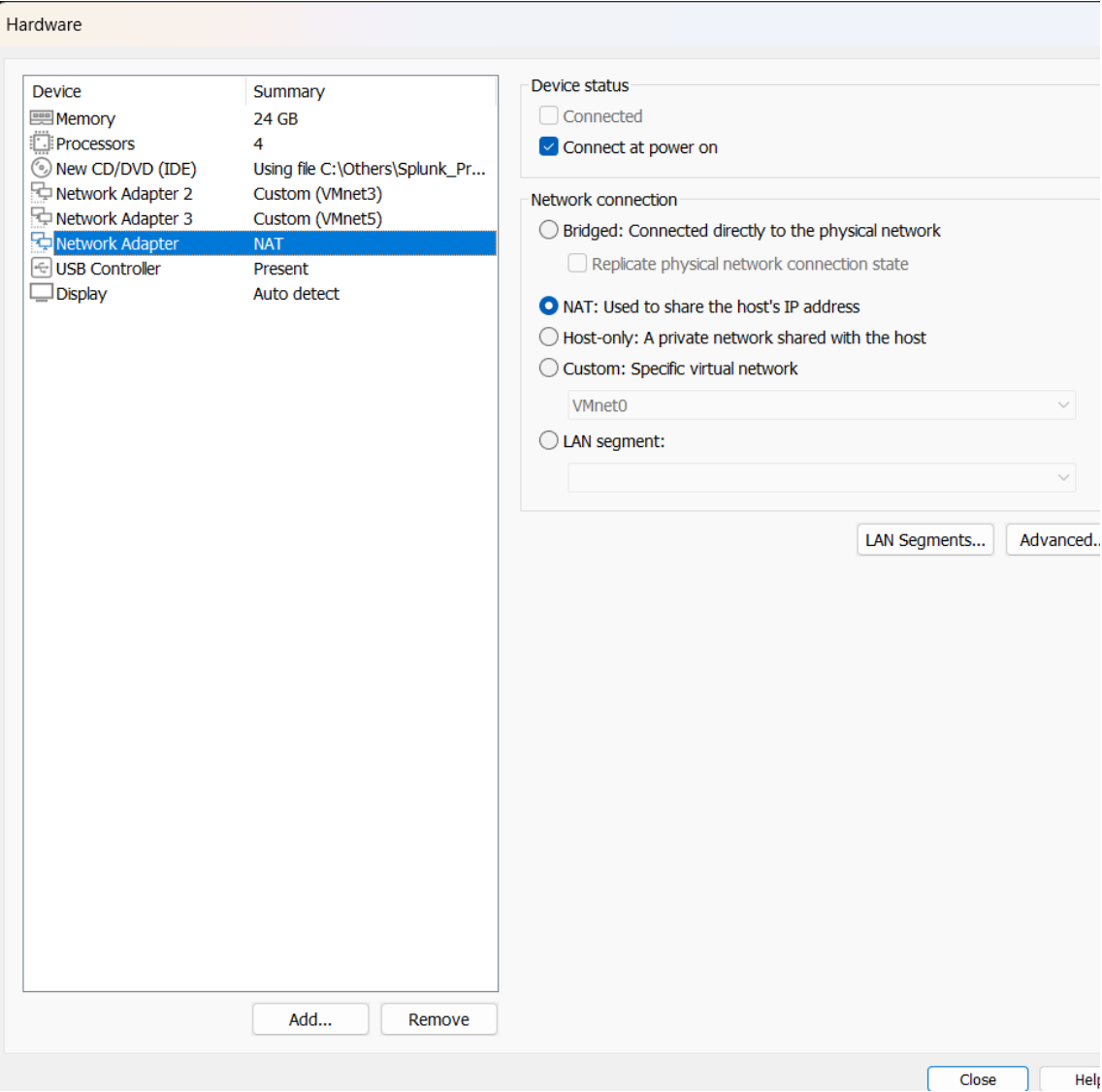
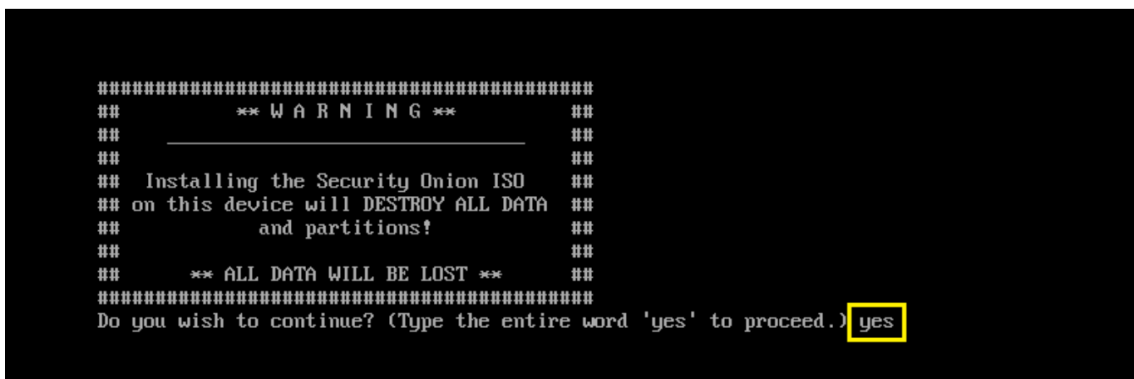
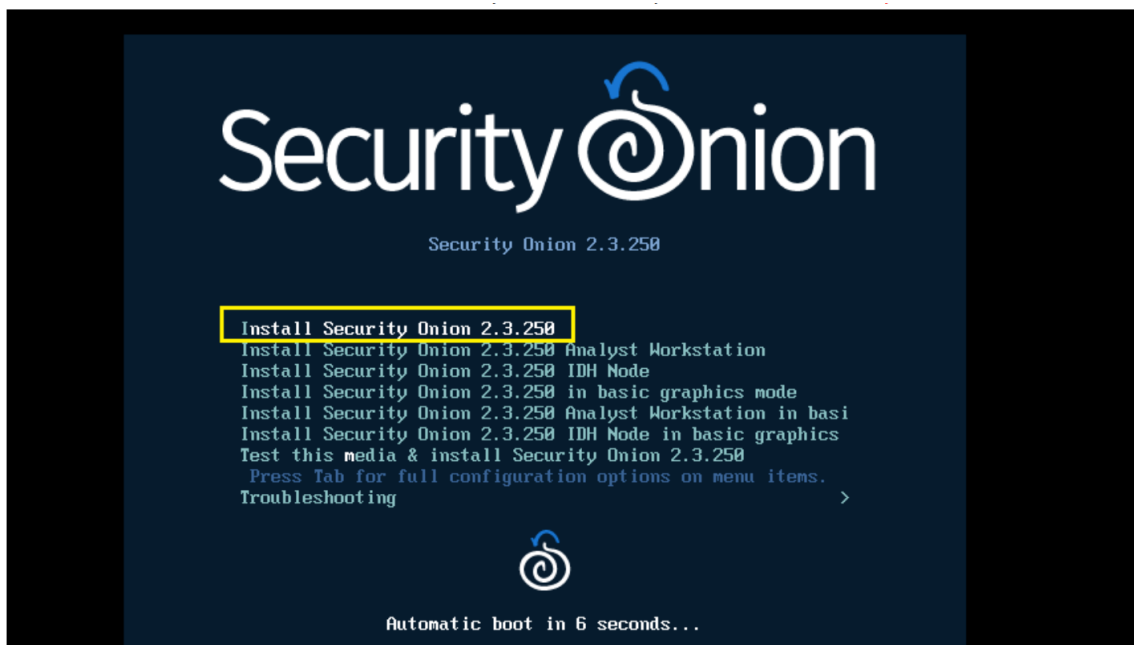


