# Table of Contents

Introduction ........................................................................................................................................... 6
  Standards and Conventions .................................................................................................................. 6
  Abbreviations ....................................................................................................................................... 7
  SecurityCenter Administrator Functions .............................................................................................. 7
    Starting/Halting SecurityCenter ......................................................................................................... 7

SecurityCenter Home Page/Dashboard .................................................................................................. 8
  Supported Platforms ............................................................................................................................. 8
  Launch SecurityCenter .......................................................................................................................... 8

System Configuration .............................................................................................................................. 10
  Configuration ....................................................................................................................................... 10
    License .............................................................................................................................................. 10
    Mail ................................................................................................................................................. 12
    LDAP .............................................................................................................................................. 13
    Data Expiration ................................................................................................................................. 16
    External Schedules ............................................................................................................................ 18
    Security ............................................................................................................................................ 18
    Miscellaneous Configuration ............................................................................................................ 21
  Plugins/Feeds Configuration .................................................................................................................. 22

Diagnostics ............................................................................................................................................. 24

Job Queue .............................................................................................................................................. 25

System Logs .......................................................................................................................................... 26

Publishing Sites ..................................................................................................................................... 26

Keys ....................................................................................................................................................... 28
  Remote LCE Key Exchange .................................................................................................................. 29

SSL Client Certificate Authentication .................................................................................................... 29
  Configure SecurityCenter for Certificates ......................................................................................... 30
  Connect with SSL Certificate Enabled Browser ................................................................................. 30

Resource Management ............................................................................................................................ 32
  Nessus Scanners ................................................................................................................................. 32
    Adding a Nessus Scanner .................................................................................................................. 34
    Configure SecurityCenter for Custom Certificates to Verify Hostname .......................................... 35
  Nessus Cloud Scanners ....................................................................................................................... 36
  Nessus Scanner Details ......................................................................................................................... 38
Deleting a Nessus Scanner ................................................................. 39
Scan Zones .......................................................... 39
Passive Vulnerability Scanners .......................................................... 40
Log Correlation Engines ............................................................. 43
Log Correlation Engine Clients ..................................................... 46
Log Correlation Engine Client Policies ......................................... 47
Data Management ........................................................................ 48
Repositories .............................................................................. 48
IPv4/IPv6 (Local) Repository .......................................................... 49
Mobile (Local) Repository ............................................................ 50
Remote Repository ................................................................... 51
Offline Repository .................................................................... 52
Accept Risk Rules ...................................................................... 54
Recast Risk Rules ..................................................................... 55
User Management ....................................................................... 56
Organizations ........................................................................... 56
Users ......................................................................................... 59
Users ......................................................................................... 59
Administrators .......................................................................... 60
Roles ......................................................................................... 62
User Access Control .................................................................. 62
Scanning ...................................................................................... 62
Audit Files ................................................................................. 62
Credentials ................................................................................ 66
CyberArk Vault Options ............................................................. 69
Policies ...................................................................................... 69
Add a Scan Policy ...................................................................... 70
Template .................................................................................. 71
Advanced Scan .......................................................................... 71
Plugins ...................................................................................... 83
Troubleshooting .......................................................................... 86
SecurityCenter ........................................................................... 86
SecurityCenter does not appear to be operational ...................... 86
Forgot login credentials ............................................................. 86
Invalid license error .................................................................. 86
Reporting does not work ............................................................ 87
Appendix 3: Manual LCE Key Exchange

About Tenable Network Security ........................................................................... 90
Appendix 1: License Declarations ........................................................................ 91
Appendix 2: Manual LCE Key Exchange ................................................................. 92
Appendix 3: Nessus SSL Configuration ................................................................. 93

Introduction............................................................................................................ 93
Overview of SSL Certificates and Keys ................................................................. 93
Certificate Authority .............................................................................................. 93
Nessus Server ......................................................................................................... 93
Nessus Client ........................................................................................................... 93
Nessus Configuration for Unix ............................................................................... 94
Commands and Relevant Files ............................................................................... 94
Certificate Authority and Nessus Server Certificate ............................................ 94
Nessus Client Keys ................................................................................................ 94
Creating and Deploying SSL Authentication for Nessus ...................................... 95
Create Keys and User on Nessus Server .............................................................. 95
Create the nessuscert.pem Key ........................................................................... 97
Configure Nessus Daemons ................................................................................. 97
Change the Nessus Mode of Authentication ....................................................... 97
Using Custom Certificates .................................................................................... 98
Deploy to Other Nessus Scanners ....................................................................... 98
Nessus Configuration for Windows ....................................................................... 99
Commands and Relevant Files ............................................................................ 99
Introduction

This document describes the administrative functions of Tenable Network Security's SecurityCenter 5.

Since many of Tenable's customers have requirements to maintain separation of duties, the SecurityCenter 5.0 documentation has been separated into the following documents to better organize the material based on the organizational role. Note that there is some overlap in roles as well as content provided with each of the following guides:

- **SecurityCenter 5.0 Installation Guide** – This document provides instructions for the installation of SecurityCenter 5. 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 5.0 Upgrade Guide** – This document describes the process of upgrading to version 5.0 of SecurityCenter.

- **SecurityCenter 5.0.1 Upgrade Guide** – This document describes the process of upgrading to version 5.0.1 of SecurityCenter.

- **SecurityCenter 5.0 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 5.0 User Guide** – This document provides instructions for using SecurityCenter by a Security Manager user or lesser account.

Please email any comments and suggestions 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 examples may or may not include the command line prompt and output text from the results of the command. Command line examples will display the command being run in **courier bold** to indicate what the user typed while the sample output generated by the system will be indicated in **courier** (not bold). Following is an example running of the Unix `pwd` command:

```
# pwd
/opt/sc/daemons
#
```

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

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

The following abbreviations are used throughout this documentation:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>SC</td>
<td>SecurityCenter</td>
</tr>
<tr>
<td>LCE</td>
<td>Log Correlation Engine</td>
</tr>
<tr>
<td>PVS</td>
<td>Passive Vulnerability Scanner</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection System</td>
</tr>
</tbody>
</table>

SecurityCenter 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
- Manage Log Correlation Engine Client configurations
- Delete accept and recast risk rules created by organizational users
- Manage what external data feeds (SecurityCenter Feed, Event Plugins, PVS plugins, and Nessus plugins) 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 queue

Starting/Halting SecurityCenter

When SecurityCenter is installed, 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 (Jobd.php httpd) 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 Home Page/Dashboard**

To navigate within the SecurityCenter user interface the preferred method is to use the menu within the web interface, not the browser’s back and forward arrow buttons.

**Supported Platforms**

The SecurityCenter user interface uses HTML5 and is best-experienced using at least the minimum version specified of the following browsers:

- Internet Explorer 10
- Firefox 32
- Chrome 37
- Safari 7.1

**Launch SecurityCenter**

To launch SecurityCenter, bring up a supported web browser on a system that has access to the SecurityCenter’s network address space and enter the URL in the following format using SecurityCenter’s IPv4 or IPv6 address or hostname:

https://<SERVER ADDRESS OR NAME>/

The SecurityCenter web interface is available using a secure web connection (https). SecurityCenter does not listen on port 80. TLS 1.0 must be enabled by the browser in order to complete the secure connection to SecurityCenter.

The dashboard is the first screen displayed when you log into the SecurityCenter user interface. It displays scanner, repository, LCE, and plugin data through predefined components. The Dashboard can also be displayed by selecting “Dashboard” from the “Home” tab. There are two options from the switch dashboard drop-down menu: “Overview” and “LCE Overview”. The Overview page contains a Scanner Status table, a Repository Statistics table, and a table containing the latest plugin feed updates. The System Status section of the dashboard is interactive. The Job Daemon’s status is displayed and may be started or stopped by clicking the appropriate link. The LCE Overview page lists the LCE servers and the status of clients attached to the LCE server (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 to configure the desired SecurityCenter system behavior. When logged in as an admin user, additional options are available, which are not available for non-admin users. Among the available admin options after selecting “Configuration” from the menu is "License", "Mail", "LDAP", "Data Expiration", "External Schedules", "Security", "Plugins / Feed" and "Miscellaneous". The sections below provide details about each of the categories and their configuration items.

License

The "License" options allow the admin user to configure the licensing and Activation Code settings for SecurityCenter and the attached Tenable products. The screen capture below shows a sample default SecurityCenter License configuration page:
This page will rarely need to be modified by the administrator. It contains two sections, the SecurityCenter license and the Additional Licenses section. This page will only be changed manually when a new or upgraded Activation Code for Nessus, PVS, or LCE has been purchased by the organization.

Offline repositories are not counted against the IP license count. Also, the following plugins are not counted against the license IP count when scanned using the Ping Host port scanner. Using other port scanners will cause the detected IPs to be counted against the license:

Nessus IDs: 10180, 10287, 19506, 12053, 11933, 11936
PVS IDs: 00003, 00012
LCE IDs: 800,000-800,099
To add a new license, use the “Choose File” button next to the “License File” field to locate the license key file (sent by Tenable via email) and then click “Submit”. Once a valid license is applied, a green field is displayed indicating a valid license and several informational fields will be shown. The fields indicate the name of the licensee, the type of license, the hostname of the SecurityCenter server, the license expiration date, IP count in use, and the maximum number of IPs allowed by the license.

For SecurityCenter installations, a valid Nessus Activation Code must also be entered to register any Nessus scanners used by SecurityCenter. A valid LCE Activation Code must be entered to download the LCE Event vulnerability plugins to SecurityCenter. A valid PVS Activation Code is required to use and manage attached PVS scanners. The Activation Codes are hyphen delimited alpha-numeric strings that enable SecurityCenter to download plugins and update Nessus scanner plugins. The LCE Activation Code allows SecurityCenter to download event plugins, but does not manage plugin updates for LCE servers. After uploading a valid license key and entering a valid Activation Code(s), click “Next” to continue.

A with + sign with a grey background indicates that there has not been a license applied for the product. A green box with a checkmark in it indicates a valid code is entered. A red box with an X indicates an invalid code. Clicking on the symbol will reveal an area to either add or reset the Activation Code. Once a new code has been entered into the text box and registered, it will indicate as valid or invalid.

A plugin download is initiated in the background. This plugin download can take several minutes and must complete before any Nessus scans are initiated. Once the plugin update has occurred, the “Last Updated” date and time are updated on the “Plugins” screen.

Mail

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

The “Return Address” defaults to “noreply@localhost”. Use a valid return email address for this field. If this field is empty or the email server requires emails from valid accounts, the email will not be sent by the email server.
LDAP

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 services becomes unreachable.

LDAP configuration settings enable 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 mandated by security policy. After selecting "LDAP", a page similar to the one below is displayed.
Fill out the LDAP configuration settings as provided by the LDAP server administrator and click “Test LDAP Settings” to confirm the validity of the settings.
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>Server Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Hostname</td>
<td>Enter the IP address or DNS name of the LDAP server in this field.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the remote LDAP port here. When Encryption is set to “none”, the LDAP port is typically 389, and when TLS or LDAPS is used, port 636 is the typical setting. Confirm the selection with your LDAP server administrators.</td>
</tr>
<tr>
<td>Encryption</td>
<td>This selection indicates if Transport Layer Security (STARTTLS) or LDAP over SSL (LDAPS) is used for communication with the LDAP server.</td>
</tr>
<tr>
<td>Username</td>
<td>If the LDAP server requires credentials to search for user data, then the &quot;Username&quot; and &quot;Password&quot; fields are required. By default, if an Active Directory server is used for LDAP queries, it 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 server requires credentials to search for user data, then the &quot;Username&quot; and &quot;Password&quot; fields are required. By default, many LDAP servers require an authenticated search. It is recommended to use passwords that meet stringent length and complexity requirements.</td>
</tr>
<tr>
<td><strong>LDAP Schema Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Base DN</td>
<td>This is the LDAP search base used as the starting point to search for the user information.</td>
</tr>
<tr>
<td>User Object Filter</td>
<td>This string may be modified to create a search based on a location or filter other than the default search base or attribute.</td>
</tr>
<tr>
<td><strong>User Schema Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Username Attribute</td>
<td>This is the attribute name on the LDAP server that contains the username for the account. This is often specified by the string “sAMAccountName” in Active Directory servers that may be used by LDAP. 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 server that contains the email address for the account. This is often specified by the string “mail” in Active Directory servers that may be used by LDAP. 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 server that contains the telephone number for the account. This is often specified by the string “telephoneNumber” in Active Directory servers that may be used by LDAP. Contact your local LDAP administrator for the correct telephone attribute to use.</td>
</tr>
</tbody>
</table>
Name Attribute

This field is the attribute name on the LDAP server that contains the name associated with the account. This is often specified by the string "CN" in Active Directory servers that may be used by LDAP. Contact your local LDAP administrator for the correct name attribute to use.

Access to Active Directory is performed via AD's LDAP mode. When using multiple AD domains, LDAP access may be configured to go through the Global Catalog. Port 3268 is the default non-SSL/TLS setting, while port 3269 is used for SSL/TLS connections by default. More general information about LDAP searches via the Global Catalog may be found at: http://technet.microsoft.com/en-us/library/cc728188(v=ws.10).aspx.

Data Expiration

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>Active</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 one (1). Setting this field to zero will remove all active vulnerabilities daily.</td>
</tr>
<tr>
<td>Passive</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 one (1). Setting this field to zero will remove all passive vulnerabilities daily.</td>
</tr>
<tr>
<td>Event</td>
<td>SecurityCenter will automatically remove any event vulnerability data that was discovered via LCE log 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 one (1). Setting this field to zero will remove all event vulnerabilities daily.</td>
</tr>
<tr>
<td>Compliance</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 one (1). Setting this field to zero will remove all compliance vulnerabilities daily.</td>
</tr>
<tr>
<td>Mitigated</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 one (1). Setting this field to zero will remove all mitigated vulnerability data daily.</td>
</tr>
<tr>
<td>Closed Tickets</td>
<td>Automatically remove any closed tickets after the designated number of days. The default value of this field is 365.</td>
</tr>
<tr>
<td>Scan Results</td>
<td>Automatically remove any scan results after the designated number of days. The default value of this field is 365.</td>
</tr>
<tr>
<td>Report Results</td>
<td>Automatically remove any report results after the designated number of days. The default value of this field is 365.</td>
</tr>
</tbody>
</table>
External Schedules

The SecurityCenter external schedule settings are used to determine the update schedule for the common tasks of pulling passive scanner data, IDS signature updates, and IDS correlation updates.

