Tenable Appliance 4.8.x User Guide

Last Updated: September 05, 2019
# Table of Contents

**Welcome to Tenable Appliance** ............................................................................. 6

**System Requirements and Installation** .................................................................. 8

Tenable VM Appliance Installation ............................................................................. 9

VM Image Prerequisites ............................................................................................. 10

Security Considerations ............................................................................................ 12

Obtaining the Tenable VMware Virtual Machine Image ............................................. 13

Obtaining the Hyper-V Virtual Machine Image ......................................................... 15

Upgrade Compatibility ............................................................................................... 16

Appliance Migration - 3.x to 4.x ................................................................................. 18

Virtual Image Migration .............................................................................................. 20

Tenable Hardware Appliance ..................................................................................... 22

Hardware Specifications ............................................................................................. 23

Hardware Features .................................................................................................... 24

Hardware Migration .................................................................................................... 25

Configuration and Operations .................................................................................... 28

Set Admin Password .................................................................................................. 30

Configuration/Operations Tab .................................................................................... 32

Appliance Tab ............................................................................................................. 33

**Appliance Interface** .............................................................................................. 34

Console Menu ............................................................................................................. 35

Appliance Tab ............................................................................................................. 36

Administration Tab ................................................................................................... 37
Parent Interface ................................................................. 68
Bulk Import/Configuration .................................................. 69
Applications Tab ................................................................ 71
Enabling Applications ......................................................... 72
The Tenable.sc Application .................................................. 73
Enable Tenable.sc ............................................................... 74
Current Disk Capacity ......................................................... 75
Manage Tenable.sc ............................................................. 76
Plugin Management ............................................................ 77
Webserver Listening Configuration ....................................... 79
Webserver Security ............................................................ 81
Tenable.sc Web Server Authentication .................................... 82
Certificate Authority Management ....................................... 83
SSH User Access ............................................................... 84
The Nessus Application ........................................................ 85
Enable the Nessus Application .............................................. 86
Manage Nessus ................................................................. 87
Additional Nessus Actions .................................................. 88
Edit Nessus Users ............................................................. 89
Certificate Management ..................................................... 90
Webserver Authentication .................................................. 91
Nessus Rules (nessusd.rules) ............................................... 92
The NNM® Application ....................................................... 93
Manage NNM ................................................................. 94
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Management</td>
<td>95</td>
</tr>
<tr>
<td>Web Server Authentication</td>
<td>96</td>
</tr>
<tr>
<td>Logs Tab</td>
<td>97</td>
</tr>
<tr>
<td>Support Tab</td>
<td>99</td>
</tr>
<tr>
<td><strong>Additional Resources</strong></td>
<td>102</td>
</tr>
<tr>
<td>Expand Virtual Disk - VMware</td>
<td>103</td>
</tr>
<tr>
<td>Expand Virtual Disk - Hyper-V</td>
<td>104</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>105</td>
</tr>
<tr>
<td>Notice and Permissions</td>
<td>108</td>
</tr>
</tbody>
</table>
Welcome to Tenable Appliance

This document describes the installation and operation of the Tenable Appliance. The Tenable Appliance is a browser-managed application that hosts various Tenable enterprise applications including Nessus, Tenable.sc, and the Nessus Network Monitor (NNM).

The Tenable Appliance is available as a Virtual Machine download. Applications are available for installation on an as-needed basis on the Appliance and may be enabled or disabled conveniently under one platform. Please email any comments and suggestions to support@tenable.com.

Abbreviations

The following abbreviations are used throughout this documentation:

- **NNM** - Nessus Network Monitor
- **SC** - Tenable.sc
- **VM** - Virtual Machine
- **SSL** - Secure Sockets Layer

Tenable Appliance Platform

The Tenable Appliance virtual machine is available for Microsoft’s HyperV®, VMware® Server, VMware® Player™, VMware® ESX®, VMware® Workstation™, and VMware Fusion® (http://vm-ware.com/). You can download the virtual machine from the Tenable Virtual Appliance 4.8 section of the Tenable Downloads page.

Skill Requirements

Tenable recommends that you configure the Tenable Appliance be configured by personnel familiar with the Nessus vulnerability scanner, Tenable Enterprise Solutions (Tenable.sc and Nessus Network Monitor), and the organization’s security policies and procedures. If training is required for Nessus or Tenable Enterprise Solutions, please visit: http://tenable.com/training/.

Tip: Some general knowledge of the Virtual Machine (VM) platform being used and network configuration is required.
**Note:** Tenable no longer sells the Hardware Appliance but will continue to provide service for existing contracts until March 2020.
System Requirements and Installation

The Tenable Appliance can be installed using hardware or a virtual appliance (also known as a virtual machine), which is a virtual reproduction of an operating system that allows you to manage that system from another computer.

Before installing the Tenable Appliance using either hardware or a virtual appliance, make sure all the system requirements and installation prerequisites have been met for your chosen installation method.

Note: Tenable no longer sells the Hardware Appliance; however, support for existing Hardware Appliance contracts is available until March, 2020.

Hardware Appliance

Virtual Appliance
Tenable VM Appliance Installation

This section describes the installation steps for the Tenable VM Appliance.

VM Image Prerequisites

Security Considerations

Obtaining the Tenable VMware Virtual Machine Image

Obtaining the Tenable Hyper-V Virtual Machine Image

VM Upgrade Compatibility

Virtual Image Migration

Appliance Migration - 3.x to 4.x
VM Image Prerequisites

Before beginning installation, please be sure to have a host system with the following resources available:

- A system with the ability to run a VM image and at least 8 GB of assigned memory.

  **Tip:** The needed assigned memory for a VM image will vary depending on the Tenable applications enabled. Please refer to the installation documentation for the individual applications for memory recommendations and adjust the VM memory setting as appropriate.

- At least 200 GB of free disk space to accommodate the base VM image for the standard appliance or 50GB for the light appliance. If you choose to increase the VM disk size, ensure the extra space is available on the VM host system.

  **Tip:** The default disk size can not be decreased. Additionally, the needed assigned disk space for a VM image will vary depending on the Tenable applications enabled. Refer to the installation documentation for individual applications for disk space recommendations and adjust the VM disk space available to Hard Disk 2 of the Appliance VM image as appropriate. More information on expanding the disk space is available here.

- A system with the ability to run a VM image with at least 4 CPUs assigned.

  **Tip:** VM ESX hotplug support has been added, allowing users to allocate additional resources like CPUs and memory to the Appliance VM without having to reboot.

- At least one IP address for the Appliance. By default, the VM Appliance will obtain an IP address from a DHCP server, if one is available. Otherwise, a fixed address, netmask, and optional gateway may be assigned during the installation process. If there is a DHCP server available, but a static IP address is to be assigned, this may be set during the configuration process. Using multiple addresses allows for multi-homing the Appliance on different network segments to cut down on the network load.

  **Tip:** As with any security management device, a static IP address (assigned manually or via DHCP) is recommended for use on the Appliance network interfaces.

Along with the IP address, the following values must be configured for the Tenable VM Appliance to be network accessible:

- The network subnet mask for the Appliance.

- The IP address of the Default Gateway for the Appliance (if applicable).
- The IP addresses of the DNS servers for the Appliance (if applicable).
- A hostname for the Appliance.

**Note:** It is necessary to have a hostname available to assign to the Appliance during installation to ensure the SSL certificate is generated properly. The Appliance ships with the default hostname of tnsAppliance. Whenever the hostname is changed, a new server certificate will be generated and the device will require a reboot.
Security Considerations

When deploying the Tenable Appliance in an internal, external, or untrusted environment, it is strongly recommended that additional security precautions be taken to protect the device from attack and illicit use. Consider implementing the following recommendations:

- Use a signed SSL Certificate from a trusted and reliable Certificate Authority.
- Configure user rules that restrict scanning to IP addresses they are permitted to scan. Adopt a `default deny` policy for user roles and scanning activity.
- When configuring the device via the web interface, avoid using a web proxy or other device that may assist a third party in obtaining sensitive information.
Obtaining the Tenable VMware Virtual Machine Image

The Tenable Appliance virtual machine is available for VMware Server, VMware Player, VMware ESX, VMware Workstation, and VMware Fusion ([http://vmware.com/](http://vmware.com/)) and can be downloaded from the Tenable Virtual Appliance 4.8 section of the Tenable Downloads page. Nessus, Tenable.sc, and Nessus Network Monitor applications are currently available on the Appliance.

There are two versions of Appliance: Light and Standard. See the table below for version options and standards.

<table>
<thead>
<tr>
<th></th>
<th>Light</th>
<th>Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Collection</td>
<td>Nessus and NNM</td>
<td>Nessus and NNM</td>
</tr>
<tr>
<td>Data Analysis</td>
<td>None</td>
<td>Tenable.sc</td>
</tr>
<tr>
<td>Automatic Updates</td>
<td>Required</td>
<td>Configurable</td>
</tr>
<tr>
<td>Offline Updates</td>
<td>Available (4.4.0)</td>
<td>Available</td>
</tr>
<tr>
<td>Download Size</td>
<td>700 MB</td>
<td>1.6 GB</td>
</tr>
<tr>
<td>CPU</td>
<td>2 CPU</td>
<td>2 CPU</td>
</tr>
<tr>
<td>Ram</td>
<td>8 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>Drive</td>
<td>50 GB</td>
<td>200 GB</td>
</tr>
</tbody>
</table>

The Tenable VMware image for VMware Server, VMware Fusion, VMware Workstation, VMware ESX server, and VMware Player is provided as an .ova file with the OS and applications in a 64-bit version.

Note: An internet connection is required when using the Light version for updates and upgrades. The Light Appliance requires a connection over port 443 to [https://appliance.cloud.tenable.com](https://appliance.cloud.tenable.com).

