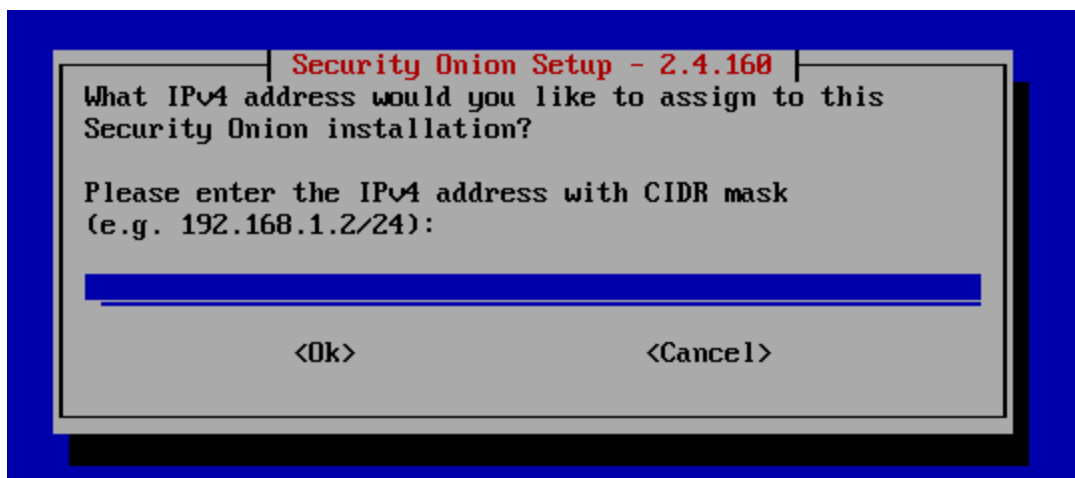
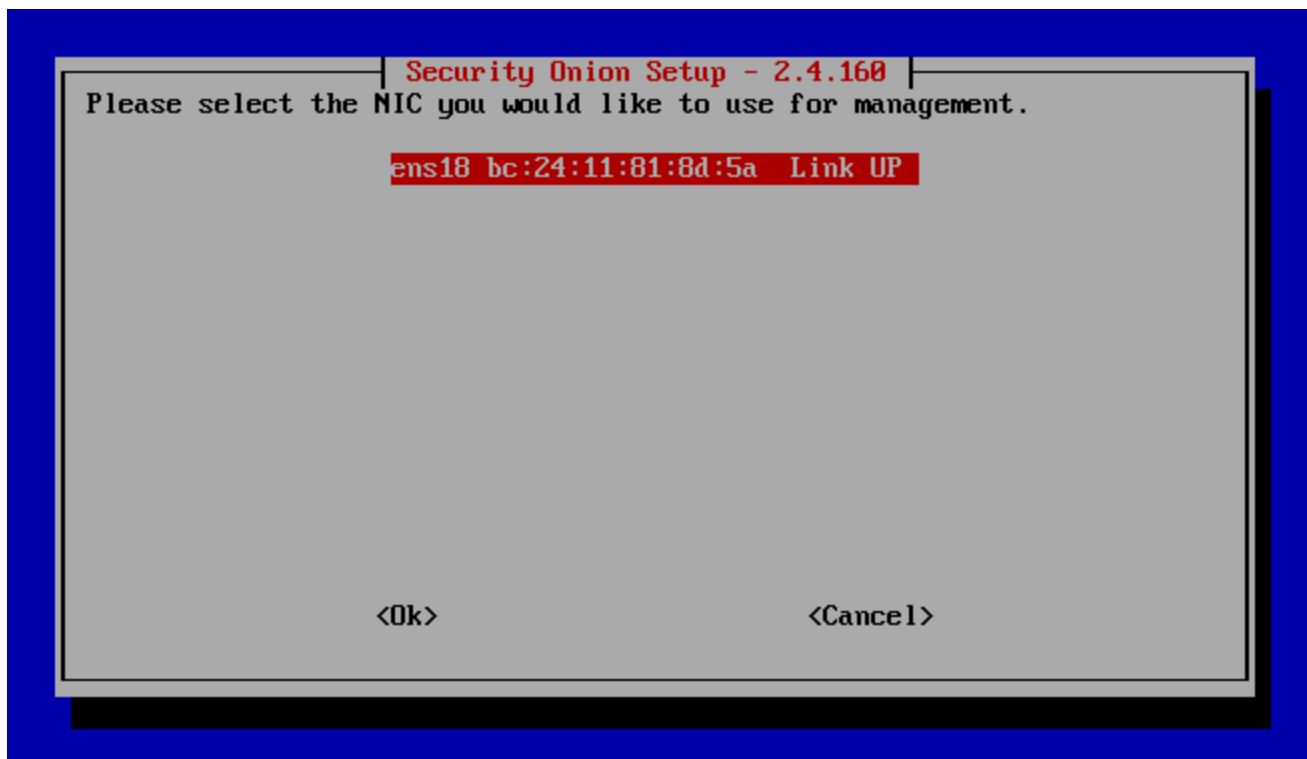


