Tenable Security Center 6.6.x User Guide

Last Revised: August 25, 2025

Table of Contents

Welcome to Tenable Security Center

This user guide describes how to install, configure, and manage Tenable Security Center™ 6.6.x.

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.

To get started, see Get Started With Tenable Security Center.

For additional information on Tenable Security Center, review the following customer education materials:

- Tenable Security Center Introduction (Tenable University)

Tenable Security Center and Tenable Security Center Director

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.

Tenable Security Center Director is an add-on to Tenable Security Center that provides centralized console insight to reduce complexity and give multiple-console customers complete visibility across their entire network.

Tenable Security Center and Tenable Security Center Director Feature Comparison

Feature	Tenable Security Center	Tenable Security Center Director
Remote repository import (for cumulative data analysis)	X	X

Retrieve data from individual scans		X
Monitor status and configuration of scanning tier instances and connected sensors		X
Centralized scan capability with scanning tiers via the API		X

Get Started With Tenable Security Center

Use the following getting started sequence to configure and mature your Tenable Security Center deployment.

1. [Prepare](#)

2. [Install](#)

3. [Configure Scans](#)

4. [Refine](#)

5. [Expand](#)

> **Tip:** For additional information on Tenable Security Center, review the following customer education materials:
>
> - [Tenable Security Center Introduction (Tenable University)](#)

Prepare

Before you begin, learn about Tenable Security Center and establish a deployment plan and analysis workflow to guide your configurations.

- Access Tenable Support and training resources for Tenable Security Center, including:

    - the [Tenable University](#) training courses

    - the [Tenable Scan Strategy](#) guide

- Design a deployment plan by identifying your organization's objectives and analyzing your network topology. Consider Tenable-recommended best practices for your environment. For more information about environment requirements, see Requirements. For information about scan types, see Scanning Overview.

- Design an analysis workflow. Identify key stakeholders in your management and operational groups, considering the data you intend to share with each stakeholder.

For more information about planning a large enterprise deployment of Tenable Security Center, see the Tenable Security Center Large Enterprise Deployment Guide.

For more information about the basic architecture of a Tenable Security Center deployment, see Tenable Security Center Architecture.

Install

Install Tenable Security Center and perform initial configuration.

1. Depending on your environment, install in your environment or deploy or install with Tenable Core.

   For complete information about Tenable Core + Tenable Security Center, see the Tenable Core User Guide.

2. Perform quick setup, as described in Quick Setup. You can:

   - Upload licenses

   - Configure one Tenable Nessus scanner

   - Configure one Tenable Network Monitor scanner (requires a Tenable Network Monitor activation license)

   - Configure one Tenable Log Correlation Engine server (requires an Tenable Log Correlation Engine® activation license)

   - Create one repository

   - Create one organization

   - Configure one LDAP server

- Create one administrator user account and one security manager account

- Configure usage statistic collection

Tenable recommends following the quick setup wizard, but you can configure these features later. For example, do not configure LDAP until you have easy access to all necessary LDAP parameters.

3. Configure SMTP settings, as described in [Mail Settings](#).

4. Configure scan zones, as described in [Add a Scan Zone](#).

5. Configure additional repositories, if necessary, as described in [Repositories](#).

6. Configure additional scanners, if necessary, as described in [Tenable Nessus Scanners](#), [Tenable Network Monitor Instances](#), and [Tenable Log Correlation Engines](#).

7. Configure security settings (e.g., password complexity requirements and custom banners), as described in [Security Settings](#).

Configure Scans

Configure and run basic scans to begin evaluating the effectiveness of your deployment plan and analysis workflow.

1. Configure credentials, as described in [Credentials](#).

2. Create static assets, as described in [Add a Custom Asset](#). For more information about asset types, see [Assets](#).

3. Configure a Host Discovery policy and a Basic Network Scan policy from Tenable-provided scan policy templates, as described in [Add a Scan Policy](#).

4. Configure and run scans for those policies, as described in [Add an Active Scan](#) and [Add an Agent Scan](#).

5. Confirm that the scans can access all areas of your network with no credential issues.

6. Configure Tenable Network Monitor scanners, as described in [Tenable Network Monitor Instances](#).

7. When the scans complete, create template-based dashboards and reports, as described in

Dashboards and Reports.

8. Search for vulnerabilities by CVE ID, as described in Search.

Tenable recommends frequently reviewing your scan results and scan coverage. You may need to modify your scan configurations to suit your organization's objectives and reach all areas of your network.

Refine

Configure other features, if necessary, and refine your existing configurations.

- Configure audit files, as described in Audit Files.

- Create additional scan policies, as described in Add a Scan Policy.

- Configure scan freeze windows, as described in Add a Freeze Window.

- Configure groups, as described in Add a Group.

- Create a custom user role, as described in Create a User Role.

- Create additional user accounts and share objects with users, as described in User Accounts.

- Create dynamic assets and combination assets, as described in Add a Custom Asset. For more information about asset types, see Assets.

- Review the plugin update schedule, as described in Edit Plugin and Feed Settings and Schedules. Consider editing the schedules to suit your needs. For example, you may want to schedule plugin and feed updates to run a few hours before your scheduled scans.

- Add queries and use filters, as described in Add or Save a Query and Apply a Filter.

- Create custom dashboards and reports, as described in Dashboards and Reports.

- Create Assurance Report Cards (ARCs), as described in Assurance Report Cards.

- Configure alerts, ticketing, accept risk rules, and recast risk rules, as described in Workflow Actions.

- View vulnerability data and use the built-in analysis tools, as described in Vulnerability Analysis.

Expand

Review and mature your deployment plan and analysis workflow.

- Conduct weekly meetings to review your organization's responses to identified vulnerabilities.

- Conduct weekly management meetings to oversee your teams executing the analysis workflow.

- Review scan automation settings and consider revising.

- Review your scan results and scan coverage. You may need to modify your scan configurations to suit your organization's objectives and reach all areas of your network.

- Optimize and operationalize your custom dashboards to meet the needs of individual user account holders.

- Optimize and operationalize your custom reports to prepare them for distribution.

- Consider configuring API integrations, as described in the *Tenable Security Center API Guide* and the *Tenable Security Center API Best Practices Guide*.

- Consider synchronizing Tenable Security Center with Tenable Lumin to take advantage of Cyber Exposure features, as described in Tenable One Synchronization.

Expand into Tenable One

> **Note:** This requires a Tenable One license. For more information about trying Tenable One, see Tenable One.

Integrate Tenable Security Center with Tenable One and leverage the following features:

- Access the **Exposure View** page, where you can gain critical business context by getting business-aligned cyber exposure score for critical business services, processes and functions, and track delivery against SLAs. Track overall risk to understand the risk contribution of assets to your overall Cyber Exposure Score, including by asset class, vendor, or by tags.

  - View and manage cyber exposure cards.

  - View CES and CES trend data for the Global and **Computing Resources** exposure cards.

  - View Remediation Service Level Agreement (SLA) data.

  - View Tag Performance data.

- Access the **Exposure Signals** page, where you can generate exposure signals that use queries to search for asset *violations*. Simply put, if an asset is impacted by a weakness related to the query, then the asset is considered a *violation*. Using this, you can gain visibility into your most critical risk scenarios.

    - Find top active threats in your environment with up-to-date feeds from Tenable Research.

    - View, generate, and interact with the data from queries and their impacted asset violations.

    - Create custom exposure signals to view business-specific risks and weaknesses

- Access the **Inventory** page, where you can enhance asset intelligence by accessing deeper asset insights, including related attack paths, tags, exposure cards, users, relationships, and more. Improve risk scoring by gaining a more complete view of asset exposure, with an asset exposure score that assesses total asset risk and asset criticality.

    - View and interact with the data on the **Assets** tab:

        - Review your AD assets to understand the strategic nature of the interface. This should help set your expectations on what features to use within Tenable Exposure Management, and when.

        - Familiarize yourself with the Global Asset Search and its objects and properties. Bookmark custom queries for later use.

        - Find devices, user accounts, software, cloud assets, SaaS applications, networks, and their weaknesses.

        - Drill down into the **Asset Details** page to view asset properties and all associated context views.

    - View and interact with the data on the **Weaknesses** tab:

        - View key context on vulnerability and misconfiguration weaknesses to make the most impactful remediation decisions.

    - View and interact with the data on the **Software** tab:

- Gain full visibility of the software deployed across your business and better understand the associated risks.

- Identify what software may be out of date, and which pieces of software may soon be End of Life (EoL).

○ View and interact with the data on the **Findings** tab:

- View instances of weaknesses (vulnerabilities or misconfigurations) appearing on an asset, identified uniquely by plugin ID, port, and protocol.

- Review insights into those findings, including descriptions, assets affected, criticality, and more to identify potential security risks, visibility on under-utilized resources, and support compliance efforts.

• Access the **Attack Path** page, where you can optimize risk prioritization by exposing risky attack paths that traverse the attack surface, including web apps, IT, OT, IoT, identities, ASM, and prevent material impact. Streamline mitigation by identifying choke points to disrupt attack paths with mitigation guidance, and gain deep expertise with AI insights **(Not supported in FedRAMP environments)**.

○ View the **Dashboard** tab for a high-level view of your vulnerable assets such as the number of attack paths leading to these critical assets, the number of open attack techniques and their severity, a matrix to view paths with different source node exposure score and ACR target value combinations, and a list of trending attack paths.

- Review the **Top Attack Path Matrix** and click the **Top Attack Paths** tile to view more information about paths leading to your "Crown Jewels", or assets with an ACR of 7 or above.

You can adjust these if needed to ensure you're viewing the most critical attack path data.

○ On the **Top Attack Techniques** tab, view all attack techniques that exist in one or more attack paths that lead to one or more critical assets by pairing your data with advanced graph analytics and the MITRE ATT&CK® Framework to create attack techniques, which allow you to understand and act on the unknowns that enable and amplify threat impact on your assets and information.

- On the **Top Attack Paths** tab, generate attack path queries to view your assets as part of potential attack paths:

  - Generate an Attack Path with a Built-in Query

  - Generate an Attack Path Query with the Attack Path Query Builder

  - Generate an Asset Query with the Asset Query Builder

  Then, you can view and interact with the Attack Path Query and Asset Query data via the query result list and the interactive graph.

  - Interact with the **MITRE ATT&CK Heatmap** tab.

- View and interact with the data in the **Tags** page:

  - Create and manage tags to highlight or combine different asset classes.

  - View the **Tag Details** page to gain further insight into the tags associated with your assets.

Tenable Security Center Architecture

Physical Architecture

At a high level, a Tenable Security Center deployment has two parts:

- A central Tenable Security Center console to manage scans, reports, user access, and other application tools.

- One or more scanners to collect data and report results to the Tenable Security Center console.
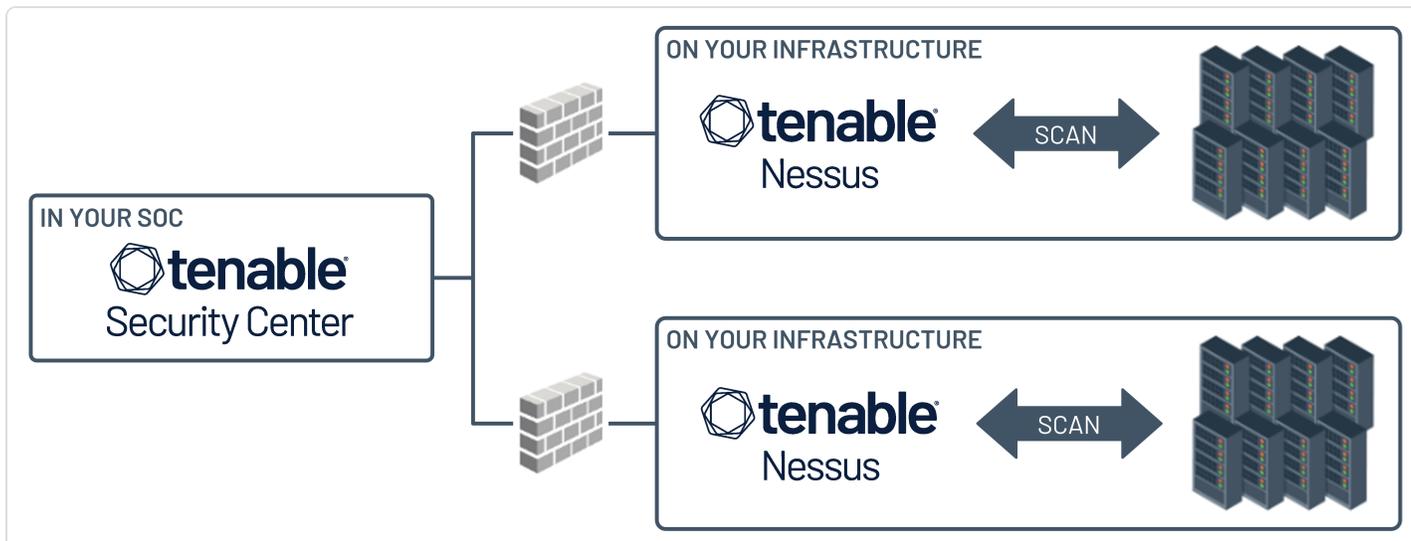
Logical Architecture

Tenable Security Center is divided into organizations. Each organization has access to one or more repositories that store scan data. For example, users in Organization 1 can only see repositories that are assigned to Organization 1, however, a repository can be assigned to more than one organization.

The highest-level user in an organization is the Security Manager. For more information about user permissions, see User Roles.

