# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLE OF CONTENTS</td>
<td>2</td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>4</td>
</tr>
<tr>
<td>TENABLE APPLIANCE PLATFORM</td>
<td>4</td>
</tr>
<tr>
<td>SKILL REQUIREMENTS</td>
<td>4</td>
</tr>
<tr>
<td>TENABLE VM APPLIANCE INSTALLATION</td>
<td>5</td>
</tr>
<tr>
<td>VM IMAGE PREREQUISITES</td>
<td>5</td>
</tr>
<tr>
<td>SECURITY CONSIDERATIONS</td>
<td>5</td>
</tr>
<tr>
<td>OBTAINING THE IMAGE</td>
<td>6</td>
</tr>
<tr>
<td>TENABLE HARDWARE APPLIANCE INSTALLATION</td>
<td>7</td>
</tr>
<tr>
<td>PREREQUISITES</td>
<td>7</td>
</tr>
<tr>
<td>UNPACKING THE BOX</td>
<td>8</td>
</tr>
<tr>
<td>RACK MOUNT INSTRUCTIONS</td>
<td>8</td>
</tr>
<tr>
<td>HARDWARE SPECIFICATIONS</td>
<td>8</td>
</tr>
<tr>
<td>HARDWARE FEATURES</td>
<td>9</td>
</tr>
<tr>
<td>NETWORK CONNECTIONS AND INITIALIZATION</td>
<td>10</td>
</tr>
<tr>
<td>CONFIGURATION AND OPERATIONS</td>
<td>11</td>
</tr>
<tr>
<td>SET ADMIN PASSWORD</td>
<td>13</td>
</tr>
<tr>
<td>CONFIGURATION/OPERATION TAB</td>
<td>15</td>
</tr>
<tr>
<td>APPLIANCE TAB</td>
<td>15</td>
</tr>
<tr>
<td>Appliance Information</td>
<td>16</td>
</tr>
<tr>
<td>Version Information</td>
<td>16</td>
</tr>
<tr>
<td>ADMINISTRATION TAB</td>
<td>16</td>
</tr>
<tr>
<td>Update Appliance</td>
<td>17</td>
</tr>
<tr>
<td>Backup Appliance</td>
<td>18</td>
</tr>
<tr>
<td>Restore from Backup</td>
<td>19</td>
</tr>
<tr>
<td>Set Appliance Time Zone</td>
<td>19</td>
</tr>
<tr>
<td>Restart/Shutdown Appliance</td>
<td>19</td>
</tr>
<tr>
<td>Configure Website SSL Certificate</td>
<td>19</td>
</tr>
<tr>
<td>Appliance Management Interface Users</td>
<td>20</td>
</tr>
<tr>
<td>System Log Forwarding</td>
<td>20</td>
</tr>
<tr>
<td>NETWORKING TAB</td>
<td>20</td>
</tr>
<tr>
<td>Configure Networking</td>
<td>21</td>
</tr>
<tr>
<td>Interfaces</td>
<td>22</td>
</tr>
<tr>
<td>LOGS TAB</td>
<td>23</td>
</tr>
<tr>
<td>SUPPORT TAB</td>
<td>24</td>
</tr>
<tr>
<td>APPLICATIONS TAB</td>
<td>25</td>
</tr>
<tr>
<td>THE SECURITY CENTER 3 APPLICATION</td>
<td>25</td>
</tr>
<tr>
<td>Enable Security Center</td>
<td>27</td>
</tr>
<tr>
<td>Upload a Security Center License Key</td>
<td>27</td>
</tr>
<tr>
<td>Manage Security Center</td>
<td>27</td>
</tr>
<tr>
<td>Audit File and Plugin Management</td>
<td>27</td>
</tr>
<tr>
<td>Webserver Security</td>
<td>29</td>
</tr>
<tr>
<td>Webserver Configuration</td>
<td>29</td>
</tr>
<tr>
<td>Customer Management</td>
<td>31</td>
</tr>
</tbody>
</table>

Copyright 2004-2010, Tenable Network Security, Inc.
Support Actions .......................................................... 32
Upgrading to SecurityCenter 4 .......................................... 32
THE SECURITYCENTER 4 APPLICATION .................................. 33
Enable SecurityCenter .................................................. 34
Initial SecurityCenter Credentials .................................... 34
Manage SecurityCenter .................................................. 34
Plugin Management ....................................................... 34
Webserver Security ...................................................... 35
Nessus User Certificate Management ................................ 36
Report Management ..................................................... 36
THE NESSUS APPLICATION .................................................. 37
Enable the Nessus Application ......................................... 39
Configure Nessus Plugin Feed ......................................... 39
Manage Nessus ............................................................ 40
Manage Nessus Plugins .................................................. 40
Proxy Settings ............................................................. 40
Current Users ............................................................... 41
Edit a Nessus User ......................................................... 41
Add a Nessus User ......................................................... 42
Certificate Management ............................................... 42
nessusd.conf .............................................................. 42
nessusd.rules ............................................................. 43
Configure Nessus to work with SecurityCenter ..................... 43
THE LCE APPLICATION ...................................................... 45
THE PVS APPLICATION ...................................................... 45
Upload a PVS License Key ............................................. 47
Manage PVS ................................................................. 47
Configure the PVS Proxy ............................................... 47
Configure PVS ............................................................. 47
Using Nessus, SecurityCenter and PVS ................................ 51
TROUBLESHOOTING ....................................................... 51
ACKNOWLEDGEMENTS .................................................. 54
ABOUT TENABLE NETWORK SECURITY .................................. 57
APPENDIX 1: MIGRATING FROM SECURITY CENTER 3 TO 4 .............. 58
Introduction

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, Security Center (SC) and Passive Vulnerability Scanner (PVS).

A link is provided for the LCE application, which will be available in a future release.

The Tenable Appliance is available as either a VM download or as a physical hardware appliance. The functionality is nearly identical for both, but there are some differences in the installation. Applications are automatically installed on the appliance and may be enabled or disabled on an “as-needed” basis conveniently under one platform. Please share your comments, suggestions and corrections with us by emailing them to support@tenable.com.

Standards and Conventions

Throughout the documentation, filenames, daemons and executables are indicated with a courier bold font such as gunzip, httpd and /etc/passwd.

Important notes and considerations are highlighted with this symbol and grey text boxes.

Tips, examples and best practices are highlighted with this symbol and white on blue text.

Abbreviations

The following abbreviations are used throughout this documentation:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCE</td>
<td>Log Correlation Engine</td>
</tr>
<tr>
<td>PVS</td>
<td>Passive Vulnerability Scanner</td>
</tr>
<tr>
<td>SC</td>
<td>Security Center</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
</tbody>
</table>

Tenable Appliance Platform

The Tenable Appliance for the Virtual Machine (VM) is available for VMware Server, VMware Player, VMware ESX, VMware Workstation and VMware Fusion (http://vmware.com/) and may be downloaded from the Tenable Support Portal located at https://support.tenable.com/support-center/. The Tenable Appliance that is available pre-installed on hardware comes in Series 100 and 200 models and can be obtained by contacting sales@tenable.com.

Skill Requirements

The Tenable Appliance must be configured by a security staff that is familiar with the Nessus vulnerability scanner, Tenable Enterprise Solutions (SC, LCE and PVS) and the site security
policies and procedures. If training is required for Nessus or Tenable Enterprise Solutions, please visit: http://tenable.com/training/.

**Tenable VM Appliance Installation**

This section describes the installation steps required to install the Tenable VM Appliance. If you have purchased the Tenable Hardware Appliance, please refer to the section titled “Tenable Hardware Appliance Installation”.

**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 1 GB of assigned memory.
- At least 32 GB of free disk space to accommodate the VMware image.
- 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, you can assign a fixed address during the installation process. If you have a DHCP server, but wish to use a static IP address, you can set this during the configuration process. VMware Player supports up to three fixed IP addresses (VMware Server supports up to four). Using multiple addresses allows you to multihome the appliance on different network segments to cut down on the network load.

If the hosted application is Security Center, or is to be managed by a Security Center, assign a static IP address or a DHCP address with a long lease.

The following values must be configured for the Tenable VM Appliance to be network accessible:

- The network subnet mask for the appliance.
- The name or IP address of the Default Gateway for the appliance (if applicable).
- The names or IP addresses of the DNS servers for the appliance (if applicable).
- A hostname for the appliance.

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”. If this 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 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 verifiable Certificate Authority.
- Create Global Nessus Rules to restrict client connections to those from trusted networks only. Adopt a “default deny” policy for all other connections.
- 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.
• Due to potential security weaknesses in VMware, it is not recommended that the Tenable Appliance VM be deployed in an external capacity (internet facing).

**Obtaining the Image**

The Tenable Appliance for the Virtual Machine (VM) 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 Support Portal located at [https://support.tenable.com/support-center/](https://support.tenable.com/support-center/). Currently Nessus, Security Center and PVS applications are available on the appliance with LCE to be released soon.

