Provision & Setup Security Onion

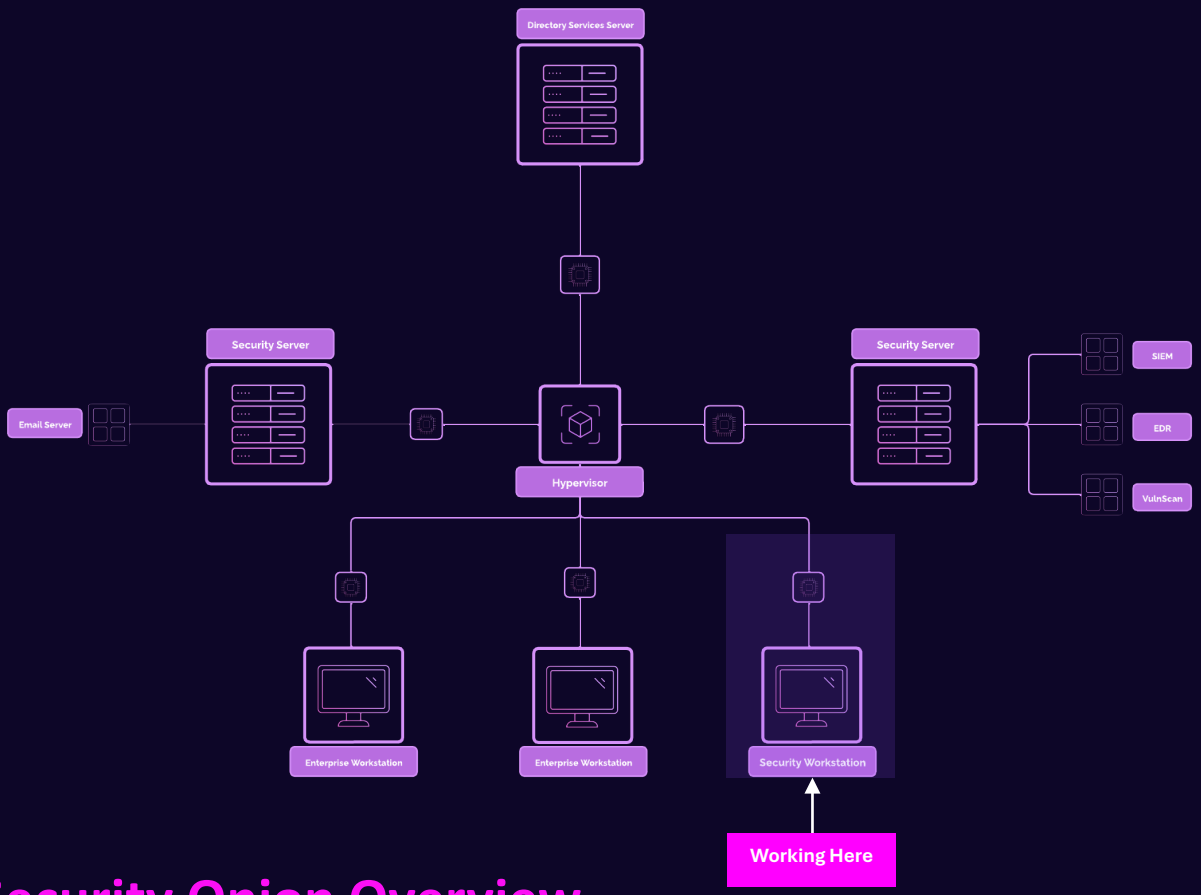
>projectsecurity_

Table of Contents

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

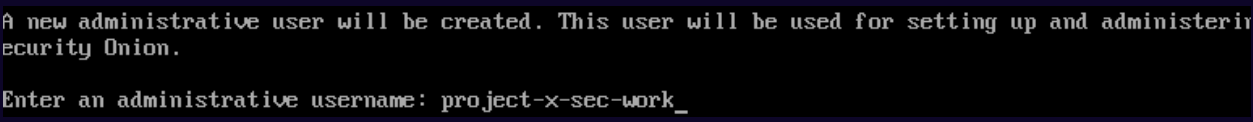
Step 1

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

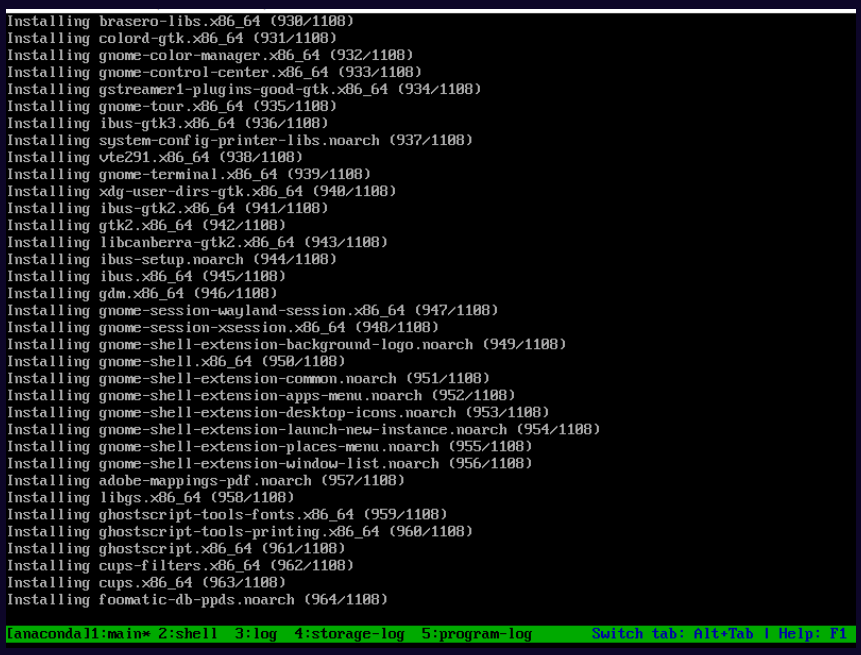
Type “Yes”. Hit “Enter” button.