The following settings are available:

Table 3 – Update Schedules

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pull Interval</td>
<td>This option configures the interval that SecurityCenter will use to pull results from the attached PVS servers. The default setting is 1 hour. The timing is based from the start of the SecurityCenter service on the host system.</td>
</tr>
<tr>
<td>IDS Signatures</td>
<td>Frequency to update SecurityCenter IDS signatures via third-party sources.</td>
</tr>
<tr>
<td>IDS Correlation Databases</td>
<td>Frequency to push vulnerability information to the LCE for correlation.</td>
</tr>
</tbody>
</table>

Each of the update schedule times may also be configured to occur by time in a particular time zone, which can be selected via the "Time Zone" link next to each hour selection.

Security

The "Security" section defines the SecurityCenter web interface login parameters and options for account logins. Banners, headers, and classification headers and footers can also be configured from this screen.
Use the table below to determine correct values for your environment:

**Table 4 - SecurityCenter Authentication Settings**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 user 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>Minimum Password Length</td>
<td>This setting defines the minimum number of characters for passwords of accounts created using the local TNS authentication access (default:3).</td>
</tr>
<tr>
<td>Startup Banner Text</td>
<td>Enter the text banner that is displayed prior to the login interface.</td>
</tr>
<tr>
<td>Header Text</td>
<td>Adds custom text to the top of the SecurityCenter screen. The text may be used to identify the company, group, or other organizational information. The field is limited to 128 characters.</td>
</tr>
</tbody>
</table>
**Classification Type**

Adds a header and footer banner to SecurityCenter to indicate the classification of the data accessible via the software. Current options are "None", "Unclassified", "Confidential", "Secret", "Top Secret", and "Top Secret – No Foreign".

When set to an option other than "None", the available report style for users will only show the "plain" report style types. The Tenable report styles do not support the classification banners.
Miscellaneous Configuration

The Miscellaneous Configuration area offers options to configure settings for web proxy, syslog, notifications, and enable or disable a variety of reporting types that are encountered and needed only in specific situations.

From this configuration page, a web proxy can be configured by entering the host URL (proxy hostname or IP address), port, authentication type, username, and password. The host name used must resolve properly from the SecurityCenter host.

The “Syslog” section allows for the configuration and sending of SecurityCenter log events to the local syslog service. When “Enable Forwarding” is enabled, the forwarding options are made available for selection. The “Facility” text entry box provides the ability to enter the desired facility that will receive the log messages. The “Severities” section determines which level(s) of syslog messages will be sent: “Informational”, “Warning”, and/or “Critical” by selection checkboxes.
The "Notifications" field defines the SecurityCenter web address used when notifications are generated for alerts and tickets.

Among the reporting standards for the Defense Information Systems Agency (DISA) are the Asset Report Format (ASR) and the Assessment Results Format (ARF) styles. Additionally, there is CyberScope reporting utilizing Lightweight Asset Summary Results Schema (LASR) style reports used by some segments of governments and industry. These formats are typically used only by select groups and organizations for specific needs that do not apply to many organizations. The ability to enable or disable their usage within SecurityCenter is controlled here. Selecting the checkbox will enable the reporting type and unselecting will disable the reporting type in the report type drop-down for SecurityCenter users.

Plugins/Feeds Configuration

The Feeds option displays information about the SecurityCenter feeds and plugin sets including the update schedule, a link to update the plugins either through SecurityCenter or by manually uploading plugins. The displayed feeds are for SecurityCenter Feed, Active Plugins, Passive Plugins, and Event Plugins. Only feeds with valid Activation Codes will be able to be updated.
Plugins are scripts used by the Nessus, PVS, and LCE servers to interpret vulnerability data. For ease of operation, Nessus and PVS plugins are managed centrally by SecurityCenter and pushed out to their respective scanners. LCE servers download their own event plugins and SecurityCenter downloads event plugins for its local reference. SecurityCenter does not currently push event plugins to LCE servers.

Clicking on "Upload Plugins" opens a file selection window that allows the user to choose an active, passive, event, or custom plugin file. All custom plugins must have unique Plugin ID numbers and have family associations based on existing SecurityCenter families.

Custom plugin uploads must now be a complete “feed”. In order to upload custom plugins the provided tar.gz file must include the relevant NASLs and a "custom_feed_info.inc" file comprised of the following two lines:

PLUGIN_SET = "201202131526";
PLUGIN_FEED = "Custom";

The administrator must manage this file and update the PLUGIN_SET option for each upload. The PLUGIN_SET format is “YYYYMMDDHHMM”.

For example, running the following command against the "custom_feed_info.inc" file and custom plugins in a directory will create a new tar and gzipped uploadable archive file called custom_nasl_archive.tar.gz that contains both custom plugins:

```
# tar -cvzf custom_nasl_archive.tar.gz custom_feed_info.inc *.nasl
```

It is recommended that the custom_nasl_archive.tar.gz file be updated for each addition and update of custom NASLs.
Diagnostics

The System menu contains a drop-down that includes Diagnostics. This page displays and creates information that assists in troubleshooting issues that may arise while using SecurityCenter.

In the “System Status” section, the following items are indicated by a green check mark for a properly working status. A red “X” icon is displayed when the item is in a critical state.

Table 5 – System Status

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correct Java Version</td>
<td>The icon is red when a minimal version of Java is not installed as required by certain SecurityCenter features.</td>
</tr>
<tr>
<td>Sufficient Disk Space</td>
<td>Once the disk that stores the SecurityCenter data is within 5% of being filled, the icon indicator will turn red.</td>
</tr>
<tr>
<td>Correct RPM Package Installed</td>
<td>This indicator is green when the correct RPM is installed for the OS architecture on which it is running.</td>
</tr>
</tbody>
</table>

The “Diagnostics File” section is used primarily when working with the Tenable Support team. In order to troubleshoot issues that may be encountered, the Support team may request that a diagnostics file be generated with one or more of the “Diagnostics File Chapters” selected. Clicking the “Generate Diagnostics File” button will open a page to set the options to be included in the diagnostic file. If selected, the “Strip IPs from Chapters” option will remove IP addresses from the log files before generating the diagnostics file.
Job Queue

Job Queue is a feature of SecurityCenter that allows specified events to be displayed in a list for review.

Job Queue notifications can be viewed and sorted in several ways by clicking on the desired sort column. Using the gear icon menu next to an item, that item may be viewed for more detail or, if the job is running, the process may be killed. Killing a process should be done only as a last resort, as killing a process may have undesirable effects on other SecurityCenter processes.
System Logs

SecurityCenter logs contain detailed filter options to troubleshoot unusual system or user activity. The logs include filters that allow users to search logs based on parameters such as Date, Initiator, Keyword, Module, and Severity.

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.

Publishing Sites

Organizations may configure publishing sites as targets to send report results to a properly configured web server or a Defense Information Systems Agency (DISA) Continuous Monitoring and Risk Scoring (CMRS) site.
Configuring the publishing sites starts with clicking the “Add a Publishing Site” link to open the “Add Publishing Site” window as shown below:

![Add Publishing Site Window](image)

### Table 6 – Publishing Site Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the publishing site.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the publishing site.</td>
</tr>
<tr>
<td>Type</td>
<td>This is the method SecurityCenter will use to publish to the site. Available options are “HTTP Post” or “CMRS”. Use the selection appropriate for the configuration of the publishing site.</td>
</tr>
<tr>
<td>URI</td>
<td>This is the target address to send the report to when completed.</td>
</tr>
<tr>
<td>Authentication</td>
<td>There are two methods of authentication available: “SSL Certificate” and “Password”. When “SSL Certificate” is selected, the option to upload a certificate is available. When “Password” is selected, fields are available to enter a username and password to authenticate to the publishing server.</td>
</tr>
<tr>
<td>Organizations</td>
<td>This field allows for selecting the Organization(s) that are allowed to publish to the configured site.</td>
</tr>
</tbody>
</table>
Keys

From the System menu one of the drop-down options is for Keys. 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 to perform a key exchange before the repository add/sync occurs.

From the "Options" drop-down the SecurityCenter key may be downloaded in a DSA or RSA format. After selecting the option, the key format dialog is displayed. Choose the type of key being requested and then click "Download":

If "DSA" was chosen during download, the DSA public key is downloaded. Likewise, choosing "RSA" downloads the RSA public key string.

Clicking on "Add" brings up the dialog box below:
In the “Type” drop-down, select DSA or RSA as the key type.

In the “Comment” box, enter an optional string of text that describes the purpose of the key being added to the system.

In the “Public Key” box, paste the text of the public key from the remote SecurityCenter and click "Submit".

**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.

**SSL Client Certificate Authentication**

SecurityCenter allows users to use SSL client certificate authentication. This allows use of SSL client certificates, smart cards, personal identity verification (PIV) cards, and common access card (CAC) authentication when the browser is configured for this method.

By default, SecurityCenter uses a password to authenticate. To configure SecurityCenter to allow SSL client certificate authentication the web server must be changed to allow such connections. To do this, the /opt/sc/support/conf/sslverify.conf file must be edited on the SecurityCenter server using any standard text editor. Edit the “SSLVerifyClient” setting to use an option of none, optional, and require as described in the following table.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>When set to &quot;none&quot;, SSL certificates for SecurityCenter will not be accepted by the server for user authentication purposes. This is the default setting for SecurityCenter.</td>
</tr>
<tr>
<td>optional</td>
<td>When set to “optional”, valid SSL certificates for SecurityCenter may be used for user authentication. If a valid certificate is not presented, the user may log in using only a password.</td>
</tr>
<tr>
<td>require</td>
<td>When set to “require”, a valid SSL certificate for SecurityCenter must be presented to gain access to the web interface. If the user has an account that uses a certificate to authenticate, that user will be logged into SecurityCenter. Otherwise the user will be presented with the standard SecurityCenter login page.</td>
</tr>
</tbody>
</table>

When a user is initially created and configured, a password must be created for the user. Users who are configured to use SSL certificates will be prompted to determine if they want to always use the current certificate when they log in to SecurityCenter through a browser. If “Yes” is selected, the certificate will be associated with their account and future access to SecurityCenter will use the client certificate. If “No” is selected, the certificate will be ignored for the current session.

**Configure SecurityCenter for Certificates**

The first step to allow SSL certificate authentication is to configure the SecurityCenter web server. This process allows the web server to trust certificates created by the Certificate Authority (CA) for authentication.

1. Copy the required PEM-encoded CA certificate (and intermediary CA, if needed) to the SecurityCenter server’s /tmp directory. For this example, the file is named `ROOTCA2.cer`.

2. Run the `installCA.php` script to create the required files for each CA in `/opt/sc/data/CA` as follows:

```
# /opt/sc/support/bin/php /opt/sc/src/tools/installCA.php /tmp/ROOTCA2.cer
```

3. Once each of your CAs has been processed, restart the SecurityCenter services with the following command:

```
# service SecurityCenter restart
```

After SecurityCenter has been configured with the proper CA certificate(s), users may log in to SecurityCenter using SSL client certificates.

**Connect with SSL Certificate Enabled Browser**

The following information is provided with the understanding that your browser is configured for SSL certificate authentication. Please refer to your browser’s help files or other documentation to configure this feature.

The process to configure a certificate login begins when a user connects to SecurityCenter for the first time. The process is completed by the user and does not require Administrator intervention.

1. Launch a browser and navigate to SecurityCenter.
2. The browser will present a list of available certificate identities to select from:

3. Once a certificate has been selected, a prompt for the PIN or password for the certificate is presented (if required) to access your certificate. When the PIN or password is successfully entered, the certificate will be available for the current session with SecurityCenter.

4. Upon the initial connection, log in using the username to be associated with the selected certificate.

   Only one SecurityCenter user may be associated with a single certificate. If one user holds multiple user names and roles, a unique certificate must be provided for each login name.

5. Once logged in, a window titled “Certificate Authentication” is presented, asking if the current certificate is to be used to authenticate the current user. If “Yes” is selected, the certificate will be associated with this user. If “No” is selected, the certificate will be ignored for the current session.

   If the user’s browser is configured for certificate authentication but is not configured for a SecurityCenter user, the following prompt will be presented for each login.

6. When a user’s account is associated with a certificate, it is displayed on the user’s profile page.
7. If a user's certificate changes or is required to be revoked, the current certificate may be disassociated from the user by clicking the "Clear Certification Details" button.

8. If a new certificate is available the next time the user logs in, SecurityCenter will again attempt to associate the user with the certificate.

If you log out of the session, you will be presented with the standard SecurityCenter login screen. If you wish to log in again with the same certificate, refresh your browser window. If you need to use a different certificate, you must restart your browser session.

Resource Management

The Resources page 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 "Resources" and then "Nessus Scanners" to retrieve a list of the scanners including their name, current status, version, host, uptime, type, and when they were last modified. If the status of a scanner is believed to have changed recently (since visiting the page), click the "Update Status" button within the "Options" drop-down to see the latest scanner status between its auto-refresh interval. The gear icon to the right of the scanner information provides a drop-down menu to view information, edit the configuration, or delete the scanner.

There are three classifications of Nessus scanners that may be added to SecurityCenter: "Managed", "Unmanaged", and "Nessus Cloud".

A "Managed" scanner is one that is managed by SecurityCenter. Managed scanners are logged into using Nessus admin credentials, and SecurityCenter has the ability to send plugin updates to the scanner. SecurityCenter also maintains the Activation Code for Managed scanners.

An "Unmanaged" scanner is one that has been logged into using a standard Nessus user's credentials. This scanner may be used to perform a scan but SecurityCenter cannot send plugin updates to an unmanaged scanner or manage its Activation Code.