After proceeding we are prompted to setup our hostname



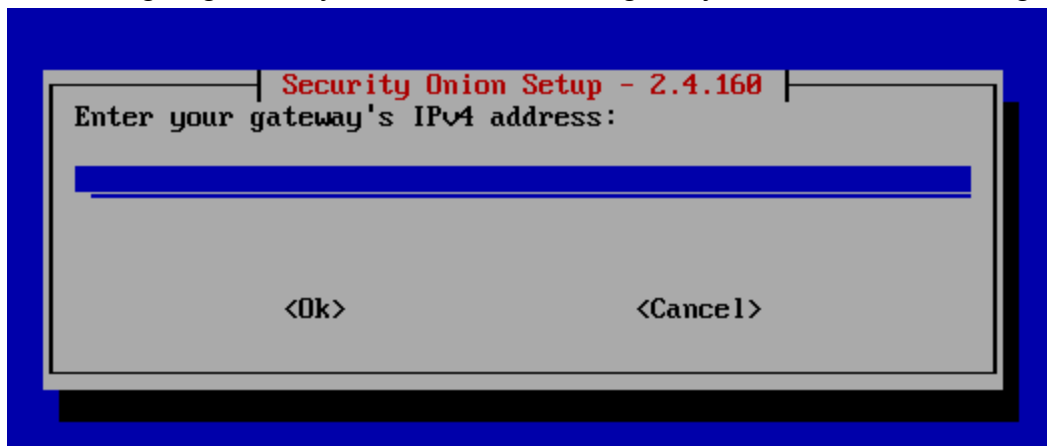
Now we need to configure out NIC for management interface; So select your NIC, and we are going to click the static option to assign the manager a static IP;