Very broadly, the logical layout / architecture of Tenable Security Center looks like this:
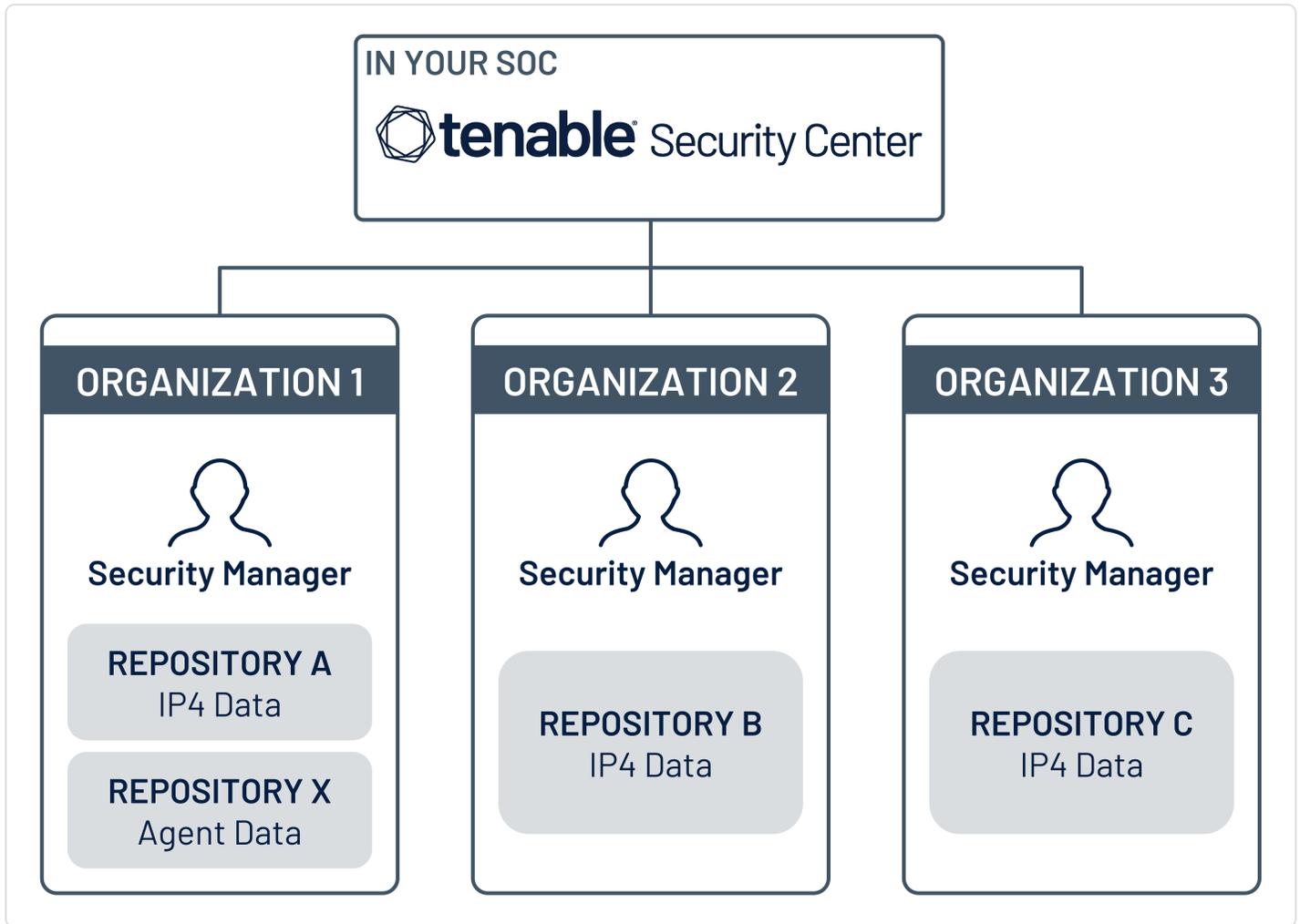
Many environments have just one organization. The following are some common use cases for multiple organizations:

- Environments where there are multiple departments or entities in a business that are logically independent, but that are all governed by the same structure.

- Acquisitions – there may be a reason to keep the acquiring company and acquired company separate.

Considerations for Air-Gapped Environments

Consider the following when deploying Tenable Security Center in an air-gapped (offline) environment.

Architecture

You must deploy a Tenable Security Center and a set of scanners within each air-gapped network.

If you want to consolidate data from other networks with the data generated in your air-gapped network, you can use offline repositories to export data from your air-gapped Tenable Security Center to your other instance of Tenable Security Center. This supports both consolidated and federated reporting structures.

Upgrades and Updates

Tenable recommends performing Tenable Security Center upgrades at least once a year (quarterly preferred) and plugin/feed updates at least once a month. After you perform a plugin update, run comprehensive scans to take advantage of the new vulnerability data and generate current scan results.

> **Note:** A few plugins require internet access and cannot run in an air-gapped environment. For example, Tenable Nessus plugin 52669 checks to see if a host is part of a botnet.

After you perform a plugin update or feed update, verify the files as described in the knowledge base article.

To perform a Tenable Security Center upgrade or a plugin/feed update offline:

> **Tip:** You can use the API to automate some Tenable Security Center upgrade and plugin update process.

1. Download the files in a browser or via the API.

2. Verify the integrity of the files.

   - Tenable Security Center upgrade: Compare the download checksum with the checksum on the Tenable downloads page

   - Plugin/feed update: Download and compare the checksums.

3. Move the files to your Tenable Security Center instance.

4. Upload the files to Tenable Security Center.

   - Tenable Security Center upgrade: via the CLI.

   - Plugin/feed update: in a browser or via the API.

Tenable Agents

If you deployed Tenable Nessus Manager to manage Tenable Agents in an air-gapped environment, perform an offline software update (`nessus-agent-updates-X.X.X.tar.gz` on the Tenable Downloads site) on your Tenable Nessus Manager. Tenable Nessus Manager pushes the update to the managed Tenable Agents.

For more information, see the knowledge base article.

Requirements

You can run Tenable Security Center in the following environments.

Environment			More Information
Tenable Core	Virtual	VMware	Requirements in the *Tenable Core User Guide*
		Microsoft Hyper-V	
	Cloud	Amazon Web Services (AWS)	
	Hardware		
Other platforms	Cloud	Amazon Web Services (AWS)	Cloud Requirements
	Hardware		Hardware Requirements

For general information about other requirements to run Tenable Security Center, see:

Hardware Requirements

Cloud Requirements

System Requirements

License Requirements

Port Requirements

Browser Requirements

Tenable Integrated Product Compatibility

Large Enterprise Deployments

Hardware Requirements

You can run Tenable Security Center on hardware, with or without Tenable Core. For more information about Tenable Core, see the [Tenable Core User Guide](#).

> **Note:** Tenable strongly discourages running Tenable Security Center or Tenable Core + Tenable Security Center in an environment shared with other Tenable applications.

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 milliseconds or less.

Tenable does not support installing Tenable Security Center on network-attached storage (NAS), including network filesystems such as NFS.

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 are heavily based on the former. Disk space requirements 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 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 2GHz cores	8 GB RAM	90 days: 125 GB 180 days: 250 GB
10,000 active IPs	8 3GHz cores	16 GB RAM	90 days: 450 GB 180 days: 900 GB
25,000 active IPs	16 3GHz cores	32 GB RAM	90 days: 2.4 TB 180 days: 5 TB
100,000 active IPs	32 3GHz 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 2GHz cores	8 GB RAM	90 days: 225 GB 180 days: 450 GB
10,000 active IPs	8 3GHz cores	16 GB RAM	90 days: 900 GB 180 days: 1.8 TB
25,000 active IPs	16 3GHz cores	32 GB RAM	90 days: 4.5 TB 180 days: 9 TB
100,000 active IPs	32 3GHz cores	128 GB RAM	90 days: 9 TB 180 days: 18 TB

Note: Tenable Security Center is a memory and disk I/O-intensive application. If you deploy Tenable Security Center in a virtualized infrastructure, take care to avoid running Tenable Security Center in a manner in which it may attempt to draw on oversubscribed resources, especially memory and disk I/O. Refer to your vendor-specific virtualized infrastructure

documentation for guidance on optimizing virtual infrastructure resource allocation, such as [Best Practices for Oversubscription of CPU, Memory and Storage in vSphere Virtual Environments](#) for VMware.

Disk Partition Requirements

Note: When you upgrade Tenable Security Center to version 6.6.x, you must have at least 6 GB of space in the `/tmp` folder, if the `/tmp` folder is in its own partition.

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

You can install Tenable Security Center in externally connected or air-gapped environments. For more information about special considerations for air-gapped environments, see [Considerations for Air-Gapped Environments](#).

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.

External PostgreSQL Requirements

You can install Tenable Security Center configured to work with a PostgreSQL instance managed by you. PostgreSQL is required for certain features. For more information about connecting a PostgreSQL database, see Connect an External PostgreSQL Server.

This is a required configuration if you have more than 100K hosts. Tenable Security Center requires PostgreSQL version 13 or later. It is also recommended that `wal_segment_size` is set to be at least 64MB.

Your PostgreSQL instance should meet the following sizing requirements. Please note that the disk space in the following table is only for PostgreSQL data, and does not include any other OS or other dependencies you have.

# of Hosts Managed by Tenable Security Center	CPU Cores	Memory	Minimum Disk Space Required for PostgreSQL Data
2,500 active IPs	4 2GHz cores	16 GB RAM	10 GB
10,000 active IPs	4 2GHz cores	32 GB RAM	40 GB
25,000 active IPs	8 2GHz cores	64 GB RAM	100 GB
100,000 active IPs	8 2GHz cores	64 GB RAM	400 GB

Cloud Requirements

The primary method to deploy Tenable Security Center in a cloud environment is with Tenable Core + Tenable Security Center. For more information, see the Tenable Core User Guide.

However, you can install Tenable Security Center in vendor-supported version of your cloud environment that meets the operating system requirements to run Tenable Security Center.

The following guidelines can help you install Tenable Security Center in an Amazon Elastic Compute Cloud (Amazon EC2) cloud-based environment or an Azure Virtual Machine (Azure Virtual Image) cloud-based environment, but they do not cover all deployment scenarios or cloud environments. For assistance with a different cloud environment, contact [Tenable Professional Services](#).

- [Supported Amazon EC2 Instance Types](#)
- [Supported Amazon Machine Images (AMIs)](#)
- [Supported Azure Instance Types](#)
- [Supported Azure Machine Images](#)
- [Tenable Security Center in Kubernetes Requirements](#)
- [External PostgreSQL Requirements](#)

Supported Amazon EC2 Instance Types

You can install Tenable Security Center in an Amazon Elastic Compute Cloud (Amazon EC2) cloud-based environment that meets all of the following requirements.

Tenable Security Center uses a balance of networking and compute resources and requires persistent storage for proper operation. To meet these requirements, Tenable supports installing Tenable Security Center on M5 instances with General Purpose SSD (gp2) EBS storage.

Tenable recommends the following Amazon EC2 instance types based on your Tenable Security Center deployment size.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable Security Center	EC2 Instance Type	Disk Space Used for Vulnerability Trending
1 to 2,500	m5.2xlarge	90 days: 125 GB 180 days: 250 GB
2,501 to 10,000	m5.4xlarge	90 days: 450 GB 180 days: 900 GB
10,001 to 25,000	m5.8xlarge	90 days: 2.4 TB

		180 days: 5 TB
25,001 to 50,000	m5.12xlarge	90 days: 4.5 TB
		180 days: 9 TB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.	

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

# of Hosts Managed by Tenable Security Center	EC2 Instance Type	Disk Space Used for Vulnerability Trending
1 to 2,500	m5.4xlarge	90 days: 225 GB
		180 days: 450 GB
2,501 to 10,000	m5.8xlarge	90 days: 900 GB
		180 days: 1.8 TB
10,001 to 25,000	m5.8xlarge	90 days: 4.5 TB
		180 days: 9 TB
25,001 to 50,000	m5.12xlarge	90 days: 9 TB
		180 days: 18 TB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.	

Supported Amazon Machine Images (AMIs)

Tenable provides an AMI for Tenable Core, but not for other cloud deployments without Tenable Core. Tenable supports using the following Amazon Marketplace AMI for Tenable Security Center without Tenable Core:

- [CentOS Stream 9 (x86_64)](#)

- [Red Hat Enterprise Linux 9](#)

- [Red Hat Enterprise Linux 8](#)

Configuration considerations:

- These AMIs may not include Java, but Tenable Security Center requires OpenJDK or the Oracle Java JRE to export PDF reports.

  You must install OpenJDK or the Oracle Java JRE onto your AMI before hosting Tenable Security Center. For more information, see [Dependencies](#).

- These AMIs may configure an SELinux enforcing mode policy, which requires customization to be compatible with Tenable Security Center.

  You must use the SELinux `sealert` tool to identify errors and solutions. For more information, see [Customize SELinux Enforcing Mode Policies for Tenable Security Center](#).

- You must confirm these AMIs meet all other standard requirements for operating systems. For more information, see [Operating System Requirements](#).

Supported Azure Instance Types

You can install Tenable Security Center in an Azure Virtual Machine (Azure Virtual Image) cloud-based environment that meets all of the following requirements.

Tenable recommends the following virtual machine instance types based on your Tenable Security Center deployment size. You may need to increase the storage allocated to the virtual machine instance depending on usage.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable Security Center	Virtual Machine Instance	Disk Space Used for Vulnerability Trending
1 to 2,500	D3V2	90 days: 125 GB 180 days: 250 GB
2,501 to 10,000	D4V2	90 days: 450 GB

		180 days: 900 GB
10,001 to 25,000	F16	90 days: 2.4 TB
		180 days: 5 TB
25,001 to 50,000	F32SV2	90 days: 4.5 TB
		180 days: 9 TB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.	

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

# of Hosts Managed by Tenable Security Center	EC2 Instance Type	Disk Space Used for Vulnerability Trending
1 to 2,500	D3V2	90 days: 125 GB
		180 days: 250 GB
2,501 to 10,000	D4V2	90 days: 900 GB
		180 days: 1.8 TB
10,001 to 25,000	F16	90 days: 4.5 TB
		180 days: 9 TB
25,001 to 50,000	D32SV3	90 days: 9 TB
		180 days: 18 TB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.	

Supported Azure Machine Images

Tenable provides an Azure image for Tenable Core, but not for other cloud deployments without Tenable Core. Tenable supports using the following Azure images for Tenable Security Center:

- [Oracle Linux 8 or 9 VM](#)

- [Red Hat Enterprise Linux 8 or 9 VM](#)

Configuration considerations:

- These images may not include Java, but Tenable Security Center requires OpenJDK or the Oracle Java JRE to export PDF reports.

  You must install OpenJDK or the Oracle Java JRE onto your image before hosting Tenable Security Center. For more information, see [Dependencies](#).

- These images may configure an SELinux enforcing mode policy, which requires customization to be compatible with Tenable Security Center.

  You must use the SELinux `sealert` tool to identify errors and solutions. For more information, see [Customize SELinux Enforcing Mode Policies for Tenable Security Center](#).

- You must confirm these images meet all other standard requirements for operating systems. For more information, see [Operating System Requirements](#).

Tenable Security Center in Kubernetes Requirements

> **Note:** Tenable recommends using an empty Kubernetes cluster for Tenable Security Center deployments. These requirements assume that the Kubernetes cluster where you install Tenable Security Center has nothing else installed.