Launch the VMware program and import the .ova file that was downloaded. Adjust the default VM settings as needed for the local environment. The boot process will be displayed in the VM console window when started. Note that it may take several minutes for the Application services to start. Once the boot process is complete, a console screen will be displayed as follows:

Please refer to the Configuration and Operations section for instructions on configuring the Appliance.
**Note:** The following VMware products work with the Virtual Appliance: ESX 5.0 or later, Fusion 4.0 or later, Workstation 8.0 or later, and most current versions of Player.
Obtaining the Hyper-V Virtual Machine Image

The Tenable Appliance VM is available for Microsoft's Hyper-V server (http://www.microsoft.com/hyper-v-server/) and can be downloaded from the Tenable Virtual Appliance 4.8 section of the Tenable Downloads page. Nessus, Tenable.sc, and Nessus Network Monitor applications are currently available on the Appliance.

The Tenable Hyper-V image for Microsoft’s Hyper-V server is provided as a .zip file in a 64-bit version with a file name in the format similar to the following:

TenableAppliance-HyperV-4.4.0-64bit.zip

Note: It may take several minutes to download the files depending on your Internet connection speed.

Note: The interface used for the Appliance should be configured with a static MAC address, not a dynamic one.

Once it has been downloaded, extract the file using an unzip utility. The zip file contains two files: OS.vhd and Data.vhd. These are the virtual hard disks to be used when creating a new hypervisor instance. This instance must be a hardware version 1 instance. During the creation, select the OS.vhd as the initial hard drive. Once created, and prior to the initial launch, edit the settings and add the Data.vhd as an additional hard disk. It may be desirable to expand the size of the Data.vhd at this time. If snapshots are associated with the disk, it may not be expanded.

Note: The OS disk is fixed and the Data disk is dynamic. The Appliance disk usage should be monitored and, possibly, expanded it if the data disk gets low.

Start the virtual machine. The boot process will be displayed in the VM console window. Note that it may take several minutes for the application services to start. Once the boot process is complete, a console screen will be displayed:

Refer to the Configuration and Operations section for instructions on configuring the Appliance.
Upgrade Compatibility

The matrix below displays the Tenable Appliance versions and the corresponding product versions supported.

<table>
<thead>
<tr>
<th>Appliance Version</th>
<th>Tenable.sc Version</th>
<th>Nessus Version</th>
<th>NNM Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.0-0</td>
<td>4.4.0.2</td>
<td>5.0.1</td>
<td>3.6.0.1-1</td>
</tr>
<tr>
<td>2.2.0-1</td>
<td>4.4.0.3</td>
<td>5.0.2</td>
<td>3.6.0.1</td>
</tr>
<tr>
<td>2.4.0-0</td>
<td>4.6.0.1</td>
<td>5.0.2</td>
<td>3.8.0</td>
</tr>
<tr>
<td>2.4.1-0</td>
<td>4.6.2.2</td>
<td>5.2.1</td>
<td>3.8.1</td>
</tr>
<tr>
<td>2.4.1-1</td>
<td>4.6.2.2</td>
<td>5.2.1</td>
<td>3.8.1</td>
</tr>
<tr>
<td>2.4.1-2</td>
<td>4.7.0</td>
<td>5.2.2</td>
<td>3.8.1</td>
</tr>
<tr>
<td>2.6.1</td>
<td>4.7.1</td>
<td>5.2.4</td>
<td>4.0.0</td>
</tr>
<tr>
<td>2.6.2</td>
<td>4.7.1</td>
<td>5.2.5</td>
<td>4.0.1</td>
</tr>
<tr>
<td>2.8.0</td>
<td>4.8.0</td>
<td>5.2.6</td>
<td>4.0.2</td>
</tr>
<tr>
<td>2.8.1</td>
<td>4.8.1</td>
<td>5.2.7</td>
<td>4.0.3</td>
</tr>
<tr>
<td>3.0.0</td>
<td>4.8.1</td>
<td>6.0.1</td>
<td>4.0.3</td>
</tr>
<tr>
<td>3.1.0</td>
<td>4.8.1</td>
<td>6.1.0</td>
<td>4.0.3</td>
</tr>
<tr>
<td>3.2.0</td>
<td>4.8.2</td>
<td>6.1.2</td>
<td>4.0.3</td>
</tr>
<tr>
<td>3.3.1</td>
<td>4.8.2</td>
<td>6.2.1</td>
<td>4.2.0</td>
</tr>
<tr>
<td>3.4.0</td>
<td>4.8.2</td>
<td>6.3.4</td>
<td>4.2.0</td>
</tr>
<tr>
<td>3.5.0</td>
<td>5.0.0.1</td>
<td>6.3.6</td>
<td>4.2.1</td>
</tr>
<tr>
<td>3.5.1</td>
<td>5.0.0.1</td>
<td>6.3.7</td>
<td>4.2.1</td>
</tr>
<tr>
<td>3.6.0</td>
<td>5.0.0.1</td>
<td>6.4.2</td>
<td>4.2.1</td>
</tr>
<tr>
<td>3.7.0</td>
<td>5.0.1</td>
<td>6.4.2</td>
<td>4.2.1</td>
</tr>
<tr>
<td>Appliance Version</td>
<td>Tenable.sc Version</td>
<td>Nessus Version</td>
<td>NNM Version</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>3.8.0</td>
<td>5.0.2</td>
<td>6.4.3</td>
<td>4.4.0</td>
</tr>
<tr>
<td>3.9.0</td>
<td>5.1.0</td>
<td>6.5.2</td>
<td>4.4.0</td>
</tr>
<tr>
<td>3.10.0</td>
<td>5.2.0</td>
<td>6.5.4</td>
<td>4.4.0</td>
</tr>
<tr>
<td>3.10.1</td>
<td>5.2.0</td>
<td>6.5.5</td>
<td>5.0.0</td>
</tr>
<tr>
<td>4.0.0</td>
<td>5.2.0</td>
<td>6.5.4</td>
<td>4.4.0</td>
</tr>
<tr>
<td>4.1.0</td>
<td>5.3.1</td>
<td>6.5.6</td>
<td>5.0.0</td>
</tr>
<tr>
<td>4.2.0</td>
<td>5.3.2</td>
<td>6.7.0</td>
<td>5.1.0</td>
</tr>
<tr>
<td>4.3.0</td>
<td>5.4.0</td>
<td>6.8.1</td>
<td>5.1.0</td>
</tr>
<tr>
<td>4.4.0</td>
<td>5.4.2</td>
<td>6.9.2</td>
<td>5.2.0</td>
</tr>
<tr>
<td>4.5.0</td>
<td>5.4.4</td>
<td>6.10.2</td>
<td>5.2.0</td>
</tr>
<tr>
<td>4.6.0</td>
<td>5.5.0</td>
<td>6.10.7</td>
<td>5.3.0</td>
</tr>
<tr>
<td>4.7.0</td>
<td>5.6.0.1</td>
<td>7.0.1</td>
<td>5.4.0</td>
</tr>
</tbody>
</table>

**Caution:** Tenable.sc will be removed from the Light version when upgrading from 4.2 to 4.3. Customers should use a virtual to move Tenable.sc to a Standard version to keep it enabled.

**Note:** Contact customer support for updating versions older than 2.2.0 or importing an older Appliance (to preserve old data).
Appliance Migration - 3.x to 4.x

This document provides instructions on how to upgrade from Tenable Appliance 3.10.1 to the latest version.

**Note:** Click the link to view the Supported Upgrade Paths.

The migration steps will require:

- Upgrade to Tenable Appliance version 3.10.1.
- Disk migration to 4.2 and upgrade to the most recent version (3.X > upgrade to 3.10.1 > migrate to 4.2 > upgrade to latest).

**Migration Steps**

1. Upgrade to Tenable Appliance 3.10.1 using the TenableAppliance-3.10.1-5-update.tar via the Administration > Updates page.

   **Note:** All upgrade files are located here. (You may have to log in before being directed to the upgrade files page.)

2. Install and configure another virtual image running Tenable Appliance v 4.2.

3. Attach the drives from Appliance 3.10.1 to Appliance 4.2 and complete the import process.

   **Note:** The steps for attaching the drives and completing the import process can be found here.

   - Click here for steps on attaching drives in VMware.
   - Click here for steps on attaching drives in Hyper-V.

4. Upgrade 4.2 to the latest 4.X version.

5. Click the Check for Updates button to install any patches.

When importing data in step 3, you may receive an import error due to version mismatch on Tenable.sc. Please note that Version 3.10.1 can update OTA to include a version of Tenable.sc that is more recent than the version that ships on version 4.2. To remediate this, update Tenable.sc via the Appliance GUI, or manually update the Appliance to version 4.3 or 4.4, then run the import again.

**Note:** See the Updates section in the Appliance user guide for instructions on updating the OTA.
Prior to performing the migration, it is recommended to make a backup of the current virtual image. This provides a recovery option if there is an issue during the migration process.

Depending on the amount of data currently on the virtual image, the migration process may take several hours to complete while the data is being copied between the old and new disks.

This process only migrates data for the Tenable applications that were previously installed. System configuration settings from the previous Appliance are not migrated. The password you set on the new virtual image won’t be replaced with data from the attached disks. You can restore a System Configuration backup (by uploading or using one on the attached disks) if you want to restore those settings.

Note: See the Restore from File section in the Appliance user guide for instructions on restoring a System Configuration backup.

Due to differences in products, platforms, and versions, the steps described here are written for general use. The specific wording of options varies depending on the software being used.

A migration option is available on the wizard if the drives are attached for import before launching the Appliance image.