SecurityCenter may also use a "Nessus Cloud" scanner to perform scans using Tenable's Nessus Cloud. This is a vulnerability scanning service that may be used to audit Internet facing IP addresses for both network and web application vulnerabilities "from the cloud". A Nessus Cloud scanner is considered to be an unmanaged scanner and therefore SecurityCenter will not push plugin updates to a Nessus Cloud scanner. More information about using the Nessus Cloud through SecurityCenter is found in the Nessus Cloud Scanners section of this document.

In the examples below, the Nessus scanners are installed on remote systems and are functioning properly.
### Nessus Scanners

<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>Host</th>
<th>Version</th>
<th>Type</th>
<th>Uptime</th>
<th>Last Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Working</td>
<td></td>
<td>6.3.3</td>
<td>Unmanaged</td>
<td>18 Days</td>
<td>4 days ago</td>
</tr>
<tr>
<td></td>
<td>Working</td>
<td></td>
<td>6.2.4</td>
<td>Unmanaged</td>
<td>7 Days</td>
<td>Mar 31, 2015 14:21</td>
</tr>
<tr>
<td></td>
<td>Working</td>
<td></td>
<td>6.3.4</td>
<td>Nessus Cloud</td>
<td>2 Days</td>
<td>Mar 24, 2015 10:42</td>
</tr>
<tr>
<td></td>
<td>Working</td>
<td></td>
<td>6.3.4</td>
<td>Nessus Cloud</td>
<td>14 Hours</td>
<td>Mar 24, 2015 10:40</td>
</tr>
<tr>
<td></td>
<td>Working</td>
<td></td>
<td>5.2.8</td>
<td>Unmanaged</td>
<td>18 Days</td>
<td>Mar 18, 2015 12:45</td>
</tr>
<tr>
<td></td>
<td>Working</td>
<td></td>
<td>6.3.3</td>
<td>Managed</td>
<td>12 Days</td>
<td>Mar 10, 2015 21:39</td>
</tr>
<tr>
<td></td>
<td>Working</td>
<td></td>
<td>6.3.3</td>
<td>Unmanaged</td>
<td>12 Days</td>
<td>Mar 04, 2015 13:24</td>
</tr>
</tbody>
</table>
Adding a Nessus Scanner

To add a scanner, click the “Add” button. Items with a star (*) next to them indicate information that is required that does not have a default setting. A screen capture of the “Add Scanner” dialog is shown below:

The table below provides details about the available options for adding a Nessus scanner:

<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>Host</td>
<td>Hostname or IP address of the scanner.</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Port</td>
<td>TCP port that the Nessus scanner listens on for communications from SecurityCenter. The default is port 8834.</td>
</tr>
<tr>
<td>Enabled</td>
<td>A scanner may be &quot;Enabled&quot; or &quot;Disabled&quot; within SecurityCenter to allow or prevent access to the scanner.</td>
</tr>
<tr>
<td>Verify Hostname</td>
<td>Adds a check to verify that the hostname or IP address entered in the &quot;Host&quot; field matches the CommonName (CN) presented in the SSL certificate from the Nessus server.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>Instructs SecurityCenter to use its configured proxy for communication with the scanner.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Select Password or SSL Certificate for the authentication type to connect to the Nessus scanner. For detailed SSL Certificate configuration options, see Appendix 3: Nessus SSL Configuration.</td>
</tr>
<tr>
<td>Username</td>
<td>Username generated during the Nessus install for daemon to client communications. This must be an administrator user in order to send plugin updates to the Nessus scanner. If the scanner will be updated by a different method, such as through another SecurityCenter, a standard Nessus user account may be used to perform scans. This field is only available if the Authentication Type is set to &quot;Password&quot;.</td>
</tr>
<tr>
<td>Password</td>
<td>The login password must be entered in this field. This field is only available if the Authentication Type is set to &quot;Password&quot;.</td>
</tr>
<tr>
<td>Certificate</td>
<td>This field is available if the Authentication Type is &quot;SSL Certificate&quot;. Select the &quot;Browse&quot; button, choose a SSL Certificate file to upload, and upload to the SecurityCenter. For more information, see Appendix 3: Nessus SSL Configuration.</td>
</tr>
<tr>
<td>Zones</td>
<td>The zone(s) within SecurityCenter that will have access to use this scanner.</td>
</tr>
</tbody>
</table>

**Configure SecurityCenter for Custom Certificates to Verify Hostname**

The first step to allow the Verify Hostname to work is to ensure the correct Certificate Authority (CA) certificate is configured for use by SecurityCenter. When using the default certificates for Nessus servers, this is not required to be done. Only when a custom CA is in use do these steps need to be performed.

1. Copy the required PEM-encoded CA certificate (and intermediary CA, if needed) to the SecurityCenter server’s /tmp directory. For this example, the file is named `ROOTCA2.cer`.
2. Run the `installCA.php` script to create the required files for each CA in `/opt/sc/data/CA` as follows:
   ```bash
   # /opt/sc/support/bin/php /opt/sc/src/tools/installCA.php /tmp/ROOTCA2.cer
   ```
3. Once each of your CAs has been processed, restart the SecurityCenter services with the following command:
   ```bash
   # service SecurityCenter restart
   ```

After SecurityCenter has been configured with the proper CA certificate(s), the Verify Hostname will verify the SSL certificate presented against the proper CA certificate.
Nessus Cloud Scanners

SecurityCenter supports the use of the **Nessus Cloud** as a Nessus scanner within SecurityCenter. The Nessus Cloud is an enterprise-class remote vulnerability scanning service that may be used to audit Internet facing IP addresses for both network and web application vulnerabilities "from the cloud". While they are not “managed” by a SecurityCenter (e.g., plugins are not pushed from SecurityCenter to the scanner), Nessus Cloud scanners can be added to SecurityCenter in the same manner that internal, local, or remote Nessus scanners are added.
To add a Nessus Cloud scanner to SecurityCenter, a valid and active Nessus Cloud subscription must be used. In SecurityCenter, select the “Resources” tab, “Nessus Scanners”, and then “Add”:

Enter a name (mandatory) and description (optional) for the Nessus Cloud scanner to be used with SecurityCenter. Enter the address cloud.tenable.com as “Host”, with the “Port” specified as 443 (HTTPS). Enter a valid Nessus Cloud username and password for authentication and select the zone(s) within SecurityCenter that will use the Nessus Cloud scanner. When finished, click “Submit” to add the authorized Nessus Cloud scanner to SecurityCenter. If successful, the Nessus Cloud scanner will be listed under “Nessus Scanners” with a status of “Working”: 
Note that existing scan reports from the Nessus Cloud are not automatically made available through SecurityCenter, but they can be manually downloaded and imported into SecurityCenter by users with permissions to do so.

**Nessus Scanner Details**

When the “View” button is clicked from the gear icon menu, information about the selected scanner is displayed. The information includes the basic information of name, description, IP address or hostname, port, username used to connect to the scanner, uptime, and when the scanner was created and last modified from SecurityCenter. The Nessus scanner version, web server version, type, and zones it is a part of are also displayed. The number of active scans (load) the server is performing is displayed and updated every 15 minutes, as well as the current loaded plugin set on the scanner.
Deleting a Nessus Scanner

In some cases it may be necessary to delete a configured Nessus scanner from SecurityCenter. When this must be done, select the gear icon next to the scanner to be deleted and select the “Delete” option from the menu. This will open a confirmation window asking to confirm the deletion of the scanner by its name. Select the “Delete” button to remove the scanner or the “Cancel” button or the “X” at the top right to not delete the selected scanner.

Scan Zones

Scan Zones define the IP ranges associated with the scanner along with organizational access. SecurityCenter allows defined 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(s) 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 “All Zones” 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 “All Zones” zone, the targets for the scan will be given to scanners in the most appropriate zone available 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:

There are four items to configure for a Scan Zone. Each zone contains a Name, optional Description, IP range(s) to be covered by the zone, and the Nessus scanner(s) used by the zone for scanning. The ranges are entered using CIDR or range notations with multiple ranges separated by commas. The scanners are selected by checking the box next to the scanner name. When hovering over a scanner name, an information icon is displayed. Hovering over this icon will display scanner information including its name, description, host, version, and current status.

Once configuration is complete, clicking the "Submit" button will create the new scan zone for use within SecurityCenter. This will return you to the Scan Zones page.

**Passive Vulnerability Scanners**

Tenable's Passive Vulnerability Scanner (PVS) is a patented network discovery and vulnerability analysis software solution, that delivers 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.

SecurityCenter communicates with PVS 4.0 or higher utilizing the XMLRPC protocol on port 8835 by default.

SecurityCenter will ask the PVS for the latest (if any) vulnerability report once every hour by default. The pull interval may be changed under the System Configuration page under the Update tab.

By default, SecurityCenter will check every 24 hours to see if any new passive vulnerability plugins have been downloaded from Tenable and will push them out to each PVS scanner. SecurityCenter must have a valid PVS Activation Code to retrieve plugin updates from Tenable and send plugin updates to the attached PVS scanners.

The screen capture below shows a listing of working PVS scanners:
To configure one or more of Tenable’s PVS servers, under the "Resources" menu select "Passive Vulnerability Scanners". This will produce a list of all configured PVS devices by name, their host, version, status, uptime, and the last time of the last retrieved report. Selecting the "Update Status" button from the Options menu will initiate a connection from SecurityCenter to obtain and refresh the status of the PVS scanners.
To add a scanner, click the "Add" button. Items with a star (*) next to them indicate information that is required that does not have a default setting. A screen capture of the "Add Scanner" dialog is shown below:

![Add Passive Vulnerability Scanner dialog](image)

The table below provides details about the available options for adding a Nessus scanner:

**Table 9 – PVS Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Descriptive name for the PVS scanner.</td>
</tr>
<tr>
<td>Description</td>
<td>Scanner description, location, or purpose.</td>
</tr>
<tr>
<td>Host</td>
<td>Hostname or IP address of the scanner.</td>
</tr>
<tr>
<td>Port</td>
<td>TCP port that the PVS scanner listens on for communications from SecurityCenter. The default is port 8835.</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>State</td>
<td>A scanner may be marked as “Enabled” or “Disabled” within SecurityCenter to allow or prevent access to the scanner.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Select Password or SSL Certificate for the authentication type to connect to the PVS scanner.</td>
</tr>
<tr>
<td>Username</td>
<td>Username generated during the PVS install for daemon to client communications. This must be an administrator user in order to send plugin updates to the PVS scanner. This field is only available if the Authentication Type is set to “Password”.</td>
</tr>
<tr>
<td>Password</td>
<td>The login password must be entered in this field. This field is only available if the Authentication Type is set to “Password”.</td>
</tr>
<tr>
<td>Certificate</td>
<td>This field is available if the Authentication Type is “SSL Certificate”. Select the &quot;Browse&quot; button, choose a SSL Certificate file to upload, and upload to the SecurityCenter.</td>
</tr>
<tr>
<td>Verify Hostname</td>
<td>Adds a check to verify that the hostname or IP address entered in the “Host” field matches the CommonName (CN) presented in the SSL certificate from the PVS server.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>Instructs SecurityCenter to use its configured proxy for communication with the scanner.</td>
</tr>
<tr>
<td>Repositories</td>
<td>The repositories which this PVS scanner will save its data to. If PVS will be reporting IPv4 and IPv6 data, at least two repositories (one for IPv4 and one for IPv6 data) must be selected.</td>
</tr>
</tbody>
</table>

SecurityCenter will add all data collected by a PVS to the repository(s) that are configured for it. Therefore it is important for the PVS to restrict the data it is collecting to only the desired IP range(s). For example, if the attached PVS collects information on 1100 hosts and the SecurityCenter is licensed for only 1000 hosts, SecurityCenter will import all of the collected data and indicate that the host count has exceeded the licensed amount of hosts.

**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. LCE also has the ability to analyze logs for vulnerabilities and allows SecurityCenter to retrieve the data. Since LCE is closely integrated with SecurityCenter, log analysis and vulnerability management can be centralized for a complete view of an organization’s security posture.

SecurityCenter performs vulnerability, compliance, and event management, but does not directly receive logs or IDS/IPS events. Combining the LCE with SecurityCenter does all of this by processing the events with the LCE and then passing the results on to SecurityCenter.

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 “Add” to display the dialog in the screen capture below. Default viewable fields include Name, Description, Host, Organizations, and an unselected switch for Import Vulnerabilities. When the Import Vulnerabilities option is selected, additional fields become available for Repositories selection and Port, Username, and Password settings.

LCE servers generate vulnerability logs. Enabling the Import Vulnerabilities option allows SecurityCenter to collect and import the vulnerability information from the LCE server. The Repositories area defines the repositories to receive the data. The Port, Username, and Password settings enable SecurityCenter to log into the LCE server to retrieve vulnerability information. The username and password are set when configuring the LCE server and is typically different than the system username and password used to configure the SSH key exchange described in the next section.

While configuring a LCE server there is a “Check Authentication” button. When clicked, SecurityCenter checks its ability to authenticate with the LCE server. If successful, a message will be displayed to acknowledge that fact. If the authentication fails, an option to enter a username and password to the LCE server is displayed. The user entered should have the ability to make changes on the remote system to enable the SSH key exchange between SecurityCenter and LCE. This is typically the root, root equivalent, or other high-level user on the LCE system. This is a one-time process to exchange SSH keys for secure communication between SecurityCenter and LCE. Once entered, click the “Push Key” button to initiate the transfer of the SSH Key. When successful, a checkbox and message will be displayed that the authentication is successful. If remote root or root equivalent user login is prohibited in your environment, refer to Appendix 2 for instructions on how to manually configure the LCE server using SSH key authentication.
Table 10 – 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>Host</td>
<td>IP address of the Log Correlation Engine.</td>
</tr>
<tr>
<td>Check Authentication</td>
<td>This button checks the status of the authentication between SecurityCenter and the LCE server.</td>
</tr>
<tr>
<td>Organizations</td>
<td>Determines which Organization(s) will be able to access data from the configured Log Correlation Engine.</td>
</tr>
</tbody>
</table>
Import Vulnerabilities  When enabled, allows Event vulnerability data to be retrieved from the configured LCE server.

