Tenable Security Center 6.2.0 Common Criteria Evaluated Configuration Guide (CCECG)

Last Revised: September 4, 2023

Contents

Introduction

Tenable Security Center is a comprehensive vulnerability management solution that provides complete visibility into the security posture of your distributed and complex IT infrastructure. Tenable Security Center consolidates and evaluates vulnerability data from across your entire IT infrastructure, illustrates vulnerability trends over time, and assesses risk with actionable context for effective remediation prioritization.

Document Purpose and Scope

This document provides supplementary administrative guidance for Tenable Security Center 6.2.0.

This document describes procedures on how to prepare and operate the Tenable Security Center to meet its Common Criteria evaluated configuration. This document is referred to as the operational user guide in the Protection Profile for Application Software, version 1.4, dated 7 October 2021 ([PP_APP_v1.4]), and supplements the product documentation available from the Tenable web site at this URL:

https://docs.tenable.com/security-center.htm.

Note that any limitations or restrictions on the operation of the TOE described in this document take precedence over other product documentation.

Assumptions

The following assumptions about the operational environment of Tenable Security Center are reproduced from [PP_APP_v1.4].

Assumption	Description
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

References

[PP_APP_v1.4] Protection Profile for Application Software, version 1.4, 7 October 2021

[PKG_TLS_v1.1] Functional Package for Transport Layer Security (TLS), version 1.1, 1 March 2019

Overview of the Target of Evaluation

The Target of Evaluation (TOE) for Tenable Security Center comprises the security functionality specified in the Tenable Security Center 6.2.0 Security Target. In general, the following Tenable Security Center capabilities are considered to be within the scope of evaluation:

- **Protection of sensitive data at rest:** the TOE uses encryption to protect credentials and other sensitive data.
- **Protection of data in transit:** the TOE secures data in transit between itself and its operational environment using TLS and HTTPS. Note that the TOE also has one logical interface that uses SSH but it relies on the underlying OS platform to provide this.
- **Trusted updates:** the TOE provides visibility into its current running version and the vendor distributes updates to it that are digitally signed so that administrators can securely maintain up-to-date software.
- **Remote administration:** the TOE provides a Web GUI to administer its security functions. Note however that the bulk of the product's administration functions are outside the scope of the App PP and TLS Package and are therefore not part of the TOE.
- **Cryptographic services:** the TOE includes an implementation of OpenSSL with NIST-validated algorithm services that it uses to secure data at rest and in transit.
- **Secure interaction with operating system:** the TOE is designed to interact with its underlying host operating system platform in such a way that the TOE cannot be used as an attack vector to compromise an operating system.

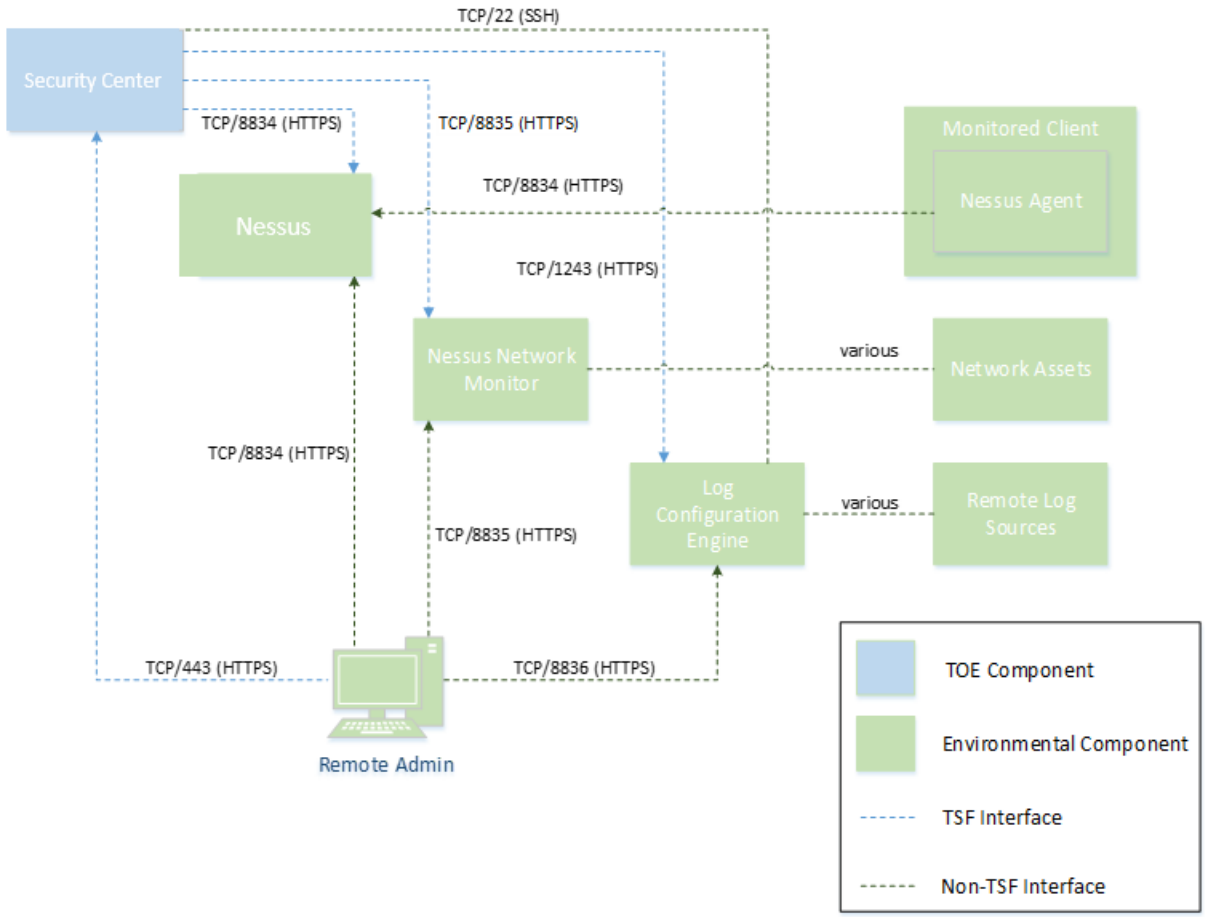
Tenable Security Center's scanning, data collection, vulnerability analysis, analytics, and incident response capabilities are outside the scope of evaluation, as is any other product behavior that is not described in [PP_APP_v1.4] or [PKG_TLS_v1.1]. The content and execution of plugins is similarly excluded from the TOE, although they are discussed in the context of network communications because Tenable Security Center must use platform network resources to acquire them and make them available to environmental applications.

Evaluated Configuration

The TOE comprises Security Center 6.2.0, which is a C application with a PHP web front-end running on Apache.

Figure 1 shows the TOE in a sample deployment with other Tenable applications in its operational environment.

Figure 1 - TOE Boundary



Access to Platform Resources

Other than the hardware resources ordinarily used by applications (such as central processing units, memory, input/output peripherals, and persistent storage), Tenable Security Center accesses only network connectivity resources provided by its platform. Tenable Security Center uses network connectivity for remote management and connections to environmental components.

Tenable Security Center restricts its access to sensitive information repositories on the platform to system configuration, which it accesses in order to generate a diagnostic report of local system configuration for troubleshooting purposes.

Hardware Requirements

Storage Requirements

Tenable recommends installing Tenable Security Center on direct-attached storage (DAS) devices (or storage area networks (SANs), if necessary) with a storage latency of 10 ms or less. Tenable does not support installing Tenable Security Center on network-attached storage (NAS).

Disk Space Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for deployments include raw network speed, the size of the network being monitored, and the configuration of the application. Processors, memory, and network cards will be heavily based on the former. Disk space requirements will vary depending on usage based on the amount and length of time data is stored on the system.