Please email any comments and suggestions to support@tenable.com.
Virtual Image Migration

The virtual Appliance supports direct import of application data from older Tenable Appliance virtual disks. The process for importation involves adding the previous Appliance's disk files to the new Appliance as a third and fourth drive.

- Prior to performing the migration it is recommended to make a backup of the current virtual image. This provides a recovery option if there is an issue during the migration process.

- Depending on the amount of data currently on the virtual image, the migration process may take several hours to complete while the data is being copied between the old and new disks.

- This process only migrates data for the Tenable applications that were previously installed. System configuration settings from the previous Appliance are not migrated. The password you set on the new VM won't be replaced with data from the attached disks. You can restore a System Configuration backup (by uploading or using one on the attached disks) if you wish to restore those settings.

- Due to differences in products, platforms, and versions, the steps described here are written for general use. The specific wording of options varies depending on the software being used.

- A migration option is available on the wizard if the drives are attached for import before launching the Appliance image.

Steps in Wizard

Use the following steps to perform virtual image migration before the Appliance has been installed.

1. The wizard that displays, provides the ability to import an application prior to setting the password and accepting the license agreement.

2. If the import is not done at this time, it can be done later in the Appliance UI by going to Administration tab (see Steps in Appliance UI below). A yellow circle if displays if disks are recognized.

3. The system will then display the VM Import page.

4. Click on the **Import Application Data** button to complete the process.

Steps in Appliance UI

Use the following steps to perform the virtual image migration after Appliance has been installed.
1. Shut down your newly deployed Tenable Appliance VM.

2. Edit the settings for the newly deployed Tenable Appliance VM within your VM software. Under the Hardware section, begin the process to add another hard disk. Choose to use an existing virtual disk and select the *-disk1/OS.vhd then *-disk2/Data.vhd files in that order from your existing Appliance. If asked, choose to keep the existing format of your .vmdk files.

   **Note:** When selecting the second .vmdk file, note that you must again browse to the directory containing your previous disk files. The VMware software does not open for browsing in the previously used directory.

3. Once the disk addition is complete, start your Tenable Appliance image.

   Some versions may display a message warning against using a duplicate UUID. Select the **Yes** button and continue to start.

   Use your web browser to navigate to your Tenable Appliance web interface.

4. At the top of the Admin page a **Tenable Application Data Import** section will be displayed.

5. When the **Import Application Data** button is clicked, it will perform the import of data in the background.

6. Once the page reloads, the **Import Application Data** button will be replaced with text indicating that the import process is in progress. The System Log contains progress messages and includes a final Application Data Migration Finished message.

7. Once the migration is complete, shut down the Tenable Appliance. Edit your virtual image and go to the **Hardware** section to remove the Appliance .vmdk disks added in step 2.

8. After removing the hard disks, boot the updated version of Tenable Appliance. You may log into your applications and find your previous data is now available.

   **Note:** To prevent disks from attaching in inverse order, disks will import a prior virtual machine.
Tenable Hardware Appliance

This section describes the features and specifications for the Tenable Hardware Appliance.

For instructions on how to reinstall the Hardware Appliance, refer to Reinstall Appliance (Hardware Appliance Only).

- Hardware Specifications
- Hardware Features
- Hardware Migration
# Hardware Specifications

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Series 100</th>
<th>Series 200</th>
<th>Series 300</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor(s)</td>
<td>1 (Quad-Core) Xeon E5-2407 2.4GHz/6.4 GT/s/10MB</td>
<td>1 (Eight-Core) Xeon E5-2450v2.5GHz/8 GT/s/20MB</td>
<td>1 (Ten-Core) E5-2470V2 2.4 Ghz, 8 GT/s, 25MB Cache</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
<td>16 GB</td>
<td>16 GB</td>
</tr>
<tr>
<td>RAM</td>
<td>DDR3-1600</td>
<td>DDR3-1600</td>
<td>DDR3-1600</td>
</tr>
<tr>
<td>Disk(s)</td>
<td>1x1TB 7200 RPM 128MB Cache SATA 6.0Gb/s - No RAID</td>
<td>2x1TB 7200 RPM 128MB Cache SATA 6.0Gb/s - RAID1 (1TB Usable)</td>
<td>2x1TB 7200 RPM 128MB Cache SATA 6.0Gb/s - RAID1 (1TB Usable)</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>4 Ports Quad Port Intel Gb Ethernet</td>
<td>4 Ports Quad Port Intel Gb Ethernet</td>
<td>4 - Intel Gb Ethernet Ports 2 - Intel 10GbE Ethernet Ports</td>
</tr>
<tr>
<td>Power Supply</td>
<td>Dual 450-watt, redundant PFC</td>
<td>Dual 450-watt, redundant PFC</td>
<td>Dual 450-watt, redundant PFC</td>
</tr>
<tr>
<td>Chassis</td>
<td>1U Rack Chassis 21&quot; depth; 28 lbs</td>
<td>1U Rack Chassis 21&quot; depth; 29 lbs</td>
<td>1U Rack Chassis 21&quot; depth; 29 lbs</td>
</tr>
<tr>
<td>Intended</td>
<td>Nessus, Tenable.sc, and NNM (Single Application)</td>
<td>Nessus, Tenable.sc, and NNM</td>
<td>Nessus, Tenable.sc, and NNM</td>
</tr>
</tbody>
</table>
Hardware Features

This section describes the features of the Series 300 Tenable Hardware Appliance.

Front Panel

Rear Panel

Note: The Series 300 Tenable Appliance comes with a dual hard drive RAID 1 configuration. In the event of a hard drive failure, the Appliance will emit a constant beeping sound. This does not necessarily indicate total system failure since the configuration is mirrored, but it is recommended that Tenable Support be contacted immediately to resolve the issue.
Hardware Migration

Following the processes below, you can migrate the Tenable Hardware Appliance.

**Note:** You must run a full system backup and download of the backup before you run the migration script.

Before you begin:

1. Download the **Hardware-Migration-4.1.0.tar.gz** script and the **Tenable Appliance-4.1.0-6-update.tar** files from the **Tenable Appliance 4.1.0 Images** section on the **Tenable Downloads** page.
2. Ensure the Hardware Appliance has been upgraded from 3.8.0 to 3.10.1 via the supported upgrade path.
3. Manually record the hostname and networking configurations. These are not retained after the migration is completed.

**Note:** If you don’t know your Tenable.sc hostname or any specific routing or network settings, you may have issues with your Tenable.sc application. Certificate information is not maintained for the Appliance.

To take and download a full system backup:

1. Navigate to the **Backup** tab.
2. Verify that the **Take Backup of field** is set to **Whole Appliance**.
3. Click **Take Backup**.
   - A dialogue box appears.
4. In the dialogue box, click **Take Backup**.
   - The system backup completes.
5. In the **Available Backups** section, click **Download Backup**.
6. Save the backup to a secure location.
7. Reboot the system.

To upload and run the migration script:
1. Click the **Administration** tab.

2. In the **Update Appliance** section, click **Choose File**.

3. Click the **Hardware-Migration-4.1.0.tar.gz** file that you previously downloaded. The support script uploads.

4. Click **Perform Action**.
   A confirmation message appears when the migration is complete.
   
   **Note:** The migration may take a substantial amount of time.

5. In the **Appliance** tab, click **Restart Appliance**.

6. Click **OK**.
   The appliance restarts.
   
   **Note:** When the Appliance restarts, the boot cycle will reinstall the Appliance image. The running post-installation scripts portion of the install may take a significant amount of time. The Appliance may restart several times during this cycle.
   
   **Note:** Tenable strongly recommends that you perform a backup again after migrating.

**To complete a factory reinstall:**

1. If the appliance previously had a statically assigned IP address:
   - After the appliance restarts, log on to the local console for the appliance.
   - In the main menu, click **Configure IP Address** to reset the IP address, default gateway, and DNS server IP addressed.
   - Enter the new IP address.
   
   **Note:** The IP address must be in CIDR, (i.e. 1.2.3.4/24) or decimal (i.e. 1.2.3.4/255.255.255.0) format.
   
   - Click **Reset**.

2. If the host name is different from the default host name:
   - Open a web browser and navigate to the **Networking** tab.
   - Update the default host name to reflect the correct host name.
• Click **Set Hostname**.
  A dialogue box appears prompting you to restart the appliance.

3. On the **Administration** tab, click **Restart Appliance**.

4. Click **OK**.

5. Take and download a full system backup. (See above process.)

**Note:** The application data will be available after migration and can be restored to the new version of the software.
Configuration and Operations

**Note:** Many of the configuration changes that are made via the Appliance web interface will not take effect until the corresponding service is restarted. For example, changing the XMLRPC port used by NNM from 8835 to another port will modify the configuration file; however, the **Restart NNM** button on the same page must first be clicked before the changes take effect (even though the page does not explicitly say a restart is required). This applies to most application-specific configuration items and is good practice when making configuration changes on the Tenable Appliance.

The Tenable Appliance configuration procedure is similar for both the VM and Hardware Appliance. The console screen enables you to display information about the Appliance, configure a static IPv4 or IPv6 address, ping an IP address or hostname, revert to factory defaults (Hardware Appliance only), and shutdown/restart the Appliance. All other functions are performed through the web browser interface.

When the Tenable VM Appliance is first booted, the system will attempt to obtain an IP address via DHCP. When the Tenable Hardware Appliance is first booted, a static IP address of 192.168.168.21 is configured by default. If you want to change this IP address via the web interface, follow the directions in the **Interfaces** section.