The Tenable VMware image for VMware Server and VMware Player is provided as a .zip archive with a filename in the following format:

TenableAppliance-1.0.4-vmw.zip

The VMware ESX Server image is provided as a .zip archive with a filename in a format similar to the following:

TenableAppliance-1.0.4-esx.zip

![It may take several minutes to download the files depending on your Internet connection speed.](https://support.tenable.com/support-center/)

Updates are available on the Tenable Support Portal located at: [https://support.tenable.com/support-center/](https://support.tenable.com/support-center/) and include “updateX” in the Tenable Appliance file name (e.g., TenableAppliance-1.0.4-update1.tar.gz) where X is the update number. The update number is incremented as new updates become available. Updates are cumulative so that “update8” contains all the changes from “update1” through “update7”.

Use the appropriate application to unpack the VM image, such as WinZip or WinRAR.

![The compressed (.zip) file will expand to consume over 3 GB of disk space. When opened with VMware, the virtual disk size is 32 GB. Please make sure the required space is available.](https://support.tenable.com/support-center/)

Launch the VMware program and open the file that was previously uncompressed. 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 as follows:
Please refer to the “Configuration and Operations” section for instructions on configuring the appliance.

**Tenable Hardware Appliance Installation**

**Prerequisites**

The Tenable Hardware Appliance must be installed by technical staff that is qualified to configure IP addresses on a Windows platform and perform basic networking tests using tools such as **ping** and **traceroute** to verify connectivity.

Before beginning installation, please be sure to have the following hardware and information available:

- At least one fixed IP addresses for the appliance (not required where DHCP will be used)
- The network subnet mask for the appliance
- The IP address of the Default Gateway for the appliance (if applicable)
- The IP address of the DNS servers for the appliance
- A hostname for the appliance
- A VGA monitor and PS2 keyboard

It is recommended that the appliance be assigned a dedicated IP address for ease of management.

**Warning**

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". If this is changed, a new server certificate will be generated automatically, requiring a reboot.

Unpacking the Box

While unpacking the box that the appliance is shipped in, please be sure to identify the following contents:

- Tenable Appliance
- Power Cable
- Network Patch Cable
- Rack Mount Kit
- Paper Documents:
  - Quick Start Guide
  - Rack Mount Instructions (inside the rack mount kit)
- Documentation CD

Either a straight-through or crossover cable can be used for appliance configuration because the appliance uses Auto-MDIX for link type determination.

Rack Mount Instructions

Follow the rack mount instructions provided in the Rack Mount Kit box to mount the appliance in your cabinets after you have completed installation and verified that the appliance is functioning properly.

Hardware Specifications

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Series 100</th>
<th>Series 200</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor(s)</td>
<td>1 (Dual-Core) Xeon E3110 3.0GHz/1333MHz/6MB</td>
<td>2 (Quad-Core) Xeon E5450 3.0GHz/1333MHz/12MB</td>
</tr>
<tr>
<td>Memory</td>
<td>2 GB</td>
<td>8 GB</td>
</tr>
<tr>
<td>RAM</td>
<td>DDR2-667</td>
<td>DDR2-667 FBDIMM</td>
</tr>
<tr>
<td>Disk(s)</td>
<td>1x250GB 7200 RPM 32MB Cache SATA 3.0Gb/s - No RAID</td>
<td>2x500GB 7200 RPM 16MB Cache SATA 3.0Gb/s - RAID1 (500GB Usable)</td>
</tr>
<tr>
<td>Power Consumption</td>
<td>1660 BTU/hour</td>
<td>2901 BTU/hour</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>4 Dual Intel Gb Ethernet (on-board) Intel Pro/1000 Dual Port Copper PCIe</td>
<td>4 Dual Intel Gb Ethernet (on-board) Intel Pro/1000 Dual Port Copper PCIe</td>
</tr>
<tr>
<td>Power Supply</td>
<td>350-watt, non-redundant PFC</td>
<td>600-watt, non-redundant PFC</td>
</tr>
</tbody>
</table>
Hardware Features

This section describes the hardware features of the Series 100 and 200 Tenable Appliances, including a description of all buttons, lights and ports.

The Tenable Appliance is compatible with PS2 keyboards and mice only. The USB ports are disabled.

Series 100 Tenable Hardware Appliance Diagram
Series 200 Tenable Hardware Appliance Diagram

The Series 200 Tenable Appliance comes with a dual hard drive RAID 1 configuration (left two drive bays). 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.

Network Connections and Initialization

The hardware appliance comes with a pre-assigned IP address of 192.168.168.21. Web configuration takes place using this IP address or one assigned via the appliance console. Initialize and access the appliance console as follows:

1. Plug a network-enabled cable into the NIC1 (lower right) port of the appliance.

Appliances with software version 1.0.3 and previous use NIC 2 (lower left) instead of NIC 1.
2. Connect a monitor and PS2 keyboard to the “Video” and “Keyboard” connectors of the appliance.
3. Connect the provided power cable to the AC power receptacle and to a suitable AC power source and turn on the appliance.
4. Once the system has booted and initialization is complete, a text-based console screen is displayed with a number of options including: “Appliance Information”, “Configure IP Address”, “Revert to Factory Defaults”, “Shutdown Appliance” and “Restart Appliance”.

If you plug the appliance into the network and you have a DHCP server, the hardware appliance will not accept a DHCP address until it has been configured to do so via the web configuration interface.

5. Choose “Configure IP Address” to enter the static IP address that will be used for web configuration along with the netmask and gateway IP address (if applicable).

No further steps are required from the console although it can be used to display appliance information, configure the static IP address, revert the appliance to factory defaults, shutdown or restart the appliance.

**Configuration and Operations**
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 configuration port used by PVS from “1243” to another port will modify the configuration file, however, the “Restart PVS” command 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 appliances. The console screen enables you to display information about the appliance, configure a static IP address, revert to factory defaults (hardware appliance only) and shutdown/restart it. 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 initially started, a static IP address of 192.168.168.21 is automatically configured. If you want to change this IP address, follow the directions in the “Interfaces” section. To validate the IP address that was set, use the arrow keys to highlight “Appliance Information” and press the “Enter” key. This will display information similar to the following:

```
Tenable Appliance Status Screen
```

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 is “https://192.168.85.130:8000/”.
The web based management interface cannot be disabled on the network interface that is in use. This prevents an administrator from accidentally removing web management functionality from all interfaces.

By default, the appliance uses a self-signed SSL certificate that may display an error 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 can safely be ignored. If you use a Certificate Authority, you can upload a custom valid certificate during configuration. See the "Administration Tab" section for details on how to perform this.

Starting with version 1.0.4 of the appliance, both single certificate and intermediary/chain certificate files are supported.

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

Click on the “Accept License Agreement” button.

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

**Initial Password Configuration Screen**

After the admin password is set, you will be prompted to log in:

**Appliance Initial Login Screen**

The authentication dialog box will look different depending on the web browser used.

Once you successfully login, the appliance home page is displayed:
Appliance Information Screen

If any applications have been enabled on the appliance, they are displayed directly below the Tenable Appliance version line similar to the screen capture below:

<table>
<thead>
<tr>
<th>Support ID:</th>
<th>No Asset Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable Appliance:</td>
<td>1.0.4-tenantable</td>
</tr>
</tbody>
</table>

Version Information

Configuration/Operation Tabs

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

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

Appliance configuration options are set through the “Networking” 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.

Appliance Tab
The “Appliance” tab, shown above, enables you to view application license information, manage interfaces and the hostname for the appliance. There are three sections under this tab: “Application License Information”, “Appliance Information” and “Version Information”.

### Appliance Information

<table>
<thead>
<tr>
<th>Date/Time:</th>
<th>Mon Dec 6 2010, 10:32 AM</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Uptime:</td>
<td>Up since Monday December 6th 2010 at 7:03 AM (0 days, 3:20)</td>
</tr>
<tr>
<td>Hostname:</td>
<td>Inappliance</td>
</tr>
<tr>
<td>Interface 0:</td>
<td>192.168.05.100</td>
</tr>
<tr>
<td>Interface 1:</td>
<td>down</td>
</tr>
<tr>
<td>Interface 2:</td>
<td>down</td>
</tr>
<tr>
<td>Interface 3:</td>
<td>down</td>
</tr>
<tr>
<td>Installed:</td>
<td>Tue Jul 13 2010, 2:39 PM</td>
</tr>
</tbody>
</table>

### Version Information

<table>
<thead>
<tr>
<th>Support ID:</th>
<th>No Asset Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable Appliance</td>
<td>1.0.4-Tenable</td>
</tr>
<tr>
<td>Nessus@:</td>
<td>4.4.0</td>
</tr>
<tr>
<td>SecurityCenter 4:</td>
<td>4.0.2 build 201009083338</td>
</tr>
</tbody>
</table>

The “Appliance” tab, shown above, enables you to view application license information, manage interfaces and the hostname for the appliance. There are three sections under this tab: “Application License Information”, “Appliance Information” and “Version Information”.

