



Provision & Setup Security Onion

>pr0jectsecurity_

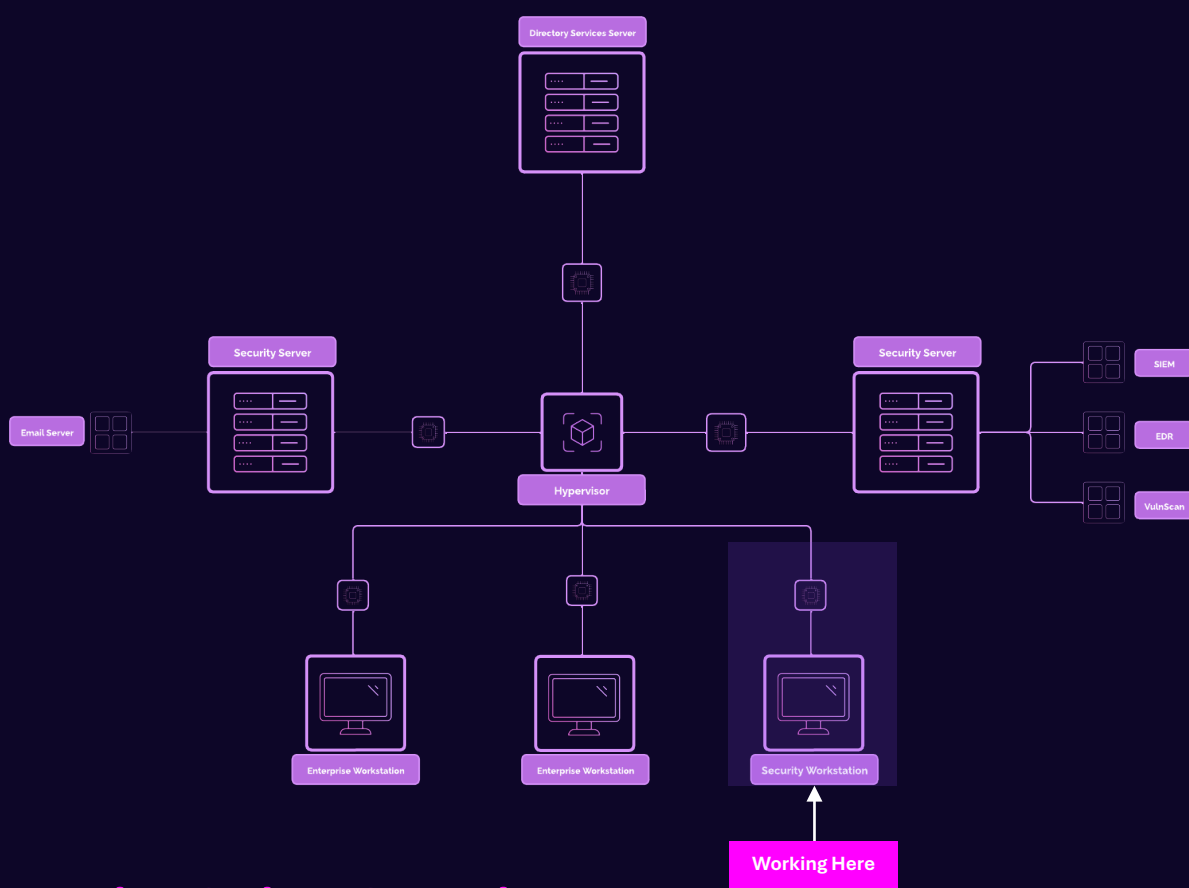
Table of Contents

Table of Contents	2
Prerequisites	3
Network Topology	3
Security Onion Overview	3
What is Security Onion?	3
How is Security Onion Used?.....	4
Security Implications	4
Setup Security Onion	5
Step 1	5
Step 2	6
Step 3	9

Prerequisites

1. Virtualbox installed.
2. Virtual Machine with Security Onion ISO has been configured and provisioned (the ISO should be attached to the new VM).
3. Security Onion Virtual Machine has at least 50.00 GB of dynamic storage available.
4. Windows Server 2025 with AD Directory Services (ADDS) configured.

Network Topology



Security Onion Overview

What is Security Onion?