If an IPv4 or IPv6 address is configured from the console using the Configure IP Address option, the appropriate IP Address, Netmask or Prefix, and Gateway addresses must be known to properly configure the settings. A DNS server is required only if further configuration of the networking will not be performed via the web interface. Once entered, you will be asked to confirm your entries. Selecting the default of ‘N’ will abort the changes, while ‘y’ will accept the changes. This applies the settings to the NIC 1 (NIC 5 for Series 300) interface and will set the listening port for the Appliance interface to the default of 8000. Only an IPv4 or IPv6 address may be configured at the console for connecting to the Appliance. More detailed configurations must be made from the web interface.

To confirm that the correct IP address was set, use the arrow keys to highlight **Appliance Information** and press the **Enter** key. This will display information similar to the following:

**Tip:** If the console display becomes unreadable for any reason (e.g., diagnostic or log messages), use **Ctrl+L** (hold down Ctrl while pressing the “L” key) to refresh.

Using a web browser, enter the URL displayed under **Appliance Information**. For example, the URL in the example above for IPv4 is https://192.168.133.136:8000/ and IPv6 is https://[fe80::20c:29ff:fe29:9147]:8000/. Note that when using a link-local IPv6 address the NIC identifier must be used at the end of the IPv6 address.
By default, the Appliance uses a self-signed SSL certificate that may display a warning in your web browser indicating the site’s security certificate was not issued by a trusted Certificate Authority (CA). During the initial installation, such errors may safely be ignored. You will be able to upload a custom certificate during configuration later. See the Administration Tab section for details on how to perform this action.

Once the administrative web interface is loaded, a license screen will be displayed as shown below:

**Note:** Be sure to read all the information in the License Agreement before proceeding with the installation. A text or PDF version of the license can be downloaded and saved, if desired.

Click **Accept License Agreement** to proceed with the installation, or the **Shutdown** button to shut down the Appliance without accepting the license.
Set Admin Password

Once you have accepted the license, the next screen prompts you to create a password for the admin user. This password can be changed at a later time and additional users can be added as required:

After the admin password is set, you will be prompted to log in:
Tip: The authentication dialog box will look different depending on the web browser and theme used.

The Tenable Appliance interface limits the number of failed login attempts. After several unsuccessful attempts, the IP address will be blocked from further login attempts for a period of ten minutes.

The QRCode image of Recovery Secret page is displayed when you first log in. While not mandatory, scanning the image or entering the text of the recovery secret to your HOTP program will provide a method to reset your password if lost or forgotten utilizing a onetime password. Once your HOTP software is set up to provide a password, enter the code and click the Check button to confirm the correct code is generated. For more information about the HOTP functionality, refer to Appliance Management Interface Users.
Configuration/Operations Tab

Each page of the Tenable Appliance displays the following navigation tabs:

- Appliance
- Administration
- Backup
- Networking
- Applications
- Logs
- Support

Appliance configuration options are set through the Networking, Backup, and Administration pages. Application configuration options are available through the Applications page. The Appliance, Logs, and Support options are used to obtain more information about the Appliance and its underlying applications. The Log Out option appears on each page and will close the current session and return the user to the login page.
Appliance Tab

The Appliance tab enables you to view application version and license information, network interface status, and other information about the Appliance at a glance. There are three sections under this tab: Application License Information, Appliance Information, and Version Information.

Application License Information

The information provided in this section displays a summary of the license information for the installed Tenable software. This provides a quick reference list to the current license status. This section is not displayed if there are no applications installed.

Appliance Information

This section contains a variety of information pertinent to your particular Appliance configuration including current date/time as seen by the Appliance, system uptime, hostname, disk utilization, Ethernet interface links, installation date, admin user password creation date, and the date the license was accepted. The Interface text contains links that you can click to navigate to the Networking tab configuration.

Note: The Installed date information is the date the Appliance software was installed (or reinstalled), not the date of the local Appliance deployment.

Version Information

This section contains the Support ID (which may read “No Asset Tag” on the VM Appliance) and the current versions of the base Appliance and all installed applications. This information is important when contacting Tenable Support.
Appliance Interface

The Appliance interface is comprised of a top navigation bar containing several options with expanded drop down lists and a main information/work section.

Click on the top navigation bar options (Appliance, Administration, Backup, Networking, Applications, Logs, and Support) in the image below to go to the corresponding Appliance sections.
Console Menu

The Tenable Appliance console menu displays when the system is initialized. Click on the corresponding menu items to access the listed options.
Appliance Tab

The **Appliance** tab enables you to view application version and license information, network interface status, and other information about the Appliance at a glance. There are three sections under this tab: **Application License Information, Appliance Information**, and **Version Information**.

Application License Information

The information provided in this section displays a summary of the license information for the installed Tenable software. This provides a quick reference list to the current license status. This section is not displayed if there are no applications installed.

Appliance Information

This section contains a variety of information pertinent to your particular Appliance configuration including current date/time as seen by the Appliance, system uptime, hostname, disk utilization, Ethernet interface links, installation date, admin user password creation date, and the date the license was accepted. The Interface text contains links that you can click to navigate to the **Networking** tab configuration.

**Note:** The Installed date information is the date the Appliance software was installed (or reinstalled), not the date of the local Appliance deployment.

Version Information

This section contains the Support ID (which may read “No Asset Tag” on the VM Appliance) and the current versions of the base Appliance and all installed applications. This information is important when contacting Tenable Support.
Administration Tab

The **Administration** tab provides several options to customize the Appliance for your environment and is divided into four sections: **System**, **Updates**, **Web Interface**, and **VM Import**.
Update Appliance

You can download updates from the Tenable Virtual Appliance 4.8 section of the Tenable Downloads page. The update(s) should be stored locally before performing the installation. Update packages can be applied to either the hardware or VM version of the Appliance unless otherwise noted.

To apply the update, click Choose File, then browse to the location that the update file was saved. A green banner will display if the update is successful. A red banner will display if the update is unsuccessful stating the problem that caused the error. After applying the update, the license will be shown again.

The update can be confirmed by viewing the version information in the Appliance tab.
Note: The best practice is to store locally. Storing locally prevents issues with browser upload.

Update Availability Detection

The Appliance has the ability to check for updates. When an update has been detected, a banner will appear at the top of the interface until it is installed.

Update Availability Detection

The Tenable Appliance is able to regularly check for updates.

- Select Do not check automatically for user initiated update checks and upgrades only.
- Select Check for updates automatically to have the appliance check for (but not apply) updates automatically.
- Select Apply updates automatically to have the appliance check for and apply updates automatically.
  (Note: some updates will require an appliance reboot and/or may otherwise impact running scans, etc.)

Click the Configure Automatic Update Detection button to set up automatic checks. The system is set to Apply Updates Automatically by default. Selecting the Check for Updates Automatically option alerts the user to updates in the interface, but does not apply them without user intervention. This feature cannot be disabled.

In addition, an HTTP proxy may be configured. This proxy setting only applies to the Update Availability Detection option.
System

The System option on the Administration tab provides options for restart/shutdown, clock configuration settings, SNMP agent configuration settings, and system log forwarding.
Restart/Shut Down

This section allows the shutdown or restart of the Appliance from the web interface rather than the console. In addition, Restart Appliance Services may be chosen to restart only the Appliance web server, NTP service, and Tenable applications being hosted on the Appliance.
Configure Clock Settings

The Appliance clock settings, including time zone and custom NTP server, are customized from the Configure Clock Settings section.

Time Zone

The drop-down box next to the **Time Zone** box allows you to select from all available time zones. By default, the Appliance will be set to the **America/New_York** time zone.

NTP Local Reference Clock

When set to **On**, the NTP service will utilize the local clock as a time reference when external time sources are unavailable. Due to the nature of VM environments, when the Appliance is run as a VM, it is recommended to turn this option off. When running and enabled on the hardware version of the Appliance, this option can be useful to maintain accurate time.

Ignore NTP Requests

Enabling this option prevents the NTP service from responding to time requests made from other devices on the network. It is recommended to enable this option in most hardware environments, and particularly when run as a VM guest.

Custom NTP Servers

The Tenable Appliance is configured with a built-in NTP client that, by default, synchronizes with public NTP servers from NTP.org. In most environments this will be modified to use an NTP server on the local network to ensure time is accurate with the Appliance’s peers. To modify the NTP servers, enter the IP address or FQDN in the field provided. Standard **ntp.conf** server configuration lines may be used for server entries. Once the appropriate settings for the environment have been selected, click on **Submit Clock Settings** for the changes to take effect and initiate the first synchronization with the updated settings.

Configure SNMP (v2c) Agent Strings

When monitoring the Appliance via SNMP, there are three settings to be configured: **SNMP Community**, **System Contact**, and **System Location**. Once set to the desired configuration, select the
Submit **SNMP Settings** button to apply the new settings. If the SNMP agent is enabled, the service will restart and enable them. Selecting the **Enable SNMP Agent** or **Disable SNMP Agent** will perform the appropriate action for the agent.
Configure SNMP Agent Strings

When monitoring the Appliance via SNMP, three settings must be configured – SNMP Community, System Contact, and System Location. After the information is entered, click Submit SNMP Settings to apply the new settings. If the SNMP agent is enabled, the service will restart and enable them. Selecting Enable SNMP Agent or Disable SNMP Agent will perform the appropriate action for the agent.
System Log Forwarding

This option allows users to add configuration lines to the **syslog** configuration. Only forwarding entries are allowed. An example **syslog** configuration line would be:

```
*.debug @192.168.0.12
```

The setting, above, sends **syslog** messages with a priority of **debug** (or higher) to a system with the IPv4 address of 192.168.0.12 (change this IP address to that of your **syslog** server). After entering the desired value, click **Configure System Log**.

- Certificates can be uploaded.
- Encrypted syslog is supported.