Repositories  Select the appropriate SecurityCenter repository(ies) to store the imported LCE data.

Port  Enter the port that the LCE reporter is listening on the LCE host.

Username  Enter the reporter username used to authenticate to the LCE to retrieve vulnerability information.

Password  Enter the reporter password used to authenticate to the LCE to retrieve vulnerability information.

Log Correlation Engine Clients

The LCE server has the ability to manage configuration files for LCE 4.x clients remotely from the command line. SecurityCenter has the ability to manage the configuration files for LCE 4.x clients via a graphical interface.

The default view for the LCE Clients page displays all of the available clients for the selected LCE server in the "Filters" section, and may be changed by changing the LCE Server filter. Using the other filter options, the displayed clients for the selected server may be narrowed down by a mix of criteria based on combinations of the displayed columns.

LCE Client versions 4.0 and higher display information in the table including their name, host address, authorization status, client type, host OS, assigned policy file, date last updated, and client version. LCE Client configurations can be managed from SecurityCenter.

Note that configured clients prior to version 4.x are displayed on the list without OS and policy information. However, these clients cannot have their policy files centrally managed from SecurityCenter.

Each client may have a name assigned to it to help easily identify the client. The currently assigned name is displayed in the "Name" column. To change the name, click on the client to edit from the list, and enter the name. Client names may not contain spaces. Once set, click the "Submit" button to save the change.

LCE Clients are initially configured to send their data to a particular LCE server, but must be authorized by the LCE server for the server to accept the data. The client's authorization status is displayed in the left-side column. If there is no icon, the client is authorized to send data to the LCE server. If there is a broken link icon, the client is not authorized to send data to the LCE server. This may be toggled by selecting the gear icon for the client and clicking either the "Authorize" or "Revoke Authorization" from the list as appropriate.
Each client must have a policy assigned to it that specifies the appropriate data to send. The currently assigned policy is displayed in the "Policy" column. To change the assigned policy, click on the client to edit from the list, and select the appropriate policy from the drop-down list. The client policies may be searched by name by entering text into the Policy field. Once set, click the "Submit" button to save the change. The policy will be updated on the client on its next connection.

Log Correlation Engine Client Policies

The LCE Client Policies page contains a list of all the client policies currently available to be used by LCE clients. The list contains the name of the policy, the OS it is configured for use on, and the type of client the policy can be applied to.

Example policy files are available for use with the names default and beginning with "TNS-". These policy files may be used as is or exported to be used as a basis for custom policy files. The example files may be updated and changed at a later time without notice, so using them as is may return different results at a later date.

The "Add" button allows customized LCE Client policy files to be added to the LCE server and made available for use. The name field is appended to the beginning of the file name and is used to offer a description of the function or use of the policy file. The OS Type is used in the file name to easily identify the OS for which the policy is designed. The Client Type indicates
the LCE Client for which the policy is written. The Source field is used to select and upload the custom policy file or enter the policy file into the text field. Clicking the Submit button saves the policy file and sends it to the LCE server.

The “default” and “TNS” prefixes are only designed to be used by policies supplied by Tenable. Using “default” or “TNS” as a prefix for custom policy files may lead to them being overwritten or manipulated in undesired ways.

Selecting a policy and clicking the “Export” option from the gear menu will allow the policy to be saved to a local drive. The format of the file is XML and may be edited with standard text or XML editors.

Selecting a policy and clicking the “View” option from the gear menu displays the policy name and source of the policy in a window within SecurityCenter. The information cannot be edited from within this window.

For more information on creating LCE Client Policy files, please see the LCE Client Guide available 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 or mobile data types. 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. Repository data can also be shared between multiple SecurityCenters. Repositories are configured by the administrative user and made available to the Security Manager user to assign to users as needed. The maximum repository size is 32GB.

When creating SecurityCenter IPv4 or IPv6 repositories, LCE event source IP ranges must be included along with the vulnerability IP ranges or the event data and event vulnerabilities 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. Note that the “Type” column only displays when there are repositories other than Local.
Repository data collected from a remote or offline repository is static and used solely for reporting purposes.

Click the "Add" button to add a new repository. The sections below contain options for adding each type of repository.

IPv4/IPv6 (Local) Repository

These are the most common types of repositories used with SecurityCenter and store IPv4 and IPv6 data from active and passive scans. 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 IPv4 and IPv6 local repositories:

<table>
<thead>
<tr>
<th>Name</th>
<th>Vulnerability Count</th>
<th>IP/Device Count</th>
<th>Type</th>
<th>Last Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3015</td>
<td>3007</td>
<td>Offline (Mobile)</td>
<td>Apr 03, 2015 17:02</td>
</tr>
<tr>
<td></td>
<td>705</td>
<td>12</td>
<td>Remote (IPv6)</td>
<td>7 hours ago</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>Mobile</td>
<td>Never</td>
</tr>
<tr>
<td></td>
<td>361</td>
<td>1</td>
<td>IPv4</td>
<td>Never</td>
</tr>
<tr>
<td></td>
<td>10331</td>
<td>72</td>
<td>Remote (IPv4)</td>
<td>9 hours ago</td>
</tr>
</tbody>
</table>
### Table 11 – Local Repository Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The repository name.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the repository.</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td></td>
</tr>
<tr>
<td>IP Ranges</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>Access</strong></td>
<td></td>
</tr>
<tr>
<td>Organizations</td>
<td>Defines Organizations that have access to the vulnerability data within the repository. When initially selecting the Organization, a prompt will appear to either grant access to all the Groups within the Organization, or not. If granted, all Groups will be given access to the repository information. If denied, Groups within the Organization must explicitly be given access on a per Group basis.</td>
</tr>
<tr>
<td><strong>Advanced Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Generate Trend Data| 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 useful in cases where tracking data changes is important. In situations where repository datasets do not change frequently – negating the need for trending – disable this option to minimize disk space usage. |
| Days Trending      | Sets the number of days for the trending data to track.                                                                                     |
| Enable Full Text Search | Determines if the trending data presented is indexed for a full text search.                                                              |
| LCE Correlation    | Log Correlation Engine servers that will receive the vulnerability correlation information from this repository.                                |

### Mobile (Local) Repository

The Mobile repository is a local type that stores data from various MDM servers. The MDM servers currently supported as of this writing include ActiveSync, AirWatch MDM, Apple Profile Manager, Good MDM, and MobileIron. The table below describes configurable fields for mobile local repositories:
### Table 12 – Local Repository Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The repository name.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the repository.</td>
</tr>
<tr>
<td><strong>MDM</strong></td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>This setting determines if the repository will store ActiveSync, AirWatch MDM, Apple Profile Manager, Good, or MobileIron types of mobile data. The authentication settings available will vary depending on the type selected.</td>
</tr>
<tr>
<td>Scanner</td>
<td>This setting determines which Nessus scanner is used when scanning the MDM server. Only one Nessus scanner may be used to add data to the mobile repository.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Sets the schedule for the MDM server to be scanned to update the Mobile repository. On each scan, the current data in the repository is removed and replaced with the information from the latest scan.</td>
</tr>
<tr>
<td><strong>Access</strong></td>
<td></td>
</tr>
<tr>
<td>Organizations</td>
<td>Defines Organizations that have access to the vulnerability data within the repository. Within the &quot;Organizations&quot; section, selecting or deselecting the checkbox next to the Organization name grants or denies that Organization access to the repository information. When initially selecting the Organization, a prompt will appear to either grant access to all the Groups within the Organization, or not. If granted, all Groups will be given access to the repository information. If denied, Groups within the Organization must explicitly be given access on a per Group basis.</td>
</tr>
</tbody>
</table>

### Remote Repository

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 13 – Remote Repository Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The repository name.</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the repository.</td>
</tr>
</tbody>
</table>
Remote SecurityCenter

| Host | Host to synchronize with to obtain the repository data. After entering the IP address of the remote SecurityCenter, click the "Request Repositories" link to enter an admin username and password for the SecurityCenter to exchange the SSH keys. Once completed, a list of available repositories will be populated. |
| Repository | Remote repository to collect IP address(es) and vulnerability data from. This is a list of the available repository names available on the remote SecurityCenter. |
| Schedule | Sets the schedule for the remote server to be queried for updated information. |

Access

| Organizations | Defines Organizations that have access to the vulnerability data within the repository. Within the "Organizations" section, selecting or deselecting the checkbox next to the Organization name grants or denies that Organization access to the repository information. When initially selecting the Organization, a prompt will appear to either grant access to all the Groups within the Organization, or not. If granted, all Groups will be given access to the repository information. If denied, Groups within the Organization must explicitly be given access on a per Group basis. |

Offline Repository

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 14 - Offline Repository Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The repository name</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the repository</td>
</tr>
<tr>
<td>Access</td>
<td></td>
</tr>
<tr>
<td>Organizations</td>
<td>Defines Organizations that have access to the vulnerability data within the repository. Within the &quot;Organizations&quot; section, selecting or deselecting the checkbox next to the Organization name grants or denies that Organization access to the repository information. When initially selecting the Organization, a prompt will appear to either grant access to all the Groups within the Organization, or not. If granted, all Groups will be given access to the repository information. If denied, Groups within the Organization must explicitly be given access on a per Group basis.</td>
</tr>
</tbody>
</table>
Advanced Settings

**Generate Trend Data**
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 useful in cases where tracking data changes is important. In situations where repository datasets do not change frequently – negating the need for trending – disable this option to minimize disk space usage.

**Days Trending**
Sets the number of days for the trending data to track.

**Enable Full Text Search**
Determines if the trending data presented is indexed for a full text search.

To initiate offline repository synchronization, first download the repository archive from an existing repository by clicking on the "Export" link from the gear icon menu.

Depending on browser choice, the option to open or save the Nessus or Compressed Tar file is presented. It is recommended that the file be saved at this time.

- 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 sufficient free disk space.

- When importing the repository archive, the default maximum file import size is 360MB. This is specified by the "post_max_size" directive in /opt/sc/support/etc/php.ini. If larger file uploads are required, increase the default value.

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 select “Upload” from the gear icon menu.

On the Upload page add a name and description for the repository. Using the “Choose File” button next to “Repository Data”, select the file to add to the repository, which was previously exported.
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 and may be filtered by 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.

To see more information about a rule, select the rule to be viewed from the list or click "View" from the gear icon menu. To remove a rule, select it from the list, click "Delete" from the gear icon menu and a confirmation dialog is displayed that confirms if you really wish to delete the accepted risk rule:

After clicking "Delete", click 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 filtered for a plugin ID, a repository, or organization combination. A screen capture of example "Recast Risk Rules" is shown below:

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

After clicking "Delete", click the "Apply Rules" button in the top left for the changes to take effect. Once completed, any vulnerabilities that had been modified by the recast risk rule are returned to their original state.
User Management

Organizations

An Organization is defined as a set of distinct Users and Groups and the resources they have available to them. These Users are assigned repositories and “zones” within one or more specified IP networks. “Users” refers to any non-administrator login account on SecurityCenter. “Groups” refers to collections of users with the same permissions within an Organization. “Zone” means that each Organization is made up of the systems within one or more IP networks.

Multiple Organizations can share the same repositories 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 organizational units.

The Organization is managed primarily by the Administrator and Security Manager users. The Administrator is responsible for creation of the Organization, the initial Security Manager creation and assignment, and maintenance. Users within the Organization are created by the Security Manager user or any user with the appropriate permission. User management is performed on a Group level and permissions to resources and objects are shared among the group.

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 multi-step process. The screen capture below contains five areas: General, Scanning, Analysis, Custom Analysis Links, and Vulnerability Weights. Once the Organization is created the option to create the initial Security Manager user is presented. See the next section on Users for specifics about user creation.
The table below describes options available during the creation of an Organization:

**Table 15 - Organization Creation Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Organization name (Required)</td>
</tr>
<tr>
<td>Description</td>
<td>Descriptive text for the Organization.</td>
</tr>
<tr>
<td>Contact Information</td>
<td>Enter the relevant contact information for the organization being created including address, city, state, country, and phone number.</td>
</tr>
<tr>
<td><strong>Scanning</strong></td>
<td></td>
</tr>
<tr>
<td>Distribution Method</td>
<td>There are three options to select for choosing a Scan Zone for the Organization in this drop-down.</td>
</tr>
<tr>
<td></td>
<td>Automatic Distribution Only will automatically select the best Scan Zone(s) available for performing a scan.</td>
</tr>
<tr>
<td></td>
<td>Locked Zone will only use the selected Scan Zone(s) as part of the Organization's available Scan Zones for performing scans.</td>
</tr>
<tr>
<td></td>
<td>Selectable Zones allows users to select from the chosen Scan Zones to perform a scan from. Additionally, automatic distribution may be</td>
</tr>
<tr>
<td></td>
<td>allowed from the chosen zones so the user does not have to make assumptions as to which zone is free or optimal for their scan.</td>
</tr>
<tr>
<td>Available Zones</td>
<td>When selecting Locked or Selectable zones for the distribution method, the list of available zones is displayed for Scan Zone selection.</td>
</tr>
<tr>
<td></td>
<td>The zones are searchable by name or by scrolling the list of zones.</td>
</tr>
<tr>
<td>Restricted Scan Ranges</td>
<td>IP range(s) that the Organization will not be able to scan</td>
</tr>
<tr>
<td><strong>Analysis</strong></td>
<td></td>
</tr>
<tr>
<td>Accessible LCEs</td>
<td>Selection from a list of LCE(s) to which this Organization has access. The LCEs are searchable by name or by scrolling a list of LCEs.</td>
</tr>
<tr>
<td>Accessible Repositories</td>
<td>Selection from a list of Repositories to which the Organization will have access. The Repositories are searchable by name or by scrolling a</td>
</tr>
<tr>
<td></td>
<td>list of Repositories.</td>
</tr>
<tr>
<td>Custom Analysis Links</td>
<td>A list of custom analysis links provided to users within the host vulnerability details when analyzing data outside of SecurityCenter is desired. Clicking the “Add Custom Link” option will create a new field to enter the link name and URL to look up additional data external to SecurityCenter.</td>
</tr>
</tbody>
</table>
For example:

http://example.com/index.htm?ip=%ip%

The “%ip%” reference is a variable that inserts the IP address of the current host into the specified URI.