# Security Onion Installation

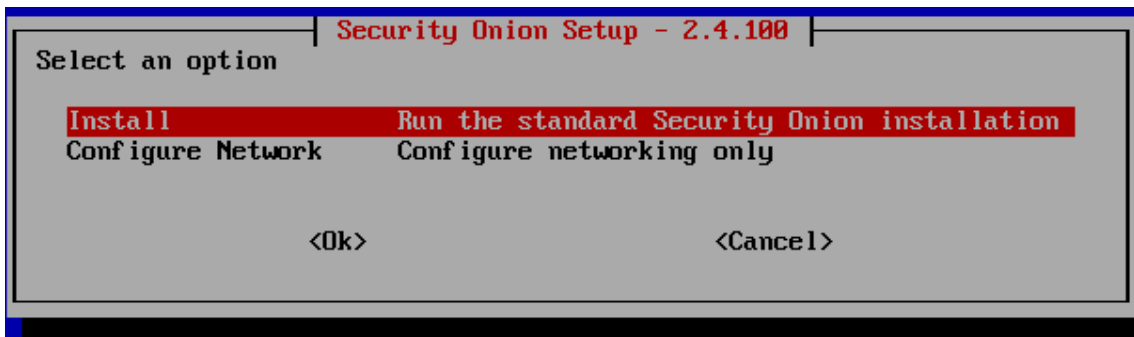
Download Security Onion, I used version 2.4.100-20240903.