---

**Note:** In the example, the Appliance selects only a subset of all possible generated syslog messages. (In this case, it specifically leaves out all the info level messages the Appliance normally generates.)
Web Interface

The **Web Interface** option under the **Administration** tab provides options for user management, response header configuration, SSL certificate configuration, generation of certificate signing request (CSR), logout redirection URL settings, and restrict console operations.
Appliance Management Interface Users

New and existing Appliance users are managed through the Appliance Management Interface Users. First, select the user to modify by selecting the drop-down box next to Set Password for. If the user is a new user, ensure New User is selected. Next, fill out the relevant details for the username and password fields. Finally, choose the button pertinent to the operation being performed. Available buttons include Add User, Set Password, and Delete User. After successful completion, a green box is displayed at the top of the screen describing the status and details of the operation.

When the Restrict Console Operations option is enabled, an additional drop-down item, Console Only User, is displayed. When set to Yes the new user can only control protected console options. The user cannot log into the web management interface of the Appliance. When set to No the indicated user can control the protected console options and log into the web management interface of the Appliance.
Recovery Code Link

The Recovery Code link displays a page that enables use of the HMAC-Based One Time Password (HOTP) authentication to change the Appliance login password when it has been forgotten and the user is unable to log in.

If you need to access the recovery codes section, go to the interface on port 8000. Navigate to Administration -> Web Interface. Next, go to Appliance Management Interface Users. Click the recovery code link. This will take you to: https://<IP address or host-name>:8000/app/recoverycodes.

The first step requires the user to download an HOTP supported application on a device. Once installed, select the recovery code link in the Tenable Appliance interface to display the information required to set up the Appliance's HOTP information on the device. Only the recovery page for the logged-in user will display. There are two different methods for entering the information.
The first method on the page is the QRCode Image of Recovery Secret. Scan the QRCode image with the HOTP application. The HOTP application will display information about the new credentials.

The second method is to manually enter the information supplied in the Text Entry of Recovery Secret section. Depending on the application used, you will need to enter one or more pieces of the supplied information. Select Counter or Key based if/when asked during the manual account setup.

A new recovery secret can be created for the user if the HOTP device should become compromised. As the compromised user, select your own username from the drop-down and enter your password in both the password and confirm password fields. Then, click Setup Recovery Secret to generate a new recovery code. A green banner will display indicating the change succeeded or a red banner will display indicating failure with a note indicating the incorrect information.

To confirm the HOTP application is configured correctly, generate a code from your software and enter it in the Enter a code from your software field and click Check. Entering the correct value will
display the correct token and a message to validate success. Entering an incorrect value will produce an error message and the page will have to be reloaded. Entering an invalid code will cause the field to turn red; you will have the option to enter the code again.

If the password is lost and must be changed, navigate to https://<IP address or hostname>:8000/password. On this page, enter your username, the new password to associate with your account, and three of the codes in sequential order as provided by your HOTP application.

**Note:** Whenever the password is changed, a new recovery code is generated. The HOTP program must be updated as the previous HOTP code becomes invalid when a new password is set.

All Appliance Management Interface Users have equal and complete access to the Appliance.
Configure Response Headers

This section contains options for enabling and disabling advanced security headers. The **Content Security Policy (CSP)** is a computer security standard used to prevent cross-site scripting (XSS), clickjacking, and other code injection attacks resulting from the execution of malicious content in a trusted web page context.

The **X-Frame-Options** HTTP response header can be used to indicate whether or not a browser should be allowed to render a page as a frame, iframe, or object. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded in other sites.
Configure Website SSL Certificate

The Appliance is shipped with a self-signed SSL certificate. To replace this with a certificate from a trusted Certificate Authority, click **Choose File**, browse for the certificate, and click **Install Server Certificates**. The Server Certificate and Server Key files must be chosen before clicking the **Install Server Certificates** button. In some environments, an Intermediate and/or Custom Root CA Certificate must also be provided at the same time.

**Note:** The private key must NOT be password protected.

After installing the certificate(s), reload the management interface to verify the changes were accepted. The **Remove Server Certificates** option will let you remove the current certificate and create a new self-signed SSL certificate.
Generate Certificate Signing Request

The Appliance provides the ability to generate a Certificate Signing Request (CSR). The options for generating the request are displayed in the screen capture below:

All fields are optional and the information entered is dependent upon the Certificate Authority (CA) being used for certificate generation. After entering the required information and clicking **Generate CSR**, a window displays providing an option to locally save the CSR in a `.tar.gz` format. This archive contains three files (`*.csr`, `*.key` and `CertificateSubject`). The `.csr` file is submitted to your CA and the `.key` file must be kept private and uploaded to the Appliance along with the certificate received from the CA. The `CertificateSubject` file contains information about the data input and is for informational purposes only.

Please refer to the specific instructions provided by your CA for more information about CSR generation. There is no requirement to use this feature to generate a CSR. It is provided as a convenience to our Appliance users only.
Restrict Console Operations

Anyone with console access to the Appliance can perform any action available on the console menu. To prevent universal access, set this option to **Yes**. This update will require users to enter a username and password to perform actions that reassign the IP address, reinstall the Appliance (hardware only option), shutdown, or restart the Appliance. There is also an additional option to make a user a Console Only User.
Reinstall Appliance (Hardware Appliance Only)

Hardware Appliance users have the option to reinstall the software system to various update levels or even factory defaults (also available from the Appliance console). From this section, choose the desired reinstall level. Only available reversion points will be enabled, in bold black lettering, for selection. Grayed lettering indicates that the previous reversion point is unavailable.

**Note:** Choosing *Factory Defaults* will revert everything back to the Appliance default as it was shipped. Backups, applied updates, etc. are all removed. Choosing *Base Version* just installs the OS as it was when it was first shipped (versions of software and update level, etc.), but backups and updates remain available.

Reinstall Appliance

Reinstallation may take anywhere from 5 to 15 minutes. Please be patient.

Reinstall appliance using:

- Current Version (2.4.1-update2)
- Current Version (2.4.1-update2)
- Last Version (2.4.1-update1)
- Base Version (2.4.0-0)
- **Factory Defaults**
Back Up Appliance

Regular backups of the Tenable Appliance data help to ensure redundancy and data recovery in the event of system failure.

- A Whole Appliance backup, backs up appliance configurations and all application data.
- A System Configuration backup, backs up the Tenable Virtual Appliance configuration. No application data is backed up.
- An application backup, backs up all application data and configuration.

To back up application data on the Tenable Appliance:

1. Log in to the Tenable Appliance.
2. In the top navigation bar, click **Backup**.
   
The Backup Appliance page appears.
3. In the Take Backup of drop-down box, select the application you want to back up.
4. Click **Take Backup**.
   
The Proceed with generating backup page appears.
5. Click **Take Backup**.
   
The backup completes and the Backup Appliance page reappears. The completed backup appears in the Available Backups section.
6. In the Available Backups section, select the completed backup you want to download.
7. Click **Download Backup** to download a backup.
   
The backup downloads.

Automated Backups

You can set up Automated Backups by selecting the Enabled option in the Automated Backups section.

1. Click the edit icon (잠금 아이콘) to set the time month, day of the week, hour and minute for the automatic backups.
2. Click **Store Automated Backups** drop down list option to select the location to store the backups.

3. Click **Save Schedule** button to confirm your selections.

   A green bar will display at the top of the screen indicating the system successfully saved your automated backup.

   **Note:** The automatic backup feature deletes the backup from the Appliance local disk after the transfer succeeds.

### Remote Backup Location

The Automated Backups section provides an option to store backups at a remote location. To use this feature, the Remote Backup Location must be configured. The table below provides descriptions for the items that need to be entered. After the information has been entered, click **Save Remote Config**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Backup Location</td>
<td>This is the location where the backup is sent. (supports SCP)</td>
</tr>
<tr>
<td>Destination Path</td>
<td>This is the location on the machine (file path location).</td>
</tr>
<tr>
<td>SSH Known Host File</td>
<td>This is the SSH public (host) key of the server the Appliance connects to. Enter an <strong>SSH Private Key</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The <strong>SSH Key</strong> must be passphrase protected.</td>
</tr>
<tr>
<td>Port</td>
<td>This is the port that is connecting to the Appliance.</td>
</tr>
<tr>
<td>Authentication</td>
<td>This information is required to access the system. Enter the <strong>Username</strong> and either a <strong>Passphrase</strong> or <strong>SSH Private Key</strong>. (The SSH Private Key is preferred.)</td>
</tr>
</tbody>
</table>

**Note:** Backups must be scheduled when no jobs are running and the system is in an idle state.
Standalone Application Import

Starting with the Tenable Appliance 3.1.0, backups of currently installed standalone versions of Tenable.sc 4.8.x and Nessus 5.x (Linux, Mac OS X, and FreeBSD versions) and higher may be imported into the Appliance via a downloadable script.

1. Download the migration script for:
   - SecurityCenter™ 4.8.1+ on Red Hat and CentOS
   - Nessus® 5.0.0+ on Linux, Mac OS X and FreeBSD
2. Transfer the migration script to the machine hosting the standalone installation to be migrated.
3. Ensure that there is sufficient disk space for a backup.
4. Stop the application service.
   - The backed up data may be corrupt if the service is running during this process.
5. From the directory containing the migration script run:
   - bash migrate_<application>.sh
6. Start the service again (if desired).
7. Upload the resulting migration archive in the Restore from File section below.

Select the link next to the application you want to backup from step 1. Following the steps provided, create a backup of the application. Copy the backup file to a system where your browser may select it to upload to the Appliance. Proceed to the Restore from File section for details on uploading the backup file.
Restore from File

If you have previously saved the Appliance configuration to a file, you can restore the configuration by selecting the file from the **Choose File** button and selecting the **Whole Appliance** or individual application to be restored from the drop-down box. If the application is not contained in the backup file selected, no restore operation will be completed. Supported versions of the backups that may be restored are listed on the screen.

To restore a backup to an Appliance that has enabled applications contained in the backup:

1. From the Backup tab, scroll to the Restore from File section, and select **Only Nessus** from the drop-down box.
2. Navigate to the Nessus Only backup file, and click **Upload Backup File**.
3. Click the **Backup Existing or Restore Backup** button.
4. Click the **Discard Existing and Backup** button.

**Note:** When restoring a backup file from a previous version of Tenable software, it will be upgraded to the currently installed version on the Appliance.
Networking Tab

The Tenable Appliance has several networking options that can be configured for your environment. To configure these options, click the Networking tab.
Configure Networking

The following networking options are available:

- **Hostname** – the hostname given to the Tenable VM/Appliance
- **Webserver Listening Port** – Change the port that the Appliance management web server listens on for incoming connections
- **Domain Name Server(s)** – the IP address(es) of the server(s) that handle DNS queries, one per line
- **Default Gateway (optional)** – the IPv4 and/or IPv6 address of the gateway system to send all packets that are not in the local network
- **Search Domain (optional)** – the domain name that is attached to unqualified DNS queries. Multiple domains can be entered for the search. For multiple domain searches, separate each value with a space.
- **Interfaces** – Configure and view settings for each of the available network interfaces

If changes are required, enter the appropriate information in the fields provided and click on the appropriate button to apply the changes.
Configure Hostname

To change the hostname from the default (tnsAppliance), enter the new hostname (less than 64 characters) in the box next to New hostname and click on the Set Hostname button. Immediately after clicking Set Hostname, a note appears indicating that the Appliance needs to be restarted for the change to take full effect. The user is presented with a screen similar to the screen capture below.

![Screen capture showing the note about the appliance hostname change](image)

Note: Changing the hostname will cause the Appliance to issue a new self-generated SSL certificate.

This reboot ensures that operating system specific changes related to the hostname change fully take effect. Perform this reboot either through the web Administration page or via the console Restart Appliance option.
Interfaces

Network interfaces can be configured from the **Networking** page.

By default, the Tenable VM Appliance obtains an IPv4 address and netmask for Interface 0 from a DHCP server. This can be changed to include IPv6 or static address.

The Tenable Hardware Appliance ships with a static IPv4 address. This can be changed to a DHCP address by selecting **Version 4** from the **Use DHCP** drop-down box.

**Note:** If the IP address is changed on the listening web interface, you will need to adjust the IP address in the URL of your browser to connect to the Appliance again.

In the configuration area for each interface, the first line displays the MAC address of the NIC. Below the **MAC Address** box is a section called **Interface In Use By**, which indicates the Appliance services are utilizing the interface. The **Negotiated Speed** displays the maximum speed at which the NIC is connected to the network.
The **Status** drop-down box determines if the interface is disabled, configured only for IPv4, or configured for both IPv4 and IPv6. The **Use DHCP** drop-down box offers options to prevent the interface from using DHCP. Only use DHCP to configure IPv4, IPv6, or both IPv4 and IPv6. The **Accept Nameservers from DHCP** drop-down offers the options - No, IPv4, IPv6, and both IPv4 and IPv6. The locally configured Domain Name Servers are not used when the **No** option is not selected.

The IPv6 protocol offers an auto configuration option. This is not the same as IPv6 DHCP. The **Accept IPv6 Auto configuration** option offers the ability to enable or disable this feature on the interface.

For interfaces other than the one being used to access the management interface, the **Web Interface Accessible** option can be configured as desired by adjusting the **Yes/No** toggle. The toggle option is disabled on the interface that is used to manage the Appliance.

**Current IP Addresses** lists the current IPv4 and IPv6 addresses configured for the interface. **Configured IP Addresses** is a text entry field to configure static IPv4 and/or IPv6 addresses. Addresses may be entered as the IP Address/Prefix, IP Address/CIDR, or IP Address/Netmask.

If static routes are required to facilitate networking needs, enter one or more static routes in the **Static Routes** box. When entered, the static route is applied to the interface on which it is entered.

**Note:** Input as: `<HOST/NETWORK> (via <GATEWAY>) (dev eth#) (metric #)`

For example: `10.200.200.0 via 10.100.201.1`

For example: `2001:db8::/32 via 2001:db8::1`

When using multiple network interfaces, there is not a provided method to configure IP forwarding or bridging between interfaces. The Appliance and its applications will use the best interface for network communications based on the system's routing table configuration.

When finished configuring additional interfaces, click **Configure Interfaces** to save and restart networking services with the new configuration. Click **Configure Interfaces** to restart networking with the current configuration.
VLANs (Configure/Export)

The Configure VLAN Interfaces option is only active when a VLAN has been configured and saved. A list of existing VLANs will display beneath this selection and will include options to edit and delete.

VLANs can be exported using the Export VLAN option. Clicking the VLAN Export Configuration button exports the VLAN data to a text file, where it can be edited with updates/changes, saved and/or re-uploaded.
Add VLAN

Users also have the option of adding a VLAN by selecting from a list of options. (The user does not have to complete this section if they have already configured the VLAN via the Bulk Import/Configuration section).

- **VLAN ID** – This is the VLAN tag ID. The number can range from 1 to 4094.

- **Status** – Specifies the type of IP address that will be used. Users will have the option to select IPv4 or IPv4 and IPv6.

- **Use DHCP** – This option should be set if the users have not specified an IP Address/Netmask pair. If No is selected, you must have an IP Address/Netmask pair on file. You have the option of using Version 4, Version 6, or Version 4 and Version 6.

- **Use Nameservers from DHCP** – This option will activate dependent on the Version selected in Use DHCP. This needs to be selected for DHCP responses. This entry is typically the same as the Use DHCP selection.

- **Accept IPv6 Auto Configuration** – This feature is offered when using the IPv6 configuration option. Selecting Yes enables the automatic configuration of connected devices over the IP network.

- **Current IP Addresses** – Lists the current IPv4 and IPv6 addresses configured for the interface.

- **Configured IP Addresses** – A text entry field to configure static IPv4 and/or IPv6 addresses.

- **Static Routes** – Use this option if static routes are preferred. Enter the data in the following format.

  **Note:** Input as: <HOST/NETWORK> (via <GATEWAY>) (dev eth#) (metric #)

  For example: 10.200.200.0 via 10.100.201.1
  For example: 2001:db8::/32 via 2001:db8::1

After the information has been entered, click **Add VLAN**. A confirmation, highlighted in green, appears at the top of the screen with a note in the **Bulk Import/Configuration** section detailing the next step. Click the **Configure VLAN Interfaces** option at the bottom of the page to import the data.

**Caution:** If you do not click **Configure VLAN Interfaces**, the added configuration will be lost.
Logout Redirection URL

The Appliance will redirect you to the login page for the Appliance management interface after logging out. You can modify this setting to a selected web page. If the page is not located on the Appliance, a full URL is required (e.g., http://www.tenable.com).
Parent Interface

The Parent Interface section provides information for the network's existing interface. The Interface Name, MAC Address, Negotiated Speed and Status appear in this section.
Bulk Import/Configuration

The **Bulk Import/Configuration** section allows for quick editing of multiple VLAN interfaces and allows for quick duplication of VLAN configuration from one Appliance to another. You can use this feature to change existing VLANs.

The configuration information should be entered in the following format:

```
[eth0.10]
IPADDR=X.X.X.X
NETMASK=Y.Y.Y.Y
[eth0.11]
[eth3.50]
IPADDR=X.X.X.X
NETMASK=Y.Y.Y.Y
```

There is also an option to upload the configuration information – click **Browse**, locate the specified file, and click **Open**.

After the configuration information has been entered or uploaded, click **Bulk Import**.

A confirmation, highlighted in green, will appear at the top of the screen with a note in the Bulk Import/Configuration section detailing the next step. You must click the **Configure VLAN Interfaces** options at the bottom of the page for the data to be imported. If you do not click Configure VLAN Interfaces, the added configuration will be lost.
Importing VLAN Configuration Succeeded

Parent Interface

- Interface Name: eth0
- MAC Address: 00:50:56:A6:4D:A0
- Negotiated Speed: 10000Mb/s
- Status: IPv4 and IPv6

Bulk Import / Configuration

The VLAN interface configuration shown below were created from your imported data.

Navigating away from this page without clicking the Configure VLAN Interfaces button below will cause this imported data to be lost.

Add VLAN

VLANs

<table>
<thead>
<tr>
<th>ID</th>
<th>Status</th>
<th>DHCP</th>
<th>IP Addresses</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>IPv4 Only</td>
<td>Version 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>IPv4 Only</td>
<td>No</td>
<td>127.1.2.3/255.255.255.0</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>IPv4 Only</td>
<td>Version 4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Applications Tab

The Tenable applications that are available for installation on the Appliance are accessed and configured through the Applications tab. The available applications require an appropriate license to be activated once enabled. Each available application page initially contains an enable it button, license agreement for the application, a link to the Tenable website’s product page, and a description of the product.

Note: The Applications tab displays Tenable.sc information for only the Standard version of the Appliance.
Enabling Applications

To use any of the available applications they must first be enabled. This is accomplished by navigating to the desired application’s page under the Applications page and clicking the enable it button on the page. Enabling an application indicates an acceptance of the corresponding license agreement.

For peak performance, Tenable strongly recommends that only one Tenable application be installed on each Appliance virtual machine. There is no additional cost associated with downloading and installing multiple VMs, provided they are properly licensed. While multiple applications can be run on a single Appliance, performance may be impacted for some applications while others are utilizing extra resources for their operations.
The Tenable.sc Application

Tenable Tenable.sc provides continuous, asset-based security and compliance monitoring. It unifies the process of asset discovery, vulnerability detection, data leakage detection, event management, and configuration auditing for small and large enterprises.

Configuration options for the Tenable.sc application after Enabling Tenable.sc.

The configuration sections and associated options for this page are detailed in the corresponding sections.
Enable Tenable.sc

Tenable.sc must be enabled before you can use it. On the Tenable Appliance Setup page, select SecurityCenter. Once selected, the System Information and Application Recommendations appear at the top of the screen. Selecting the SecurityCenter application enables the Accept License Agreement button below. Read and scroll through the Licensing Information and click Accept License Agreement. You will also have to log in to proceed.
Current Disk Capacity

When the Tenable Appliance VM is initially deployed, it provides a total of approximately 200 GB of usable disk space by default. This is in part to provide a smaller initial download size. However, when using Tenable.sc in most environments you will want to increase the virtual disk size as the data collected will quickly fill the available space. Please refer to the Tenable.sc documentation or contact Tenable Support for guidelines to adequate disk space allocation.

Once the available disk capacity is over 60 GB the disk capacity notification area will not be displayed.
Manage Tenable.sc

A link is provided to directly access the installed Tenable.sc instance. Information about the Tenable.sc license is displayed and when it is green there are no issues to note. The running states of the Tenable.sc process and its accompanying daemons are displayed along with the current version of Tenable.sc as reported by the system and by the Tenable.sc database. Below the version information are three buttons used to stop, start, and restart the Tenable.sc processes.
Plugin Management

The Plugin Management section enables users to manually update their Nessus plugin set. This is particularly useful in offline situations where Tenable.sc will not have direct access to the Tenable plugin servers. It is important to disable the Tenable.sc nightly plugin update process when using the manual method.

A hyperlink is provided on the screen labeled manual plugin update page. If you need to perform a manual plugin update, click this link and follow the step-by-step directions. Once completed, click Submit the Information to save the information received for later.

After the plugins have been manually updated, the page changes to include a link where plugin updates can be manually retrieved, or where the plugin feed can be reset in the event a reset is
required (e.g., new activation code). The screen capture below contains a sampling of the updated page.

**Apply Offline Plugin Update for SecurityCenter™**


3. Upload tarballs through the SecurityCenter™ Web UI interface.

Upload these plugins as type **Active** through the Tenable.sc **Upload Plugin** page.
Webserver Listening Configuration

The Tenable.sc web server may be configured to listen on ports other than the HTTPS default of 443 if desired.

When entering a port, it is assumed to be an HTTPS enabled port. Multiple ports may be selected by separating them with commas.
When **Listen on All IP Addresses** is set to **No**, each IP address may be individually configured to listen or not for Tenable.sc requests. Each interface may be configured to listen on designated port(s).
Webserver Security

The status of the Tenable.sc SSL certificates is displayed in this section. Using this interface, custom web server SSL certificates may be installed for Tenable.sc. Click Remove Server Certificates to generate a generic, self-signed and untrusted SSL certificate for use by Tenable.sc, overwriting the current certificate in use.
Tenable.sc Web Server Authentication

The Web Server Authentication section controls the configuration of the SSL Client Certificate authentication permissions. The three options are **Required**, **Allowed**, or **Forbidden**.

- **Required** configures the Tenable.sc web server to only accept connections from web browsers that present a valid SSL client certificate. Other connection attempts will be rejected by the web server with the exact message displayed dependent on the web browser in use.

- **Allowed** configures the Tenable.sc web server to accept a SSL client certificate if it is available, or proceed if a certificate is not present or used for the session. Due to their security configurations, some browsers may encounter connection issues when this setting is used.

- **Forbidden** configures the Tenable.sc web server to ignore any SSL client certificates but allow the web browser connection. This is the default setting.
Certificate Authority Management

This section enables the administrator to install custom SSL CA certificates to Tenable.sc for custom HTTPS SSL certificates, Nessus/NNM server certificate verification, and Tenable.sc client SSL certificates.

Clicking the Browse button opens a dialog box to select a custom CA certificate to upload to the Appliance for Tenable.sc to use. Once selected, clicking the Install CA Certificate will install the custom certificate and will list it in the Certificate Authorities field.

**Note:** All certificate files uploaded must contain only a single CA certificate. Multiple certificates in a single file will result in an error message.

Selecting a CA certificate from those available in the list will allow downloading of the certificate to confirm it is the one expected or to delete a certificate that is no longer valid for use with the Tenable.sc installation.
SSH User Access

This option provides TNS users the ability to enable SSH access to the Appliance.

After the SSH configuration is complete, a confirmation banner will display at the top of the page.
The Nessus Application

Tenable Nessus vulnerability scanner is the world-leader in active scanners, featuring high-speed discovery, asset profiling and vulnerability analysis of the organization’s security posture. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs, and across physically separate networks.

The Nessus application must be activated and configured to make the system manageable via a web browser or SecurityCenter.

Until a valid Activation Code is entered or the Nessus scanner has been configured to be managed by SecurityCenter, the message **Invalid/Expired Activation Code** will be displayed in red on the Appliance page.

Configuration options for Nessus are available under the **Applications** tab by clicking **Nessus®**.
Enable the Nessus Application

To enable the Nessus application, click enable it in the line with the caption: Nessus is not enabled. Would you like to enable it? text.

The back-end processes are now enabled and a dialogue box appears indicating the success of the operation.

**Note:** If the process fails, an error message dialogue box appears to indicate the failure.
Manage Nessus

The Manage Nessus section of this page displays information about the current state of Nessus including the Web UI Link, plugin code status, running state, and Nessus version. In addition, three buttons are available to perform the following Nessus actions:

- Start Nessus
- Restart Nessus
- Stop Nessus

**Note:** Refer to the Nessus User Guide for specifics on initial configuration of the Nessus application, including instructions on how to obtain and apply the appropriate Nessus license.
Additional Nessus Actions

This section offers an option to manually trigger a rebuild of the Nessus plugin database or to remove the existing plugins. The need to perform a rebuild or remove all the plugins is rare, and therefore this section is presented as collapsed by default.

Under certain circumstances it may become necessary to trigger a full Nessus plugin database rebuild. Should one of those occasions arise, Support can help determine this, the button below will trigger the rebuild.

A full plugin database rebuild may take a fair amount of time.

[Rebuild Plugin Database] [Remove Plugins]
Edit Nessus Users

Nessus users are created and managed primarily via the Nessus web user interface. However users may be edited using the Tenable Appliance interface to change their password or the Nessus rules for the user.
Certificate Management

From this section, custom Nessus certificates can be installed or removed. These certificates are used for accessing the Nessus Web interface with a proper CA certificate and for Nessus to Tenable.sc communications. The top section contains a browse dialog for the Server Certificate and Server Key File and optionally the Intermediate and Custom Root CA Certificates that are utilized for Nessus web user interface browser (and Tenable.sc) access, while the bottom section (CA Certificate) is used for client (Tenable.sc or web browser) to Nessus server certificate-based communications.

This Certificate Authority (CA) is used to validate the user certificate used by SecurityCenter when it connects to Nessus using a certificate.
Webserver Authentication

The Webserver Authentication section controls the configuration of the SSL Client Certificate authentication permissions. The two options are a password or an SSL Client Certificate. This setting will control the option available for users to log into the Nessus server via SSL client certificate or password authentication.

- The an SSL Client Certificate option configures the Nessus web server to only accept connections from web browsers that present a valid SSL client certificate. Other connection attempts will be rejected by the web server with the exact message displayed dependent on the web browser in use.

- The a password option configures the Nessus web server to ignore any SSL client certificates but allow the web browser connection. This is the default setting and works with most web browsers without issue.
Nessus Rules (nessusd.rules)

This section allows you to define the `nessusd.rules`, that function the same as the user rules, to forbid/allow `nessusd` to connect to some/all ports for the specified IP address or Plugin ID. These rules affect Nessus globally regardless of the defined Nessus user rules.
The NNM® Application

Tenable Nessus Network Monitor is a network discovery and vulnerability analysis software solution, delivering real-time network profiling and monitoring for continuous assessment of an organization’s security posture in a non-intrusive manner. The Nessus Network Monitor (NNM) monitors network traffic at the packet layer to determine topology, services, and vulnerabilities. Where an active scanner takes a snapshot of the network in time, the Nessus Network Monitor behaves like a security motion detector on the network.

The Nessus Network Monitor application must be activated and configured to make the system manageable via a web browser or used by SecurityCenter.

Note: Until a valid Activation Code is entered, the message Invalid/Expired Activation Code will be displayed in red on the Appliance page.
Manage NNM

The Manage NNM section of this page displays information about the current state of the NNM including the license state, running state, and version. There is a link to the Network Nessus Monitor Web UI that may be selected to perform setup, configuration, and view scan results of the NNM application. In addition, three buttons are available to perform the following actions:

- Start NNM
- Restart NNM
- Stop NNM
Certificate Management

In this section, custom certificates for Nessus Network Monitor can be installed or removed. These certificates are used to access the NNM Web interface with a proper CA certificate. The top section contains a browse dialog for the Server Certificate and Server Key File and optionally the Intermediate and Custom Root CA Certificates that are used for NNM web user interface browser access, while the bottom section (CA Certificate) is used for client to NNM server certificate-based communications.
Web Server Authentication

The Web Server Authentication section controls the configuration of the SSL Client Certificate authentication permissions. The two options are a **password** or a **SSL Client Certificate**. This setting will control the option available for users to log into the NNM server via password authentication or SSL client certificate.

- The **SSL Client Certificate** option configures the NNM web server to only accept connections from web browsers that present a valid SSL client certificate. Other connection attempts will be rejected by the web server with the exact message displayed dependent on the web browser in use.

