SecurityCenter 4.2
Administration Guide
January 24, 2012
(Revision 5)

The newest version of this document is available at the following URL:
http://static.tenable.com/prod_docs/SecurityCenter_4.2_Admin_Guide.pdf
# Table of Contents

- **Introduction** .............................................................................................................................................. 5
- **Standards and Conventions** ......................................................................................................................... 5
- **Abbreviations** .................................................................................................................................................. 6
- **SecurityCenter Administrator Functions** .................................................................................................... 6
  - Starting/Halting SecurityCenter ................................................................................................................... 6

- **SecurityCenter Home Page/Dashboard** ....................................................................................................... 7

- **System Configuration** ................................................................................................................................... 9
  - Configuration .................................................................................................................................................. 9
    - Basic ......................................................................................................................................................... 9
    - Mail ......................................................................................................................................................... 10
    - LDAP ..................................................................................................................................................... 11
    - Miscellaneous ......................................................................................................................................... 13
    - Update .................................................................................................................................................... 15
  - Preferences .................................................................................................................................................. 16
    - Basic ......................................................................................................................................................... 16
    - Notifications .......................................................................................................................................... 16
  - Logs ............................................................................................................................................................ 17
  - Keys ........................................................................................................................................................... 18
    - Remote LCE Key Exchange ..................................................................................................................... 19

- **Resource Management** .................................................................................................................................. 19
  - Nessus Scanners ........................................................................................................................................... 19
    - Adding a Nessus Scanner .......................................................................................................................... 20
    - Scan Zones ............................................................................................................................................. 21
  - Passive Vulnerability Scanners .................................................................................................................... 22
  - Log Correlation Engines ............................................................................................................................... 23
  - IDS Sources ............................................................................................................................................... 25

- **Data Management** ......................................................................................................................................... 25
  - Repositories .................................................................................................................................................. 25
    - Local Repository .................................................................................................................................... 26
    - Remote Repository .................................................................................................................................. 27
    - Offline Repository .................................................................................................................................... 29
  - Accept Risk Rules ....................................................................................................................................... 32
  - Recast Risk Rules ....................................................................................................................................... 33

- **User Management** ......................................................................................................................................... 34
  - Organizations ............................................................................................................................................... 34
  - Users ............................................................................................................................................................ 40
    - Administrators ......................................................................................................................................... 40
    - Roles ......................................................................................................................................................... 41
    - User Visibility ......................................................................................................................................... 43
    - User Access Control ............................................................................................................................... 43
Creating and Deploying SSL Authentication for Nessus ................................................................. 91
Create Keys and User on Nessus Server ..................................................................................... 91
Transfer Certificates and Keys to SecurityCenter ........................................................................ 93
Check Permissions on Security Center ....................................................................................... 94
Restart Nessus Daemons ........................................................................................................... 94
Change the Nessus Mode of Authentication ............................................................................. 94

Appendix 4: Using a Custom SSL Certificate .............................................................................. 95

Appendix 5: Offline SecurityCenter Plugin Updates ................................................................. 96
Nessus ........................................................................................................................................... 96
PVS (SecurityCenter 4.2 and greater only) .................................................................................. 97

Appendix 6: Configuring LDAP with Multiple Organizational Units ...................................... 98
Option 1 (Preferred) .................................................................................................................... 98
  Option 1 Example ...................................................................................................................... 98
Option 2 ....................................................................................................................................... 99
  Option 2 Example ...................................................................................................................... 100
Option 3 ....................................................................................................................................... 101
  Option 3 Example ...................................................................................................................... 102
INTRODUCTION

This document describes the administrative functions of Tenable Network Security’s SecurityCenter 4.2.

Since many of Tenable’s customers have requirements to maintain separation of duties, the SecurityCenter 4.2 documentation has been separated into the following documents to better organize the material based on the organizational role. Note that there may be some overlap in roles as well as content provided with each of the following guides:

> **SecurityCenter 4.2 Architecture** – This document describes the SecurityCenter architecture and provides a high-level view of how the components interact. This document is beneficial for those who are considering purchasing SecurityCenter.

> **SecurityCenter 4.2 Installation Guide** – This document provides instructions for the installation of SecurityCenter 4. The target audience for this document is system administrators who need to install the SecurityCenter application. Included in this document are quick instructions for the **admin** user to add a Nessus scanner and create a user account to launch a test scan to ensure SecurityCenter is correctly installed.

> **SecurityCenter 4.2 Upgrade Guide** – This document describes the process of upgrading to the latest version of SecurityCenter 4.

> **SecurityCenter 4.2 Administration Guide** – This document provides instructions for the administration of SecurityCenter by the **admin** user. The **admin** user is the first user to log in to the SecurityCenter after the initial installation and is responsible for configuration tasks such as defining organizations, repositories, Nessus scanners, LCE servers and PVS sensors. The **admin** user does not have the ability to create and launch Nessus scans.

> **SecurityCenter 4.2 User Guide** – This document provides instructions for using SecurityCenter by an Organization Head user or lesser account.

Please share your comments and suggestions with us by emailing them to support@tenable.com.

A basic understanding of Linux/Unix, Windows, vulnerability scanning with Nessus, intrusion detection, computer hardware and log analysis is assumed.

STANDARDS AND CONVENTIONS

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

Command line options and keywords are also indicated with the courier bold font. Command line options may or may not include the command line prompt and output text from the results of the command. Often, the command being run will be **boldfaced** to indicate what the user typed. Below is an example running of the Unix `pwd` command:

```
# pwd
/opt/sc4/daemons
#
```

Important notes and considerations are highlighted with this symbol and grey text boxes.
ABBREVIATIONS
The following abbreviations are used throughout this documentation:

LCE  Log Correlation Engine
PVS  Passive Vulnerability Scanner
SC   SecurityCenter
SSH  Secure Shell
IDS  Intrusion Detection System

SECURITY CENTER ADMINISTRATOR FUNCTIONS
SecurityCenter administrators have the following responsibilities:

> Manage the configuration of each SecurityCenter organization and which networks they are allowed to scan
> Manage scan policies, custom audit files and credentials for all organizations
> Manage the network of active Nessus scanners, the network “zones” they belong to and the networks they are allowed to scan
> Manage the network of Passive Vulnerability Scanners and what organizations have access to their detected real-time vulnerabilities
> Manage which Log Correlation Engines each organization has access to and what repositories the LCE will correlate against
> Delete accept and recast risk rules created by organizational users
> Manage what external data feeds (ICAT, Snort, Nessus plugins, etc.) SecurityCenter is subscribed to
> Manage the SecurityCenter services
> Add and manage other SecurityCenter administration users
> Add and manage custom roles that are available to all organizations
> Review SecurityCenter log files and job queues

Starting/Halting SecurityCenter
When SecurityCenter is installed and licensed, the required services are started by default. To display the status of SecurityCenter services, enter the following command as the root user on the SecurityCenter server:

```
# service SecurityCenter status
```

If SecurityCenter services are running, the following message will be displayed:

```
SecurityCenter (httpd lightning-proxy Jobd.php) is running...
```

Otherwise, the message will state “SecurityCenter is stopped”.

To start SecurityCenter, enter the following command:
# service SecurityCenter start

To halt SecurityCenter, enter the following command:

# service SecurityCenter stop

To restart SecurityCenter, enter the following command:

# service SecurityCenter restart

SecurityCenter services can also be started and stopped from the admin web management interface. Simply click on the status circle (the green circle in the lower right of the image below) in the lower right-hand corner of the web page. A popup similar to the one below is displayed:

<table>
<thead>
<tr>
<th>License</th>
<th>Valid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Feed</td>
<td>Valid</td>
</tr>
<tr>
<td>Last Plugin Update</td>
<td>Apr 25, 2010 4:00</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Job Scheduler</th>
<th>Running</th>
<th>Start</th>
<th>Stop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Processor</td>
<td>Running</td>
<td>Start</td>
<td>Stop</td>
</tr>
</tbody>
</table>

If the system status is normal, the circle is green and the “Job Scheduler” and “Scan Processor” indicators show “Running”. Click on “Stop” and then “Start” to restart any of the two processes manually. If any problems exist with the SecurityCenter status, they will be displayed on this popup and in the logs described in the “Logs” section of this document.

SECURITYCENTER HOME PAGE/DASHBOARD

To navigate within the SecurityCenter user interface, use the menu on the web interface screen, not the browser’s back and forward arrows.

Adobe Flash Player must be installed to use the SecurityCenter 4 web interface. It can be obtained at [http://get.adobe.com/flashplayer/](http://get.adobe.com/flashplayer/).
The minimum recommended browser window size is 1024x580. Resizing the browser window below this size when viewing the SecurityCenter web interface causes some items to display incorrectly.

To launch SecurityCenter, bring up a web browser on a system that has access to the SecurityCenter’s network address space and enter the URL in the following format:

https://<SERVER ADDRESS OR NAME>/

The SecurityCenter web interface is available using a secure web connection (https). SecurityCenter 4 does not listen on port 80.

The dashboard is the first screen displayed when you log in to the SecurityCenter user interface. It displays scanner, LCE and plugin data through predefined components. The Dashboard can also be displayed by selecting “Dashboard” from the “Home” tab. There are two tabs: “Overview” and “LCE Overview”. The Overview tab contains a Scanner Status table, a Repository Statistics table and a table containing the latest plugin feed updates. The LCE Overview tab lists the current LCE server and client status (up to 1,000 clients displayed).

Sample SecurityCenter Administrator Dashboard – Overview
SYSTEM CONFIGURATION
The “System” link at the top right of the SecurityCenter web interface contains a number of options for configuring the desired SecurityCenter system behavior. When logged in as the admin user, additional options are available that are not available for non-admin users. Among the available admin options are “Basic” (licensing and activation), “Mail”, “LDAP”, “Miscellaneous” and “Update”. The sections below go into detail about each of the categories and their configuration items.

CONFIGURATION

Basic
The “Basic” options allow the admin user to configure the licensing and activation code settings for SecurityCenter. The screen capture below shows a sample SecurityCenter Basic option configuration page:
For most installations, this page will not be modified by the administrator, except when an upgraded IP Count license or Nessus Activation Code has been purchased by the organization and needs to be added.

To view currently used IPs in your license, log in to SecurityCenter as the “admin” user and go to “Repositories” -> “Repositories”. Hover the cursor over the “Total Active IPs” graphic at the bottom of the screen to view currently used IPs, total IP license count and IPs remaining.

The following plugins are not counted against your license IP count:
Nessus IDs: 10180, 10287, 19506, 12053, 11933
PVS IDs: 00003, 00012

To add a new license, use the “Browse” button next to the “License” field to locate the license key file received in your email and then click on “Submit”. The same general procedure applies to adding an Activation Code. Enter the Activation Code string in the appropriate field and then verify it. If an Activation Code already exists on SecurityCenter, click on “Reset” to allow the new Activation Code to be entered.

The current license status is displayed in the “License Status” box and indicates the current license state, maximum IP count allowed by the current license, the hostname that the license applies to and the expiration date, if any.

**Mail**
The “Mail” option designates SMTP settings for all email related functions of SecurityCenter. Available options include SMTP host, port, authentication method, secure connection and return address. In addition, a “Test SMTP Settings” link is displayed in the upper right-hand corner of the page to confirm the validity of the settings.

The “Return Address” defaults to “noreplys@localhost”. Please use a valid return email address. If this field is cleared or the email server requires emails from valid accounts, the email will not process.
If LDAP authentication is to be used, it is recommended to leave at least one SecurityCenter administrator account and one manager account for each organization in SecurityCenter set to use TNS authentication in the event that the LDAP/AD services becomes unreachable.

LDAP configuration settings enable your SecurityCenter to utilize any LDAP server for authentication purposes. This enhances the security of SecurityCenter by facilitating “single sign-on” and password complexity requirements in environments where security policy mandates it. After clicking on the “LDAP” tab, a page similar to the one below is displayed.
Fill out the LDAP configuration settings as provided by the LDAP server administrator and click on “Test LDAP Settings”. If the settings are correct, a dialog will be displayed similar to the screen capture below indicating that the LDAP settings are valid.

If the LDAP settings are incorrect, the dialog box will indicate failure and provide details on why it failed (e.g., incorrect “Search Base” or “server could not be contacted”).

This table provides a detailed breakdown of the available LDAP parameters:

**Table 1 – LDAP Directory Information**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>Use TLS</td>
<td>This selection indicates if Transport Layer Security (TLS) is enabled in the LDAP server.</td>
</tr>
<tr>
<td>Username</td>
<td>If the LDAP or Active Directory server requires credentials to search the user data within it, then the “User name” and “Password” fields are required. By default, Active Directory requires an authenticated search. Enter the username within this field in the “email” style format (<a href="mailto:user@domain.com">user@domain.com</a>).</td>
</tr>
<tr>
<td>Password (optional)</td>
<td>If the LDAP or Active Directory requires credentials to search for user data, then the “User name” and “Password” fields are required. By default, Active Directory requires an authenticated search.</td>
</tr>
<tr>
<td></td>
<td>Please use complex and lengthy passwords based on your local security policy password requirements.</td>
</tr>
<tr>
<td><strong>Server</strong></td>
<td></td>
</tr>
<tr>
<td>Directory Server</td>
<td>Enter the IP address or DNS name of the LDAP or Active Directory server in this field.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the remote LDAP port here. When TLS is set to “no”, the port will default to 389, and when TLS is set to “yes”, port 636 is automatically selected as these are the default ports used with LDAP.</td>
</tr>
</tbody>
</table>
Search Base

This is the LDAP search base used as the starting point to search for the user information.

Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username Attribute</td>
<td>This is the attribute name on the LDAP/AD server that contains the username for the account. For Active Directory, this is often specified by the string “sAMAccountName”. Contact your local LDAP administrator for the correct username attribute to use.</td>
</tr>
<tr>
<td>Email Attribute</td>
<td>This is the attribute name on the LDAP/AD server that contains the email address for the account. For Active Directory, this is often specified by the string “mail”. Contact your local LDAP administrator for the correct email attribute to use.</td>
</tr>
<tr>
<td>Phone Attribute</td>
<td>This is the attribute name on the LDAP/AD server that contains the telephone number for the account. For Active Directory, this is often specified by the string “telephoneNumber”. Contact your local LDAP administrator for the correct telephone attribute to use.</td>
</tr>
<tr>
<td>Name Attribute</td>
<td>This field is the attribute name on the LDAP/AD server that contains the name associated with the account. For Active Directory, this is often specified by the string “displayName”. Contact your local LDAP administrator for the correct name attribute to use.</td>
</tr>
</tbody>
</table>

Miscellaneous

Miscellaneous settings cover proxy setup, data expiration and web authentication settings. A sample SecurityCenter screen capture is included below:

From this configuration page, a web proxy can be configured if desired by entering the host URL (protocol, proxy host name or IP address), port, username and password. The host name used must resolve properly from the SecurityCenter host.
Data expiration determines how long SecurityCenter retains acquired data. Use the table below to determine default and minimum values for these settings:

**Table 2 – Data Expiration**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Data</strong></td>
<td>SecurityCenter will automatically remove any vulnerability data that was discovered via active scanning after the designated number of days. The default value of this field is 365. If this field is left blank, the value is set to zero. Setting this field to zero will remove all active vulnerabilities from the database each night.</td>
</tr>
<tr>
<td><strong>Passive Data</strong></td>
<td>By default, SecurityCenter will automatically remove any passive vulnerability data that is older than seven days. If this field is left blank, the value will be set to zero. Setting this field to zero will remove all passive vulnerabilities from the database each night.</td>
</tr>
<tr>
<td><strong>Compliance Data</strong></td>
<td>SecurityCenter will automatically remove any compliance data after the designated number of days. The default value of this field is 365. If this field is left blank, the value is set to zero. Setting this field to zero will remove all compliance vulnerabilities from the database each night.</td>
</tr>
<tr>
<td><strong>Mitigated Data</strong></td>
<td>Automatically remove any mitigated vulnerability data after the designated number of days. The default value of this field is 365. If this field is left blank, the value is set to zero. Setting this field to zero will remove all mitigated vulnerability data from the database each night.</td>
</tr>
<tr>
<td><strong>Vulnerability Trending Data</strong></td>
<td>Prior to SecurityCenter 4.2 the default was 365 days. Upgraded installations will maintain the 365 day default unless manually changed. SecurityCenter will automatically remove any vulnerability trending data after the designated number of days. The default value of this field is 90. If this field is left blank, the value is set to zero. Setting this field to zero will remove all trend snapshots from the database each night.</td>
</tr>
<tr>
<td><strong>Scan Results</strong></td>
<td>Automatically remove any scan results after the designated number of days. The default value of this field is 365. If this field is left blank, the value is set to zero. Setting this field to zero will remove all scan results from the database each night.</td>
</tr>
<tr>
<td><strong>Report Results</strong></td>
<td>Automatically remove any report results after the designated number of days. The default value of this field is 365. If this field is left blank, the value is set to zero. Setting this field to zero will remove all report results from the database each night.</td>
</tr>
</tbody>
</table>
Closed Tickets

Automatically remove any closed tickets after the designated number of days. The default value of this field is 365. If this field is left blank, the value is set to zero. Setting this field to zero will remove all closed tickets from the database each night.