1. **Create a New Virtual Machine** and choose **Typical**
2. Browse **securityonion-2.4.100-20240903.iso**
3. Name the virtual machine and Next
4. Configure Maximum disk size to **250GB** and **Store virtual disk as a single file**
5. **Customize Hardware** and change memory to **16GB or more**, processors to **4**. Then **Add two Network Adapter**. Network Adapter(NAT) is connected to public network,
6. Network Adapter 2(VMnet3) is SPAN port to receive traffic copies from LAN, Network Adapter 3(VMnet5) is under subnet 192.168.4.x/24





7. After reboot, choose **Install** and **OK**



7. **EVAL** and **OK**



## 8. AGREE

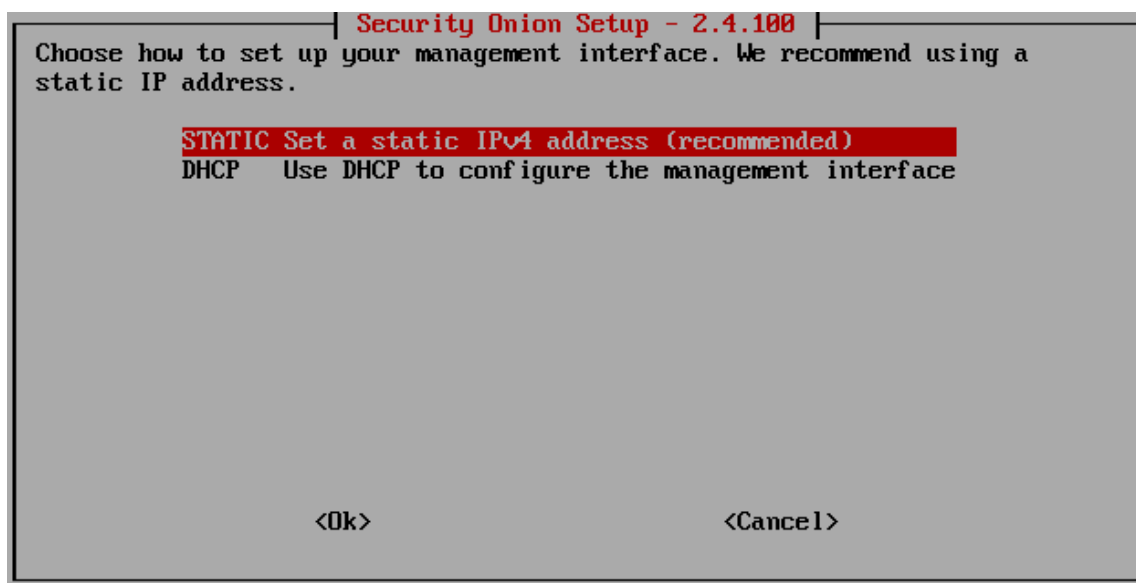
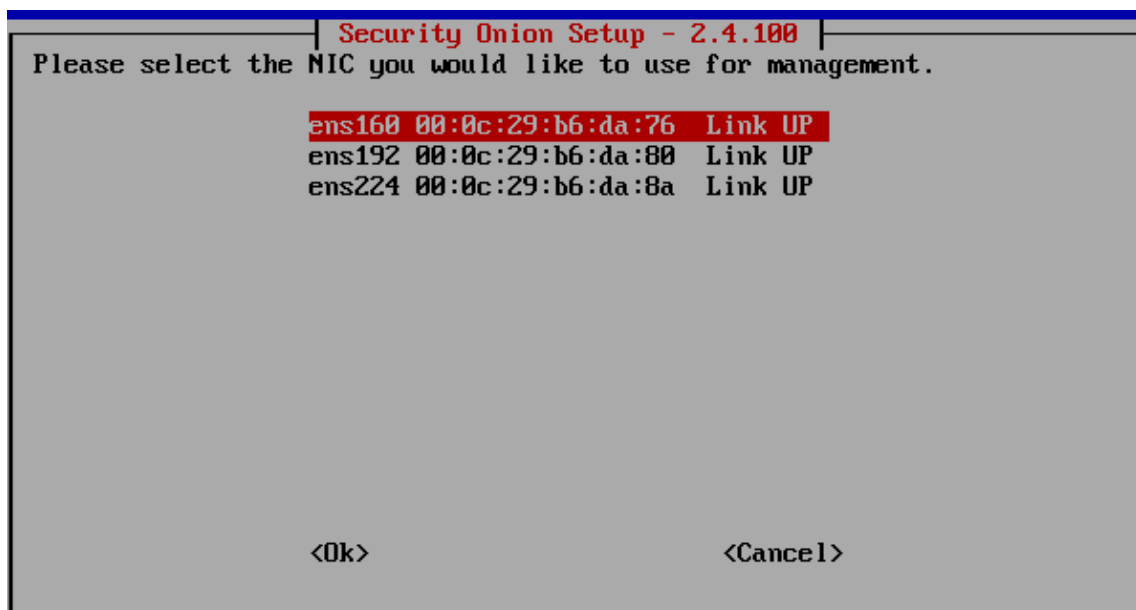
Security Union Setup - 2.4.100	
<p>Elastic Stack binaries and Security Union components are only available under the Elastic License version 2 (ELv2): <a href="https://securityunion.net/license/">https://securityunion.net/license/</a></p> <p>Do you agree to the terms of ELv2?</p> <p>If so, type AGREE to accept ELv2 and continue. Otherwise, press Enter to exit this program without making any changes.</p> <p><b>AGREE</b></p> <p>&lt;Ok&gt; &lt;Cancel&gt;</p>	