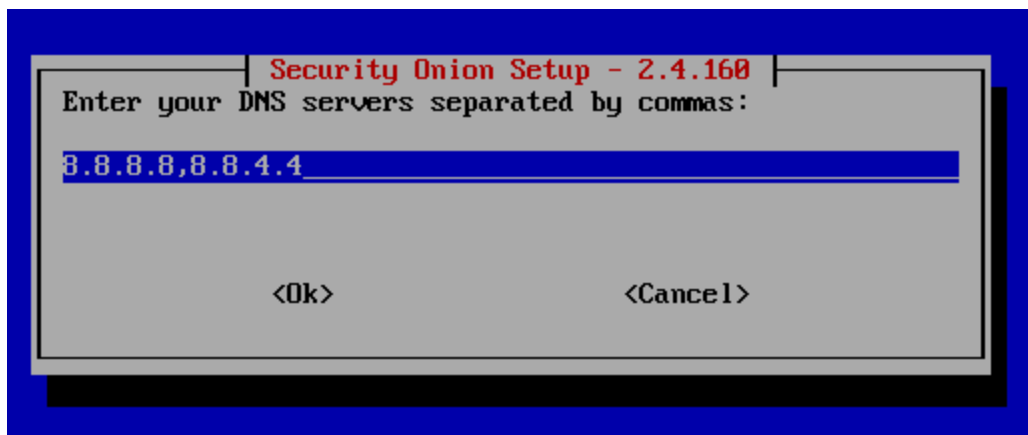


I am going to be giving the interface the IP of 10.0.0.120/24

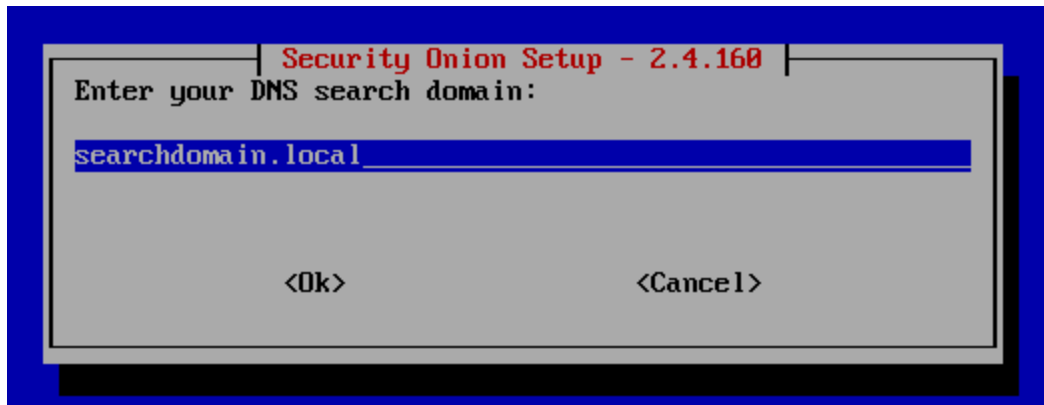
After assigning the IP you are asked to assigned your networks default gateway



Then nameservers, and since this is my home environment I am going to be leaving them as the defaults;



After we need to setup the DNS



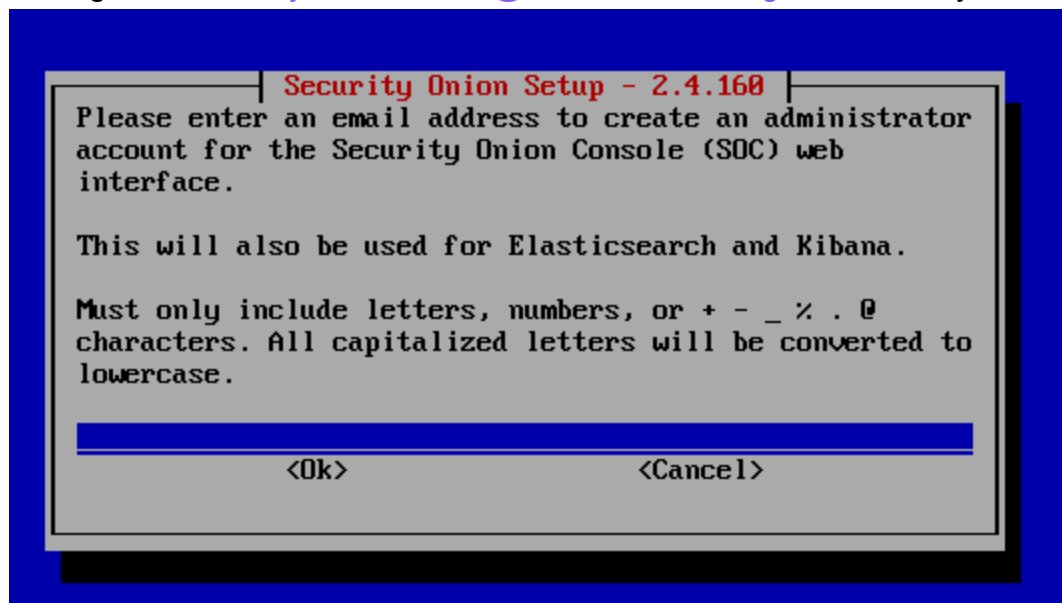
I am going to be setting mine to somanagerdev.local