- The **password** option configures the server to ignore any SSL client certificates but allows the web browser connection. This is the default setting and works with most web browsers without issue.
Logs Tab

Clicking on the **Logs** tab will display a selection of available logs based on the installed software as shown in the following screen capture.

![Logs Tab Screen Capture](image)

Available logs are displayed as grouped together under a heading for the Tenable Appliance itself or the application they belong to.

To display a log, highlight the desired log in the View Logs section and select the number of Lines to view from the drop-down menu then click on the **View Log File Snippet** button. Selecting a log file from the available list and clicking the **Download Log File** button will download the complete log file, regardless of the number of lines selected.

**Note:** The Tenable Appliance Logs text at the top of the list is not an option, but a heading and cannot be selected.

Nessus Network Monitor reports are able to be viewed and downloaded from this page as well.
You also have the option to download a monthly log archive by selecting the month you want to download from the drop-down box and clicking **Download Log Archive**.

**Note:** The log display may be cached by your browser. Click on your browser's refresh button to ensure you are viewing the current log.
Support Tab

If you have an issue that you are working with Tenable Support on, you may be asked to generate a support report to aid in troubleshooting the problem. If this is requested, click the Support tab and then Generate Support Report. Optionally, select Sanitize the generated support report to remove IP addresses from the logs in the Tenable applications that support the feature.

Once the report is generated, it will be accessible on the Available Support Reports drop-down list. Select the report to download, click Download Report, and then send the full report (the entire .tar.gz file) to support@tenable.com. When the support archive is no longer needed it may safely be deleted. Select the report to delete from the drop-down and click the Delete Report button. While multiple support archives may be created each day, a daily task runs to delete all but the 10 most recent support reports each day.

Network Tests

Network tests can be done using traceroute or ping options. These tests are available from the Support tab of the web interface and Network Tests entry on the console menu.

From the Support menu in the UI.

or command line on the console.
Generate Packet Capture

The **Generate Packet Capture** option gives the user the ability to create a packet capture of one or all of the available interfaces from a drop-down list. The capture time is for a period ranging from 1-15 minutes, incremented by minutes, and uses the tcpdump utility. Providing a filter string for tcpdump gives the ability to filter the results of the report provided by tcpdump. This utility is useful for troubleshooting network connectivity issues.

The **Available Packet Captures** section provides a drop-down list of the completed packet capture (pcap) files. Selecting a capture file from the list and selecting the download button will download the pcap file uncompressed or compressed as a gzipped file if the **Compress Capture** feature was used. Selecting a capture file and selecting the **View Capture Snippet** option displays the selected number of lines of the capture file without downloading the entire file. Clicking the **Delete Capture** button permanently deletes the selected capture file.
**Note:** Information about tcpdump and its filter options is available at [http://www.tcpdump.org](http://www.tcpdump.org).
Additional Resources

The topics in this section offer guidance in areas related to Tenable Appliance.

Expand Virtual Disk - VMware

Expand Virtual Disk - Hyper-V

Acknowledgments
Expand Virtual Disk - VMware

The Tenable Appliance supports expanding the virtual hard disk to increase the storage capacity of the Appliance. Follow the steps described in this appendix to expand your virtual disk.

**Note:** The instructions provided here are to be used as guidelines. Two VMware products are described here: VMware Player and the vSphere Client. Due to differing VMware platforms, products, and versions, the specifics may be slightly different for your environment. Please reference the appropriate VMware manual for your environment.

**Locate Disk to be Expanded**

Power off your VM and navigate to the properties of your VM host. There you will find two hard disks. The first one, labeled **Hard Disk (SCSI)**, is 20 GB in size. The second drive, labeled **Hard Disk 2 (SCSI)**, is 30/180 GB in size by default and is the disk to choose for expansion.

**Note:** Once you increase the size of the virtual drive, you cannot reduce it later. Additionally, do not expand it to a larger size than your physical hard disk can store.
Expand Virtual Disk - Hyper-V

The Tenable Appliance supports expanding the virtual hard disk to increase the storage capacity of the Appliance.

Note: The instructions provided here are to be used as guidelines. The specifics may be slightly different for your environment. Please refer to the appropriate Hyper-V manual for your environment.

Locate Disk to be Expanded

Power off your VM and navigate to the settings of your VM host. Two hard drives will be configured. The first disk is named **OS.vhd** and should not be altered unless instructed to by Tenable Support. The second drive, named **Data.vhd**, is the disk to choose for expansion.

Note: Once you increase the size of the virtual drive, it cannot be reduced later. Additionally, do not expand it to a size larger than your physical storage can accommodate.

Click on the **Edit** button for the properties of the disk. Select Expand from the Choose Action option, and select **Next** to display the screen to select the new size. Enter the new size value and click Finish to close the window and expand the drive to the new size.

Ignore Repartition Notice

Once the process completes you may be presented with a dialog box indicating that you must repartition and expand the file system on the guest operating system.

Note: Disregard this notice as the Tenable Appliance will apply the required changes on its next boot.

Boot Appliance

Once the process is complete you can boot your Tenable Appliance VM and make use of the additional space on the newly expanded disk.
Troubleshooting

Q. I forgot the IP address of the Appliance. How do I retrieve it?

A. If you forget the IP address of the Appliance, access the Appliance console and move the arrow keys to highlight Appliance Information and press Enter.

Q. Nessus will not start.

A. This could mean a corrupt plugin database. Select Applications/Nessus® and select Rebuild Plugin Database under Additional Nessus Actions. Wait approximately 5-60 minutes for the processing to complete. Refresh the page and see if Nessus starts. If not, ensure you have saved the current configuration and then perform a reinstallation and restore the saved configuration. If you are still experiencing issues, please contact Tenable Support for assistance.

Q. I lost my password to the admin account. How do I reset it?

A. To set up password recovery, follow the steps in Appliance Management Interface Users.

If the password recovery steps have not been performed, another admin account may reset the password for the affected user.
If the first two options are not available to be used, the following steps must be performed, and all data will be lost.

VM Appliance

For the VM Appliance, deploy a new VM using the most recent version available from the downloads page and proceed to complete the initial system configuration. You can then use backups previously downloaded to restore older data or follow the directions for importing your existing application data using disks from the previous Appliance VM. See Virtual Image Migration for more details on importing data from VM disks.

Hardware Appliance

For the Hardware Appliance, use the Appliance console Remove Password option to restore the Appliance to the default configuration. Doing so zeros out the current admin password and allows you to create a new password the next time you log in to the Appliance UI.

Note: Reverting to factory defaults or going back to an original VM image will cause you to lose any data that has not been captured and restored from a previous backup. Refer to Backup Appliance for more information.

Q. I have modified one of the application configuration items but the change doesn’t seem to have taken effect.
A. Many of the configuration changes that are made via the Appliance web interface will not take effect until the corresponding service is restarted. This applies to most application-specific configuration items and is good practice when making configuration changes on the Tenable Appliance.

Q. On the Tenable.sc application page I get a message that I have XX GB of disk space and need to increase the size of the disk. How do I expand my virtual disk to add more space?

A. Depending on your VM platform, there are different methods to expand the disk size. Refer to the proper method for your platform and increase the virtual disk file used for data to the new desired size. Once restarted, your Tenable Appliance VM will automatically recognize and use the additional disk space.

Q. I cannot log into the web interface for the Tenable Appliance. Is it possible to see error messages on the console?

A. While a history of messages is not available, you can see the current messages being written to the system log. If you go to the console of your Appliance and type Alt-F3 (hold down Alt while pressing the F3 key), you will see the current messages which may help narrow down issues with the Appliance. Typing Alt-F1 (hold down Alt while pressing the F1 key) will return you to the main Appliance console screen. Typing Alt-LeftArrow, and Alt-RightArrow also works to switch between the console menu and system logs.
Notice and Permissions

This product uses the scripting language written by Lua.org (http://www.lua.org/). Copyright © 1994-2011 Lua.org, PUC-Rio.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product uses the lighttpd web server written by Jan Kneschke.

Copyright (c) 2004, Jan Kneschke, incremental. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the 'incremental' nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS...
INTERUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product uses Arana, a Lua/FastCGI web application platform written by Daniel Silverstone (dsilvers@digital-scurf.org).

Copyright 2004-2008 Daniel Silverstone dsilvers@digital-scurf.org

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The Tenable Appliance console menu is provided by Pdmenu (http://kitenet.net/~joey/code/pdmenu/), written by Joey Hess joey@kitenet.net.

This program is Copyright 1995-2002 by Joey Hess, and may be distributed under the terms of the GPL.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details (http://www.gnu.org/licenses/).

The Tenable Appliance internal interface uses lbase64 (http://www.tecgraf.puc-rio.br/~lhf/ftp/lua/#lbase64), software that has been placed in the public domain.
The Tenable Appliance internal interface uses LuaFileSystem (http://kepler-project.org/luafilesystem/), designed and implemented by Roberto Ierusalimschy, André Carregal and Tomás Guisasola.

Copyright © 2003 Kepler Project.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The Tenable Appliance internal interface uses LuaLogging (http://keplerproject.org/lualogging/), designed by Danilo Tuler and implemented by Danilo Tuler, Thiago Ponte and André Carregal.

Copyright © 2004-2007 Kepler Project.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.
The Tenable Appliance internal interface uses (Lua) MD5 ([http://www.keplerproject.org/md5/](http://www.keplerproject.org/md5/)), designed and implemented by Roberto Ierusalimschy and Marcela Ozório Suarez. The DES 56 C library, as used in (Lua) MD5, was implemented by Stuart Levy.

Copyright © 2003 PUC-Rio. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.