## 9. Standard

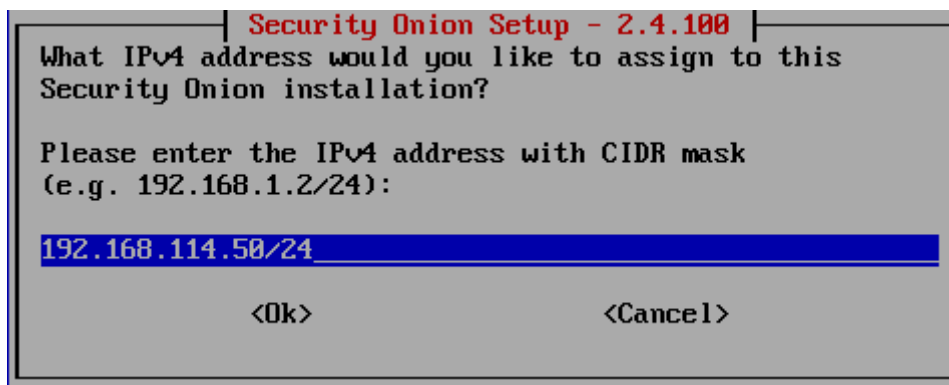
Security Union Setup - 2.4.100					
<p>How should this node be installed?</p> <p>For more information, please see: <a href="https://docs.securityunion.net/en/2.4/airgap.html">https://docs.securityunion.net/en/2.4/airgap.html</a></p> <table><tr><td><b>Standard</b></td><td><b>This node has access to the Internet</b></td></tr><tr><td>Airgap</td><td>This node does not have access to the Internet</td></tr></table> <p>&lt;Ok&gt; &lt;Cancel&gt;</p>		<b>Standard</b>	<b>This node has access to the Internet</b>	Airgap	This node does not have access to the Internet
<b>Standard</b>	<b>This node has access to the Internet</b>				
Airgap	This node does not have access to the Internet				