An important consideration is that Tenable Security Center can be configured to save a snapshot of vulnerability archives each day. In addition, the size of the vulnerability data stored by Tenable Security Center depends on the number and types of vulnerabilities, not just the number of hosts. For example, 100 hosts with 100 vulnerabilities each could consume as much data as 1,000 hosts with 10 vulnerabilities each. In addition, the output for vulnerability check plugins that do directory listings, etc. is much larger than Open Port plugins from discovery scans.

For networks of 35,000 to 50,000 hosts, Tenable has encountered data sizes of up to 25 GB. That number is based on storage of 50,000 hosts and approximately 500 KB per host.

Additionally, during active scanning sessions, large scans and multiple smaller scans have been reported to consume as much as 150 GB of disk space as results are acquired. Once a scan has completed and its results are imported, that disk space is freed up.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable Security Center	CPU Cores	Memory	Disk Space used for Vulnerability Trending
2,500 active IPs	4 x 2 GHz cores	8 GB RAM	90 days: 125 GB 180 days: 250 GB
10,000 active IPs	8 x 3 GHz cores	16 GB RAM	90 days: 450 GB 180 days: 900 GB
25,000 active IPs	16 x 3 GHz cores	32 GB RAM	90 days: 1.2 TB 180 days: 2.4 TB
100,000 active IPs	32 x 3 GHz cores	64 GB RAM	90 days: 4.5 TB 180 days: 9 TB

Requirements When Running Basic Network Scans + Local Checks + 1 Configuration Audit

# of Hosts Managed by Tenable Security Center	CPU Cores	Memory	Disk Space used for Vulnerability Trending
2,500 active IPs	4 x 2 GHz cores	8 GB RAM	90 days: 225 GB 180 days: 450 GB
10,000 active IPs	8 x 3 GHz cores	16 GB RAM	90 days: 900 GB 180 days: 1.8 TB
25,000 active IPs	16 x 3 GHz cores	32 GB RAM	90 days: 2.25 TB 180 days: 4.5 TB
100,000 active IPs	32 x 3 GHz cores	128 GB RAM	90 days: 9 TB 180 days: 18 TB

Disk Partition Requirements

Tenable Security Center installs into `/opt/sc`. Tenable highly recommends that you create the `/opt` directory on a separate disk partition. If you want to increase performance, consider using two disks: one for the operating system and one for the system deployed to `/opt`.

Tenable strongly recommends using high performance disks. Tenable Security Center is a disk-intensive application and using disks with high read/write speeds, such as SSDs, results in the best performance.

If required disk space exists outside of the `/opt` file system, mount the desired target directory using the command `mount --bind <olddir> <newdir>`. Make sure that the file system is automatically mounted on reboot by editing the `/etc/fstab` file appropriately.

Note: Tenable Security Center does not support using symbolic links for `/opt/sc/`. You can use symbolic links within `/opt/sc/` subdirectories if instructed by Tenable Security Center documentation or Tenable Support.

Deploying Tenable Security Center on a server configured with RAID disks can also dramatically boost performance.

Tip: Tenable does not require RAID disks for even our largest customers. However, in one instance, response times for queries with a faster RAID disk for a customer with more than 1 million managed vulnerabilities moved from a few seconds to less than a second.

Network Interface Requirements

Gigabit or faster network cards are recommended for use on the Tenable Security Center server. This is to increase the overall performance of web sessions, emails, Tenable Log Correlation Engine queries, and other network activities.

System Requirements

Operating System Requirements

The evaluated version of Tenable Security Center is supported on Red Hat Enterprise Linux 8 (RHEL) 8, 64-bit.

Evaluated Configuration Requirements

Confirm you have enabled the full disk encryption capabilities provided by the operating system on the host running Tenable Security Center. In addition, follow the instructions in Configure Tenable Security Center for NIAP Compliance. Tenable Security Center includes an implementation of OpenSSL with NIST-validated algorithm services that it uses to secure data at rest and in transit. The section Configure Tenable Security Center for NIAP Compliance provides instructions that configure the TOE's OpenSSL cryptographic module for conformance with the evaluated configuration. Use of other cryptographic engines was not evaluated or tested during the Common Criteria evaluation of Tenable Security Center.

SELinux Requirements

Tenable Security Center supports disabled, permissive, and enforcing mode Security-Enhanced Linux (SELinux) policy configurations.

- Disabled and permissive mode policies typically do not require customization to interact with Tenable Security Center
- Enforcing mode policies require customization to interact with Tenable Security Center. For more information, see Evaluated Configuration Requirements

Confirm you have enabled the full disk encryption capabilities provided by the operating system on the host running Tenable Security Center. In addition, follow the instructions in Configure Tenable Security Center for NIAP Compliance. Tenable Security Center includes an implementation of OpenSSL with NIST-validated algorithm services that it uses to secure data at rest and in transit. The section Configure Tenable Security Center for NIAP Compliance provides instructions that configure the TOE's OpenSSL cryptographic module for conformance with the evaluated configuration. Use of other cryptographic engines was not evaluated or tested during the Common Criteria evaluation of Tenable Security Center.

- SELinux Requirements.

> **Note:** Tenable recommends testing your SELinux configurations before deploying on a live network.

Secure Environment Requirements

Tenable recommends adhering to security best practices, including:

- Configure the operating system to ensure that security controls cannot be bypassed.
- Configure the network to ensure that the Tenable Security Center system resides in a secure network segment that is not accessible from the Internet.
- Configure network time synchronization to ensure that accurate time stamps are recorded in reports and log files.

  > **Note:** The time zone is set automatically during the installation process with no user interaction. The time zone configured in `php.ini` must be synchronized with the system time zone in `/etc/sysconfig/clock`.

- Configure access control to ensure that only authorized users have access to the operating system platform.

- Monitor system resources to ensure that adequate disk space and memory are available, as described in Hardware Requirements. If system resources are exhausted, Tenable Security Center may not log audit data during system administrator troubleshooting or other activities.

Dependencies

Note: Either OpenJDK or the Oracle Java JRE along with their accompanying dependencies must be installed on the system along with any additional Java installations removed for reporting to function properly.

Note: Tenable does not recommend forcing the installation without all required dependencies. If your installation of RHEL 8 is missing certain dependencies, it will cause problems that are not readily apparent with a wide variety of functions. Tenable Support has observed different types of failure modes for Tenable Security Center when dependencies are missing.

All dependencies must be installed on the system prior to installing the Tenable Security Center package. While they are not all required by the installation RPM file, some functionality of Tenable Security Center may not work properly if the packages are not installed.

Note: Tenable recommends using the latest stable production version of each package.

For a list of required packages, run the following command against the Tenable Security Center RPM file:

```
# yum deplist SecurityCenter-x.x.x-el8.x86_64.rpm
```

or

```
# dnf deplist SecurityCenter-x.x.x-el8.x86_64.rpm
```

To determine which version of a dependency is installed on your system, run the following command for each of the packages (replace “libtool” with the appropriate package):

```
# yum list installed | grep libtool
```

or

```
# dnf list installed | grep libtool
```

If one of the prerequisite packages is missing, it can be installed using the “yum” or “dnf” package managers. For example, install Java 1.8.0 with “yum” using the command below:

```
# yum -y install java-1.8.0-openjdk.x86_64
```

Tenable Security Center Communications and Directories

The following table summarizes the components' primary directories and communication methods.