Tenable strongly recommends using high-performance disks when you deploy Tenable Security Center in a Kubernetes cluster. Tenable Security Center is a disk-intensive application and using disks with high read/write speeds (for example, SSDs or NVMe SSDs) results in the best performance. The requirements in the following tables are based on AWS M5 or better processor specifications. Using slower processors, like those found in AWS M5a instances, will impact performance for your Tenable Security Center in Kubernetes deployment.

For supported Kubernetes environments and installation instructions, see [Tenable Security Center in Kubernetes](#).

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable Security Center	CPU	Memory	Disk Space used for Vulnerability Trending
1 to 2,500 active IPs	8000 m	32 GiB	90 days: 125 GB 180 days: 250 GB
2,501 to 10,000 active IPs	16000 m	64 GiB	90 days: 450 GB 180 days: 900 GB
10,001 to 25,000 active IPs	32000 m	128 GiB	90 days: 2.4 TB 180 days: 5 TB
25,001 to 50,000 active IPs	48000 m	192 GiB	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	Memory	Disk Space used for Vulnerability Trending
1 to 2,500 active IPs	16000 m	64 GiB	90 days: 225 GB 180 days: 450 GB
2,501 to 10,000 active IPs	32000 m	128 GiB	90 days: 900 GB 180 days: 1.8 TB
10,001 to 25,000 active IPs	32000 m	128 GiB	90 days: 4.5 TB 180 days: 9 TB
25,001 to 50,000 active IPs	48000 m	192 GiB	90 days: 9 TB 180 days: 18 TB

External PostgreSQL Requirements

You can install Tenable Security Center configured to work with a PostgreSQL instance managed by you. PostgreSQL is required for certain features. For more information about connecting a PostgreSQL database, see Connect an External PostgreSQL Server.

This is a required configuration if you have more than 100K hosts. Tenable Security Center requires PostgreSQLversion 13 or later.It is also recommended that `wal_segment_size` is set to be at least 64MB.

If you set up your PostgreSQL instance in a cloud environment, the following are guidelines for choosing your instance size. Note that the disk space in the following table is only for PostgreSQL data, and does not include any other OS or other dependencies you have.

# of Hosts Managed by Tenable Security Center	AWS	Azure	Minimum Disk Space Required for PostgreSQL Data
2,500 active IPs	r6g.xlarge	E4ps	10 GB
10,000 active IPs	r6g.2xlarge	E8ps	40 GB
25,000 active IPs	r6g.4xlarge	E16ps	100 GB
100,000 active IPs	r6g.8xlarge	E32ps	400 GB

System Requirements

- Operating System Requirements

- SELinux Requirements

- Secure Environment Requirements

- Dependencies

- Tenable Security Center Communications and Directories

Operating System Requirements

This version of Tenable Security Center is available for:

- Red Hat Enterprise Linux 8 (RHEL 8), 64-bit

- Red Hat Enterprise Linux 9 (RHEL 9), 64-bit

- CentOS Stream 9, 64-bit

- Oracle Linux 8, 64-bit

- Oracle Linux 9, 64-bit

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 Customize SELinux Enforcing Mode Policies for Tenable Security Center.

> **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. For more information about troubleshooting resource exhaustion, see [General Tenable Security Center Troubleshooting](#).

For information about secure administration of a Red Hat installation, see the *Red Hat Enterprise Linux Security Guide* for your version.

> **Note:** As with any application, the security and reliability of the installation is dependent on the environment that supports it. It is strongly recommended that organizations deploying Tenable Security Center have an established and applied IT management policy that covers system administration integrity, resource monitoring, physical security, and disaster recovery.

Dependencies

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.

- 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.

- You must upgrade pyTenable to version 1.4.2 or later.

- To run Tenable Security Center, you must install binutils and initscripts. If you try to migrate from Tenable Security Center 5.23.x or earlier to a current version of Tenable Security Center on a system that does not have binutils or initscripts installed, the migration will fail.

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

> **Note:** Tenable does not recommend forcing the installation without all required dependencies. If your version of Red Hat or CentOS 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.

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

```
# yum deplist SecurityCenter-x.x.x-el6.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.

> **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.

Tenable Security Center Directories	
Installation Directory	`/opt/sc`
User Data	`/opt/sc/orgs/<Organization Serial Number>`

Tenable Security Center Directories	
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 or 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, as described in <u>Start, Stop, or Restart Tenable Security</u> <u>Center</u>.

   Tenable Security Center restarts.

4. Run the `sealert` tool again to confirm you resolved the error alerts.

Use /dev/random for Random Number Data Generation

Required Tenable Security Center User Role: Root user

If your organization requires 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 using an environment variable.

Unlike `/dev/urandom`, `/dev/random` blocks HTTPS and SSL/TLS functions if there is not enough entropy to perform the functions. The functions resume after the system generates enough entropy.

Note: If `/dev/random` blocks during an installation or upgrade, the system waits up to 10 minutes for more entropy to be generated before halting the operation.

Tenable does not recommend using `/dev/random` unless required by your organization.

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 Install Tenable Security Center or Upgrade Tenable Security Center.

Tenable Security Center Database Journaling Modes

By default, Tenable Security Center databases that can significantly impact performance use write-ahead logging (WAL) journaling mode. All other databases use DELETE mode. Tenable Security Center also supports converting WAL journaling mode databases to DELETE mode.

For Tenable Security Center installations where WAL is not enabled, enabling WAL may resolve issues with excessive database locks. If your Tenable Security Center does not experience database locking issues, Tenable recommends leaving your Tenable Security Center databases in the default journaling mode.

Tenable strongly recommends performing a backup before converting database journaling modes and performing regular backups after converting database journaling modes. For more information, see Backup and Restore.

For general information about SQLite3 database journaling modes, see the SQLite3 documentation.

For more information, see:

- Enable Write-Ahead Logging

- Disable Write-Ahead Logging

> **Note:** If you previously converted one or more Tenable Security Center databases to WAL journaling mode without using the `convertDatabaseMode.php` script, you must use the `convertDatabaseMode.php` script to ensure your Tenable Security Center databases are fully converted to WAL journaling mode.

WAL Requirements

> **Note**: Write-ahead logging mode typically uses more disk space than DELETE mode. Consider your disk space availability before enabling write-ahead logging. Tenable recommends the same amount of disk space that is occupied by the database.

In addition to the requirements to run Tenable Security Center, your Tenable Security Center installation must be running Tenable Security Center 5.19.x or later.

Databases Affected

Enabling or disabling WAL converts the database journaling mode for the following Tenable Security Center databases:

- `/opt/sc/application.db`

- `/opt/sc/hosts.db`

- `/opt/sc/jobqueue.db`

- `/opt/sc/plugins.db`

- `/opt/sc/remediationHierarchy.db`

- `/opt/sc/orgs/<orgID>/organization.db` (for each organization in your Tenable Security Center)

- `/opt/sc/orgs/<orgID>/assets.db` (for each organization in your Tenable Security Center)

The `convertDatabaseMode.php` script only converts the database journaling mode for Tenable Security Center databases that can significantly impact performance.

Enable Write-Ahead Logging

> **Required Tenable Security Center User Role:** Root user

> **Note:** This topic assumes a basic understanding of Linux.

You can use the `convertDatabaseMode.php` script to enable write-ahead logging (WAL) journaling mode for Tenable Security Center databases. Enabling WAL may resolve issues with excessive database locks. If your Tenable Security Center does not experience database locking issues, Tenable recommends leaving your Tenable Security Center databases in the default DELETE journaling mode.

For more information, see Tenable Security Center Database Journaling Modes.

Before you begin:

- Confirm your Tenable Security Center installation meets the requirements to enable WAL. For more information, see WAL Requirements.

- Write-ahead logging mode typically uses more disk space than DELETE mode. Consider your disk space availability before enabling write-ahead logging. Tenable recommends the same amount of disk space that is occupied by the database.

- Perform a backup of Tenable Security Center, as described in [Perform a Backup](#).

To enable WAL:

1. Log in to Tenable Security Center via the command line interface (CLI).

2. Stop Tenable Security Center, as described in [Start, Stop, or Restart Tenable Security Center](#).

3. In the CLI in Tenable Security Center, run the following command to start the `converDatabaseMode.php` script:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/convertDatabaseMode.php -m WAL
   ```

   The script runs.

4. If the script detects any running `tns` user processes, repeat the following steps for each `tns` user process detected:

   a. Follow the prompts in the error output to halt the `tns` user process.

   Example error output:

   ```
   Error! The Tenable Security Center process with PID '10135' is still running
   and needs to be halted before this script can be executed successfully.
      Command: /opt/sc/support/bin/php -f /opt/sc/daemons/Jobd.php
   Bailing with 146.
   ```

   b. Run the following command to restart the `converDatabaseMode.php` script:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/convertDatabaseMode.php -m WAL
   ```

   The script restarts.

   Tenable Security Center converts supported databases to WAL journaling mode. For more information, see [Databases Affected](#).

5. Start Tenable Security Center, as described in [Start, Stop, or Restart Tenable Security Center](#).

What to do next:

- Perform regular backups of Tenable Security Center, as described in [Perform a Backup](#).

Disable Write-Ahead Logging

> **Required Tenable Security Center User Role:** Root user

> **Note:** This topic assumes a basic understanding of Linux.

If you experience issues with write-ahead logging (WAL), disable WAL by reverting your Tenable Security Center databases to DELETE journaling mode. For more information, see [Tenable Security Center Database Journaling Modes](#).

Before you begin:

- Perform a backup of Tenable Security Center, as described in [Perform a Backup](#).

To disable WAL:

1. Log in to Tenable Security Center via the command line interface (CLI).

2. Stop Tenable Security Center, as described in [Start, Stop, or Restart Tenable Security Center](#).

3. In the CLI in Tenable Security Center, run the following command to start the `converDatabaseMode.php` script:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/convertDatabaseMode.php -m DELETE
   ```

   The script runs.

4. If the script detects any running `tns` user processes, repeat the following steps for each `tns` user process detected:

   a. Follow the prompts in the error output to halt the `tns` user process.

   Example error output:

```
Error! The Tenable Security Center process with PID '10135' is still running
and needs to be halted before this script can be executed successfully.
   Command: /opt/sc/support/bin/php -f /opt/sc/daemons/Jobd.php
Bailing with 146.
```

b. Run the following command to restart the `converDatabaseMode.php` script:

```
/opt/sc/support/bin/php /opt/sc/src/tools/convertDatabaseMode.php -m DELETE
```

The script restarts.

Tenable Security Center converts supported databases to DELETE journaling mode. For more information, see [Databases Affected](#).

5. Start Tenable Security Center, as described in [Start, Stop, or Restart Tenable Security Center](#).

What to do next:

- Perform regular backups of Tenable Security Center, as described in [Perform a Backup](#).

License Requirements

This topic breaks down the licensing process for Tenable Security Center as a standalone product. It also explains how assets are counted, lists add-on components you can purchase, and describes what happens during license overages or expiration.

Tenable Security Center Versions

Tenable Security Center has two versions:

- **Tenable Security Center** — Includes Tenable Network Monitor in discovery mode and unlimited Tenable Nessus scanners.

- **Tenable Security Center+** — Includes all of the above plus Tenable Network Monitor with vulnerability detection and metrics such as [Asset Exposure Score (AES)](#) and [Asset Criticality Rating (ACR)](#).

Tenable Security Center Director is available for both versions. Tenable Security Center Director is an add-on with which you can manage multiple Tenable Security Center instances from one location. For more information, see the [Tenable Security Center Director User Guide](#).

Note: You cannot upgrade a Tenable Security Center license to a Tenable Security Center Director license or downgrade a Tenable Tenable Security Center Director license to a Tenable Security Center license.

Licensing Tenable Security Center

To use any version of Tenable Security Center, you purchase licenses based on your organizational needs and environmental details. Tenable Security Center assigns those licenses to your *assets*, which are assessed hosts from Tenable Cloud Security or imported from other Tenable products.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

Note: Tenable offers simplified pricing to managed security service providers (MSSPs). To learn more, contact your Tenable representative.

How Assets are Counted

Tenable Security Center licenses are valid for specific hosts and a maximum number of active assets identified by IP address or UUID. Assets count towards your license depending on how Tenable Security Center discovers them. In general, assets do not count unless they have been assessed for vulnerabilities.

For example, if you purchase a 500 asset license, you can perform host discovery on your network, but you cannot assess more than 500 assets. For more information about discovery and assessment scanning, see Scanning Overview in the *Tenable Security Center User Guide*.

The following table explains when assets count towards your license.

Counted Towards Your License	Not Counted Towards Your License
- Assets from active scans. - Assets from Log Correlation Engine instances. - Assets from Tenable Network Monitor instances not in discovery mode.	- Assets present only from imports to offline or remote repositories. - Assets present only from Tenable Network Monitor instances in discovery mode.

Counted Towards Your License	Not Counted Towards Your License
- UUIDs from OT Security instances. - Assets in offline or remote repositories that you downloaded using the same Tenable Security Center instance or license. **Note**: In agent or IPv4 repositories, each single IP address or UUID counts once toward your license, even if it was scanned via multiple methods or stored in multiple repositories. In universal repositories, each asset with a UUID is counted toward your license. For example, if an asset in an IPv4 repository does not have a UUID, and the same asset is stored in a universal repository with a UUID, the asset is counted twice. **Note**: If you use an alternative port scanner, Tenable Security Center counts the detected IP addresses against your license.	- Assets in offline or remote repositories that you downloaded using the same Tenable Security Center instance with a different license. - Assets in offline or remote repositories that you downloaded using a different Tenable Security Center instance and license. - In the latest versions of Tenable Security Center and Tenable Security Center Director, the following excluded plugins: **Tenable Nessus** — 10180, 10287, 10335, 11219, 11933, 11936, 12053, 14272, 14274, 19506, 22964, 33812, 33813, 34220, 34277, 45590, 54615, 87413, 112154, 161455, 179042, 209654, and 204872. **Tenable Network Monitor** — 0, 12, 18, 19, 20, 113, and 132. **Tenable Log Correlation Engine** — 800000 through 800099.

Note: In the context of this table, assets are differentiated by the type of repository the data is stored in. For example:

- in IPv4 and IPv6 repositories, *assets* are *IP addresses*.
- in agent repositories, *assets* are *agents*.

Counted Towards Your License	Not Counted Towards Your License

> - in universal repositories, *assets* are *hosts*.
>
> For more information, see [Asset Tracking in Tenable Security Center](#).

Tenable Security Center Components

You can customize Tenable Security Center for your use case by adding components. Some components are add-ons that you purchase.