## 10. leave hostname default and OK

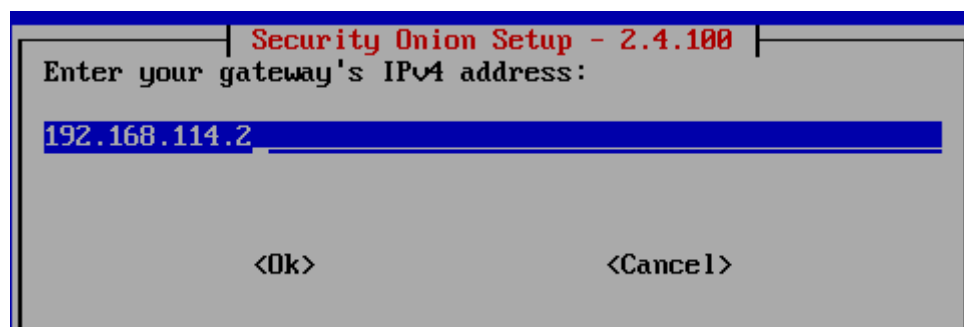
Security Union Setup - 2.4.100	
<p>Enter the hostname (not FQDN) you would like to set:</p> <p><b>securityunion</b></p> <p>&lt;Ok&gt; &lt;Cancel&gt;</p>	
<p>To prevent hostname conflicts, avoid using the default 'securityunion' hostname in a distributed environment.</p> <p>You can choose to use this default hostname anyway, or change it to a new hostname.</p> <p><b>&lt;Use Anyway&gt;</b> &lt;Change&gt;</p>	