### Vulnerability Weights

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>The vulnerability weighting to apply to “Low” criticality vulnerabilities for scoring purposes. (Default: 1)</td>
</tr>
<tr>
<td>Medium</td>
<td>The vulnerability weighting to apply to “Medium” criticality vulnerabilities for scoring purposes. (Default: 3)</td>
</tr>
<tr>
<td>High</td>
<td>The vulnerability weighting to apply to “High” criticality vulnerabilities for scoring purposes. (Default: 10)</td>
</tr>
<tr>
<td>Critical</td>
<td>The vulnerability weighting to apply to “Critical” criticality vulnerabilities for scoring purposes. (Default: 40)</td>
</tr>
</tbody>
</table>

### Users

SecurityCenter administrators and Security Managers are configured via the “Users” menu. More than one administrator can be created per SecurityCenter, and multiple Security Managers may be created per Organization. It is recommended to make at least one administrator and Security Manager (per Organization) user using TNS authentication. This will enable at least one high-level account to log in should the LDAP service become unavailable.

The Users page displays the user’s name, username, role, title, and last login. When searching for particular users the columns may be sorted on any of the options. Additionally, filters may be applied to search by name, username, or organization.
Administrators

The administrative user can create and manage other administrator and Security Manager users. All administrators have the same permission level and resources. Security Managers are created with complete control of the Organization to which they are assigned and may not have their assigned Organization changed. Clicking the “Add” button opens the add user page. Fields with a red asterisk are required.
The table below details fields from the add user page:

**Table 16 – Add User Page**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authentication Information</strong></td>
<td></td>
</tr>
<tr>
<td>First Name/Last Name</td>
<td>These fields are to enter the actual first and last name of the user.</td>
</tr>
<tr>
<td><strong>Type – TNS</strong></td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>This is the account name the user will use to log into 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”. The username value is case-sensitive.</td>
</tr>
<tr>
<td><strong>Password/Confirm Password</strong></td>
<td>The login password is entered twice to confirm the correct text. It is recommended to use passwords that meet stringent length and complexity requirements.</td>
</tr>
<tr>
<td><strong>User must change password</strong></td>
<td>Require password change on next login. (TNS Authentication only)</td>
</tr>
<tr>
<td><strong>Type – LDAP</strong></td>
<td></td>
</tr>
<tr>
<td>Search String</td>
<td>This is the LDAP search string to use to narrow down user searches. Proper format is: “attribute=&lt;filter text&gt;“. Wildcards are permitted and the field accepts up to 1024 characters. For example: sAMAccountName=* mail=a* displayName=C*</td>
</tr>
<tr>
<td>User</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>Username</td>
<td>User that is selected from the list of users above.</td>
</tr>
<tr>
<td><strong>Membership</strong></td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td><strong>Administrator</strong> – This role is assigned to users who will be managing the SecurityCenter as a whole. These types of users do not have direct access to the data collected by SecurityCenter.</td>
</tr>
</tbody>
</table>
Security Manager – This role is assigned to users who will be in charge of Organizations. These users have complete access to all data available to their assigned Organization.

Basic/Contact Information

<table>
<thead>
<tr>
<th>Title, Address Information, Email, Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact information for the user can be entered here.</td>
</tr>
</tbody>
</table>

Roles

The pre-defined roles of Administrator, No Role, and Security Manager cannot be edited.

Roles determine what a user can or cannot do from their account. They can be configured to a great degree. SecurityCenter comes with eight pre-defined roles; however, custom roles can be created by the Administrator or Security Manager user in an organization to facilitate organizations with a 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 a user has a custom role with “Create Policies” enabled and “Update Feeds” disabled, that user can only create users with “Create Policies” enabled.

The Administrator, No Role, and Security Manager 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 install and configure each Organization. In addition, the Administrator adds components to SecurityCenter such as PVS, LCE, and Nessus to extend its capabilities. The Administrator is automatically assigned the “Manage Application” role.

A Security Manager 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 and has the ability to launch scans, configure users (except for the Administrator user), vulnerability policies, and other objects that belong to their Organization.

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. The permissions are described on the “Add Role” page.

Scanning

The scanning section for the Administrator user is a collection of Audit Files, Credentials, and Policies that are created and managed for use in SecurityCenter globally by one or more Organizations.

Audit Files

The Nessus vulnerability scanner includes the ability to perform compliance audits of numerous platforms including (but not limited to) 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 can be written for specific environments. Common audit files are maintained on the Tenable Support Portal and through the SecurityCenter feed for users who wish to perform compliance
and configuration auditing. The screen capture below contains a listing of an audit file page with audit file information displayed including the name, owner, group, type, version, and the last time the audit file was modified.

Audit files and/or their information can be edited, exported, viewed, shared, and deleted from the web interface utilizing the gear icon. The list of audit files displayed may be modified using the filters to search on name, type, or type of access to the audit file.

Clicking on the “Add” button will display a list of audit template categories and an option for a Custom audit file to be added.
The audit file templates may be selected using two methods to find the templates. The first is to select the category of templates and select the specific template from the list available. The other option is to use the search field in the top right to search by keyword across all the available audit file templates. Once a template is selected there will be a field to add a custom name and description and, if applicable, additional fields to customize the audit file for the local environment.
Clicking "**Advanced**" in the custom section displays the following "Add Audit File" dialog screen, while selecting edit will display a similar screen titled Edit Audit File:

![Add Audit File Dialog]

Available fields include:

**Table 17 – 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>Audit File</td>
<td>An interface that allows you to browse your local system or file shares for an audit file to upload. When editing, clicking the &quot;X&quot; next to the existing audit file deletes it and allows for uploading a new 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 document located at [https://support.tenable.com](https://support.tenable.com).
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. There are five options for authentication methods: Password, Kerberos, LM Hash, NTLM Hash, and CyberArk Vault.

  To use the standard Windows password authentication method, enter the Username, Password, and Domain in the text boxes.

  When using the Kerberos option to authenticate to a Windows host, enter the username, password, domain, KDC Host, KDC port, and KDC transport options.

  The LM and NTLM hash methods require the username, hash, and domain to be entered for the account to be used for logins.

  When using CyberArk Vault credentials for authentication to Windows hosts, a variety of information is required to be entered including the username to authenticate with, the domain, and information about the CyberArk Vault server as described in the table at the end of this section.

  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 Linux, Unix, and Cisco IOS systems for patch auditing or compliance checks. There are five options for authentication methods: Password, Kerberos, Public Key, Certificate, and CyberArk Vault.

  Using the password method for SSH authentication requires entering a username and password for the account. Additionally, adding a privilege escalation method may be selected if needed.

  To use the Kerberos option to authenticate using a SSH login, enter the username, password, domain, KDC Host, KDC port, KDC transport, and Realm options. Additionally, adding a privilege escalation method may be selected if needed.

  The Public Key authentication option requires entering a username, uploading a private key, and entering the passphrase if needed. Additionally, adding a privilege escalation method may be selected if needed.

  The Certificate authentication option requires entering a username, uploading a user certificate, uploading a private key, and entering the passphrase if needed. Additionally, adding a privilege escalation method may be selected if needed.

  When using CyberArk Valut credentials for authentication to SSH hosts, a variety of information is required to be entered including the username to authenticate with and information about the CyberArk Vault server as described in the table at the end of this section. Additionally, adding a privilege escalation method may be selected if needed.

  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” for security reasons, a Nessus user account can invoke a variety of privilege
escalation options including: “su”, “sudo”, “su+sudo”, “DirectAuthorize (dzdo)”, “PowerBroker (pbrun)”, “k5login”, and “Cisco Enable”.

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

- **PowerBroker (pbrun), from BeyondTrust and DirectAuthorize (dzdo), from Centrify, are proprietary root task delegation methods for Unix and Linux systems.**

- **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](http://www.gratisoft.us/sudo/man/sudo.htm)**

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

- **Database** – The Database option allows for entering credentials and options for various types of database servers, including MSSQL, DB2, Informix/DRDA, MySQL, Oracle, and PostgreSQL.
An example Windows credential window with CyberArk Vault as the authentication method is displayed below:

Some aspects of credential options are based on Nessus plugins. Therefore, specific credential options may differ from the descriptions documented here.
CyberArk Vault Options

The following table describes the options when using CyberArk Vault as the Authentication Method for Windows and SSH credentials.

Table 18 – CyberArk Vault Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The target system’s username.</td>
</tr>
<tr>
<td>Domain</td>
<td>This is an optional field if the above username is part of a domain.</td>
</tr>
<tr>
<td>Central Credential Provider Host</td>
<td>The CyberArk Central Credential Provider IP/DNS address.</td>
</tr>
<tr>
<td>Central Credential Provider Port</td>
<td>The port the CyberArk Central Credential Provider is listening on.</td>
</tr>
<tr>
<td>Vault Username (optional)</td>
<td>If the CyberArk Central Credential Provider is configured to use basic authentication you can fill in this field for authentication.</td>
</tr>
<tr>
<td>Vault Password (optional)</td>
<td>If the CyberArk Central Credential Provider is configured to use basic authentication you can fill in this field for authentication.</td>
</tr>
<tr>
<td>Safe</td>
<td>The safe on the CyberArk Central Credential Provider server that contained the authentication information you would like to retrieve.</td>
</tr>
<tr>
<td>AppId</td>
<td>The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.</td>
</tr>
<tr>
<td>Folder</td>
<td>The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.</td>
</tr>
<tr>
<td>PolicyId</td>
<td>The PolicyID assigned to the credentials you would like to retrieve from the CyberArk Central Credential Provider.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.</td>
</tr>
</tbody>
</table>

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 “Scanning” and then “Policies” to display a listing of all currently available policies. Policies created using Nessus may be uploaded with the Upload Policy link under the Options drop-down menu. This will open a window enabling the selection of the policy file and addition of a name, description, and group. Audit files and credentials from the original policy are not exported and copied with the policy file. The “Add” button allows for the creation of a new policy. The gear icon next to existing policies provide the ability to copy, edit, share, view (view details of), export, and delete existing policies.
Add a Scan Policy

Clicking “Add” opens the Add Policy screen, which is used to configure the new scan policy. The initial screen presents options for Advanced or Template configurations. Items from either section may be selected to begin the process of creating a policy.
Template

The Template section allows users to create scan policies based on industry standards. After selecting a policy template the user is presented with a configuration screen to configure settings unique to the network being scanned. This will include options such as web directories to scan, compliance audit files to use, credentials to use, and other scan options depending on the template selected.

Advanced Scan

The tables below contain detailed descriptions of options available on each of the tabs displayed under the “Advanced Scan” Add Policy screen. The Advanced Scan option gives the ability to build a finely tuned scan policy utilizing all the available settings.

The “Basic” option sets the name and description of the policy:

Table 19 - Basic Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Unique policy name</td>
</tr>
</tbody>
</table>
### Description

Policy description (optional)

The "Advanced" frame controls options for the scan:

**Table 20 - Scan Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable Safe Checks</td>
<td>Nessus can attempt to identify remote vulnerabilities by interpreting banner information and attempting to exercise a vulnerability. When &quot;Enable Safe Checks&quot; 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>Log scan details to server</td>
<td>Saves details of the scan to the server for later analysis.</td>
</tr>
<tr>
<td>Stop scanning hosts that become unresponsive</td>
<td>During a scan hosts may become unresponsive after a period of time. Enabling this setting will stop scan attempts against hosts that stop sending results.</td>
</tr>
<tr>
<td><strong>Performance Options</strong></td>
<td></td>
</tr>
<tr>
<td>Slow down the scan when network congestion is</td>
<td>When Nessus detects congestion during a scan, it will slow the speed of the scan in an attempt to ease the burden on the affected segment(s).</td>
</tr>
<tr>
<td>detected</td>
<td></td>
</tr>
<tr>
<td>Use Linux kernel congestion detection</td>
<td>Use Linux kernel congestion detection during the scan to help alleviate system lockups on the Nessus scanner server.</td>
</tr>
<tr>
<td>Network Timeout (in seconds)</td>
<td>Determines the amount of time, in seconds, to determine if there is an issue communicating over the network.</td>
</tr>
<tr>
<td>Max Simultaneous 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 Simultaneous Hosts Per Scan</td>
<td>This setting limits the maximum number of hosts that a single Nessus scanner will scan at the same time. If the scan is using a zone with multiple scanners, each scanner will accept up to the amount specified in the Max Hosts Per Scan option. For example, if the Max Simultaneous Hosts Per Scan is set to 5 and there are five scanners per zone, each scanner will accept five hosts to scan, allowing a total of 25 hosts to be scanned between the five scanners.</td>
</tr>
<tr>
<td>Max number of concurrent TCP sessions per host</td>
<td>This setting limits the maximum number of TCP sessions established by any of the active scanners while scanning a single host.</td>
</tr>
<tr>
<td>Max number of concurrent TCP sessions per scan</td>
<td>This setting limits the maximum number of TCP sessions established by any of the active scanners during a scan.</td>
</tr>
</tbody>
</table>
The **Host Discovery** section controls discovery options for the scan:

**Table 21 – Host Discovery**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ping the remote host</td>
<td>When enabled, Nessus attempts to ping the hosts in the scan to determine if the host is alive or not.</td>
</tr>
<tr>
<td><strong>General Settings (available when Ping the remote host is enabled)</strong></td>
<td></td>
</tr>
<tr>
<td>Always 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>Use Fast Network Discovery</td>
<td>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 even when there is no service behind the device). Such checks can take some time, especially if the remote host is firewalled. If the “Use Fast Network Discovery” option is enabled, Nessus will not perform these checks.</td>
</tr>
<tr>
<td><strong>Ping Methods (available when Ping the remote host is enabled)</strong></td>
<td></td>
</tr>
<tr>
<td>ARP</td>
<td>Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.</td>
</tr>
<tr>
<td>TCP</td>
<td>Ping a host using TCP.</td>
</tr>
<tr>
<td>Destination ports</td>
<td>Destination ports can be configured to use specific ports for TCP ping. This 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>ICMP</td>
<td>Ping a host using the Internet Control Message Protocol (ICMP).</td>
</tr>
<tr>
<td>Assume ICMP unreachable means the host is down</td>
<td>When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When enabled, this option will consider this to mean the host is dead. This is to help speed up discovery on some networks. Note that some firewalls and packet filters use this same behavior for hosts that are up but are connecting to a port or protocol that is filtered. With this option enabled, this will lead to the scan considering the host is down when it is indeed up.</td>
</tr>
<tr>
<td>Maximum Number of Retries (ICMP enable)</td>
<td>Allows you to specify the number of attempts to try to ping the remote host. The default is two attempts.</td>
</tr>
<tr>
<td>UDP</td>
<td>Ping a host using the User Datagram Protocol (UDP).</td>
</tr>
</tbody>
</table>

**Warning**: UDP is a “stateless” protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.
### Fragile Devices

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan Network Printers</strong></td>
<td>Instructs the Nessus scanner not to scan network printers if unselected. Since many printers are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.</td>
</tr>
<tr>
<td><strong>Scan Novell Netware Hosts</strong></td>
<td>Instructs the Nessus scanner not to scan Novell Netware hosts if unselected. Since many Novell Netware hosts are prone to denial of service conditions, Nessus can skip scanning them once identified. This is particularly recommended if scanning is performed on production networks.</td>
</tr>
</tbody>
</table>

### Wake-on-LAN

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>List of MAC addresses</strong></td>
<td>Wake on Lan (WOL) packets will be sent to the hosts listed, one on each line, in an attempt to wake the specified host(s) during a scan.</td>
</tr>
<tr>
<td><strong>Boot time wait (in minutes)</strong></td>
<td>The number of minutes Nessus will wait to attempt a scan of hosts sent a WOL packet.</td>
</tr>
</tbody>
</table>

### Network Type

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network Type</strong></td>
<td>Allows you to specify if you are using publicly 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>
</tbody>
</table>

The “Port Scanning” section controls discovery options for the scan:

#### Table 22 - Network Discovery

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ports</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Consider Unscanned Ports as Closed</strong></td>
<td>If a port is not scanned with a selected port scanner (e.g., out of the range specified), the scanner will consider it closed.</td>
</tr>
<tr>
<td><strong>Port scan range</strong></td>
<td>Directs the scanner to target a specific range of ports. Accepts “default” (a list of approximately 4,790 common ports found in the <code>nessus-services</code> file), “all” (scans all ports from 0-65535), or a custom list of ports specified by the user. The custom list may contain individual ports and ranges; for example, “21,23,25,80,110” and “1-1024,8080,9000-9200” are valid values. Specifying “1-65535” will scan all ports.</td>
</tr>
<tr>
<td><strong>Local Port Enumerators</strong></td>
<td>This option uses <code>netstat</code> to check for open ports on the target host. It relies on the <code>netstat</code> command being available via a SSH connection to the target. This scan is intended for Unix-based systems and requires authentication credentials.</td>
</tr>
<tr>
<td><strong>SSH (netstat)</strong></td>
<td>This option uses <code>netstat</code> to check for open ports from the local machine. It relies on the <code>netstat</code> command being available via a WMI connection to the target. This scan is intended for Windows-based systems and requires authentication credentials.</td>
</tr>
</tbody>
</table>
SNMP

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.

Only run network port scanners if local port enumeration failed

Rely on local port enumeration first before relying on network port scans.

Verify open TCP ports found by local port enumerators

If a local port enumerator (e.g., WMI or netstat) 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).

Network Port Scanners

TCP

Use Nessus' built-in TCP scanner to identify open TCP ports on the targets. This scanner is optimized and has some self-tuning features.

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.

SYN

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 then determines port state based on a reply – or lack of.

Only run network port scanners if local port enumeration failed

Rely on local port enumeration first before relying on network port scans.

UDP

This option engages Nessus' built-in UDP scanner to identify open UDP ports on the targets.

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. Utilizing the UDP scanner will noticeably increase scanning time.

The “Service Discovery” screen directs the scanner on how it looks for services running on the target’s ports. The following values are allowed for the “Service Discovery” option:

Table 23 – Values for Service Discovery Options

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Probe all ports to find services</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>
</tbody>
</table>
Search for SSL based services: 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.

Search for SSL on: If selected, choose between Known SSL ports (e.g., 443) and All ports. Testing for SSL capability on all ports may be disruptive for the tested host.

Enumerate all SSL ciphers: When SecurityCenter performs an SSL scan, it tries to determine the SSL ciphers used by the remote server by attempting to establish a connection with each different documented SSL cipher, regardless of what the server says is available.

Enable CRL checking (connects to the Internet): Direct Nessus to check SSL certificates against known Certificate Revocation Lists (CRL). Enabling this option will make a connection and query one or more servers on the internet.

The “Assessment” screen directs the scanner on how it tests for certain information during the scan. The following values are allowed for the “Assessment” option:

Table 24 – Values for Assessment Options

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td></td>
</tr>
<tr>
<td>Override normal accuracy</td>
<td>In some cases, Nessus cannot remotely determine whether a flaw is present or not. If report paranoia is set to &quot;Paranoid&quot; 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 alarms” will cause Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. Not changing from “Normal” is a middle ground between these two settings.</td>
</tr>
<tr>
<td>Perform thorough tests (may disrupt your network or impact scan speed)</td>
<td>Causes various plugins to use more aggressive settings. For example, when looking through SMB file shares, a plugin can analyze 3 directory levels deep instead of its default 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 providing better audit results.</td>
</tr>
<tr>
<td>Antivirus</td>
<td></td>
</tr>
<tr>
<td>Antivirus definition grace period (in days)</td>
<td>This option determines the delay in the number of days of reporting the software as being outdated. The valid values are between 0 (no delay, default) and 7.</td>
</tr>
<tr>
<td>SMTP</td>
<td></td>
</tr>
<tr>
<td>Third Party Domain</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 may be aborted by the SMTP server.</td>
</tr>
<tr>
<td>From address</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>To Address</td>
<td>Nessus will attempt to send messages addressed to the mail recipient listed in this field. The postmaster address is the default value since it is a valid address on most mail servers.</td>
</tr>
</tbody>
</table>
The "Brute Force" screen directs the scanner on how it tests for certain information against SCADA systems during the scan. The following values are allowed for the "Brute Force" option:

**Table 25 – Values for Brute Force Options**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General</strong></td>
<td></td>
</tr>
<tr>
<td>Only use credentials provided by the user</td>
<td>In some cases, Nessus can test default accounts and known default passwords. This can cause the account to be locked out if too many consecutive invalid attempts trigger security protocols on the operating system or application. By default, this setting is enabled to prevent Nessus from performing these tests.</td>
</tr>
<tr>
<td><strong>Oracle Database</strong></td>
<td></td>
</tr>
<tr>
<td>Test default Oracle accounts (slow)</td>
<td>Test for known default accounts in Oracle software.</td>
</tr>
</tbody>
</table>

The "SCADA" screen directs the scanner on how it tests for certain information against SCADA systems during the scan. The following values are allowed for the "SCADA" option:

**Table 26 – Values for SCADA Options**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Modbus/TCP Coil Access</strong></td>
<td></td>
</tr>
<tr>
<td>Start at register</td>
<td>These options are available for commercial users. This drop-down menu item is dynamically generated by the SCADA plugins available with the commercial version of Nessus. Modbus uses a function code of 1 to read &quot;coils&quot; 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 &quot;write coil&quot; message. The defaults for this are &quot;0&quot; for the “Start reg” and “16” for the “End reg”.</td>
</tr>
<tr>
<td>End at register</td>
<td></td>
</tr>
<tr>
<td><strong>ICCP/COTP TSAP Addressing Weakness</strong></td>
<td></td>
</tr>
<tr>
<td>Start COTP TSAP</td>
<td>The “ICCP/COTP TSAP Addressing” menu 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.</td>
</tr>
<tr>
<td>Stop COTP TSAP</td>
<td></td>
</tr>
</tbody>
</table>
The "Web Applications" screen directs the scanner on how it tests for certain information against web servers applications during the scan. The following values are available for the "Web Application" option when the "Scan web applications" option is enabled:

**Table 27 – Values for Web Applications Options**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Use a custom User-Agent</strong></td>
<td>Specifies which type of web browser Nessus will impersonate while scanning.</td>
</tr>
<tr>
<td><strong>Web Crawler</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Start crawling from</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., &quot;/:/php4:/base&quot;).</td>
</tr>
<tr>
<td><strong>Excluded pages (regex)</strong></td>
<td>Enable exclusion of portions of the website from being crawled. For example, to exclude the &quot;/manual&quot; directory and all Perl CGI, set this field to: (^/manual)</td>
</tr>
<tr>
<td><strong>Maximum pages to crawl</strong></td>
<td>The maximum number of pages to crawl.</td>
</tr>
<tr>
<td><strong>Maximum depth to crawl</strong></td>
<td>Limit the number of links Nessus will follow for each start page.</td>
</tr>
<tr>
<td><strong>Follow dynamic pages</strong></td>
<td>If selected, Nessus will follow dynamic links and may exceed the parameters set above.</td>
</tr>
<tr>
<td><strong>Web Applications</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Enable generic web application tests</strong></td>
<td>When enabled, the following options for scanning web applications are displayed.</td>
</tr>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Use a custom User-Agent</strong></td>
<td>Specifies which type of web browser Nessus will impersonate while scanning.</td>
</tr>
<tr>
<td><strong>Web Crawler</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Start crawling from</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., &quot;/:/php4:/base&quot;).</td>
</tr>
<tr>
<td><strong>Excluded pages (regex)</strong></td>
<td>Enable exclusion of portions of the website from being crawled. For example, to exclude the &quot;/manual&quot; directory and all Perl CGI, set this field to: (^/manual)</td>
</tr>
<tr>
<td><strong>Maximum pages to crawl</strong></td>
<td>The maximum number of pages to crawl.</td>
</tr>
<tr>
<td><strong>Maximum depth to crawl</strong></td>
<td>Limit the number of links Nessus will follow for each start page.</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Follow dynamically generated pages</strong></td>
<td>If selected, Nessus will follow dynamic links and may exceed the parameters set above.</td>
</tr>
<tr>
<td><strong>Application Test Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Enable generic web application tests</strong></td>
<td>Enables the options listed below.</td>
</tr>
<tr>
<td><strong>Abort web application tests if HTTP login fails</strong></td>
<td>If Nessus cannot login to the target via HTTP, then do not run any web application tests.</td>
</tr>
<tr>
<td><strong>Try all HTTP Methods</strong></td>
<td>This option will instruct Nessus to also use &quot;POST requests&quot; 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. When selected, Nessus will test each script/variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.</td>
</tr>
<tr>
<td><strong>Attempt HTTP Parameter Pollution</strong></td>
<td>When performing web application tests, attempt to bypass 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;.</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>Test more than one parameter at a time per form</strong></td>
<td>This option manages the combination of argument values used in the HTTP requests. The default, without checking this option, is testing one parameter at a time with an attack string, without trying &quot;non-attack&quot; variations for additional parameters. For example, Nessus would attempt &quot;/test.php?arg1=XSS&amp;b=1&amp;c=1&quot; where &quot;b&quot; and “c” allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. This drop-down has four options:</td>
</tr>
<tr>
<td><strong>Some pairs</strong> – This form of testing will randomly check a combination of random pairs of parameters. This is the fastest way to test multiple parameters.</td>
<td></td>
</tr>
<tr>
<td><strong>All pairs (slower but efficient)</strong> – This form of testing is slightly slower but more efficient than the &quot;one value&quot; 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 &quot;/test.php?a=XSS&amp;b=1&amp;c=1&amp;d=1&quot; 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 &quot;/test.php?a=XSS&amp;b=3&amp;c=3&amp;d=3&quot; when the first value of each variable is &quot;1&quot;.</td>
<td></td>
</tr>
<tr>
<td><strong>Some combinations (slower)</strong> – This form of testing will randomly check a combination of</td>
<td></td>
</tr>
</tbody>
</table>
three or more parameters. This is more thorough than testing only pairs of parameters. Note that increasing the amount of combinations by three or more increases the web application test time.

**All combinations (slowest)** – 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.

| Do not stop after the first flaw is found per web page | This option determines when a new flaw is targeted. 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, unless “thorough tests” is set. Note that several flaws of the same type (e.g., XSS, SQLi, etc.) may be reported sometimes, if they were caught by the same attack. The drop-down has four options:

- **Per port (fastest)** – 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.

- **Per parameter (slow)** – As soon as one type of flaw is found in a parameter of a CGI (e.g., XSS), Nessus switches to the next parameter of the same CGI, or the next known CGI, or to the next port/server.