Security Onion is a free, open-source platform for network security monitoring (NSM), log management, and intrusion detection. It provides a comprehensive suite of tools designed to help analysts detect, investigate, and respond to cyber threats in real time. Think of Security Onion as the operating system equivalent of Kali Linux. Security Onion comes set

with a suite of preconfigured tools, including Zeek (formerly Bro), Suricata, and Elastic Stack (Elasticsearch, Logstash, and Kibana).

How is Security Onion Used?

Security Onion is used for a wide range of security monitoring and incident response tasks:

1. Network Security Monitoring (NSM)

- **Packet Capture and Analysis:** Tools like Zeek analyze network traffic for anomalies or suspicious activity.
- **Intrusion Detection Systems (IDS):** Suricata performs real-time deep packet inspection to identify malicious activity.

2. Log Management and Analysis

- Collects and aggregates logs from endpoints, firewalls, servers, and other devices to provide visibility into network activity.
- Elastic Stack enables querying, visualizing, and analyzing logs in an intuitive dashboard.

3. Incident Response

- **Alerts and Correlation:** Generates alerts for suspicious activities, helping analysts prioritize threats.
- **Threat Hunting:** Analysts can proactively search for signs of compromise using enriched datasets.

Security Implications

Security Onion plays a critical role in enhancing an organization's security posture by providing advanced detection and monitoring capabilities.

- **Proactive Threat Detection:** Identifies threats before they escalate, reducing the impact of cyberattacks.
- **Comprehensive Visibility:** Aggregates network and endpoint data for a holistic view of the environment.
- **Incident Response Readiness:** Equips analysts with tools to quickly investigate and respond to alerts.

Best Practice - Separate Monitoring Infrastructure: Keep Security Onion servers isolated to minimize the risk of compromise.

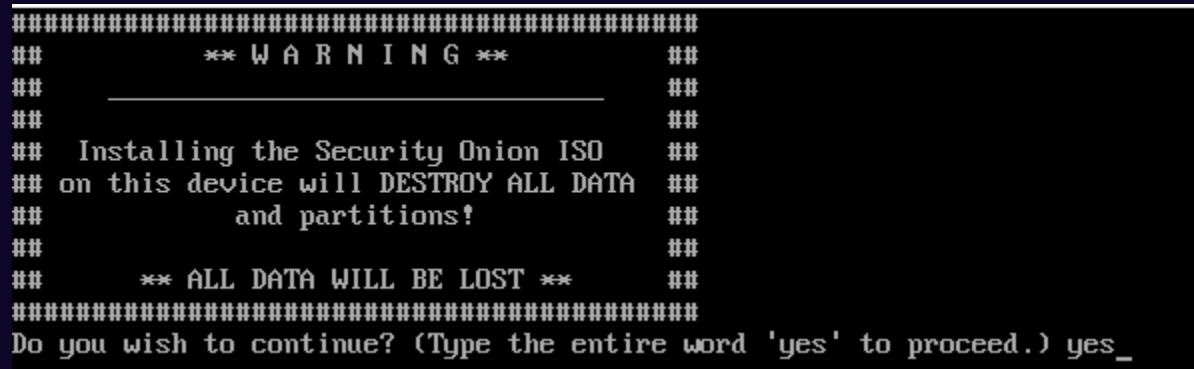
Setup Security Onion

Step 1

Arrow down to “Install Security Onion 2.4.110 Desktop”. Hit “Enter”.



Type “Yes”. Hit “Enter” button.



Create a new administrator account, project-x-sec-work. A new password prompt will appear, use the user password (@password123!).

👉 Refer to the “[Project Overview](#)” guide for more information on default usernames and passwords.

A new administrative user will be created. This user will be used for setting up and administering Security Onion.

Enter an administrative username: project-x-sec-work_

Allow for the system to install, this may take a few minutes.