After proceeding you will be prompted to use the default docker IP ranges, for the sake of this lab I am going to be selecting yes

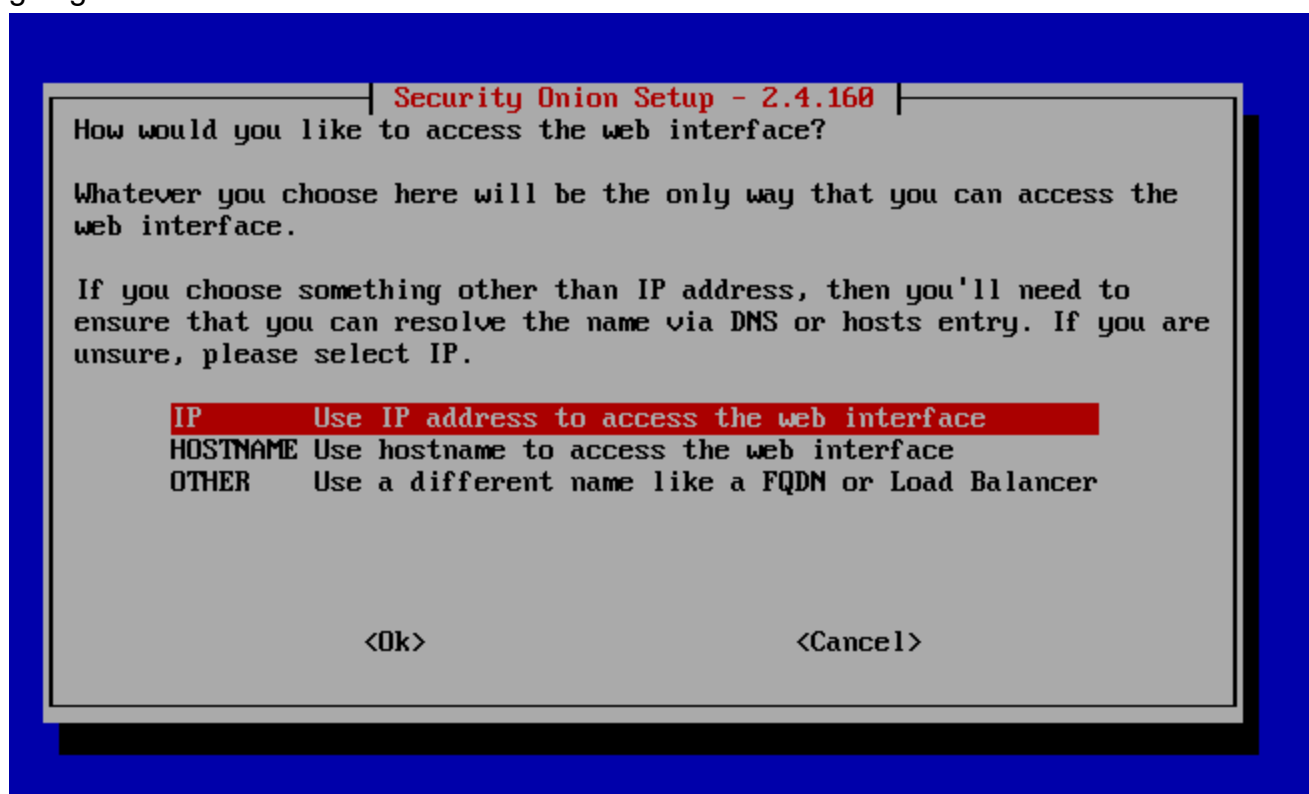


After setting the docker IP ranges, you will be prompted to enter a email & pass for the

