

# **SO Configuration Guide**

Created by

Harish. R

## **NOTE**

Security Onion 2.3.110 (SO) Operating system has been installed in the system as a Production standalone setup. This document is to record the configurations made during the initial setup on 6<sup>th</sup> April 2022 for future verifications. Further changes in the setup will be updated under this section.

#### **User Roles:**

- The user-created during installation will be considered as a "superuser" by default.
- Other users that are created manually after installation will be added as an "analyst".

### **Pre-requisites:**

- A bootable device with the latest SO iso image:
  - We have downloaded the latest version of security onion from their official site (https://github.com/Security-Onion-
  - <u>Solutions/securityonion/blob/master/VERIFY\_ISO.md</u>) and formatted the Pendrive as a bootable device with this iso image using the tool "Etcher"
  - [ Note: Formatting the Pendrive using the Rufus tool gives an error "Invalid signature check" during booting the image].
- 16 Gb RAM and 2 TB Hard disks are used for this installation

#### **Installation Screenshots:**

After mounting the USB device, the following configurations are performed.



Figure 1

```
Fultiple drives detected. Let's somer one questions.

Sevice Size

als SIIGS

There are 2 available diskip!

Which device senid you like to use as the operating system filesystem (must be larger than 79 GH);

als

als SIIGS - US Brive

shuld you like to use the same device for RSM storage? (yearns)

so

Sovice Size

als SIIGS

which device would you like to use for RSM storage;

als SIIGS

which device would you like to use for RSM storage;

als
```

Figure 2

Figure 3

```
SUBSTRACT OF A DESCRIPTION ALL DATA OF A DESCRIPTION AND A
```

Figure 4

Figure 5

```
Harting installer, one means an analysis of the foreign of the second 21.40.22.147-2 for Gents 2 wasper and the installation and the installation and the installation are providing for STV2 and an approve state of the second control of the se
```

Figure 6

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

Figure 7

```
CentOS Limax 7 (Core)
Kernel 3.18.8-1168.55.1 e17.x66_64 on an x86_64
localbort login: cysonion
```

Figure 8

```
CentOS Linux 7 (Core)
Servel 3.18.8-1168.59.1.c17.x[0_64 on an x86_64
localhest login: cynonion
Password:
```

Figure 9

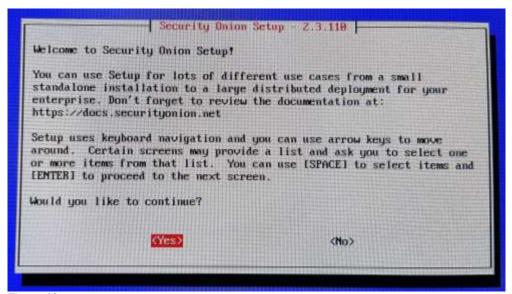


Figure 10



Figure 11

Figure 12 - Standalone mode was selected

Security Unio	n Setup - 2.3.110
Starting in Elastic Stack version only available under the Elastic https://securityonion.net/elastic	7.11, the Elastic Stack binaries are License: -license
Please review the Elastic License https://www.elastic.co/licensing/e	
Do you agree to the terms of the I	Elastic License?
If so, type AGREE to accept the El Otherwise, press Enter to exit thi	astic License and continue. is program without making any changes.
AGREE	
<0k>	<cancel></cancel>

Figure 13

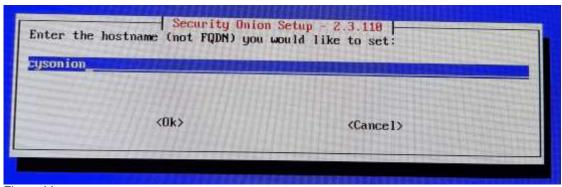


Figure 14

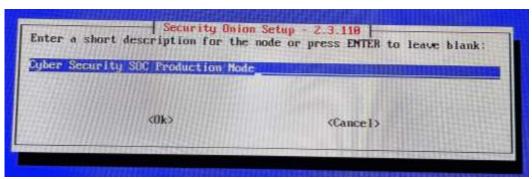


Figure 15

```
Please select your management NIC:

| Company | Concel |
```

Figure 16

```
Choose how to set up your management interface:

(**) STATIC Set a static IPv1 address
(**) DHCP Use DHCP to configure the Management Interface

(Ok)

(Cancel)
```