### Appliance Information

This section contains a variety of information pertinent to your particular appliance configuration including current date/time as seen by the appliance, hostname, Ethernet interface links and installation date. The “Interface” text contains clickable links that go to the “Networking” tab configuration.

### Version Information

This section contains the Support ID (if applicable) and the current versions of the base appliance and all installed applications. This information is important when contacting Tenable Support.

### Administration Tab

The “Administration” page provides several options to customize the appliance for your environment. An example screen capture is shown below:
### Update Appliance

Update Appliance from binary: [Browse...]

File uploads may take a little while.

Apply Update

### Backup Appliance

Taking a backup of the Appliance may take some time. Please be patient.

A System Configuration backup contains the configuration data from the Administration and Networking pages.

A Whole Appliance backup contains the above data but also includes data from each installed Application.

See the documentation for further details.

The new backup will be shown in the list below when the process completes (will require a refresh of this page).

Take Backup of: Whole Appliance

Take Backup

### Available Backups

Available Backup Archives: [Download Backup]

[Restore Backup] [Delete Backup]

### Restore from File

Restore Whole Appliance From: [Browse...]

File uploads may take a little while.

Restore Backup

### Set Appliance Time Zone

- **Time Zone:** America/New_York

- **Custom NTP server:** [Submit Clock Settings] [Synchronize Time]

### Restart/Shutdown Appliance

- Restart Appliance
- Shutdown Appliance
- Restart Appliance Services

### Configure Website SSL Certificate

- **Certificate Subject:** 192.168.169.21
- **Certificate Issuer:** 192.168.169.21
- **Not Valid Before:** May 18 18:41:38 2010 GMT
- **Not Valid After:** May 18 18:41:38 2011 GMT

- **SSL Certificate:** [Browse]

[Upload Cert] [Delete Cert]

### Appliance Management Interface Users

- **Set Password for:** New User

- **Username:**

- **Password:**

- **Confirm Password:**

[Add User] [Set Password] [Delete User]

### System Log Forwarding

Enter lines to be added to syslog.conf. Only forwarding entries will be accepted.

Configure System Log

---

**Appliance Administration Page**

**Update Appliance**

---

Copyright 2004-2010, Tenable Network Security, Inc.
Support scripts, available from the Tenable Support Portal under “Support Actions” on the Tenable Appliance download page, must not be applied through the “Update Appliance” tool.

Available updates can be downloaded from the Tenable Support Portal and are located under “Updates” on the Tenable Appliance download page. They include “updateX” in the Tenable Appliance file name (e.g., TenableAppliance-1.0.4-updateX.tar.gz) where X is the update number. The update number is incremented as new updates become available. Updates are cumulative so that “update8” contains all the changes from “update1” through “update7”. Save these locally before installing on the appliance.

To apply an update, browse to the location where the update file archive was saved and click on “Apply Update”. If the update was successful, a green band will be displayed at the top of the screen. If there was an error, a red band will be displayed indicating what occurred to prevent the update.

**Backup Appliance**

Since there is no direct upgrade path between different versions of the Tenable Appliance, use the “Take Backup” utility to take a backup of the appliance and applications before installing the new appliance version. In the same manner, use the “Restore Backup” functionality to restore the original configuration to the new appliance. The full steps to perform this procedure are detailed in Appendix 1.

Regular backups of the Tenable Appliance data help to ensure redundancy and fault tolerance in the event of system failure. In addition, backups can be performed prior to an Appliance upgrade to retain settings so that an entire appliance configuration rebuild is not required.

From the “Administration” page, there are a number of options under “Backup Appliance”. Select “Take Backup” to backup the general appliance data.

The backup process occurs without notification in the background. After several minutes, refresh the browser window to see the newly generated backup.

To back up the entire appliance configuration, including Tenable application specific data, choose “Whole Appliance” from the dropdown. Other options include “System Configuration” and application specific backups. In addition, it is strongly recommended that you select “Download Backup” to save the .tar archive to a secondary storage device for fault tolerance. The dropdown next to “Download Backup” contains a list of all backups that have been taken on the appliance:

<table>
<thead>
<tr>
<th>Available Backups</th>
<th>Download Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available Backup Archives:</td>
<td></td>
</tr>
<tr>
<td>Wednesday May 26th, 2010 at 12:48PM</td>
<td></td>
</tr>
<tr>
<td>WholeAppliance Backups</td>
<td></td>
</tr>
<tr>
<td>Wednesday May 26th, 2010 at 12:48PM</td>
<td></td>
</tr>
<tr>
<td>SystemConfiguration Backups</td>
<td></td>
</tr>
<tr>
<td>Wednesday May 26th, 2010 at 12:48PM</td>
<td></td>
</tr>
<tr>
<td>pvs Backups</td>
<td></td>
</tr>
<tr>
<td>Wednesday May 26th, 2010 at 12:52PM</td>
<td></td>
</tr>
<tr>
<td>pvs Backups</td>
<td></td>
</tr>
<tr>
<td>Wednesday May 26th, 2010 at 12:48PM</td>
<td></td>
</tr>
</tbody>
</table>

Choose “Delete Backup” to remove previously saved backups.
**Restore from Backup**

If you have previously saved the appliance configuration, you can restore it by choosing a previous backup or selecting a backup file via a browse dialog.

The options to restore “To Appliance Defaults” and “To Factory Defaults” are available only on the hardware appliance.

**Set Appliance Time Zone**

The appliance clock settings, including time zone and custom NTP server, are customized from the “Set Appliance Time Zone” section.

**Time Zone**

The pull-down menu 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.

**Custom NTP Server**

The Tenable appliance is configured with a built-in NTP client that, by default, synchronizes with public NTP servers from NTP.org. To use an additional NTP server, enter the IP address, FQDN or local host in the field provided. The appliance tries the default NTP servers along with any manually added NTP server. Once the appropriate settings for the environment have been selected, click on “Submit Clock Settings” for the changes to take effect.

In addition to the “Submit Clock Settings” command button, a “Synchronize Time” command button is provided to allow the user to manually synchronize the appliance time if required. Using this option is not required under normal circumstances.

**Restart/Shutdown Appliance**

This section allows you to shutdown or restart the appliance or appliance services (NTP, the web server and Tenable applications) from the web interface rather than the VM console. In addition to “Shutdown Appliance” and “Restart Appliance”, you can choose “Restart Appliance Services” to restart only the Tenable applications being hosted on the appliance.

After the appliance is restarted, you must reload the management interface in your web browser. Use the “reload” or “refresh” function in your browser after the device has rebooted.

**Configure Website SSL Certificate**
The appliance is shipped with a self-signed SSL certificate. To replace this with a trusted certificate from a Certificate Authority, browse for the certificate and click on the “Upload Cert” button to load the certificate. The certificate must be in .pem format that contains both the certificate and private key. This can be created manually before uploading:

```
# cat server.crt server.key > server.pem
```

The private key must NOT be password protected or the web server will not be able to start.

Starting with version 1.0.4 of the appliance, both single certificate and intermediary/chain certificate files are supported.

The order of concatenation of the .crt and .key files does not matter.

After loading the certificate, test its validity by reloading your browser. If needed, the “Delete Cert” button will let you remove an existing certificate.

**Appliance Management Interface Users**

New and existing appliance users are managed through the “Appliance Management Interface Users” section. First, select the user to modify by selecting the dropdown box next to “Set Password for”. If the user is a new user, make sure “New User” is selected. Next, fill out the relevant details for the username and password fields, if applicable. Finally, choose the command button pertinent to the operation being performed. Available commands 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.

**System Log Forwarding**

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

```
*.err @192.168.0.12
```

The setting above sends syslog messages with a priority of “error” (or higher) to a system with the IP address of 192.168.0.12 (change this IP address to that of your syslog server). After entering the desired value, click on “Configure System Log” to write the entries to the syslog configuration.

**Networking Tab**

The Tenable Appliance has several networking options that can be configured for your environment. To configure these options, click on the “Networking” tab. A page is displayed as follows:
Configure Networking

The following networking options are available:

- **Hostname** – the hostname given to the Tenable VM/appliance
- **Search Domain (optional)** – the domain name that is attached to unqualified DNS queries
- **Default Gateway (optional)** – the IP address of the gateway system to send all packets that are not in the local network
- **Nameserver(s)** – the servers that handle DNS queries

If changes are required, enter the appropriate information in the fields provided and click on the “Configure Networking” button.

**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 “Configure Networking”, a note appears indicating that the appliance networking setup is being restarted. The user is presented with a screen
similar to the screen capture below and prompted to wait a minute and then reenter the “Networking” page by clicking on the provided link.