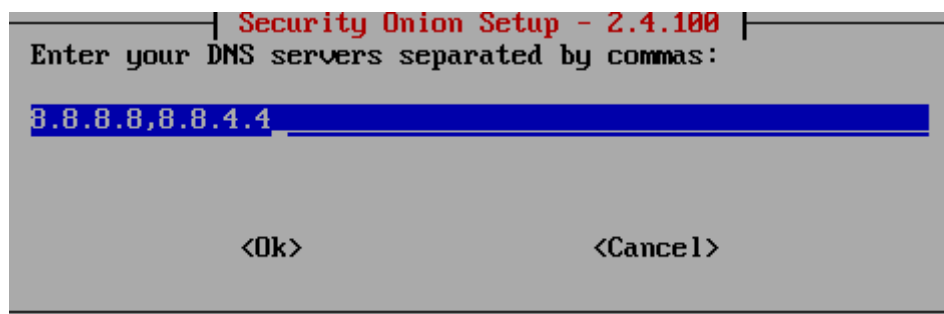


11. Type the static IP address for Management Interface, I type 192.168.114.50/24

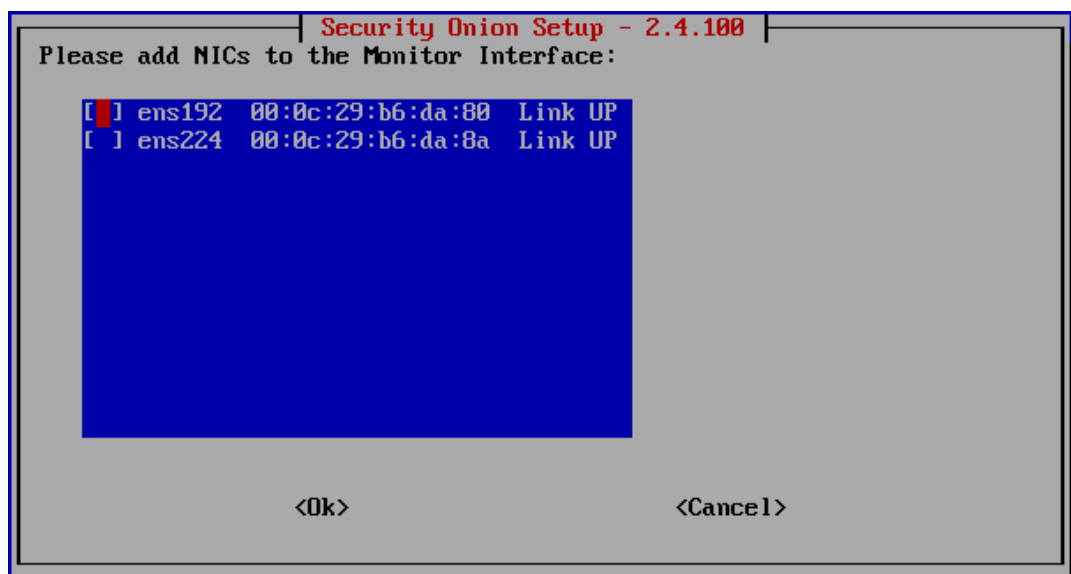
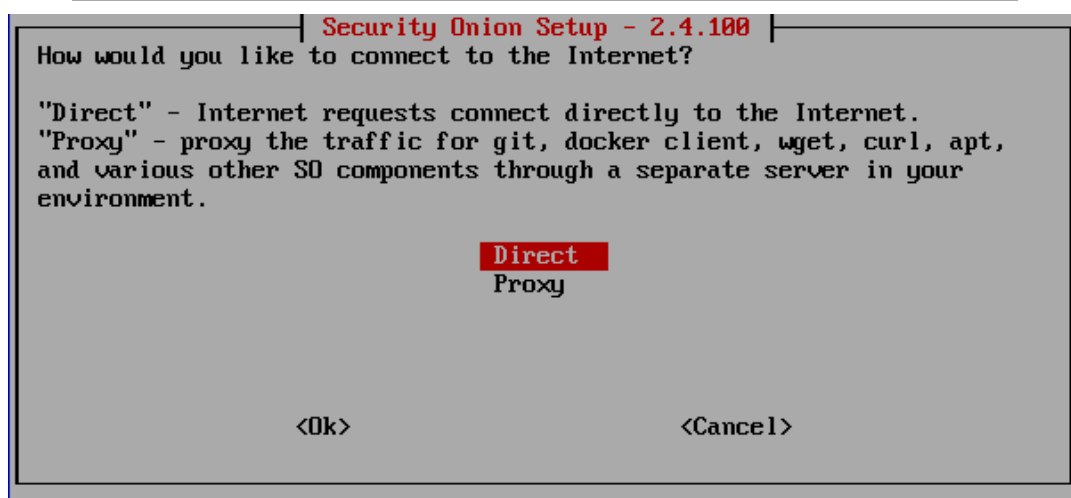
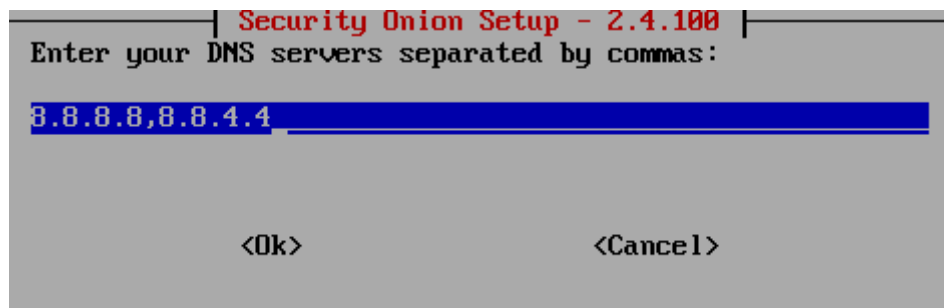


12. Type Gateway 192.168.114.2

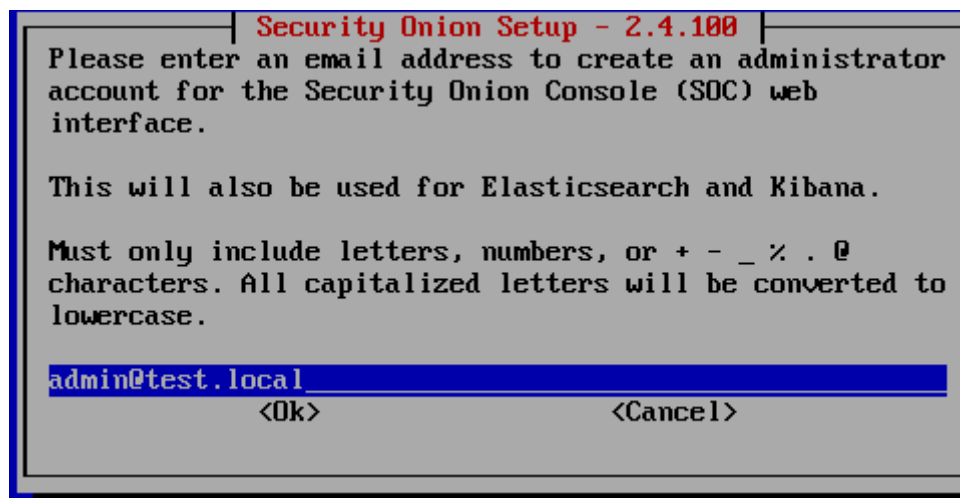




13. Type DNS search domain **test.local**

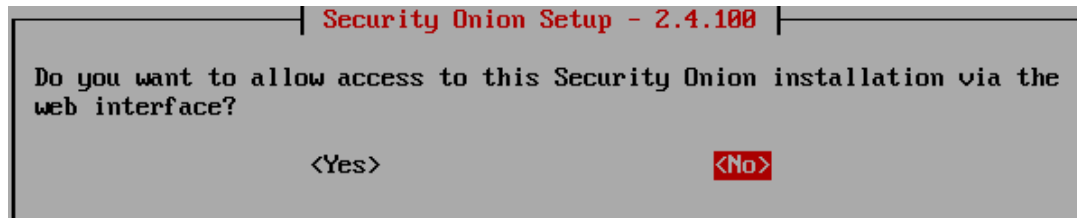
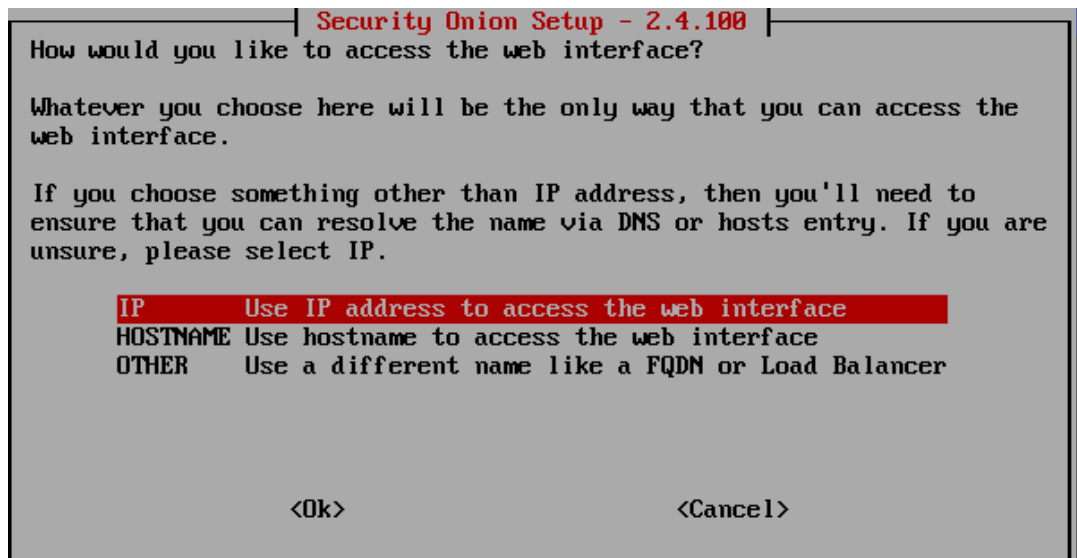


14. type email address, this is for accessing Security Onion Console web interface, I choose **admin@test.local**