Tenable Security Center Directories	
Installation Directory	`/opt/sc`
User Data	`/opt/sc/orgs/<Organization Serial Number>`
Repositories	`/opt/sc/repositories/<Repository Number>`
Admin Logs	`/opt/sc/admin/logs/`
Organization Logs	`/opt/sc/orgs/<Organization Number>/logs/`
Communication Interfaces	• User Access—HTTPS • Feed Updates—Acquired over SSL from Tenable servers directly to Tenable Security Center of for offline installation. Plugin packages are secured via 4096-bit RSA digital signatures. For more information, see Port Requirements.

For information about data encryption in Tenable Security Center, see Encryption Strength.

Customize SELinux Enforcing Mode Policies for Tenable Security Center

Security-Enhanced Linux (SELinux) enforcing mode policies require customization to interact with Tenable Security Center.

Tenable Support does not assist with customizing SELinux policies, but Tenable recommends monitoring your SELinux logs to identify errors and solutions for your policy configuration.

Before you begin:

- Install the SELinux `sealert` tool in a test environment that resembles your production environment.

To monitor your SELinux logs to identify errors and solutions:

1. Run the `sealert` tool, where `/var/log/audit/audit.log` is the location of your SELinux audit log:

   ```
   sealert -a /var/log/audit/audit.log
   ```

   The tool runs and generates a summary of error alerts and solutions. For example:

```
SELinux is preventing /usr/sbin/sshd from write access on the
sock_file /dev/log
SELinux is preventing /usr/libexec/postfix/pickup from using the
rlimitinh access on a process
```

2. Execute the recommended solution for each error alert.
3. Restart Tenable Security Center.
4. Run the `sealert` tool again to confirm you resolved the error alerts.

Use /dev/ random for Random Number Data Generation

Required User Role: Root user

To use `/dev/random` for random number data generation in Tenable Security Center.

1. Log in to Tenable Security Center via the command line interface (CLI).
2. In the CLI in Tenable Security Center, run the following command:

   ```
   export TSC_ENTROPY_CHECK=true
   ```

   Tenable Security Center recognizes the environment variable and uses `/dev/random`.

What to do next:

- Install or upgrade Tenable Security Center in order for your changes to take effect, as described in Verify and Install Tenable Security Center or Upgrade Tenable Security Center.

Port Requirements

Your Tenable Security Center instances require access to the following specific ports for inbound and outbound traffic.

Port	Inbound/Outbound	Traffic
TCP 22	Outbound	Communicating with Log Correlation Engine for event query (parsed log data).
TCP 443	Inbound	Accessing the Tenable Security Center interface.
TCP 1243	Outbound	Communicating with Log Correlation Engine to collect unaltered bulk log data.
TCP 8834	Outbound	Communicating with Nessus to retrieve scan results.
TCP 8835	Outbound	Communicating with Nessus Network Monitor to collect network traffic data.

Browser Requirements

Note: Tenable recommends using the newest available version of your browser.

You can access the Tenable Security Center user interface using the following browsers:

- Mozilla Firefox 87 or later
- Google Chrome 89 or later
- Mac OS Safari 14.02 or later
- Microsoft Edge 99 or later.

System Settings

The **System** menu in the left navigation and the **Username** menus in the top navigation bar contain several options to configure Tenable Security Center system settings, including Configuration Settings, User Profile Menu Settings, and Diagnostic Settings.

Configuration Settings

The Configuration menu includes the following settings:

- Data expiration settings—determine how long Tenable Security Center retains artefacts such as scan results and report results.
- External schedules settings—determine the update schedule for the common tasks of pulling Tenable Nessus Network Monitor and Tenable Log Correlation Engine data.

- Mail settings—designates SMTP settings for all email-related Tenable Security Center functions.
- Plugins/Feed Settings—displays the **Plugin Detail Locale** for Tenable Security Center and the feed and plugin update schedules. It also provides access to the **Tenable Security Center Software Updates** settings.

Tenable Security Center Software Updates

New updates and patches for Tenable Security Center appear in the **Tenable Security Center Software Updates** section of the **Plugins/Feed Configuration** page.

If you enable the **Enable Software Updates Through the Tenable Security Center Feed** option, then Tenable Security Center automatically applies Tenable Security Center patches during feed updates.

User Profile Menu Settings

The user profile icon in the top navigation bar includes the **About** menu item, which displays the Tenable Security Center version.

Diagnostic Settings

This page displays and creates information that assists in troubleshooting issues that may arise while using Tenable Security Center.

System Status

You can use this section to view the current status of system functions.

System Function	Description
Correct Java Version	Indicates whether the minimum version of Java required to support Tenable Security Center functionality is installed.
Sufficient Disk Space	Indicates whether you have enough disk space to support Tenable Security Center functionality. A red X indicates the disk is at 95%capacity or higher.
Correct RPM Package Installed	Indicates whether you have the correct Tenable Security Center RPM installed for your operating system.
Debugging	Indicates whether debugging is enabled. You may experience performance and storage issues if you leave debugging enabled for extended periods of time.
Migration Errors	Indicates whether an error occurred during a recent Tenable Security Center update.
PHP Integrity Errors	Indicates whether any PHP files have been modified from the original version included in the Tenable Security Center RPM.

Generate a Diagnostics File

Required User Role: Administrator

Tenable Support may ask you to generate a diagnostics file to assist with troubleshooting. The `debug.zip` diagnostics file contains files related to the selected chapters. For more information about diagnostics file options, see Diagnostics File Options.

To generate a diagnostics file for Tenable Support:

1. Log in to Tenable Security Center via the user interface.
2. In the left navigation, click **System > Diagnostics**.

   The **Diagnostics** page appears.
3. In the **Diagnostics File** section, click **Create Diagnostics File**.

   The page updates with options to configure the diagnostics file.
4. In the **General** section, if you want to omit IP addresses from the diagnostics file, click to enable the **Strip IPs from Chapters** toggle.
5. In the **Chapters** section, click the toggles to enable or disable the chapters you want to include in the diagnostics file.
6. Click **Generate** File.

   Tenable Security Center generates the diagnostics file.

7. Click **Download Diagnostics File**.

   The `debug.zip` file downloads.

What to do next:

- Share the `debug.zip` file with Tenable Support for troubleshooting.

Diagnostics File Options

Option	Description	Default
General		
Strip IPs from Chapters	When enabled, Tenable Security Center omits IP addresses from the following files: • `sc-configuration.txt` • `sc-scans.txt` • `sc-setup.txt` • `sc-logs.txt` • `sc-error.log` • `cert.log` • `install.log` • `upgrade.log` • `schemaUpdates*.log` • `sc-environment.txt` • `sc-telemetry.txt` • `/opt/sc/support/error_Log` • `/opt/sc/support/*.conf`	Disabled
Chapters		
System Information	Include information about the Tenable Security Center host system in the diagnostic file (`sc-systeminfo.txt`).	Enabled
Scan information	Include information about scans, scan results, and freeze windows in the diagnostic file (`sc-sscaninfo.txt`).	Enabled
Setup	Include information about Tenable Security Center resources in the diagnostic file (`sc-setup.txt`):	Enabled

Option	Description	Default
Logs	Include administrator logs, organization logs, Tenable Security Center error logs, and the certificate log in the diagnostic file (`sc-logs.txt`, `sc-error.log`, and `cert.log`).	Enabled
Environment	Include information about the `tns` user environment in the diagnostic file (`sc-environment.txt`).	Enabled
Directory Listing	Include a directory listing in the diagnostic file (`sc-dirlisting.txt`).	Enabled
Dependency	Include information about Tenable Security Center dependencies in the diagnostic file (`sc-depsinfo.txt`).	Enabled
Upgrade Log	Include a log of Tenable Security Center upgrade events in the diagnostic file (`upgrade.log`).	Enabled
Install Log	Include a log of Tenable Security Center installation events in the diagnostic file (`install.log`).	Enabled
Apache Log	Include a log of web server requests in the diagnostic file (`/opt/sc/support/error_Log`).	Enabled
Application Conf	Include Tenable Security Center configuration details in the diagnostic file (`sc-configuration.txt`).	Enabled
Server Conf	Include server configuration details in the diagnostic file (`/opt/sc/support/*.conf`).	Enabled
User Information	Include a list of users in the diagnostic file (`scusers. txt`). The list includes the following details: • For administrators, the user ID and role ID • For organizational users, the user ID, role ID, and group ID	Enabled
Include Names	(If **User Information** is enabled) Include usernames and user display names for each user in the diagnostic file.	Disabled

Installation and Upgrade

Tenable distributes Tenable Security Center for installation and upgrade as a .rpm file digitally signed by Tenable using a 2048-bit RSA key. The RPM package manager verifies the digital signature prior to performing the install or upgrade operation.

