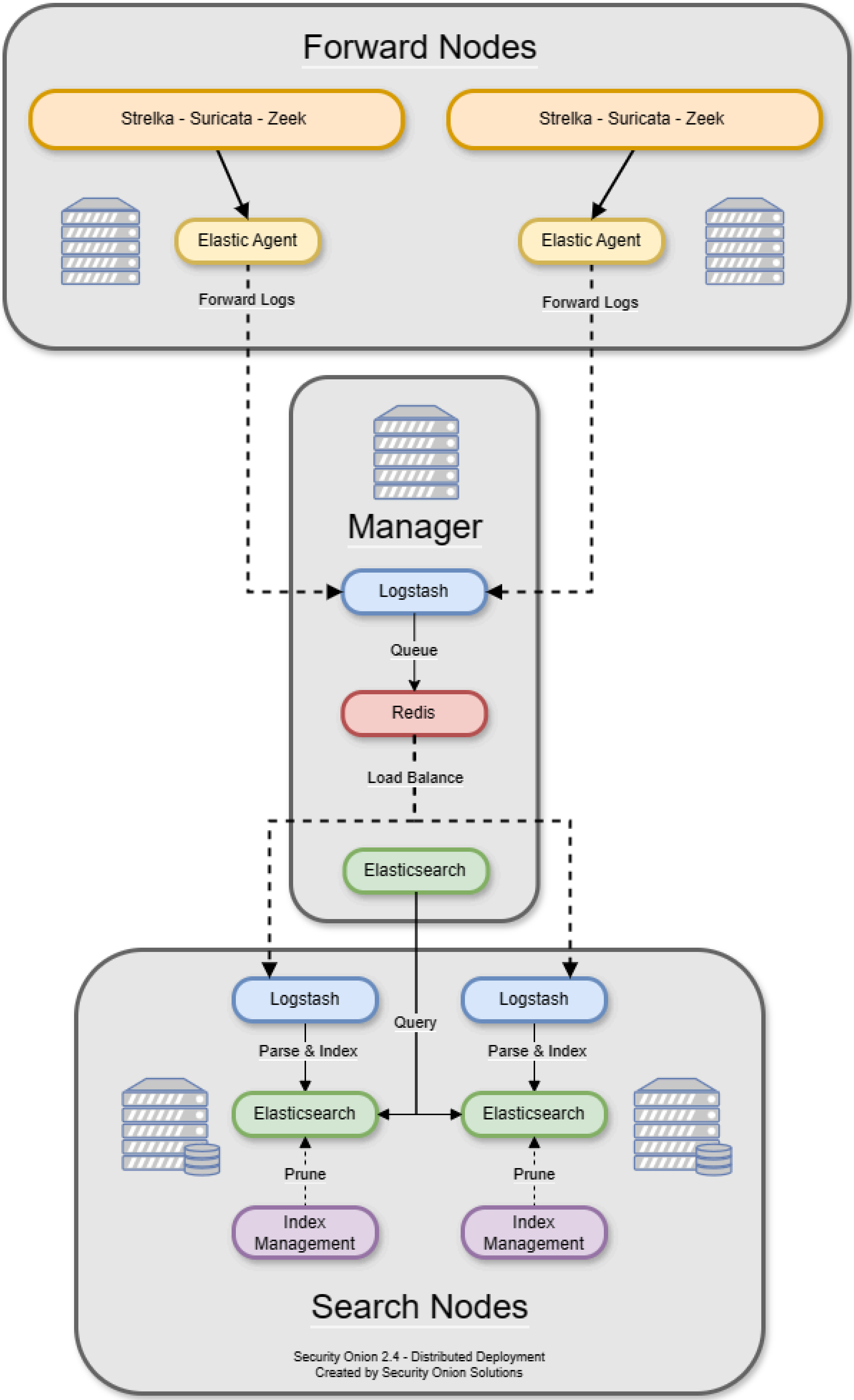
Forward Nodes - Security Onion Distributed Installation

8/1/2025 - *Security Onion 2.4.160*

So based on the architecture we have officially setup our manager node, now we need to setup out forward nodes which will be sending information to the manager then the search nodes. These forward nodes include sensors, agents, etc. Since agents are done from the Kibana menu which we already did in the manager installation we can deploy separate fleet servers for different machines, companies & groups of people.

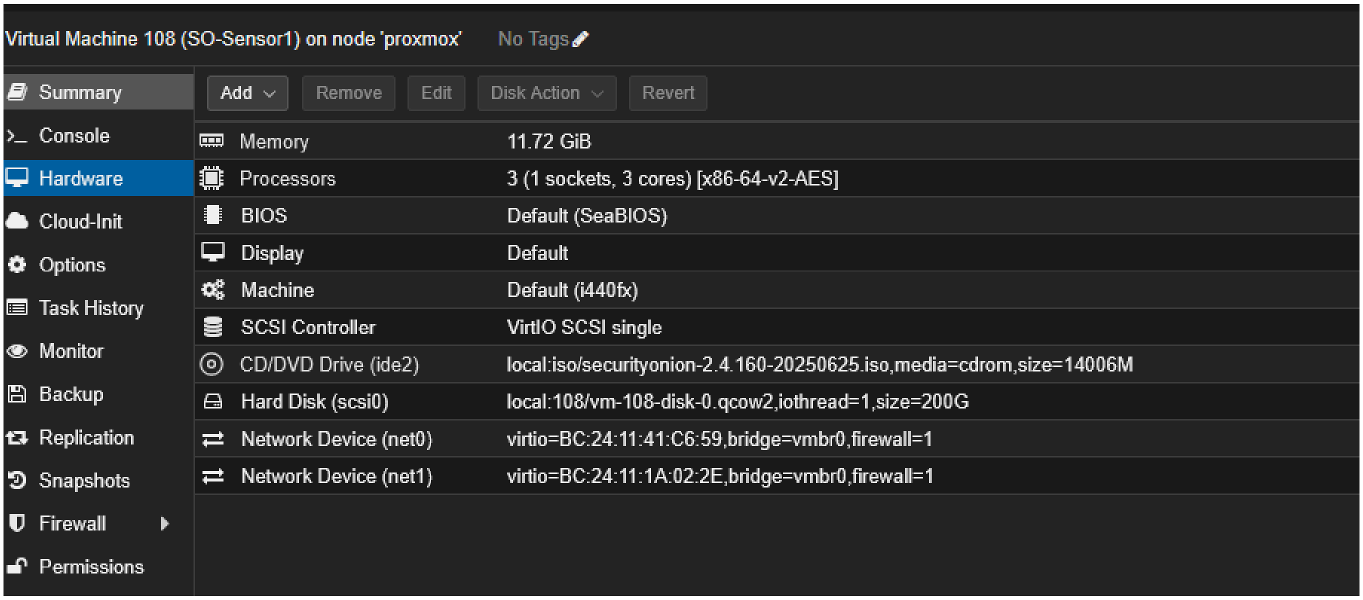

Forward Nodes
Strelka - Suricata - Zeek
Strelka - Suricata - Zeek
Elastic Agent
Elastic Agent
Forward Logs
Forward Logs
Manager
Logstash
Queue
Redis
Load Balance
Elasticsearch
Logstash
Logstash
Query
Parse & Index
Parse & Index
Elasticsearch
Elasticsearch
Prune
Prune
Index Management
Index Management
Search Nodes
Security Onion 2.4 - Distributed Deployment
Created by Security Onion Solutions

Step 1: Creating The Node VM & Preparing the ISO

Create your VM using the Security Onion ISO, here Machine Requirements is a photo of the required resources needed per application, since we have deployed the manager node and we are now setting up the sensor we are going to be creating a VM with 3 cores & 10 GBs of ram.

This sensor will be sending network traffic from the network to Security onion to be analyzed and processed.

Since we are deploying a network sniffing device like Suricata or zeek we need 2 NICs on the device to ensure one to communicate with the manager and the other for network monitoring (in a actual organization environment this would be connected to a SPAN port on a switch which has all network traffic being mirrored to that port).

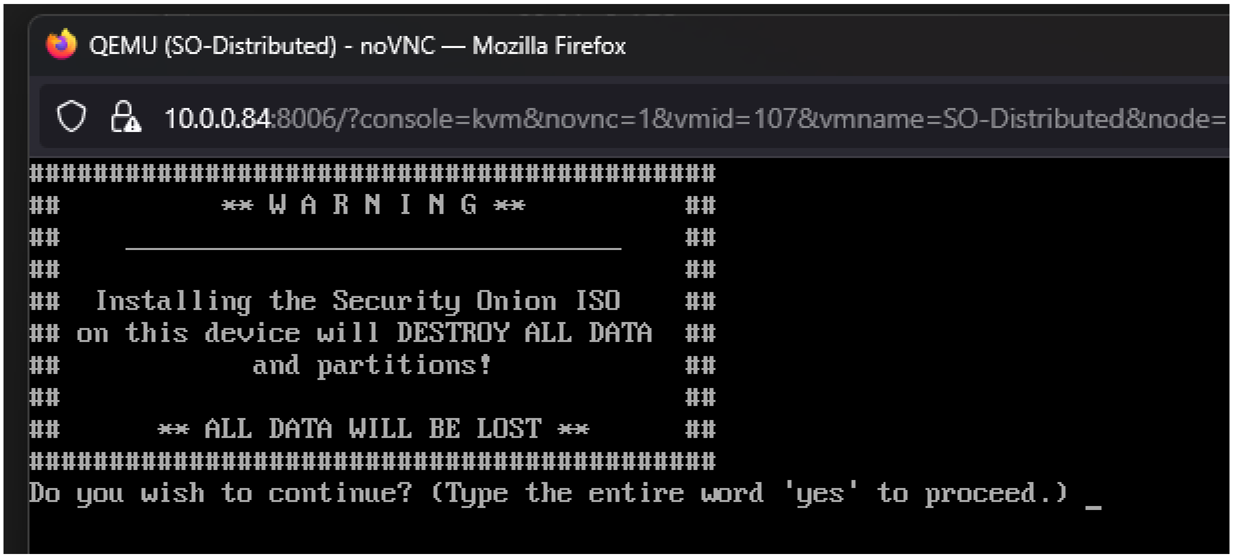


Virtual Machine 108 (SO-Sensor1) on node 'proxmox'

Memory	11.72 GiB
Processors	3 (1 sockets, 3 cores) [x86-64-v2-AES]
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	local:iso/securityonion-2.4.160-20250625.iso,media=cdrom,size=14006M
Hard Disk (scsi0)	local:108/vm-108-disk-0.qcow2,iothread=1,size=200G
Network Device (net0)	virtio=BC:24:11:41:C6:59,bridge=vmbr0,firewall=1
Network Device (net1)	virtio=BC:24:11:1A:02:2E,bridge=vmbr0,firewall=1

Once you have created the VM make sure you start it

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;



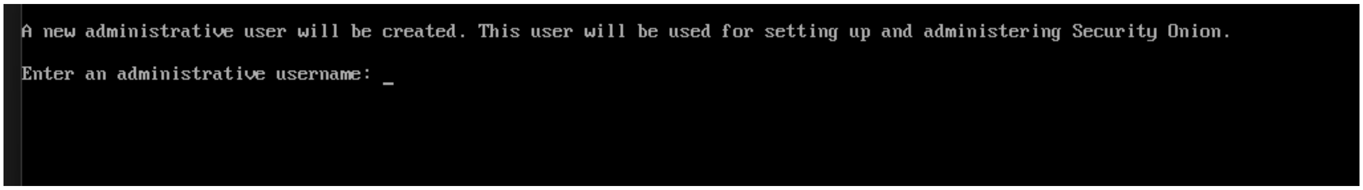
QEMU (SO-Distributed) - noVNC — Mozilla Firefox

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'

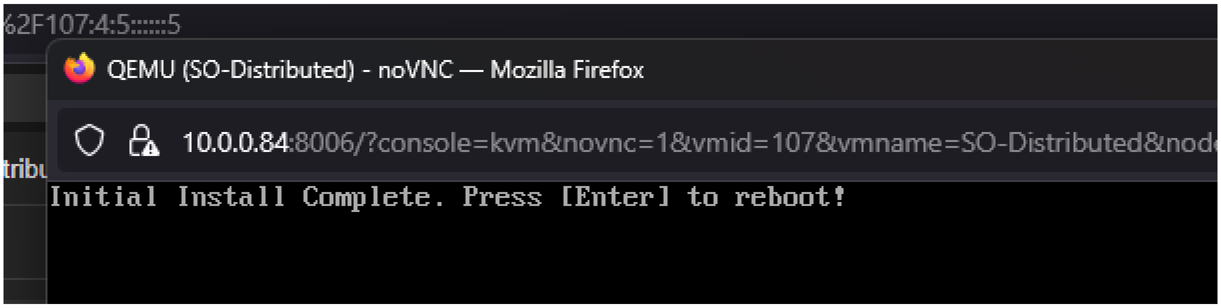
After proceeding you will be required to enter a administrator username & pass, for the sake of the lab I am going to keep it very simple and provide the username & pass ***securityonion:securityonion***



```
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;

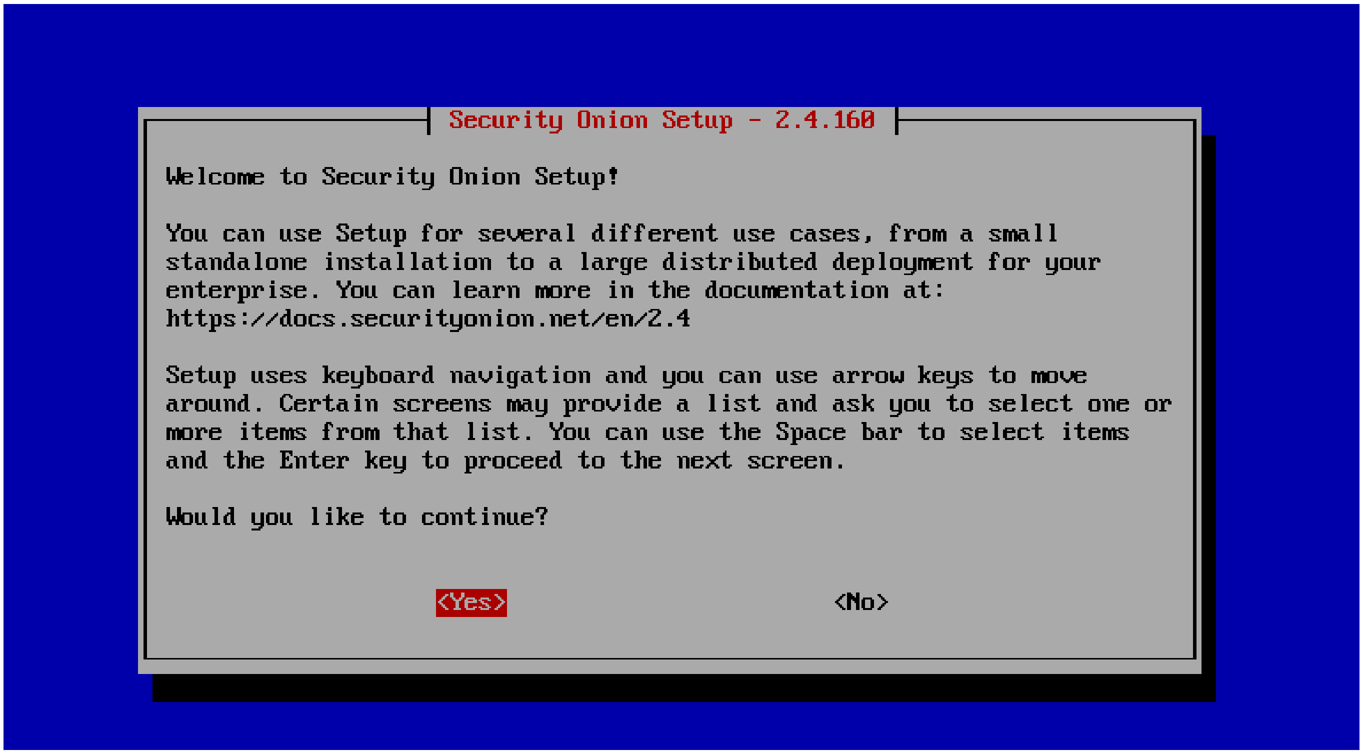

%2F107:4:5:::::5
QEMU (SO-Distributed) - noVNC — Mozilla Firefox
10.0.0.84:8006/?console=kvm&novnc=1&vmid=107&vmname=SO-Distributed&nod
tribu

```
Initial Install Complete. Press [Enter] to reboot!
```

So hit enter and carry on with the installation;

Step 2: Installing & Configuring The Forward Node

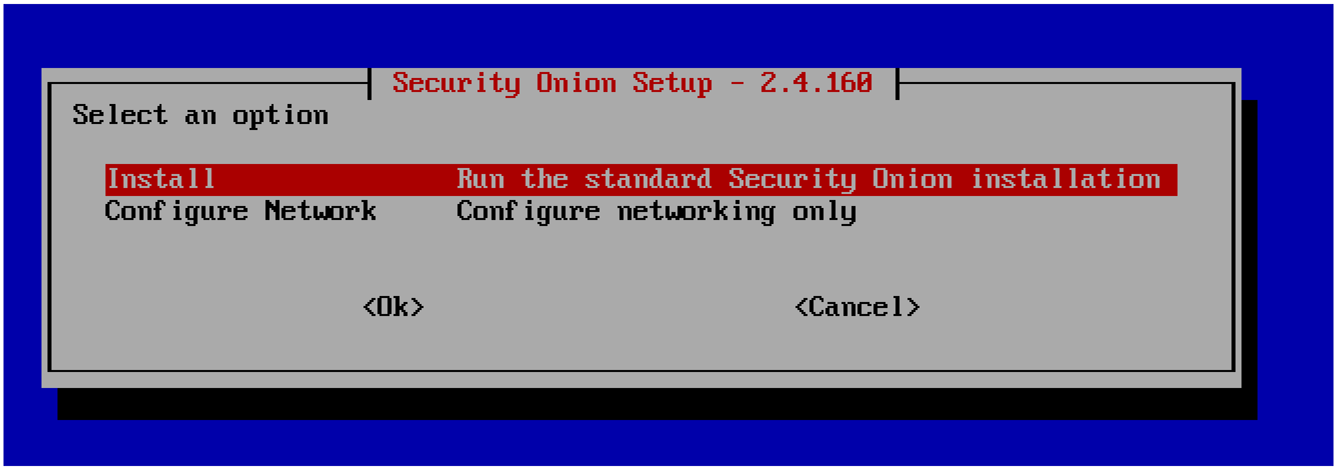
After the machine reboots, you will be prompted to enter you user & pass you previously entered.
After you have entered the credentials, you will see the configuration screen pop up.



```
Security Onion Setup - 2.4.160

Welcome to Security Onion Setup!

You can use Setup for several different use cases, from a small
standalone installation to a large distributed deployment for your
enterprise. You can learn more in the documentation at:
https://docs.securityonion.net/en/2.4

Setup uses keyboard navigation and you can use arrow keys to move
around. Certain screens may provide a list and ask you to select one or
more items from that list. You can use the Space bar to select items
and the Enter key to proceed to the next screen.

Would you like to continue?

                <Yes>                        <No>
```

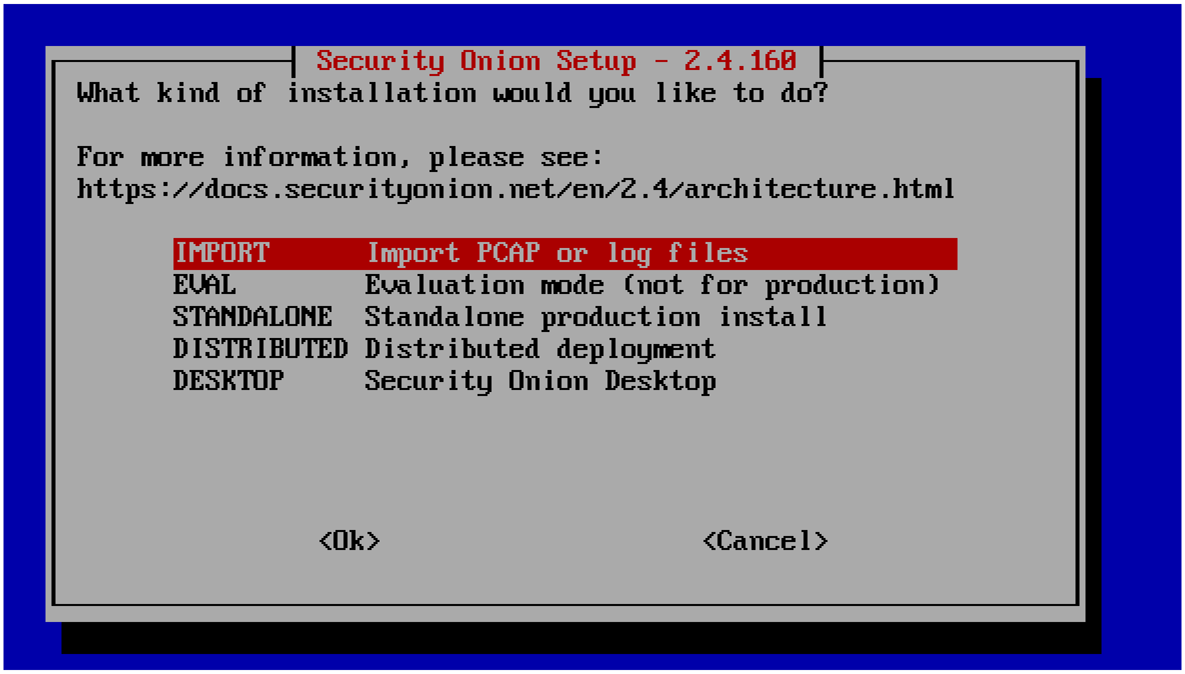
This is where we begin to configure security onion; so obviously we wish to continue so I will be selecting "yes"

After selecting yes, you will be prompted on a screen with 2 options, this screen gives you the option to do the full install / configuration or just setup networking first. I'm going to be doing the install option as I want to do everything.



```
Security Onion Setup - 2.4.160
Select an option

  Install               Run the standard Security Onion installation
  Configure Network     Configure networking only

            <Ok>                      <Cancel>
```

After selecting install, you are prompted with what kind of installation you want to do

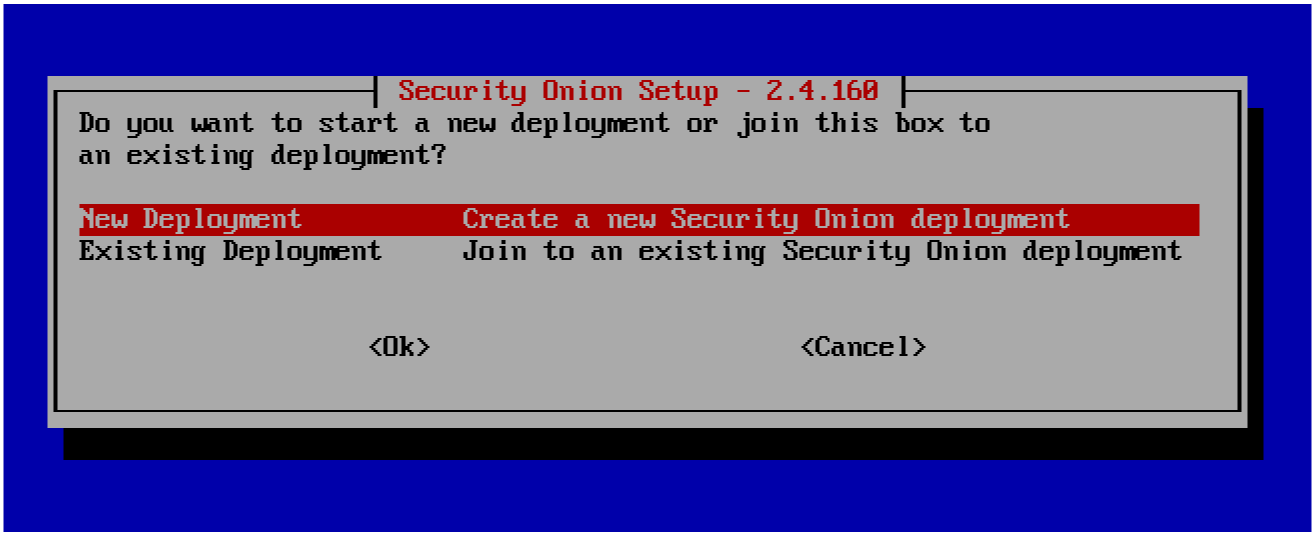


```
Security Onion Setup - 2.4.160
What kind of installation would you like to do?

For more information, please see:
https://docs.securityonion.net/en/2.4/architecture.html

       IMPORT      Import PCAP or log files
       EVAL        Evaluation mode (not for production)
       STANDALONE  Standalone production install
       DISTRIBUTED Distributed deployment
       DESKTOP     Security Onion Desktop

             <Ok>                    <Cancel>
```

For more information regarding the different kinds of installs please visit; https://docs.securityonion.net/en/2.4/architecture.html

Since we have previously installed a manager using the distributed type, we are going to be selecting that type

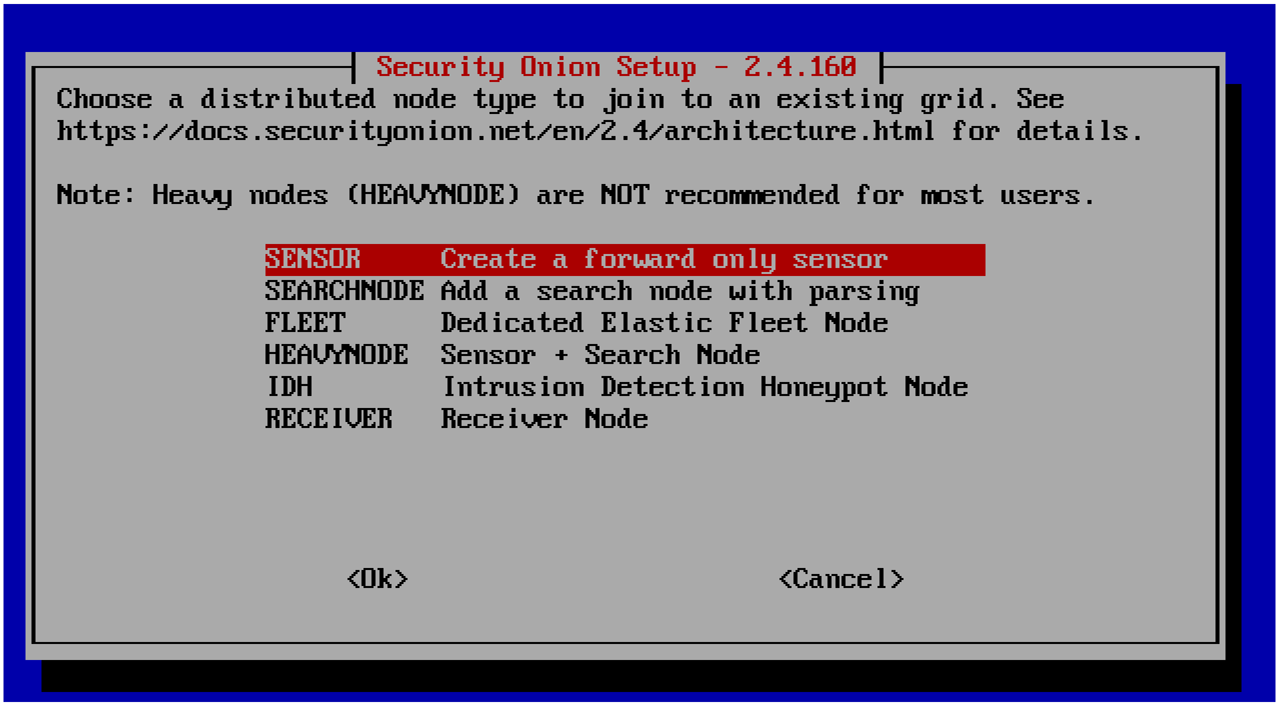
After you will receive a pop up asking what kind of deployment you want to do, since we already created the manager we are going to doing the existing deployment again to connect our Sensor or whatever we decide to setup to the manager



```
Security Onion Setup - 2.4.160
Do you want to start a new deployment or join this box to
an existing deployment?

New Deployment          Create a new Security Onion deployment
Existing Deployment     Join to an existing Security Onion deployment

             <Ok>                         <Cancel>
```

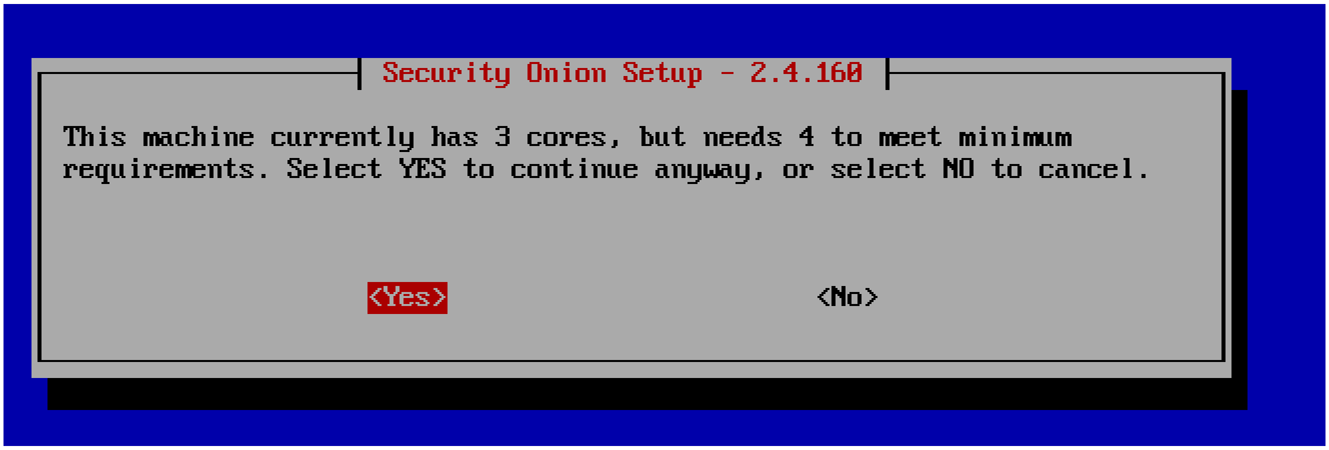
After you selected existing deployment you are going to be prompted with what you want to deploy a senser we want to select the sensor option, but notice how there are a lot of different options for us to use, we can deploy another elastic fleet server, IDH (Intrusion Detection

Honeypot), more backend storage by doing a search node, and a receiver node.



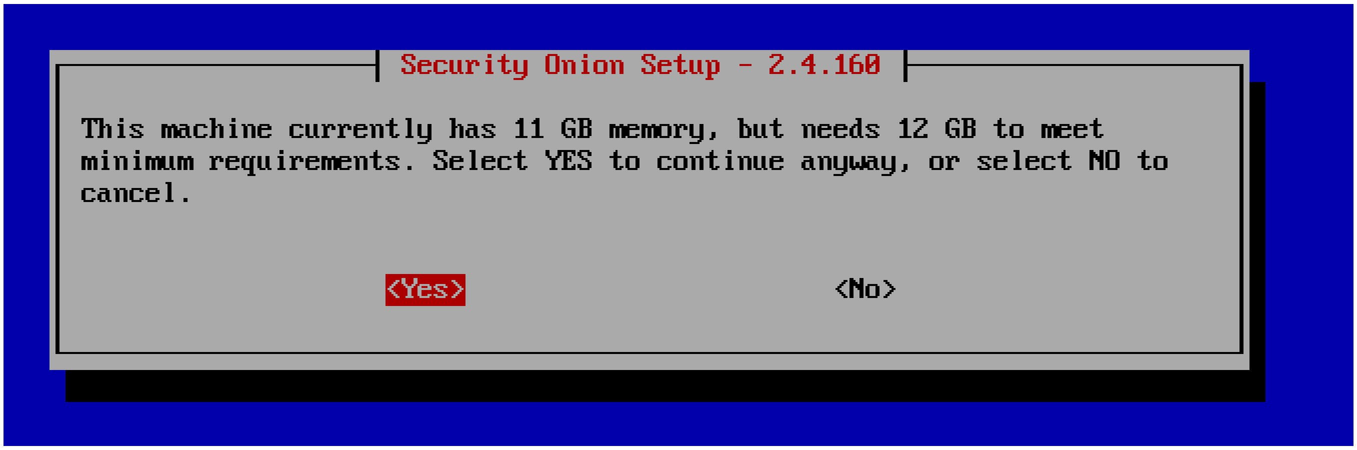
```
Security Onion Setup - 2.4.160

Choose a distributed node type to join to an existing grid. See
https://docs.securityonion.net/en/2.4/architecture.html for details.

Note: Heavy nodes (HEAVYNODE) are NOT recommended for most users.

          SENSOR      Create a forward only sensor
          SEARCHNODE  Add a search node with parsing
          FLEET       Dedicated Elastic Fleet Node
          HEAVYNODE   Sensor + Search Node
          IDH         Intrusion Detection Honeypot Node
          RECEIVER    Receiver Node

            <Ok>                    <Cancel>
```

After selecting the sensor I am prompted with this, since I don't have anymore cores available I will be selecting yes and ignoring the warning.



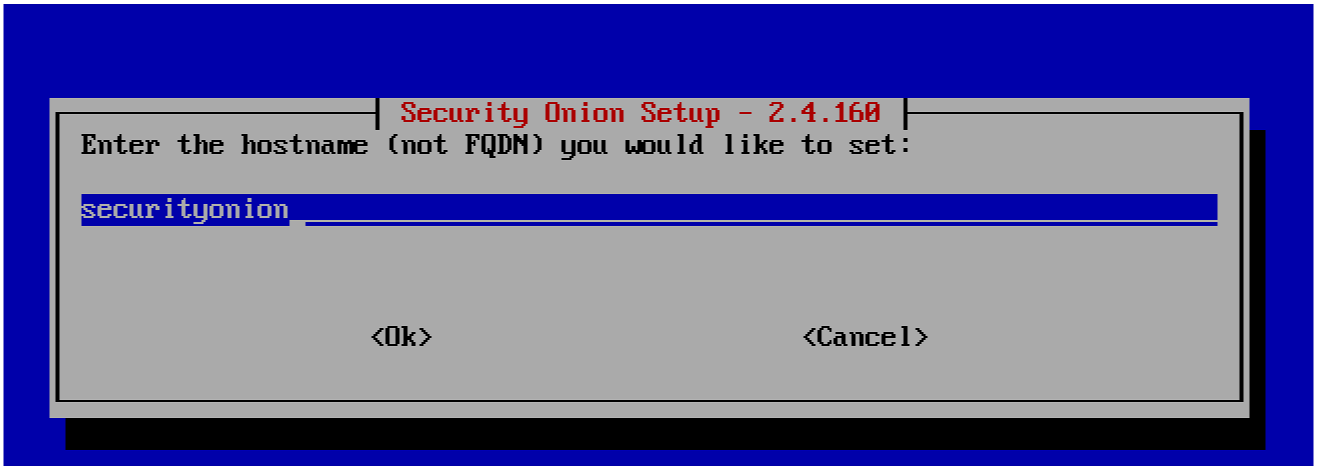
```
Security Onion Setup - 2.4.160

This machine currently has 3 cores, but needs 4 to meet minimum
requirements. Select YES to continue anyway, or select NO to cancel.

              <Yes>                   <No>
```

Same with the RAM



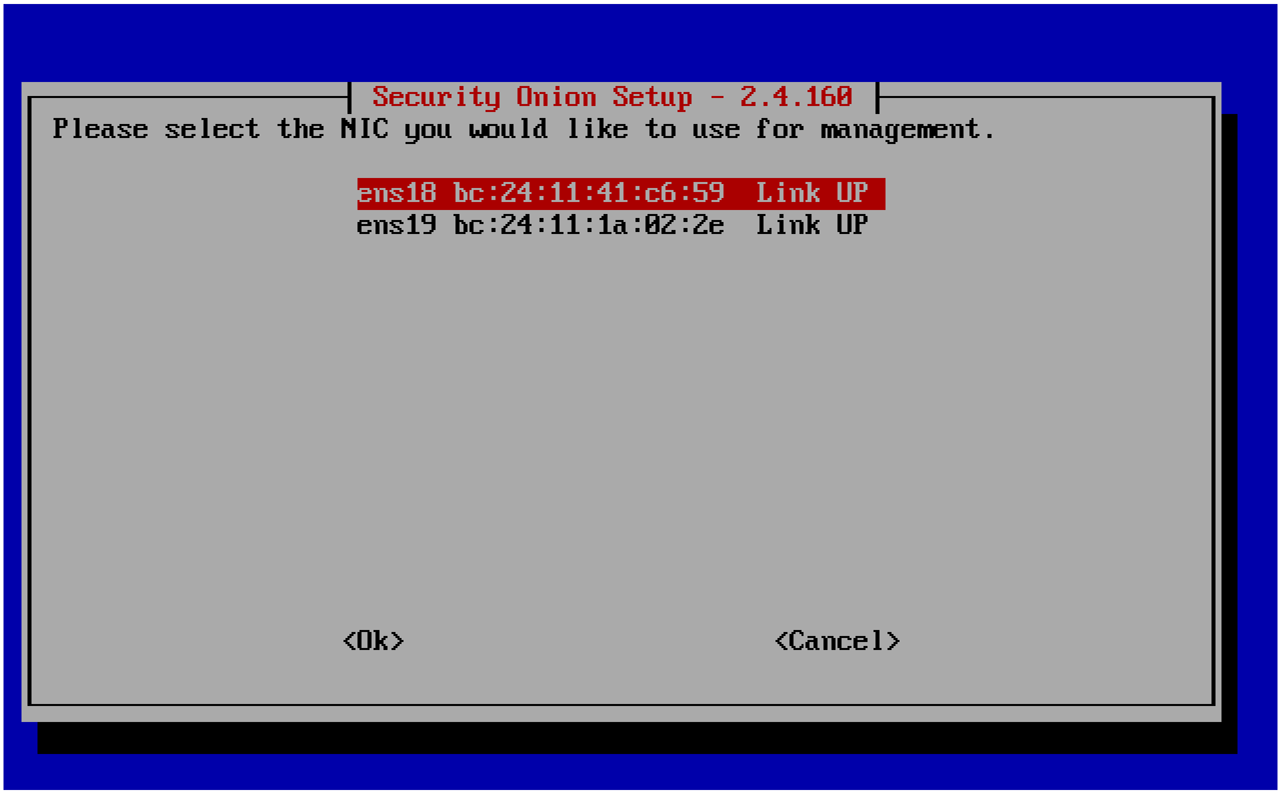
```
Security Onion Setup - 2.4.160

This machine currently has 11 GB memory, but needs 12 GB to meet
minimum requirements. Select YES to continue anyway, or select NO to
cancel.

              <Yes>                   <No>
```

After we will be prompted to set a hostname, I am going to set it as securityonionsensor1



```
Security Onion Setup - 2.4.160
Enter the hostname (not FQDN) you would like to set:

securityonion

        <Ok>                    <Cancel>
```

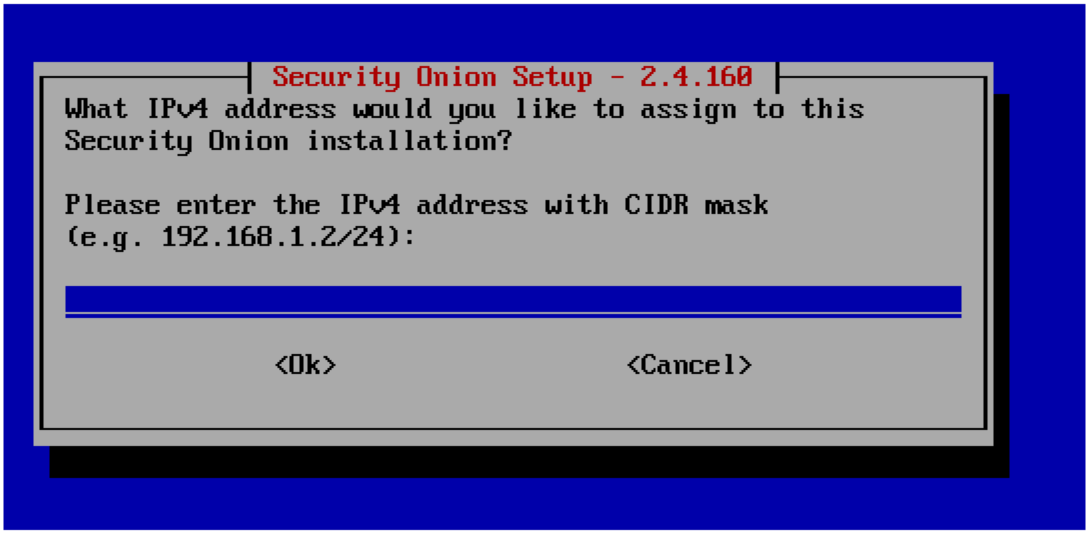
Now we need to configure our interfaces; I am going to use the ens18 interface for the management interface and assign it a static IP



```
Security Onion Setup - 2.4.160
Please select the NIC you would like to use for management.

           ens18 bc:24:11:41:c6:59  Link UP
           ens19 bc:24:11:1a:02:2e  Link UP

        <Ok>                    <Cancel>
```

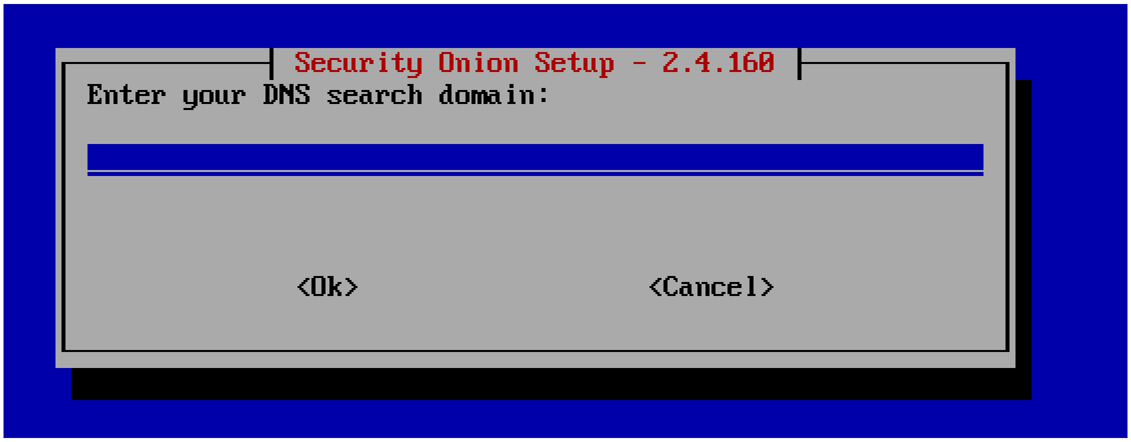
After selecting that interface and static, you will be prompted to enter the IP of the interface, as well as the default gateway and the name servers you want to use, I am going to leave the DNS servers as default and just specify my IP address and default gateway

10.0.0.121/24



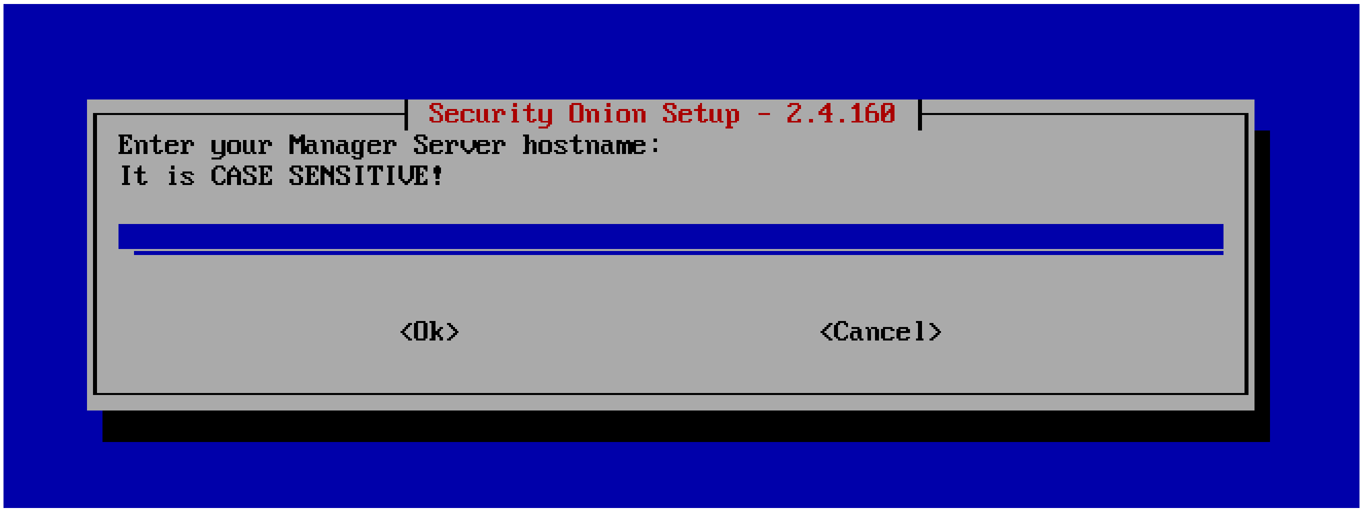
```
Security Onion Setup - 2.4.160
What IPv4 address would you like to assign to this
Security Onion installation?

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

After you need to assign the DNS name, I am just going to do sosenser1.local



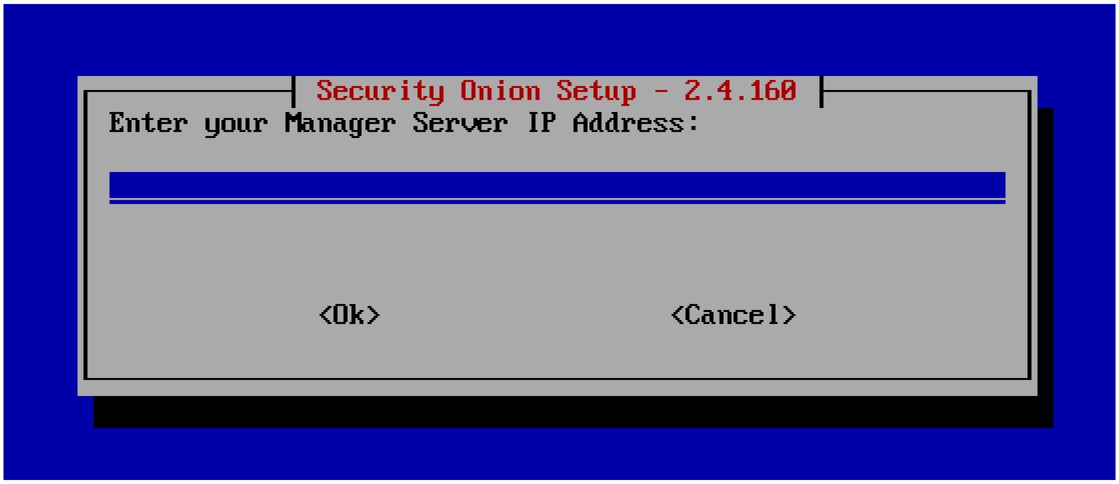
```
Security Onion Setup - 2.4.160
Enter your DNS search domain:
```

After setting your DNS name you are prompted to set your manager nodes hostname previously we set our managers hostname in Manager - Security Onion Distributed Installation as "securityoniontester"



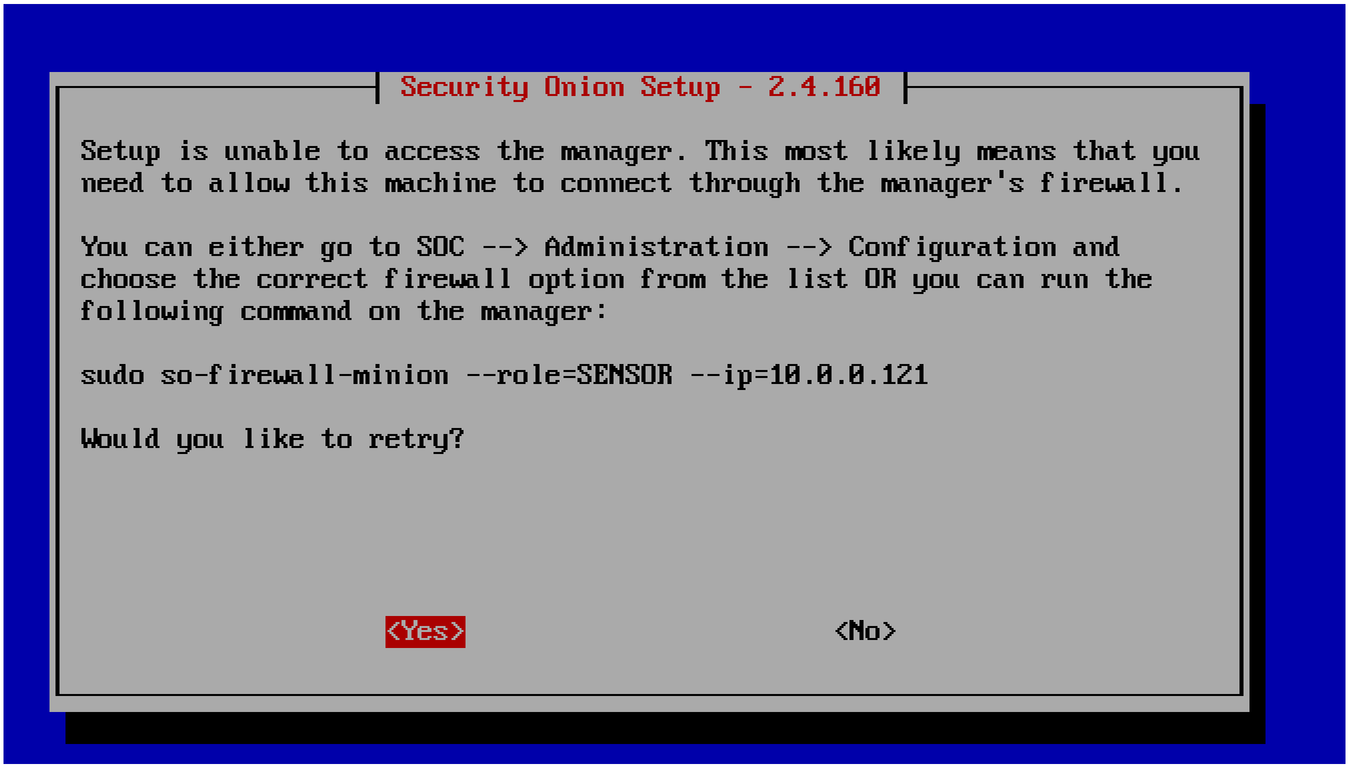
```
Security Onion Setup - 2.4.160
Enter your Manager Server hostname:
It is CASE SENSITIVE!
```

Then after enter the managers server Ip, in our case 10.0.0.200



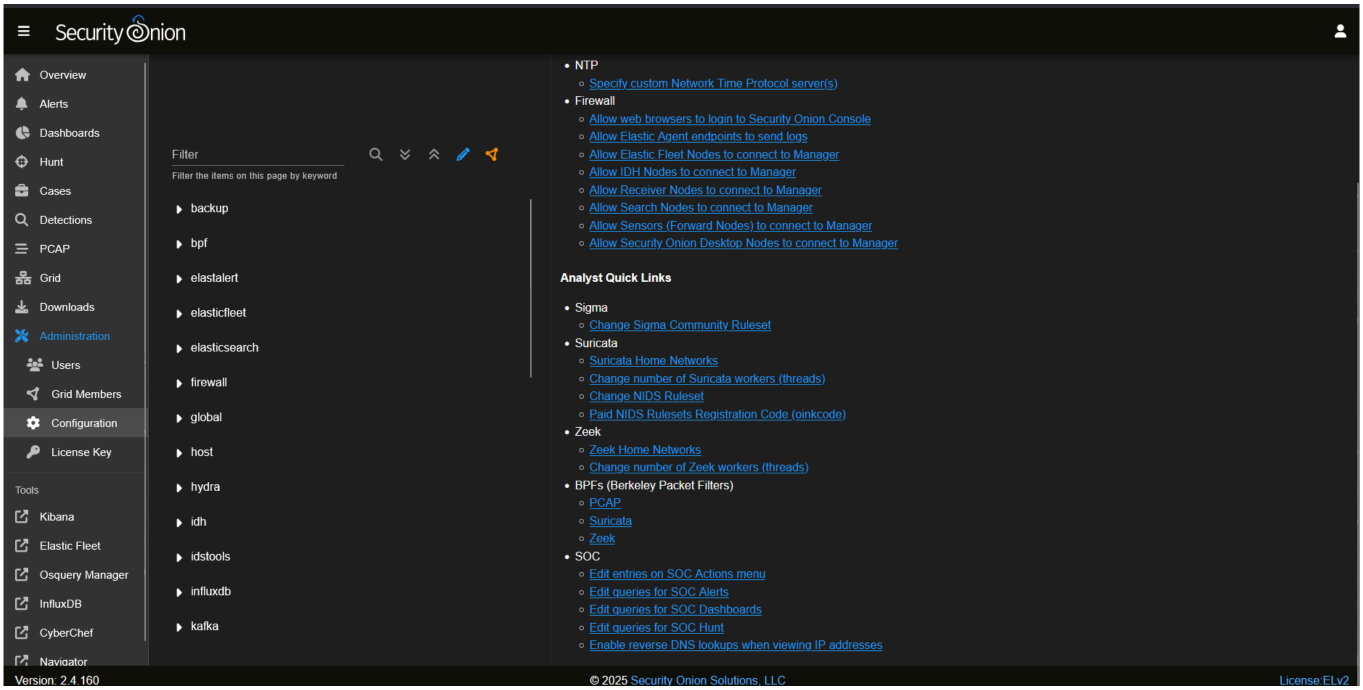
```
Security Onion Setup - 2.4.160
Enter your Manager Server IP Address:
```

So we actually got a error;



```
Security Onion Setup - 2.4.160

Setup is unable to access the manager. This most likely means that you
need to allow this machine to connect through the manager's firewall.

You can either go to SOC --> Administration --> Configuration and
choose the correct firewall option from the list OR you can run the
following command on the manager:

sudo so-firewall-minion --role=SENSOR --ip=10.0.0.121

Would you like to retry?
```

Although it seems like they provided a possible fix on how we can solve this; So heading over to the SOC web interface we can go to the administration bar on the left, then configuration



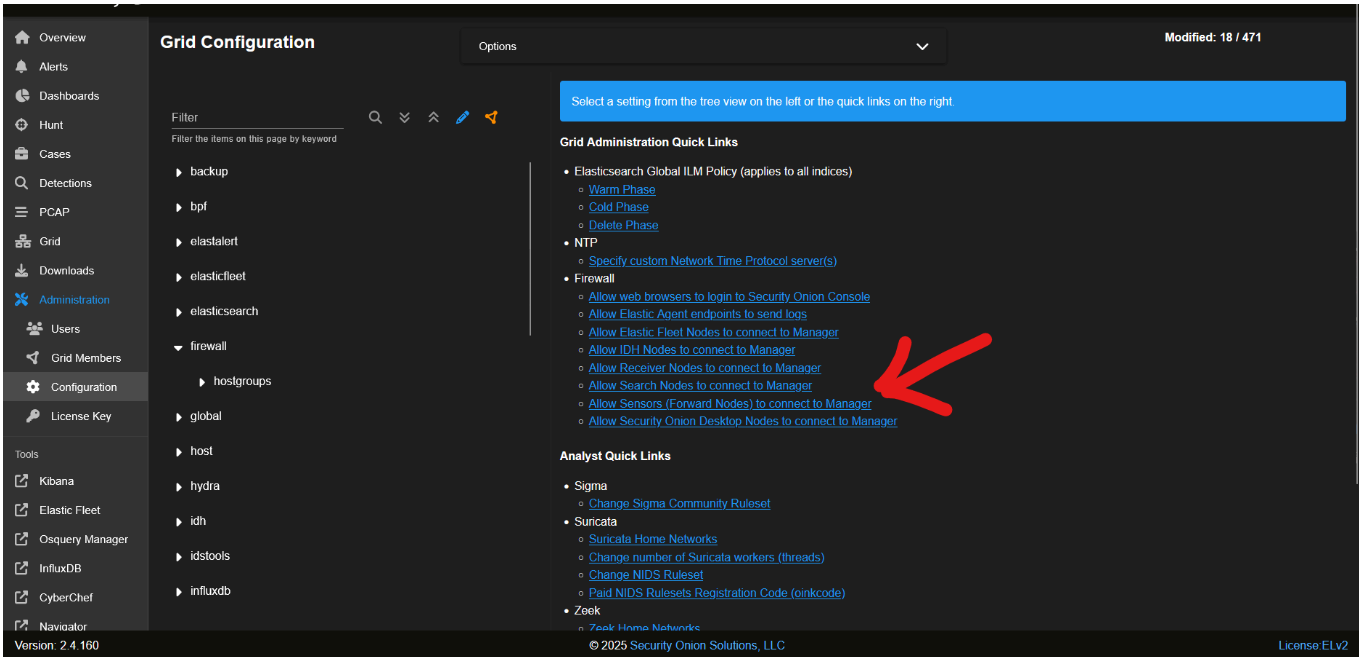
- NTP
  - Specify custom Network Time Protocol server(s)
- Firewall
  - Allow web browsers to login to Security Onion Console
  - Allow Elastic Agent endpoints to send logs
  - Allow Elastic Fleet Nodes to connect to Manager
  - Allow IDH Nodes to connect to Manager
  - Allow Receiver Nodes to connect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

Analyst Quick Links

- Sigma
  - Change Sigma Community Ruleset
- Suricata
  - Suricata Home Networks
  - Change number of Suricata workers (threads)
  - Change NIDS Ruleset
  - Paid NIDS Rulesets Registration Code (oinkcode)
- Zeek
  - Zeek Home Networks
  - Change number of Zeek workers (threads)
- BPFs (Berkeley Packet Filters)
  - PCAP
  - Suricata
  - Zeek
- SOC
  - Edit entries on SOC Actions menu
  - Edit queries for SOC Alerts
  - Edit queries for SOC Dashboards
  - Edit queries for SOC Hunt
  - Enable reverse DNS lookups when viewing IP addresses

Version: 2.4.160 © 2025 Security Onion Solutions, LLC License:ELv2

After we can click the firewall option and click on this option;



Grid Configuration

Modified: 18 / 471

Select a setting from the tree view on the left or the quick links on the right.

Grid Administration Quick Links

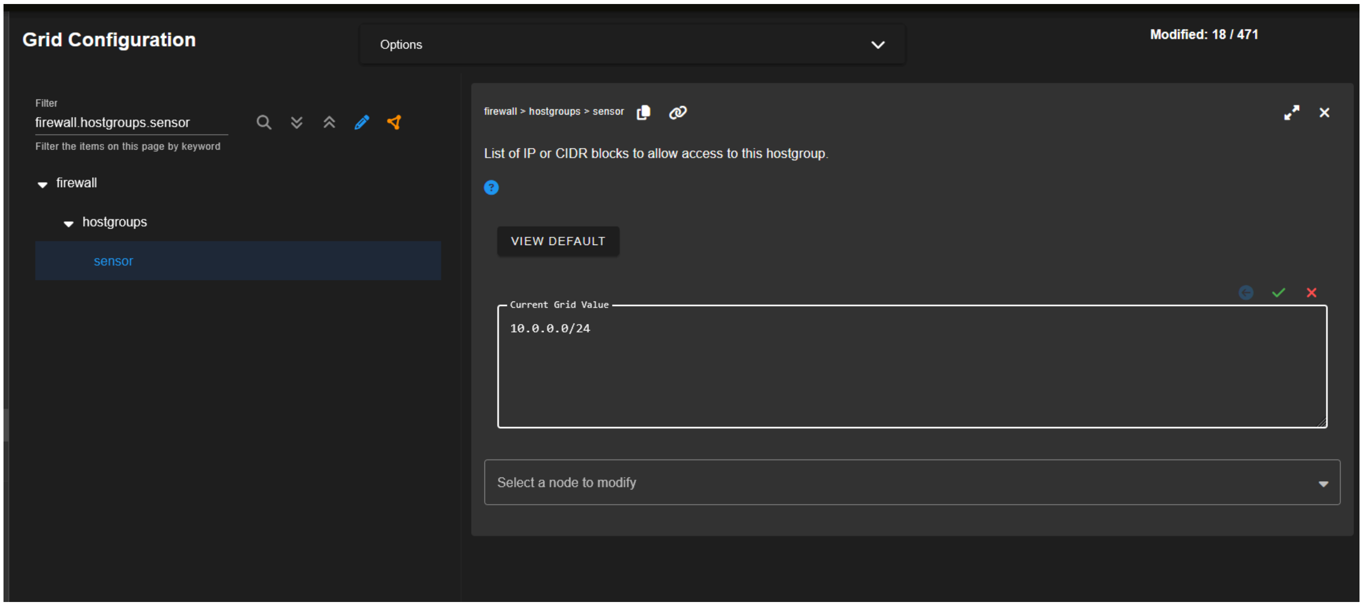
- Elasticsearch Global ILM Policy (applies to all indices)
  - Warm Phase
  - Cold Phase
  - Delete Phase
- NTP
  - Specify custom Network Time Protocol server(s)
- Firewall
  - Allow web browsers to login to Security Onion Console
  - Allow Elastic Agent endpoints to send logs
  - Allow Elastic Fleet 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
  - Allow Security Onion Desktop Nodes to connect to Manager

Analyst Quick Links

- Sigma
  - Change Sigma Community Ruleset
- Suricata
  - Suricata Home Networks
  - Change number of Suricata workers (threads)
  - Change NIDS Ruleset
  - Paid NIDS Rulesets Registration Code (oinkcode)
- Zeek
  - Zeek Home Networks

Version: 2.4.160 © 2025 Security Onion Solutions, LLC License:ELv2

In the configuration I am going to set the IP(s) of the forward nodes to be passed onto into the firewall, I am going to add 10.0.0.121 (the ip of my sensor) to ensure it is able to connect



Filter: firewall.hostgroups.sensor

firewall > hostgroups > sensor

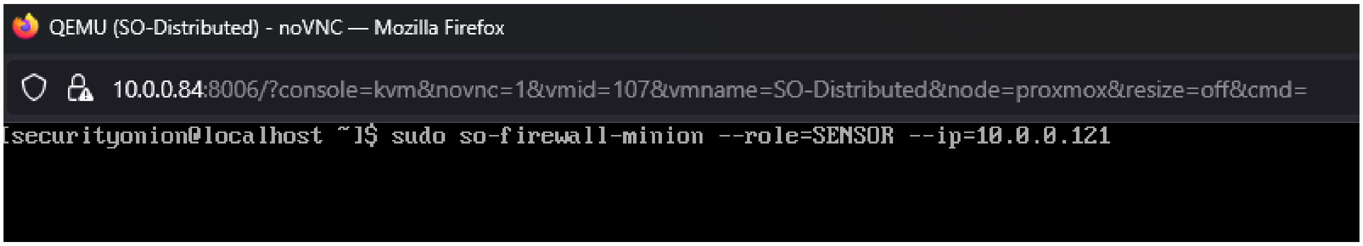
List of IP or CIDR blocks to allow access to this hostgroup.

Current Grid Value

```
10.0.0.0/24
```

After make sure you check the green button then if you select options at the top, there should be a drop down menu that allows you to sync which will push all the rules out instead of having to wait 15ish minutes.

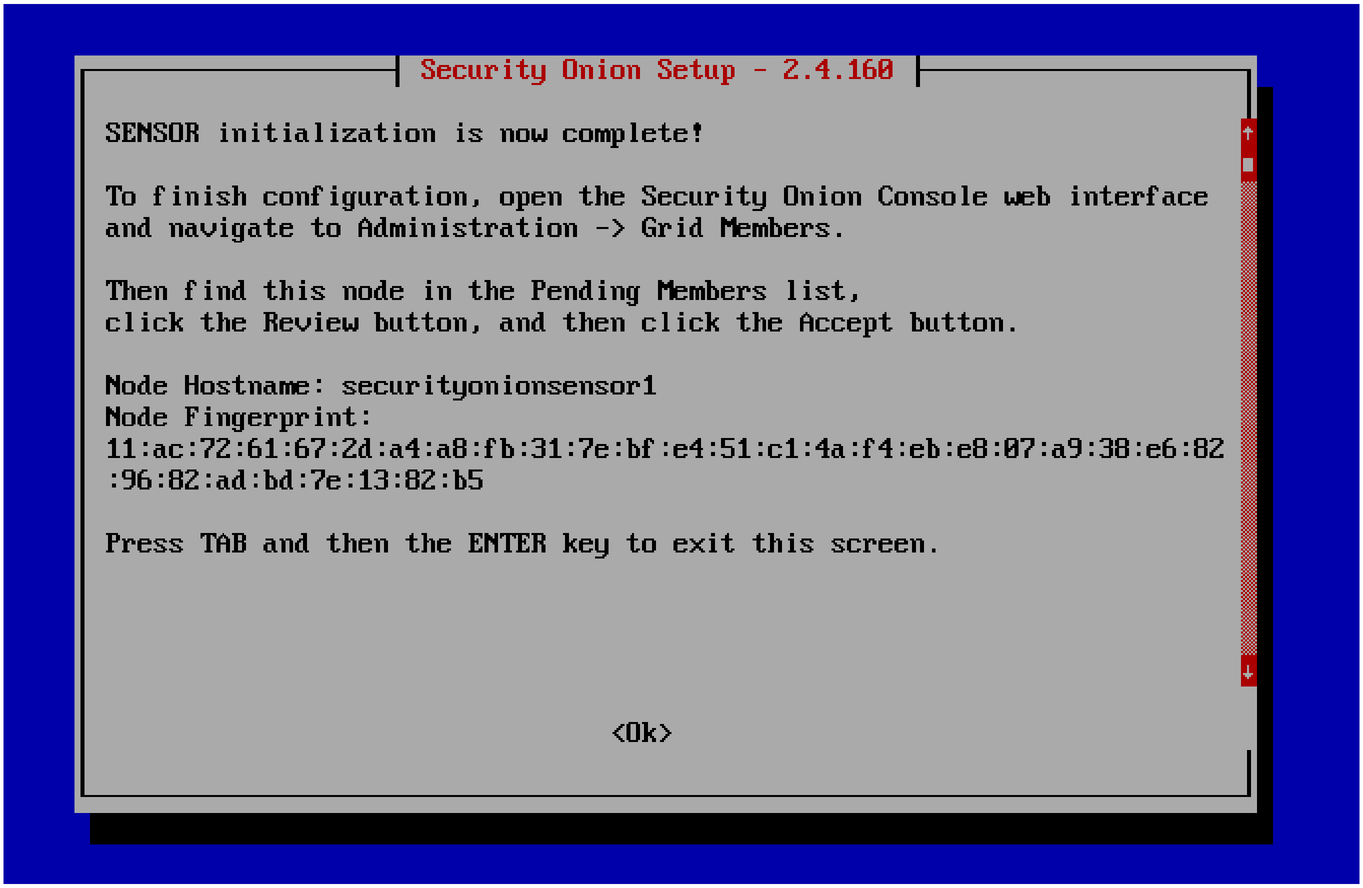
And just to make sure it works I am going to log onto the manager consoles and enter this command;


QEMU (SO-Distributed) - noVNC — Mozilla Firefox
10.0.0.84:8006/?console=kvm&novnc=1&vmid=107&vmname=SO-Distributed&node=proxmox&resize=off&cmd=

```
[securityonion@localhost ~]$ sudo so-firewall-minion --role=SENSOR --ip=10.0.0.121
```

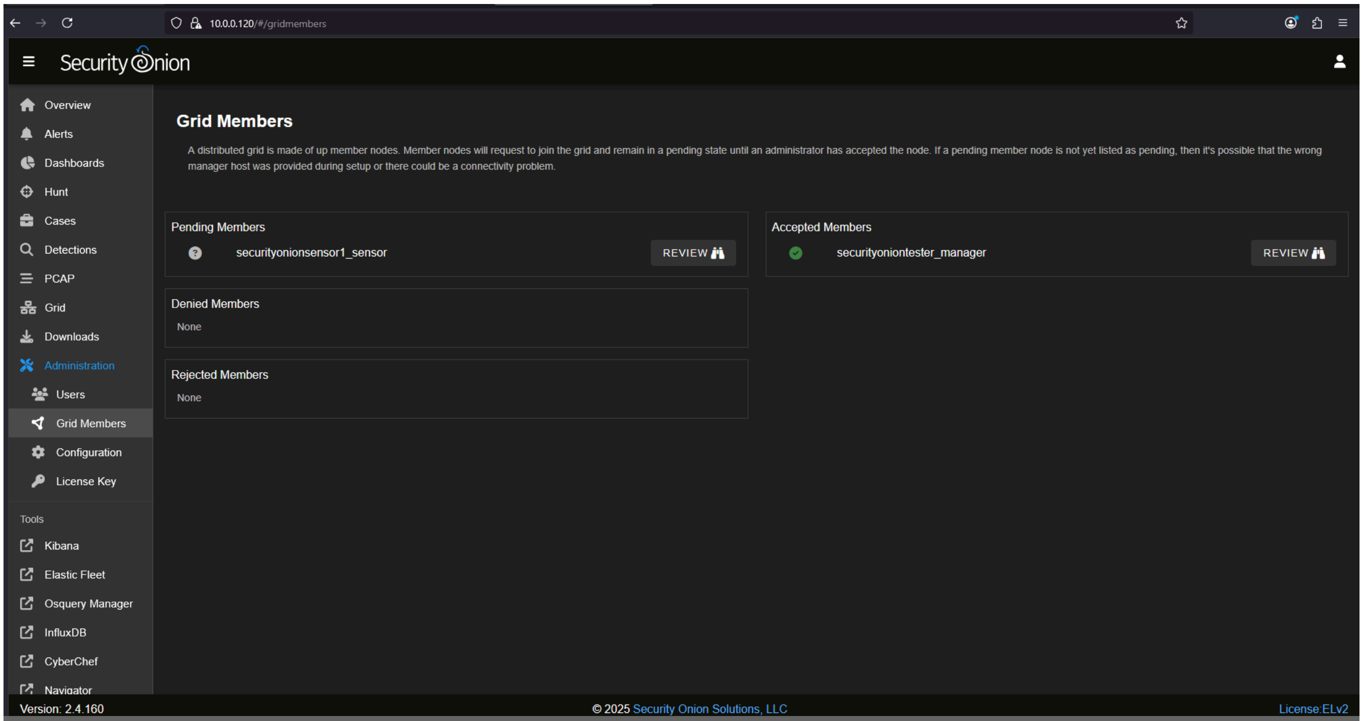
And boom the connection worked, after you will have to select the second interface for the monitoring network traffic, after you will be given a summary of the configuration you have done, select yes and proceed with the installation. FYI this may take some time.

And boom;



```
Security Onion Setup - 2.4.160

SENSOR initialization is now complete!

To finish configuration, open the Security Onion Console web interface
and navigate to Administration -> Grid Members.

Then find this node in the Pending Members list,
click the Review button, and then click the Accept button.

Node Hostname: securityonionsensor1
Node Fingerprint:
11:ac:72:61:67:2d:a4:a8:fb:31:7e:bf:e4:51:c1:4a:f4:eb:e8:07:a9:38:e6:82
:96:82:ad:bd:7e:13:82:b5

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

Now if we log onto the web interface and go administration then grid members we can see the sensor in the pending members, so lets select review and get this sensor involved.



Grid Members

A distributed grid is made of up member nodes. Member nodes will request to join the grid and remain in a pending state until an administrator has accepted the node. If a pending member node is not yet listed as pending, then it's possible that the wrong manager host was provided during setup or there could be a connectivity problem.

Pending Members

securityonionsensor1_sensor REVIEW

Accepted Members

securityoniontester_manager REVIEW

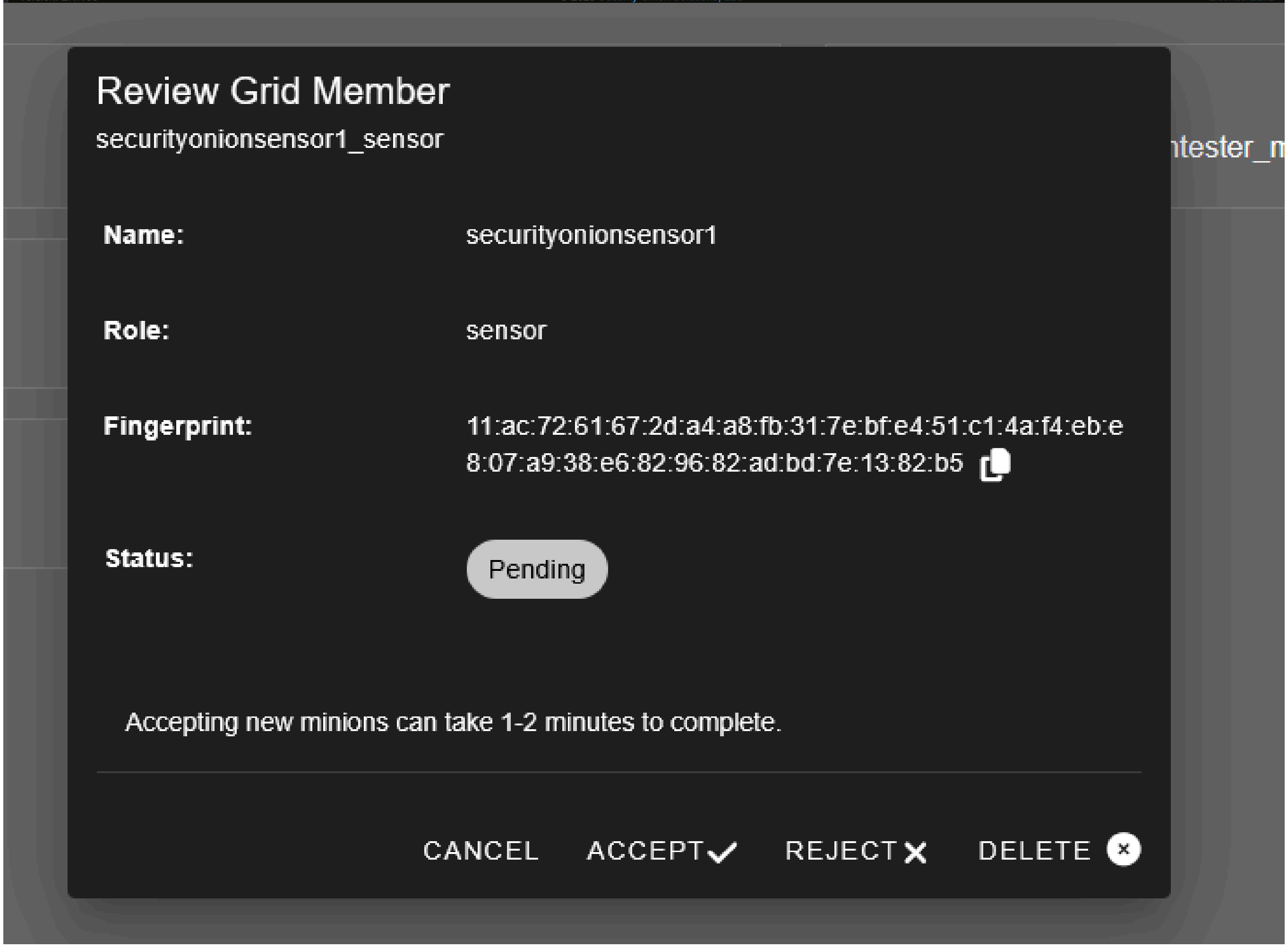
Denied Members

None

Rejected Members

None

Version: 2.4.160 © 2025 Security Onion Solutions, LLC License:ELv2



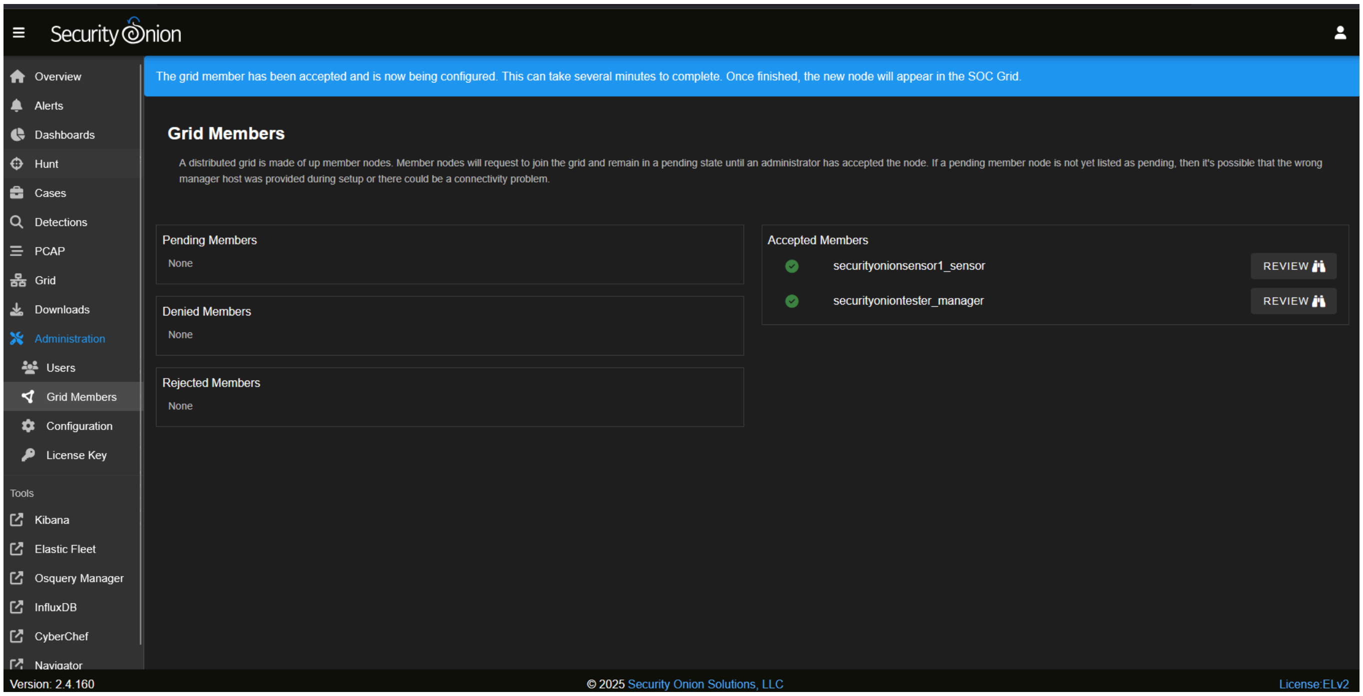
Review Grid Member

securityonionsensor1_sensor

Name:	securityonionsensor1
Role:	sensor
Fingerprint:	11:ac:72:61:67:2d:a4:a8:fb:31:7e:bf:e4:51:c1:4a:f4:eb:e8:07:a9:38:e6:82:96:82:ad:bd:7e:13:82:b5
Status:	Pending

Accepting new minions can take 1-2 minutes to complete.

And now we can see it in the accepted members tab



The grid member has been accepted and is now being configured. This can take several minutes to complete. Once finished, the new node will appear in the SOC Grid.

Grid Members

A distributed grid is made of up member nodes. Member nodes will request to join the grid and remain in a pending state until an administrator has accepted the node. If a pending member node is not yet listed as pending, then it's possible that the wrong manager host was provided during setup or there could be a connectivity problem.

Pending Members
None

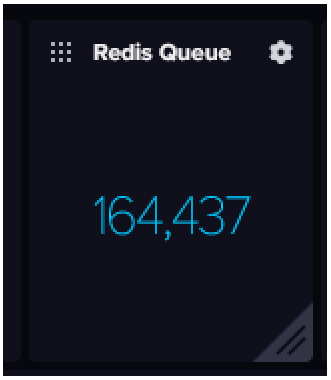
Denied Members
None

Rejected Members
None

Accepted Members
securityonionsensor1_sensor
securityoniontester_manager

Version: 2.4.160
© 2025 Security Onion Solutions, LLC
License:ELv2

After this obviously we aren't going to be seeing any logs, we still need to deploy the backend storage, to do so just follow the same steps above but instead of selecting sensor select searchnode and follow the installation steps. We know this because when we go to influx we can see the high amount of logs and information stuck in queue



Redis Queue

164,437

Search Node - Security Onion Distribution Installation