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.



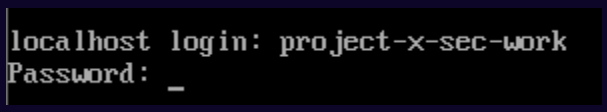
Allow for the system to install, this may take a few minutes.



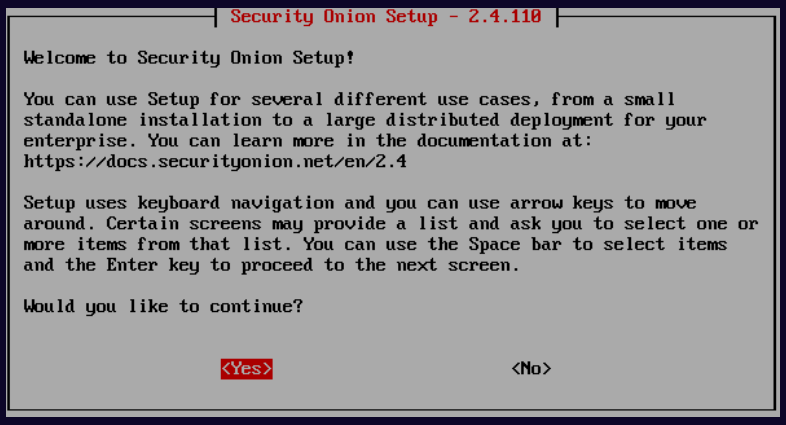
Hit “Enter” when the installation has been completed.

Step 2

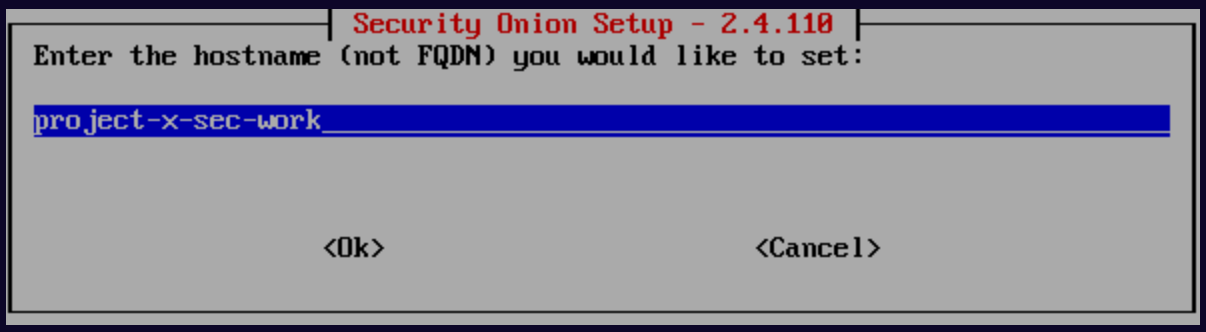
Let the VM reboot, then enter username and password.