Before You Install

> **Note:** A basic understanding of Linux is assumed throughout the installation and upgrade processes.

Understand Tenable Security Center Licenses

Confirm your licenses are valid for your Tenable Security Center deployment. Tenable Security Center does not support an unlicensed demo mode.

Disable Default Web Servers

Tenable Security Center provides its own Apache web server listening on port 443. If the installation target already has another web server or other service listening on port 443, you must disable that service on that port or configure Tenable Security Center to use a different port after installation.

Identify which services, if any, are listening on port 443 by running the following command:

```
# ss -pan | grep ':443 '
```

If there are any services listening on port 443, you must either disable them or run them on a different port.

Modify Security Settings

Tenable Security Center supports disabled, permissive, and enforcing mode Security-Enhanced Linux (SELinux) policy configurations. For more information, see Evaluated Configuration Requirements

Confirm you have enabled the full disk encryption capabilities provided by the operating system on the host running Tenable Security Center. In addition, follow the instructions in Configure Tenable Security Center for NIAP Compliance. Tenable Security Center includes an implementation of OpenSSL with NIST-validated algorithm services that it uses to secure data at rest and in transit. The section Configure Tenable Security Center for NIAP Compliance provides instructions that configure the TOE's OpenSSL cryptographic module for conformance with the evaluated configuration. Use of other cryptographic engines was not evaluated or tested during the Common Criteria evaluation of Tenable Security Center.

SELinux Requirements.

Perform Log File Rotation

The installation does not include a log rotate utility; however, the native Linux `logrotate` tool is supported post-installation. In most Red Hat environments, `logrotate` is installed by default. The following logs are rotated if the `logrotate` utility is installed:

- All files in `/opt/sc/support/logs` matching `*log`
- `/opt/sc/admin/logs/sc-error.log`

During an install/upgrade, the installer drops a file named `SecurityCenter` into `/etc/logrotate.d/` that contains log rotate rules for the files mentioned above.

Log files are rotated on a monthly basis. This file is owned by `root/root`.

Allow Tenable Sites

To allow Tenable Security Center to communicate with Tenable servers for product updates and plugin updates, Tenable recommends adding Tenable sites to an allow list at the perimeter firewall.

Obtain Signing Key

To allow installation packages to be verified, it is necessary to obtain Tenable's public key for signature. This can be obtained from the Tenable Downloads Site under "Signing Keys" – "RPM-GPG-KEY-Tenable-4096."

Once this file has been downloaded, run the following:

```
# rpm --import <public key file>
```

NOTE: the same signing key is used for upgrade packages; do not remove it following initial installation.

Verify and Install Tenable Security Center

Required User Role: Root user

Caution: When performing `sudo` installs, use `sudo -i` to ensure the proper use of environmental variables.

Caution: During the installation process, Tenable Security Center produces a log file in a temporary location: `/tmp/sc.install.log`. Once the installation process finishes, the file is stored here: `/opt/sc/admin/logs/install.log`. Do not remove or modify these files; they are important for debugging in case of a failed installation.

Before you begin:

- Complete system prerequisites, as described above in Before You Install.
- Download the installation RPM file from the Tenable Security Center downloads page. If necessary, depending on the operating system of the host, move the installation RPM file onto the host.
- In order to enable Tenable Security Center to use `/dev/random` instead of `/dev/urandom` to generate random number data for secure communication functions, modify the random data source as described in Use /dev/ random for Random Number Data Generation.

To install Tenable Security Center:

1. On the host where you want to install Tenable Security Center, open the command line interface (CLI).
2. Verify the integrity of the RPM file by running the following:

   ```
   # rpm -Kv SecurityCenter-x.x.x-el8.x86_64.rpm
   ```

3. Run one of the following commands to install the RPM:

   ```
   # yum install SecurityCenter-x.x.x-el8.x86_64.rpm
   ```

   or

   ```
   # dnf install SecurityCenter-x.x.x-el8.x86_64.rpm
   ```

   Output similar to the following is generated:

   ```
   # dnf install SecurityCenter-x.x.x-el8.x86_64.rpm
   Preparing... ########################################## [100%]
   1:SecurityCenter ##########################################
   [100%]
   Installing Nessus plugins ... complete
   Applying database updates ... complete.
   By default, SecurityCenter will listen for HTTPS requests on
   ALL available interfaces. To complete your installation, please
   point your web browser to one of the following URL(s):
   https://x.x.x.x
   Starting SecurityCenter services
   [ OK ] SecurityCenter services: [ OK ]
   #
   ```

   The system installs the package into `/opt/sc` and attempts to start all required daemons and web server services.

   Tip: In rare cases, a system restart is required after installation in order to start all services.

Before You Upgrade

Note: A basic understanding of Linux is assumed throughout the installation and upgrade processes.

Java Version Requirements

If you have not installed the Oracle Java JRE or OpenJDK, Tenable Security Center displays the following warning:

```
[WARNING] SecurityCenter has determined that Oracle Java JRE and
OpenJDK is not installed. One of two must be installed for
SecurityCenter reporting to function properly.
```

You must install the latest version of Oracle Java JRE or OpenJDK to take full advantage of Tenable Security Center reporting.

Halt or Complete Running Jobs

Tenable recommends stopping all running Tenable Security Center processes before beginning an upgrade. If processes are running (for example, Tenable Nessus scans), Tenable Security Center displays the following message along with the related process names and their PIDs:

```
SecurityCenter has determined that the following jobs are still
running. Please wait a few minutes before performing the upgrade
again. This will allow the running jobs to complete their tasks.
```

Stop the processes manually or retry the upgrade after the processes complete.

Perform a Tenable Security Center Backup

Perform a backup of Tenable Security Center before beginning your upgrade.

Rename Your Mount Point

If the existing `/opt/sc` directory is or contains a mount point to another location, rename the mount point. During the RPM upgrade process, a message appears with information about the discovered mount point. Contact your system administrator for assistance.

Upgrade Tenable Security Center

Required User Role: Root user

Caution: During the upgrade process, Tenable Security Center produces a log file in a temporary location: `/tmp/sc.install.log`. Once the upgrade process finishes, the file is stored here: `/opt/sc/admin/logs/install.log`. Do not remove or modify these files; they are important for debugging in case of a failed upgrade.

Before you begin:

- Complete system prerequisites, as described above in Before You Upgrade.
- Download the upgrade RPM file from the Tenable Security Center downloads page. If necessary, depending on the operating system of the host, move the upgrade RPM file onto the host.
- In order to enable Tenable Security Center to use `/dev/random` instead of `/dev/urandom` to generate random number data for secure communication functions, modify the random data source as described in Use /dev/ random for Random Number Data Generation.

To upgrade Tenable Security Center:

1. On the host where you want to install Tenable Security Center, open the command line interface (CLI).
2. Pause all running scans.
4. Prepare the upgrade command you intend to run:
    - Use `yum` or `dnf` with the `upgrade` switch from the command-line of the Tenable Security Center server.
    - Use "`sudo -i`" when performing `sudo` upgrades of Tenable Security Center to ensure the proper use of environmental variables.

    For example:

    ```
    # yum upgrade SecurityCenter-x.x.x-el8.x86_64.rpm
    ```

    or

    ```
    # dnf upgrade SecurityCenter-x.x.x-el8.x86_64.rpm
    ```

    The upgrade begins. Tenable Security Center is not available until the upgrade finishes.

    ```
    # dnf upgrade SecurityCenter-x.x.x-el8.x86_64.rpm
    Preparing... ########################################## [100%]
    Shutting down SecurityCenter services: [ OK ]
    Backing up previous application files ... complete.
    1:SecurityCenter ##########################################
    [100%]
    Applying database updates ... complete.
    Beginning data migration.
    Starting plugins database migration...complete.
    (1 of 4) Converting Repository 1 ... complete.
    (2 of 4) Converting Repository 2 ... complete.
    (3 of 4) Converting Repository 3 ... complete.
    (4 of 4) Converting Repository 4 ... complete.
    ```

```
Migration complete.
Starting SecurityCenter services: [ OK ]
#
```

Configure Scans

Resources

Nessus Scanners

Add a Nessus Scanner

Required User Role: Administrator

To add a Tenable Nessus scanner to Tenable Security Center:

1. Log in to Tenable Security Center via the user interface.
2. Click **Resources > Tenable Nessus Scanners**.

   The **Tenable Nessus Scanners** page appears.
3. At the top of the table, click **Add**.

   The **Add Tenable Nessus Scanner** page appears.
4. Configure Tenable Nessus scanner options.
   a. In the **Name** box, type a name for the scanner.
   b. In the **Description** box, type a description for the scanner.
   c. In the **Host** box, type the hostname or IP address for the scanner.
   d. In the **Port** box, view the default (**8834**) and modify, if necessary.
   e. If you want to disable this scanner's connection to Tenable Security Center, click **Enabled** to disable the connection.
   f. If you want to verify that the hostname or IP address entered in the **Host** option matches the CommonName (CN) presented in the SSL certificate from the Tenable Nessus scanner, click **Verify Hostname** to enable the toggle.
   g. If you want to use the proxy configured in Tenable Nessus for communication with the scanner, click **Use Proxy** to enable the toggle.
   h. In the **Type** drop-down box, select the authentication type.
   i. If you selected **Password** as the **Type**:
      i. In the **Username** box, type the username for the account generated during the Tenable Nessus installation for daemon-to-client client communications.
      ii. In the **Password** box, type the password associated with the username you provided.

j. If you selected **SSL Certificate** as the **Type**:

i. Click **Choose File** to upload the `nessuscert.pem` file you want to use for authentication to the scanner. For more information, see Manual Tenable Nessus SSL Certificate Exchange.

ii. (Optional) If the private key that decrypts your SSL certificate is encrypted with a passphrase, in the **Certificate Passphrase** box, type the passphrase for the private key.

k. Check the box for all active scan zones you want to use this scanner.

l. If you want this scanner to provide Tenable Nessus Agent scan results to Tenable Security Center:

i. Click **Agent Capable** to enable the toggle.

ii. Check the box for one or more **Organizations** that you want to grant access to import Tenable Nessus Agent data into Tenable Security Center.

iii. If you want to use secure API keys when importing agent scan data from Tenable Nessus scanners:

1. Click **API Keys** to enable the toggle.
2. In the **Access Key** box, type the access key.
3. In the **Secret Key** box, type the secret key.

5. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

- Configure a scan zone, repository, and active scan objects.

Nessus Network Monitor Instances

Add a Nessus Network Monitor Instance

Required User Role: Administrator

To add a Tenable Nessus Network Monitor instance to Tenable Security Center:

1. Log in to Tenable Security Center via the user interface.
2. Click **Resources > Tenable Nessus Network Monitors**.

   The **Tenable Nessus Network Monitor Scanners** page appears.

3. At the top of the table, click **Add**.

   The **Add Tenable Nessus Network Monitor Scanner** page appears.

4. Configure the settings as follows:
    a. In the **Name** box, type a name for the scanner.
    b. In the **Description** box, type a description for the scanner.
    c. In the **Host** box, type the hostname or IP address for the scanner.
    d. In the **Port** box, view the default (**8835**) and modify, if necessary.
    e. If you want to disable this scanner's connection to Tenable Security Center, click **Enabled** to disable the connection.
    f. If you want to verify that the hostname or IP address entered in the **Host** option matches the CommonName (CN) presented in the SSL certificate from the Tenable Nessus Network Monitor server, click **Verify Hostname** to enable the toggle.
    g. If you want to use the proxy configured in Tenable Nessus Network Monitor for communication with the scanner, click **Use Proxy** to enable the toggle.
    h. In the **Type** drop-down box, select the authentication type.
    i. If you selected **Password** as the **Type**:
        i. In the **Username** box, type the username for the account generated during the Tenable Nessus Network Monitor installation for daemon-to-client client communications.
        ii. In the **Password** box, type the password for the account generated during the Tenable Nessus Network Monitor installation for daemon-to-client client communications.
    j. If you selected **SSL Certificate** as the **Type**:
        i. Click **Choose File** to upload a certificate.
        ii. (Optional) If the private key that decrypts your SSL certificate is encrypted with a passphrase, in the **Certificate Passphrase** box, type the passphrase for the private key.
    k. In the **Repositories** list, select one or more repositories where you want Tenable Security Center to store the scanner data.
5. Click **Submit**.

    Tenable Security Center saves your configuration.

Analyze Data

Dashboards

Required User Role: Administrator or organizational user with appropriate permissions

Administrator users can view Tenable-provided **Overview**, **LCE Overview**, and **Health Overview** dashboards.

Organizational users can configure custom or template-based *dashboards* that contain *dashboard components*, which display vulnerability, event, ticket, user, and alert data for analysis. When viewing vulnerability or event data, you can drill into the underlying dataset for further evaluation.

Tip: Tenable provides many dashboard templates (for example, the VPR Summary dashboard).

Dashboards allow you to organize similar dashboard components to streamline your analysis. Instead of creating a single dashboard with several dozen dashboard components, you can create several dashboards that group similar dashboard components together. For example, you can create two separate dashboards to view active scanning data and passive scanning data.

Note: Dashboards display vulnerability, event, and other scan data. Tenable recommends configuring several data sources to optimize the data you see in dashboards.

Tip: Tenable provides many dashboard templates (for example, the VPR Summary dashboard).

View a Dashboard

To view a dashboard:

1. Log in to Tenable Security Center via the user interface.
2. Click **Dashboard > Dashboard**.

   The **Dashboards** page appears, displaying your default dashboard.
3. If you want to switch to a different dashboard:
   a. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.
   b. Click the dashboard you want to view.

      The dashboard appears.

      If you are an organizational user, you can:

      - Add a dashboard component to the dashboard in view.

- Manage dashboard components on the dashboard in view.
- Edit the dashboard settings for the dashboard in view.
- Share or revoke access to the dashboard in view.
- Create a report from the dashboard in view.
- Delete the dashboard in view.
- Customize the table.

Workflow Actions

Workflow actions allow organizational users to configure and manage alerting, ticketing, and accept risk or recast risk rules. These functions allow the user to be notified of and properly handle vulnerabilities and events as they come in.

Alerts

Tenable Security Center can be configured to perform actions, such as email alerts, for select vulnerability or alert occurrences to various users regardless of whether the events correlate to a local vulnerability or not. Other alert actions include UI notifications, creating or assigning tickets, remediation scans, launching a report, email notifications, and syslog alerting. Multiple actions can be assigned for each ticket.