Figure 17

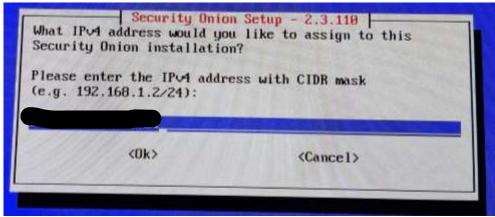


Figure 18

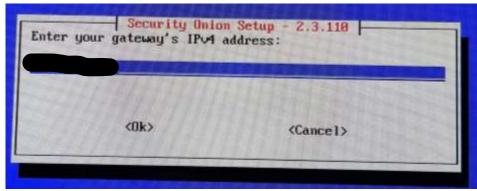


Figure 19

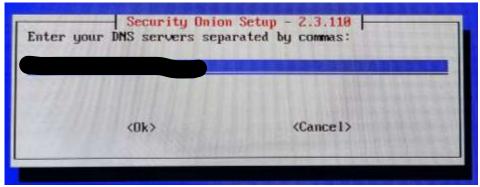


Figure 20

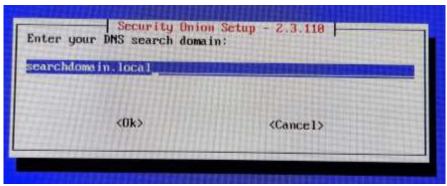


Figure 21

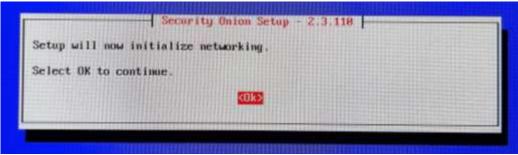


Figure 22

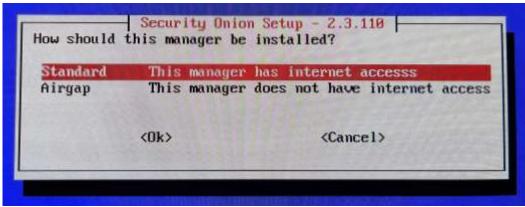


Figure 23

```
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)
```

Figure 24

```
Security Onion Setup - 2.3.110

Running preflight checks...
```

Figure 25

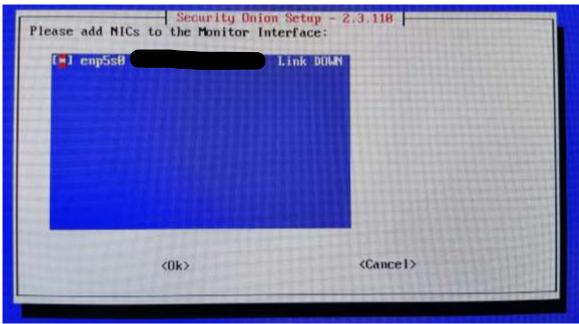


Figure 26

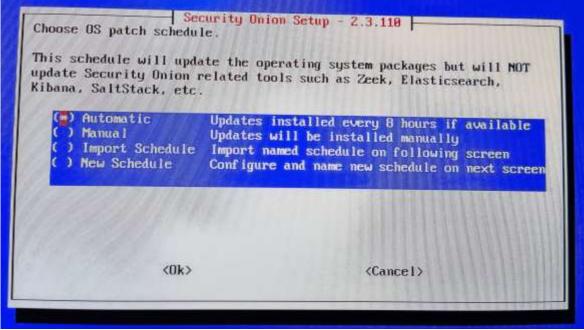