- **Look for all flaws (slowest)** – Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases. |

| URL for Remote File Inclusion | 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 by Tenable for RFI testing. If the scanner cannot reach the Internet, using an internally hosted file is recommended for more accurate RFI testing. |

| Maximum run time (minutes) | This option manages the amount of time in minutes spent performing web application tests. This option defaults to 60 minutes and applies to all ports and CGIs for a given web site. Scanning the local network for web sites with small applications will typically complete in under an hour, however web sites with large applications may require a higher value. |

The “Windows” option controls basic Windows SMB domain options:

**Table 28 – Values for Windows Scan Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Settings</td>
<td>When enabled, information about the SMB domain is obtained.</td>
</tr>
<tr>
<td>Enumerate Domain Users</td>
<td>This option determines the start and end Domain UIDs that will be reported on.</td>
</tr>
<tr>
<td>Enumerate Local Users</td>
<td>This option determines the start and end Local UIDs that will be reported on.</td>
</tr>
<tr>
<td>Malware</td>
<td></td>
</tr>
<tr>
<td>Provide your own list of</td>
<td>Additional known bad MD5 hashes can be uploaded via a text file that contains one MD5 hash.</td>
</tr>
</tbody>
</table>
known bad MD5 hashes

| hash per line.  
| It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target and a description was provided for the hash, the description will show up in the scan results. Standard hash-delimited comments (e.g., #) can optionally be used in addition to the comma-delimited ones. |

Provide your own list of known good MD5 hashes

| Additional known good MD5 hashes can be uploaded via a text file that contains one MD5 hash per line.  
| It is possible to (optionally) add a description for each hash in the uploaded file. This is done by adding a comma after the hash, followed by the description. If any matches are found when scanning a target, and a description was provided for the hash, the description will show up in the scan results. Standard hash-delimited comments (e.g., #) can optionally be used in addition to the comma-delimited ones. |

Hosts file whitelist

| Nessus checks system `hosts` files for signs of a compromise (e.g., Plugin ID 23910 titled "Compromised Windows System (hosts File Check)"). This option allows you to upload a file containing a list of hostnames that will be ignored by Nessus during a scan. Include one hostname per line in a regular text file. |

The **Report** options control information that is included in the scan’s report:

**Table 29 – Values for Scan Report Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Report processing | **Report Verbosity** – Determines the verbosity of the detail in the output of the scan results as Normal, Quiet, or Verbose.  
**Show missing patches that have been superseded** – Show patches in the report that have not been applied but have been superseded by a newer patch if enabled.  
**Hide results from plugins initiated as a dependency** – If a plugin is only run due to it being a dependency of a selected plugin, hide the results if enabled. |
| Report Output | **Designate hosts by their DNS name** – When possible, designate hosts by their DNS name rather than IP address in the reports.  
**Display hosts that respond to ping** – When enabled, show a list of hosts that respond to pings sent as part of the scan.  
**Display unreachable hosts** – Display a list of hosts within the scan range that were not able to be reached during the scan, if enabled.  
**Generate SCAP XML Results** – Generate a SCAP XML results file as a part of the report output for the scan. |
The "Authentication" option controls authentication options during a scan:

Table 30 - Value for Authentication Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>When added, authentication methods may be used to login to the scan target machines to gather more complete results of the host’s status. The authentication types include host, database, miscellaneous, plaintext authentication, and patch management. For each type, various relevant options are presented such as SNMPv3, MongoDB, VMWare APIs, and similar.</td>
</tr>
<tr>
<td>SNMP</td>
<td></td>
</tr>
<tr>
<td>UDP Port</td>
<td>This is the UDP port that will be used when performing certain SNMP scans. Up to four different ports may be configured, with the default port being 161.</td>
</tr>
<tr>
<td>SSH</td>
<td></td>
</tr>
<tr>
<td>known_hosts file</td>
<td>If an SSH known_hosts file is provided for the scan policy in the “known_hosts file” field, Nessus will only attempt to log into hosts defined in this file. This helps to ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a login to a system that may not be under your control.</td>
</tr>
<tr>
<td>Preferred port</td>
<td>This option is set to direct the scan to connect to a specific port if SSH is known to be listening on a port other than the default of 22.</td>
</tr>
<tr>
<td>Client Version</td>
<td>Specifies which type of SSH client to impersonate while performing scans.</td>
</tr>
<tr>
<td>Windows</td>
<td></td>
</tr>
<tr>
<td>Never send credentials in the clear</td>
<td>By default, Windows credentials are not sent to the target host in the clear.</td>
</tr>
<tr>
<td>Do not use NTLMv1 authentication</td>
<td>If the &quot;Do not use NTLMv1 authentication&quot; option is disabled, then it is theoretically possible to trick Nessus into attempting to log into a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a &quot;hash&quot; obtained from Nessus. This &quot;hash&quot; can be potentially cracked to reveal a username or password. It may also be used to directly log into other servers. Because NTLMv1 is an insecure protocol this option is enabled by default.</td>
</tr>
<tr>
<td>Start the Remote Registry service during the scan</td>
<td>This option tells Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Nessus to execute some Windows local check plugins.</td>
</tr>
<tr>
<td>Enable administrative shares during the scan</td>
<td>This option will allow Nessus to access certain registry entries that can be read with administrator privileges.</td>
</tr>
<tr>
<td>Plaintext Authentication</td>
<td></td>
</tr>
<tr>
<td>Perform patch audits over telnet</td>
<td>When enabled, patch audits will be permitted over a telnet connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.</td>
</tr>
</tbody>
</table>
Perform patch audits over rsh

When enabled, patch audits will be permitted over a rsh connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.

Perform patch audits over rexec

When enabled, patch audits will be permitted over a rexec connection. However this protocol is cleartext and usernames and passwords are unencrypted and are able to be intercepted. This option is therefore disabled by default.

HTTP

Login method

Specify if the login action is performed via a GET or POST request.

Re-authenticate delay (seconds)

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

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.

Invert authenticated regex

A regex pattern to look for on the login page, that if found, tells Nessus authentication was not successful (e.g., “Authentication failed!”).

Use authenticated 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 authenticated regex

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

The “Compliance” section allows for adding compliance audit files to the scan. Once the type of Unix or Windows File Content is selected from the drop-down, a list of available audit files of that type will be available in the second drop-down menu. The list of audit files may be searched by entering text into the field or scrolling the list of available names. Hovering over a name will enable an information icon which, when hovered over, will display the name, description, and type of the audit file. Selecting the check mark to the right will add the chosen audit file to the policy. Clicking the X will remove it.

When an audit file exists in a policy, it may be edited to select a new compliance file or deleted by selecting the appropriate icon when hovered over.

Plugins

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

On each page of plugins there is a “Show Enabled” link that will show only the enabled plugins or families with one or more plugins enabled. The “Show All” link shows all of the plugins or families no matter if they are enabled or not. The “Enable All” link will enable all of the available plugins in the family while the “Disable All” link will disable all of the plugins.

The “Select Filter” drop-down provides a list of items to filter plugins off of. Filterable items include Name, CVE ID, MS Bulletin ID, Plugin ID, and others. These filters are available on the plugin families page and the family plugin list page. Selecting a filterable option will then display either a drop-down box to select options or a text entry box to enter text to search on within that option. Selecting the “Apply” button will apply the search criteria to the list and selecting the “Clear” button will clear the search parameters for the list of plugins.
Clicking the status next to a plugin family allows you to enable or disable the entire family. The rectangles next to the name of the Families will show green and read Enabled when all of the plugins for that family are enabled, will show blue and read Mixed when some of the plugins for that family are enabled, and will show red and read Disabled when none of the plugins are enabled for the family. Additionally, the number in the status column indicates the total number of enabled plugins for the family.

Clicking the name of a plugin family will display a list of that family’s plugins.
The displayed list of plugins will show the status of the individual plugin, the plugin name, and plugin ID. To the right of the plugin ID is an information icon. When the information icon is clicked, the Plugin Details will be displayed and provide more information about the vulnerability being examined. Scrolling down in the “Plugin Details” pane will also show solution information, additional references if available, the CVSSv2 score that provides a basic risk rating (as applicable), and other information provided by the plugin.

When a plugin family is selected, its name appears in a drop-down box. Selecting this drop-down box will display a list of all the available plugin families. Selecting one of these will change the list of vulnerabilities to display that family’s plugins. Clicking the “Back” link next to the drop-down list will return to the list of plugin families.

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 network hosts 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.
Troubleshooting

SecurityCenter

SecurityCenter does not appear to be operational

- Close and reopen the web browser if a login page does not appear.
- Ensure that the remote `httpd` service is running on the SecurityCenter host:
  
  ```
  # ps ax | grep httpd
  1990 ? Ss 0:01 /opt/sc/support/bin/httpd -k start
  ```

- Ensure that sufficient drive space exists on the SecurityCenter host:
  
  ```
  # df
  Filesystem      1K-blocks     Used       Available Use% Mounted on
  /dev/mapper/VolGroup00-LogVol00  8506784      8506784        0   100% /
  /dev/sda1     101086      24455       71412    26% /boot
  tmpfs         1037732      0    1037732     0% /dev/shm
  ```

  If drive space has become exhausted for any reason, sufficient space must be recovered and the SecurityCenter service must be restarted for SecurityCenter to become operational:

  ```
  # df
  Filesystem      1K-blocks     Used       Available Use% Mounted on
  /dev/mapper/VolGroup00-LogVol00  8506784   6816420    1251276    85% /
  /dev/sda1     101086      24455       71412    26% /boot
  tmpfs         1037732      0    1037732     0% /dev/shm
  ```

  ```
  # service SecurityCenter restart
  Shutting down SecurityCenter services:          [  OK  ]
  Starting SecurityCenter services:              [  OK  ]
  ```

Forgot login credentials

- Contact Tenable Support ([support@tenable.com](mailto:support@tenable.com)).

Invalid license error

- If you receive an invalid license error while attempting to log in as a Security Manager or lower, an administrator must log in and upload a new valid license key. A user with access to the host OS and valid permissions can also check that an up-to-date license exists in `/opt/sc/daemons`. Licenses are obtained from Tenable and copied to the daemons directory as the "tns" user.

  `-rw-r--r-- 1 tns tns 1942 Oct 29 12:14 license.key`
Reporting does not work

- Check your Java version. Only OpenJDK and Oracle JRE are supported. The existence of another type of Java on the system will likely break reporting.

LCE

LCE server does not appear to be operational

- Log into the SecurityCenter UI as admin and confirm that the LCE server state is “Working” along with all attached LCE clients.
- Check that you can SSH from the SecurityCenter host to the LCE host.
- Check that the LCE daemon is running on its host and listening on the configured port (TCP port 31300 by default):
  ```
  # netstat -pan | grep lced
  tcp   0      0 0.0.0.0:31300 0.0.0.0:*     LISTEN      30339/lced
  ```
- Check that the listening ports can be reached from the network and are not blocked by a firewall.
- If the LCE server is not operational, attempt to start the service:
  ```
  # service lce start
  Starting Log Correlation Engine
  ```

No events from an attached LCE server

- Log into the SecurityCenter UI as admin and confirm that the LCE server state is “Working” along with all attached LCE clients.
- Confirm connectivity by checking that heartbeat events show up in the SecurityCenter UI.
- Check the LCE configuration settings in accordance with the LCE documentation.
- Check the individual LCE client configuration and authorization in the LCE Clients screen. If syslog is being used to collect information and events, ensure that the syslog service is running and configured correctly on the target syslog server in accordance with LCE documentation.
- Check for NTP time synchronization between the SecurityCenter, LCE, and LCE clients.

Invalid LCE license

- Check that an up-to-date license exists on the LCE server.
Nessus

Nessus server does not appear to be operational

- Verify in the SecurityCenter UI that the Nessus scanner appears as “Unable to Connect” under “Status”.
- SSH to the remote Nessus host to make sure the underlying operating system is operational.
- Confirm that the Nessus daemon is running (Linux example below):
  ```bash
  # service nessusd status
  nessusd (pid 3853) is running...
  ```
- If the Nessus service is not running, start the service:
  ```bash
  # service nessusd start
  Starting Nessus services:
  # ps -ef | grep nessusd
  root  8201  8200  60 11:41 pts/2    00:00:05 nessusd -q
  root  8206  7842  0 11:41 pts/2    00:00:00 grep nessusd
  #
  ```

Cannot add a Nessus server

- Make sure the Nessus daemon was registered using the SecurityCenter option for registration.
- Check connectivity by telnetting from the SecurityCenter to the Nessus system on port 8834. If successful, the response will include: **Escape character is ‘^[’**.

Nessus scans fail to complete

- Ensure that the Nessus service is running on the Nessus host.
- Ensure that Nessus scanner is listed in SecurityCenter under “Resources” and “Nessus Scanners” and that the status of the Nessus scanner is listed as “Working”. Click “Edit” to ensure that the IP address or hostname, port, username, password, and selected repositories for the Nessus scanner are all correct. Edit any incorrect entries to their correct state and click “Submit” to attempt to reinitialize the Nessus scanning interface.
- Right click the scan results and click “Scan Details” to obtain a more detailed description of the error. If the scan details indicate a “Blocking” error, this is indicative of a license IP count that has reached the limit. Either remove a repository to free up IP addresses or obtain a license for more IP addresses.
- Ensure that scan targets are permitted within the configured scan zones.

Nessus plugins fail to update

- Under “System”, “Configuration”, “License” in SecurityCenter, ensure that the Nessus Activation Code is marked as “Valid”.
- Ensure that the user used to connect to the Nessus server is configured as an ‘admin’ class user.
- Ensure that the SecurityCenter system is allowed outbound HTTP(S) connectivity to the Nessus Plugin Update Site. If it is not, refer to the Nessus 6.x Installation and Configuration Guide for information on offline plugin updates.
Under “System”, “Configuration”, and “Update” in SecurityCenter, ensure that Active Plugins is not set to “Never”. Manually test a plugin update under “Plugins” with “Update Plugins”. If successful, the line “Active Plugins Last Updated” will update to the current date and time.

For all other Nessus plugin update issues, contact Tenable Support at support@tenable.com.

**PVS**

**PVS server does not appear to be operational**

- Verify in the SecurityCenter GUI that the PVS server appears as “Unable to Connect” under “Status”.
- SSH to the remote PVS host to make sure the underlying operating system is operational.
- Confirm that the PVS is running (Linux example below):
  ```
  # service pvs status
  PVS is stopped
  PVS Proxy (pid 3142) is running
  #
  ```
  If the PVS service is not running, start the service:
  ```
  # service pvs start
  Starting PVS Proxy [ OK ]
  Starting PVS [ OK ]
  #
  ```

**Can’t add a PVS server**

- Confirm that the PVS proxy is listening on the same port as is configured in SecurityCenter (port 8835 by default):
  ```
  # netstat -pan | grep 8835
  tcp      0      0 0.0.0.0:8835 0.0.0.0:*      LISTEN      406/pvs
  ```
- Check connectivity by telnetting from the SecurityCenter console yum into the PVS server on port 8835 (the pvs listening port). If successful, the response will include: *Escape character is ‘^]’.*

**No vulnerabilities are being received from the PVS server**

- Ensure that the PVS service is running on the PVS host.
- Ensure that the PVS is listed in SecurityCenter under “Resources” and “Passive Scanners” and that the status of the PVS is listed as “Working”. Click “Edit” to ensure that the IP address or hostname, port, username, password, and selected repositories for the PVS are all correct. Edit any incorrect entries to their correct state and click “Submit” to attempt to reinitialize the PVS’ scanning interface.