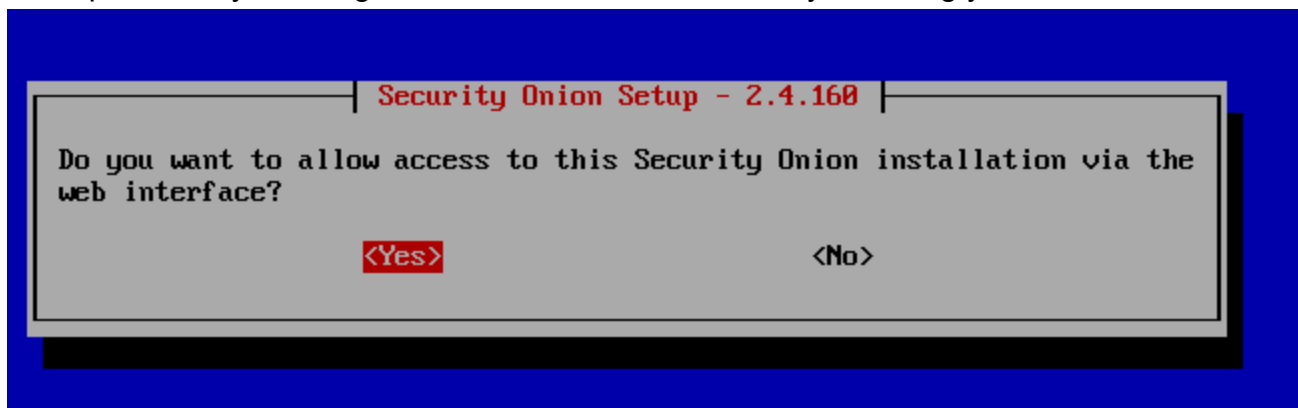
managers interface [jonah.dacosta@dacostaconsulting.ca](mailto:jonah.dacosta@dacostaconsulting.ca) & securityonion are what I am using



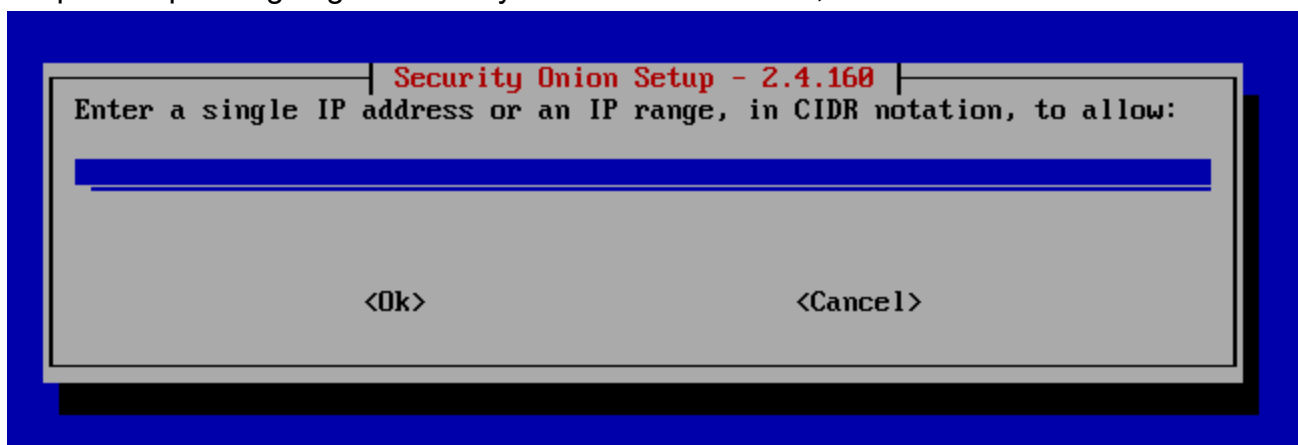
After that you will be prompted to select how you want the web interface to be accessed, I am going to use IP to access the web interface



Then proceed by allowing the interface to be accessed by selecting yes;



After you will be prompted to put a range of IP(s) or singular Ip to access the web interface for simple setup I am going to allow my whole home network;



Then after selecting Ok, you are given a summary of everything you have done, review what is there and if you are happy select "Yes" to proceed with the installation

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

Security Onion Version: 2.4.160  
Node Type: MANAGER  
Hostname: securityoniontester  
Airgap: True  
Network: STATIC  
Management NIC: ens18  
Management IP: 10.0.0.120  
Gateway: 10.0.0.1  
DNS: 8.8.8.8 8.8.4.4  
DNS Domain: somanagerdev.local  
Proxy: N/A  
Allowed IP or Subnet: 10.0.0.0/24  
Web User: jonah.dacosta@dacostaconsulting.ca

Press the TAB key to select yes or no.