>projectsecurity_

```

Installing brasero-libs.x86_64 (930/1108)
Installing colord-gtk.x86_64 (931/1108)
Installing gnome-color-manager.x86_64 (932/1108)
Installing gnome-control-center.x86_64 (933/1108)
Installing gstreamer1-plugins-good-gtk.x86_64 (934/1108)
Installing gnome-tour.x86_64 (935/1108)
Installing ibus-gtk3.x86_64 (936/1108)
Installing system-config-printer-libs.noarch (937/1108)
Installing vte291.x86_64 (938/1108)
Installing gnome-terminal.x86_64 (939/1108)
Installing xdg-user-dirs-gtk.x86_64 (940/1108)
Installing ibus-gtk2.x86_64 (941/1108)
Installing gtk2.x86_64 (942/1108)
Installing libcanberra-gtk2.x86_64 (943/1108)
Installing ibus-setup.noarch (944/1108)
Installing ibus.x86_64 (945/1108)
Installing gdm.x86_64 (946/1108)
Installing gnome-session-wayland-session.x86_64 (947/1108)
Installing gnome-session-xsession.x86_64 (948/1108)
Installing gnome-shell-extension-background-logo.noarch (949/1108)
Installing gnome-shell.x86_64 (950/1108)
Installing gnome-shell-extension-common.noarch (951/1108)
Installing gnome-shell-extension-apps-menu.noarch (952/1108)
Installing gnome-shell-extension-desktop-icons.noarch (953/1108)
Installing gnome-shell-extension-launch-new-instance.noarch (954/1108)
Installing gnome-shell-extension-places-menu.noarch (955/1108)
Installing gnome-shell-extension-window-list.noarch (956/1108)
Installing adobe-mappings-pdf.noarch (957/1108)
Installing libgs.x86_64 (958/1108)
Installing ghostscript-tools-fonts.x86_64 (959/1108)
Installing ghostscript-tools-printing.x86_64 (960/1108)
Installing ghostscript.x86_64 (961/1108)
Installing cups-filters.x86_64 (962/1108)
Installing cups.x86_64 (963/1108)
Installing foomatic-db-ppds.noarch (964/1108)

```

[anaconda11:main* 2:shell 3:log 4:storage-log 5:program-log Switch tab: Alt+Tab | Help: F1]

Hit “Enter” when the installation has been completed.

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

Step 2

Let the VM reboot, then enter username and password.

```
localhost login: project-x-sec-work
Password: _
```

Select “Yes”.

```

Security Union Setup - 2.4.118

Welcome to Security Union 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.securityunion.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>

```

Enter the following hostname.

Security Onion Setup - 2.4.110

Enter the hostname (not FQDN) you would like to set:

project-x-sec-work

<Ok> <Cancel>

Hit "Enter" until you get to the IPv4 address. Add the IP address (10.0.0.103/24).

Security Onion Setup - 2.4.110

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):

10.0.0.103/24

<Ok> <Cancel>

Add the default gateway (10.0.0.1).

Security Onion Setup - 2.4.110

Enter your gateway's IPv4 address:

10.0.0.1

<Ok> <Cancel>

Yes the default DNS servers provided.

Security Onion Setup - 2.4.110

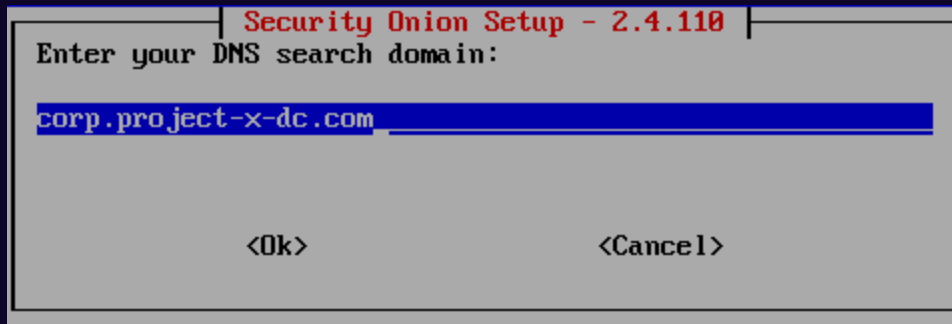
Enter your DNS servers separated by commas:

8.8.8.8,8.8.4.4

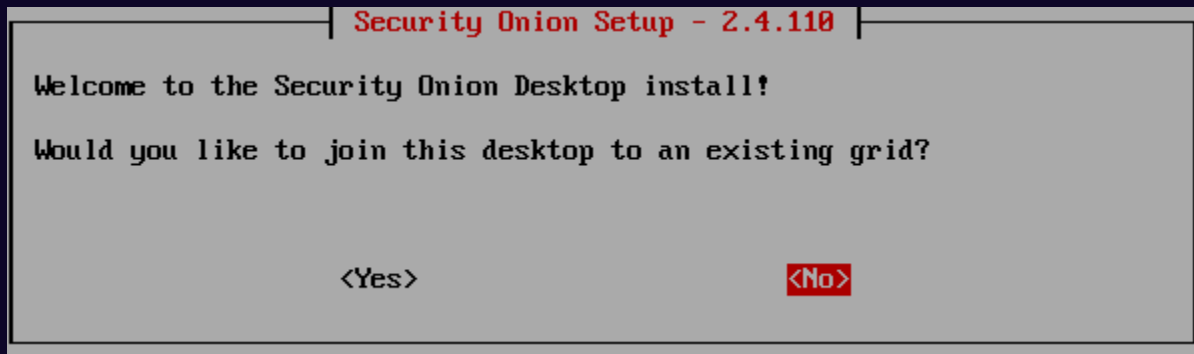
<Ok> <Cancel>

Add in the DNS, corp.project-x-dc.com.

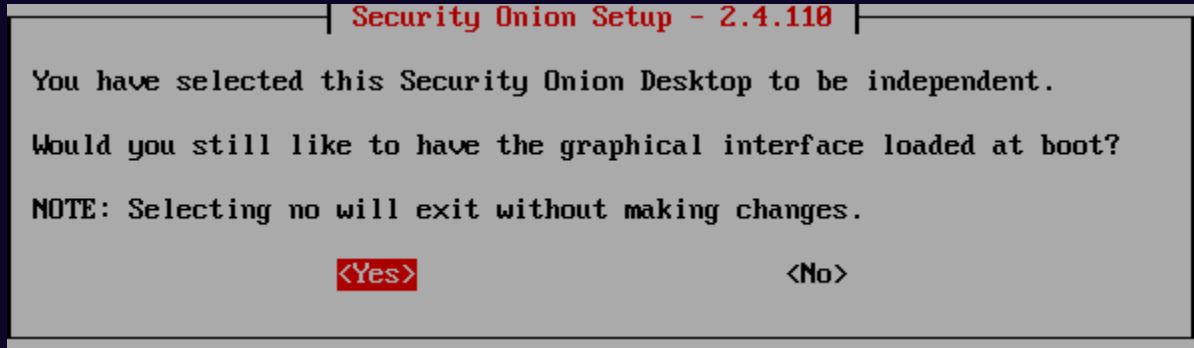
>projectsecurity_



Select the default "No". Hit "Enter".



Use the Left Arrow Key to select "Yes".



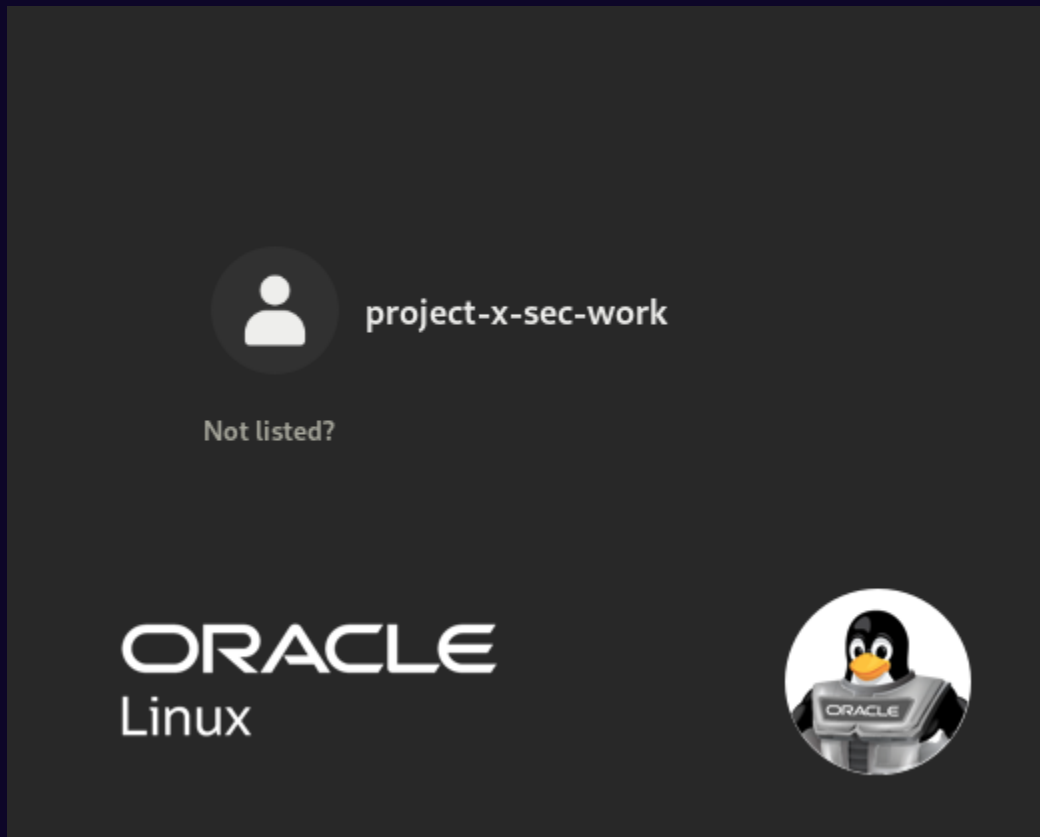
The graphical menu will close and return to a terminal. Enter a reboot command to restart the machine.

reboot

```
Please reboot to start graphical interface.  
[project-x-sec-work@localhost ~]# reboot_
```

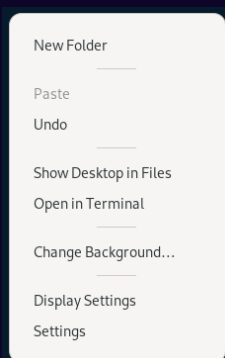
Success! Log into Security Onion.

>pr0jectsecurity_



Step 3

Open a new terminal session. Right-click the desktop, select Open in Terminal.

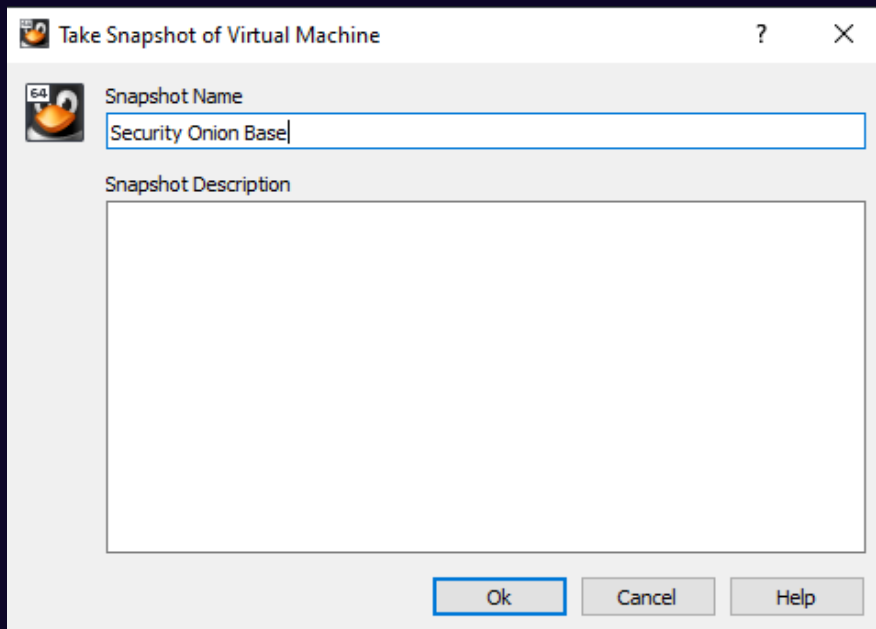


Issue the following command to change the root password to (@password123!).

```
sudo passwd root
```

```
[project-x-sec-work@project-x-sec-work VBox_GAs_7.0.22]$ sudo passwd root
[sudo] password for project-x-sec-work:
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
```

Take Snapshot!



Take Snapshot of Virtual Machine

Snapshot Name

Security Onion Base

Snapshot Description

Ok Cancel Help