The "Authentication Settings" apply to the SecurityCenter web interface login parameters. Use the table below to determine correct values for your environment:

### Table 3 – SecurityCenter Authentication Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurityCenter Location</td>
<td>The URL used for emails originating from SecurityCenter with links back to SecurityCenter. This is especially useful in cases where a web proxy is in use.</td>
</tr>
<tr>
<td>Session Timeout</td>
<td>The web session timeout in minutes (default: 60 minutes).</td>
</tr>
<tr>
<td>Maximum Login Attempts</td>
<td>The maximum number of login attempts allowed by SecurityCenter before the account is locked out (default: 20). Setting this value to zero disables this feature.</td>
</tr>
<tr>
<td>Startup Banner Text</td>
<td>Enter the text banner that is displayed prior to the login interface.</td>
</tr>
</tbody>
</table>

**Update**

The SecurityCenter update settings are used to determine the update schedule for common tasks such as plugin updates, IDS signature updates, IDS correlation updates and Nessus synchronization. All updates are configured daily by default except for Nessus synchronization (plugin synchronization), which occurs hourly.

The following settings are available:
Table 4 – Update Schedules

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Plugins</strong></td>
<td>Frequency that SecurityCenter will update active plugins.</td>
</tr>
<tr>
<td><strong>IDS Signatures</strong></td>
<td>Frequency that SecurityCenter will update IDS signatures via third-party sources.</td>
</tr>
<tr>
<td><strong>IDS Correlation Databases</strong></td>
<td>Frequency that the vulnerability information is pushed to the LCE for correlation.</td>
</tr>
<tr>
<td><strong>Passive Plugins</strong></td>
<td>Enables regular downloads of the PVS signatures. These plugins will be pushed out to every PVS that SecurityCenter is managing. Manual update of the PVS plugins is also supported under the &quot;Plugins&quot; tab.</td>
</tr>
<tr>
<td><strong>Nessus Synchronization in hours (720 max)</strong></td>
<td>This setting specifies how often SecurityCenter will push plugins out to its configured Nessus and PVS scanners. Synchronizing the scanners more frequently assures they have the most current plugins, but also puts a performance load on SecurityCenter. Increase the default setting (12) if scan completion times are impacted by the plugin indexing and distribution process.</td>
</tr>
</tbody>
</table>

**PREFERENCES**

On the upper right hand of the SecurityCenter web interface, the System option contains a dropdown that includes Preferences. This option includes both location and notification settings.

**Basic**

The basic option tab allows the admin to configure the local time zone. **Important:** This affects the date/time displayed on reports and within the user interface and not the actual system time on the server itself.

**Notifications**

Notifications are a new feature of SecurityCenter 4 that allows specified events to display a popup in the lower right-hand corner of the SecurityCenter web UI.
Current notifications can be viewed by clicking on the left-hand circle at the lower right-hand corner of the SecurityCenter web page. Unread notifications will have a blue circle while a black circle indicates no unread notifications. Clicking on “Mark All As Read” removes the blue circle, but leaves the notifications there for later review. To view notification details, click on the highlighted title to expand out the notification details.

Notifications can also be deleted by clicking on the “X” to the right of the notification text or clicking on the “Delete All” command button within the Notification box dialog. Admin configurable notifications are displayed in the screen capture below:

Logs

On the upper right hand of the SecurityCenter web interface, the System option provides a dropdown that includes a Logs section. In addition, for the admin user, the same log interface is available by accessing “Status” and then “Logs”.

The SecurityCenter logs contain detailed filter options to troubleshoot unusual system or user activity. The logs include filters that allow the user to search logs based on parameters such as date, user, module, severity, keywords and source. An example keyword and user search based on the word “attempt” is displayed below:
This search flexibility improves debugging and maintains an audit trail of users who access SecurityCenter or perform basic functions such as changing passwords, recasting risks or running Nessus scans.

**Keys**

On the upper right hand of the SecurityCenter web interface, the **System** option contains a dropdown that includes a **Keys** section. Keys allow the administrator to use key-based authentication with a remote SecurityCenter (remote repository) or between a SecurityCenter and an LCE server. This also removes the need for the SecurityCenter administrator to know the administrator login or password of the remote system.

The public key from the local SecurityCenter must be added to the “Keys” section of the SecurityCenter that you wish to retrieve a repository from. If the keys are not added properly, the remote repository “add” process will prompt for the root username and password of the remote host before the repository add/sync occurs.

Available options include “Download Key”, “Add” and “Delete”. To download the local SecurityCenter’s key, click on “Download Key”. After doing this, the key format dialog is displayed. Choose the type of key being requested and then click on “Submit”:
If “DSA Key” was chosen during download, the DSA public key is downloaded and likewise, choosing “RSA Key” downloads the RSA public key string.

Clicking on “Add” brings up the dialog box below:

In the “Public Key” box, paste the public key from the remote SecurityCenter and click on “Submit”. If a valid public key was entered, a “Success” message is displayed and the key will show up in the key list.

Remote LCE Key Exchange
A manual key exchange between the SecurityCenter and the LCE is normally not required; however, in some cases where remote root login is prohibited or key exchange debugging is required, you will need to manually exchange the keys.

For the remote LCE to recognize the SecurityCenter, you need to copy the SSH public key of the SecurityCenter and append it to the “/opt/lce/.ssh/authorized_keys” file. The “/opt/lce/daemons/lce-install-key.sh” script performs this function. The steps are outlined in Appendix 2 of this document.

RESOURCE MANAGEMENT
The Resources tab provides the Admin user with the ability to configure supporting resources such as Log Correlation Engines, Nessus scanners (and scan zones) and Passive Vulnerability Scanners. This section describes the various resources and configuration options.

NESSUS SCANNERS
In the SecurityCenter framework, the Nessus scanner behaves as a server, while SecurityCenter serves as a client that schedules and initiates scans, retrieves results,
reports results and performs a wide variety of other important functions. Click on “Resources” and then “Nessus Scanners” to retrieve a list of the scanners and their current state. If the status of a scanner has changed recently (since visiting the page), click the “Update Status” button to see the latest scanner status. In the example below, the Nessus scanner is installed on the same system as SecurityCenter and is functioning properly. This type of configuration is fine for small to medium size enterprises.

### Adding a Nessus Scanner

To add a scanner, click on the “Add” button. A screen capture of the add dialog is shown below:

![Add Scanner Dialog](image)

The table below goes into more detail about the available options for adding a Nessus scanner:

### Table 5 – Nessus Scanner Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Descriptive name for the Nessus scanner.</td>
</tr>
<tr>
<td>Description</td>
<td>Scanner description, location or purpose.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the scanner.</td>
</tr>
</tbody>
</table>

---

[Image of the Nessus Scanner add dialog]

---

Copyright © 2002-2012 Tenable Network Security, Inc.
Port
TCP port that the Nessus scanner listens on for communications from SecurityCenter. The default is port 1241.

Username
Username generated during the Nessus install for daemon to client communications. This must be an administrator user.

Starting with Nessus 4.4, the Nessus scanner is available via its web interface, even after it has been added to the SecurityCenter. Use this username to log in to the Nessus web interface, if desired. Because this login ability is independent of the SecurityCenter, SC-created objects such as policies and credentials are not available when the Nessus scanner is accessed directly.

Authentication Type
Password Based or SSL Certificate. For detailed SSL Certificate configuration options, see Appendix 3: Nessus SSL Configuration.

Password
The login password.

Zones
The zone(s) that will contain this scanner.

Scan Zones
Scan Zones define the IP ranges associated with the scanner along with the organizational access. SecurityCenter allows organizations to be configured with two different scan zone modes: “selectable” and “forced”. If an organization is in “selectable” mode, any available zones can be associated with the organization and made available to users for scanning configuration. If an organization is in “forced” mode, the selected zone will always be used for every scan performed by users in that organization.

When in “selectable” mode, at scan time, the zones associated with the organization and “default” are available to the user. When a scan is configured to use a specific zone in either selectable or forced mode, the zone’s ranges are ignored and any IPs in the managed ranges for that user will be scanned by the Nessus scanners associated with the chosen zone.

When a scan is configured to use the “default” zone, the targets for the scan will be given to scanners in ALL zones in the application based on the zone’s specified ranges (20K character limit). This facilitates optimal scanning and is very useful if an organization has devices placed behind a firewall or NAT device and has conflicting RFC 1918 non-internet-routable address space with another organization. In addition, some organizations may benefit from the ability to override their default scanner(s) with one(s) from a different zone. This allows an organization to more easily run internal and external vulnerability scans.
Sometimes forcing a scan to use a “non-ideal” scanner is helpful to analyze the vulnerability stance from a new perspective. For example, setting the default scanner to an external one allows you to see the attack surface from an external attacker’s perspective.

An example Scan Zone configuration screen capture is displayed below:

**PASSIVE VULNERABILITY SCANNERS**

Tenable’s Passive Vulnerability Scanner (PVS) 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 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.

When deployed as a “stand alone” sensor, the PVS simply records its detected vulnerabilities to a .nsr, .nessus, .xml or .html file(s), depending on the configuration of the PVS. When deployed for operation with SecurityCenter, the PVS ships with an agent named the PVS Proxy. This agent is a server that waits for inbound connections from SecurityCenter.

By default, the PVS Proxy listens on port 1243. This is similar to a typical Nessus daemon that listens on port 1241 and the default port for SecurityCenter’s external scan connection requests that listen on port 1242. None of these ports is hard-coded, and they can easily be modified for operation on different ports.

On connection, SecurityCenter will ask the PVS Proxy for the latest (if any) vulnerability report. If the PVS is configured to record its passive vulnerability data every six hours, then new passive vulnerability data will only be available every six hours.
By default, SecurityCenter will also check every 12 hours to see if any new passive vulnerability plugins have been downloaded from Tenable and will push them out to each PVS scanner.

The screen capture below shows a listing of several working PVS scanners:

To configure one or more of Tenable’s PVS servers, under the “Resources” tab select “Passive Scanners”. This will produce a form that lists all configured PVS devices and their current status.

To enable a PVS, add the PVS scanner IP address, the port its proxy is listening on (which defaults to 1243), its password and then click on the repositories that will be subscribed to the PVS data.

**Please use complex and lengthy passwords based on your local security policy password requirements.**

**LOG CORRELATION ENGINES**

Tenable’s Log Correlation Engine (LCE) is a software module that aggregates, normalizes, correlates and analyzes event log data from the myriad of devices within the infrastructure. Since the LCE is closely integrated with the SecurityCenter, log analysis and vulnerability management can be centralized for a complete view of the security posture.
SecurityCenter performs vulnerability, compliance and event management, but does not directly receive logs or IDS/IPS events. The LCE upgrade to SecurityCenter does all of this by processing the events and then passing them on to SecurityCenter. Once on SecurityCenter, the logs are aggregated further and made available for analysis and reporting.

LCE 3.6.1 or greater is required for SecurityCenter 4.2.

Note that more than one Log Correlation Engine can be configured to work with SecurityCenter.

To configure LCE servers, select “Log Correlation Engines” under the “Resources” tab. A screen will be displayed similar to the following:

Click on “Add” to bring up the dialog in the screen capture below. Available fields include Name, Description, IP Address and Organizations.

Earlier versions of SecurityCenter had a “Managed Ranges” field that was used for event direction determination. This field has been removed in SecurityCenter 4.2 and event direction is now determined by the ranges specified in the lce.conf configuration file “include-networks” directive.

During the LCE add process, the remote LCE login prompt will occur so that the SecurityCenter authenticate with the LCE. If remote credential login is prohibited in your environment, refer to Appendix 2 for instructions on how to authenticate to the LCE server using key authentication.
If company policy prohibits remote root login, a manual key exchange process can be used. See Appendix 2: Manual LCE Key Exchange for detailed guidance.

Table 6 – LCE Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name used to describe the Log Correlation Engine.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the Log Correlation Engine.</td>
</tr>
<tr>
<td>IP Address</td>
<td>IP address of the Log Correlation Engine.</td>
</tr>
<tr>
<td>Organizations</td>
<td>Determines which Organizations will be able to access data from the configured Log Correlation Engine.</td>
</tr>
</tbody>
</table>

**IDS SOURCES**

Starting with SecurityCenter 4, IDS sources are configured solely on the Log Correlation Engine (LCE) instead of through the SecurityCenter interface. This change enhances SecurityCenter performance and event correlation. For more information on configuring IDS sources, please see the LCE documentation located on the Tenable Support Portal.

**DATA MANAGEMENT**

**REPOSITORIES**

A repository is essentially a database of vulnerability data defined by one or more ranges of IP addresses. SecurityCenter integrates repositories of vulnerability data that are shared as
needed among users and organizations based on manager-defined assets. The use of repositories allows for scalable and configurable data storage for organizations. Repositories can also be shared between multiple SecurityCenters. Repositories are configured by the administrative user and made available to the Organization Head to assign to users as needed.

When creating SecurityCenter 4 repositories, LCE event source IP ranges must be included along with the vulnerability IP ranges or the event data will not be accessible from the SecurityCenter UI.

There are three types of repositories: “Local”, “Remote” and “Offline”. Local repositories are active repositories of SecurityCenter data collected via scanners attached to the local SecurityCenter. Remote repositories contain IP address and vulnerability information obtained via network synchronization with a second (remote) SecurityCenter. Offline repositories enable SecurityCenter to obtain repository data via manual export/import from a remote SecurityCenter that is not network-accessible. The screen capture below shows several configured repositories.

Repository data collected from a remote or offline repository is static and used solely for reporting purposes.

Click on the “Add” button to add a new repository. The sections below contain options for adding each of the three types of repositories.

**Local Repository**
This is the default repository type. Data stored in local repositories can be shared between Organizations and includes the full range of event and vulnerability metadata. The table below describes configurable fields for a local repository:
### Table 7 – Local Repository Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>The repository name.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Descriptive text for the repository.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Local</td>
</tr>
<tr>
<td><strong>Trending</strong></td>
<td>If trending is not selected, any query that uses comparisons between repository snapshots (e.g., trending line charts) will not be available. This option allows for a periodic snapshot of the .nessus data for vulnerability trending purposes. This option is particularly useful in cases where trending is important. In situations where repository datasets do not change frequently – negating the need for trending – disable this option to minimize disk space usage.</td>
</tr>
<tr>
<td><strong>Generate Nessus File</strong></td>
<td>Use this option to schedule how frequently the Nessus file snapshot will be taken. Available options include: Never, Daily, Weekly, Monthly (Day) and Monthly (Date).</td>
</tr>
<tr>
<td><strong>IP Ranges</strong></td>
<td>Allowed ranges for importing vulnerability data. Addresses may be a single IP address, IP range, CIDR block or any comma-delimited combination (20 K character limit).</td>
</tr>
<tr>
<td><strong>LCE Correlation</strong></td>
<td>Log Correlation Engine servers that will receive the vulnerability correlation information from this repository.</td>
</tr>
<tr>
<td><strong>Organizations</strong></td>
<td>Organizations that have access to the vulnerability data within the repository. Within the “Organizations” section, click the green key icon for access control options. Access is available for the “Organization Head” user or for “All Users” within the organization (affects existing users only). For existing repository edits, an additional option labeled “Existing Users” is available. This option leaves the current user access intact. Click on “Submit” to apply the changes.</td>
</tr>
</tbody>
</table>

**Remote Repository**
Remote repository synchronization is a feature of SecurityCenter 4.0 and greater; however, SecurityCenter 4.2 to 4.0 synchronization is not supported and will generate a license error.

Remote repositories are useful because they allow separate SecurityCenters to share repository data via a SSH session. The table below describes configurable fields for a remote repository:

### Table 8 – Remote Repository Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The repository name.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the repository.</td>
</tr>
<tr>
<td>Type</td>
<td>Remote</td>
</tr>
<tr>
<td>Remote Repository</td>
<td>Host to synchronize with to obtain the repository data.</td>
</tr>
<tr>
<td>Repository</td>
<td>Remote repository to collect IP address(es) and vulnerability data from.</td>
</tr>
</tbody>
</table>
| Trending          | If trending is not selected, any query that uses comparisons between repository snapshots (e.g., trending line charts) will not be available.  
This option allows for a periodic snapshot of the `.nessus` data for vulnerability trending purposes. This option is particularly useful in cases where trending is important. In situations where repository datasets do not change frequently – negating the need for trending – disable this option to minimize disk space usage. |
| Generate Nessus File | Use this option to schedule how frequently the Nessus file snapshot will be taken. Available options include: Never, Daily, Weekly, Monthly (Day) and Monthly (Date). The `.nessus` files generated by this process can be imported into Nessus scanners or any third-party tool that accepts the `.nessus` format as required. This option is not related to the “Sync Schedule” below, which relates to automating the synchronization of vulnerability data between SecurityCenters. |
| Sync Schedule     | Frequency with which the local and remote repositories are synchronized. Synchronization options include: “Never”, “Daily”, “Weekly”, “Monthly (Date)” and “Monthly (Day)”. |
IP Ranges

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed ranges for importing vulnerability data. Addresses may be a single IP address, IP range, CIDR block or any comma-delimited combination (20 K character limit).</td>
</tr>
</tbody>
</table>

Organizations

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizations that have access to the vulnerability data within the repository. Within the “Organizations” section, access control is available for the “Organization Head” user, “Existing Users” (editing existing repositories only) or for all users within the organization. Select the desired organization and then click on the illuminated “P” (Permissions) box to the right to bring up the applicable access control dialog. Click on “Submit” to apply the changes.</td>
</tr>
</tbody>
</table>

To share data, enter the IP address of the remote SecurityCenter in the “Host” field and click on “Retrieve Repositories”.

![Image of Remote Repository interface]

If a key for the current SecurityCenter has not been added to the remote SecurityCenter key list, the retrieve process will prompt for the SecurityCenter admin credentials of the remote host.

If the key authentication is not configured (System -> Keys), you will be prompted for the administrator username and password for the remote host. Repository IP addresses and vulnerability/event data is then retrieved from the remote SecurityCenter for use in the new one.

**Offline Repository**

Offline synchronization is a feature of SecurityCenter 4.0 and greater; however, SecurityCenter 4.2 to 4.0 synchronization is not supported and will generate a license error. SecurityCenter 4.0 to 4.2 synchronization will work, however.

Offline repositories are similar to remote repositories with the exception that data is synchronized manually using an archive file (.tar.gz) and not via network transmission. The table below describes configurable fields for an offline repository:

**Table 9 – Offline Repository Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The repository name</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Descriptive text for the repository</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Offline</td>
</tr>
<tr>
<td><strong>Trending</strong></td>
<td>If trending is not selected, any query that uses comparisons between repository snapshots (e.g., trending line charts) will not be available. This option allows for a periodic snapshot of the .nessus data for vulnerability trending purposes. This option is particularly useful in cases where trending is important. In situations where repository datasets do not change frequently – negating the need for trending – disable this option to minimize disk space usage.</td>
</tr>
<tr>
<td><strong>Generate Nessus File</strong></td>
<td>Use this option to schedule how frequently the Nessus file snapshot will be taken. Available options include: Never, Daily, Weekly, Monthly (Day) and Monthly (Date). The .nessus files generated by this process can be imported into Nessus scanners or any third-party tool that accepts the .nessus format as required.</td>
</tr>
<tr>
<td><strong>IP Ranges</strong></td>
<td>Allowed ranges for importing vulnerability data. Addresses may be a single IP address, IP range, CIDR block or any comma-delimited combination (20 K character limit).</td>
</tr>
<tr>
<td><strong>Organizations</strong></td>
<td>Organizations that have access to the vulnerability data within the repository. Within the “Organizations” section, access control is available for the “Organization Head” user, “Existing Users” (editing existing repositories only) or for all users within the organization. Select the desired organization and then click on the illuminated “P” (Permissions) box to the right to bring up the applicable access control dialog. Click on “Submit” to apply the changes.</td>
</tr>
</tbody>
</table>

To initiate offline repository synchronization, first download the repository archive from an existing repository by clicking on the “Download” link.
The option to open or save the archive file is presented.

⚠️ Depending on the size of the repository database, this file can be quite large. It is important to save the file to a location with plenty of free disk space.

⚠️ When importing the repository archive, the default maximum file import size is 150MB. This is specified by the “max file size” directive in `/opt/sc4/support/etc/php.ini`. Increase the default value if larger file uploads are required.

To load the repository archive to the offline repository, copy it to a location where the offline repository is accessible via the SecurityCenter GUI, open the “Repositories” page, highlight the offline repository and click on “Sync”.
Browse for the repository archive and click on “Submit” to load the offline repository archive file.

**ACCEPT RISK RULES**

Any non-admin user has the ability to accept a vulnerability risk by adding an “Accept Risk Rule”. Adding a rule moves vulnerabilities from the unfiltered cumulative database view. These vulnerabilities are not deleted, but only display in the cumulative database vulnerability view if the “Accepted Risk” filter option is checked. Once a risk has been accepted, the admin user can view the details of and delete the accept rules associated with the risk if they deem that the risk is still valid. This is accomplished by clicking on “Repositories” and then “Accept Risk Rules”. From there a list of available rules is displayed for the selected Plugin ID, Repository and Organization combination. Choose “All” for Repository and “Any” for Organization if plugin IDS are to be accepted across these boundaries. This is especially useful in setups where hundreds of repositories or organizations have been configured and the same accept risk rule must be applied globally.

Select the rule to be removed and click on “Details” to view the highlighted “Accept Risk Rule”. To remove the rule, click on “Delete” and a confirmation dialog is displayed that confirms if you really wish to delete the accepted risk rule:
After clicking on “Delete”, click on the “Apply Rules” button in the top left for the changes to take effect. Once completed, any vulnerabilities that had been modified by the accept risk rule are displayed unfiltered in the cumulative database.

**Recast Risk Rules**

Similar to “Accept Risk Rules”, “Recast Risk Rules” are rules that have been recast to a different risk level by a non-admin user. The admin user can display and delete these rules if desired. As with “Accept Risk Rules”, rules can be applied for a single plugin ID against a single repository/organization combination or globally. A screen capture of example “Recast Risk Rules” is shown below.

To view the rule details, click on “Details” to view the highlighted “Recast Risk Rule”. To remove the rule, click on “Delete”. A confirmation dialog is displayed and confirms that you really wish to delete the recasted risk rule:

After clicking on “Delete”, click on the “Apply Rules” button in the top left for the changes to take effect. Once completed, any vulnerabilities that had been modified by the recasted risk rule are returned to their original state.
USER MANAGEMENT

Organizations

Many of the concepts in this section such as zones, multiple organizations and repositories apply to the SecurityCenter only.

An organization is defined as a set of distinct users. These users are assigned repositories and “zones” within one or more specified IP networks. “Users” refers to any non-administrator login account on SecurityCenter. By “zone” we mean that each organization is made up of the systems within one or more IP networks.

Multiple organizations can share the same repository, if desired, and the vulnerability data associated with the overlapping ranges will be shared between each organization. Conversely, organizations can be configured with their own discrete repositories to facilitate situations where data must be kept confidential between different business units.

The organization is managed primarily by the Administrator and Organization Head users. The Administrator is responsible for organization and organization head creation and maintenance. Users within the organization are created by the Organization Head user or any user with the “Manage Users” permissions. User management is strictly hierarchical. For example, consider the diagram below:
In Organization A, the Org Head user has control over all users and managers in Organization A. Manager 1 similarly has control over all users and managers (except the Org Head user). Manager 2, however, only has control over users B through G since user A and Manager 1 are not in their hierarchy.

In Organization B, Manager 3 has control over all organizational users except for the Org Head user. We have created two users with custom roles. These custom roles have the “Manage Users” role and subsequently were able to create users H through J. Custom 1 has control over Custom 2 along with all users; however, Custom 2 only has control over users I and J.

It is important to consider these concepts when working with the built-in roles and creating custom ones as they relate to your organizational structure.

Creation of an Organization is a two-step process. The screen capture below contains two tabs: one for the actual organization detail entry and the second for creation of the Organization Head user.
The table below describes options required during the creation of an organization:

**Table 10 – Organization Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Organization name</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the organization.</td>
</tr>
<tr>
<td>Address</td>
<td>Organization address</td>
</tr>
<tr>
<td>City</td>
<td>Organization city</td>
</tr>
<tr>
<td>State</td>
<td>Organization state</td>
</tr>
<tr>
<td>Country</td>
<td>Organization country</td>
</tr>
<tr>
<td>Phone</td>
<td>Organizational telephone number</td>
</tr>
<tr>
<td><strong>Event Analysis Setup</strong></td>
<td></td>
</tr>
<tr>
<td>Accessible LCEs</td>
<td>LCE(s) to which this organization has access.</td>
</tr>
<tr>
<td><strong>Vulnerability Weights</strong></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>The vulnerability weighting to apply to “Low” criticality vulnerabilities for scoring purposes. (Default: 1)</td>
</tr>
</tbody>
</table>
### Medium
The vulnerability weighting to apply to “Medium” criticality vulnerabilities for scoring purposes. (Default: 3)

### High
The vulnerability weighting to apply to “High” criticality vulnerabilities for scoring purposes. (Default: 10)

### Critical
The vulnerability weighting to apply to “Critical” criticality vulnerabilities for scoring purposes. (Default: 40)

No vulnerabilities are assigned the “Critical” level by default; however, users can recast risks at this level based on corporate security policy or temporal factors.

---

**Scanning Setup**

**Repositories**
Repositories that the organization will have access to. Next to each repository checkbox is a key image that is used to determine repository access. Clicking on that image brings up the dialog below:

Choose “All Users” if all users within the organization will have access to the selected repository. Likewise, choose “Organization Head” if only the organization’s Organization Head will have access. Choose “Existing Users” to maintain the current user permissions (applicable when editing an existing organization).

**Restricted Scan Ranges**
IP Range(s) that the scanner will not scan (20 K character limit).

**Zone Selection**
Forced or Selectable. When in “selectable” mode, the user can select from the list of associated zones and choose one or more zones, or set the zone to default. When in “forced” mode, one zone will always be used for every scan.

**Zones**
Scan zones available to Nessus scanners.

---

**Custom IP Information Links**
Add New Custom Link

This tool allows the user to add a custom link within the host vulnerability details. Specify the desired link name and URI.

For example:

http://fakeuri.dom/index.html?ip=%ip%

The %ip% reference is a variable that inserts the IP address of the current host into the specified URI. In the example above, if the IP address of the host is 192.168.0.1, the link URI would be:

http://fakeuri.dom/index.htm?ip=192.168.0.1

This link is displayed under “Useful Links” from the Host Detail view (Vulnerabilities -> IP Summary -> Host Detail). Access the “Host Detail” view by clicking on the IP Address link on the IP Summary page.

This link is useful for organizations that want to reference an internal web page with IP specific information. For example, in many cases large organizations will have large numbers of hosts that analysts do not have specific knowledge about. This link could include organization-specific information about
the host in question, which could assist with vulnerability or event analysis.

The table below describes options required during the creation of an Organization Head:

**Table 11 – Organization Head Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Lock</strong></td>
<td>This command button gives the administrator the ability to lock or unlock the Organization Head user. When a user is locked, they are prevented from logging into their account until the administrator unlocks them.</td>
</tr>
</tbody>
</table>

**Authentication Information**

**Type – TNS**

<table>
<thead>
<tr>
<th>Username</th>
<th>Unique organizational login name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
<td>Organization Head password</td>
</tr>
</tbody>
</table>

**Type – LDAP**

| Search String        | This is the LDAP search string to use to narrow down user searches. Proper format is: “attribute=<filter text>”. Wildcards are permitted and the field accepts up to 1024 characters. For Example: sAMAccountName=*
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Users</strong></td>
<td>This box contains a list of users obtained from the configured LDAP server that match the Search String above.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>User that is selected from the list of users above.</td>
</tr>
</tbody>
</table>

**Notification**

| **Email user their account information** | Email the Organization Head their account information using the supplied email address. |

The username value is case-sensitive.
**Email user their password**  Email the Organization Head their password using the supplied email address.

**User must change their password on login**  Force the Organization Head to change their password on next login.

**Basic/Contact Information**

| Name, Title, Address Information, Email, Phone | Contact information for the Organization Head can be entered here. |

**USERS**

SecurityCenter administrators are configured via the “Users” tab. More than one administrator can be created per SecurityCenter.

**Administrators**

The administrative user can create other administrator users; however, they may only modify the “Basic” fields for the new user being created. “Access” and “Resources” tabs are displayed, but not editable for administrative users. All administrators have the same permission level and resources. The table below details fields from the “Basic” view:

**Table 12 – Basic Options for Adding Administrators**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Information</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Type – TNS</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **Username** | This is the account name the user will use to log in to SecurityCenter. When selecting this account name, it is sometimes easier to focus on the person’s real name as a convention (e.g., John Galt would become “jgalt”). However, it may also be useful to assign names based on role, such as “auditNY”.  

![Warning] The username value is case-sensitive. |
| **Password** | The login password  

![Warning] Please use complex and lengthy passwords based on your local security policy password requirements. |
| **Type – LDAP** |                                                                                                                                                   |
| **Search String** | This is the LDAP search string to use to narrow down user searches. Proper format is: “attribute=<filter text>”. Wildcards are permitted and the field accepts up to 1024 characters. For example:  
sAMAccountName=*  
mail=a*  
displayName=C* |
| **Users** | This box contains a list of users obtained from the configured LDAP server that match the Search String above. |
| **Username** | User that is selected from the list of users above. |

**Notification**

| **Email user their account information** | When the user is created, you can choose to have them notified via email of their account by selecting this check box.  
If the following error message is received when attempting to add a user:  
Error creating email notifying user 'test'. Invalid address: noreply@localhost  
Check the **System -> Configuration -> Mail -> Return Address** settings. The email address defaults to “noreply@localhost” if left blank. Many email servers will disallow emails from this address. |
| **Email user their password** | There is an option to include the user’s password within the email if desired. If this is not included, contact information of the security manager will be included. |
| **User must change their password on login** | Require password change on next login. |

**Basic/Contact Information**

| **Name, Title, Address Information, Email, Phone** | Contact information for the user can be entered here. |

**Roles**

| | Pre-defined roles cannot be edited. Use the admin or Organization Head user to create custom roles if customization is required. |
Roles determine what a user can or cannot do from their account. They are configurable to a great degree. SecurityCenter comes with five pre-defined roles; however, custom roles (SecurityCenter only) can be created by the “Organization Head” user to facilitate organizations with complex security policy needs. In keeping with the SecurityCenter convention, role assignments are hierarchical. Users may only assign permissions that they currently own. For example, if my user has a custom role with “View Vulnerability Data” enabled and “Update Plugins” disabled, I can only create users with “View Vulnerability Data” enabled.

Available pre-defined roles include:

- Administrator
- End User
- Manager
- No Role
- Organization Head

These roles are static and cannot be modified. An administrator is an account that has management responsibility over the console. The primary task of the administrator is to correctly install and configure each organization. In addition, the administrator adds components to SecurityCenter such as PVS, LCE and Nessus to extend its capability. The administrator is automatically assigned the “Manage Application” role.

An Organization Head is the account within an organization that has a broad range of security roles within the defined organization. This is the initial user that is created when a new organization is created. They have the ability to launch scans, configure users (except for the administrator user), vulnerability policies and other objects belonging to their organization. Each organization has an **Organization Head** account that cannot be deleted. Permission-wise, the Organization Head user is nearly identical to the Manager user, however there are differences:

1. The Organization Head can add/edit/delete roles, while the Manager cannot.
2. The Organization Head can add users that are the subordinate of any manager or user with the “Manage Users” permission. The manager can only add users as a subordinate of themselves.
3. The Organization Head has visibility of scan schedules and report definitions for the entire organization, while the manager can only see those of his/her subordinate.

Additional users may be created and assigned either one of three possible roles or a custom one. These roles are “Manager”, “End User” and “No Role”.

The “Manager” role is intended for security team managers who have the need to manage end-user objects along with vulnerability, resource and scans. The manager user is very similar in capability to the Organization Head user except that they cannot manage roles and cannot manage objects not in their hierarchy (all organizational users are in the Organization Head’s hierarchy).

An end-user is a system administrator, network engineer or auditor. They use their account to review their security data, create and view reports, enter in their remediation actions to close tickets and if given proper credentials, launch scans.
“No Role” is the default “catch-all” role for users or objects for which no role has been assigned or explicit roles have been removed.

User Visibility
An important concept of SecurityCenter 4 is that of “Visibility”. Objects can have one of four possible visibilities.

The table below describes each of the available visibility options:

Table 13 – Visibility Options

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Objects created by an organizational user are created by default with <strong>User</strong> visibility and are available only to their creator. To allow an object to be used by another user, it must be created with organizational visibility or explicitly shared with one or more users.</td>
</tr>
<tr>
<td>Organizational</td>
<td>Objects created with <strong>Organizational</strong> visibility are available to any user within the current organization. They are indicated by the following icon: [icon]</td>
</tr>
<tr>
<td>Application</td>
<td>Objects created with <strong>Application</strong> visibility are available to any user within any organization on SecurityCenter. They are indicated by the following icon: [icon]</td>
</tr>
<tr>
<td></td>
<td>Objects created by the administrator user automatically inherit <strong>Application</strong> visibility and cannot be shared (since they are already available to all organizational users).</td>
</tr>
<tr>
<td></td>
<td>Only administrators can create objects with this visibility.</td>
</tr>
<tr>
<td>Shared</td>
<td>Objects created with <strong>User</strong> or <strong>Organizational</strong> visibility can be converted to <strong>Shared</strong> visibility after being shared by a user with the required permissions. They are indicated by the following icon: [icon]</td>
</tr>
<tr>
<td></td>
<td>If you edit an object that has a shared visibility, you have the option to change it to <strong>User</strong> visibility, which would remove all existing shares. In addition, if an object is unshared from everyone it reverts to user visibility.</td>
</tr>
</tbody>
</table>

User Access Control
Within the defined user roles, granular permissions are applied that enable users to perform various tasks. Custom roles can also be created with any combination of desired permissions based on enterprise needs.

Role permissions are broken down based on user visibility. In all cases except policy roles, an “Organizational” designation indicates that the user with that role can create objects with
either “User” or “Organizational” visibility. In the case of scan policy creation, users with the “Create Policies” permission can only create policies with “User” visibility. Users with “Create Organizational Policies” and “Create Policies” permissions can create policies with either “User” or “Organizational” visibility. Users with only the “Create Organizational Policies” permission cannot create any scan policies.

The table below defines the various permissions available within the SecurityCenter architecture:

**Table 14 – Available Permissions**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
<th>Organization Head</th>
<th>Administrator</th>
<th>Manager</th>
<th>End User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept Risks</td>
<td>Accept the risk of vulnerabilities</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Alerts</td>
<td>Create custom alerts</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Create Audit Files</td>
<td>Upload custom audit files</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Create Application Roles</td>
<td>Create roles with application visibility. This is not a configurable role.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Organization Roles</td>
<td>Create roles with organizational visibility. This is not a configurable role.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Organization Assets</td>
<td>Create assets</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Create Organization Credentials</td>
<td>Create credentials</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Create Organization Policies</td>
<td>Create scan policies with organizational visibility. This option must be used in conjunction with the “Create Policies” permission.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Create Organization Queries</td>
<td>Create queries</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Create Policies</td>
<td>Create scan policies with “User” visibility.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

This option must be set for the “Create”
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Create Tickets</th>
<th>Edit/Delete Organization Assets</th>
<th>Edit/Delete Organization Credentials</th>
<th>Edit/Delete Organization Policy</th>
<th>Edit/Delete Organization Query</th>
<th>Manage Applications</th>
<th>Manage Users</th>
<th>Purge Tickets</th>
<th>Recast Risk</th>
<th>Scan Privileges</th>
<th>Share Assets</th>
<th>Share Credentials</th>
<th>Share Dashboard Tabs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Policies” option to function.</td>
<td>Use this option for users who will create policies for themselves, but, not shared policies. This can be useful for new users.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Tickets</td>
<td>Create tickets</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit/Delete Organization Assets</td>
<td>Edit or delete assets belonging to the user’s organization regardless of what organizational user created it.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit/Delete Organization Credentials</td>
<td>Edit or delete credentials belonging to the user’s organization regardless of what organizational user created it.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit/Delete Organization Policy</td>
<td>Edit or delete policies belonging to the user’s organization regardless of what organizational user created it.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit/Delete Organization Query</td>
<td>Edit or delete queries belonging to the user’s organization regardless of what organizational user created it.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Applications</td>
<td>Manage SecurityCenter applications and services. Any role with the “Manage Applications” permission is non-editable. The permission column is removed.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manage Users</td>
<td>Manage non-administrative users.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purge Tickets</td>
<td>Purge tickets</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recast Risk</td>
<td>Recast the risk of vulnerabilities.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scan Privileges</td>
<td>Perform Nessus scans.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Share Assets</td>
<td>Share assets with other users.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Share Credentials</td>
<td>Share credentials with other users.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Share Dashboard Tabs</td>
<td>Share dashboard tabs with other users.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Description</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Share Policies</td>
<td>Share policies with other users.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Share Queries</td>
<td>Share queries with other users.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Update Plugins</td>
<td>Update Active, Passive and Custom plugins.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upload Nessus Scan Results</td>
<td>Upload Nessus scan results.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Event Data</td>
<td>View event data.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Organization Logs</td>
<td>View organization logs.</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Raw Logs</td>
<td>View raw logs.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Vulnerability Data</td>
<td>View vulnerabilities within the organizational repository.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SCAN MANAGEMENT**

**Support**

**Audit Files**

The Nessus vulnerability scanner includes the ability to perform compliance audits of numerous platforms including databases, Cisco, Unix and Windows configurations as well as sensitive data discovery based on regex contained in "audit" files. Audit files are XML-based text files that contain the specific configuration, file permission and access control tests to be performed.

Tenable provides a wide range of "audit" files and new ones are easy to write. These "audit" files are maintained on the Tenable Support Portal for users who wish to perform compliance and configuration auditing. The screen capture below contains a listing of an audit file page with some more commonly used audits.

Audit files are added, edited, viewed and deleted from this web interface. Clicking on “Add” displays the following add dialog screen:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Owner</th>
<th>Version</th>
<th>Visibility</th>
<th>Modified Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flake</td>
<td>Windows</td>
<td>Administrator</td>
<td>2</td>
<td>Application</td>
<td>4 days ago</td>
</tr>
<tr>
<td>PH4</td>
<td>Unix</td>
<td>Administrator</td>
<td>1</td>
<td>Application</td>
<td>Mar 1, 2010 15:14</td>
</tr>
</tbody>
</table>
Available fields include:

**Table 15 – Audit File Fields**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A descriptive name assigned to the audit file (not necessarily the actual file name)</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text about the audit file</td>
</tr>
<tr>
<td>File</td>
<td>An interface that allows you to browse on your local system for the audit file</td>
</tr>
</tbody>
</table>

Once an audit file has been uploaded, it can be referenced from within scan policies for enhanced security policy auditing. For more information about SecurityCenter compliance auditing and `.audit` files, refer to the Nessus Compliance Checks documents located at [https://support.tenable.com/support-center/](https://support.tenable.com/support-center/).

**Credentials**

Credentials are reusable objects that facilitate scan target login. Credentials created by the admin user are available to all organizations, while those created by organizational users are only available to the applicable organization. Various types of credentials can be configured for use in scan policies. Credentials can be shared between users for scanning purposes and allow the user to scan a remote host without actually knowing the login credentials of the host. Available credential types include:

- Windows – Nessus has vulnerability checks that can use a Microsoft Windows domain account to find local information from a remote Windows host. For example, using credentials enables Nessus to determine if important security patches have been
applied. To use this feature, enter the Username, Password and Domain in the text boxes.

Using a non-administrator account will greatly affect the quality of the scan results. Often it makes sense to create a special Nessus user with administrative privileges that is used solely for scheduled scanning.

SSH (password with optional privilege escalation and key-based) – SSH credentials are used to obtain local information from remote Unix and Cisco IOS systems for patch auditing or compliance checks. There is a field for entering the SSH user name for the account that will perform the checks on the target system, along with either the SSH password or the SSH public key and private key pair. There is also a field for entering the Passphrase for the SSH key, if it is required. In case of invalid or expired SSH keys use the “Clear” button to remove the current SSH keys.

The most effective credentialed scans are those with “root” privileges (“enable” privileges for Cisco IOS). Since many sites do not permit a remote login as root, a Nessus user account can invoke a variety of privilege escalation options including: "su", "sudo", "su+sudo" and “enable”.

Scans run using “su+sudo” allow the user to scan with a non-privileged account and then switch to a user with “sudo” privileges on the remote host. This is important for locations where remote privileged login is prohibited.

Scans run using “sudo” vs. the root user do not always return the same results because of the different environmental variables applied to the “sudo” user and other subtle differences. Please refer to the “sudo” man pages or the following web page for more information:
http://www.gratisoft.us/sudo/man/sudo.htm#Security%20Notes

To direct the Nessus scanner to use privilege escalation, click on the drop-down menu labeled “Privilege Escalation” and select the appropriate option for your target system. Enter the escalation information in the provided box.

If an SSH known_hosts file is available and provided as part of the scan policy (located within the SSH Settings in the scan policy preferences), Nessus will only attempt to log in to hosts in this file. This ensures that the same username and password used to audit your known SSH servers is not used to attempt a login to a system that may not be under your control.

SNMP community string – Enter the SNMP community string used for authentication.

Kerberos – The Kerberos IP, Port, Protocol and Realm are available for this type of authentication.

An example Windows credential with options is displayed below:
Scan Policies

The scan policy contains plugin settings and advanced directives used during the course of the Nessus scan. Scan policies created by the admin user are available to all organizations configured on the SecurityCenter. Click on “Support” and then “Scan Policies” to display a listing of all currently available policies. Tabs at the upper-right hand portion of this page give the user the ability to Add, Copy, Edit, Share, Details (view details of) and Delete existing policies.

Add a Scan Policy
Clicking on “Add” opens the following screen that is used to configure the new scan policy. Four tabs are displayed including:

- Basic
- Audit Files
Basic

The Basic tab contains basic scan policy settings and allows the user to load a predefined scan policy template if desired. The “Load Policy Template” option is a command button located in the upper right-hand corner of the “Basic” tab page and allows the user to load scan policy options based on a variety of predefined scan policy templates. Available templates include: “Web Safe Scan”, “FTP Safe Scan”, “SMTP Safe Scan”, “Cisco Safe Scan”, “Full Safe Scan – All Ports”, “Full Safe Scan – Common Ports”, “Microsoft Scan”, “PCI DSS Scan”, “Topology Scan”, “Peer-To-Peer Scan”, “Virus Check Scan”, “Operating System Identification”, “Patch Audit and Local Security Checks” and “Netstat Port Scan”. These templates use optimized plugin and configuration settings for their specified scan type.

The tables below contain detailed descriptions of options available on each of the five frames displayed under the “Basic” tab:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique policy name</td>
</tr>
<tr>
<td>Description</td>
<td>Policy description (optional)</td>
</tr>
<tr>
<td>Group</td>
<td>Policy group name (optional)</td>
</tr>
<tr>
<td>Type</td>
<td>Family or Plugin. If “Family” is chosen, then when plugin updates occur, new plugins will automatically be enabled for plugin families that are enabled. If “Plugin” is enabled, only the currently enabled plugins are enabled. New plugins must</td>
</tr>
</tbody>
</table>
be manually enabled by the user. This is beneficial where strict control over new plugins is required.

Changing from “Family” to “Plugin”, or vice-versa, clears all currently enabled plugins. Please make a note of all enabled plugins before changing this option so that they can be enabled afterwards.

The “Scan” frame controls basic scan options for the scan:

**Table 17 – Scan Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe Checks</td>
<td>Nessus can attempt to identify remote vulnerabilities by interpreting banner information and attempting to exercise a vulnerability. When “Safe Checks” is enabled, the second step is skipped. This is not as reliable as a full probe, but is less likely to negatively impact a targeted system.</td>
</tr>
<tr>
<td>Silent Dependencies</td>
<td>If this option is checked, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, uncheck the box.</td>
</tr>
<tr>
<td>Consider Unscanned Ports as Closed</td>
<td>With this setting enabled, ports that are not enumerated by the port scan will not be tested. For example, scanning ports 21, 22 and 23 will only test those ports and not any other port.</td>
</tr>
</tbody>
</table>

The “Port Scanners” frame controls which methods of port scanning should be enabled for the scan:

**Table 18 – Port Scanner Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP Scan</td>
<td>Use Nessus’ built-in TCP scanner to identify open TCP ports on the targets. This scanner is optimized and has some self-tuning features.</td>
</tr>
<tr>
<td></td>
<td>On some platforms (e.g., Windows and Mac OS X), if the operating system is causing serious performance issues using the TCP scanner, Nessus will launch the SYN scanner instead.</td>
</tr>
<tr>
<td>UDP Scan</td>
<td>This option engages Nessus’ built-in UDP scanner to identify open UDP ports on the targets.</td>
</tr>
</tbody>
</table>
UDP is a “stateless” protocol, meaning that communication is not done with handshake dialogues. UDP based communication is not reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.

**SYN Scan**

Use Nessus’ built-in SYN scanner to identify open TCP ports on the targets. SYN scans are a popular method for conducting port scans and generally considered to be a bit less intrusive than TCP scans. The scanner sends a SYN packet to the port, waits for SYN-ACK reply and determines port state based on a reply – or lack of.

**SNMP Scan**

Direct Nessus to scan targets for a SNMP service. Nessus will guess relevant SNMP settings during a scan. If the settings are provided by the user under “Preferences”, this will allow Nessus to better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.

**Netstat SSH Scan**

This option uses `netstat` to check for open ports on the target host. It relies on the `netstat` command being available via a SSH connection to the target. This scan is intended for Unix-based systems and requires authentication credentials.

**Netstat WMI Scan**

This option uses `netstat` to check for open ports from the local machine. It relies on the `netstat` command being available via a WMI connection to the target. This scan is intended for Windows-based systems and requires authentication credentials.

**Ping Host**

This option enables the pinging of remote hosts to determine if they are alive.

This option is not recommended when scanning between virtual hosts on the same system.

The “**Port Scan Options**” frame directs the scanner to target a specific range of ports. The following values are allowed for the “Port Scan Range” option:

**Table 19 – Values for Port Scan Options**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“default”</td>
<td>Using the keyword “default”, Nessus will scan approximately 4,789 common ports (found in the <code>nessus-services</code> file).</td>
</tr>
</tbody>
</table>
Using the keyword “all”, Nessus will scan all 65,535 ports.

**Custom List**
A custom range of ports can be selected by using a comma delimited list of ports or port ranges. For example, “21,23,25,80,110” or “1-1024,8080,9000-9200” are allowed. Specifying “1-65535” will scan all ports.

The range specified for a port scan will be applied to both TCP and UDP scans.

The **Performance** frame provides two options that control how many scans will be launched. These options are perhaps the most important when configuring a scan as they have the biggest impact on scan times and network activity.

**Table 20 – Performance Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max Checks Per Host</td>
<td>This setting limits the maximum number of checks a Nessus scanner will perform against a single host at one time.</td>
</tr>
<tr>
<td>Max Hosts Per Scan</td>
<td>This setting limits the maximum number of hosts that a Nessus scanner will scan at the same time.</td>
</tr>
<tr>
<td>Max Scan Time (hours)</td>
<td>This setting limits the length of time a scan is allowed to run. If a scan reaches this limit, the unscanned targets are captured in a new “rollover” scan that can be run manually or scheduled at a later time.</td>
</tr>
<tr>
<td>Max TCP Connections</td>
<td>This setting limits the maximum number of established TCP sessions for a single host.</td>
</tr>
</tbody>
</table>

**Audit Files**
The **Audit Files** tab contains two options related to Nessus compliance scans. Note that you must at least name the scan from the “Basic” frame to be able to open the “Audit Files” tab.

**Table 21 – Audit File Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Audit File</td>
<td>Tenable provides a variety of .audit files that provide a template check for compliance audits against various established standards, such as the Center for Internet Security (CIS) benchmarks, healthcare industry standards (HIPAA), Payment Card Industry (PCI) requirements and many more. To perform a compliance check, you must have the ability to perform authenticated Unix and/or Windows local checks.</td>
</tr>
</tbody>
</table>
**Perform PCI DSS Analysis**

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of security standards established by the founding members of the PCI Security Standards Council, including Visa, American Express, Discover Financial Services and MasterCard. The PCI DSS is intended to provide a common baseline to safeguard sensitive cardholder data for all bankcard brands and is in use by many e-commerce vendors who accept and store credit card data.