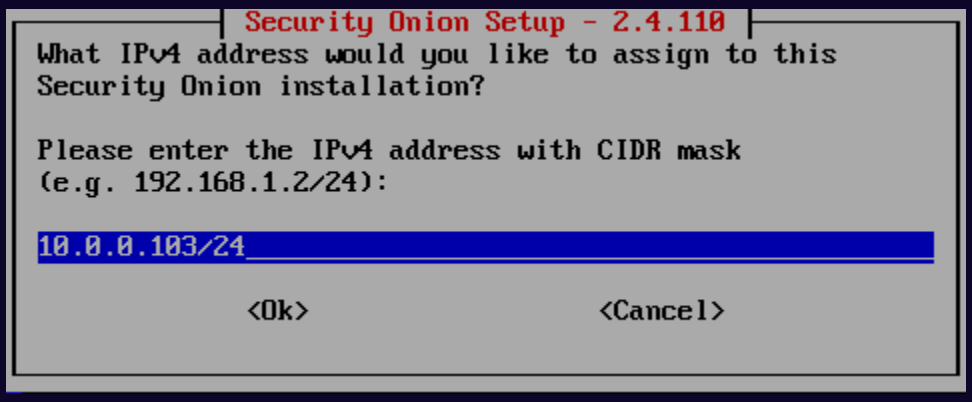
Select “Yes”.



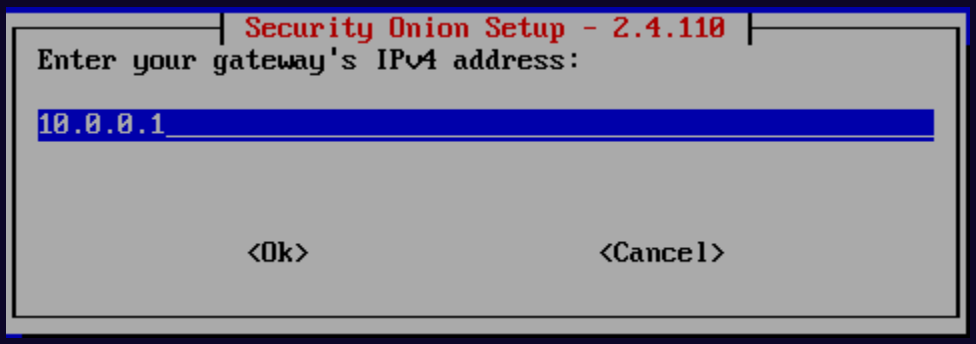
Enter the following hostname.



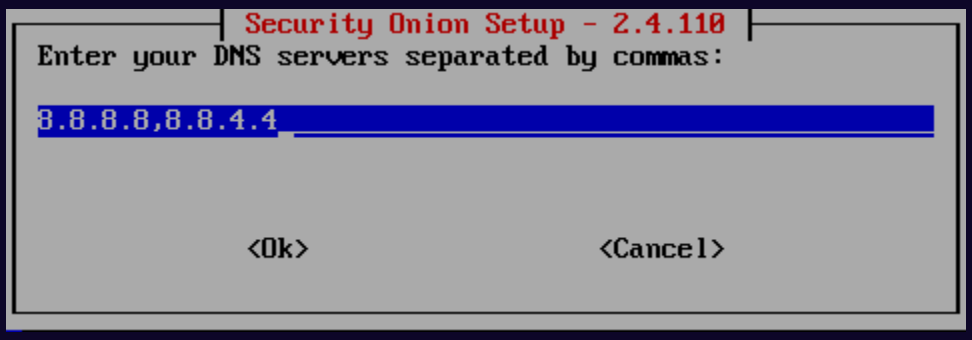
Hit “Enter” until you get to the IPv4 address. Add the IP address (10.0.0.103/24).