Version	Included with Purchase	Add-on Component
Tenable Security Center	- One console (or more with additional IP addresses). - Tenable Network Monitor in discovery mode. - Tenable Nessus scanners. - Vulnerability Probability Rating (VPR). - (Subscription-only) The same number of on-premises Tenable Agents as your licensed assets, provided on request.	- Cloud Tenable Agents. - Tenable Network Monitors in high-performance mode. - (Subscription-only) Additional consoles. - (Subscription-only) Security Center Lab License. - (Subscription-only) Tenable Lumin connector. > **Note:** The standalone Tenable Lumin SKU's will reach End of Sale (EOS) on March 31, 2025. Customers currently using Tenable Lumin and Tenable Lumin Connector will be upgraded to the Tenable One Platform for both new and renewal purchases. Contact your CSM if you want to migrate before this date to take advantage of all Tenable One capabilities. For more information, see the [Tenable Lumin End of Sale Bulletin](#). - Tenable Web App Scanning, to scan web applications with a Tenable Nessus scanner in

Tenable Security Center. Scan up to your number of licensed fully qualified domain names (FQDNs). For more information, see [Web App Scans](#) in the *Tenable Security Center User Guide*.

> **Note**: If you already have a Tenable Security Center license and you upgrade to Tenable Security Center version 6.2.x or later, there are two ways to enable web application scans. Either update your Tenable Web App Scanning plugins manually in Tenable Security Center or wait for the nightly plugin update to run.

- (Subscription-only) Tenable Security Center Director.

- (Perpetual-only) On-Premises Tenable Agents, which Perpetual customers must purchase separately.

- Tenable Attack Surface Management.

- Tenable Lumin, if you want to view your data in Tenable Vulnerability Management.

> **Tip:** Synchronized assets that count toward your Tenable Security Center license also count toward your Tenable Vulnerability Management license.

- Vulnerability Intelligence.

- Log Correlation Engine.

> **Note:** Tenable no longer supports Log Correlation Engine and will deprecate it at the end of 2024.

Tenable Security Center+	- One console (or more with additional IP addresses). - Tenable Network Monitor in discovery mode. - Tenable Network Monitors with vulnerability detection. - Tenable Nessus scanners. - Asset Exposure Score (AES). - Asset Criticality Rating (ACR). - Vulnerability Priority Rating (VPR). (Subscription-only) The same number of on-premises Tenable Agents as your licensed assets, provided on request.	- Cloud Tenable Agents. - Tenable Network Monitors in high-performance mode. (Subscription-only) Additional consoles. (Subscription-only) Security Center Lab License. (Subscription-only) Tenable Lumin connector. **Note:** The standalone Tenable Lumin SKU's will reach End of Sale (EOS) on March 31, 2025. Customers currently using Tenable Lumin and Tenable Lumin Connector will be upgraded to the Tenable One Platform for both new and renewal purchases. Contact your CSM if you want to migrate before this date to take advantage of all Tenable One capabilities. For more information, see the Tenable Lumin End of Sale Bulletin. - Tenable Web App Scanning, to scan web applications with a Tenable Nessus scanner in Tenable Security Center. Scan up to your number of licensed fully qualified domain names (FQDNs). For more information, see Web App Scans in the *Tenable Security Center User Guide*. **Note**: If you already have a Tenable Security Center license and you upgrade to Tenable Security Center version 6.2.x or later, there are two ways to enable web application scans. Either update your Tenable Web App Scanning plugins manually in Tenable Security Center or wait for the nightly plugin update to run.

		• (Subscription-only) Tenable Security Center Director.
		• (Perpetual-only) On-Premises Tenable Agents, which Perpetual customers must purchase separately.
		• Tenable Attack Surface Management.
		• Tenable Lumin, if you want to view your data in Tenable Vulnerability Management.
		Tip: Synchronized assets that count toward your Tenable Security Center license also count toward your Tenable Vulnerability Management license.
		• Vulnerability Intelligence.
		• Log Correlation Engine.
		Note: Tenable no longer supports Log Correlation Engine and will deprecate it at the end of 2024.

Reclaiming Licenses

Tenable Security Center's license count updates when you delete a repository, run a license report, or upload a new license. If you set assets to age out, they are removed during nightly cleanup. If you configure your scan settings to remove unresponsive hosts, they are removed at scan import.

For more information, see License Count in the *Tenable Security Center Best Practices Guide*.

Exceeding the License Limit

As you approach or exceed your license limit, a warning appears in the Tenable Security Center interface. If you exceed your limit, Tenable disables your access to Tenable Security Center. To monitor your license limit, use the **Licensing Status** widget, as described in Overview Dashboard. To upgrade your license, contact your Tenable representative.

Expired Licenses

The Tenable Security Center licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, your Tenable products and components are affected as follows:

- **Tenable Security Center Console (Perpetual license)** — The software remains fully functional. All user data is accessible.

- **Tenable Security Center Console (Subscription license)** — To access the console, you must enter a new license key. Once you enter a new license key, normal operation resumes.

- **Tenable Nessus (Perpetual license)** — When your maintenance period expires, plugin updates are no longer available. After 90 days, Tenable Nessus stops working and you cannot perform new scans. Because Tenable Security Center stops receiving feeds, the Tenable Nessus scanners managed by Tenable Security Center no longer receive updates and also stop working.

- **Tenable Network Monitor (Perpetual license)** — After 30 days with no updates, new data is no longer processed.

- **Tenable Log Correlation Engine** — On the day of license expiration, new logs are no longer processed.

Working with License Keys

The following sections explain how to work with Tenable license keys and link to additional details.

Get a Tenable Security Center License Key

To get a Tenable Security Center license key, enter the hostname of the installation machine in a form on the Tenable Community site, as described in the Tenable Community Guide. You can also email the key to licenses@tenable.com. In both cases, you receive a Tenable Security Center license key to use when activating your products.

> **Tip**: To obtain the hostname of the installation machine, in a system shell prompt, type hostname.

You can also use the install UUID in place of the hostname. The install UUID appears on the license activation page of the initial setup wizard, and is also available on disk in the install log and in the `install-uuid.txt` file.

Add or Update a Tenable Security Center License Key

In most cases, adding a license key to Tenable Security Center or its attached products requires the Tenable Security Center console to contact a product registration server. The server connection is encrypted, as described in Encryption Strength.

Tip: To learn which Tenable sites to allow through your firewall, see the Tenable Knowledge Base.

Note: For instructions to use in offline or air-gapped environments, see Offline Plugin and Feed Updates for Tenable Security Center.

See the following topics for instructions to upload a new license key or update an existing one:

- Quick Setup — Upload a new Tenable Security Center license and add activation codes for any attached products.

- Apply a New License — Upload a new license for attached Tenable products only.

- Update an Existing License — Update an existing Tenable Security Center license or existing attached Tenable product licenses.

Apply a New License

Required Tenable Security Center User Role: Administrator

To apply a license for an additional Tenable product, add the license activation code. To update a license for an existing Tenable product, see Update an Existing License.

For general information about licensing, see License Requirements. For information about adding a license during quick setup, see Quick Setup.

To download Tenable Security Center, see the Tenable Security Center downloads page.

To apply a new Tenable Nessus, Tenable Network Monitor, or Log Correlation Engine license:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **License** tile.

   The **License Configuration** page appears.

4. Click the product box for the license you want to apply.

5. In the box, type the activation code for the product.

6. Click **Register**.

   Tenable Security Center updates the page to reflect the activation code status:

   - Valid Code: A green box with a check mark.

   - Invalid Code: A red box with an X.

   If the code is valid, Tenable Security Center initiates a plugin download.

Update an Existing License

Required Tenable Security Center User Role: Administrator

Tip: Tenable rebranded Tenable Security Center Continuous View as Tenable Security Center+.

If you need to replace your Tenable Security Center or Tenable Security Center+ license or the license activation code for your Tenable Nessus, Tenable Network Monitor, or Tenable Log Correlation Engine license, update the license.

To apply a new license for another Tenable product for the first time, see Apply a New License.

You can update your Tenable Security Center license in an externally connected or air-gapped environment. Tenable Security Center requires an internet connection to validate product licenses for Tenable Nessus, Tenable Network Monitor, or Log Correlation Engine.

For instructions on how to install a Tenable Security Center patch, see Install a Tenable Security Center Patch.

To download Tenable Security Center, see the Tenable Security Center Downloads page.

For general information about licensing, see [License Requirements](#).

To update a license:

1. Log in to Tenable Security Center via the user interface.

2. Click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **License** tile.

   The **License Configuration** page appears.

4. To replace your Tenable Security Center license, in the **Tenable Security Center License** section:

   a. Click **Update License**.

   b. Click **Choose File** and browse to the license file you want to upload.

      Tenable Security Center applies the new license.

5. To replace an activation code for an integrated product license, in the **Activation Codes** section:

   a. Click the green check mark.

   b. Click **Reset Activation Code**.

   c. In the box, paste your product license activation code.

   d. Click **Register**.

      Tenable Security Center communicates with the Tenable product registration server to validate your license activation code.

      If the code is valid, Tenable Security Center applies the new license and initiates a plugin download.

Port Requirements

Tenable Security Center port requirements include Tenable Security Center-specific and application-specific requirements.

- [Tenable Security Center](#)

- [Tenable Nessus Scanner](#)

- [Tenable Agent](#)

- [Tenable Network Monitor](#)

- [Tenable Log Correlation Engine](#)

Tenable Security Center

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

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 22	Performing remote repository synchronization with another Tenable Security Center.
TCP 443	Accessing the Tenable Security Center interface.
	Communicating with Tenable Security Center Director instances.
	Communicating with OT Security instances.
	Performing the initial key push for remote repository synchronization with another Tenable Security Center.
	Interacting with the API.
TCP 8837	Communicating with Sensor Proxy.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 22	Communicating with Log Correlation Engine for event query.
TCP 25	Sending SMTP email notifications.
TCP 443	Communicating with Tenable Lumin for synchronization. Communicating with the `plugins.nessus.org` server for plugin updates.
TCP 1243	Communicating with Tenable Log Correlation Engine.
TCP 8834	Communicating with Tenable Nessus.
TCP 8835	Communicating with Tenable Network Monitor.
TCP 8837	Communicating with Apache.
UDP 53	Performing DNS resolution.

Tenable Nessus Scanner

Your Tenable Nessus instances require access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 8834	Accessing the Tenable Nessus interface. Communicating with Tenable Security Center. Interacting with the API.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 25	Sending SMTP email notifications.

Port	Traffic
TCP 443	Communicating with Tenable Vulnerability Management (sensor.cloud.tenable.com or sensor.cloud.tenablecloud.cn). Communicating with the `plugins.nessus.org` server for plugin updates.
UDP 53	Performing DNS resolution.

Tenable Agent

Your Tenable Agents require access to specific ports for outbound traffic.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 443	Communicating with Tenable Vulnerability Management.
TCP 8834	Communicating with Tenable Nessus Manager. **Note:** The default Tenable Nessus Manager port is TCP 8834. However, this port is configurable and may be different for your organization.
UDP 53	External DNS support for the host that Tenable Agent is installed on. Several plugins use DNS resolution in their operation.

Note: Operating system installation commands, such as `dnf install`, may require other connections besides Tenable Vulnerability Management or Tenable Nessus Manager. Consult your operating system administrator for more information.

Tenable Network Monitor

Your Tenable Network Monitor instances require access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
TCP 8835	Accessing the Tenable Network Monitor interface. Communicating with Tenable Security Center.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
TCP 443	Communicating with Tenable Vulnerability Management (sensor.cloud.tenable.com or sensor.cloud.tenablecloud.cn). Communicating with the `plugins.nessus.org` server for plugin updates.
TCP 601	Communications for reliable TCP syslog forwarding.
UDP 53	Performing DNS resolution.
UDP 514	Communications for UDP syslog forwarding.

Tenable Log Correlation Engine

Your Log Correlation Engine and Log Correlation Engine client instances require access to specific ports for inbound and outbound traffic.

Inbound Traffic

You must allow inbound traffic to the following ports.

Port	Traffic
Log Correlation Engine	
TCP 22	Communicating with Tenable Security Center for Log Correlation Engine event query.
TCP 601	Communications for reliable TCP syslog forwarding.
TCP 1243	Communicating with Tenable Security Center for Log Correlation Engine event vulnerability import.

Port	Traffic
TCP 8836	Accessing the Log Correlation Engine interface.
TCP 31300	Communicating with Log Correlation Engine clients.
UDP 162	Communicating with SNMP server for receiving SNMP traps.
UDP 514	Communications for UDP syslog forwarding.
Log Correlation Engine Client	
TCP 1468	Communications between network devices and the Tenable Network Monitor.
TCP 9800	Communications between Splunk and the Log Correlation Engine Splunk Client.
TCP 18185	Communications between Check Point firewalls and the Log Correlation Engine OPSEC Client.
UDP 514	Communications between network devices and the Tenable Network Monitor.
UDP 2055	Communications between routers and the Tenable NetFlow Monitor.

Outbound Traffic

You must allow outbound traffic to the following ports.

Port	Traffic
Log Correlation Engine	
TCP 25	Sending SMTP email notifications.
TCP 443	Communicating with Tenable Vulnerability Management (sensor.cloud.tenable.com or sensor.cloud.tenablecloud.cn). Communicating with the `plugins.nessus.org` server for plugin updates.
TCP 601	Communications for reliable TCP syslog forwarding.
UDP 53	Performing DNS resolution.
UDP 514	Communications for UDP syslog forwarding.

Port	Traffic
Log Correlation Engine Client	
TCP 135	Communicating with the targets of the Log Correlation Engine WMI Monitor Client.
TCP 443	Communicating with the web host of the Log Correlation Engine Web Query Client.
TCP 445	Communicating with the targets of the Log Correlation Engine WMI Monitor Client.
TCP 31300	Communicating with Log Correlation Engine.

Browser Requirements

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

> **Note**: Tenable Security Center does not officially support any browser extensions. If you encounter issues related to browser extensions, please report them to the relevant browser extension developer for further assistance.

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

- Microsoft Internet Explorer 11 or later

  > **Tip:** Tenable Security Center versions 5.22 and later do not support Internet Explorer.

Tenable Integrated Product Compatibility

The versions of Tenable products tested with Tenable Security Center 6.6.x are available in the release notes. For more information, see the [Tenable Security Center Release Notes](#) for your version.

Large Enterprise Deployments

You may have a number of unique technical and business requirements to consider when planning a large enterprise deployment of Tenable Security Center. If your organization scans 100,000 or more IP addresses, consider the information in the [Tenable Security Center Large Enterprise Deployment Guide](#) when planning, configuring, and operationalizing your Tenable Security Center deployment.

Installation and Upgrade

To perform a fresh installation of Tenable Security Center, see [Before You Install](#) and [Install Tenable Security Center](#).

To perform an upgrade of Tenable Security Center, see [Before You Upgrade](#) and [Upgrade Tenable Security Center](#).

To uninstall Tenable Security Center, see [Uninstall Tenable Security Center](#).

Before You Install

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

For more information, see [License Requirements](#).

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 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 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. For more information, see the knowledge base article.

Connect a PostgreSQL server

You must configure an external PostgreSQL database if your Tenable Security Center installation meets any of the following criteria:

- Your Tenable Security Center instance has over 100,000 assets.

- Your Tenable Security Center instance is a non-rpm installation.

Before you install or upgrade Tenable Security Center, you must configure some environment variables to connect the PostgreSQL server. For more information, see Connect an External PostgreSQL Server.

Connect an External PostgreSQL Server

You must configure an external PostgreSQL database if your Tenable Security Center installation meets any of the following criteria:

- Your Tenable Security Center instance has over 100,000 assets.

- Your Tenable Security Center instance is a non-rpm installation.

> **Note:** Tenable Security Center does not support multiple Tenable Security Center instances using the same database name in the same PostgreSQL server. The database name should be unique in the PostgreSQL instance.

> **Note:** The minimum required PostgreSQL version is 13.x.

For information about how to configure a PostgreSQL server, see the PostgreSQL documentation.

For sizing recommendations, see the Hardware Requirements and Cloud Requirements.

To connect your Tenable Security Center instance to your PostgreSQL server:

1. Before you install or upgrade Tenable Security Center, populate the following environment variables:

   > **Note:** You must set the environment variables with a `root` or `tns` user account.

   - `SC_PG_HOST` (required)– The IP address or hostname of the external PostgreSQL server.

   - `SC_PG_USER` (required) – The PostgreSQL username. The user must have CREATEDB and read/write permissions.

   - `SC_PG_PORT` – The port number. The default port is **5432**.

   - `SC_PG_PASSWORD` – The password for the PostgreSQL user. If you do not provide a password, Tenable Security Center will assume an empty password for the external PostgreSQL user.

   - `SC_PG_DATABASE` – The database name for the Tenable Security Center data. The default database name is **SecurityCenter**.

   - `SC_PG_CA_PATH` – The absolute path to the cert file. When you specify the location of the root certificate, Tenable Security Center verifies the root certificate used by

PostgreSQL.

- **SC_PG_REQUIRE_TLS** - Whether PostgreSQL will use SSL. Available options are *NULL*, *require*, and *prefer*. If this variable is not set, then the Tenable Security Center client ssl_ mode will be set to *prefer*.

After you install or upgrade to Tenable Security Center 6.5.0 or later, then Tenable Security Center will attempt to connect to the PostgreSQL instance using the values provided and create a database with the specified database name.

Install Tenable Security Center

Required Tenable Security Center User Role: Root user

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

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.

Note: If your Tenable Security Center will manage more than 10,000 active IPs, you must update the Apache configuration file after you install and before you use Tenable Security Center.

Note: You must connect an external PostgreSQL database if your Tenable Security Center installation meets any of the following criteria:

- Your Tenable Security Center instance has over 100,000 assets.
- Your Tenable Security Center instance is a non-rpm installation.

For information about new features, resolved issues, third-party product updates, and supported upgrade paths, see the release notes for Tenable Security Center 6.6.x.

Before you begin:

- Complete system prerequisites, as described 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.

- Confirm the integrity of the installation RPM file by comparing the download checksum with the checksum on the Tenable Security Center downloads page, as described in the knowledge base article.

- If your organization requires 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. Run one of the following commands to install the RPM:

```
# yum install SecurityCenter-x.x.x-el6.x86_64.rpm
```

- or -

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

Output similar to the following is generated:

```
# dnf install SecurityCenter-6.x.x-es6.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. For more information, see Start, Stop, or Restart Tenable Security Center.

What to do next:

- If you are scanning more than 10,000 hosts, update the Apache configuration file before using Tenable Security Center.

Quick Setup

The Tenable Security Center Quick Setup Guide walks through the following configurations:

- License

- Tenable Nessus Scanner

- Tenable Network Monitor

- Log Correlation Engine

- Repository

- Organization

- LDAP

- User

- Additional Settings

After configuring, Review and confirm.

License

> **Note:** These settings are not available in Tenable Enclave Security.

Upload your Tenable Security Center license and apply additional product licenses.

Tenable Security Center License

1. Click **Choose File** to upload the Tenable Security Center license file you received from Tenable.

   The file should follow the format:

   `<CompanyName>_SC<IP Count>-<#>-<#>.key`

2. Click **Activate**.

   The page confirms successful upload and activation of a valid license.

Activation Codes

Consider adding additional license activation codes:

- Tenable Security Center license activation code — required before adding any Tenable Nessus scanners. The Tenable Security Center license activation code allows Tenable Security Center to download plugins and update Tenable Nessus scanner plugins.

  In the **Tenable Nessus** section, type the Tenable Security Center activation code and click **Register**.

- Tenable Network Monitor license activation code — required before using and managing attached Tenable Network Monitor scanners.

  In the **Tenable Network Monitor** section, type the Tenable Network Monitor activation code and click **Register**.

- Log Correlation Engine Activation Code — required before downloading Log Correlation Engine Event vulnerability plugins to Tenable Security Center. The Log Correlation Engine Activation Code allows Tenable Security Center to download event plugins, but it does not manage plugin updates for Log Correlation Engine servers.

  In the **Log Correlation Engine** section, type the Tenable Log Correlation Engine activation code and click **Register**.

Click **Next** to continue.

A plus (+) sign indicates that no license is applied for the product. A box with an X indicates an invalid activation code. Click on the plus (+) or X to add or reset a license activation code.

A box with a checkmark indicates a valid license is applied and that Tenable Security Center initiated a plugin download in the background.

The download may take several minutes and must complete before initiating any Tenable Nessus scans. After the download completes, the **Last Updated** date and time update on the Plugins page.

Tenable Nessus Scanner

Configure your first Tenable Nessus scanner. For information about the options you can configure, see Tenable Nessus Scanners. There are some limitations on the scanner options you can configure during Quick Start:

- **Agent Capable**: If you use a Tenable Vulnerability Management or Tenable Nessus Manager scanner for Tenable Agent scan imports, do not configure that scanner during the Quick Start.

- **Zones**: If you want to grant scan zones access to this scanner, you must configure the **Zones** option after the Quick Start.

Tenable Network Monitor

> **Note:** These settings are not available in Tenable Enclave Security.

If you added an Tenable Network Monitor license activation code, you can configure your first Tenable Network Monitor scanner. For information about the options you can configure, see Tenable Network Monitor Instances. There are some limitations on the scanner options you can configure during Quick Start:

- **Repositories**: If you want to select repositories to store the scanner's data, you must configure the **Repositories** option after the Quick Start.

Log Correlation Engine

> **Note:** Tenable Enclave Security does not support Tenable Log Correlation Engine.

If you added an Log Correlation Engine Activation Code, you can configure your first Tenable Log Correlation Engine scanner. For information about the options you can configure, see Tenable Log Correlation Engines. There are some limitations on the scanner options you can configure during Quick Start:

- **Organizations**: If you want to select organizations that can access the scanner's data, you must configure the **Organizations** option after the Quick Start.

- **Repositories**: If you want to select repositories to store the scanner's data, you must configure the **Repositories** option after the Quick Start.

Repository

You can configure your first local IPv4 or IPv6 repository.

> **Caution:** When creating repositories, note that IPv4 and IPv6 addresses must be stored separately. Additional repositories may be created once the initial configuration is complete.

A repository is essentially a database of vulnerability data defined by one or more ranges of IP addresses. When the repository is created, a selection for IPv4 or IPv6 addresses must be made. Only IP addresses of the designated type may be imported to the designated repository. The organization created in steps that follow can take advantage of one or more repositories. During installation, a single local repository is created with the ability to modify its configuration and add others post-install.

> **Caution:** When creating Tenable Security Center repositories, Tenable Log Correlation Engine event source IP address ranges must be included along with the vulnerability IP address ranges or the event data is not accessible from the Tenable Security Center UI.

Local repositories are based on the IP addresses specified in the **IP Ranges** option on this page during the initial setup. *Remote* repositories use addressing information pulled over the network from a remote Tenable Security Center. Remote repositories are useful in multi-Tenable Security Center configurations where security installations are separate but reports are shared. *Offline* repositories also contain addressing information from another Tenable Security Center. However, the information is imported to the new installation via a configuration file and not via a direct network connection. For information about how this works in air-gapped environments, see Considerations for Air-Gapped Environments.

For information about the options you can configure, see [Local Repositories](#). There are some limitations on the repositories and repository options you can configure during Quick Start:

- You cannot configure a local mobile repository during Quick Start.

- You cannot configure a local agent repository during Quick Start.

- You cannot configure an external repository during Quick Start.

- **Organizations**: If you want to select organizations that can access the repository's data, you must configure the **Organizations** option after the Quick Start.

- **Log Correlation Engine Correlation**: If you want to select Log Correlation Engine servers where you want Tenable Security Center to retrieve data, you must configure the **Log Correlation Engine Correlation** option after the Quick Start.

Organization

> **Note:** These settings are not available in Tenable Enclave Security.

An organization is a set of distinct users and groups and the resources they have available to them. For information about the options you can configure, see [Organizations](#).

You can configure one organization during initial setup. If you want to use multiple organizations, you must configure other organizations after the Quick Start.

LDAP

> **Note:** These settings are not available in Tenable Enclave Security.

Configuring LDAP allows you to use external LDAP servers for the Tenable Security Center user account authentication or as LDAP query assets. Type all required LDAP server settings and click **Next**. Click **Skip** if you do not want to configure LDAP during initial configuration.

You can configure one LDAP server connection during initial setup. If you want to use multiple LDAP servers, or if you want to configure additional options, you must continue configuring LDAP after the Quick Start.

For information about the options you can configure, see [LDAP Authentication](#).

User

> **Note:** These settings are not available in Tenable Enclave Security.

You must create one administrator and one security manager during initial setup. For more information, see User Roles.

- Security manager — a user to manage the organization you just created. After you finish initial setup, the security manager can create other user accounts within the organization.

- Administrator — a user to manage Tenable Security Center. After you finish initial setup, the administrator can create other organizations and user accounts.

If you already configured an LDAP server, you have the option to create an LDAP user account. For more information about user account options, see User Accounts.

After creating the security manager user and setting the administrator password, click **Next** to finish initial setup. The **Admin Dashboard** page appears, where you can review login configuration data.

Additional Settings

The **Enable Usage Statistics** option specifies whether Tenable collects anonymous telemetry data about your Tenable Security Center deployment.

When enabled, Tenable collects usage statistics that cannot be attributed to a specific user or customer. Tenable does not collect personal data or personally identifying information (PII).

Usage statistics include, but are not limited to, data about your visited pages, your used reports and dashboards, your Tenable Security Center license, and your configured features. Tenable uses the data to improve your user experience in future Tenable Security Center releases. You can disable this option at any time to stop sharing usage statistics with Tenable.

For more information about enabling or disabling this option after initial setup, see Configuration Settings.

Review

The review page displays your currently selected configurations. If you want to make further changes, click the links in the left navigation bar.

When you are finished, click **Confirm**.

Install a Tenable Security Center Patch

> **Required Tenable Security Center User Role:** Root user

> **Note:** This topic assumes a basic understanding of Linux.

For information about new patches, see the [release notes](#) for Tenable Security Center.

Some patches are available through the Tenable Security Center feed. For more information, see [Configuration Settings](#).

To apply a Tenable Security Center patch manually:

1. Download the patch TGZ file from the [Tenable downloads](#) page. If necessary, depending on the operating system of the host, move the upgrade TGZ file onto the host.

2. Confirm the integrity of the patch TGZ file by comparing the download checksum with the checksum on the [Tenable downloads](#) page.

3. If your organization requires 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](#).

4. Access the command line as a user with root-level permissions.

5. Run the following command to untar the patch file, where [*patch file name*] is the name of the TGZ patch file you downloaded:

   `tar zxf [patch file name]`

6. Run the following command to change the directory to the extracted directory, where [*directory*] is the extracted directory:

   `cd [directory]`

7. Run the following command to begin the installation:

   `sh ./install.sh`

   The installation begins and Tenable Security Center stops. After the installation finishes, Tenable Security Center automatically restarts.

8. (Optional) Confirm the patch successfully applied to Tenable Security Center, as described in the [knowledge base](#) article.

To apply a patch through the Tenable Security Center feed:

1. Log in to Tenable Security Center as an Administrator.

2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **Plugins/Feed** tile.

   The **Plugins/Feed Configuration** page appears.

4. On the **Plugins/Feed Configuration** page, in the **Tenable Security Center Software Updates** section, enable the **Enable Updates Through the Tenable Security Center Feed** option.

   During the next scheduled feed update, Tenable Security Center applies the patch. In the **Tenable Security Center Software Updates** table, a timestamp appears in the row for the patch in the **Last Updated** column.

Before You Upgrade

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

- [Tenable Security Center Upgrade Path](#)
- [Java Version Requirements](#)
- [Halt or Complete Running Jobs](#)
- [Perform a Tenable Security Center Backup](#)
- [Rename Your Mount Point](#)

Tenable Security Center Upgrade Path

For more information about the upgrade paths to Tenable Security Center version 6.6.x, see the [Tenable Security Center Release Notes](#).

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. For more information, see Backup and Restore.

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 Tenable Security Center User Role: Root user

Note: This topic assumes a basic understanding of Linux.

Caution: During the upgrade 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 upgrade.

Caution: If your plugin set is more than 30 days old, the upgrade will fail. Ensure you have updated your plugin set within the last 30 days before you upgrade Tenable Security Center.

For information about new features, resolved issues, third-party product updates, and supported upgrade paths, see the release notes for Tenable Security Center 6.6.x.

These steps describe how to upgrade to the latest version of Tenable Security Center from a previous version. You can also use these steps to upgrade from an early access version of Tenable Security Center.

Note: If you are upgrading from Tenable Security Center version 6.2.1 or earlier to version 6.3.x or later, you must update the Apache configuration file after you upgrade and before you use Tenable Security Center.

Before you begin:

1. Complete system prerequisites, as described in Before You Upgrade.

   Note: Tenable recommends creating a backup of your Tenable Security Center data before upgrading, as described in Perform a Backup.

2. Download the upgrade RPM file from the Tenable downloads page. If necessary, depending on the operating system of the host, move the upgrade RPM file onto the host.

3. Confirm the integrity of the upgrade RPM file by comparing the download checksum with the checksum on the Tenable downloads page.

4. If your organization requires 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 to Tenable Security Center 6.6.x:

1. Log in to Tenable Security Center via the user interface.

2. Pause all running scans, as described in [Start or Pause a Scan](#).

3. 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-el6.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-el6.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  ]
   ~]#
   ```

What to do next:

- If you are upgrading from Tenable Security Center version 6.2.1 or earlier to Tenable Security Center version 6.3.x or later, update the Apache configuration file before using Tenable Security Center.

- (Optional) If you used custom Apache SSL certificates before upgrading Tenable Security Center, restore the custom SSL certificates, as described in Restore Custom SSL Certificates.

Restore Custom SSL Certificates

> **Required Tenable Security Center User Role:** Root user

If you used custom Apache SSL certificates before upgrading Tenable Security Center, you must restore the custom Apache SSL certificates after you upgrade Tenable Security Center.

Tenable Security Center creates a backup of the certificates during the upgrade process. Tenable Security Center copies the existing custom SSL certificates to the Apache configuration backup directory that the upgrade process creates in the `/tmp/[version].apache.conf-########` directory. The exact name of the directory varies, but the system displays the name during the upgrade process and reports it in the `/opt/sc/admin/log/install.log` file.

Before you begin:

- Upgrade to a new version of Tenable Security Center, as described in Upgrade Tenable Security Center.

To restore custom SSL certificates after upgrading 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:

   ```
   # cp /tmp/[version].apache.conf-########/SecurityCenter.cert
   /opt/sc/support/conf/SecurityCenter.crt
   ```

3. Select `yes` to overwrite the existing file.

4. In the CLI in Tenable Security Center, run the following command:

```
# cp /tmp/[version].apache.conf-########/SecurityCenter.pem
/opt/sc/support/conf/SecurityCenter.key
```

5. Select **yes** to overwrite the existing file.

> **Caution:** Ensure that the newly copied files have permissions of 0640 and ownership of tns:tns.

6. Modify the **servername** parameter in **/opt/sc/support/conf/servername** to match the Common Name (CN) of the SSL certificate.

> **Tip:** To obtain the CN, run the following command and note the **CN=** portion of the result.

```
# /opt/sc/support/bin/openssl verify /opt/sc/support/conf/SecurityCenter.crt
```

7. In the CLI in Tenable Security Center, run one of the following commands to restart the Apache server:

```
# /opt/sc/support/bin/apachectl restart
```

-or-

```
# service SecurityCenter restart
```

The Apache server restarts.

Update the Apache Configuration File

> **Required Tenable Security Center User Role:** Root user

Tenable Security Center 6.3.x updated the Apache web server configuration to resolve a memory leak issue. When your Tenable Security Center instance meets the following criteria, you must update some values in the Apache configuration file located at **/opt/sc/support/conf/mpm.conf**:

- You are upgrading to Tenable Security Center version 6.6.x from version 6.2.1 or earlier.

  -or-

- Your Tenable Security Center instance manages more than 10,000 active IPs.

The default settings in the Apache configuration file are sufficient if you are upgrading from Tenable Security Center version 6.3.x or later, and your instance manages fewer than 10,000 active IPs.

Before you begin:

- Stop Tenable Security Center, as described in [Start, Stop, or Restart Tenable Security Center](#).

- [Install Tenable Security Center](#) or [Upgrade Tenable Security Center](#)

To update the Apache configuration file:

1. Navigate to the Apache configuration file, located at `/opt/sc/support/conf/mpm.conf`

2. Update the values in the configuration file. Tenable recommends the following settings based on the size of your deployment:

# Hosts Managed by Tenable Security Center	Recommended Settings

Fewer than 10,000 active IPs	`StartServers 5`
	`MinSpareServers 5`
	`MaxSpareServers 10`
	`MaxRequestWorkers 32`

10,000 to 25,000 active IPs	`StartServers 10`
	`MinSpareServers 10`
	`MaxSpareServers 20`
	`MaxRequestWorkers 64`

25,001 to 100,000 active IPs	`StartServers 20` `MinSpareServers 20`

# Hosts Managed by Tenable Security Center	Recommended Settings
	MaxSpareServers 40
	MaxRequestWorkers 128
100,001 or more active IPs	StartServers 40
	MinSpareServers 40
	MaxSpareServers 80
	MaxRequestWorkers 256

3. Restart Tenable Security Center, as described in Start, Stop, or Restart Tenable Security Center.

What to do next:

- After the Tenable Security Center build has run for a period of time, check the log located at `/opt/sc/support/logs/error_log` for any errors related to the **MaxRequestWorkers** setting. For more information, see Generate a Diagnostics File.

Uninstall Tenable Security Center

Required Tenable Security Center User Role: Root user

To uninstall Tenable Security Center:

1. On the host where you want to uninstall Tenable Security Center, open the command line interface (CLI).

2. In the CLI, run the following command to stop Tenable Security Center:

```
service SecurityCenter stop
```

3. Run the following command to remove Tenable Security Center:

```
dnf remove SecurityCenter
```

4. Run the following command to remove user-created and user-modified files:

```
rm -rf /opt/sc
```

Tenable Security Center is removed.

User Access

The **Users** page provides the ability to add, edit, delete, or view the details of Tenable Security Center user accounts. When you view the **Users** page, you see a list of users and actions, limited by your account privileges. Your *user role*, *organization* membership, and/or *group* membership determine your account privileges. For more information, see [User Roles](#) and [Organizations and Groups](#).

There are two categories of user accounts:

- *Administrator* users have the system-provided administrator role and do not belong to organizations.

- *Organizational* users have the system-provided security manager, auditor, credential manager, executive, security analyst, security manager, or vulnerability analyst role, or a custom role, and belong to an organization.

Tenable Security Center supports three types of user account authentication: TNS, LDAP, and SAML. For more information, see [User Accounts](#).

To log in to the Tenable Security Center web interface with a user account, see [Log In to the Web Interface](#) or [Log in to the Web Interface via SSL Client Certificate](#).

Log In to the Web Interface

Required Tenable Security Center User Role: Any

To log in to the Tenable Security Center configuration interface:

1. Open a supported web browser on a system that has access to the system's network address space.

   Note: You must access the Tenable Security Center web interface using a secure web connection (HTTPS) with SSL/TLS 1.2 enabled. Tenable Security Center recommends

configuring the strongest encryption supported by your browser.

For more information, see [Encryption Strength](#).

2. Clear your web browser's cache.

3. Navigate to the URL for your Tenable Security Center: *https://<SERVER ADDRESS OR NAME>/*.

   Where *<SERVER ADDRESS OR NAME>* is the IPv4 or IPv6 address or hostname for your Tenable Security Center.

   The Tenable Security Center web interface appears.

4. Log in using the supported method for your account configuration.

   Note: If you are the first administrator user logging in to Tenable Security Center, see [Initial Login Considerations](#).

   - To log in via a username and password, type your Tenable Security Center credentials and click **Log In**.

   - To log in via SAML authentication, click **Sign In Using Identity Provider**. When presented with your identity provider login page, type your identity provider credentials.

     For more information about SAML authentication, see [Configure SAML Authentication Manually via the User Interface](#).

   - To log in via certificate, see [Log in to the Web Interface via SSL Client Certificate](#).

Tenable Security Center logs you in and displays the dashboard with different elements depending on your user role.

Initial Login Considerations

When you log in to Tenable Security Center for the first time, Tenable Security Center displays the Quick Setup Guide welcome page to begin a multi-step setup process for initial configuration. For more information about quick setup, see [Quick Setup](#).

If you prefer to configure the system manually, click **Exit Quick Setup Guide**. For more information about getting started with Tenable Security Center, see [Get Started With Tenable Security Center](#).

Log in to the Web Interface via SSL Client Certificate

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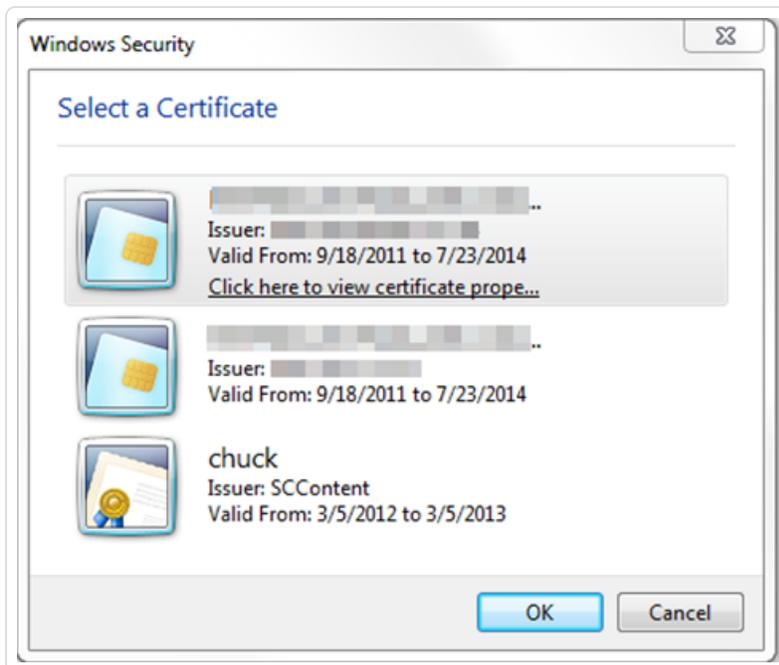
   For information about Tenable Security Center-browser communications encryption, see Encryption Strength.

2. Select a certificate.

3. Click **OK**.

   An authentication prompt appears (if required to access your certificate).
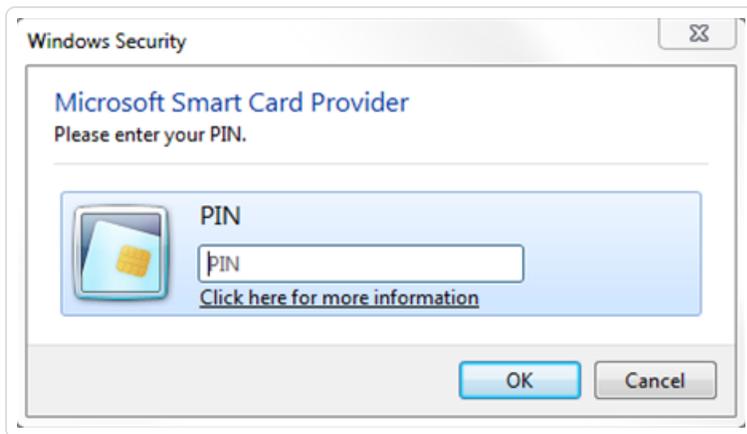
4. (Optional) If prompted, type a PIN or password.

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.

User Roles

Roles determine what a user can or cannot access from their account. Tenable Security Center comes with eight system-provided roles, but you can also create custom roles to satisfy complex security policy needs. You can customize the permissions on some, but not all, system-provided user roles.

You can create *linked user accounts* and *linked non-admin user accounts* to allow users to switch between accounts without logging out and logging back in to Tenable Security Center. For more information, see Linked User Accounts.

For more information about user roles in Tenable Security Center, see Create a User Role, Edit a User Role, View User Role Details, and Delete a User Role.

Roles

User Role	Customizable Permissions?	Description
Administrator	No	An account that manages Tenable Security Center as a whole. The primary task of the Administrator is to install and configure each organization. In addition, the Administrator adds components to Tenable Security Center such as Tenable Network Monitor, Tenable Log Correlation Engine, and Tenable Nessus to extend its capabilities. The Administrator is automatically assigned the "Manage Application" role. Because administrators do not belong to an organization, they do not have access to the data collected by Tenable Security Center.
Organizational User Roles		
Security Manager	No	An account that manages an individual organization. This is the role assigned to the initial user that is assigned when a new organization is created. They

| | | can launch scans, configure users (except for administrator user roles), vulnerability policies, and other objects belonging to their organization.

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 the user can launch scans, configure users (except for the Administrator user), vulnerability policies, and other objects that belong to their organization. This initial Security Manager account cannot be deleted without deleting the entire organization.

Security Managers have complete access to all data collected by their organization. |
|---|---|---|
| **SM-Linked** | No | A linked account that has the same abilities as a Security Manager, except an SM-Linked account cannot configure users. |
| **Auditor** | Yes | An account that can access summary information to perform third-party audits. An Auditor can view dashboards, reports, and logs, but cannot perform scans or create tickets. |
| **Credential Manager** | Yes | An account that can be used specifically for handling credentials. A Credential Manager can create and share credentials without revealing the contents of the credential. This can be used by someone outside the security team to keep scanning credentials up to date. |
| **Executive** | Yes | An account intended for users who are interested in a high-level overview of their security posture and risk profile. Executives would most likely browse |

		dashboards and review reports, but would not be concerned with monitoring running scans or managing users. Executives would also be able to assign tasks to other users using the ticketing interface.
Security Analyst	Yes	An account that has permissions to perform all actions at the Organizational level except managing groups and users. A Security Analyst is most likely an advanced user who can be trusted with some system-related tasks such as setting freeze windows or updating plugins.
Vulnerability Analyst	Yes	An account that can perform basic tasks within the application. A Vulnerability Analyst is allowed to view security data, perform scans, share objects, view logs, and work with tickets.
No Role	No	An account with virtually no permissions. No Role is assigned to a user if their designated role is deleted.
Custom Role	Yes	A custom role that you create by enabling or disabling individual permissions.

Role Options

Permissions Option	Description
General	
Name	Custom role name
Description	Custom role description
Scanning Permissions	
Create Scans	Allows the user to create policy-based scans. Disabling **Create Policies** while enabling this permission allows you to lock user into specific set of policies for scanning.

Permissions Option	Description
Create Plugin Scans	(Appears when **Create Scans** is enabled) Allows the user to create single plugin remediation scans.
Create Agent Synchronization Jobs	Allows the user to add agent synchronization jobs that fetch agent scan results from Tenable Vulnerability Management or Tenable Nessus Manager.
Create Agent Scans	Allows the user to add agent scans that create and launch parallel scans in Tenable Nessus Manager, then import the scan results to Tenable Security Center.
Create Audit Files	Allows the user to upload audit files, which can be used for configuration audit scans.
Create Policies	Allows the user to set scan parameters and select plugins for scanning.
Upload Nessus Scan Results	Allows the user to import results from an external Nessus scanner. Result upload will be limited to user's repositories and restricted by user's IP address ranges.
Manage Freeze Windows	Allows the user to add, edit, and delete organization-wide freeze windows. Freeze windows prevent scans from launching and stop any scans in progress.
Asset Permissions	
Create LDAP Query Assets	Allows the user to create LDAP Query Assets, which update a list of hosts based on a user-defined LDAP query.
Analysis Permissions	
Accept Risks	Allows the user to accept risks for vulnerabilities, which removes them from the default view for analysis, dashboards, and reports.
Recast Risks	Allows the user to change the severity for vulnerabilities.
Manage Risks	(Appears when **Accept Risks** or **Recast Risks** is enabled) Allows the user to modify accept and recast risk rules created by other users.

Permissions Option	Description
Organizational Permissions	
Share Objects Between Groups	Allows the user to share assets, audit files, credentials, queries, and policies with any group. Users in groups to which these objects have been shared can use the objects for filtering and scan creation.
View Organization Logs	Allows the user to view logs for entire organization.
User Permissions	
Manage Roles	Allows the user to create new roles and edit and delete organizational roles. Any roles added must have permissions equal to or lesser than the user's role.
Manage Groups	Allows the user to add, edit, and delete groups. Users with this permission are allowed to create groups with access to any vulnerability and event data available to the organization.
Manage Group Relationships	Allows the user to set other user's relationship with any other groups. Group relationships allow for a user to view and manage objects and users in other groups.
Report Permissions	
Manage Images	Allows the user to upload images, so anyone in the organization can use the images in reports.
Manage Attribute Sets	Allows the user to add, edit, and delete attribute sets.
System Permissions	
Update Feeds	Allows the user to request a plugin update or a Tenable Security Center feed update.
Workflow Permissions	
Create Alerts	Allows the user to create alerts which are used to trigger actions (e.g.,

Permissions Option	Description
	launch scans, run reports, send emails) when specified vulnerability or event conditions occur.
Create Tickets	Allows the user to create tickets, which are typically used to delegate work to other users.
Attack Surface Discovery Permissions	
Manage Attack Surface Discovery Domains	Allows the user to manage Attack Surface Discovery Domains.
View Domain Inventory Assets	Allows the user to view domain inventory assets.
Host Assets Permissions	
View Host Assets	Allows the user to view host assets.

Create a User Role

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information about user role options, see User Roles.

To create a custom user role:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Roles**.

   The **Roles** page appears.

3. Click **Add**.

   The **Add Role** page appears.

4. In the **Name** box, type a name for the role.

5. (Optional) In the **Description** box, type a description for the role.

6. Set the following permissions, as described in User Roles:

- **Scanning Permissions**

- **Asset Permissions**

- **Analysis Permissions**

- **Domain Permissions**

- **Organization Permissions**

- **User Permissions**

- **Reporting Permissions**

- **System Permissions**

- **Workflow Permissions**

7. Click **Submit**.

Tenable Security Center saves your configuration.

Edit a User Role

Required Tenable Security Center User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information about user role options, see User Roles.

To edit the permissions of a custom or system-provided role:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Roles**.

The **Roles** page appears.

3. Right-click the row for the user role you want to edit.

The actions menu appears.

-or-

Select the check box for the user role you want to edit.

The available actions appear at the top of the table.

4. Click **More** > **Edit**.

   The **Edit Role** page appears.

5. (Optional) Modify the **Name**

6. (Optional) Modify the **Description**.

7. (Optional) Modify the following permissions, as described in User Roles:

   - **Scanning Permissions**

   - **Asset Permissions**

   - **Analysis Permissions**

   - **Domain Permissions**

   - **Organization Permissions**

   - **User Permissions**

   - **Reporting Permissions**

   - **System Permissions**

   - **Workflow Permissions**

8. Click **Submit**.

   Tenable Security Center saves your configuration.

View User Role Details

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can view details for any user role. For more information, see User Roles.

To view role details:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Roles**.

The **Roles** page appears.

3. Right-click the row for the user role you want to view.

   The actions menu appears.

   -or-

   Select the check box for the user role you want to view.

   The available actions appear at the top of the table.

4. Click **View**.

   The **View Role** page appears.

Section	Action
General	View general information for the user role. • **Name** — The user role name. • **Description** — The user role description. • **User Count** — The number of users with this role. • **Created** — The date the user role was created. • **Last Modified** — The date the user role was last modified. • **ID** — The user role ID.
Scanning Permissions	View a summary of permissions for the role. For more information, see User Roles.
Asset Permissions	
Analysis Permissions	
Organization Permissions	
User Permissions	

Section	Action
Reporting Permissions	
System Permissions	
Workflow Permissions	

Delete a User Role

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see User Roles.

To delete a custom or system-provided user role:

> **Note:** Deleting a role will cause all users with that role to lose all assigned permissions.

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Roles**.

   The **Roles** page appears.

3. Select the role you want to delete:

   To delete a single user role:

   a. In the table, right-click the row for the role you want to delete.

      The actions menu appears.

   b. Click **Delete**.

   To delete multiple user roles:

a. In the table, select the check box for each role you want to delete.

The available actions appear at the top of the table.

b. At the top of the table, click **More** > **Delete**.

A confirmation window appears.

4. Click **Delete**.

Tenable Security Center deletes the role.

Organizations and Groups

An *organization* is 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 address networks. *Users* refers to any non-administrator user account on Tenable Security Center. *Groups* refers to collections of users with the same permissions within an organization.

For more information, see Organizations and Groups.

Organizations

An *organization* is a set of distinct users and groups and the resources (for example, scanners, repositories, and LDAP servers) they have available to them.

The organization is managed primarily by the administrator users and security manager users. The administrator user creates the organization and creates, assigns, and maintains the security manager user account. The security manager user (or any organizational user with appropriate permissions) creates other users within the organization. Groups allow you to manage users and share permissions to resources and objects among the group. For more information, see User Access.

Multiple organizations can share the same repositories, and the vulnerability data associated with the overlapping ranges is 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.

Creation of an organization is a multi-step process. After you create an organization, Tenable Security Center prompts you to create the initial security manager user. For more information, see Add an Organization and Delete an Organization.

To view details for any organization, see View Organization Details.

To view the users in an organization, filter by the organization on the [Users](#) page. For more information about filters, see [Apply a Filter](#).

Organization Options

Option	Description
General	
Name	(Required) The organization name.
Description	A description for the organization.
Contact Information	The relevant contact information for the organization including address, city, state, country, and phone number.
Password Expiration	
Enable Password Expiration	When enabled, passwords for users in the organization will expire after the number of days specified in the **Expiration Days** box.
Expiration Days	The number of days before the user's password expires. You can enter a number between 1 and 365. The user will receive daily password expiration notifications at login, starting 14 days before the password expires. After the password expires, the user must change their password at the next login. For more information about Tenable Security Center notifications, see [Notifications](#).
Scanning	
Distribution Method	The scan distribution mode you want to use for this organization: • **Automatic Distribution Only**: Tenable Security Center chooses one or more scan zones to run the scan. Organizational users cannot choose a scan zone when configuring a scan.

Option	Description
	Tenable Security Center distributes targets for scans based on your configured scan zone ranges. This facilitates optimal scanning and is useful if an organization has devices placed behind a firewall or NAT device or has conflicting RFC 1918 non-internet-routable address spaces. • **Locked Zone**: Tenable Security Center uses the one **Available Zone** you specify to run the scan. Organizational users cannot modify the scan zone when configuring a scan. • **Selectable Zones**: Tenable Security Center allows organizational users to select a scan zone when configuring a scan. This mode allows organizational users to use scanners to run internal and external vulnerability scans and analyze the vulnerability stance from a new perspective. For example, an organizational user can choose an external scanner to see the attack surface from an external attacker's perspective. For more information about scan zones, see Scan Zones.
Available Zones	One or more scan zones that you want organizational users to have access to when configuring scans.
Allow for Automatic Distribution	Enable or disable this option to specify whether you want Tenable Security Center to select one or more scan zones automatically if an organizational user does not specify a scan zone when configuring a scan. • When enabled, Tenable Security Center chooses one or more scan zones as specified by your **Restrict to Selected Zones** setting.

Option	Description
	• When disabled, Tenable Security Center requires the organizational user to specify a scan zone when configuring a scan.
Restrict to Selected Zones	If **Allow for Automatic Distribution** is enabled, enable or disable this option to specify the zones you want Tenable Security Center to choose from when automatically distributing zones. • When enabled, Tenable Security Center chooses from the **Available Zones** shared with the organization. • When disabled, Tenable Security Center chooses from all zones on Tenable Security Center.
Restricted Scan Ranges	The IP address ranges you do not want users in this organization to scan.
Analysis	
Accessible LCEs	The Log Correlation Engines that you want this organization to have access to. You can search for the Log Correlation Engines by name or scroll through the list.
Accessible Repositories	The repositories that you want this organization to have access to. You can search for the repositories by name or scroll through the list.
Accessible Agent Capable Scanners	The Tenable Nessus scanners (with Tenable Agents enabled) that you want this organization to have access to. Select one or more of the available scanners to allow the organization to import Tenable Agent results from the selected scanner.
Accessible LDAP Servers	The LDAP servers that you want this organization to have access to. An organization must have access to an LDAP server to perform LDAP authentication on user accounts within that organization, and to configure LDAP query assets.

Option	Description
	Note: If you revoke access to an LDAP server, users in the organization cannot authenticate and LDAP query assets cannot run.
Custom Analysis Links	
A list of custom analysis links provided to users within the host vulnerability details when analyzing data outside of Tenable Security Center is desired. Click **Add Custom Link** to create a new option to type the link name and URL to look up additional data external to Tenable Security Center. 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	
Low	The vulnerability weighting to apply to **Low** criticality vulnerabilities for scoring purposes. (Default: 1)
Medium	The vulnerability weighting to apply to **Medium** criticality vulnerabilities for scoring purposes. (Default: 3)
High	The vulnerability weighting to apply to **High** criticality vulnerabilities for scoring purposes. (Default: 10)
Critical	The vulnerability weighting to apply to **Critical** criticality vulnerabilities for scoring purposes. (Default: 40)
Vulnerability Scoring System	
Scoring System	The scoring system Tenable Security Center uses to assess the severity of vulnerabilities: **CVSS v2**, **CVSS v3**, or **CVSS v4**. **Note:** Changing the **Scoring System** while Tenable Security Center is running certain operations, such as preparing reports or dashboard data, results in data using mixed CVSS v2, CVSS v3, and CVSS v4 scores.

Option	Description
	Note: Changing the **Scoring System** does not impact historical dashboard trend data. For example, if you change the **Scoring System** from **CVSS v3** to **CVSS v4**, dashboard trend data before the change displays CVSS v3 scores while dashboard trend data after the change displays CVSS v4 scores.

Add an Organization

Required Tenable Security Center User Role: Administrator

For more information about organization options, see Organizations.

To add an organization:

1. Log in to Tenable Security Center via the user interface.

2. Click **Organizations**.

   The **Organizations** page appears.

3. Click **Add**.

   The **Add Organization** page appears.

4. Configure the following settings:

   - **General**

   - **Password Expiration**

   - **Scanning**

   - **Analysis**

   - **Custom Analysis Links**

   - **Vulnerability Weights**

   - **Vulnerability Scoring System**

5. Click **Submit**.

   Tenable Security Center saves your configuration.

View Organization Details

> **Required Tenable Security Center User Role:** Administrator

You can view details for any organization. For more information, see [Organizations](#).

To view organization details:

1. Log in to Tenable Security Center via the user interface.

2. Click **Organizations**.

   The **Organizations** page appears.

3. Right-click the row for the organization you want to view.

   The actions menu appears.

   -or-

   Select the check box for the organization you want to view.

   The available actions appear at the top of the table.

4. Click **View**.

   The **View Organization** page appears.

Section	Action
General	View general information for the organization. • **Name** — The organization name. • **Description** — The organization description. • **Address** / **City** / **State** / **Country** / **Phone** — The contact information for the organization. • **Created** — The date the organization was created.

Section	Action
	• **Last Modified** — The date the organization was last modified. • **ID** — The organization ID.
Password Expiration	View a summary of your password expiration settings for the organization. For more information about a setting, see Organizations.
Scanning	View a summary of your scanning settings for the organization. For more information about a setting, see Organizations.
Analysis	View a summary of your analysis settings for the organization. For more information about a setting, see Organizations.
Custom Analysis Links	View a summary of your custom analysis link settings for the organization. For more information about a setting, see Organizations.
Vulnerability Weights	View a summary of your vulnerability weights settings for the organization. For more information about a setting, see Organizations.
Vulnerability Scoring System	View the vulnerability scoring system selected for the organization. For more information, see Organizations.

Delete an Organization

Required Tenable Security Center User Role: Administrator

For more information, see Organizations.

To delete an organization:

Note: Deleting an organization deletes all of the users in that organization.

1. Log in to Tenable Security Center via the user interface.

2. Click **Organizations**.

The **Organizations** page appears.

3. Select the organization you want to delete:

   To delete a single organization:

   a. In the table, right-click the row for the organization you want to delete.

      The actions menu appears.

   b. Click **Delete**.

   To delete multiple organizations:

   a. In the table, select the check box for each organization you want to delete.

      The available actions appear at the top of the table.

   b. At the top of the table, click **Delete**.

   A confirmation window appears.

4. Click **Delete**.

   A confirmation window appears.

5. Click **Delete**.

   Tenable Security Center deletes the organization.

Groups

User groups are a way to group rights to objects within an organization, and then quickly assign these rights to one or more users. A user's group membership determines their access to security data. When a user creates various objects such as reports, scan policies, dashboards, and other similar items, these objects are automatically shared among the group members if the group permissions allow view and control.

For more information, see Add a Group, View Group Details, and Delete a Group.

Group Options

Option	Description
General tab	
Name	The name for the group.
Description	A description for the group (e.g., **security team at the central office** or **executives on the east coast**).
Viewable Hosts	The IP addresses and agent IDs that are viewable by the group. The selection is made by all defined assets or the selection of one or more asset lists.
Repositories	The repositories you want to share with the group.
Log Correlation Engines	The Log Correlation Engines you want to assign to the group.
Sample Content	When enabled, Tenable provides sample content objects to users in the group: • sample dashboards **(Executive 7 Day**, **Executive Summary**, and **Vulnerability Overview**) • sample reports (**Critical and Exploitable Vulnerabilities**, **Monthly Executive**, and **Remediation Instructions by Host**) • sample ARCs (**CCC 1: Maintain an Inventory of Software and Hardware**, **CCC 2: Remove Vulnerabilities and Misconfigurations**, **CCC 3: Deploy a Secure Network**, **CCC 4: Authorize Users**, **and CCC 5: Search for Malware and Intruders**) • sample assets required for the sample ARCs After enabling **Sample Content**, you must add a new user to the group before all users in the group can access the sample content. **Note:** If a user in a group deletes a sample content object, the object is deleted for all other users in that group. **Note:** If you move a sample content object owner (e.g., move the first

Option	Description
	user in group A to group B), Tenable Security Center: 1. Assigns their dashboards and ARCs to a new sample content object owner in group A. Tenable Security Center does not reassign reports or assets. 2. Recreates their dashboards, ARCs, and assets required for ARCs in group B. Tenable Security Center does not recreate reports.
Share to Group tab	
Available Objects	The list of available objects to be shared with the group on creation or edit in a bulk operation.