Tenable provides three plugins to all SecurityCenter users that automate the process of performing a PCI-DSS audit. These plugins are:

- PCI DSS compliance: tests requirements
- PCI DSS compliance: passed
- PCI DSS compliance

These plugins evaluate the results of your scan and the actual configuration of your scan to determine if the target server is PCI compliant. The plugins do not perform actual scanning; they just look at the results from other plugins.

To activate the PCI DSS plugins, simply check the box labeled “Perform PCI DSS Analysis” from the “Compliance” screen.

---

**Plugins**

The **Plugins** tab gives the user the option to customize which plugins are used during the policy’s Nessus scan.

---

It is important to note that a secure infrastructure is achieved through a fusion of people, processes and technology. Tenable’s solutions provide the technology to aid in compliance requirements and are intended to be used in conjunction with a comprehensive security strategy. Please consult with your organization’s Audit and Compliance group for guidance and directives specific to your organization.
Clicking on the circle next to a plugin family allows you to enable or disable the entire family. When the circle next to a family is yellow, that family and all plugins within that family are enabled. Selecting a family will display the list of its plugins in the upper right pane. Individual plugins can be enabled or disabled to create very specific scan policies. As adjustments are made, the total number of families and plugins selected is displayed at the bottom. If the circle next to a plugin family is half grey and half yellow, it denotes that some, but not all, of the plugins are enabled.

Selecting a specific plugin will display the plugin output that will be displayed as seen in a report. The synopsis and description will provide more details of the vulnerability being examined. Scrolling down in the “Plugin Description” pane will also show solution
information, additional references if available and the CVSSv2 score that provides a basic risk rating.

When a policy is created and saved, it records all of the plugins that are initially selected. When new plugins are received via a plugin feed update, they will automatically be enabled if the family they are associated with is enabled. If the family has been disabled or partially enabled, new plugins in that family will automatically be disabled as well.

The “Denial of Service” family contains some plugins that could cause outages on a corporate network if the “Safe Checks” option is not enabled, but does contain some useful checks that will not cause any harm. The “Denial of Service” family can be used in conjunction with “Safe Checks” to ensure that any potentially dangerous plugins are not run. However, it is recommended that the “Denial of Service” family not be used on a production network.

The following table describes options that will assist you in selecting plugins.

Table 22 – Plugin Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plugin Filters</td>
<td>Display plugins based on selected parameters (Name, ID, and Family). Select the parameter you wish to search and type in some text to look for and hit Enter.</td>
</tr>
<tr>
<td>Show Only Enabled</td>
<td>Select this checkbox to only show currently enabled plugins.</td>
</tr>
<tr>
<td>Enable All Plugins</td>
<td>Enable all available plugins.</td>
</tr>
<tr>
<td>Disable All Plugins</td>
<td>Disable all available plugins.</td>
</tr>
</tbody>
</table>

Preferences
The “Preferences” tab includes means for granular control over scan settings. Selecting an item from the drop-down menu will display further configuration items for the selected category. Note that this is a dynamic list of configuration options that is dependent on the plugin feed, audit policies and additional functionality that the connected Nessus scanner has access to. This list may also change as plugins are added or modified.

If a secure method of performing credentialed checks is not available, users can force Nessus to try to perform checks over insecure protocols by configuring the Cleartext protocol settings (plugin 21744) drop-down menu item. The cleartext protocols supported for this option are telnet, rsh and rexec.
The **Database settings** (plugin 33815) options apply to database compliance audits and are used to specify the type of database to be tested, relevant settings and credentials:

![Database settings plugin](image)

### Table 23 – Database Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>The username for the database.</td>
</tr>
<tr>
<td>Password</td>
<td>The password for the supplied username.</td>
</tr>
<tr>
<td>DB Type</td>
<td>Oracle, SQL Server, MySQL, DB2, Informix/DRDA and PostgreSQL are supported.</td>
</tr>
<tr>
<td>Database SID</td>
<td>Database system ID to audit (Oracle only).</td>
</tr>
<tr>
<td>Database port to use</td>
<td>Port the database listens on. This is useful where the database is configured to listen on a non-standard port. If this field is not specified, the default port for the chosen database is used:</td>
</tr>
</tbody>
</table>
> Oracle: 1521  
> MySQL: 3306  
> SQL Server: 1433  
> Informix: 1526  
> DB2: 50000

**Oracle auth type**

NORMAL, SYSOPER and SYSDBA are supported. Depending on the privileges required by the .audit commands, enhanced privileges such as "SYSOPER" or "SYSDBA" may be required. In most cases, however, the "NORMAL" auth type will suffice.

**SQL Server auth type**

Windows or SQL are supported.

Do not scan fragile devices (plugin 22481) instructs the Nessus scanner not to scan network printers or Novell Netware hosts if selected. Since both of these technologies are more prone to denial of service conditions, Nessus can skip scanning them. This is recommended if scanning is performed during business hours.

Global variable settings (plugin 12288) contains a wide variety of configuration options for the Nessus server.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Probe services on every port</strong></td>
<td>Attempts to map each open port with the service that is running on that port. Note that in some rare cases, this might disrupt some services and cause unforeseen side effects.</td>
</tr>
<tr>
<td><strong>Do not log in with user accounts not specified in the policy</strong></td>
<td>Used to prevent account lockouts if your password policy is set to lock out accounts after several invalid attempts.</td>
</tr>
<tr>
<td><strong>Enable CGI scanning</strong></td>
<td>Activates CGI checking. Disabling this option will tremendously speed up the audit of a local network. This option must be enabled in conjunction with the web application testing plugin for a full web audit to occur.</td>
</tr>
<tr>
<td><strong>Network type</strong></td>
<td>Allows you to specify if you are using public routable IPs, private non-internet routable IPs or a mix of these. Select “Mixed” if you are using RFC 1918 addresses and have multiple routers within your network.</td>
</tr>
<tr>
<td><strong>Enable experimental scripts</strong></td>
<td>Causes plugins that are considered experimental to be used in the scan. Do not enable this setting while scanning a production network.</td>
</tr>
<tr>
<td></td>
<td>Tenable does not release scripts flagged “experimental” in either plugin feed.</td>
</tr>
<tr>
<td><strong>Thorough tests (slow)</strong></td>
<td>Causes various plugins to “work harder”. For example, when looking through SMB file shares, a plugin can analyze 3 levels deep instead of 1. This could cause much more network traffic and analysis in some cases. Note that by being more thorough, the scan will be more intrusive and is more likely to disrupt the network, while potentially having better audit results. For more information about “thorough tests” see this blog entry.</td>
</tr>
<tr>
<td><strong>Report verbosity</strong></td>
<td>A higher setting will provide more information in the report.</td>
</tr>
<tr>
<td><strong>Report paranoia</strong></td>
<td>In some cases, Nessus cannot remotely determine whether a flaw is present or not. If the report paranoia is set to “Paranoid” then a flaw will be reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of “Avoid false alarm” will cause Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. The default option (“Normal”) will be a middle ground between these two settings.</td>
</tr>
<tr>
<td><strong>HTTP User-Agent</strong></td>
<td>Specifies which type of web browser Nessus will impersonate while scanning.</td>
</tr>
</tbody>
</table>
SSL certificate to use | Allows Nessus to use a client side SSL certificate for communicating with a remote host.
---|---
SSL CA to trust | Specifies a Certificate Authority (CA) that Nessus will trust.
SSL key to use | Specifies a local SSL key to use for communicating with the remote host.
SSL password for SSL key | The password for managing the SSL key specified.

To facilitate web application testing, Nessus can import HTTP cookies from another piece of software (e.g., web browser, web proxy, etc.) with the **HTTP cookies import** (plugin 42893) settings. A cookie file can be uploaded so that Nessus uses the cookies when attempting to access a web application. The cookie file must be in Netscape format.

The **HTTP login page** (plugin 11149) settings provide control over where authenticated testing of a custom web-based application begins. See this blog entry for more details about configuring web applications that require authentication.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login page</td>
<td>The base URL to the login page of the application.</td>
</tr>
</tbody>
</table>
### Login form

The “action” parameter for the form method. For example, the login form for `<form method="POST" name="auth_form" action="/login.php">` would be `"/login.php"`.  

This option is not required if the “Automated login page search” option specified below is used.

### Login form fields

Specify the authentication parameters (e.g., `login=%USER%&password=%PASS%`). If the keywords %USER% and %PASS% are used, they will be substituted with values supplied on the “Login configurations” drop-down menu.  

This option is not required if the “Automated login page search” option specified below is used.

### Login form method

Specify POST or GET based on the login form requirements.  

This option is not required if the “Automated login page search” option specified below is used.

### Automated login page search

Gives Nessus the option to parse the login page for form options and attempt to login based on detected fields. This option works in conjunction with the HTTP cookies import (plugin 42893) to simplify form-based authentication.

If more than one form is available on a web page (uncommon), use the manual login form parameters specified above instead.

### Re-authenticate delay (seconds)

The time delay between authentication attempts. This is useful to avoid triggering brute force lockout mechanisms.

### Check authentication on page

The URL of a protected web page that requires authentication, to better assist Nessus in determining authentication status.

### Follow 30x redirections (# of levels)

If a 30x redirect code is received from a web server, this directs Nessus to follow the link provided or not.

### Authenticated regex

A regex pattern to look for on the login page. Simply receiving a 200 response code is not always sufficient to determine session state. Nessus can attempt to match a given string such as “Authentication successful!”

### Invert test (disconnected if regex matches)

A regex pattern to look for on the login page, that if found, tells Nessus authentication was not successful (e.g., “Authentication failed!”).
**Match regex on HTTP headers**
Rather than search the body of a response, Nessus can search the HTTP response headers for a given regex pattern to better determine authentication state.

**Case insensitive regex**
The regex searches are case sensitive by default. This instructs Nessus to ignore case.

The **ICCP/COTP TSAP Addressing** (plugin 23812) menu deals specifically with SCADA checks. It determines a Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values. The start and stop values are set to “8” by default.

**Login configurations** (plugin 10870) allows the Nessus scanner to use credentials when testing HTTP, NNTP, FTP, POP2, POP3 or IMAP. By supplying credentials, Nessus may have the ability to do more extensive checks to determine vulnerabilities. HTTP credentials supplied here will be used for Basic and Digest authentication only. For configuring credentials for a custom web application (e.g., form-based login), use the “HTTP login page” pull-down menu. Two checkboxes are available on this page, “Never send SMB credentials in clear text” and “Only use NTLMv2”. Both of these settings affect the security of credentials sent out during Nessus scans.

Using cleartext credentials in any fashion is **not** recommended! If the credentials are sent remotely, via a Nessus scan or e-mailing a policy to another administrator, the credentials could be intercepted by anyone with access to the network. Use encrypted authentication mechanisms whenever possible.
The **Modbus/TCP Coil Access** (plugin 23817) drop-down menu item is dynamically generated by the SCADA plugins available with the ProfessionalFeed. Modbus uses a function code of 1 to read “coils” in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a “write coil” message. The defaults for this are “0” for the “Start reg” and “16” for the “End reg”.

**Nessus SYN scanner** (plugin 11219) and **Nessus TCP scanner** (plugin 10335) options allow you to better tune the native SYN and TCP scanner to detect the presence of a firewall.

**Table 26 – Nessus SYN and TCP Scanner Settings**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Automatic (normal)</strong></td>
<td>This option can help identify if a firewall is located between the scanner and the target <em>(default)</em>.</td>
</tr>
<tr>
<td><strong>Disabled (softer)</strong></td>
<td>Disables the <strong>Firewall detection</strong> feature.</td>
</tr>
</tbody>
</table>
Do not detect RST rate limitation (soft) | Disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device.

Ignore closed ports (aggressive) | Will attempt to run plugins even if the port appears to be closed. It is recommended that this option not be used on a production network.

**News Server (NNTP) Information Disclosure** (plugin 11033) can be used to determine if there are news servers that are able to relay spam. Nessus will attempt to post a news message to a NNTP (Network News Transport Protocol) server(s), and can test if it is possible to post a message to upstream news servers as well.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From address</strong></td>
<td>The address that Nessus will use as it attempts to post a message to the news server(s). This message will delete itself automatically after a short period of time.</td>
</tr>
<tr>
<td><strong>Test group name regex</strong></td>
<td>The name of the news group(s) that will receive a test message from the specified address. The name can be specified as a regular expression (regex) so that the message can be posted to multiple news groups simultaneously. For example, the default value “f[a-z]\tests?” will broadcast a mail message to all news groups with names that begin with any letter (from “a” to “z”) and end with “.tests” (or some variation that matched the string). The question mark acts as an optional wildcard.</td>
</tr>
<tr>
<td><strong>Max crosspost</strong></td>
<td>The maximum number of news servers that will receive the test posting, regardless of the number of name matches. For example, if the Max crosspost is “7”, the test message will only be sent to seven news servers, even if there are 2000 news servers that match the regex in this field.</td>
</tr>
<tr>
<td><strong>Local distribution</strong></td>
<td>If this option is selected, Nessus will only attempt to post a message to the local news server(s). Otherwise, an attempt will be made to forward the message upstream.</td>
</tr>
</tbody>
</table>

---

**Table 27 – News Server (NNTP) Information Disclosure Settings**

---

Copyright © 2002-2012 Tenable Network Security, Inc. 64
No archive

If this option is selected, Nessus will request to not archive the test message being sent to the news server(s). Otherwise, the message will be archived like any other posting.

Oracle settings (plugin 22076) allows the user to enter the Oracle database SID to specify which database to test. In addition, “Test default accounts (slow)” enables the Nessus scan to probe for default accounts within the remote database for vulnerabilities.

Ping the remote host (plugin 10180) options allow for granular control over Nessus’ ability to ping hosts during discovery scanning. This can be done via ARP ping, TCP ping, ICMP ping or applicative UDP ping.

Table 28 – Ping the Remote Host Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP ping destination port(s)</td>
<td>Specifies the list of ports that will be checked via TCP ping. If you are not sure of the ports, leave this setting to the default of “built-in”.</td>
</tr>
<tr>
<td>Do an ARP ping</td>
<td>Utilize the ARP protocol for pings.</td>
</tr>
<tr>
<td>Do a TCP ping</td>
<td>Utilize the TCP protocol for pings.</td>
</tr>
<tr>
<td>Do an ICMP ping</td>
<td>Utilize the ICMP protocol for pings.</td>
</tr>
<tr>
<td>Number of Retries (ICMP)&quot;</td>
<td>Allows you to specify the number of attempts to try to ping the remote host. The default is set to 2.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Do an applicative UDP ping (DNS, RPC...)</td>
<td>Perform a UDP ping against specific UDP-based applications including DNS (port 53), RPC (port 111), NTP (port 123) and RIP (port 520).</td>
</tr>
<tr>
<td>Make the dead hosts appear in the report</td>
<td>If this option is selected, hosts that did not reply to the ping request will be included in the security report as dead hosts.</td>
</tr>
<tr>
<td>Log live hosts in the report</td>
<td>Select this option to specifically report on the ability to successfully ping a remote host.</td>
</tr>
<tr>
<td>Test the local Nessus host</td>
<td>This option allows you to include or exclude the local Nessus host from the scan. This is used when the Nessus host falls within the target network range for the scan.</td>
</tr>
<tr>
<td>Fast network discovery</td>
<td>By default, when Nessus “pings” a remote IP and receives a reply, it performs extra checks to make sure that it is not a transparent proxy or a load balancer that would return noise but no result (some devices answer to every port 1-65535 but there is no service behind). Such checks can take some time, especially if the remote host is firewalled. If the “fast network discovery” option is enabled, Nessus will not perform these checks.</td>
</tr>
</tbody>
</table>

Port scanner settings (plugin 33812) provide two options for further controlling port scanning activity:

**Table 29 – Port Scanner Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check open TCP ports found by local port enumerators</td>
<td>If a local port enumerator (e.g., WMI or <code>netstat</code>) finds a port, Nessus will also verify it is open remotely. This helps determine if some form of access control is being used (e.g., TCP wrappers, firewall).</td>
</tr>
<tr>
<td>Only run network port scanners if local port enumeration failed</td>
<td>Rely on local port enumeration.</td>
</tr>
</tbody>
</table>

**SMB Registry: Start the Registry Service during the scan** (plugin 35703) enables the service to facilitate some of the scanning requirements for machines that may not have the “Remote Registry” service running all the time.