Alert Actions

Tenable Security Center automatically performs alert actions when an alert triggers. You can configure the following types of alert actions:

- Assign Ticket
- Email
- Generate Syslog
- Launch Scan
- Launch Report
- Notify Users.

Add an Alert

Required User Role: Organizational user with appropriate permissions

You can configure Tenable Security Center to send alerts for vulnerability occurrences.

To add an alert:

1. Log in to Tenable Security Center via the user interface.
2. Click **Workflow > Alerts**.

The **Alerts** page appears.

3. Click **Add**.

   The **Add Alert** page appears.

4. In the **Name** box, type a name.
5. (Optional) In the **Description** box, type a description.
6. (Optional) Click the **Schedule** field to select the frequency of alerts, time, timezone, and whether to repeat sending alerts at the specified time.
7. (Optional) In the **Behavior** drop-down box, select the condition you want to trigger the alert. The default is **Perform actions only on first trigger**.
8. (Optional) In the **Type** drop-down box, select the data type for the condition.
9. In the **Trigger** drop-down box, select the trigger for the alerts.
10. (Optional) In the **Query** drop-down box, select the dataset to compare with the trigger condition.
11. (Optional) Click **Add Filter** and provide the details of the selected filter.
12. Click **Add Actions** to specify an action that occurs when the alert triggers.
13. Click **Submit**.

    Tenable Security Center creates the alert.

View an Alert

Required User Role: Organizational user with appropriate permissions

You can view the summary details of an alert with the name, behavior, condition applied, status, created date, owner, and ID.

To view the details of an alert:

1. Log in to Tenable Security Center via the user interface.
2. Click **Workflow > Alerts**.

   The **Alerts** page appears.

3. In the table, right-click the row for the alert you want to view.

   The actions menu appears.

   -or-

   In the table, select the check box for the alert you want to view.

   The available actions appear at the top of the table.

4. Click **View**.

   The **View Alert** page appears.

Edit an Alert

Required User Role: Organizational user with appropriate permissions

To edit an alert:

1. Log in to Tenable Security Center via the user interface.
2. Click **Workflow > Alerts**.

   The **Alerts** page appears.
3. In the table, right-click the row for the alert you want to edit.

   The actions menu appears.

   -or-

   In the table, select the check box for the alert you want to edit.

   The available actions appear at the top of the table.
4. Click **More > Edit**.

   The **Edit Alert** page appears.
5. Modify the alert options.
6. Click **Submit**.

   Tenable Security Center saves the modified alert.

Evaluate an Alert

Required User Role: Organizational user with appropriate permissions

To evaluate an alert:

1. Log in to Tenable Security Center via the user interface.
2. Click **Workflow > Alerts**.

   The **Alerts** page appears.
3. In the table, right-click the row for the alert you want to edit.

   The actions menu appears.

   -or-

   In the table, select the check box for the alert you want to edit.

   The available actions appear at the top of the table.

4. Click **Evaluate**.

   The alert is submitted for evaluation.

   Tenable Security Center returns the evaluation results for the alert.

Delete an Alert

Required User Role: Organizational user with appropriate permissions

To delete an alert:

1. Log in to Tenable Security Center via the user interface.
2. Click **Workflow > Alerts**.

   The **Alerts** page appears.
3. In the table, right-click the row for the alert you want to edit.

   The actions menu appears.

   -or-

   In the table, select the check box for the alert you want to edit.

   The available actions appear at the top of the table.
4. Click **More > Delete**.

   A confirmation window appears.
5. Click **Delete**.

   Tenable Security Center deletes the alert.

Additional Resources

Encryption Strength

Tenable Security Center uses the following default encryption for storage and communications.

Function	Encryption
Storing TNS user account passwords	SHA-512 and the PBKDF2 function
Storing user and service accounts for scan credentials	AES-256-CBC
Storing scan data	None
Communications between Tenable Security Center and clients (Tenable Security Center users).	TLS 1.2 with the strongest encryption method supported by Tenable Security Center Apache and your browser: EECDH+AESGCM, EDH+AESGCM, AES256+EECDH, or AES256+EDH.
Communications between Tenable Security Center and the Tenable product registration server	TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384
Communications between Tenable Security Center and the Tenable plugin update server	TLS 1.2 with ECDHE-RSA-AES256-GCM-SHA384
Communications between Tenable Security Center and: • Tenable Nessus • Tenable Nessus Network Monitor • Tenable Log Correlation Engine	TLS 1.2 with the strongest encryption method supported by Tenable Security Center Apache and your browser: ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-SHA384, or ECDHE-RSA-AES256-GCM-SHA384

Configure SSL/TLS Strong Encryption

To configure SSL/TLS strong encryptions for Tenable Security Center communications:

1. Open the `/opt/sc/support/conf/sslciphers.conf` file in a text editor.
2. Add the following content at the end of the file:

```
SSLCipherSuite <cipher you want to use for SSL/TLS encryption>
```

For example:

```
# SSL Ciphers
SSLProtocol ALL -SSLv2 -SSLv3
SSLHonorCipherOrder On
SSLCompression off
SSLCipherSuite ECDHE-RSA-AES128-SHA256:ECDHE-RSA-AES128-GCM-
SHA256:ECDHE-RSAAES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384
```

3. Restart Tenable Security Center.
4. In `/opt/sc/support/logs`, open `ssl_request_log`.
5. Verify the configuration in `ssl_request_log` matches the cipher you specified. If the configuration and cipher do not match, investigate the following:
   - Confirm that you provided the cipher using correct syntax.
   - Confirm that your browser supports the cipher you provided.
   - Confirm that you do not have other applications installed that redirect or layer additional encryption for SSL traffic.

Configure Tenable Security Center for NIAP Compliance

Before you begin:

- If you are using SSL certificates to log in to Tenable Security Center, ensure your server and client certificates are NIAP-compliant. For more information about certificate authentication, see Certificate Authentication.
- Confirm you have enabled the full disk encryption capabilities provided by the operating system on the host running Tenable Security Center.

To configure Tenable Security Center for NIAP compliance:

1. Log in as the `root` or `tns` user to the Tenable Security Center host server via the command line interface (CLI)
2. Run the following commands to configure evaluated TLS encryption for Tenable Security Center communications:

```
# /opt/sc/support/bin/sqlite3 /opt/sc/application.db "INSERT
INTO Configuration (type,name,value,visible,editable ) VALUES (
64, 'SSLVersion', 'TLSv1_2', 'false','false' )"
```

```
# /opt/sc/support/bin/sqlite3 /opt/sc/application.db "INSERT
INTO Configuration (type,name,value,visible,editable ) VALUES (
64, 'SSLCipherList', 'ECDHE-RSAAES128-SHA256:ECDHE-RSA-AES128-
GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSAAES256-GCM-SHA384',
'false', 'false' )"
```

3. Configure the Tenable Security Center web server to use strong encryption for storage and communications, as described above in Configure SSL/TLS Strong Encryption.

   Note: For NIAP compliance, you must configure TLS 1.2 encryption with any of the following ciphers: ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-SHA384, or ECDHE-RSA-AES256-GCM-SHA384.

4. If you connect Tenable Security Center to Tenable Nessus, Tenable Nessus Network Monitor, or Tenable Log Correlation Engine, you must use certificates to authenticate the TLS connection. For more information, see the next section (Manual Tenable Nessus SSL Certificate Exchange).

Manual Tenable Nessus SSL Certificate Exchange

Caution: 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 Tenable Nessus SSL Certificates and Keys

Nessus supports authentication protocols based on the OpenSSL toolkit (for more information about the toolkit, see http://www.openssl.org/). This provides cryptographic protection and secure authentication.