**PVS plugins fail to update**

- Manually test a plugin update under “Plugins” with “Update Plugins”. If successful, the line “Passive Plugins Last Updated” will update to the current date and time.
- Ensure that the SecurityCenter host is allowed outbound HTTP(S) connectivity to the PVS Plugin Update Site.
- For all other PVS plugin update issues, contact Tenable Support at support@tenable.com.
About Tenable Network Security

Tenable Network Security provides continuous network monitoring to identify vulnerabilities, reduce risk, and ensure compliance. Our family of products includes SecurityCenter Continuous View™, which provides the most comprehensive and integrated view of network health, and Nessus®, the global standard in detecting and assessing network data. Tenable is relied upon by many of the world’s largest corporations, not-for-profit organizations and public sector agencies, including the entire U.S. Department of Defense. For more information, visit tenable.com.
Appendix 1: License Declarations

SecurityCenter’s Software License Agreement can be found on the machine SecurityCenter is installed on in the directory 
\texttt{/opt/sc/docs}.

For a list of third-party software packages that Tenable utilizes with SecurityCenter 5, see the “Tenable Third-Party License
Declarations” document.
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. The LCE server must have a valid license key installed and the LCE daemon must be running before performing the steps below.

The LCE server must have a valid license key installed and the LCE daemon must be running before performing the steps below.

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 "Download Key", choose the desired key format (both DSA or RSA work for this process) and then click "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/SSHKey.pub

   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 5.0 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/sc/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/nessuscli 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><code>/opt/nessus/com/nessus/CA/cacert.pem</code></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><code>/opt/nessus/com/nessus/CA</code> on the initial Nessus server and any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
<tr>
<td><code>/opt/nessus/com/nessus/CA/servercert.pem</code></td>
<td>This is the public certificate for the Nessus server that is sent in response to a CSR.</td>
<td><code>/opt/nessus/com/nessus/CA</code> on any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
<tr>
<td><code>/opt/nessus/var/nessus/CA/cakey.pem</code></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><code>/opt/nessus/var/nessus/CA</code> on any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
<tr>
<td><code>/opt/nessus/var/nessus/CA/serverkey.pem</code></td>
<td>This is the private key of the Nessus server.</td>
<td><code>/opt/nessus/var/nessus/CA</code> 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:

```
# /opt/nessus/sbin/nessuscli 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/nessuscli 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 `nessuscli adduser` command; the user will be created if it does not already exist. The following files are created by this command:
### 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/nessuscli mkcert

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 cli mkcert -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:

```bash
# ./opt/nessus/sbin/nessus-cli mkcert -client
Do you want to register the users in the Nessus server as soon as you create their certificates? [n]: y

--------------------------------------------------------------------
Creation Nessus SSL client Certificate
--------------------------------------------------------------------

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:

```
# cd /tmp/nessus-043c22b5
# cat cert_paul.pem key_paul.pem > nessuscert.pem
```

The nessuscert.pem file will be used when configuring the Nessus scanner on SecurityCenter. This file needs to be copied to somewhere accessible for selection from your web browser during the Nessus configuration.

Configure Nessus Daemons

To enable certificate authentication on the Nessus server, the force_pubkey_auth setting must be enabled. Once enabled, log in to the Nessus server may only be completed by SSL certificates. Username and password login will be disabled. As the root (or equivalent) user on the Nessus server, run the following command:

```
# /opt/nessus/sbin/nessuscli fix --set force_pubkey_auth=yes
```

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”. During the setup of the Nessus scanner, select the previously created nessuscert.pem file for the “Certificate” field, then click “Submit” to confirm.
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/sc/support/conf directory to avoid overwriting existing files.

Deploy to Other Nessus Scanners

Configure any other Nessus scanners for SecurityCenter use and certificate authentication prior to performing the following tasks.

If you have other Nessus servers that will need to authenticate using the same SSL certificates and user names, simply copy the files to the other servers as follows:

```
# cd /opt/nessus/var/nessus/CA
# scp 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
```
You will then need to copy the Nessus user(s) to all the Nessus servers, replacing ‘admin’ in the following command with the user’s name:

```
# 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:

```
#/sbin/service nessusd restart
```

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 command `C:\Program Files\Tenable\Nessus\nessuscli mkcert` 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>C:\Program Files\Tenable\Nessus\nessus\CA on any additional Nessus servers that need to authenticate using SSL.</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 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 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 on any additional Nessus servers that need to authenticate using SSL.</td>
</tr>
</tbody>
</table>
**Nessus Client Keys**

The Nessus user, which in this case is the user ID that SecurityCenter uses to communicate with the Nessus server, is created by the command `C:\Program Files\Tenable\Nessus\nessuscli 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”.

The following files are created by this command:

<table>
<thead>
<tr>
<th>File Name Created</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Documents and Settings&lt;UserAccount&gt;\Local Settings\Temp\nessus-xxxxxxxx\cert_&lt;user&gt;.pem</td>
<td>This is the public certificate for the specified user.</td>
</tr>
<tr>
<td>C:\Documents and Settings&lt;UserAccount&gt;\Local Settings\Temp\nessus-xxxxxxxx\key_&lt;user&gt;.pem</td>
<td>This is the private key for the specified user.</td>
</tr>
</tbody>
</table>
| C:\Program Files\Tenable\Nessus\nessus\users\<user_name>\auth\dname | 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: 
"/C={country}/ST={state}/L={location}/OU={organizational unit}/O={organization/CN={common name}" |

**Creating and Deploying SSL Authentication for Nessus**

**Create Keys and User on Nessus Server**

Create the Certificate Authority and Nessus server certificate using the command `C:\Program Files\Tenable\Nessus\nessuscli mkcert` and provide the requested information.

- Any Nessus Scanner that has previously processed scans will not initially accept these keys as a `policy.db` will have already been created on the Nessus Scanner. Remove the `policy.db` from the Nessus Scanner to ensure the deployment finishes successfully.

- To remove the `policy.db` on a Linux system issue this command as root: `rm /opt/nessus/var/nessus/users/<UserName>/policy.db`

- To remove the `policy.db` on a Windows system, navigate to the `C:\Program Files\Tenable\Nessus` folder and remove the `policy.db` file. Actual location of the `policy.db` differs depending on the version of Windows that is running.
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 `C:\Program Files\Tenable\Nessus\nessuscli mkcert-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:

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
```

The `nessuscert.pem` file will be used when configuring the Nessus scanner on SecurityCenter. This file needs to be copied to somewhere accessible for selection from your web browser during the Nessus configuration.

**Configure Nessus Daemons**

To enable certificate authentication on the Nessus server, the `force_pubkey_auth` setting must be enabled. Once enabled, log in to the Nessus server may only be completed by SSL certificates. Username and password login will be disabled. As the root (or equivalent) user on the Nessus server, run the following command:

```
C:\Program Files\Tenable\Nessus\nessuscli fix --set force_pubkey_auth=yes
```

Open the Nessus Server Manager GUI, click "Stop Nessus Server" and then click "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". During the setup of the Nessus scanner, select the previously created "nessuscert.pem" file for the "Certificate" field, then click "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.crt” 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/sc/support/conf directory. These files are named SecurityCenter.crt and SecurityCenter.key. In the example below, we are placing the files in /tmp.

   ```bash
   # cp /opt/sc/support/conf/SecurityCenter.crt /tmp/SecurityCenter.crt.bak
   # cp /opt/sc/support/conf/SecurityCenter.key /tmp/SecurityCenter.key.bak
   ```

2. Copy the new certificates (e.g., host.crt and host.key) to the /opt/sc/support/conf directory and overwrite the current certificates. If prompted to overwrite, press “y”.

   ```bash
   # cp host.crt /opt/sc/support/conf/SecurityCenter.crt
   # cp host.key /opt/sc/support/conf/SecurityCenter.key
   ```

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

   ```bash
   # ls -l /opt/sc/support/conf/SecurityCenter.crt
   -rw-r--r-- 1 tns tns  4389 May 15 15:12 SecurityCenter.crt
   # ls -l /opt/sc/support/conf/SecurityCenter.key
   -rw-r--r-- 1 tns tns  887 May 15 15:12 SecurityCenter.key
   ```

   If an intermediate certificate is required, it must be copied to the system and given the correct permissions (644) and ownership (tns). Additionally, the line in /opt/sc/support/conf/vhostssl.conf that begins with #SSLCertificateChainFile must have the “#” removed from the beginning of the line to enable the setting. Modify the path and filename to match the certificate that was uploaded.

4. Restart the SecurityCenter services:

   ```bash
   # service SecurityCenter restart
   ```

5. Browse to SecurityCenter using SSL (e.g., https://192.168.1.5). When prompted to confirm the SSL certificate, verify the new certificate details.
Appendix 5: Offline SecurityCenter Plugin Updates

**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 otherwise configured.

   ![Tip]

   To prevent the Nessus scanner from starting automatically upon restarting the system, run the following command:

   ```bash
   # /sbin/chkconfig nessusd off
   ```

2. Run the following command and save the challenge string that is displayed:

   ```bash
   # /opt/nessus/sbin/nessuscli fetch --challenge
   ```

3. Navigate your browser to https://plugins.nessus.org/offline.php

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.

5. On the next page, copy the link that starts with `http://plugins.nessus.org/get.php...` and save it as a favorite. Within the saved link change `all-2.0.tar.gz` to `sc-plugins-diff.tar.gz`. This link will be needed for future use. Do not click the link for `nessus-fetch.rc` as it is not needed.

6. Go to the favorite you created, which will prompt you to download a file. Download the file, which will be called `sc-plugins-diff.tar.gz`.

7. Save the `sc-plugins-diff.tar.gz` on the system used to access your SecurityCenter GUI.

8. Log in to the SecurityCenter GUI as the admin user.

9. Navigate to the System -> Configuration page and select the Plugins/Feed option.

10. Click "Upload Plugins" on the Active Plugins line and browse to the saved `sc-plugins-diff.tar.gz` file, and then upload to SecurityCenter.

11. The plugin update will take a few to several minutes. The date and time will change in the "Last Updated" field when completed.

**PVS (SecurityCenter 4.2 and greater only)**

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

   ![Tip]

   To prevent the PVS scanner from starting automatically upon restarting the system, run the following command:

   ```bash
   # /sbin/chkconfig pvs off
   ```

2. Run the following command and save the challenge string that is displayed:

   ```bash
   # /opt/pvs/bin/pvs -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.

5. On the next page, copy the link that starts with http://plugins.nessus.org/v2/pvs.php... and bookmark it in your browser. The other information on the page is not relevant for use with SecurityCenter.

6. Select the bookmarked link, which will prompt you to download a file. Download the file, which will be called sc-passive.tar.gz.

7. Save the sc-passive.tar.gz on the system used to access your SecurityCenter GUI.

8. Log in to the SecurityCenter GUI as the admin user.

9. Navigate to the System -> Configuration page and select the Plugins/Feed option.

10. Click "Upload" on the Passive Plugins line and browse to the saved sc-passive.tar.gz file, and then upload to SecurityCenter.

11. The plugin update will take a few to several minutes to complete. The date and time will change in the "Last Updated" field when completed.

SecurityCenter Feed

If the Nessus offline plugin update process has already been performed, start at step 5 using the same link that was used for the Nessus offline plugin process, which starts with "http://plugins.nessus.org/get.php...".

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

To prevent the Nessus scanner from starting automatically upon restarting the system, run the following command:

```
# /sbin/chkconfig nessusd off
```

2. Run the following command and save the challenge string that is displayed:

```
# /opt/nessus/sbin/nessuscli 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.

5. On the next page, copy the link that starts with http://plugins.nessus.org/get.php... and save it as a favorite. Within the saved link change "all-2.0.tar.gz" to "SecurityCenterFeed48.tar.gz". This link will be needed for future use. Do not click the link for nessus-fetch.rc as it is not needed.

6. Go to the favorite you created, which will prompt you to download a file. Download the file, which will be called SecurityCenterFeed48.tar.gz.

7. Save the SecurityCenterFeed48.tar.gz on the system used to access your SecurityCenter GUI.
8. Log in to the SecurityCenter GUI as the admin user.

9. Navigate to the System -> Configuration page and select the Plugins/Feed option.

10. Click “Upload” on the SecurityCenter Feed line and browse to the saved `SecurityCenterFeed48.tar.gz` file, and then upload to SecurityCenter.

11. The plugin update will take several minutes to complete. The date and time will change in the “Last Updated” field when completed.
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. Two 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=target, DC=example, 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
LDAP Configuration

**Authentication**
- **Encryption**: None
- **Username**: ________________
- **Password**: ________________

**Server**
- **Directory Server**: ________________
- **Port**: ________________
- **Search Base**: ________________
- **Search String**: ________________

**Attributes**
- **Username Attribute**: ________________
- **E-mail Attribute**: ________________
- **Phone Attribute**: ________________
- **Name Attribute**: ________________

---

Submit  Cancel
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 “=*”:
Option 2

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

DC=target,DC=example,DC=com

The example above could be used along with a "Search String" for global usage. This search string, when used in the configuration, will apply to all LDAP searches.

memberOf=CN=nested1,OU=cftest1,DC=target,DC=example,DC=com

This field is currently limited to 128 characters; we will extend the viewable window and increase the allowed length going forward.

Option 2 Example

Step One:

a. Log in as an admin user.

b. Choose System -> Configuration -> LDAP
c. Click "Test LDAP Settings" to test configurations.
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: