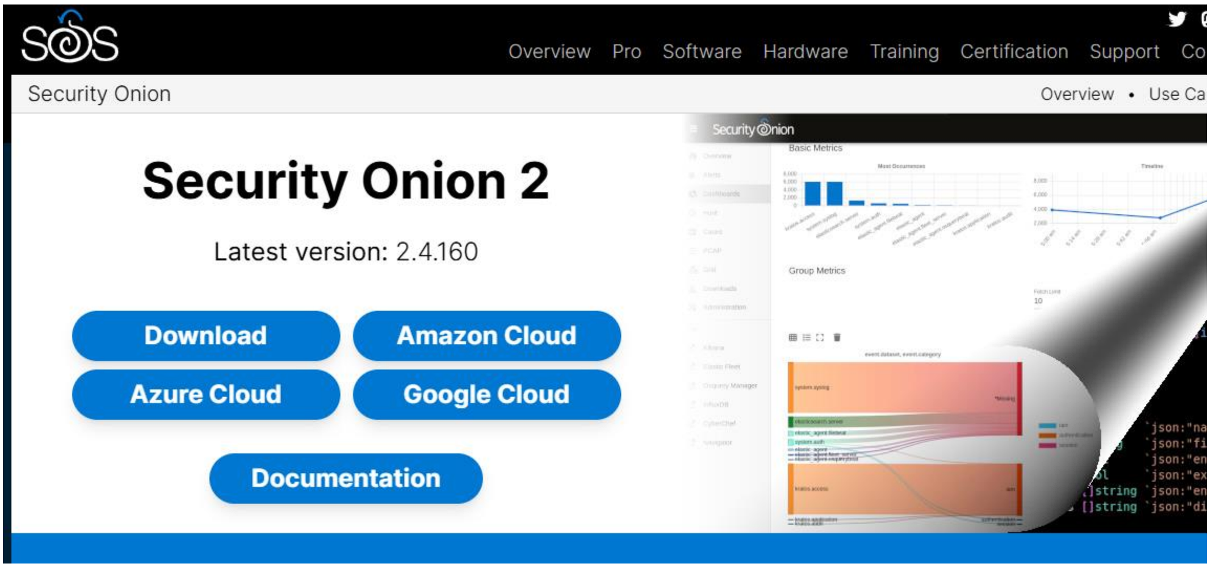
Security Onion installation

Download the security onion from the below link.

https://download.securityonion.net/file/securityonion/securityonion-2.4.160-20250625.iso

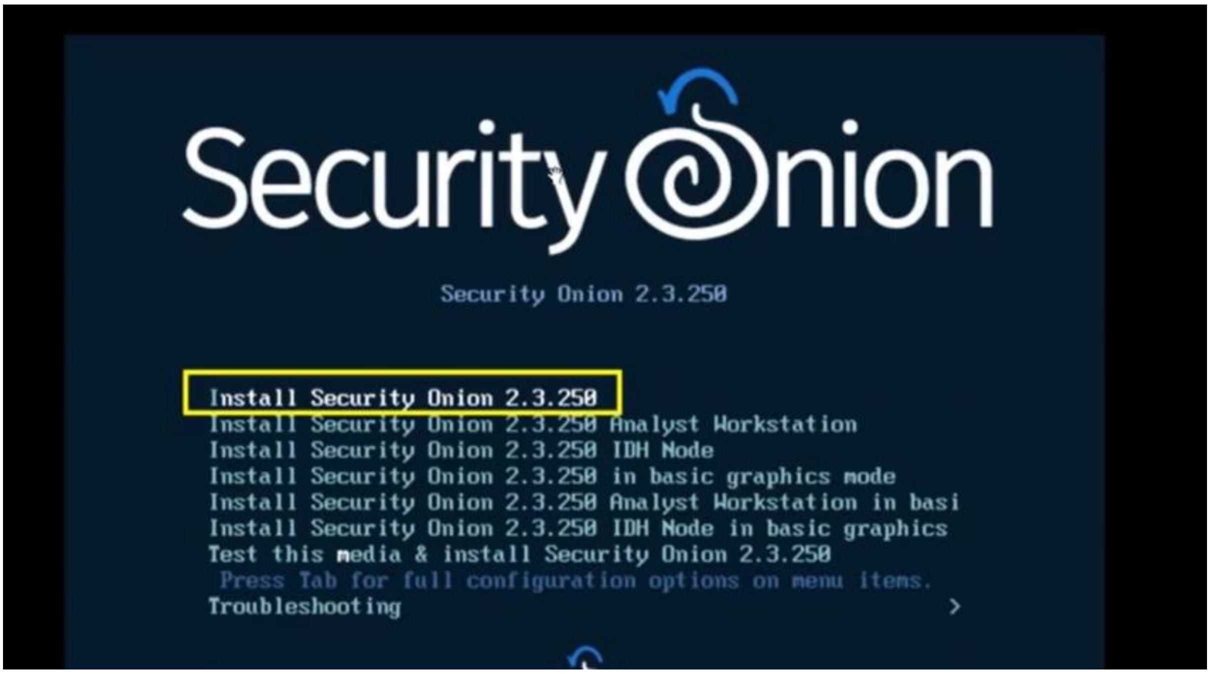


It will **.iso** file.

First read the important work at end of this notes.

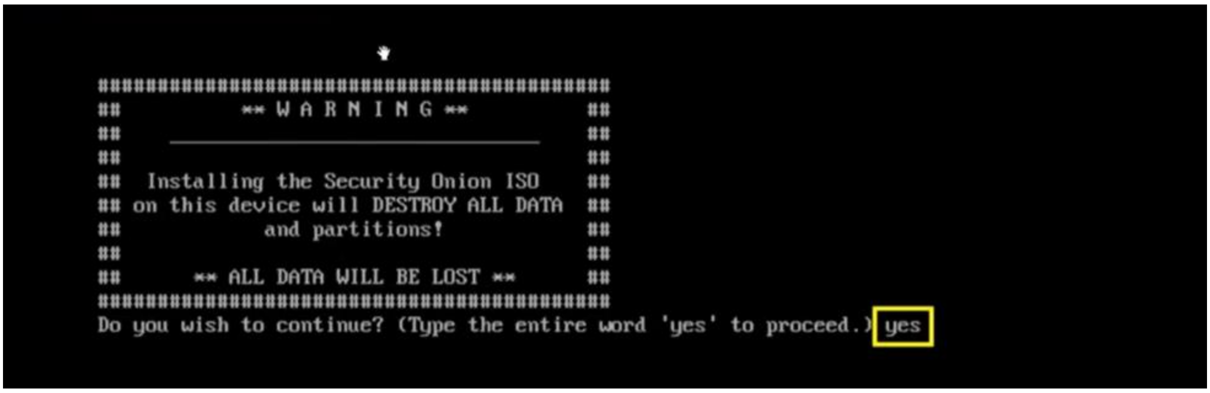
The process of installation is given below

- Go to vmare
- Open new virtual machine
- Select the file as like we do before for other machine installation like ubuntu
- Select 2nd option for install now by browsing the file location
- Name this machine **securityonion.**
- Select machine type of **Linux** and type of **CentOS 64bit**. As like we do for ubuntu as select the software linux and type ubuntu 64bit.
- The purpose of select CentOS 64bit is that it is linux base and have centos kernel based.
- **NOTE:** after all setting before finish go to hardware setting and 2 new network adapter in this machine. According to lab
- 2nd is at vmnat3 and 3rd at vmnat5 and 1st at NAT.
- RAM require 16 GB and ROM 200 GB
- Then finish it and power on the machine.



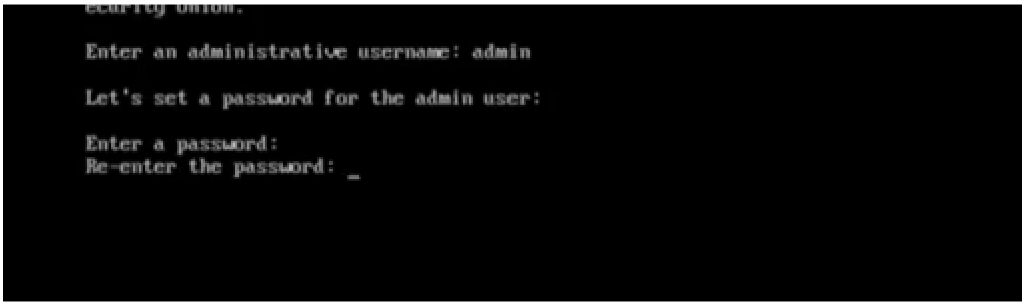
```
Security Onion 2.3.250

Install Security Onion 2.3.250
Install Security Onion 2.3.250 Analyst Workstation
Install Security Onion 2.3.250 IDH Node
Install Security Onion 2.3.250 in basic graphics mode
Install Security Onion 2.3.250 Analyst Workstation in basi
Install Security Onion 2.3.250 IDH Node in basic graphics
Test this media & install Security Onion 2.3.250
 Press Tab for full configuration options on menu items.
Troubleshooting                                          >
```

- Here we chose the 1st option and press enter
- We use tab and enter key in this setup.
- Then write yes and press enter.



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

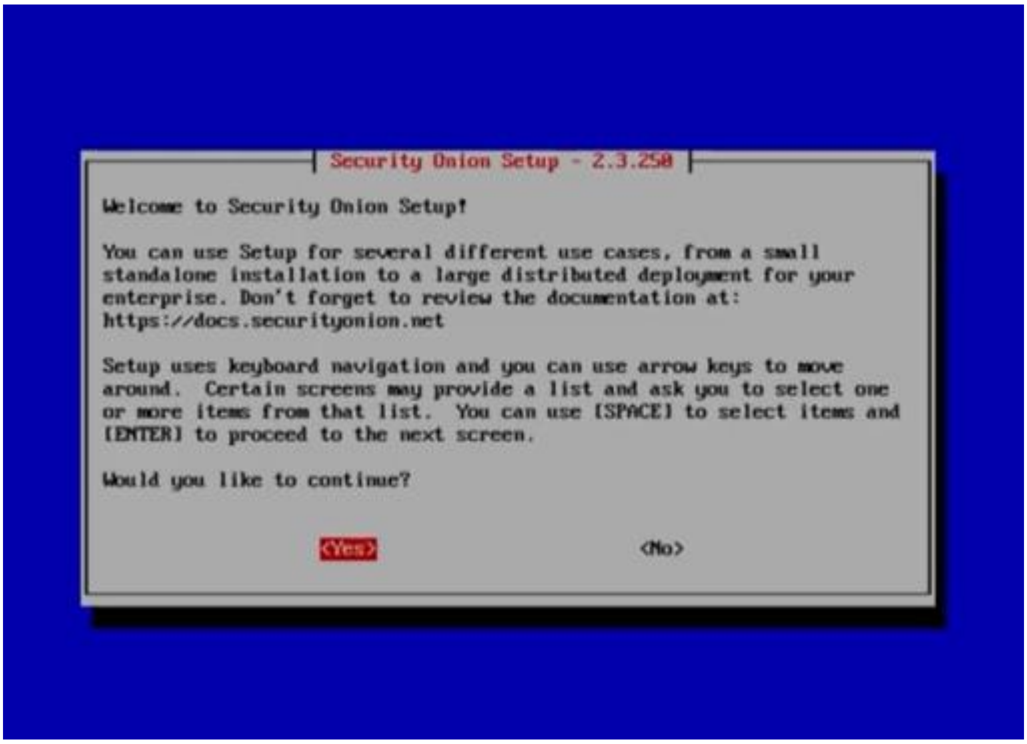
- Then enter the username and password that you want to take
- I using admin and Admin@12345 in my case.



```
ecurity Onion.

Enter an administrative username: admin

Let's set a password for the admin user:

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

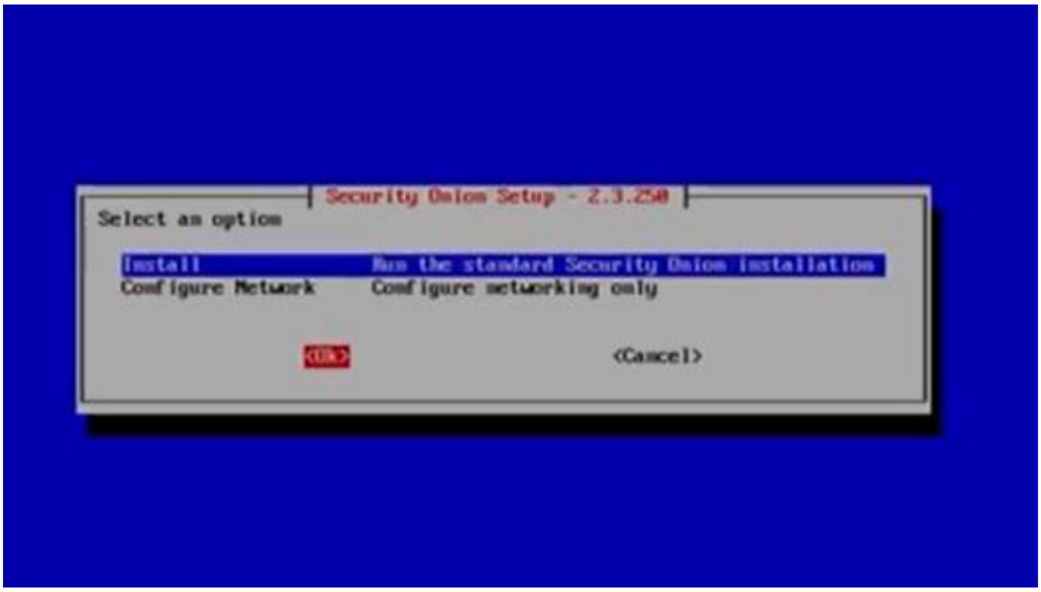
- After this installation will start, it will take time as compare to other machines.
- When it complete then hit enter and restart is start.
- Then login again and installation settings will start.

- Select YES and enter



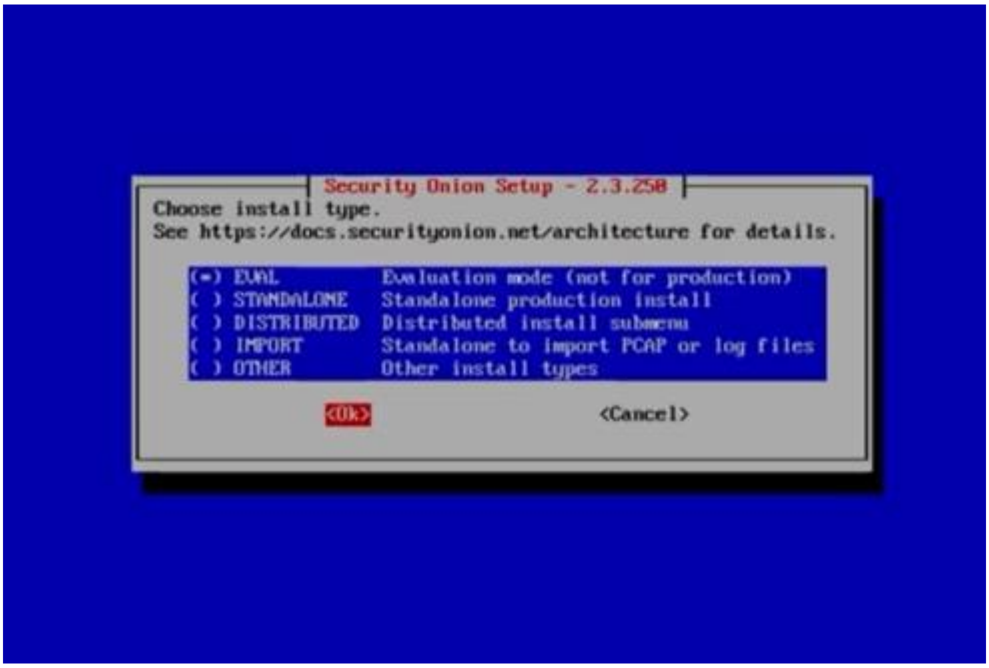
```
Security Onion Setup - 2.3.250

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. Don't forget to review the documentation at:
https://docs.securityonion.net

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 [SPACE] to select items and
[ENTER] to proceed to the next screen.

Would you like to continue?

              <Yes>                         <No>
```

- Then tab for select the install option and hit enter for yes option.



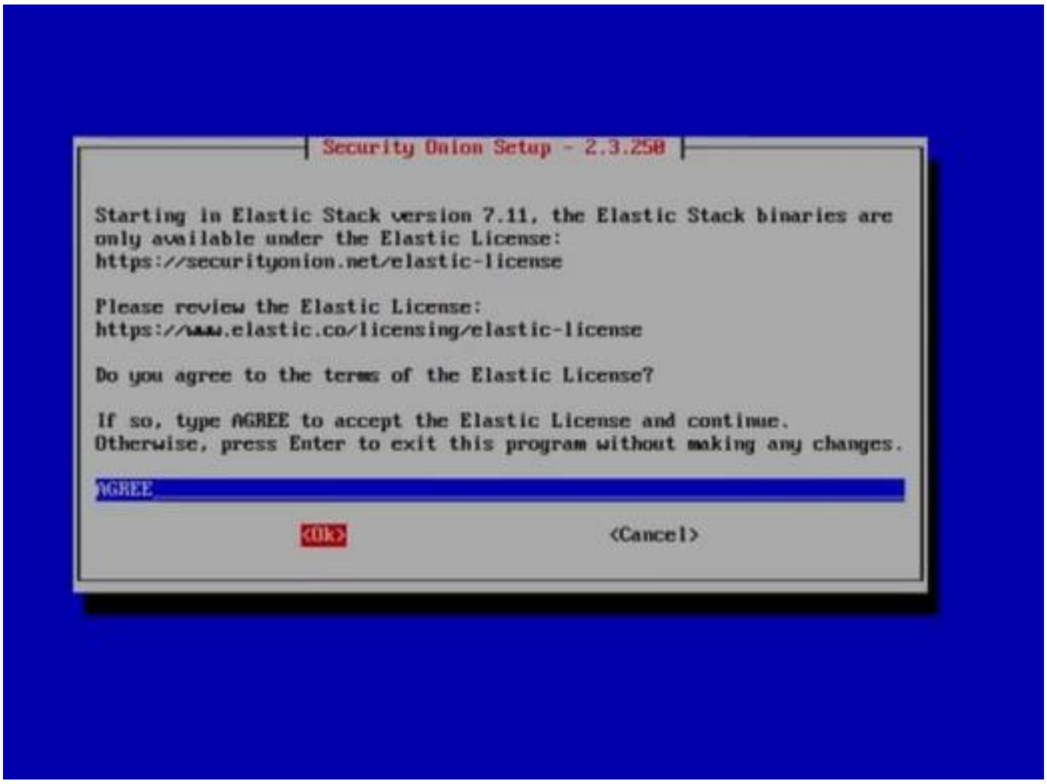
```
Security Onion Setup - 2.3.250
Select an option

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

            <Ok>                        <Cancel>
```

- Select EVAL(evaluation first option) and then hit enter for ok



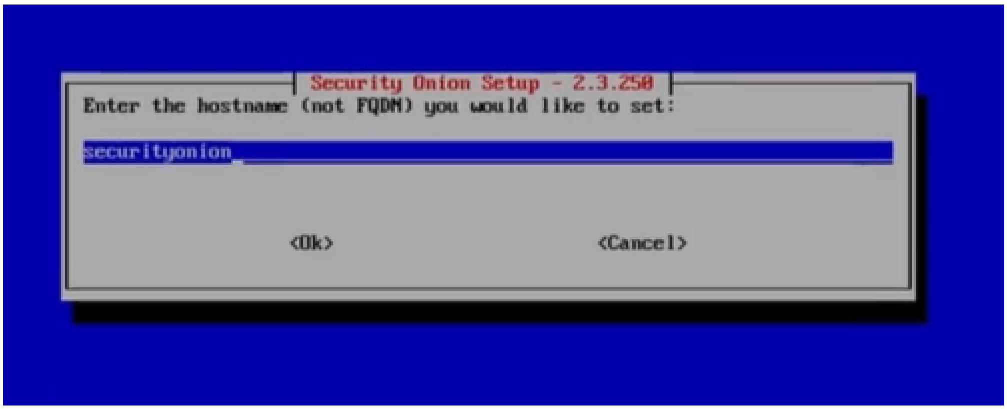
```
Security Onion Setup - 2.3.250
Choose install type.
See https://docs.securityonion.net/architecture for details.

(*) EVAL          Evaluation mode (not for production)
( ) STANDALONE    Standalone production install
( ) DISTRIBUTED   Distributed install submenu
( ) IMPORT        Standalone to import PCAP or log files
( ) OTHER         Other install types

          <Ok>                    <Cancel>
```

- Write agree and then hit enter



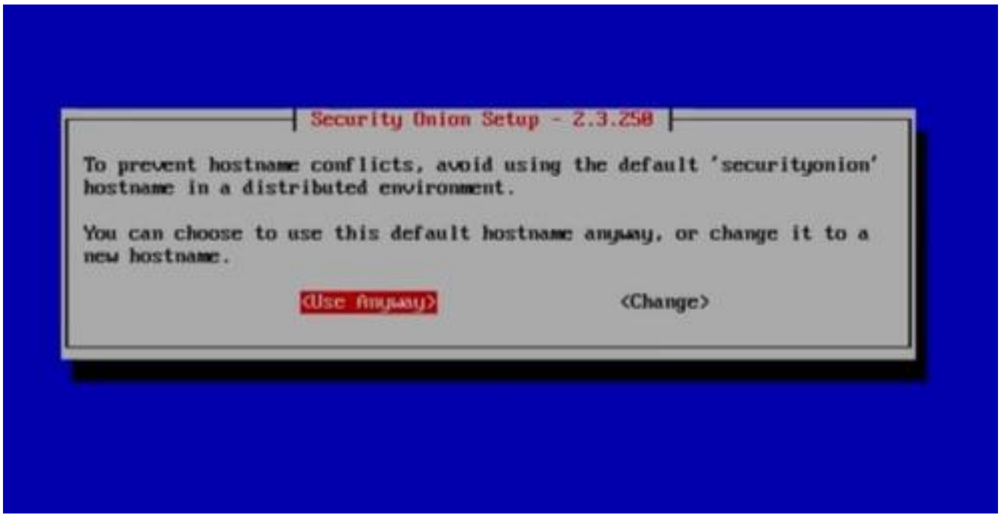
```
Security Onion Setup - 2.3.250

Starting in Elastic Stack version 7.11, the Elastic Stack binaries are
only available under the Elastic License:
https://securityonion.net/elastic-license

Please review the Elastic License:
https://www.elastic.co/licensing/elastic-license

Do you agree to the terms of the Elastic License?

If so, type AGREE to accept the Elastic License and continue.
Otherwise, press Enter to exit this program without making any changes.

AGREE

          <Ok>                    <Cancel>
```

- if you want to change the username do in this step and then hit enter by tab to move at ok button.



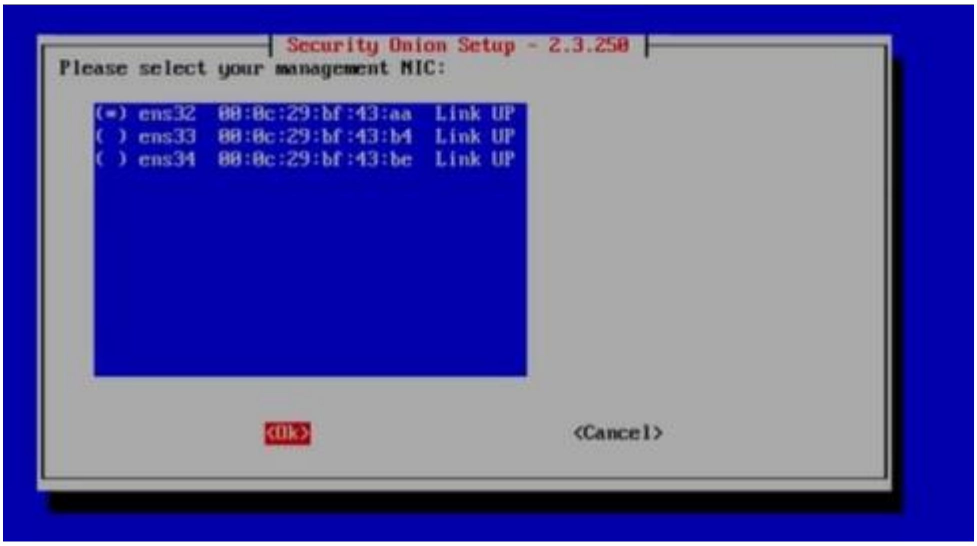
```
Security Onion Setup - 2.3.250
Enter the hostname (not FQDN) you would like to set:

securityonion_

            <Ok>                    <Cancel>
```

- Then select use anyway option and hit enter, to ensure that username you want ot use.



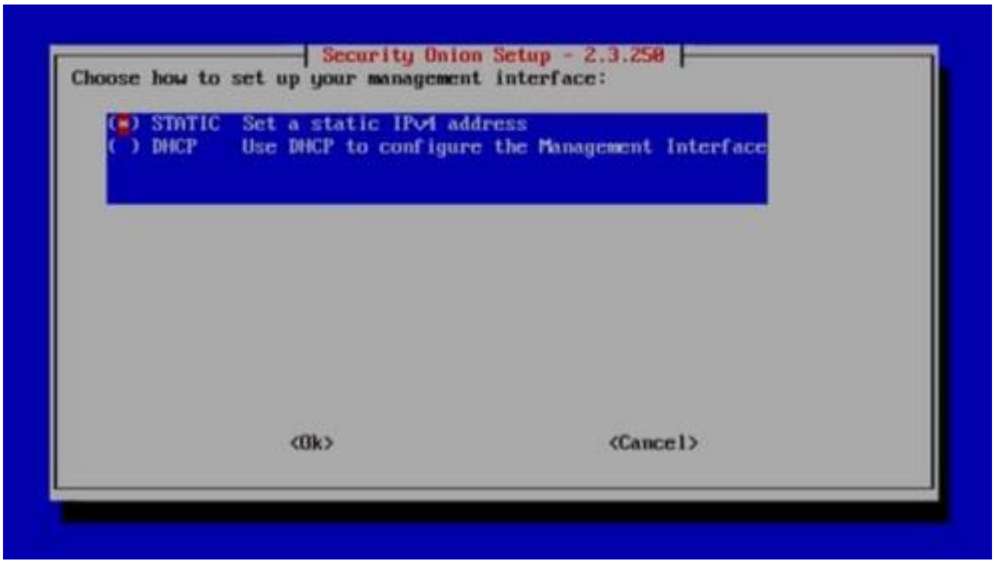
```
Security Onion Setup - 2.3.250

To prevent hostname conflicts, avoid using the default 'securityonion'
hostname in a distributed environment.

You can choose to use this default hostname anyway, or change it to a
new hostname.

            <Use Anyway>            <Change>
```

- Here it ask for select management nic, the first is our management interface.
- Here you use spacebar for select it(star appear on selected option) and then hit enter.



```
Security Onion Setup - 2.3.250
Please select your management NIC:

  (*) ens32  00:0c:29:bf:43:aa  Link UP
  ( ) ens33  00:0c:29:bf:43:b4  Link UP
  ( ) ens34  00:0c:29:bf:43:be  Link UP

            <Ok>                    <Cancel>
```

- Here you choose to use static ip and hit enter

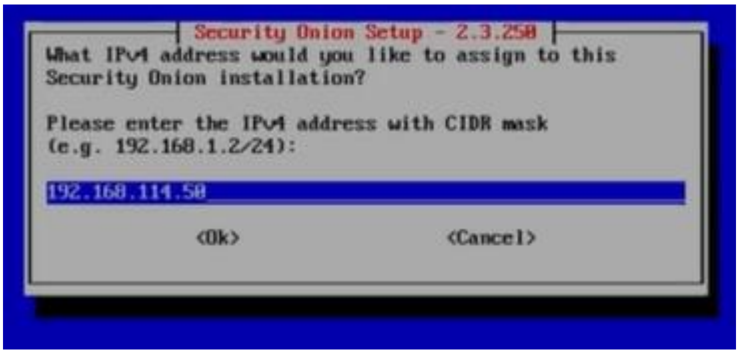


```
Security Onion Setup - 2.3.250
Choose how to set up your management interface:

  (*) STATIC   Set a static IPv4 address
  ( ) DHCP     Use DHCP to configure the Management Interface

            <Ok>                      <Cancel>
```

- Then enter the ip

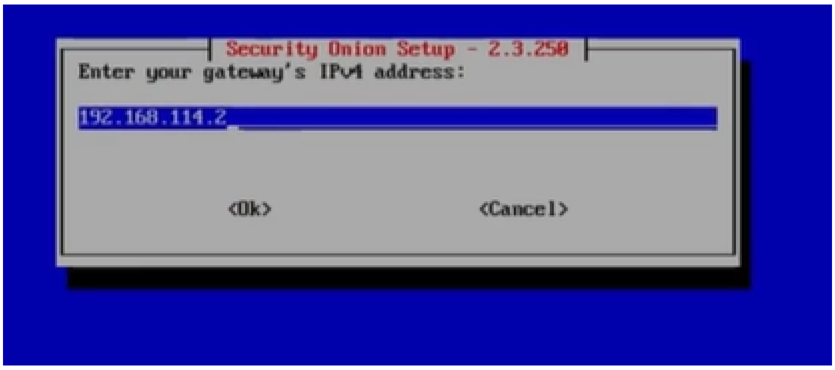
    192.168.144.50/24

- Enter ip with subnet mask as write above. Then hit enter.



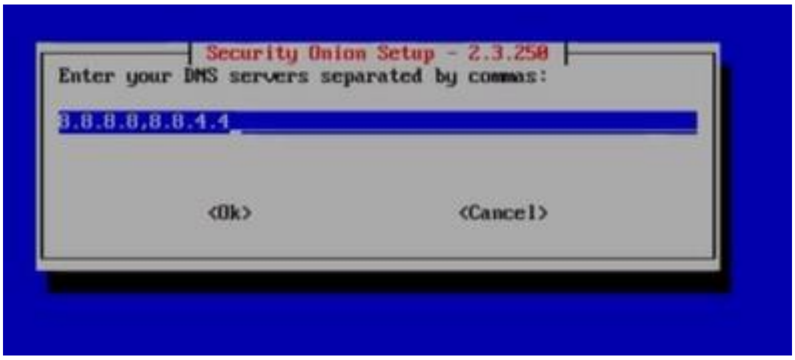
```
Security Onion Setup - 2.3.250
What IPv4 address would you like to assign to this
Security Onion installation?

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

192.168.114.50

         <Ok>                <Cancel>
```

- Enter the gateway and hit enter



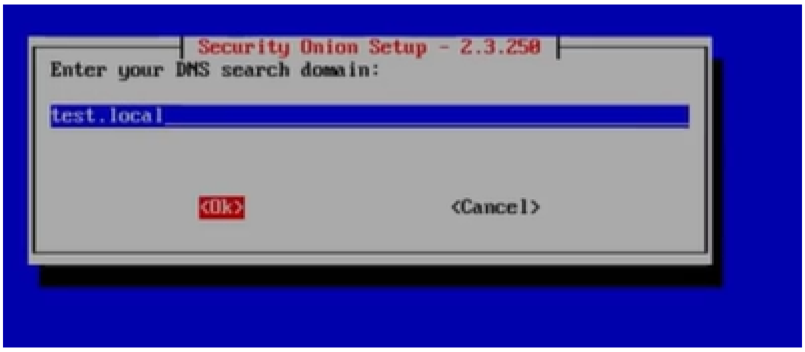
```
Security Onion Setup - 2.3.250
Enter your gateway's IPv4 address:

192.168.114.2

         <Ok>                <Cancel>
```

- Enter DNS server , I use default and hit enter



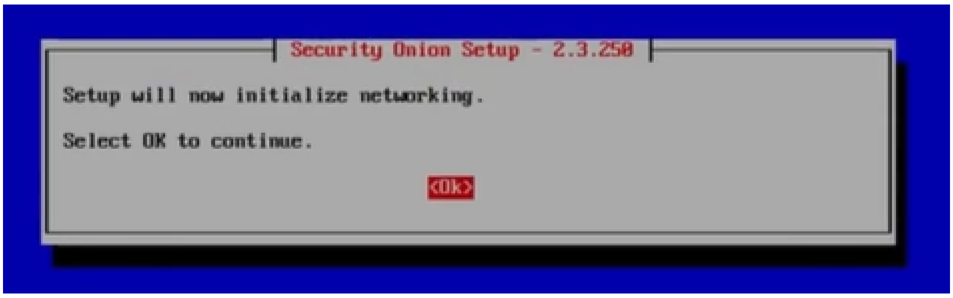
```
Security Onion Setup - 2.3.250
Enter your DNS servers separated by commas:

8.8.8.8,8.8.4.4
```

- Here enter the DNS name by which you access the web for security onion.



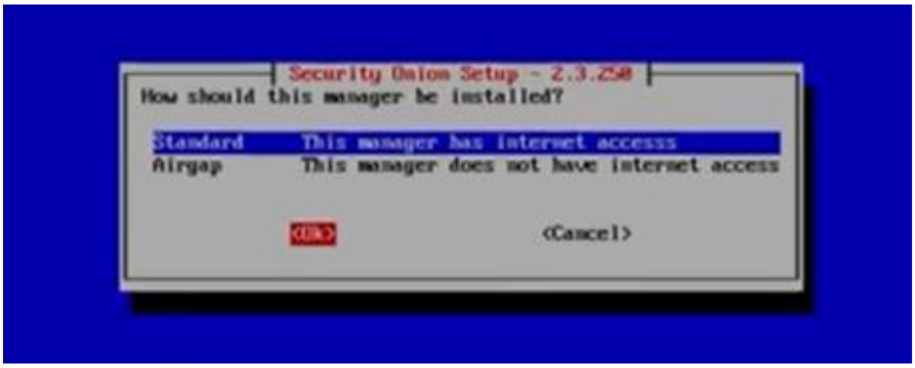
```
Security Onion Setup - 2.3.250
Enter your DNS search domain:

test.local
```

- Hit okay in this step



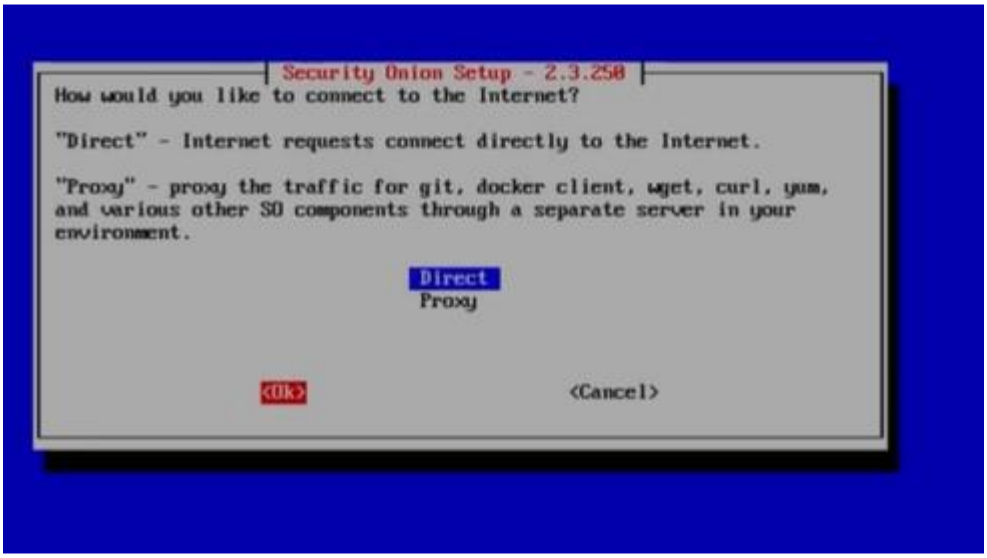
```
Security Onion Setup - 2.3.250

Setup will now initialize networking.

Select OK to continue.
```

- Here select standard and hit enter



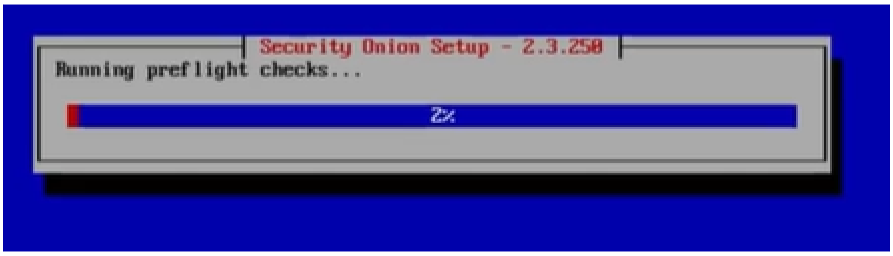
```
Security Onion Setup - 2.3.250
How should this manager be installed?

Standard      This manager has internet accesss
Airgap        This manager does not have internet access
```

- Here we select Direct and hit enter
- Because we directly connected with internet without proxy



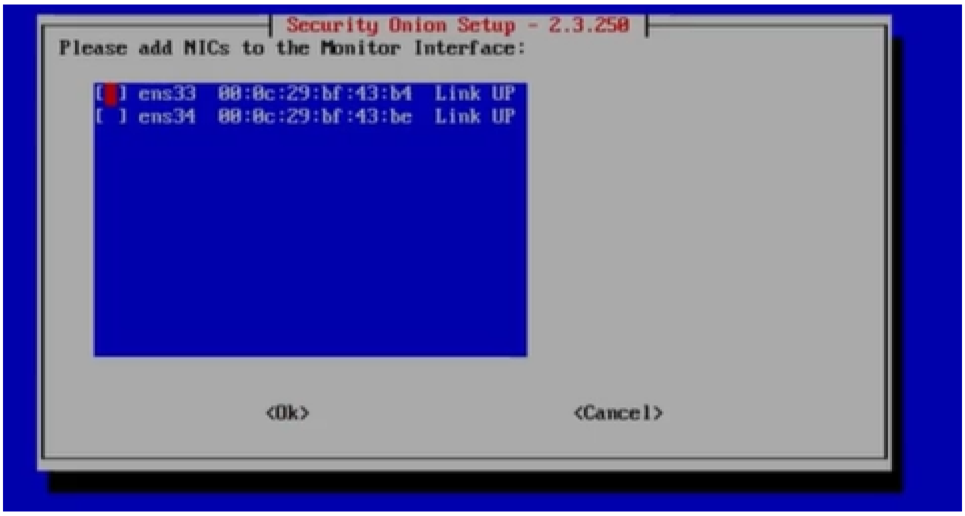
```
Security Onion Setup - 2.3.250
How would you like to connect to the Internet?

"Direct" - Internet requests connect directly to the Internet.

"Proxy" - proxy the traffic for git, docker client, wget, curl, yum,
and various other SO components through a separate server in your
environment.

                    Direct
                    Proxy

         <Ok>                          <Cancel>
```

- Then this start.
- It will takr some time.



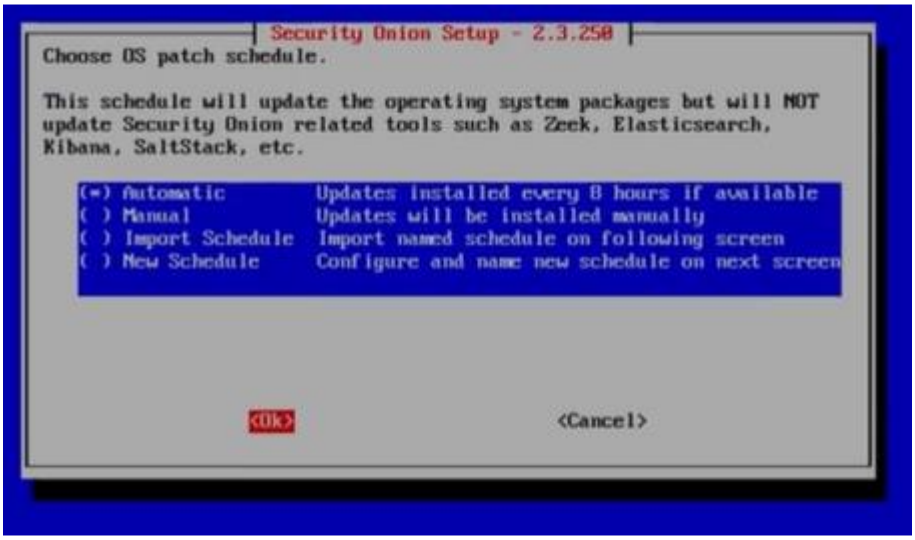
```
Security Onion Setup - 2.3.250
Running preflight checks...
                    2%
```

- Here select the monitoring interface ens33 and hit enter



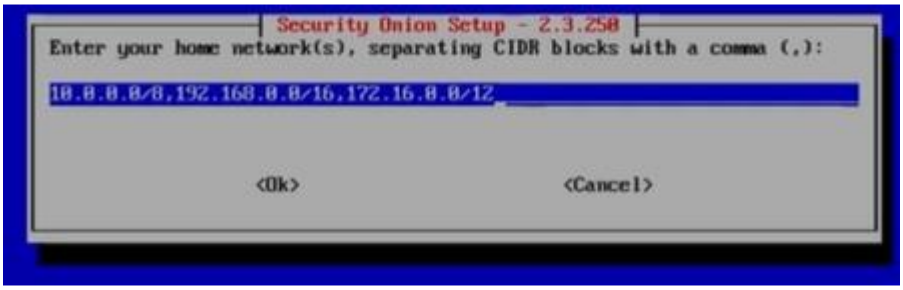
```
Security Onion Setup - 2.3.250
Please add NICs to the Monitor Interface:

   [ ] ens33   00:0c:29:bf:43:b4   Link UP
   [ ] ens34   00:0c:29:bf:43:be   Link UP

         <Ok>                          <Cancel>
```

- Here select the automatic and hit enter



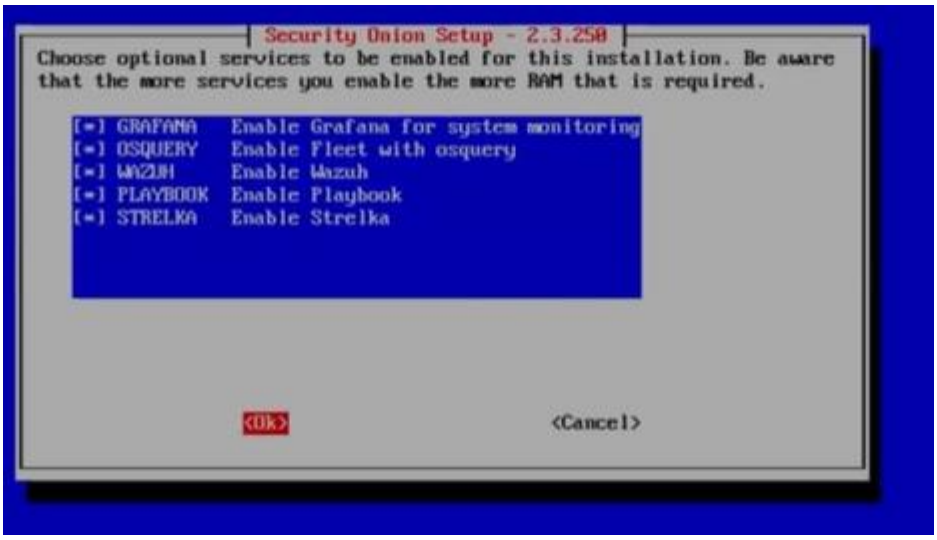
```
Security Onion Setup - 2.3.250
Choose OS patch schedule.

This schedule will update the operating system packages but will NOT
update Security Onion related tools such as Zeek, Elasticsearch,
Kibana, SaltStack, etc.

(*) Automatic         Updates installed every 8 hours if available
( ) Manual            Updates will be installed manually
( ) Import Schedule   Import named schedule on following screen
( ) New Schedule      Configure and name new schedule on next screen

            <Ok>                          <Cancel>
```

- Here select the allowed subnet and hit ok.
- I use default



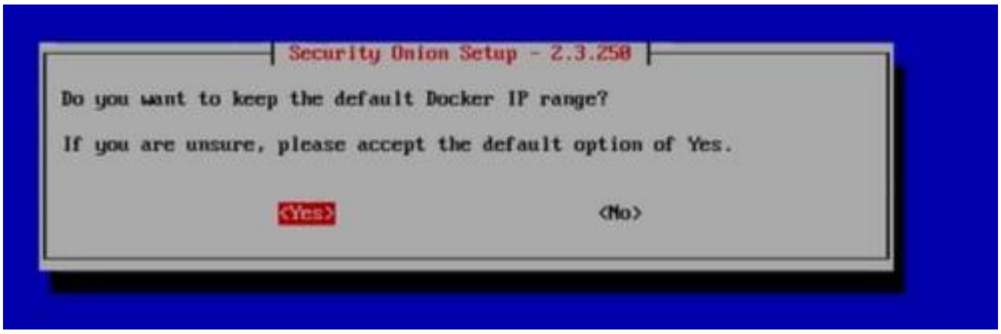
```
Security Onion Setup - 2.3.250
Enter your home network(s), separating CIDR blocks with a comma (,):

10.0.0.0/8,192.168.0.0/16,172.16.0.0/12

            <Ok>                          <Cancel>
```

- This take as default and hit ok



```
Security Onion Setup - 2.3.250
Choose optional services to be enabled for this installation. Be aware
that the more services you enable the more RAM that is required.

[*] GRAFANA    Enable Grafana for system monitoring
[*] OSQUERY    Enable Fleet with osquery
[*] WAZUH      Enable Wazuh
[*] PLAYBOOK   Enable Playbook
[*] STRELKA    Enable Strelka

            <Ok>                          <Cancel>
```

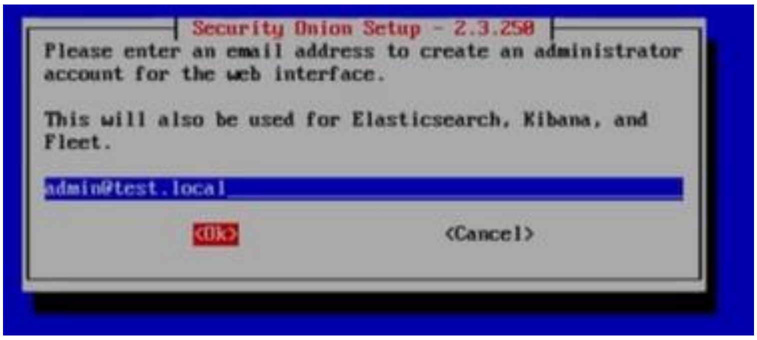
- Select Default Docker and hit enter



Do you want to keep the default Docker IP range?

If you are unsure, please accept the default option of Yes.

- Here enter email for administrator and hit enter
- I use   admin@testlocal

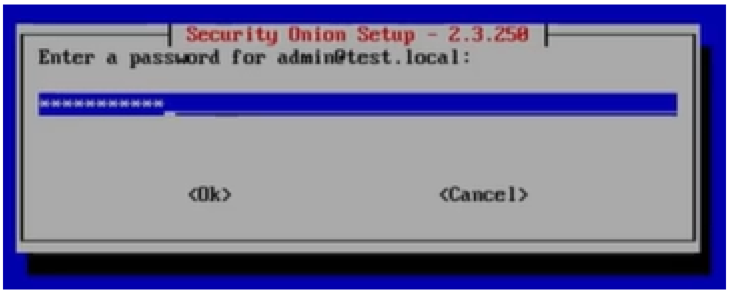


Please enter an email address to create an administrator account for the web interface.

This will also be used for Elasticsearch, Kibana, and Fleet.

admin@test.local

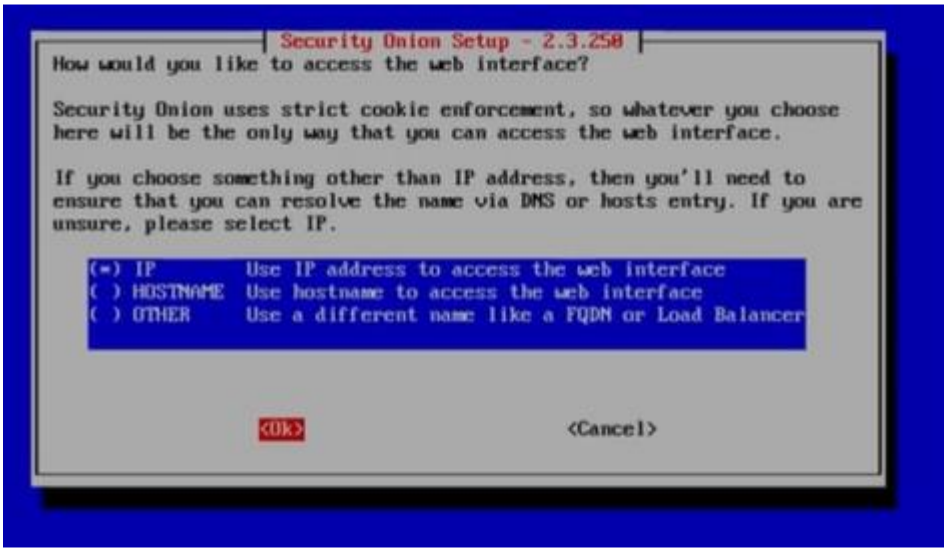
- Here enter password
- I use same as before Admin@12345



Enter a password for admin@test.local:

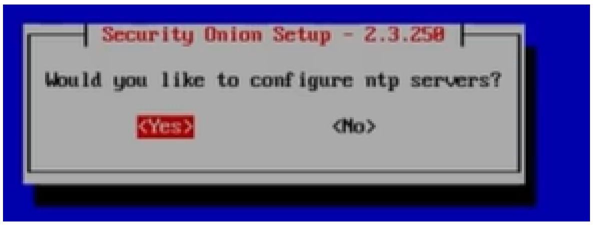
****

- Here it say how to access the interface
- I select ip and hit enter



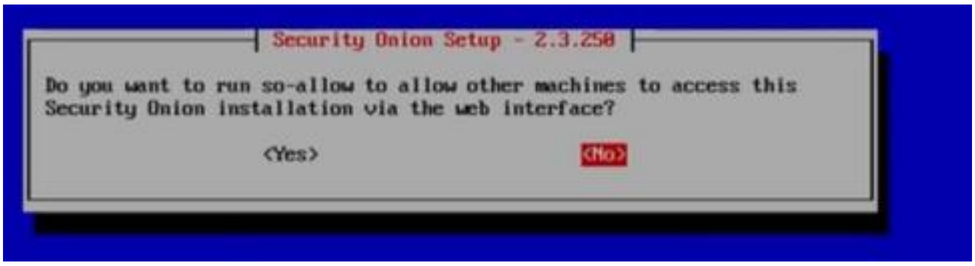
```
Security Onion Setup - 2.3.250
How would you like to access the web interface?

Security Onion uses strict cookie enforcement, so 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>
```

- Hit at yes for config NTP



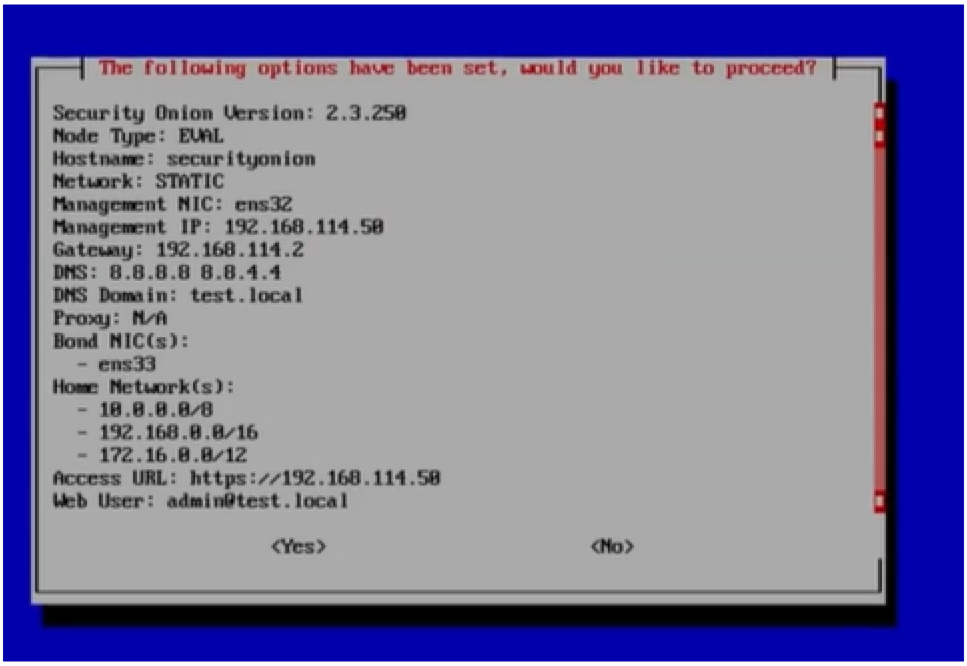
```
Security Onion Setup - 2.3.250
Would you like to configure ntp servers?

          <Yes>               <No>
```

- Her select NO, because we allowed it later.



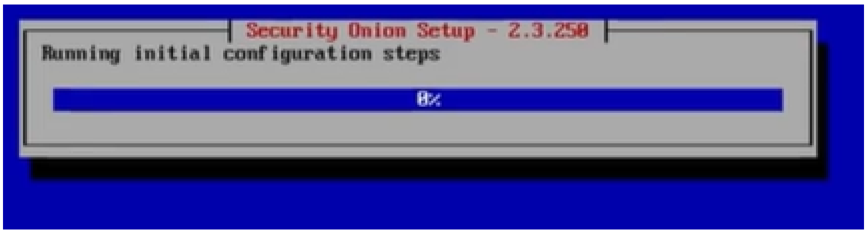
```
Security Onion Setup - 2.3.250
Do you want to run so-allow to allow other machines to access this
Security Onion installation via the web interface?

                 <Yes>                          <No>
```

- Then summery will appear, select yes and hit enter



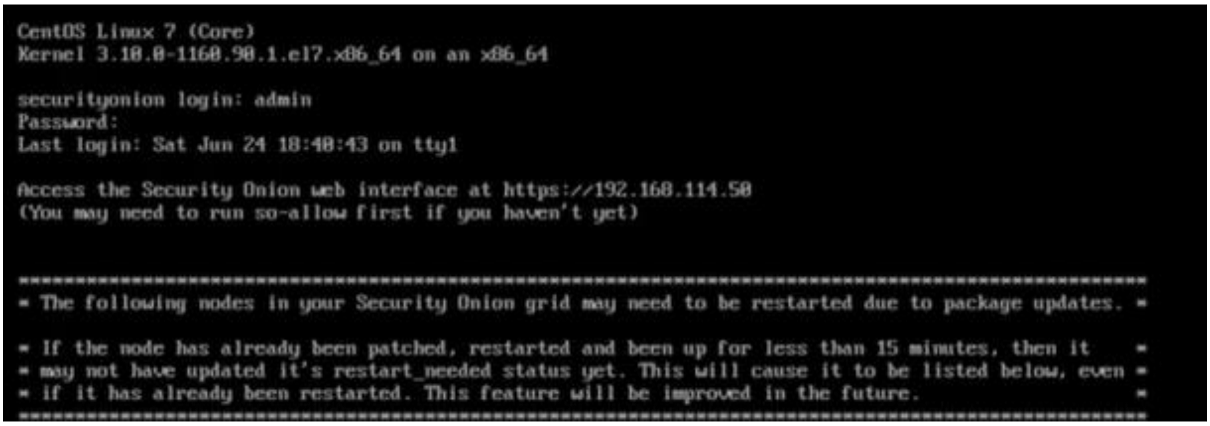
```
The following options have been set, would you like to proceed?

Security Onion Version: 2.3.250
Node Type: EVAL
Hostname: securityonion
Network: STATIC
Management NIC: ens32
Management IP: 192.168.114.50
Gateway: 192.168.114.2
DNS: 8.8.8.8 8.8.4.4
DNS Domain: test.local
Proxy: N/A
Bond NIC(s):
  - ens33
Home Network(s):
  - 10.0.0.0/8
  - 192.168.0.0/16
  - 172.16.0.0/12
Access URL: https://192.168.114.50
Web User: admin@test.local
```

- It take time 10 – 15 minutes.



```
Security Onion Setup - 2.3.250
Running initial configuration steps
```

- When it complete you login in it



```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.90.1.el7.x86_64 on an x86_64

securityonion login: admin
Password:
Last login: Sat Jun 24 18:40:43 on tty1

Access the Security Onion web interface at https://192.168.114.50
(You may need to run so-allow first if you haven't yet)


***********************************************************************************************
* The following nodes in your Security Onion grid may need to be restarted due to package updates. *

* If the node has already been patched, restarted and been up for less than 15 minutes, then it   *
* may not have updated it's restart_needed status yet. This will cause it to be listed below, even *
* if it has already been restarted. This feature will be improved in the future.                    *
***********************************************************************************************
```

- **In above image you see that ip is 192.168.144.50 that I give to it.**

➢ Important work

You will face problem in internet ip that you have.

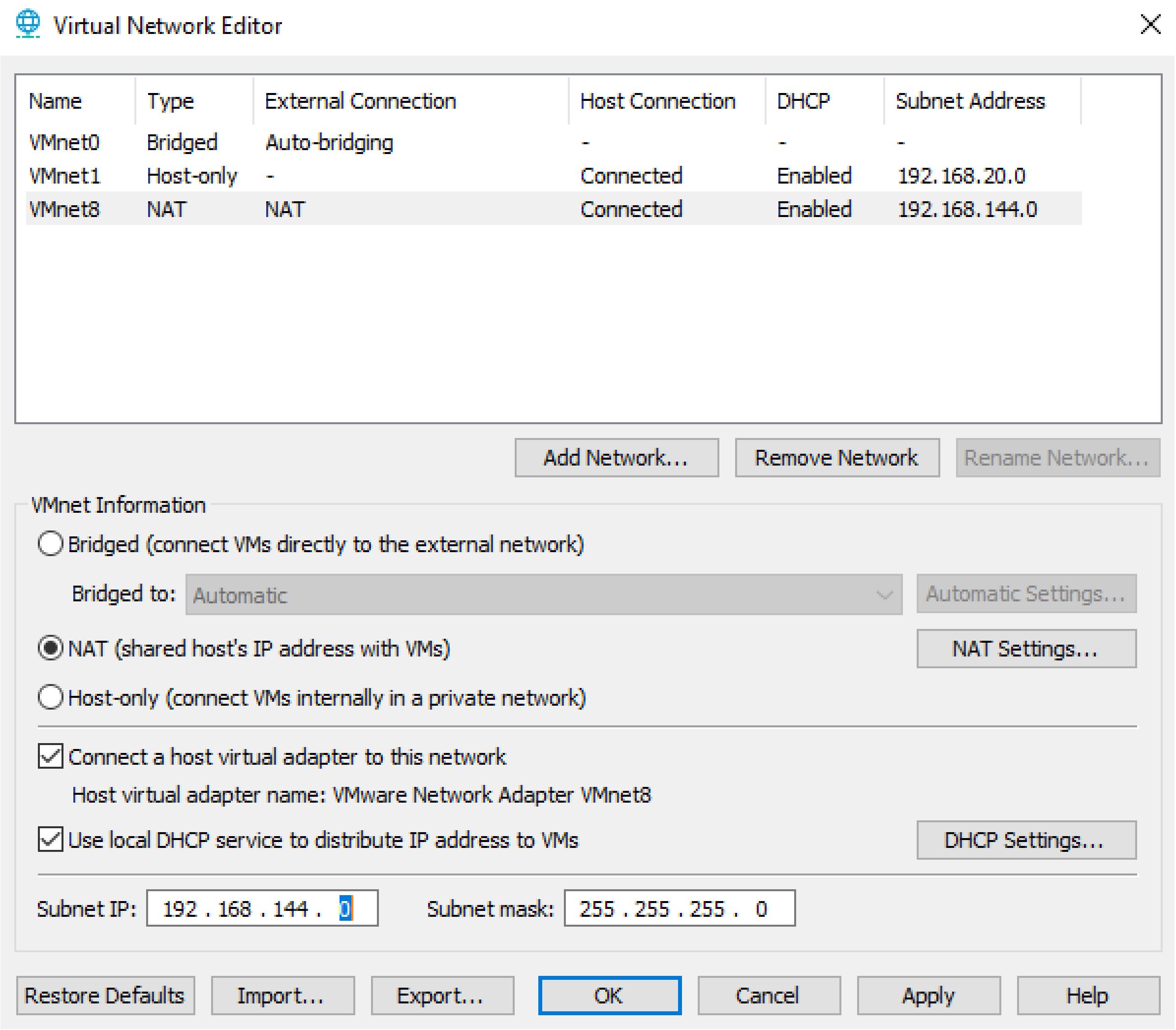
I will have 192.168.144.*

In your case it will be same 16 bit but next 16 bit were change.

❖ Case 1:

Go to virtual text editor

Click at change settings and select NAT from above.



Virtual Network Editor

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Auto-bridging	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.20.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.144.0

VMnet Information

○ Bridged (connect VMs directly to the external network)

Bridged to: Automatic

● NAT (shared host's IP address with VMs)

○ Host-only (connect VMs internally in a private network)

☑ Connect a host virtual adapter to this network

Host virtual adapter name: VMware Network Adapter VMnet8

☑ Use local DHCP service to distribute IP address to VMs

Subnet IP: 192 . 168 . 144 . 0   Subnet mask: 255 . 255 . 255 . 0

Change your subnet ip at 192.168.144.0 and then check the gateway ip

Go to control panel -> network and internet -> network connection

Here select the vm adapter and check the gateway that youenter in the onion

- ❖ Case 2:

In this you can use ip according to ip address range and select ip according to your own network .

---complete --