The appliance networking setup is currently being restarted, this should only take a few moments. Please wait a minute and then click here to return to the Networking page.

Network Restart Warning

Note that changing the hostname will cause the appliance to issue a new SSL certificate. Please wait at least 60 seconds before refreshing the page to give the system time to create the new certificate. If you will be using a trusted certificate from a Certificate Authority, you will need to set the hostname to correspond with the trusted certificate before uploading the certificate to the appliance.

After reentering the “Networking” page, a note appears at the top of the page indicating that an appliance reboot is required. This reboot ensures that operating system specific changes fully take effect. Perform this reboot either through the web “Administration” page or via the VM console “Restart Appliance” option.

Interfaces

Network interfaces can also be configured from the “Networking” page.

<table>
<thead>
<tr>
<th>Interface 0</th>
<th>00:0c:29:2e:66:d4</th>
<th>DHCP</th>
<th>Web Interface</th>
<th>Interface Used By</th>
<th>Interface Used By</th>
<th>Interface Used By</th>
<th>Interface Used By</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.0.173</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Network Interface Configuration

By default, the Tenable VM Appliance obtains an IP address and netmask for Interface 0 from a DHCP server. This can be changed to a static address if required. Click on the drop down menu next to the “Type” box, select “Static” and enter the IP address and netmask in the appropriate fields.

If the IP address is changed, you will need to adjust the IP in the URL of your browser to connect to the appliance again.

The Tenable Hardware Appliance ships with a static IP. This can be changed to a DHCP address by selecting “DHCP” from the “Type” drop-down menu. Below the interface “Type” box are two sections that indicate what the interface is used by: “Interface Used By” and
whether the interface is web accessible: “Web Interface Accessible”. For non-active network interfaces, the “Web Interface Accessible” option can be configured as desired by adjusting the “Yes/No” toggle.

To configure additional interfaces, click on the interface name/mac address and enter the appropriate information in the same manner as Interface 0. When finished configuring additional interfaces, click on the “Restart Interfaces” button.

**Logs Tab**

Clicking on the “Logs” tab will display a selection of available logs as shown in the following screen capture:

<table>
<thead>
<tr>
<th>View Logs</th>
<th>Appliance</th>
<th>Administration</th>
<th>Networking</th>
<th>Applications</th>
<th>Logs</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nessus Log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nessus Web Log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Websrv Access Log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Websrv Error Log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Center Websrv Access Log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Center Websrv Error Log</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Center Admin Log December 2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Center Admin Log November 2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Center Admin Log September 2009</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Log View Screen

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.
Log View Output

You also have the option to download a log archive by selecting the month you wish to download from the drop down menu and clicking on the “Download Log Archive” button.

⚠️ 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 Customer Support on, you may be asked to generate a support report to aid in troubleshooting the problem. If this is requested, click on the “Support” tab and then the “Generate Support Report” button as shown in the following screen capture:
Click on "Download Report" after the report has been generated and then send the full report (the entire .tar.gz file) to support@tenable.com.

Applications Tab

Use the links at the top of this page to access the individual applications and not the links located in the main body of the “Applications” page.

Within this document there are two distinct references used: “Security Center” and “SecurityCenter”. When used with a space between the names, Security Center 3.X is intended. When used without the space, we are referring to SecurityCenter 4 and greater.

The Tenable applications that are pre-installed on the appliance are accessed and configured through the “Applications” tab. The available applications are displayed on the second line, and require a license to be activated.

The Security Center 3 Application

Tenable recommends running the latest version of the Tenable applications on the Appliance (e.g., SecurityCenter 4). Updated applications are available through new appliance version updates.

The Security Center 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 Security Center application are available from the “Applications” tab by clicking on “Security Center 3”. An example configuration screen is shown below:
### Webserver Security

- **Certificate Subject:** SecurityCenter
- **Certificate Issuer:** SecurityCenter
- **Not Valid Before:** Wed May 14 2008, 2:01 PM GMT
- **Not Valid After:** Fri May 14 2010, 2:01 PM GMT
- **Certificate File:**
- **Private Key File:**
- **Install Custom Certificate**
- **Remove Custom Certificate**

### Customer Management

- **Certificate Subject:** delusion.fr.nessus.org
- **Certificate Issuer:** delusion.fr.nessus.org
- **Not Valid Before:** Wed Jul 24 2002, 1:41 PM GMT
- **Not Valid After:** Thu Jul 24 2003, 2:42 PM GMT
- **CA Certificate File:**
- **Server Certificate File:**
- **Server Key File:**
- **Install Nessus User Certificate**
- **Remove Nessus User Certificate**

### Security Center 3

- **Security Center 3 License:** Cannot open key file for reading
- **Security Center is currently:** Running
- **Active Daemons:**
  - http-lightning 
  - log-importd
- **Security Center Version:** 3.4.5 build 7556
- **Active Managed IPs:** 0

### Support Actions

**Name** | **Serial** | **Primary Security Manager** | **IP Ranges** | **Active IPs** |
--- | --- | --- | --- | --- |
No customers currently configured.

---

Support actions are intended for use only at the direction of Tenable Support.
Enable Security Center

Before Security Center can be used, the Security Center processes must be enabled. At the top of the Security Center application configuration page is the text: "Security Center is currently disabled. Would you like to enable it?" The words "Security Center" are a hyperlink to a page containing more information about Security Center. The words, "enable it" are a command button that will enable the Security Center processes. If the Security Center processes have already been started, "disable it" is displayed instead.

Upload a Security Center License Key

This section provides an interface to upload a License Key and activate the Security Center. Click on "Browse" to locate the activation key file that was received via email from Tenable and then click "Upload Key" to apply the License Key to the Security Center.

<table>
<thead>
<tr>
<th>Upload a Security Center License Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Key for tnsappliance:</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>[Browse...]</td>
</tr>
<tr>
<td>Upload Key</td>
</tr>
</tbody>
</table>

Once the key is uploaded, a green banner is displayed across the top of the application configuration page indicating the success of the operation. The license key is hostname-specific. Make sure that the hostname used to generate the key matches the hostname specified within the key upload dialog.

Manage Security Center

The running state of the Security Center process and its accompanying daemons are displayed along with the current version and number of Active Managed IP addresses. Below the version information are three command buttons used to stop, start and restart the Security Center processes.

<table>
<thead>
<tr>
<th>Manage Security Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Center License: Evaluation key has 25 days left, will expire on Saturday the 19th of December 2009</td>
</tr>
<tr>
<td>Security Center is currently: Running</td>
</tr>
<tr>
<td>Active Daemons: httpd lightningd lightning-proxy logd importd maild</td>
</tr>
<tr>
<td>Security Center Version: 3.4.5 build 17166</td>
</tr>
<tr>
<td>Active Managed IPs: 33</td>
</tr>
<tr>
<td>[Start Security Center] [Restart Security Center] [Stop Security Center]</td>
</tr>
</tbody>
</table>

Audit File and Plugin Management
The "Audit File and Plugin Management" section enables users to manually update their Nessus plugin set, manually upload custom plugins and remove .audit files that are no longer needed. If this appliance is not able to connect directly to the Internet, the Nessus plugins can be updated manually. It is recommended that you disable the Security Center nightly plugin update process when using the manual method.

Subsequent manual uploads of a given custom plugin (by plugin name) will overwrite the previous plugin.

A hyperlink is provided towards the top of the screen labeled "manual plugin update page". If you wish to perform a manual plugin update, click on this link and follow the step-by-step directions and then click on "Submit the Update" to manually perform a plugin update.

The Security Center 3 Appliance Audit File and Plugin Management Screen

A hyperlink is provided towards the top of the screen labeled "manual plugin update page". If you wish to perform a manual plugin update, click on this link and follow the step-by-step directions and then click on "Submit the Update" to manually perform a plugin update.

The next option on the "Audit File and Plugin Management" page is "Delete Audit File". Next to the "Delete Audit File" command button is a dropdown list of all installed .audit files on the Security Center. To remove an .audit file, select the file in question and then click "Delete Audit File".

The final option allows users to upload custom Nessus and PVS plugins to their Security Center. Nessus custom plugins must use a plugin ID between 50,000 and 52,999 to ensure that they do not conflict with Tenable Nessus or PVS plugins.

Starting with Security Center 4, the plugin ranges have changed. Please use the recommended ranges below:

- Passive: 1 - 10,000
- Active: 10,001 - 900,000
- Custom: 900,001 - 999,999
- Compliance: 1,000,000+
Webserver Security

Various web server security options are configured in this section. Among the options are custom certificate installation, encrypted web browsing configuration and non-standard SSL port configuration.

The key/cert specified below is also used for Nessus client connections, so after changing it you will need a valid (customer-CA supplied) client certificate for each client (you would also need to be able to upload the correct cacert.pem file to allow Nessus to validate the certificates).

| Certificate Subject: | SecurityCenter |
| Certificate Issuer:  | SecurityCenter |
| Not Valid Before:    | Wed May 14 2008, 2:01 PM GMT |
| Not Valid After:     | Fri May 14 2010, 2:01 PM GMT |
| Private Key File:    | Browse... |

Security Center ships configured to accept connections from web browsers on the standard HTTP port (80) and on the SSL encrypted HTTPS port (currently 443).

Changing this will cause the Security Center webserver to restart.

Security Center is currently set to **allow** connections on port 80.

Webserver SSL/HTTPS Port 443

The Webserver configuration section is collapsed by default to hide the configuration options. Click on “Webserver Configuration” to display configurable options.

The “Webserver Configuration” section contains custom HTTP configuration settings used by the Security Center web server. An example screen capture of the “Webserver Configuration” is shown below:
The option name and detailed description are in the following table:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Admin Contact Address</strong></td>
<td>Email address used on custom error pages provided by Security Center.</td>
</tr>
<tr>
<td><strong>Logging Level</strong></td>
<td>Available logging levels include: debug, info, notice, warning, error, critical, alert and emergency. <strong>Default “Warning”</strong>.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>The number of seconds before sends and receives times out. <strong>Default 300</strong>.</td>
</tr>
<tr>
<td><strong>KeepAlive</strong></td>
<td>Enable or disable persistent connections (more than one request per connection). <strong>Default “on”</strong>.</td>
</tr>
<tr>
<td><strong>MaxKeepAliveRequests</strong></td>
<td>The maximum number of requests to allow during a persistent connection. A setting of zero enables unlimited requests. We recommend setting this number high for maximum performance. <strong>Default 100</strong>.</td>
</tr>
<tr>
<td><strong>KeepAliveTimeout</strong></td>
<td>Number of seconds to wait for a new request from the existing client on the existing connection. <strong>Default 15</strong>.</td>
</tr>
<tr>
<td><strong>UseCanonicalName</strong></td>
<td>Determines how the web server constructs self-referencing URLs and the SERVER_NAME and SERVER_PORT variables. When set &quot;Off&quot;, the server will use the hostname and port</td>
</tr>
</tbody>
</table>
supplied by the client. When set to “On” the server will use the value of the “ServerName” directive.

| **ServerTokens** | Configures what is used for the http response header. Values include: “Full”, “OS”, “Minor”, “Minimal”, “Major” and “Prod”. “Full” conveys the most information, while, “Prod” conveys the least. **Default “Prod”**. |
| **ServerSignature** | Add a line containing server version and virtual host name to server-generated pages. This does not apply to CGI-generated pages. **Default “Off”**. |
| **HostnameLookups** | Log the names of client hosts, or just their IP Addresses. **Default “Off”**. |

### Customer Management

The following screen capture contains an example “Customer Management” configuration. This section is used for configuring custom certificates and viewing customer details.

#### Security Center 3 Customer View Screen
Clicking on the “View Customer” link displays information relevant to the customer. Other tasks available through this interface include basic workflow, log and scan analysis. A sample screen capture is displayed below:
Security Center 3 Customer Management Screen

From within this page, customer workflows can be downloaded, checked and reset.

Clicking on “View Scans” returns a drop-down menu containing available scans.

Other scan options include “Download Scan”, which allows you to download the scan support files from the server (only needed if requested by Tenable Support) and “Delete Scan”, which enables removal of old scans that are no longer needed.

Support Actions

The “Support Actions” buttons are not intended for daily use and must be performed only at the direction of Tenable Support. For more information on the available Support Actions, contact Tenable Support at support@tenable.com.

Upgrading to SecurityCenter 4

To upgrade from Security Center 3 to SecurityCenter 4 simply enable the SecurityCenter 4 process via the appliance web interface and then access the SecurityCenter web interface to walk through the migration process. Detailed instructions for upgrading in conjunction with an appliance upgrade (1.0.3 to 1.0.4) are provided in Appendix 1 of this document.

The SecurityCenter 4 URL is formatted differently than that of Security Center 3. It has changed from: http://<ip>/sc3 to https://<ip>/sc4. Note the change to https only and the “sc4” suffix.

Please reference the SecurityCenter 4 Upgrade Guide for detailed steps for the migration process.
## The SecurityCenter 4 Application

Tenable's SecurityCenter 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 SecurityCenter 4 application are available from the "Applications" tab by clicking on "SecurityCenter 4". An example screen capture is shown below:

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Administration</th>
<th>Networking</th>
<th>Applications</th>
<th>Logs</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Center 3</td>
<td>SecurityCenter 4</td>
<td>Nessus®</td>
<td>LCE</td>
<td>PVS</td>
<td></td>
</tr>
</tbody>
</table>

SecurityCenter 4 is enabled. Would you like to disable it?

SecurityCenter 4 Configuration Page

Copyright 2004-2010, Tenable Network Security, Inc.

---

**Manage SecurityCenter**

SecurityCenter 4: Key has 25 days left, will expire on Friday the 31st of December 2010

SecurityCenter is currently: Running

Active Directories: http://lightning-proxy.jobd.php

SecurityCenter Version: 4.0.2 build 2010090310

Start SecurityCenter | Restart SecurityCenter | Stop SecurityCenter

**Plugin Management**

If this appliance is not able to connect directly to the internet the Nessus plugins can be updated manually.

It is recommended that you **disable** the SecurityCenter nightly plugin update process when using the manual method.

Follow the directions on the **manual plugin update page** to do so.

**Webserver Security**

Certificate Subject: SecurityCenter

Certificate Issuer: SecurityCenter

Not Valid Before: Wed Dec 1 2010, 7:12 PM GMT

Not Valid After: Fri Nov 30 2012, 7:12 PM GMT

Certificate File: Browse...

Private Key File: Browse...

Install Custom Certificate | Remove Custom Certificate

SecurityCenter ships configured to accept connections from web browsers only on the SSL encrypted HTTPS port (currently 443) and not on the normal HTTP port (80). Changing this will restart the SecurityCenter webserver.

SecurityCenter is currently set **not to allow** connections on port 80.

Enable Connections on Port 80 | Disable Connections on Port 80

Set SSL Port

**Nessus User Certificate Management**

CA Certificate File: Browse...

Server Certificate File: Browse...

Server Key File: Browse...

Install Nessus User Certificate | Remove Nessus User Certificate

If the Server Certificate does not already contain the Server Key include it below.

**Report Management**

Report Watermark: Browse...

Install Custom Watermark | Remove Custom Watermark

---

SecurityCenter 4 Configuration Page

Copyright 2004-2010, Tenable Network Security, Inc.
The configuration sections and associated options for this page are detailed below.

**Enable SecurityCenter**

Before SecurityCenter can be used, the SecurityCenter processes must be enabled. At the top of the SecurityCenter application configuration page is the text: "SecurityCenter 4 is currently disabled. Would you like to \textit{enable it}?" The words “SecurityCenter” are a hyperlink to a page containing more information about SecurityCenter. The words, “enable it” are a command button that will enable/disable the SecurityCenter processes. If the SecurityCenter processes have already been started, the enabled and disabled options are reversed.

**Initial SecurityCenter Credentials**

The initial SecurityCenter credentials of “admin” and “password” are displayed here as a reminder before attempting to login to the SecurityCenter web interface. If the SecurityCenter instance is an upgrade from a previous Security Center 3 installation, you must reset the default password to that used in the previous installation.

**Manage SecurityCenter**

The running state of the SecurityCenter process and its accompanying daemons are displayed along with the current version and number of Active Managed IP addresses. Below the version information are three command buttons used to stop, start and restart the SecurityCenter processes.

<table>
<thead>
<tr>
<th>Manage SecurityCenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurityCenter 4:</td>
</tr>
<tr>
<td>SecurityCenter is currently: Running</td>
</tr>
<tr>
<td>Active Daemons:</td>
</tr>
<tr>
<td>httpd lightning-proxy Jobd.php</td>
</tr>
<tr>
<td>SecurityCenter Version:</td>
</tr>
<tr>
<td>4.0.1 build 20100625263</td>
</tr>
<tr>
<td>Start SecurityCenter</td>
</tr>
</tbody>
</table>

**SecurityCenter 4 Management Interface**

**Plugin Management**

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

**SecurityCenter 4 Plugin Management Screen**
A hyperlink is provided on the screen labeled “manual plugin update page”. If you wish to perform a manual plugin update, click on this link and follow the step-by-step directions and then click on “Submit the Information” to manually perform a plugin update.

### Step-by-step directions for manually updating installed Nessus plugins for Security Center 4

1. Go to [https://plugins.nessus.org/offline.php](https://plugins.nessus.org/offline.php)
2. Enter this machine's challenge code: 
3. Enter your activation code.
4. Submit the information.
5. Input the returned URL below.
6. Input your activation code as used in step 3: 
7. Input URL received from step 4: 
8. Submit the Information or Cancel

### SecurityCenter 4 Offline Plugin Update

After the plugins have been manually updated, the page changes to include a link where future 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.

### Webserver Security

Various web server security options are configured in this section. Among the options are custom certificate installation, encrypted web browsing configuration and non-standard SSL port configuration. Unlike Security Center 3, SecurityCenter 4 does not accept connections from web browsers over HTTP port 80 by default. On this page port 80 connections can be enabled if desired.

SecurityCenter 4 by default only listens for web connections on port 443. Port 80 connections are disabled.
**SecurityCenter 4 Webserver Security Configuration Page**

### Nessus User Certificate Management

This section enables the administrator to configure custom SSL certificates with SecurityCenter 4 for authentication with the Nessus server.

#### SecurityCenter 4 Nessus User Certificate Management

Upload the CA Certificate File, Server Certificate File and Server Key File generated on the Nessus server using the certificate creation process.

### Report Management

The new image file does not need to be the same size/shape as the default image file; however, report appearance could suffer if there is a marked difference. Note: Watermarks viewed through the SecurityCenter web interface are much lighter when they are printed. Consider this when creating a .png image file.

The “**Report Management**” section allows the administrator to install or remove a custom watermark to be used for SecurityCenter reporting.
SecurityCenter 4 Report Watermark Configuration

Choose “Browse” to select the desired .png image file for inclusion in all SecurityCenter reports.

The Nessus Application

Tenable’s 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 the Security Center, the message “Invalid” will be displayed in red on the appliance page.

Configuration options for Nessus are available under the “Applications” tab by clicking on “Nessus®”. An example screen capture is shown below:
Enable the Nessus Application

To enable the Nessus application, click on the command button on the line with the caption: “Nessus is disabled. Would you like to enable it?” After clicking on this command button, the back-end processes are enabled and a message pops up to show the success or failure of the operation.

Configure Nessus Plugin Feed

The Nessus Plugin Feed information is typically set during installation, but can be updated as needed within the “Manage Nessus Plugins” section of this screen. If the appliance is to be managed by a SecurityCenter, check the box labeled “Manage Nessus from SecurityCenter” and click on the “Apply” button. Do not enter a feed activation code since the plugin update is managed from the SecurityCenter. See the sections below titled “Add a Nessus User” and “Configure for use with SecurityCenter” for further steps required for appliance scanners that will be managed by the SecurityCenter only.

- Plugin updates are not available through the Nessus application user interface if Nessus is managed by SecurityCenter.

- If the Nessus application will not be managed by the SecurityCenter, use the activation code that was provided to you via email that is also accessible on the Tenable Support Portal under “Activation Codes”.

- Use the “Manually Update Plugins” link to update the plugins if the scanner will be used in an offline situation where internet access is not available.

Enter the code in the box provided and click on the “Apply” button. A message is displayed indicating whether the code is valid or not. Once the code is successfully entered and the feed is activated, the web interface will display a green banner at the top of the page and green text under the “ProfessionalFeed Activation Code” field indicating success:

![Tenable Network Security](image)

**Appliance Valid Activation Code**

- If the registration code is not valid, please contact Tenable Support by emailing support@tenable.com.

Once a valid Activation Code has been entered, a plugin update will automatically occur. The plugin update process occurs transparently and is complete once the “Plugin feed type” and “Last plugin update was on” fields are populated.
Manage Nessus

The “Manage Nessus” section of this page displays information about the current state of Nessus including the running state, version and interface configuration. Under the “Nessus accepts client connections on: (requires a Nessus restart)” dropdown, Nessus may be configured to scan on individual interfaces or all available interfaces. Where individual interfaces are chosen, the IP address of the interface is displayed to help the user determine the appropriate scan interface. In addition, three command buttons are available to perform the following Nessus actions:

- Start Nessus
- Restart Nessus
- Stop Nessus

Manage Nessus Plugins

Plugin updates are not available through the Nessus application user interface if Nessus is managed by the Security Center.

This section provides information on the type of Nessus plugin feed subscribed to and the time of the last plugin update. It also provides options for updating Nessus plugins. To schedule automatic Nessus plugin updates, select a frequency from the dropdown menu and click on the “Schedule Updates” button. There are also options to update plugins immediately and to rebuild the plugin database.

If the appliance does not have access to the Internet, the “Manually Update Plugins” link provides instructions to manually update the plugins as follows:

1. Go to https://plugins.nessus.org/offline.php
2. Enter this machine’s challenge code: [input field]
3. Enter your activation code: [input field]
4. Submit the information.
5. Download the linked plugin update.
6. Download the linked nessus-fetch.rc file.
7. Select the downloaded files and input the returned URL below.
8. Input your activation code as used in step 3: [input field]
9. Input URL received from step 4: [input field]
10. Select downloaded nessus-fetch.rc: [Browse...]
11. Select downloaded plugin archive: [Browse...]
12. Submit the Update or Cancel

Manual Plugin Update Screen

After the initial offline registration of your ProfessionalFeed Code, this page will update with the link necessary to download future plugin updates.

Proxy Settings
Nessus supports product registration and plugin updates through web proxies that may require authentication. If your site uses a proxy server, enter the proxy host (HTTP) and proxy port (HTTP) for the proxy server. If the proxy server requires authentication, enter the credentials used to authenticate with the proxy server.

**Current Users**

Nessus “users” are the users utilized by Nessus or the Security Center for logging into the Nessus server and performing scan operations. Administrative users are indicated with an asterisk (*) and may perform operations not available to “non-Administrative” users such as plugin updates and user management. Nessus users can also have scan results, including data obtained during the scan, saved to the Knowledge Base (KB). If a KB has been created for a Nessus user, it can be downloaded or deleted from this section.

**Edit a Nessus User**

Under “Current Users”, the available users of the appliance are listed. To edit the information associated with a user, click on the “Edit” link next to the name. The subsequent screen allows you to change the user’s password and manage the rules associated with the user.

Each Nessus user may have a set of rules that control what they can and cannot scan. A rule can forbid/allow the Nessus user to connect to some/all ports for the specified IP or Plugin ID. By default, if user rules are not entered during the creation of a new Nessus user, then the user can scan any IP range. The “Default Rule” can be changed to reject all IPs/Plugins that are not specified as acceptable by a user rule.

The “Edit Rules” options are not available if a SecurityCenter is used to manage the Nessus application.

<table>
<thead>
<tr>
<th>Admin Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>User admin is currently an admin user.</td>
</tr>
<tr>
<td>Make Admin User</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Edit Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password:</td>
</tr>
<tr>
<td>Save Password</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Edit Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Save Rules</td>
</tr>
</tbody>
</table>

**User Configuration Screen**

Once updates have been performed, click on the “Save Password” or “Save Rules” button and then click “Done”.

Copyright 2004-2010, Tenable Network Security, Inc.
Add a Nessus User

To add a Nessus user, enter the user name and password as indicated.

The first user added has administrator rights to the Nessus scanner. If a SecurityCenter is to be used to manage the Nessus application, the administrator user ID must be used with the SecurityCenter for plugin updates.

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 SecurityCenter communications. The top section contains a browse dialog for files (Server Certificate and Server Key File) that are utilized for Nessus web user interface browser access, while the bottom section (CA Certificate and Key File) is used for Nessus server to client (SecurityCenter) certificate-based communications.

Certificate Management Interface

Certificate files can be obtained from any valid certificate authority (CA).

nessusd.conf

This section provides several options that can tune the behavior of nessusd. If you do not want to use a specific variable, check the box labeled “Disable” next to the variable name. To set a new value for the variable, make sure the “Disable” box is unchecked and enter the new value in the field provided. When you have finished updating the variable values, click on the “Write Configuration” button to save your changes.