Figure 27

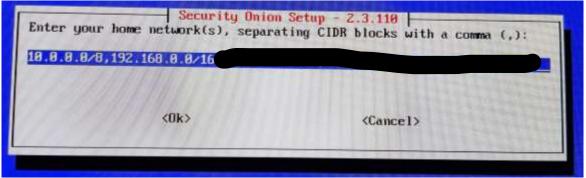


Figure 28

Figure 29

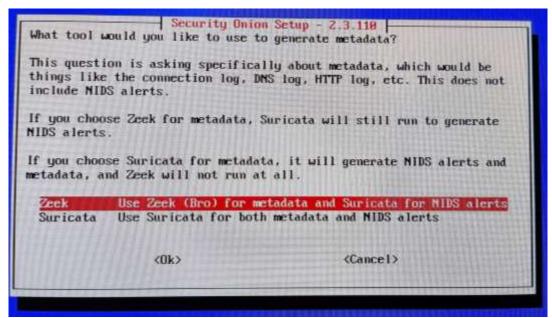


Figure 30

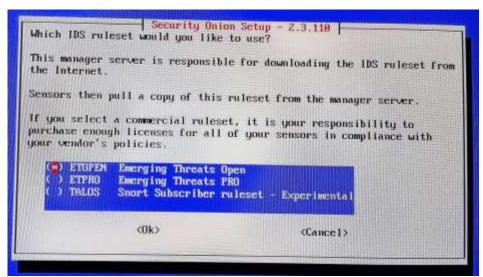


Figure 31

Figure 32

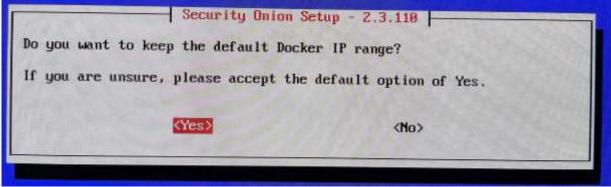


Figure 33

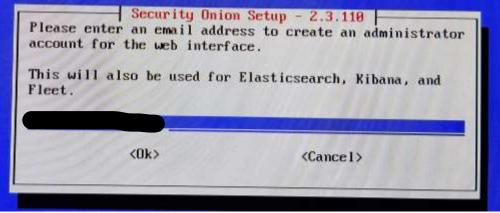


Figure 34

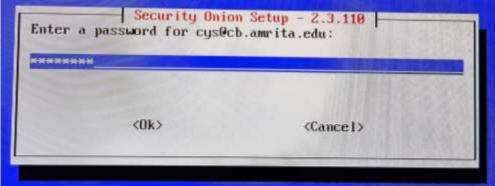


Figure 35

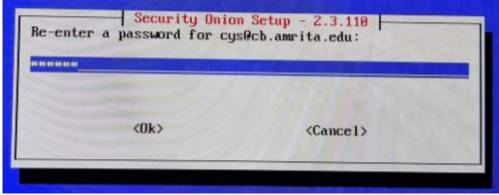


Figure 36

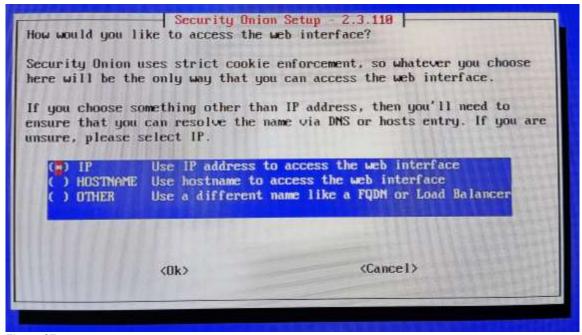


Figure 37

```
Set a password for the soremote user. This account is used for adding sensors remotely.
```

Figure 38

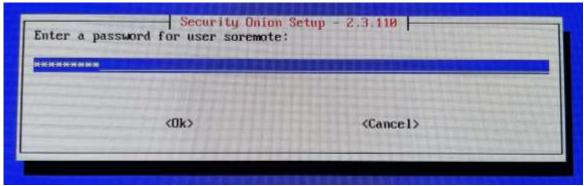


Figure 39

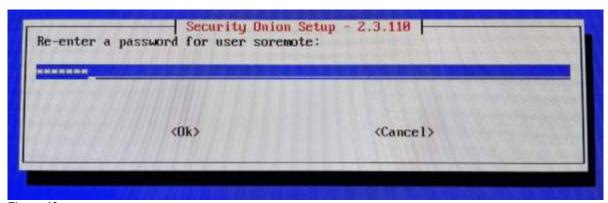


Figure 40

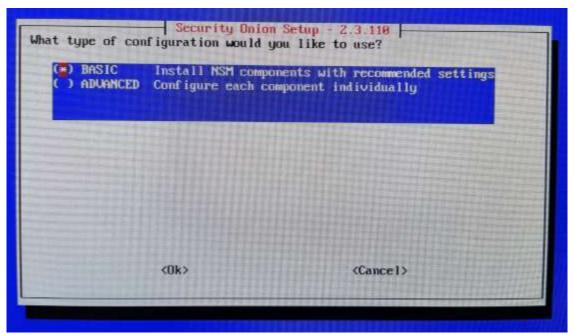


Figure 41

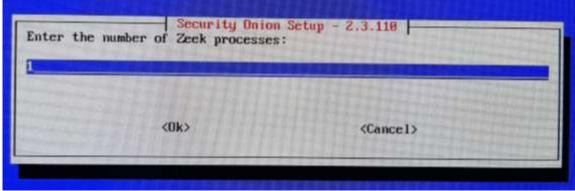


Figure 42

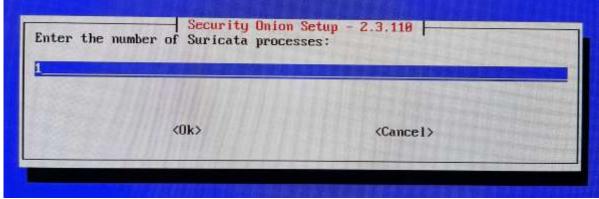


Figure 43

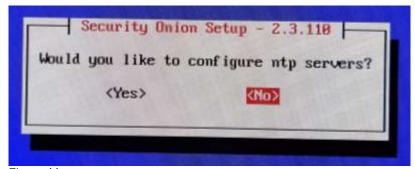


Figure 44

Figure 45

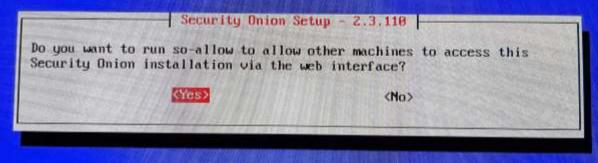


Figure 46

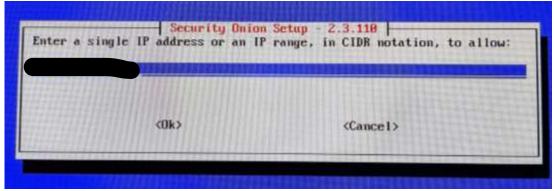


Figure 47

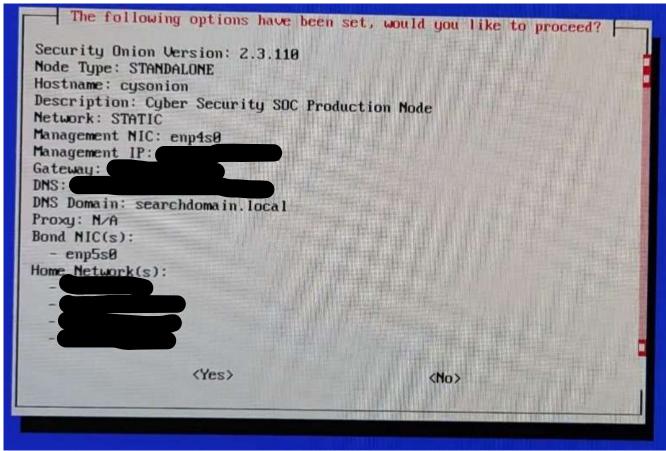


Figure 48

```
Updating packages

ZX
```

Figure 49

```
Security Onion Setup - 2.3.118

Pinished STANDALONE installation.

Access the web interface at: https:/

Press ENTER to reboot.
```

Figure 50

Figure 51

```
tent fortied begins and for 10 cm this cm commonly language and the first of the fi
```

Figure 52

## **FINAL SUMMARY**

After this installation and configuration, the GUI of security Onion can be accessed by typing "configured ip/hostname" on the browsers of any system in the same LAN. So, these are the configurations performed to install the security onion successfully in standalone mode.

### **References**

- https://securityonionsolutions.com/software/
- https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY\_ISO.md
- https://docs.securityonion.net/en/2.3/
- https://chrissanders.org/2017/06/security-onion-cheat-sheet/