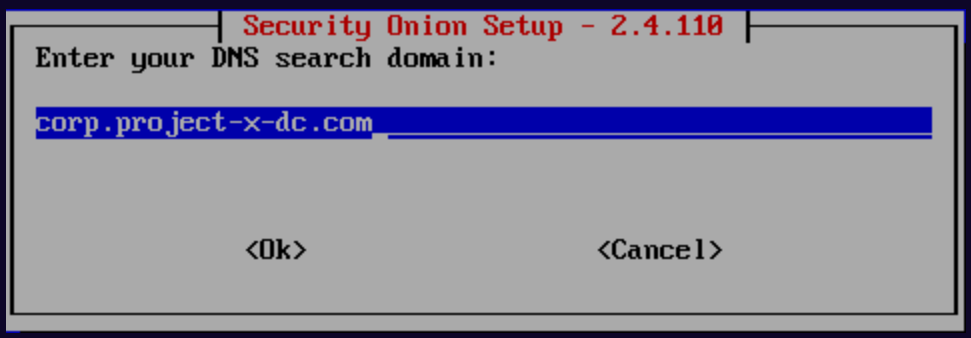
Add the default gateway (10.0.0.1).



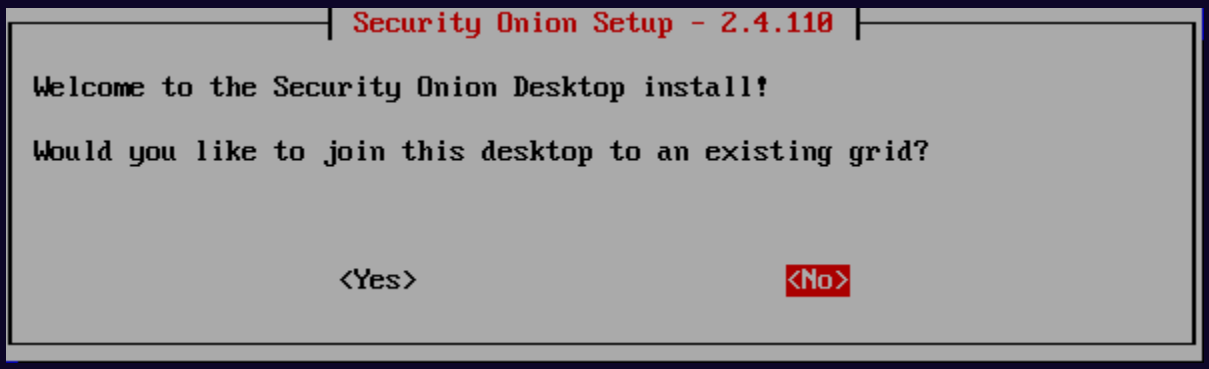
Yes the default DNS servers provided.



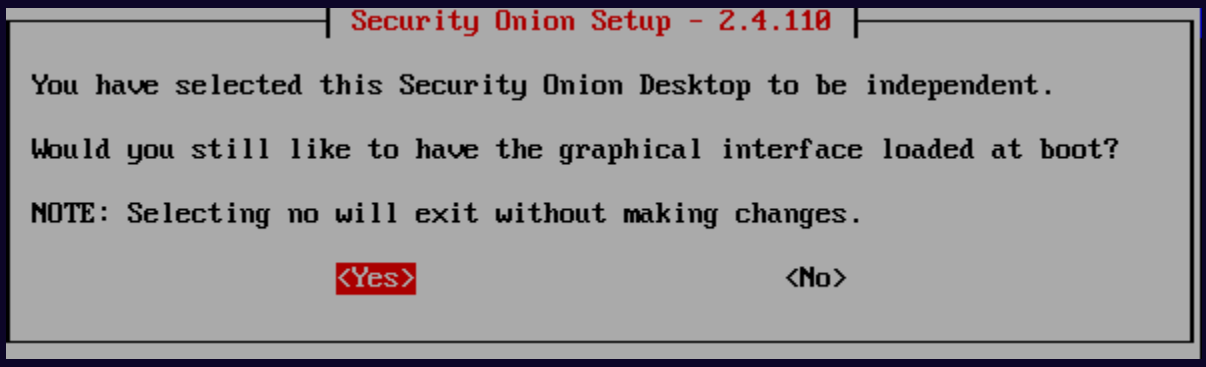
Add in the DNS, corp.project-x-dc.com.



Select the default “No”. Hit “Enter”.



Use the Left Arrow Key to select “Yes”.

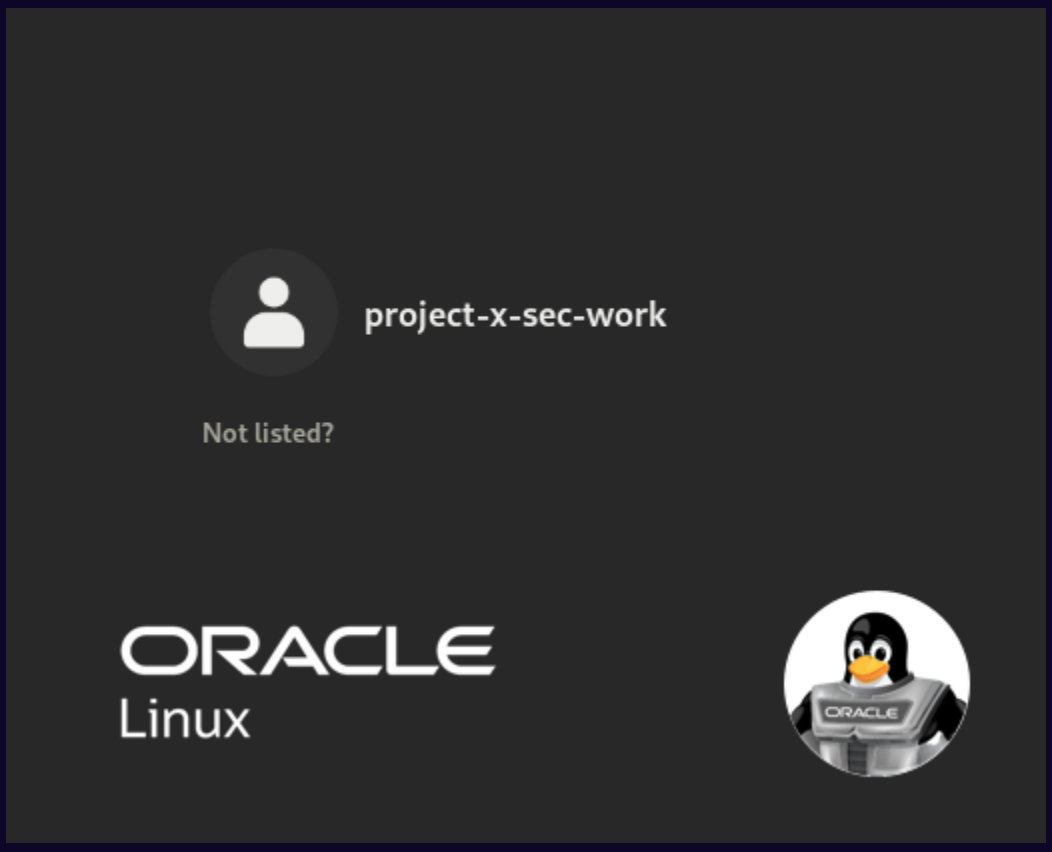


The graphical menu will close and return to a terminal. Enter a reboot command to restart the machine.

```
reboot
```

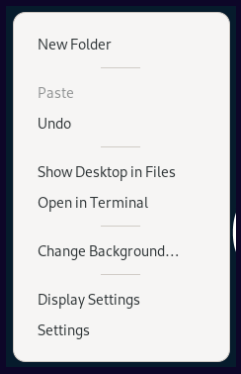
```
Please reboot to start graphical interface.
[project-x-sec-work@localhost ~]$ reboot_
```

Success! Log into Security Onion.



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!**