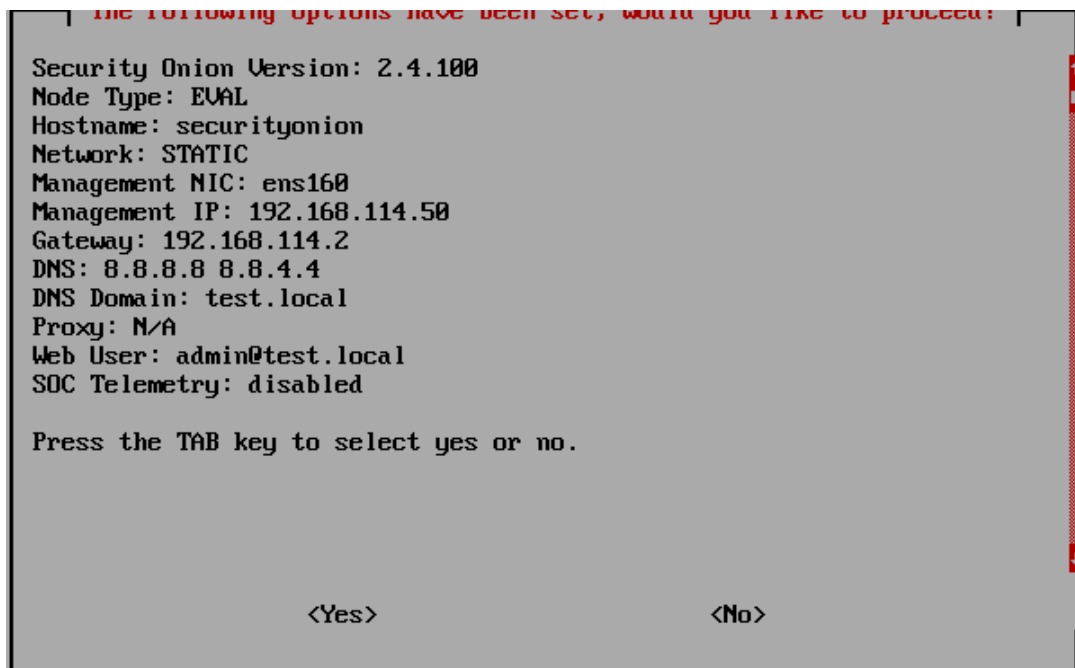


15. type password for web interface

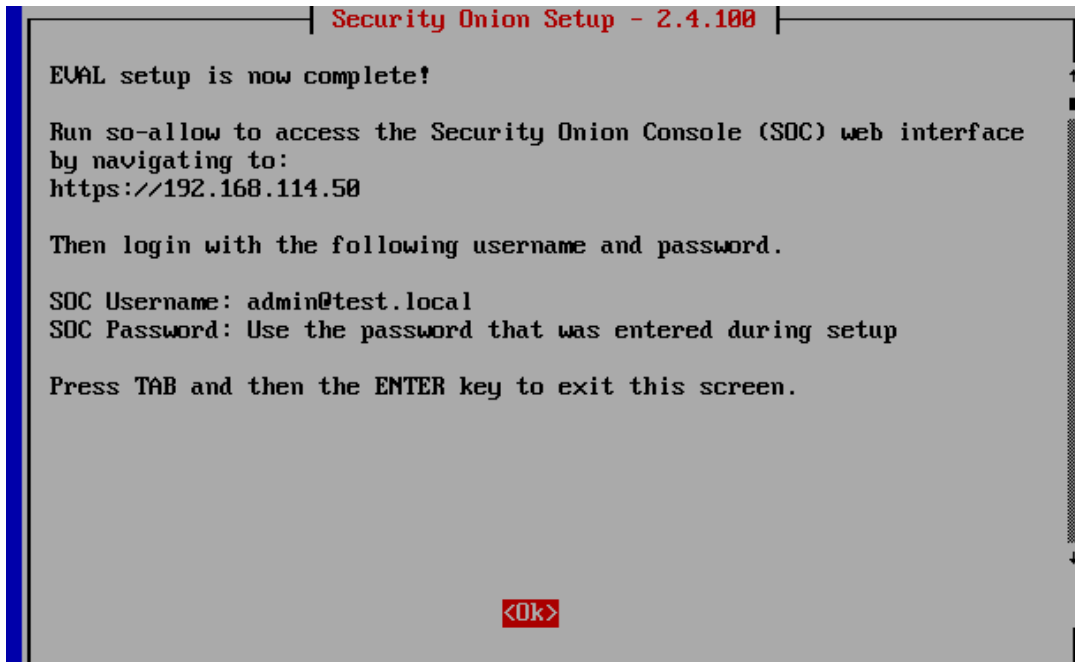
16. Select **IP**



17. Final step before installation



18. Installation is done



## Update & Allow Access to Security Onion Console

1. After reboot, login to the security onion, type **sudo soup**. soup stands for Security Onion Updater, run the command to install updates.
2. To access security onion via web interface, need first add a firewall rules which allow security onion is accessible to certain IP addresses range. To achieve this goal, in the past, sudo so-allow is used. But sudo so-allow is no longer supported on version 2.4.x, instead use **sudo so-firewall includehost analyst** . In this case, **sudo so-firewall includehost analyst 192.168.0.0/16**. This command allows any machines under subnet 192.168.x.x can access manage security onion via link <https://192.168.114.50>

3. after command **sudo so-firewall includehost analyst 192.168.0.0/16**, may still cannot access the Security Onion Console via web interface, so use **sudo so-ip-update** to update IP address for a single-node install. And this time, Security Onion can be accessed via web interface

**This may take a little bit time**, but eventually, it will work.

Login Info: **admin@test.local** and your pre-configured password