Under the **SMB Scope** (plugin 10917) menu, if the option “**Request information about the domain**” is set, then domain users will be queried instead of local users.

**SMB use domain SID to enumerate users** (plugin 10399) specifies the SID range to use to perform a reverse lookup on usernames on the domain. The default setting (1000 to 1200) is recommended for most scans.

**SMB use host SID to enumerate local users** (plugin 10860) specifies the SID range to use to perform a reverse lookup on local usernames. The default setting (1000 to 1200) is recommended for most scans.
**SMTP settings** (plugin 11038) specify options for SMTP (Simple Mail Transport Protocol) tests that run on all devices within the scanned domain that are running SMTP services. Nessus will attempt to relay messages through the device to the specified “**Third party domain**”. If the message sent to the “**Third party domain**” is rejected by the address specified in the “**To address**” field, the spam attempt failed. If the message is accepted, then the SMTP server was successfully used to relay spam.

![SMTP settings plugin 11038](image)

### Table 30 – SMTP Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Third party domain</strong></td>
<td>Nessus will attempt to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test might be aborted by the SMTP server.</td>
</tr>
<tr>
<td><strong>From address</strong></td>
<td>The test messages sent to the SMTP server(s) will appear as if they originated from the address specified in this field.</td>
</tr>
<tr>
<td><strong>To address</strong></td>
<td>Nessus will attempt to send messages addressed to the mail recipient listed in this field. The <strong>postmaster</strong> address is the default value since it is a valid address on most mail servers.</td>
</tr>
</tbody>
</table>

**SNMP settings** (plugin 19762) allow you to configure Nessus to connect and authenticate to the SNMP service of the target. During the course of scanning, Nessus will make some attempts to guess the community string and use it for subsequent tests. If Nessus is unable to guess the community string and/or password, it may not perform a full audit against the service.
### Table 31 – SNMP Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UDP port</strong></td>
<td>Direct Nessus to scan a different port in the event that SNMP is running on a port other than 161.</td>
</tr>
<tr>
<td><strong>SNMPv3 user name</strong></td>
<td>The username for a SNMPv3 based account.</td>
</tr>
<tr>
<td><strong>SNMPv3 authentication password</strong></td>
<td>The password for the username specified.</td>
</tr>
<tr>
<td><strong>SNMPv3 authentication algorithm</strong></td>
<td>Select MD5 or SHA1 based on which algorithm the remote service supports.</td>
</tr>
<tr>
<td><strong>SNMPv3 privacy password</strong></td>
<td>A password used to protect encrypted SNMP communication.</td>
</tr>
<tr>
<td><strong>SNMPv3 privacy algorithm</strong></td>
<td>The encryption algorithm to use for SNMP traffic.</td>
</tr>
</tbody>
</table>

**SSH settings** (plugin 14273) – Users can select “**SSH settings**” from the drop-down menu and enter a “known hosts” file for scanning Unix systems. There is also a field for entering the “Preferred SSH Port”. By default Nessus will use the standard TCP port 22 for credentialed Unix scans, however, this setting enables the user to specify a non-standard port for SSH login attempts.

**Service Detection** (plugin 22964) controls how Nessus will test SSL based services; known SSL ports (e.g., 443), all ports or none. Testing for SSL capability on all ports may be disruptive for the tested host.

**Wake-on-LAN** (plugin 52616) controls what hosts to send WOL magic packets to before performing a scan and how long to wait (in minutes) for the systems to boot. The list of MAC addresses for WOL is entered using an uploaded text file with one host MAC address per line.

**Web Application Tests Settings** (plugin 39471) tests the arguments of the remote CGIs (Common Gateway Interface) discovered in the web mirroring process by attempting to
pass common CGI programming errors such as cross-site scripting, remote file inclusion, command execution, traversal attacks and SQL injection. Enable this option by selecting the “Enable web applications tests” checkbox.

These tests are not intended to target web applications implementing client-side technologies such as AJAX or Flash; however, there is a limited amount of testing performed against these technologies when the full plugin set is enabled.

This following plugins depend on plugin #39471:

The following web application related plugins depend on plugin 39471:

> 11139 – CGI Generic SQL Injection Vulnerability (CGI abuses)
> 39465 – CGI Generic Command Execution Vulnerability (CGI abuses)
> 39466 – CGI Generic Cross-Site Scripting Vulnerability (quick test) (CGI abuses: XSS)
> 39467 – CGI Generic Path Traversal Vulnerability (CGI abuses)
> 39468 – CGI Generic Header Injection Vulnerability (CGI abuses: XSS)
> 39469 – CGI Generic Remote File Inclusion Vulnerability (CGI abuses)
> 40406 – CGI Generic Tests HTTP Errors (CGI abuses)
> 42054 – CGI Generic SSI Injection Vulnerability (CGI abuses)
> 42055 – CGI Generic Format String Vulnerability (CGI abuses)
> 42056 – CGI Generic Local File Inclusion Vulnerability (CGI abuses)
> 42423 – CGI Generic SSI Injection Vulnerability (HTTP headers) (CGI abuses)
> 42424 – CGI Generic SQL Injection (blind) (CGI abuses)
> 42425 – CGI Generic Persistent Cross-Site Scripting Vulnerability (CGI abuses: XSS)
> 42426 – CGI Generic SQL Injection Vulnerability (HTTP Cookies) (CGI abuses)
> 42427 – CGI Generic SQL Injection Vulnerability (HTTP Headers) (CGI abuses)
> 42479 – CGI Generic SQL Injection Vulnerability (2nd pass) (CGI abuses)
> 42872 – CGI Generic Local File Inclusion Vulnerability (2nd pass) (CGI abuses)
> 43160 – CGI Generic SQL Injection (blind, time based) (CGI abuses)
> 44134 – CGI Generic Unseen Parameters Discovery (CGI abuses)
> 44136 – CGI Generic Cookie Injection Scripting (CGI abuses)
> 44670 – Web Application SQL Backend Identification (CGI abuses)
> 44676 – CGI Generic Command Execution Vulnerability (time based) (CGI abuses)
> 46193 – CGI Generic Cross Site Scripting (HTTP Headers) (CGI abuses: XSS)
> 46194 – CGI Generic Path Traversal Vulnerability (write test) (CGI abuses)
> 46195 – CGI Generic Path Traversal Vulnerability (extended test) (CGI abuses)
> 46196 – CGI Generic XML Injection (CGI abuses)
> 47830 – CGI Generic Injectable Parameter Weakness (CGI abuses)
> 47831 – CGI Generic Cross-Site Scripting Vulnerability (extended test) (CGI abuses: XSS)
> 47832 – CGI Generic On Site Request Forgery Vulnerability (CGI abuses)
> 47834 – CGI Generic Redirection Vulnerability (CGI abuses)
> 48926 – CGI Generic 2nd Order SQL Injection Detection (potential) (CGI abuses)
> 48927 – CGI Generic SQL Injection Detection (potential, 2nd order, 2nd pass) (CGI abuses)
> 49067 – CGI Generic HTML Injections (quick test) (CGI abuses: XSS)
> 49218 – Web Application Session Cookies Not Marked Secure (Web Servers)
> 50418 – CGI Generic Fragile Parameters Detection (Potential) (CGI abuses)
> 50494 – CGI Generic Path Traversal (Quick Test) (CGI abuses)

The screen capture below is the “Web Application Tests Settings” input page:

![Web Application Tests Settings](image)

### Table 32 – Web Application Tests Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable web application tests</td>
<td>This check box enables web application tests and causes the settings below to be evaluated during the test.</td>
</tr>
</tbody>
</table>
| Maximum run time (min)        | This option manages the amount of time in minutes spent per NASL script performing web application tests. These NASL scripts are listed above. At the time of this writing, there were 36 web application test NASLs. The run time of each script varies widely, however the following generic formula applies to the Maximum_run_time:  

\[
\text{scan\_time} = \left(\frac{\text{num\_scripts}}{\text{max\_checks}}\right) \times \text{Maximum\_run\_time} 
\]

For example:

\[
(36/5) \times 60 = 432 \text{ minutes} 
\]
This option defaults to 60 minutes and applies to all ports and CGIs for a given web site.

**Send POST requests**

“POST requests” tests are used for enhanced web form testing. By default, the web application tests will only use GET requests, unless this option is enabled. Generally, more complex applications use the POST method when a user submits data to the application. This setting provides more thorough testing, but may considerably increase the time required.

**Combinations of arguments values**

This option manages the combination of argument values used in the HTTP requests. This dropdown has five options:

- **one value** – This tests one parameter at a time with an attack string, without trying “non-attack” variations for additional parameters. For example, Nessus would attempt “/test.php?arg1=XSS&b=1&c=1” where “b” and “c” allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated.

- **some pairs** – Like “all pairs” testing, this will try to test a representative data set based on the “All-pairs” method. However, for each parameter discovered, Nessus will only test using a maximum of three valid input variables.

- **all pairs (slower but efficient)** – This form of testing is slightly slower but more efficient than the “one value” test. While testing multiple parameters, it will test an attack string, variations for a single variable and then use the first value for all other variables. For example, Nessus would attempt “/test.php?a=XSS&b=1&c=1&d=1” and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Nessus would never test for “/test.php?a=XSS&b=3&c=3&d=3” when the first value of each variable is “1”.

- **some combinations** – Like “all combinations” testing, this will perform tests using a combination of attack strings and valid input. However, for each parameter discovered, Nessus will only test using a maximum of three valid input variables.

- **all combinations (extremely slow)** – This method of testing will do a fully exhaustive test of all possible combinations of attack strings with valid input to variables. Where “All-pairs” testing seeks to create a smaller data set as a tradeoff for speed, “all combinations” makes no compromise on time and uses a complete data set of tests. This testing method may take a **long** time to complete.
<table>
<thead>
<tr>
<th><strong>HTTP Parameter Pollution</strong></th>
<th>When performing web application tests, attempt to bypass any filtering mechanisms by injecting content into a variable while supplying the same variable with valid content as well. For example, a normal SQL injection test may look like &quot;'/target.cgi?a='&amp;b=2&quot;. With HTTP Parameter Pollution (HPP) enabled, the request may look like &quot;'/target.cgi?a='&amp;a=1&amp;b=2&quot;.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Stop at first flaw</strong></td>
<td>This option determines when a new flaw is targeted. The dropdown has four options:</td>
</tr>
<tr>
<td></td>
<td><strong>per CGI</strong> (default) – As soon as a flaw is found on a CGI by a script, Nessus switches to the next known CGI on the same server, or if there is no other CGI, to the next port/server.</td>
</tr>
<tr>
<td></td>
<td><strong>per port</strong> (quicker) – As soon as a flaw is found on a web server by a script, Nessus stops and switches to another web server on a different port. This applies at the script level; finding an XSS flaw will not disable searching for SQL injection or header injection, but you will have at most one report for each type on a given port.</td>
</tr>
<tr>
<td></td>
<td><strong>per parameter</strong> (slow) – As soon as one flaw is found in a parameter of a CGI, Nessus stops and switches to the next parameter of the same script.</td>
</tr>
<tr>
<td></td>
<td><strong>look for all flaws</strong> (slower) – Perform extensive tests regardless of flaws found. This option can take a long time and is not recommend in most cases.</td>
</tr>
<tr>
<td><strong>Test Embedded web servers</strong></td>
<td>Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.</td>
</tr>
<tr>
<td><strong>URL for Remote File Inclusion</strong></td>
<td>During Remote File Inclusion (RFI) testing, this option specifies a file on a remote host to use for tests. By default, Nessus will use a safe file hosted on Tenable’s web server for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended for more accurate RFI testing.</td>
</tr>
<tr>
<td><strong>Fully Qualified Domain Names</strong></td>
<td>Fully Qualified Domain Names attached to the host being tested. Format of this check is “IP:FQDN”. This is useful for virtual host systems with more than one fully qualified domain name on a single system.</td>
</tr>
</tbody>
</table>

This option is limited to one FQDN per scan. To target more than one FQDN, multiple scans are required.
**Web Mirroring** (plugin 10662) sets configuration parameters for Nessus’ native web server content mirroring utility. Nessus will mirror web content to better analyze the contents for vulnerabilities and help minimize the impact on the server.

![Web Mirroring Settings](image)

**Table 33 – Web Mirroring Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of pages to mirror</strong></td>
<td>The maximum number of pages to mirror.</td>
</tr>
<tr>
<td><strong>Maximum depth</strong></td>
<td>Limit the number of links Nessus will follow for each start page.</td>
</tr>
<tr>
<td><strong>Start page</strong></td>
<td>The URL of the first page that will be tested. If multiple pages are required, use a colon delimiter to separate them (e.g., “/:/php4:/base”).</td>
</tr>
<tr>
<td><strong>Excluded items regex</strong></td>
<td>Enable exclusion of portions of the web site from being crawled. For example, to exclude the “/manual” directory and all Perl CGI, set this field to: (^/\ manual) (./\ pl\ (.?\ *)?)$.</td>
</tr>
<tr>
<td><strong>Follow dynamic pages</strong></td>
<td>If this checkbox is selected, Nessus will follow dynamic links and may exceed the other &quot;Web Mirroring Settings&quot; parameters.</td>
</tr>
</tbody>
</table>

When all of the options have been configured as desired, click on “Submit” to save the policy and return to the **Policies** tab. At any time, you can click on “Edit” to make changes to a policy you have already created or click on “Delete” to remove a policy completely.

**STATUS**

**Job Queue**
The SecurityCenter Job Queue contains a listing of scheduled and running jobs along with job metadata.
Available fields include Job ID, Type, Obj ID, Status, PID, Organization, Initiator, Start Time and Targeted Time. This information is not generally required for the day to day operations of SecurityCenter, but may be requested by Tenable Support when troubleshooting issues.

Job options include "Details", which lets you view individual job details and "Kill Job", which lets you kill a currently running job. Killing any process is not recommended except at the request of Tenable Support.

**Logs**
See the “Logs” section above. The functionality of these two links is identical for the Admin user.

**Plugins**
Plugins are scripts used by the Nessus and PVS scanners to collect and interpret vulnerability data. For ease of operation, plugins are managed centrally by SecurityCenter and pushed out to their respective scanners.

Within the **Plugins** interface, the user has the ability to perform a wide variety of plugin-related functions including update both active and passive plugins, upload custom plugins, clear custom plugins, view plugin details/source and search for specific plugins. Clicking on the “Plugins” tab displays a page similar to the one below:
Update Plugins

Immediately after installing SecurityCenter, plugins are automatically updated on a regular basis. Manually updating plugins simply involves clicking on the “Update Plugins” button and waiting for the process to complete. Due to the large quantity of plugins and inconsistency of network speeds, this process can take a long time to complete. Please refer to Appendix 5 of this document for more information about performing offline plugin updates with SecurityCenter.

The date and time of the last successful plugin update is displayed at the top of the page to the right of the “Clear Custom Plugins” command button. After a successful download, the plugins are displayed in the plugin table with the date of successful download in the “Date Downloaded” field.

Upload Plugins

Clicking on “Upload Plugins” opens a dialog box that allows the user to upload one or more active, passive or custom plugins. Choose “Custom” for any active or passive plugins that you have created. All custom plugins must have unique Plugin ID numbers and have family associations based on existing SecurityCenter families. Choose “Active” for Tenable-signed active plugins or “Passive” for any Tenable-signed passive plugins. An additional option to “Override Plugins” is displayed for custom plugin uploads. Choose this option if you wish to override previously uploaded custom plugins.

All custom plugin files must be compressed using the Unix Tar utility before uploading. Once compressed the files will have a .tar.gz extension.

For example, running the following command against two new custom plugins will create an uploadable archive file called custom_nasl_archive.tar.gz that contains both custom plugins:

```
# tar -cvzf custom_nasl_archive.tar.gz custom1.nasl custom2.nasl
```
After browsing for the plugin archive and uploading it, confirm the plugin type and whether you wish to override previous custom plugins and then click on “Submit” to extract the plugins to SecurityCenter. Shortly after completion a notification message is displayed indicating a successful plugin upload.

**Clear Custom Plugins**

This option removes all custom plugins and may affect scan policies using those plugins. Use this option at your own risk!

This option enables the user to remove all custom plugins from SecurityCenter. Before clicking this option, ensure that you wish for all custom plugins to be removed.

**Other Plugin Options**

Other plugin options include “Details” and “Source”. The “Details” option loads a popup with plugin details such as the plugin ID, Name, Family, Type, Version, Modified Time, CVE/BID, Copyright and Description. The “Source” option displays the plugin source code for the user. The “Search” option allows you to search for plugins based on several plugin attributes including: ID, Name, Description, Type, Version, Copyright, CVE/BID (CVE or Bugtraq ID number), MSFT (Microsoft Bulletin), XRef and Exploit Availability.
ABOUT TENABLE NETWORK SECURITY

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG and PCI compliance. Tenable’s award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.
APPENDIX 1: NON-TENABLE LICENSE DECLARATIONS

Below you will find third-party software packages that Tenable provides for use with SecurityCenter 4.

Section 1 (b) (ii) of the SecurityCenter License Agreement reads:

(ii) The Software may include code or other intellectual property provided to Tenable by third parties, including Plug-Ins that are not owned by Tenable, (collectively, “Third Party Components”). Any Third Party Component that is not marked as copyrighted by Tenable is subject to other license terms that are specified in the Documentation. By using the Software, you hereby agree to be bound by such other license terms as specified in the Documentation.

SecurityCenter’s Software License Agreement can be found on the machine SecurityCenter is installed on in the directory /admin/misc.

RELATED THIRD-PARTY AND OPEN-SOURCE LICENSES

- Apache – http://www.apache.org/licenses/LICENSE-2.0
- glibc – http://www.gnu.org/copyleft/lesser.html (Nessus 3 uses part of this open-source library)
- jQuery – http://jquery.org/license
- libpng – http://www.libpng.org/pub/png/src/libpng-LICENSE.txt
- libxml2 – http://www.opensource.org/licenses/mit-license.html
- Nessus Plugins (not copyrighted to Tenable) – http://www.gnu.org/copyleft/gpl.html
- OpenLDAP – http://www.openldap.org/software/release/license.html
- OpenSSL – http://www.openssl.org/source/license.html
- PHP – http://us3.php.net/license/3_01.txt

This product includes cryptographic software written by Eric Young (eay@mincom.oz.au). Copyright (C) 1995-1997 Eric Young. All rights reserved. THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “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 AUTHOR 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.

Tenable Third-Party Licensed Software
**ChartDirector Version 5.0**
ChartDirector Version 5.0.2
Copyright (C) 2009 Advanced Software Engineering Limited
All Rights Reserved

*************** LICENSE AGREEMENT ***************

You should carefully read the following terms and conditions before using the ChartDirector software. Your use of the ChartDirector software indicates your acceptance of this license agreement. Do not use the ChartDirector software if you do not agree with the license agreement.

Disclaimer of Warranty

The ChartDirector software and the accompanying files are distributed and licensed "as is". Advanced Software Engineering Limited disclaims all warranties, either express or implied, including, but not limited to implied warranties of merchantability and fitness for a particular purpose. Should the ChartDirector software prove defective, the licensee assumes the risk of paying the entire cost of all necessary servicing, repair, or correction and any incidental or consequential damages. In no event will Advanced Software Engineering Limited be liable for any damages whatsoever (including without limitation damages for loss of business profits, business interruption, loss of business information and the like) arising out of the use or the inability to use the ChartDirector software even if Advanced Software Engineering Limited has been advised of the possibility of such damages.

Intellectual Property

The ChartDirector software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The ChartDirector software is licensed, not sold. Title to the ChartDirector software shall at all times remain with Advanced Software Engineering Limited.

You agree not to modify, decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the ChartDirector software.

Trial Version

The trial version of the ChartDirector software will produce yellow banner messages at the bottom of the chart images generated by it. You agree to not remove, obscure, or alter this message.

SubJECTED to the conditions in this license agreement:

- You may use the unmodified trial version of the ChartDirector software without charge.
- You may redistribute the unmodified trial version of the ChartDirector software, provided you do not charge for it.

- You may embed the unmodified trial version of the ChartDirector software (or part of it), in a product and distribute the product, provided you do not charge for the product.

If you do not want the yellow banner messages appearing in the charts, or you want to embed the ChartDirector software (or part of it) in a product that is not free, you must purchase a commercial license to use the ChartDirector software from Advanced Software Engineering Limited. Please refer to Advanced Software Engineering's web site at www.advsofteng.com for details.

Credits

The ASP/COM/VB, PHP, Perl, Python, Ruby and C++ editions of ChartDirector contains code from the Independent JPEG Group and the FreeType team. Any software that is derived from these editions of ChartDirector must include the following text in its documentation. This applies to both the trial version as well as to the commercial licensed version of ChartDirector.

- This software is based in part on the work of the Independent JPEG Group

- This software is based in part of the work of the FreeType Team

Nessus Plugins

Nessus Plugins (copyrighted by Tenable) – http://cgi.tenable.com/Subscription_Agreement.pdf
APPENDIX 2: MANUAL LCE KEY EXCHANGE

A manual key exchange between SecurityCenter and the LCE is normally not required; however, in some cases where remote root login is prohibited or key exchange debugging is required, you will need to manually exchange the keys.

For the remote LCE to recognize SecurityCenter, you need to copy the SSH public key of SecurityCenter and append it to the “/opt/lce/.ssh/authorized_keys” file. The “/opt/lce/daemons/lce-install-key.sh” script performs this function. The following steps describe how to complete this process:

1. Download the SSH public key for SecurityCenter by logging in as the SecurityCenter administrator user and navigating to the “Keys” section (“System” -> “Keys”).

2. Click on “Download Key”, choose the desired key format (both DSA or RSA work for this process) and then click on “submit”.

3. Save the key file (SSHKey.pub) to your local workstation. Do not edit the file or save it to any specific file type.

4. From the workstation where you downloaded the key file, use a secure copy program, such as “scp” or “WinSCP” to copy the SSHKey.pub file to the LCE system. You will need to have the credentials of an authorized user on the LCE server to perform this step. For example, if you have a user “bob” configured on the LCE server (hostname “lceserver”) whose home directory is /home/bob, the command on a Unix system would be as follows:

   # scp SSHKey.pub bob@lceserver:/home/bob

5. On the LCE server, as the root user, change the ownership of the ssh key file to lce as follows:

   # chown lce /home/bob/lce

   Then append the SSH public key to the “/opt/lce/.ssh/authorized_keys” file with the following steps:

   # su lce
   # /opt/lce/daemons/lce-install-key.sh /home/bob/SSHKey.pub

6. To test the communication, as the user “tns” on the SecurityCenter system, attempt to run the id command:

   # su tns
   # ssh -C -o PreferredAuthentications=publickey lce@<LCE-IP> id

   If a connection has not been previously established, you will see a warning similar to the following:
The authenticity of host '192.168.15.82 (192.168.15.82)' can't be established.
Are you sure you want to continue connecting (yes/no)?

Answer “yes” to this prompt.

If the key exchange worked correctly, a message similar to the following will be displayed:

```
# uid=251(lce) gid=251(lce) groups=251(lce)
```

7. The IP address of SecurityCenter can be added to the LCE system’s /etc/hosts file. This prevents the SSH daemon from performing a DNS lookup that can add seconds to your query times.

8. The LCE can now be added to SecurityCenter via the normal administrator “LCE add” process documented in the SecurityCenter 4.2 Administration Guide.
APPENDIX 3: NESSUS SSL CONFIGURATION

INTRODUCTION
This section describes how to generate and exchange SSL certificates for the Nessus vulnerability scanner to use with SecurityCenter. For this procedure, you will need to have administrative (root) access to the SecurityCenter system, as well as all Nessus scanner systems.

Please note that users should be familiar with PKI deployments and it is not recommended that the Nessus server be used as the site’s PKI system. The method described here is intended to assist in testing the functionality of the certificate exchange to assist users in the incorporation of the certificates into their current PKI system. In this method, the same key is shared between multiple servers. This may not be acceptable in some installations.

OVERVIEW OF SSL CERTIFICATES AND KEYS
Nessus supports authentication protocols based on the OpenSSL toolkit (please see http://www.openssl.org/ for more details about the toolkit). This provides cryptographic protection and secure authentication. This section provides an overview of the certificates and keys necessary for SSL communication with Nessus. In the example described in this document, there are three key system components: the Certificate Authority, the Nessus Server and the Nessus client, which in this case is SecurityCenter. It is necessary to generate the keys required for the SSL communication and copy them to the appropriate directories.

Certificate Authority
The Certificate Authority (CA) ensures that the certificate holder is authentic and not an impersonator. The Certificate Authority holds a copy of the certificates for registered users to certify that the certificate is genuine. When the Certificate Authority receives a Certificate Signing Request (CSR), it validates and signs the certificate. In the example provided in this document, the Certificate Authority resides on the Nessus server, but this is not the recommended method for a production environment. In proper PKI deployments, the Certificate Authority would be a separate system or entity, such as Thawte or Verisign.

Nessus Server
In the example described in this document, the Nessus server is the same physical system that holds the Certificate Authority, but this will not likely be the case in a production environment. The Nessus server is the target of the secure communication and its keys must be generated locally and copied to the systems that will need to communicate with it using the SSL protocol. The Nessus server has users defined that authenticate to it either by simple login and password or via SSL. These users will also have keys associated with them.

Nessus Client
The Nessus client, which is SecurityCenter in this case, communicates with the Nessus server via SSL. It uses keys generated for a Nessus client and stores these keys and the certificate for the Certificate Authority in the /opt/sc4/daemons directory. These keys must be owned by the “tns” userid.
NESSUS CONFIGURATION FOR UNIX

Commands and Relevant Files
The following section describes the commands and relevant files involved in the Nessus SSL process on a Red Hat Linux system.

Certificate Authority and Nessus Server Certificate
The /opt/nessus/sbin/nessus-mkcert command creates the Certificate Authority and generates the server certificate. This command creates the following files:

<table>
<thead>
<tr>
<th>File Name Created</th>
<th>Purpose</th>
<th>Where to Copy to</th>
</tr>
</thead>
<tbody>
<tr>
<td>/opt/nessus/com/nessus/CA/cacert.pem</td>
<td>This is the certificate for the Certificate Authority. If using an existing PKI, this will be provided to you by the PKI and must be copied to this location.</td>
<td>/opt/sc4/daemons on SecurityCenter and rename it to “nessusca.pem”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/opt/nessus/var/nessus/CA on the initial Nessus server and any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/opt/nessus/com/nessus/CA on any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
<tr>
<td>/opt/nessus/com/nessus/CA/servercert.pem</td>
<td>This is the public certificate for the Nessus server that is sent in response to a CSR.</td>
<td>/opt/nessus/com/nessus/CA on any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
<tr>
<td>/opt/nessus/var/nessus/CA/cakey.pem</td>
<td>This is the private key of the Certificate Authority. It may or may not be provided by the Certificate Authority, depending on if they allow the creation of sub users.</td>
<td>/opt/nessus/var/nessus/CA on any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
<tr>
<td>/opt/nessus/var/nessus/CA/serverkey.pem</td>
<td>This is the private key of the Nessus server.</td>
<td>/opt/nessus/var/nessus/CA on any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
</tbody>
</table>

Nessus Client Keys
The Nessus user, in this case the user ID that SecurityCenter uses to communicate with the Nessus server, is created by the following command:

```bash
# /opt/nessus/sbin/nessus-mkcert-client
```
This command creates the keys for the Nessus clients and optionally registers them appropriately with the Nessus server by associating a distinguished name (dname) with the user ID. It is important to respond “y” (yes) when prompted to register the user with the Nessus server for this to take effect. The user name may vary and is referred to here as “user”.

The certificate filename will be a concatenation of “cert_”, the user name you entered and “.pem”. Additionally, the key filename will be a concatenation of “key_”, the user name you entered and “.pem”.

If the user was previously added via the /opt/nessus/sbin/nessus-adduser command, you will still need to run this program to register the user. If you have not previously created the user, it is not necessary to also run the nessus-adduser command; the user will be created if it does not already exist. The following files are created by this command:

<table>
<thead>
<tr>
<th>File Name Created</th>
<th>Purpose</th>
<th>Where to Copy to</th>
</tr>
</thead>
<tbody>
<tr>
<td>/tmp/nessus-xxxxxxxxxx/cert_{user}.pem</td>
<td>This is the public certificate for the specified user.</td>
<td>Concatenate with key_{user}.pem as &quot;nessuscert.pem&quot; and copy to the /opt/sc4/daemons directory on SecurityCenter.</td>
</tr>
<tr>
<td>/tmp/nessus-xxxxxxxxxx/key_{user}.pem</td>
<td>This is the private key for the specified user.</td>
<td>Concatenate with cert_{user}.pem as &quot;nessuscert.pem&quot; and copy to the /opt/sc4/daemons directory on SecurityCenter.</td>
</tr>
<tr>
<td>/opt/nessus/var/nessus/users/{user}/auth/dname</td>
<td>This is the distinguished name to be associated with this user. The distinguished name consists of a number of fields separated by commas in the following format:</td>
<td>&quot;/C={country}/ST={state}/L={location}/OU={organizational unit}/O={organization/CN={common name}&quot;</td>
</tr>
</tbody>
</table>

Creating and Deploying SSL Authentication for Nessus

An example SSL Certificate configuration for Nessus to SecurityCenter authentication is included below:

In the example described here, SecurityCenter and the Nessus scanner are defined as follows. Your configuration will vary:

**SecurityCenter:**
IP: 192.168.10.10
OS: Red Hat ES 5
Nessus Scanner:
IP: 192.168.11.30
OS: Red Hat ES 5

Create Keys and User on Nessus Server
Log in to the Nessus scanner and use the su command to become the root user. Create the Certificate Authority and Nessus server certificate as follows:

```
# /opt/nessus/sbin/nessus-mkcrt

-------------------------------------------------------------------------
Creation of the Nessus SSL Certificate
-------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL certificate of Nessus. Note that this information will *NOT* be sent to anybody (everything stays local), but anyone with the ability to connect to your Nessus daemon will be able to retrieve this information.

CA certificate life time in days [1460]:
Server certificate life time in days [365]:
Your country (two letter code) [US]:
Your state or province name [NY]:
Your location (e.g. town) [New York]:
Your organization [Nessus Users United]: Tenable Network Security
This host name [Nessus4_2]:

Congratulations. Your server certificate was properly created.
The following files were created:

  . Certification authority :
       Certificate = /opt/nessus/com/nessus/CA/cacert.pem
       Private key = /opt/nessus/var/nessus/CA/cakey.pem

  . Nessus Server :
       Certificate = /opt/nessus/com/nessus/CA/servercert.pem
       Private key = /opt/nessus/var/nessus/CA/serverkey.pem

Next, create the user ID for the Nessus client, which is SecurityCenter in this case, to log in to the Nessus server with, key and certificate. This is done with the command
/opt/nessus/sbin/nessus-mkcrt-client. If the user does not exist in the Nessus user database, it will be created. If it does exist, it will be registered to the Nessus server and have a distinguished name (dname) associated with it. It is important to respond "y" (yes) when prompted to register the user with the Nessus server for this to take effect. The user must be a Nessus admin, so answer "y" when asked. The following example shows the prompts and typical answers:

```
# /opt/nessus/sbin/nessus-mkcrt-client
Do you want to register the users in the Nessus server as soon as you create their certificates ? [n]: y
```
This script will now ask you the relevant information to create the SSL client certificates for Nessus.
Client certificate life time in days [365]:
Your country (two letter code) [FR]: US
Your state or province name []: MD
Your location (e.g. town) [Paris]: Columbia
Your organization []: Tenable Network Security
Your organizational unit []:

We are going to ask you some question for each client certificate
If some question have a default answer, you can force an empty answer by entering a single dot '.

User #1 name (e.g. Nessus username) []: paul
User paul already exists
Do you want to go on and overwrite the credentials? [y]: y
Should this user be administrator? [n]: y
Country (two letter code) [US]:
State or province name [MD]:
Location (e.g. town) [Columbia]:
Organization [Tenable Network Security]:
Organizational unit []:
E-mail []:

User rules
---------
nessusd has a rules system which allows you to restrict the hosts that $login has the right to test. For instance, you may want him to be able to scan his own host only.
Please see the nessus-adduser(8) man page for the rules syntax

Enter the rules for this user, and enter a BLANK LINE once you are done:
(the user can have an empty rules set)

User added to Nessus.
Another client certificate? [n]: n
Your client certificates are in /tmp/nessus-043c22b5
You will have to copy them by hand
#

The certificates created contain the username entered previously, in this case "paul", and are located in the directory as listed in the example above (e.g., /tmp/nessus-043c22b5).

Create the nessuscert.pem Key
In the above specified tmp directory, the certificate and key files in this example are named "cert_paul.pem" and "key_paul.pem". These files must be concatenated to create nessuscert.pem as follows:
Copy Certificate Authority to the Nessus Server Directory
Copy the Certificate Authority certificate to the directory `/opt/nessus/var/nessus/CA`:

```
# cp /opt/nessus/com/nessus/CA/cacert.pem /opt/nessus/var/nessus/CA
# ls -l /opt/nessus/var/nessus/CA
total 12
-rw-r--r-- 1 root root 1086 Nov 18 09:44 cacert.pem
-rw-r--r-- 1 root root  887 Nov 18 09:25 cakey.pem
-rw-r--r-- 1 root root  887 Nov 18 09:25 serverkey.pem
```

Transfer Certificates and Keys to SecurityCenter
Copy the newly created `nessuscert.pem` file to the remote SecurityCenter system `daemons` directory as follows:

```
# scp nessuscert.pem root@192.168.10.10:/opt/sc4/daemons
```

You will also need to transfer and rename the Certificate Authority’s public certificate to the remote SecurityCenter as follows:

```
# cd /opt/nessus/com/nessus/CA
# scp cacert.pem root@192.168.10.10:/opt/sc4/daemons/nessusca.pem
```

Check Permissions on SecurityCenter
On SecurityCenter (in this example 192.168.10.10), make sure all “.pem” files in the `/opt/sc4/daemons` directory are owned by the “tns” user:

```
# cd /opt/sc4/daemons
# chown tns:tns *.pem
```

Restart Nessus Daemons
Restart the Nessus daemons with the appropriate command for your system. The example here is for Red Hat:
# /sbin/service nessusd restart

**Change the Nessus Mode of Authentication**
From the SecurityCenter web UI, go to "Resources" and then "Nessus Scanners". Change the authentication mode from "Password Based" to "SSL Certificate" and then click on "Submit" to confirm.

![Nessus Scanners](image)

**Using Custom Certificates**
During an upgrade, SecurityCenter will check for the presence of custom SSL certificates. If certificates are found and the owner is not Tenable, any newly generated certificates will be named with a "new" extension and placed in the `/opt/sc4/support/conf` directory to avoid overwriting existing files.

**Deploy to other Nessus Scanners**
If you have other Nessus servers that will need to authenticate using SSL, simply copy the files to the other servers as follows:

```
# cd /opt/nessus/var/nessus/CA
# scp cacert.pem cakey.pem serverkey.pem root@nessusIP:/opt/nessus/var/nessus/CA
# cd /opt/nessus/com/nessus/CA
# scp cacert.pem servercert.pem root@nessusIP:/opt/nessus/com/nessus/CA
```

Then, you will need to copy the Nessus users to all the Nessus servers:

```
# cd /opt/nessus/var/nessus/users
# tar -zcvf - admin | ssh -C root@nessusIP "tar -zxvf - -C
/opt/nessus/var/nessus/users"
```

Finally, restart the Nessus service on all the Nessus servers with the appropriate command for your system. This example is for Red Hat:
Use the steps from above (Changing the Nessus Mode of Authentication) to add the new server(s) to SecurityCenter using certificate-based authentication.

**NESSUS CONFIGURATION FOR WINDOWS**

**Commands and Relevant Files**
The following section describes the commands and relevant files involved in the Nessus SSL process on a Windows system.

**Certificate Authority and Nessus Server Certificate**
The `nessus-mkcert.exe` executable located in C:\Program Files\Tenable\Nessus creates the Certificate Authority and generates the server certificate. This command creates the following files:

<table>
<thead>
<tr>
<th>File Name Created</th>
<th>Purpose</th>
<th>Where to Copy to</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Program Files\Tenable\Nessus\nessus\CA\cacert.pem</td>
<td>This is the certificate for the Certificate Authority. If using an existing PKI, this will be provided to you by the PKI and must be copied to this location.</td>
<td>/opt/sc4/demons on SecurityCenter and rename it to “nessusca.pem”.</td>
</tr>
<tr>
<td>C:\Program Files\Tenable\Nessus\nessus\CA\servercert.pem</td>
<td>This is the public certificate for the Nessus server that is sent in response to a CSR.</td>
<td>C:\Program Files\Tenable\Nessus\nessus\CA\servercert.pem on any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
<tr>
<td>C:\Program Files\Tenable\Nessus\nessus\CA\cakey.pem</td>
<td>This is the private key of the Certificate Authority. It may or may not be provided by the Certificate Authority, depending on if they allow the creation of sub users.</td>
<td>C:\Program Files\Tenable\Nessus\nessus\CA\cakey.pem on any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
<tr>
<td>C:\Program Files\Tenable\Nessus\nessus\CA\serverkey.pem</td>
<td>This is the private key of the Nessus server.</td>
<td>C:\Program Files\Tenable\Nessus\nessus\CA\serverkey.pem on any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
</tbody>
</table>

# /sbin/service nessusd restart
Nessus Client Keys
The Nessus user, in this case the user ID that SecurityCenter uses to communicate with the Nessus server, is created by the `nessus-mkcert-client.exe` executable located in `C:\Program Files\Tenable\Nessus`.

This command creates the keys for the Nessus clients and optionally registers them appropriately with the Nessus server by associating a distinguished name (dname) with the user ID. It is important to respond “y” (yes) when prompted to register the user with the Nessus server for this to take effect. The user name may vary and is referred to here as “user”.

The certificate filename will be a concatenation of “cert_”, the user name you entered and “.pem”. Additionally, the key filename will be a concatenation of “key_”, the user name you entered and “.pem”.

The following files are created by this command:

<table>
<thead>
<tr>
<th>File Name Created</th>
<th>Purpose</th>
<th>Where to Copy to</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>C:\Documents and Settings\&lt;UserAccount&gt;\Local Settings\Temp\nessus-xxxxxxxx\cert_&lt;user&gt;.pem</code></td>
<td>This is the public certificate for the specified user.</td>
<td>Concatenate with <code>key_&lt;user&gt;.pem</code> as “nessuscert.pem” and copy to the <code>/opt/sc4/daemons</code> directory on SecurityCenter.</td>
</tr>
<tr>
<td><code>C:\Documents and Settings\&lt;UserAccount&gt;\Local Settings\Temp\nessus-xxxxxxxx\key_&lt;user&gt;.pem</code></td>
<td>This is the private key for the specified user.</td>
<td>Concatenate with <code>cert_&lt;user&gt;.pem</code> as “nessuscert.pem” and copy to the <code>/opt/sc4/daemons</code> directory on SecurityCenter.</td>
</tr>
<tr>
<td><code>C:\Program Files\Tenable\Nessus\nessus\users\&lt;user_name&gt;\auth\dname</code></td>
<td>This is the distinguished name to be associated with this user. The distinguished name consists of a number of fields separated by commas in the following format: &quot;/C={country}/ST={state}/L={location}/OU={organizational unit}/O={organization/CN={common name}&quot;</td>
<td></td>
</tr>
</tbody>
</table>

Creating and Deploying SSL Authentication for Nessus

Create Keys and User on Nessus Server
Create the Certificate Authority and Nessus server certificate using the `nessus-mkcert.exe` executable located in `C:\Program Files\Tenable\Nessus` as follows:
Next, create the user ID for the Nessus client, which is SecurityCenter in this case, to log in to the Nessus server with, key and certificate. This is done with the `nessus-mkcert-client.exe` executable located in `C:\Program Files\Tenable\Nessus`. If the user does not exist in the Nessus user database, it will be created. If it does exist, it will be registered to the Nessus server and have a distinguished name (dname) associated with it. It is important to respond “y” (yes) when prompted to register the user with the Nessus server for this to take effect. The user must be a Nessus admin, so answer “y” when asked. The following example shows the prompts and typical answers:
The certificates created contain the username entered previously, in this case “admin”, and are located in the directory as listed in the example screen capture above (e.g., C:\Documents and Settings\<UserAccount>\Local Settings\Temp\nessus-00007fb1). In the specified directory, the certificate and key files in this example are named “cert_admin.pem” and “key_admin.pem”.

**Transfer Certificates and Keys to SecurityCenter**

Transfer the “cert_admin.pem” and “key_admin.pem” files to a desired location on SecurityCenter, change into that directory and concatenate them as follows:

```
# cat cert_admin.pem key_admin.pem > nessuscert.pem
```

Copy the newly created “nessuscert.pem” to the /opt/sc4/daemons/ directory as follows:
You will also need to transfer and rename the Certificate Authority’s public certificate C:\Program Files\Tenable\Nessus\nessus\CA\cacert.pem to SecurityCenter in the /opt/sc4/daemons/ directory. After the transfer, cacert.pem must be renamed "nessusca.pem".

Check Permissions on Security Center
On SecurityCenter, make sure all "pem" files in the /opt/sc4/daemons directory are owned by the "tns" user:

```
# cd /opt/sc4/daemons
# chown tns:tns *.pem
```

Restart Nessus Daemons
Open the Nessus Server Manager GUI, click on “Stop Nessus Server” and then click on “Start Nessus Server”.

Change the Nessus Mode of Authentication
From the SecurityCenter web UI, go to "Resources" and then "Nessus Scanners". Change the authentication mode from “Password Based” to “SSL Certificate” and then click on "Submit" to confirm.
APPENDIX 4: USING A CUSTOM SSL CERTIFICATE

SecurityCenter ships with its own default SSL certificate; however, in many cases it is desirable to obtain a custom SSL certificate for enhanced security.

In the example below, two certificate files were received from the CA: "host.cert" and "host.key". These file names will vary depending on the CA used.

The custom certificate email address must not be "SecurityCenter@SecurityCenter" or subsequent upgrades will not retain the new certificate.

Use the steps below to upload a custom SSL certificate to your SecurityCenter:

1. Backup the current certificates that are located in the /opt/sc4/support/conf directory. These files are named SecurityCenter.cert and SecurityCenter.pem. In the example below, we are placing the files in /tmp.

   ```bash
   # cp /opt/sc4/support/conf/SecurityCenter.cert /tmp/SecurityCenter.cert.bak
   # cp /opt/sc4/support/conf/SecurityCenter.pem /tmp/SecurityCenter.pem.bak
   ``

2. Copy the new certificates (e.g., host.cert and host.key) to the /opt/sc4/support/conf directory and overwrite the current certificates. If prompted to overwrite, press "y".

   ```bash
   # cp host.cert /opt/sc4/support/conf/SecurityCenter.cert
   # cp host.key /opt/sc4/support/conf/SecurityCenter.pem
   ``

3. Make sure the files have the correct permissions (644) and ownership (tns) as follows:

   ```bash
   # ls -l /opt/sc4/support/conf/SecurityCenter.cert
   -rw-r--r-- 1 tns tns 4389 May 15 15:12 SecurityCenter.cert
   # ls -l /opt/sc4/support/conf/SecurityCenter.pem
   -rw-r--r-- 1 tns tns 887 May 15 15:12 SecurityCenter.pem
   ``

4. Restart the SecurityCenter services:

   ```bash
   # service SecurityCenter restart
   ``

5. Browse to SecurityCenter using SSL (e.g., https://192.168.1.5/sc4). When prompted to confirm the SSL certificate, verify the new certificate details.
APPENDIX 5: OFFLINE SECURITYCENTER PLUGIN UPDATES

The steps outlined below for offline SecurityCenter plugin updates are different than the steps used to perform an offline plugin update for a standalone Nessus scanner. Please read and follow the steps below carefully to ensure a successful offline SecurityCenter plugin update.

NESSUS

1. If not already in place, install a Nessus scanner on the same host as SecurityCenter. It does not need to be started or used though.

2. Run this command and save the challenge string:

   ```
   # /opt/nessus/bin/nessus-fetch --challenge
   ```


4. Take the challenge string from Step 2 and your Activation Code, and place those values in the appropriate fields on the web page. Click the “Submit” button.

   After clicking the “Submit” button in the step above, proceed directly to step 5. Do not follow the directions provided on the download page.

5. On the download page, copy the link that starts with http://plugins.nessus.org/get.php... and save it as a favorite or bookmark (do not click on the link to download the file). Within the saved link, change the “all-2.0.tar.gz” portion of the URL to “sc-plugins.tar.gz”. You will need this link to perform future offline updates. Do not click on the link for nessus-fetch.rc, as it is not needed for this process. For all future offline SecurityCenter plugin updates, start the process with Step 6.

6. Clicking the favorite or bookmark you created will prompt you to download a file. Save the file (sc-plugins.tar.gz). Do not change this file name either before or after the download process.

7. Take the sc-plugins.tar.gz and save this on the PC where you access your SecurityCenter GUI.

8. Log into the SecurityCenter GUI as admin.

9. Go to Plugins -> Plugins.

10. Click on “Upload Plugins” and browse to the saved sc-plugins.tar.gz file, and then click on “Submit”.

11. The plugin update will take a few to several minutes, depending how many Nessus scanners you have attached. You will see a message with the current date for the updated active plugins when it is finished.
PVS (SecurityCenter 4.2 and greater only)

1. Go to http://downloads.nessus.org/sc-passive.tar.gz and download the archive to a location browsable from SecurityCenter.

2. Log into SecurityCenter and go to “Plugins” and then “Upload”. Choose the sc-passive.tar.gz file. For type, select “Passive” and then complete the PVS plugin upload.
APPENDIX 6: CONFIGURING LDAP WITH MULTIPLE ORGANIZATIONAL UNITS

Tenable’s SecurityCenter LDAP configuration does not currently support the direct addition of multiple Organizational Units (OUs) in the LDAP configuration screen. Three deployment options are possible for those with multiple OUs:

**Option 1 (Preferred)**
Add a container (i.e., Group) only for SecurityCenter users and allow existing Active Directory users to become members of the newly created group. Use the Distinguished Name (DN) of this group as the “Search Base”. For example:

CN=SecurityCenter,DC=devlab,DC=domain,DC=com

Save the changes and new users who are members of this group will be able to log in. No restart is required.

**Option 1 Example**
Step One:

a. Log in as an admin user.
b. Choose System -> Configuration -> LDAP
c. Log out as the admin user and then log in as the organizational user who will be managing the user in question.

d. Create the new user and when entering the LDAP "Search String" enter "=*":

\[
\text{memberOf=CN=nested1,OU=cftest1,DC=devlab,DC=domain,DC=com}
\]

**OPTION 2**

Use a high level "Search Base" in the LDAP configuration. For example:

\[
\text{DC=devlab,DC=domain,DC=com}
\]

When adding users you will need to enter the "Search String" each time (currently not saved; we are considering adding this as a configurable setting in a future release):

\[
\text{memberOf=CN=nested1,OU=cftest1,DC=devlab,DC=domain,DC=com}
\]
Option 2 Example
Step One:

a. Log in as an admin user.
b. Choose System -> Configuration -> LDAP

c. Click on "Test LDAP Settings" to test configurations (Top RHS).
d. Log out as the admin user and then log in as the organizational user who will be managing the user in question.
e. Create the new user:

Choose LDAP:
OPTION 3
Use a specific “Search Base” in the LDAP configuration. For example:

CN=nested1,OU=cftest1,DC=devlab,DC=domain,DC=com

In the example above, user searches are limited to this container and below. The “Search String” will default to the defined username attribute in the LDAP configuration (such as “sAMAccountName”).

Testing from the command line:
# /opt/sc4/support/bin/ldapsearch -h x.x.x.x -b "DC=devlab, DC=domain, DC=com" -p 389 -s sub "(memberOf=CN=nested1,ou=cftest1,DC=devlab,DC=domain,DC=com)" -D binduser@devlab.domain.com -W sAMAccountName

Returns:

user 1, cftest1, devlab.domain.com
dn: CN=user 1,OU=cftest1,DC=devlab,DC=domain,DC=com
sAMAccountName: user1

**Option 3 Example**

**Step One:**

a. Log in as an admin user.

b. Choose System -> Configuration -> LDAP

Create the user:
Tenable makes use of the "ldapsearch" command to test LDAP connectivity between your SecurityCenter 4 and the LDAP server.

Use the following command to check for a particular user:

```
# /opt/sc4/support/bin/ldapsearch -h x.x.x.x -b "DC=devlab, DC=domain, DC=com" -p 389 -s sub "(memberOf=CN=nested1,ou=cftest1,DC=devlab,DC=domain,DC=com)" -D binduser@devlab.domain.com -W sAMAccountName
```

Returns:

```
user 1, cftest1, devlab.domain.com
dn: CN=user 1,OU=cftest1,DC=devlab,DC=domain,DC=com
sAMAccountName: user1
```