The option name and detailed description are in the following table:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>

All variables except those that begin with the word “global” can be overwritten by any Nessus client on a per scan basis. If the appliance is to be managed by a SecurityCenter, this information may be overwritten by the SecurityCenter’s scan template.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>report_crashes</code></td>
<td>Anonymously report crashes to Tenable.</td>
</tr>
<tr>
<td><code>throttle_scan</code></td>
<td>Throttle scan when CPU is overloaded.</td>
</tr>
<tr>
<td><code>disable_ntp</code></td>
<td>Disable the old NTP legacy protocol.</td>
</tr>
<tr>
<td><code>disable_xmlrpc</code></td>
<td>Disable the new XMLRPC (Web Server) interface.</td>
</tr>
<tr>
<td><code>listen_port</code></td>
<td>Port to listen to (legacy NTP protocol). Used for pre 4.2 NessusClient connections.</td>
</tr>
<tr>
<td><code>xmlrpc_listen_port</code></td>
<td>Port for the Nessus Web Server to listen to (new XMLRPC protocol).</td>
</tr>
<tr>
<td><code>global.max_scans</code></td>
<td>If set to non-zero, this defines the maximum number of scans that may take place in parallel. <strong>Note:</strong> If this option is not used, no limit is enforced.</td>
</tr>
<tr>
<td><code>max_hosts</code></td>
<td>Maximum number of simultaneous hosts tested.</td>
</tr>
<tr>
<td><code>global.max_hosts</code></td>
<td>The same as <code>max_hosts</code> except that it cannot be overwritten by any Nessus client on a per scan basis.</td>
</tr>
<tr>
<td><code>global.max_web_users</code></td>
<td>If set to non-zero, this defines the maximum of (web) users who can connect in parallel. <strong>Note:</strong> If this option is not used, no limit is enforced.</td>
</tr>
<tr>
<td><code>max_simult_tcp_sessions</code></td>
<td>Maximum number of simultaneous TCP sessions per scan.</td>
</tr>
<tr>
<td><code>global.max_simult_tcp_sessions</code></td>
<td>Maximum number of simultaneous TCP sessions between all scans. <strong>Note:</strong> If this option is not used, no limit is enforced.</td>
</tr>
</tbody>
</table>

**nessusd.rules**

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

⚠️ The option `nessusd.rules` is not available for Tenable Appliance Nessus scanners managed by a SecurityCenter since this behavior is managed by SecurityCenter.

**Configure Nessus to work with SecurityCenter**
If the Tenable Appliance running the Nessus application is to be used with SecurityCenter, the appliance must be configured as follows:

1. From the “Networking” tab, make sure the IP address and interface to be used is one that the SecurityCenter can always reach. This means that it will either need to be a DHCP address with a long lease or a static address. This address is what will be entered in to the SecurityCenter.

2. From the “Nessus” page under the “Applications” tab, in the “Configure Nessus Plugin Feed” section, check the box labeled “Manage Nessus from SecurityCenter” and click on the “Apply” button.

3. From the “Nessus” page, make sure a Nessus administrative user has been configured and make note of the user name and password so this can be added to SecurityCenter. The administrative user is marked with an asterisk (*).

The sections below highlight the steps for adding the Nessus scanner to Security Center 3 and SecurityCenter 4:

**Security Center 3**

On the Security Center, under the “Console” tab click on “Nessus Scanner Management”. If no zones exist yet, add a new one by clicking on “Add Zone” and entering both zone and scanner configuration information. If the zone exists already, highlight the zone, select “Add Scanner” and then enter the IP address and login information for the Nessus administrative user. Click on “Submit” and then restart the services to initiate a plugin update. Monitor the Security Center admin log to ensure the plugins are pushed to the appliance. See the Security Center documentation for more information on configuring the Security Center.

From the Nessus application verify that the plugins were updated by viewing the Applications -> Nessus page and noting the “Last plugin update” date under the “Manage Nessus Plugins” section. This date and time will be the last build of plugins, not the exact date and time of the plugin update on the appliance.

**SecurityCenter 4**

On SecurityCenter, under “Resources”, click on “Nessus Scanners” and then “Add Scanner”. A page similar to the screen capture below is displayed:
Complete all required fields and click on "Submit" to confirm the successful add. You are now ready to use SecurityCenter to scan via the Nessus application.

**The LCE Application**

This application is not currently available for installation on the appliance and must be installed on a system accessible from SecurityCenter. Tenable’s Log Correlation Engine is a software module that aggregates, normalizes, correlates and analyzes event log data from the myriad of devices within the infrastructure. Since the Log Correlation Engine is closely integrated with the SecurityCenter, log analysis and vulnerability management can be centralized for a complete view of the security posture.

**The PVS Application**

Tenable’s Passive Vulnerability Scanner (patent 7,761,918 B2) 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 Passive Vulnerability Scanner (PVS) 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 PVS behaves like a security motion detector on the network.

The screen below displays options available to enabled and configure the PVS application with SecurityCenter.
### Configure PVS

<table>
<thead>
<tr>
<th>Name</th>
<th>Enable/Disable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen on Interface 0</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Listen on Interface 1</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Listen on Interface 2</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Listen on Interface 3</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>report-threshold</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>failure-threshold</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>memory</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>report-lifetime</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>save-knowledge-base</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>db-max-age</td>
<td>804060</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>report-frequency</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>detect-encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>detect-interactive-sessions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>high-speed</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>realtime-syslog</td>
<td>#192.168.20.10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>#192.168.20.11</td>
<td></td>
</tr>
<tr>
<td>vulndata-syslog</td>
<td>#192.168.20.20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>#192.168.20.21</td>
<td></td>
</tr>
<tr>
<td>connections-to-services</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>allow-connections</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>detect-portsans</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>portscan-report-frequency</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>portscan-memory-threshold</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>portscan-port-threshold</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>new-host-alert</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>backup-interval</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>excluded-networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Manage PVS

- **PVS License Key**: Key has 31 days left, will expire on Friday the 2nd of July 2010
- **PVS is currently**: Unstable - no listening interfaces configured below
- **PVS proxy is currently**: Unstable
- **Start PVS**
- **Restart PVS**
- **Step PVS**

### Configure PVS Proxy

- **Username**: [Input]
- **Password**: [Input]
- **Confirm Password**: [Input]

Submitting the form with empty password entries will re-use the existing password, when one has previously been set.
Upload a PVS License Key

This section provides an interface to upload a License Key and activate the PVS. Click on “Browse” to locate the activation key file that was received via email from Tenable and then click “Upload Key” to apply the License Key to the PVS.

![Upload a PVS License Key](image)

_PVS Key Upload Interface_

Once the key is uploaded, a green banner is displayed across the top of the application configuration page indicating the success of the operation. The license key is hostname-specific. Make sure that the hostname used to generate the key matches the hostname specified within the key upload dialog.

Manage PVS

The “Manage PVS” section of this page displays information about the current state of the PVS including the running state, version and interface configuration. In the “Configure PVS” section below, PVS can be configured to listen on individual interfaces or all available interfaces. Where individual interfaces are chosen, the IP address of the interface is displayed to help the user determine the appropriate scan interface. In addition, three command buttons are available to perform the following actions:

- Start PVS
- Restart PVS
- Stop PVS

Configure the PVS Proxy

This section allows the administrator to configure the PVS credentials that are used by SecurityCenter to login to the PVS to retrieve vulnerability data. In addition, the PVS Proxy listening interface and port are configurable. These settings affect connections by SecurityCenter and not those utilized by the PVS daemon for listening.

Configure PVS

This section is used to configure basic PVS settings contained within the PVS daemon configuration file (pvs.conf). Sections of this file can be disabled along with editing various daemon settings.

*Modifying any setting within this file will write the change to the configuration file, however, the settings do not take effect until the PVS daemon is restarted within the “Manage PVS” section above.*

The following table lists the available options that can be configured:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listen on Interface</td>
<td>Interface(s) that the PVS daemon will listen on. Available options are &quot;no&quot; and &quot;yes&quot;. In addition, the interface IP address and current state are displayed.</td>
</tr>
<tr>
<td>report-threshold</td>
<td>When adding new port, application or vulnerability information to the PVS’s model of the observed network, this threshold is used to limit false positives and stray ports that open and close quickly. For example, during an FTP file transfer, a client may temporarily open a port. However, with the report-threshold variable, a vulnerability will not be reported until it has occurred a specified number of times. This variable has a default of “3”.</td>
</tr>
<tr>
<td>failure-threshold</td>
<td>This keyword indicates how many times the PVS will attempt to process a plugin that has failed regular expression matching before disabling the plugin for the life of the report. For example, if failure-threshold is set to 10 and a plugin’s regular expression match fails for a particular host 10 or more times, PVS will stop evaluating that plugin for the life of the report.</td>
</tr>
<tr>
<td>memory</td>
<td>When reconstructing network sessions, the PVS will pre-allocate as many megabytes of memory as specified by this variable. By default, the PVS is installed with a memory value of “50” megabytes. Networks with sustained speeds larger than 100 Mb/s or more than 5,000 unique IP addresses can modify this value to “100” MB. For customers running in front of multiple Class B networks, use values of “400” MB if the system has enough spare memory. However, if you have a large network (such as a university network with 10,000 nodes or more) use a setting of 500. In addition to the session table, the PVS also will use another 200 to 300 MB to store the host vulnerability information and port-scan information.</td>
</tr>
<tr>
<td>report-lifetime</td>
<td>With this variable, the PVS’s entire model of a discovered network is completely removed. The PVS starts over again learning about the hosts that are involved on the network. This setting can be set extremely high, such as 365 days, if this behavior is not desired. However, it is very useful to have fresh reports on a weekly or monthly basis. The default value is 30 days.</td>
</tr>
<tr>
<td>save-knowledge-base</td>
<td>When this option is enabled, the PVS knowledge base will be saved on disk for recovery after the program is restarted.</td>
</tr>
<tr>
<td>kb-max-age</td>
<td>The maximum length of time in seconds that a knowledge-base entry remains valid after its addition.</td>
</tr>
<tr>
<td><strong>report-frequency</strong></td>
<td>This variable specifies in minutes how often the PVS will write a report. The PVS can be configured to write its current model of the network into a Nessus compatible “.nsr” file a specified number of minutes. If the PVS is being managed by a SecurityCenter, the report frequency should not be less than 15 minutes since PVS sensors are only polled once every 15 minutes. The default value is 60 minutes.</td>
</tr>
</tbody>
</table>
| **detect-encryption** | This keyword block specifies a set of “dependency” and “exclude” statements that the PVS uses to analyze sessions containing encrypted traffic. The dependency keywords identify the specific PVS IDs that have been detected on a host before an analysis of a session occurs. The exclude keyword specifies a list of protocol filters for which the PVS should avoid performing encryption detection. When an encrypted session is detected, an alert is generated showing source, destination, ports and session type. The session type may be one of the following:  
  - internal-interactive-session (4)  
  - outbound-interactive-session (5)  
  - inbound-interactive-session (6)  
  - internal-encrypted-session (7)  
  - outbound-encrypted-session (8)  
  - inbound-encrypted-session (9)  
  The number in parentheses represents the corresponding plugin ID field. |
<p>| <strong>detect-interactive-sessions</strong> | This keyword block specifies a set of “dependency” and “exclude” statements that the PVS uses to analyze sessions that contain interactive traffic. The dependency keywords identify the specific PVS IDs that have been detected on a host before an analysis of a session occurs. The exclude keyword specifies a list of protocol filters for which the PVS will avoid performing interactive detection. When an encrypted session is detected, an alert is generated showing source, destination, ports and session type. For a list of session types, refer to the detect-encryption option above. |
| <strong>high-speed</strong> | The PVS is designed to look for various protocols on non-standard ports. For example, the PVS can easily find an Apache server running on a port other than 80. However, on a high-speed network, the PVS can be placed into a “high-speed” mode that allows it to focus certain plugins on specific ports. When the high-speed keyword is specified, any plugin that has the keywords hs_dport or hs_sport defined in the plugin will run the plugin only on traffic traversing the specified ports. The high-speed keyword takes no arguments. |</p>
<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>realtime-syslog</td>
<td>Specifies the IP address of a SYSLOG server to receive real-time events from the PVS. Up to sixteen SYSLOG servers can be specified for alerting. A local SYSLOG daemon is not required. Multiple <code>realtime-syslog</code> keywords can be used to specific more than one SYSLOG server.</td>
</tr>
<tr>
<td>vulndata-syslog</td>
<td>Specifies the IP address of a SYSLOG server to receive vulnerability data from the PVS. Up to sixteen SYSLOG servers can be specified for alerting. A local SYSLOG daemon is not required. While PVS can display multiple log events related to one connection, it would only send a single event to the remote SYSLOG server(s).</td>
</tr>
<tr>
<td>connections-to-services</td>
<td>When enabled, this keyword causes PVS to log which clients are attempting to connect to servers on the network and what port they are attempting to connect. They do not indicate if the connection was successful, but only that an attempt to connect was made. Events detected by the PVS of this type are logged as Nessus ID “00002”.</td>
</tr>
<tr>
<td>show-connections</td>
<td>When enabled, PVS will record clients in the focus network that attempt to connect to a server IP address and port and receive a positive response from the server. The record will contain the client IP address, the server IP address and the server port that the client was attempting to connect to. For example, if four different hosts within the focus network attempted to connect to a particular server over port 80 and received a positive response, then a list of those hosts would be reported under event “00003” and port 80. By default, this feature is not enabled.</td>
</tr>
<tr>
<td>detect-portscans</td>
<td>This keyword specifies a set of variables (defined below) that are used to determine how portscan detection will occur and what a portscan and portsweep behave like.</td>
</tr>
<tr>
<td>portscan-report-frequency</td>
<td>This variable specifies, in minutes, how often the PVS will write a report on portscans. By default, this is set to 5 minutes.</td>
</tr>
<tr>
<td>portscan-memory-threshold</td>
<td>Specifies the amount of memory to be used by the PVS while collecting unique session information to be evaluated. If this threshold is reached, the collected data will be immediately evaluated.</td>
</tr>
<tr>
<td>portscan-addr-threshold</td>
<td>Specifies the maximum number of unique destination addresses on one port occurring from one host, which will be considered portsweep activity.</td>
</tr>
<tr>
<td>portscan-port-threshold</td>
<td>Specifies the maximum number of unique destination ports to one server occurring from one host, which will be considered</td>
</tr>
</tbody>
</table>
**new-host-alert**  
The PVS listens to network traffic and attempts to discover when a new host has been added. To do this, the PVS constantly compares a list of hosts that have generated traffic in the past to those currently generating traffic. If it finds a new host generating traffic, it will issue a “new host alert” via the real-time log. For large networks, the PVS can be configured to run for several days to gain knowledge about which hosts are active. This prevents the PVS from issuing an alert for hosts that already exist. The number of days the PVS will monitor traffic to learn which hosts are active is specified by this setting. For large networks, Tenable recommends that the PVS operate for at least one day before detecting new hosts.

**backup-interval**  
The PVS constantly compares its list of active hosts to the list of hosts generating traffic to discover newly added or missing hosts. To prevent rediscovery of the entire network, the PVS can frequently write the list of active hosts to a file so that the information is available to PVS across restarts. Tenable recommends that this file be updated every 120 minutes.

**networks**  
Specifies the networks to be monitored. This is set by the PVS installation script in Unix.

**excluded-networks**  
Specifies any networks that will be excluded from PVS monitoring. Networks are specified using CIDR notation and placed between the brackets after this directive. If left blank, no addresses will be excluded.

### Using Nessus, SecurityCenter and PVS

Extensive documentation for the applications installed on the Tenable Appliance is available at [https://support.tenable.com/support-center/](https://support.tenable.com/support-center/).

### 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 the button labeled “Rebuild Plugin Database”. Wait approximately 5-10 minutes for the processing to complete. Refresh the page and see if Nessus starts. If not, make sure 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. The Nessus user interface or Security Center will not connect to the server.

A. Ensure the correct Nessus user is configured.

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

A. For the VM appliance, you must reload the image from a saved VM copy or from the original on the Tenable Support Portal. If you reload the original image from the Tenable Support Portal, you may apply your saved configuration. If you did not save a copy of your configuration, you will need to re-enter the information.

For the hardware appliance, use the appliance console “Revert to Factory Defaults” option to restore the appliance to the default configuration. Immediately after reverting, login to the appliance web interface to set the initial administrative password.

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. For example, changing the configuration port used by PVS from “1243” to another port will modify the configuration file, however, the “Restart PVS” command 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.

**Q. How can I upgrade from previous versions of the Tenable Appliance to version 1.0.4?**

**A.** While there is no direct upgrade path available, creating a backup of the appliance configuration and application settings and then restoring that backup post-install ensures that settings are not lost. See Appendix 1 below for migrating the Security Center 3 application settings and data during an upgrade from version 1.0.3 to 1.0.4.
Acknowledgements

This product uses the scripting language written by Lua.org (http://www.lua.org/).
Copyright © 1994-2008 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 INTERRUPTION) 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 Aranha, 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://keplerproject.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/), designed and implemented by Roberto Ierusalimschy and Marcela Ozório Suárez. 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.
About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. For more information, please visit us at http://www.tenable.com/.
Appendix 1: Migrating from Security Center 3 to 4

The steps below detail how to migrate from Security Center 3 to SecurityCenter 4 in conjunction with upgrading from Tenable Appliance version 1.0.3 to 1.0.4.

1. Login to the Tenable Appliance (version 1.0.3) and go to the Applications page. Take a backup of the Security Center 3 application and download the backup file locally.
2. Install the new TenableAppliance-1.0.4 VM image.
3. Login to the appliance and go to the Administration Page. Choose “Restore from File” and select “Only Security Center 3” from the available restore options.
4. Select the backup file, click on “Restore Backup” and wait while the file loads.
5. Click on “Restore Backup” again.
6. Upload the Security Center 3 license key.
7. Login and verify Security Center 3 data
8. Disable the Security Center 3 application
9. Enable the SecurityCenter 4 application
10. Login using the credentials “admin”/“password” and complete the migration wizard
11. Wait for the upgrade process to complete.
12. Login to SecurityCenter 4 and verify the product version:

<table>
<thead>
<tr>
<th>Version Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support ID:</td>
</tr>
<tr>
<td>Tenable Appliance:</td>
</tr>
<tr>
<td>SecurityCenter 4:</td>
</tr>
</tbody>
</table>