<Yes>

<No>

After selecting yes, the backend will begin installing, give it some time this can take a bit

After the installation is complete you should see this;

Security Onion Setup - 2.4.160

MANAGER setup is now complete!

Access the Security Onion Console (SOC) web interface by navigating to:  
<https://10.0.0.120>

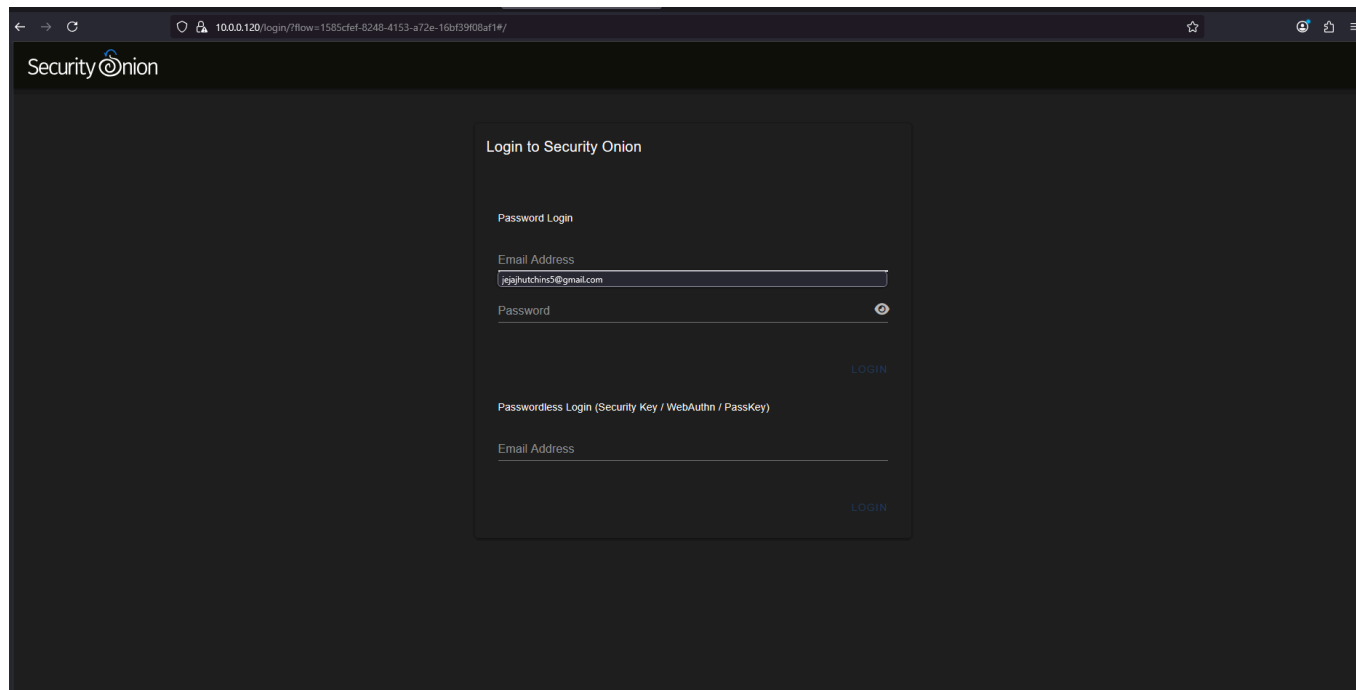
Then login with the following username and password.

SOC Username: jonah.dacosta@dacostaconsulting.ca  
SOC Password: Use the password that was entered during setup

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

<Ok>

And if we visit the IP provided in the summary we are served with the login page;



Ok so once we logged in we can verify everything is correct, and now we must move onto deploying the following

Please move on to the next step [Forward Nodes - Security Onion Distributed Installation](#)