In the example described in this document, there are three key system components: the certificate authority; the Nessus server; and the Nessus client (Tenable Security Center). It is necessary to generate the keys required for the TLS 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 CA holds a copy of the certificates for registered users to certify that the certificate is genuine. When the CA receives a certificate signing request (CSR), it validates and signs the certificate.

In the example provided in this document, the CA resides on the Nessus server (which is not the recommended method for a production environment). In a proper PKI deployment, the CA 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 CA, 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 TLS. The Nessus server has users defined that authenticate to it either by simple login and password or via TLS. These users will also have keys associated with them.

Nessus Client (Tenable Security Center)

The Nessus client, Tenable Security Center, communicates with the Nessus server via TLS. It uses keys generated for a Nessus client and stores these keys and the certificate for the CA in the `/opt/sc/daemons` directory. These keys must be owned by the "`tns`" userid.

Tenable Nessus Certificate Configuration for Unix

The following topic describes the commands and relevant files involved in the Nessus TLS process on a Red Hat Linux system. This process creates the following files:

File Name Created and its Purpose	Where to Copy to
`/opt/nessus/com/nessus/CA/cacert.pem` 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.	`/opt/nessus/com/nessus/CA` on the initial Nessus server and any additional Nessus servers that need to authenticate using TLS.
`/opt/nessus/com/nessus/CA/servercert.pem` This is the public certificate for the Nessus server that is sent in response to a CSR.	`/opt/nessus/com/nessus/CA` on any additional Nessus servers that need to authenticate using TLS.
`/opt/nessus/var/nessus/CA/cakey.pem` 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	`/opt/nessus/com/nessus/CA` on any additional Nessus servers that need to authenticate using TLS.
`/opt/nessus/var/nessus/CA/serverkey.pem` This is the private key of the Nessus server.	`/opt/nessus/com/nessus/CA` on any additional Nessus servers that need to authenticate using TLS.

Create Nessus Client Keys

The Nessus user, in this case the user ID that Tenable Security Center 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 is a concatenation of **cert**_, the user name you entered and .**pem**. Additionally, the key filename is 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 is created if it does not already exist. The following files are created by this command:

File Name Created	Purpose
`/tmp/nessus-xxxxxxxx/cert_{user-}.pem`	This is the public certificate for the specified user.
`/tmp/nessus-xxxxxxxx/key_{user-}.pem`	This is the private key for the specified user.
`/opt/nessus/var/nessus/users/{user}/auth/dname`	This is the distinguished name to be associated with this user. The distinguished name consists of a number of options separated by commas in the following format: /C={country}/ST={state}/L={location}/OU={organizational unit}/O={organization}/CN={common name}

Create and Deploy TLS Authentication for Nessus

An example SSL Certificate configuration for Nessus to Tenable Security Center authentication is included below:

In the example described here, Tenable Security Center and the Nessus scanner are defined as follows. Your configuration varies:

Tenable Security Center:
IP: 192.0.2.50
OS: Red Hat ES 5

Nessus Scanner:
IP: 192.0.2.202
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
-------------------------------------------------------------------
                Creation of the Nessus SSL Certificate
-------------------------------------------------------------------
This script will now ask you the relevant information to create the
SSL certificate of Nessus. Note that this information will *NOT* be
sent to anybody (everything stays local), but anyone with the ability
to connect to your Nessus daemon will be able to retrieve this
information.
CA certificate life time in days [1460]:
Server certificate life time in days [365]:
Your country (two letter code) [US]:
Your state or province name [NY]:
Your location (e.g. town) [New York]:
Your organization [Nessus Users United]: Tenable Network Security
This host name [Nessus4_2]:

Congratulations. Your server certificate was properly created.

The following files were created :
. Certification authority :
   Certificate = /opt/nessus//com/nessus/CA/cacert.pem
   Private key = /opt/nessus//var/nessus/CA/cakey.pem
. Nessus Server :
   Certificate = /opt/nessus//com/nessus/CA/servercert.pem
   Private key = /opt/nessus//var/nessus/CA/serverkey.pem
```

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

```
# /opt/nessus/sbin/nessuscli 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
Type 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
```

Note: The `nessuscert.pem` file is used when configuring the Nessus scanner on Tenable Security Center. 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 are 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 following command for your system. The example here is for Red Hat:

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

Change the Nessus Mode of Authentication

In Tenable Security Center, update your Tenable Nessus scanner configuration to use SSL certificate-based authentication.

Considerations for Custom Certificates

During an upgrade, Tenable Security Center 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

After you configure authentication on one Tenable Nessus scanner, you can use the same SSL certificates and user names to authenticate other Tenable Nessus scanners.

User Access

Log In to the Web Interface

Log In to the Web Interface via SSL Client Certificate

Required User Role: Any

Before you begin:

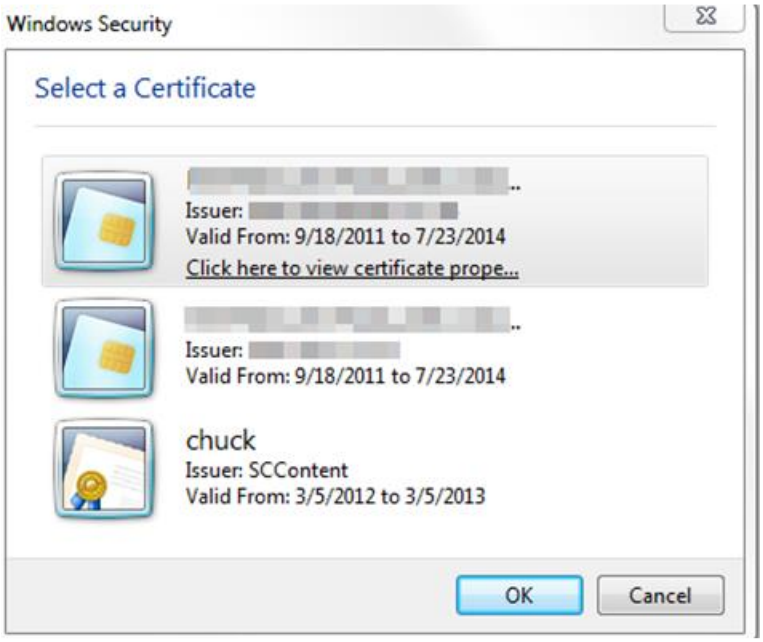
- Confirm your Tenable Security Center administrator fully configured Tenable Security Center for certificate authentication, as described in Certificate Authentication.

To perform a certificate-based Tenable Security Center login:

Note: 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.

1. Open a browser window and navigate to Tenable Security Center.

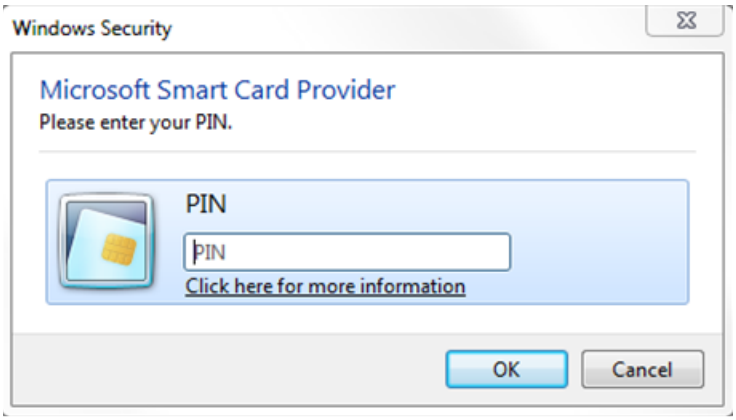
   The browser presents a list of available certificate identities.



   For information about Tenable Security Center-browser communications encryption, see Encryption Strength.

2. Select a certificate.
3. Click **OK**.

   An authentication prompt appears (if required to access your certificate).



4. (Optional) If prompted, type a PIN or password.
5. Click **OK**.

   The Tenable Security Center login page appears.
6. Log in using the username to be associated with the selected certificate.

   Caution: Only one Tenable Security Center 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.

   The **Certificate Authentication** window appears.
7. When prompted, specify whether the current certificate is to be used to authenticate the current user.
   - Click **Yes** to always use the certificate for authentication.
   - Click **No** to ignore the certificate and log in via TNS authentication.

   Tenable Security Center logs you in.

Subsequent Logins

After you log out of Tenable Security Center, the login page appears. If you want to log in again with the same certificate, refresh your browser window. If you want to use a different certificate, you must start a new browser session.

After you perform your second certificate login, edit your account from the **Profile** page to view your certificate details. If your certificate changes or you need to revoke it, click the **Clear Certification Details** button to disassociate the certificate from your account.

Certificate Authentication

You can use configure SSL client certificate authentication for Tenable Security Center user account authentication. Tenable Security Center supports:

- SSL client certificates
- smart cards

- personal identity verification (PIV) cards
- Common Access Cards (CAC).

Configuring certificate authentication is a multi-step process.

To fully configure SSL client certificate authentication for Tenable Security Center user accounts:

1. Configure Tenable Security Center to allow SSL client certificate authentication, as described in Configure Tenable Security Center to Allow SSL Client Certificate Authentication.
2. Configure Tenable Security Center to trust certificates from your CA, as described in Trust a Custom CA.
3. Add TNS-authenticated user accounts for the users you want to authenticate via certificate, as described in Add a TNS-Authenticated User.
4. In order to validate client certificates, configure OCSP in Tenable Security Center, as described in Configure OCSP Validation in Tenable SecurityCenter.

What to do next:

- Instruct users to log in to Tenable Security Center via certificate, as described in Log In to the Web Interface via SSL Client Certificate.

Configure Tenable Security Center to Allow SSL Client Certificate Authentication

You must configure the Tenable Security Center server to allow SSL client certificate connections. For complete information about certificate authentication, see Certificate Authentication.

To allow SSL client certificate authentication:

1. Open the `/opt/sc/support/conf/sslverify.conf` file in a text editor.
2. Edit the **SSLVerifyClient** setting:

Value	Description
none (default)	Tenable Security Center does not accept SSL certificates for user authentication.
require	Tenable Security Center requires a valid SSL certificate for user authentication.
optional	Tenable Security Center accepts but does not require a valid SSL certificate for user authentication. If a user does not present a certificate, they can log in via username and password. **Note:** Some browsers may not connect to Tenable Security Center when you use the optional setting.

Value	Description
optional_no_ca	Tenable Security Center accepts valid and invalid SSL certificates for user authentication. **Tip:** This setting does not configure reliable user authentication, but you can use it to troubleshoot issues with your SSL connection and determine whether there is an issue with the key or the CA.

3. Edit the **SSLVerifyDepth** setting to specify the length of the certificate chain you want Tenable Security Center to accept for user authentication. For example:
   - When set to **0**, Tenable Security Center accepts self-signed certificates.
   - When set to **1**, Tenable Security Center does not accept intermediate certificates. Tenable Security Center accepts self-signed certificates or certificates signed by known CAs.
   - When set to **2**, Tenable Security Center accepts up to 1 intermediate certificate. Tenable Security Center accepts self-signed certificates, certificates signed by known CAs, or certificates signed by unknown CAs whose certificate was signed by a known CA.
4. Save the file.

   Tenable Security Center saves your configuration.

Trust a Custom CA

Required User Role: tns user

You can configure Tenable Security Center to trust a custom CA for certificate authentication or other uses.

To configure Tenable Security Center to trust a custom CA:

1. Log in to Tenable Security Center via the user interface.
2. Copy the required PEM-encoded CA certificate (and intermediate CA certificate, if needed) to the Tenable Security Center server's `/tmp` directory.

   In this example, the file is named `ROOTCA2.cer`.
3. Run the `installCA.php` script to create the required files for each CA in `/opt/sc/data/CA`:

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

   Tenable Security Center processes all the CAs in the file.
4. Restart Tenable Security Center.

Add a TNS-Authenticated User

Required User Role: Administrator or organizational user with appropriate permissions.

To add a TNS-authenticated user account as an administrator user:

1. Log in to Tenable Security Center via the user interface.
2. Click **Users > Users**.

   The **Users** page appears.
3. Click **Add**.

   The **Add User** page appears.
4. Select a **Role**.
5. If you selected **Security Manager** as the **Role**, select an **Organization**.
6. (Optional) Type a **First Name** and **Last Name**.
7. Type a **Username** and **Password** for the user.
8. If the **Type** drop-down box is visible, select **TNS**.
9. (Optional) Enable **User Must Change Password**.
10. Select a **Time Zone**.
11. (Optional) Select a **Scan Result Default Timeframe**.
12. (Optional) Enable **Cached Fetching**.
13. (Optional) Enable **Password Expiration** for the user.
14. (Optional) Enable **Dark Mode** for the user.
15. (Optional) Type **Contact Information** for the user.
16. Click **Submit**.

    Tenable Security Center saves your configuration.

To add a TNS-authenticated user account as an organizational user:

1. Log in to Tenable Security Center via the user interface. You must log in with a user account belonging to the organization where you want to create a new user.
2. Click **Users > Users**.

   The **Users** page appears.
3. Click **Add**.

   The **Add User** page appears.
4. (Optional) Type a **First Name** and **Last Name** for the user.
5. If the **Type** drop-down box is visible, select **TNS**.

6. Type a **Username** and **Password** for the user.
7. (Optional) Enable **User Must Change Password**.
8. Select a **Time Zone**.
9. (Optional) Select a **Scan Result Default Timeframe**.
10. (Optional) Enable **Cached Fetching**.
11. (Optional) Enable **Password Expiration** for the user.
12. Select a **Role**.
13. Select a **Group**.
14. (Optional) If you want to customize the group-related permissions for the user, modify the **Group Permissions**.
15. (Optional) If you want to share an asset list with the user, select an **Asset**.
16. (Optional) Enable **Dark Mode** for the user.
17. (Optional) Type **Contact Information** for the user.
18. Click **Submit**.

    Tenable Security Center saves your configuration.

Configure OCSP Validation in Tenable SecurityCenter

Required User Role: Root user

You can configure Online Certificate Status Protocol (OCSP) validation in Tenable Security Center to prevent users from authenticating to Tenable Security Center if their certificate matches a revocation on your OCSP server.

Note: Tenable Support does not assist with OCSP configuration in Tenable Security Center.

Before you begin:

- Confirm that you have an OCSP server configured in your environment.

To configure OCSP validation in Tenable Security Center:

1. In a text editor, open the `/opt/sc/support/conf/sslverify.conf` file.
    a. Set the **SSLVerifyClient** setting to **Require** or **Optional**.
    b. Set the **SSLVerifyDepth** setting.
    c. Save the file.

    Tenable Security Center saves your configuration.
2. In a text editor, open the `/opt/sc/support/conf/vhostssl.conf` file.
    a. Add the following content at the end of the file:

```
SSLOCSPEnable on
SSLOCSPDefaultResponder <URI>
SSLOCSPOverrideResponder on
```

Where <URI> is the URI for your OCSP server.

b. Save the file.

Tenable Security Center saves your configuration.

3. Restart Tenable Security Center.