**Security Onion Installation for presenting my work**

**ALWAYS verify the checksum of the ISO image before booting! This ensures that the ISO image hasn’t been tampered with or corrupted during download. If it fails to verify, try downloading again. If it still fails to verify, try downloading from another computer or another network.**

**A screen shot of a computer

Description automatically generated**

**Download and verify our ISO image as shown at**[**https://github.com/Security-Onion-Solutions/securityonion/blob/2.4/main/DOWNLOAD\_AND\_VERIFY\_ISO.md**](https://github.com/Security-Onion-Solutions/securityonion/blob/2.4/main/DOWNLOAD_AND_VERIFY_ISO.md)**.**

**Antivirus software may alert on the ISO image but any alerts are most likely false positives. If you look at the antivirus scan details, it will most likely tell you that it alerted on a file in SecurityOnion\agrules\. These are rules that look for malicious activity but the rules themselves are not actually malicious.**

**Minimum Specs**[**ℑ**](https://docs.securityonion.net/en/2.4/hardware.html#minimum-specs)

| **Node Type** | **CPUs** | **RAM** | **Storage** | **NICs** |
| --- | --- | --- | --- | --- |
| **Import** | **2** | **4GB** | **50GB** | **1** |
| **Eval** | **4** | **8GB** | **200GB** | **2** |
| **Standalone** | **4** | **16GB** | **200GB** | **2** |
| **Manager** | **4** | **16GB** | **200GB** | **1** |
| **ManagerSearch** | **8** | **16GB** | **200GB** | **1** |
| **Search node** | **4** | **16GB** | **200GB** | **1** |
| **Sensor** | **4** | **12GB** | **200GB** | **2** |
| **Heavy node** | **4** | **16GB** | **200GB** | **2** |
| **IDH node** | **2** | **1GB** | **12GB** | **1** |
| **Fleet node** | **4** | **4GB** | **200GB** | **1** |
| **Receiver node** | **2** | **8GB** | **200GB** | **1** |

**Eval**

**An Eval installation runs the minimal processes required for a single machine to sniff live network traffic from a TAP or span port and view the results. Therefore, its hardware requirements are higher than Import as shown in the table above. Eval is designed for temporary installations or homelab installations on a budget. Unlike a full Standalone installation, Evaluation is NOT designed for production usage.**

**In order to minimize RAM usage, Eval does not run**[**Logstash**](https://docs.securityonion.net/en/2.4/logstash.html#logstash)**or**[**Redis**](https://docs.securityonion.net/en/2.4/redis.html#redis)**at all. Also, Eval defaults to using**[**Suricata**](https://docs.securityonion.net/en/2.4/suricata.html#suricata)**for writing full packet capture to disk (instead of**[**Stenographer**](https://docs.securityonion.net/en/2.4/stenographer.html#stenographer)**).**

**NIC**

**You’ll need at least one wired network interface dedicated to management (preferably connected to a dedicated management network). We recommend using static IP addresses where possible.**

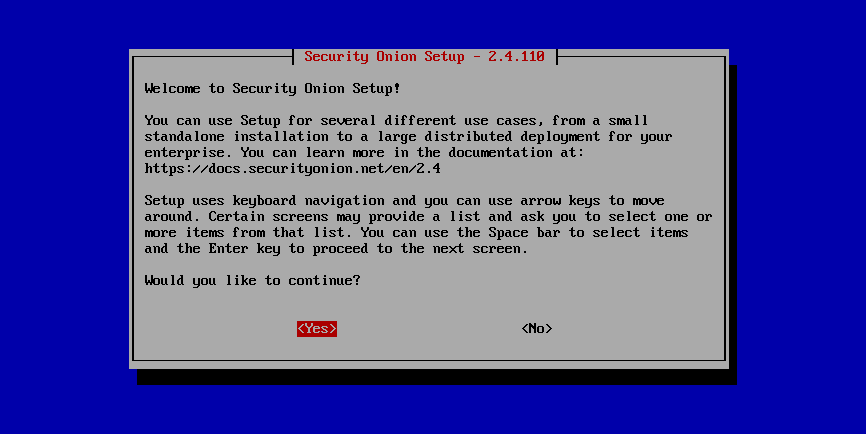
**If you plan to sniff network traffic from a tap or span port, then you will need one or more interfaces dedicated to sniffing (no IP address). The installer will automatically disable NIC offloading functions such as tso, gso, and gro on sniffing interfaces to ensure that**[**Suricata**](https://docs.securityonion.net/en/2.4/suricata.html#suricata)**and**[**Zeek**](https://docs.securityonion.net/en/2.4/zeek.html#zeek)**get an accurate view of the traffic.**

**Make sure you get good quality network cards, especially for sniffing. Most users report good experiences with Intel cards.**

**Security Onion is designed to use wired interfaces. You may be able to make wireless interfaces work, but we don’t recommend or support it.**

**Security Onion Setup will automatically start. If for some reason you have to exit Setup and need to restart it, you can log out of your account and then log back in and it should automatically start. If that doesn’t work, you can manually run it as follows:**

**sudo SecurityOnion/setup/so-setup iso**



**Import**

**One of the easiest ways to get started with Security Onion is using it to forensically analyze pcap and log files. Simply select the IMPORT option, follow the prompts, and then import pcap files or Windows event logs in EVTX format using the**[**Grid**](https://docs.securityonion.net/en/2.4/grid.html#grid)**page.**

**Evaluation**

**Evaluation mode is ideal for classroom or small lab environments. Evaluation is not designed for production usage. Choose the EVAL option, follow the prompts, and then proceed to the**[**After Installation**](https://docs.securityonion.net/en/2.4/post-installation.html#post-installation)**section.**

**Production Server - Standalone**

**Standalone is similar to Evaluation in that it only requires a single box, but Standalone is more ready for production usage. Choose STANDALONE, follow the prompts, and then proceed to the**[**After Installation**](https://docs.securityonion.net/en/2.4/post-installation.html#post-installation)**section.**

**Production Server - Distributed Deployment**

**If deploying a distributed environment, install and configure the manager node first and then join the other nodes to it. For best performance, the manager node should be dedicated to just being a manager for the other nodes (the manager node should not do any network sniffing, that should be handled by dedicated forward nodes).**

**Build the manager by running Setup, selecting the DISTRIBUTED deployment option, and choosing the  option. You can choose either MANAGER or MANAGERSEARCH. If you choose MANAGER, then you must join one or more search nodes (this is optional if you choose MANAGERSEARCH) and you will want to do this before you start joining other node types.**

**Build nodes by running Setup, selecting the DISTRIBUTED deployment option, choosing Existing Deployment, and selecting the appropriate option. Please note that all nodes will need to be able to connect to the manager node on several ports and the manager will need to connect to search nodes and heavy nodes. You’ll need to make sure that any network firewalls have firewall rules to allow this traffic as defined in the**[**Firewall**](https://docs.securityonion.net/en/2.4/firewall.html#firewall)**section. In addition to network firewalls, you’ll need to make sure the manager’s host-based firewall allows the connections. You can do this in two ways. The first option is going to**[**Administration**](https://docs.securityonion.net/en/2.4/administration.html#administration)**–> Configuration –> firewall –> hostgroups, selecting the appropriate node type, and adding the IP address. The second option is to wait until the node tries to join and it will prompt you to run a specific command on the manager. Regardless of which of the two options you choose, it will eventually prompt you to go to**[**Administration**](https://docs.securityonion.net/en/2.4/administration.html#administration)**–> Grid Members, find the node in the Pending Members list, click the Review button, and then click the Accept button.**