Add a Group

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information about group options, see Groups.

To add a group:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Users** > **Groups**.

   The **Groups** page appears.

3. Click **Add**.

   The **Add Group** page appears.

4. Configure the **General** options.

5. Configure the **Share to Group** options.

6. Click **Submit**.

   Tenable Security Center saves your configuration.

View Group Details

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can view details for any group. For more information, see Groups.

To view group details:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Groups**.

   The **Groups** page appears.

3. Right-click the row for the group you want to view.

   The actions menu appears.

   -or-

   Select the check box for the group you want to view.

   The available actions appear at the top of the table.

4. Click **View**.

   The **View Group** page appears.

Section	Action
General	View general information for the group. • **Name** — The group name. • **Description** — The group description. • **Created** — The date the group was created. • **Last Modified** — The date the group options were last modified. • **ID** — The group ID.
Access	View the lists of **Viewable Hosts**, **Repositories**, and **LCEs** users in the group can access. For more information, see Group Options.
Preferences	View whether you enabled **Sample Content** for the group. For more

Section	Action
	information, see [Group Options](#).
Users	View the list of users associated with the group.

Delete a Group

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To delete a group:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Groups**.

   The **Groups** page appears.

3. Select the group you want to delete:

   ### To delete a single group:

   a. In the table, right-click the row for the group you want to delete.

      The actions menu appears.

   b. Click **Delete**.

   ### To delete multiple groups:

   a. In the table, select the check box for each group you want to delete.

      The available actions appear at the top of the table.

   b. At the top of the table, click **Delete**.

   A confirmation window appears.

4. Click **Delete**.

   Tenable Security Center deletes the group.

User Accounts

The **Users** page displays the user accounts on Tenable Security Center, limited by your account privileges. You can sort the columns or apply filters to locate specific user accounts. You can also add a user (Add a TNS-Authenticated User, Add an LDAP-Authenticated User, or Add a SAML-Authenticated User) or Delete a User.

You can create one or more administrator accounts on Tenable Security Center. You can create one or more organizational users (security managers and custom roles) per organization. Tenable recommends you make at least one TNS-authenticated administrator and security manager user per organization so that you can still log in if the LDAP or SAML service becomes unavailable. For more information about user account types, see User Access.

For more information about options available when configuring user accounts, see User Account Options.

Linked User Accounts

You can create *linked user accounts* and *linked non-admin user accounts* to allow users to switch between accounts without logging out and logging back in to Tenable Security Center. For more information, see Linked User Accounts.

API Keys

You can generate API keys to authenticate as a specific user for Tenable Security Center API requests. For more information, see API Key Authentication.

Add a TNS-Authenticated User

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information about user account configuration options, see TNS User Account Options.

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**. For more information, see User Roles.

13. Select a **Group**. For more information, see Organizations and Groups.

14. (Optional) If you want to customize the group-related permissions for the user, modify the **Group Permissions** as described in Custom Group Permissions.

15. (Optional) If you want to share an asset list with the user, select an **Asset**. For more information, see Assets.

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.

Add an LDAP-Authenticated User

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information about user account configuration options, see User Accounts To automatically add LDAP-authenticated users by importing users from your LDAP identity provider, see Configure LDAP User Provisioning.

To add an LDAP-authenticated user account as an administrator user:

1. Log in to Tenable Security Center via the user interface.

2. Configure an LDAP server, as described in [LDAP Authentication](LDAP%20Authentication). If you want the new user to be a member of an organization, associate the LDAP server with an organization.

3. Click **Users** > **Users**.

   The **Users** page appears.

4. Click **Add**.

   The **Add User** page appears.

5. Select a **Role** for the user account.

6. If you selected **Security Manager** as the **Role**, select an **Organization** for the user account. You must select an organization with an associated LDAP server.

7. (Optional) Type a **First Name** and **Last Name** for the user.

8. In the **Type** drop-down list, select **LDAP**. If **LDAP** does not appear in the drop-down list, add an LDAP server as described in [Add an LDAP Server](Add%20an%20LDAP%20Server).

9. Select the **LDAP Server** where you want to authenticate the user.

10. Type a **Search String** to find existing users on the LDAP server.

11. Click **Search**.

    The page displays the **LDAP Users Found** by the LDAP search string.

12. Select an LDAP user from the **LDAP Users Found** drop-down box.

    The page populates the **Username** option with your selection.

13. View the **Username**. Tenable does not recommend modifying the **Username** since it must match the username on the LDAP server.

14. Select a **Time Zone**.

15. (Optional) Select a **Scan Result Default Timeframe**.

16. (Optional) Enable **Cached Fetching**.

17. (Optional) Enable **Dark Mode** for the user.

18. (Optional) Type **Contact Information** for the user.

19. Click **Submit.**

    Tenable Security Center saves your configuration.

To add an LDAP-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. Confirm that an administrator user configured an LDAP server, and that the LDAP server was associated with the organization where you want to create a user account.

3. Click **Users** > **Users**.

   The **Users** page appears.

4. Click **Add**.

   The **Add User** page appears.

5. (Optional) Type a **First Name** and **Last Name** for the user.

6. In the **Type** drop-down list, select **LDAP**. If **LDAP** does not appear in the drop-down list, add an LDAP server as described in Add an LDAP Server.

7. Select the **LDAP Server** where you want to authenticate the user.

8. Select an LDAP user from the **LDAP Users Found** drop-down box.

   The page populates the **Username** option with your selection.

9. View the **Username**. Tenable does not recommend modifying the **Username** since it must match the username on the LDAP server.

10. Select a **Time Zone**.

11. (Optional) Select a **Scan Result Default Timeframe**.

12. (Optional) Enable **Cached Fetching**.

13. Select a **Role**. For more information, see User Roles.

14. Select a **Group**. For more information, see Organizations and Groups.

15. (Optional) If you want to customize the group-related permissions for the user, modify the **Group Permissions** as described in [Custom Group Permissions](Custom%20Group%20Permissions).

16. (Optional) If you want to share an asset list with the user, select an **Asset**. For more information, see Assets.

17. (Optional) Enable **Dark Mode** for the user.

18. (Optional) Type **Contact Information** for the user.

19. Click **Submit**.

    Tenable Security Center saves your configuration.

Add a SAML-Authenticated User

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](User%20Roles).

For more information about user account configuration options, see [SAML User Account Options](SAML%20User%20Account%20Options). To automatically add SAML-authenticated users by importing users from your SAML identity provider, see [Configure SAML User Provisioning](Configure%20SAML%20User%20Provisioning).

Before you begin:

- Review the [Tenable SAML Configuration Quick-Reference](Tenable%20SAML%20Configuration%20Quick-Reference) guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center.

- Configure SAML authentication, as described in [Configure SAML Authentication Manually via the User Interface](Configure%20SAML%20Authentication%20Manually%20via%20the%20User%20Interface).

To add a SAML-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. (Optional) Type a **First Name** and **Last Name** for the user.

5. In the **Type** drop-down box, select **SAML**. If **SAML** does not appear in the drop-down box, configure SAML authentication as described in Configure SAML Authentication Manually via the User Interface.

6. In the **Username** box, type the user's SAML username exactly as it appears in your identity provider SAML configuration for this user.

7. Select a **Time Zone**.

8. (Optional) Select a **Scan Result Default Timeframe**.

9. (Optional) Enable **Cached Fetching**.

10. (Optional) Enable **Dark Mode** for the user.

11. (Optional) Type **Contact Information** for the user.

12. Click **Submit**.

Tenable Security Center saves your configuration.

To add a SAML-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. In the **Type** drop-down list, select **SAML**. If **SAML** does not appear in the drop-down list, configure SAML authentication as described in Configure SAML Authentication Manually via the User Interface.

6. In the **Username** box, type the user's SAML username exactly as it appears in your identity provider SAML configuration for this user.

7. Select a **Time Zone**.

8. (Optional) Select a **Scan Result Default Timeframe**.

9. (Optional) Enable **Cached Fetching**.

10. Select a **Role**. For more information, see User Roles.

11. Select a **Group**. For more information, see Organizations and Groups.

12. (Optional) To customize the user's object and user account management permissions, modify the **Group Permissions** as described in Custom Group Permissions.

13. (Optional) To share an asset list with the user, select an **Asset**. For more information, see Assets.

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.

Manage User Accounts

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information about user accounts, see User Accounts.

To view or edit a user account:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Users** > **Users**.

   The **Users** page appears.

3. To filter the users that appear on the page, apply a filter as described in Apply a Filter.

> **Note:** If you are logged in with an administrator account, the **Organization** filter is set to **System** by default. To view users from other organizations, select a different organization for the **Organization** filter.

4. To view details for a user, see View User Details.

5. To edit a user:

   a. Right-click the row for the user you want to edit.

      The actions menu appears.

      -or-

      Select the check box for the user you want to edit.

      The available actions appear at the top of the table.

   b. Click **Edit**.

      The **Edit User** page appears.

   c. Modify the user details.

      > **Note:** If you want to edit a Tenable Security Center user that was created via user provisioning and you enabled **User Data Sync**, edit the user in your SAML or LDAP identity provider. Otherwise, the Tenable Security Center user data synchronization overwrites your changes the next time the user logs in to Tenable Security Center using your SAML or LDAP identity provider. For more information about **User Data Sync**, see SAML Authentication Options or LDAP Authentication Options.

   d. Click **Submit**.

      Tenable Security Center saves your configuration.

6. To delete a user, see Delete a User.

Edit Your User Account

Required Tenable Security Center User Role: Any

You can edit your user account to update your password, contact information, display preferences, and other settings depending on your user role. If you want to edit a linked user account, see Edit a Linked User Account.

> **Note:** The username can be changed for all users except the first Security Manager and the first administrator of each organization.

To edit your user account as an administrator:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Users**.

   The **Users** page appears.

3. Right-click the row for your user account.

   The actions menu appears.

   -or-

   Select the check box for your user account.

   The available actions appear at the top of the table.

4. Click **More** > **Edit**.

   The **Edit User** page appears.

5. Modify your user account settings. For more information, see User Account Options.

6. Click **Submit**.

   Tenable Security Center saves your configuration.

To edit your user account as an organizational user:

1. Log in to Tenable Security Center via the user interface.

2. Click **Username** > **Profile**.

   The **Edit User Profile** page appears.

3. Modify your user account settings. For more information, see User Account Options.

4. Click **Submit**.

   Tenable Security Center saves your configuration.

View User Details

Required Tenable Security Center User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information about user accounts, see [User Accounts](#).

To view details for a user:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Users**.

   The **Users** page appears.

3. Right-click the row for the user you want to view.

   The actions menu appears.

   -or-

   Select the check box for the user you want to view.

   The available actions appear at the top of the table.

4. Click **View**.

   The **View User** page appears.

5. View the following information for the user:

Section	Action
General	View general information for the user. • **Created** — The date the user was created. • **Last Modified** — The date the user was last modified. • **ID** — The user ID.
Membership	View role and organization information for the user. For more information, see [User Account Options](#).
Password Expiration	View password expiration settings for the user. For more information, see [User Account Options](#).
Display Options	View dark mode settings for the user. For more information, see [User Account Options](#).

Contact Information	View contact information for the user. For more information, see [User Account Options](#).
API Key	If the user has API keys, view the access key for the user. For more information, see [Enable API Key Authentication](#).
Linked User Details	**Required Tenable Security Center User Role:** Administrator View linked user accounts associated with the user: • **Linked Users** — If the user is an Administrator, view the linked Security Manager users. If the user is a Security Manager, view the linked SM-Linked users. • **Primary User** — If the user is a linked Security Manager, view the associated Administrator user. If the user is an SM-Linked user, view the associated Security Manager user. For more information, see [Linked User Accounts](#).

Replace First User

> **Required Tenable Security Center User Role:** Administrator

By default, the first user is the first Security Manager user account you create during setup. You can promote a different Security Manager account to first user to replace the previous Security Manager account.

When you replace a first user with a different Security Manager account, the promoted Security Manager will absorb the contents of the previous Security Manager's account. The promoted Security Manager account will keep both its objects and the objects of the previous Security Manager account, because that data is not cleared before the migration. After the replacement, the promoted Security Manager loses any previous notifications and running jobs.

> **Note:** When you promote a certificate-based user account to first user, the promoted user account automatically changes to password-based authentication.

Before you begin

- These steps assume you already have more than one Security Manager account. If you do not already have a second Security Manager account, create a new user account with the Security Manager role. For more information about creating user accounts, see User Accounts.

To replace the first user with a different Security Manager user account:

1. Log in to Tenable Security Center via the Admin user interface.

2. Click **Users** > **Users**.

   The **Users** page appears.

3. On the left side of the page, select the organization by which you want to filter the page.

4. Right-click the row for the current Security Manager first user.

   The actions menu appears.

   -or-

   Select the check box for the current Security Manager first user.

   The available actions appear under **More** at the top of the table.

5. Click **Replace First User**.

   The **Replace First User** window appears.

6. In the **Users** drop-down, select the Security Manager that you want to promote to first user.

7. In the **New Password** box, type a new password for the user.

8. Click **Replace**.

   The Security Manager you selected in step 5 is promoted to first user.

Delete a User

Required Tenable Security Center User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

If you want to migrate a user's objects, you must use a Security Manager account in the user's organization to delete the user. Other roles cannot migrate user objects.

Note: You cannot delete the initially created Administrator and Security role users from any of your organizations. You can replace the initial Security Manager user. For more information, see Replace First User.

Note: If you want to delete an Administrator or Security Manager with linked user accounts, you must delete the linked accounts associated with the Administrator or Security Manager before deleting the Administrator or Security Manager, as described in Delete a Linked User Account. For more information about linked user accounts, see Linked User Accounts.

Note: If you want to delete a Tenable Security Center user that was created via user provisioning, delete the user from your SAML or LDAP identity provider. If you delete a user in Tenable Security Center that was created via user provisioning without deleting the user in your SAML or LDAP identity provider, Tenable Security Center automatically re-creates the user in Tenable Security Center the next time they log in using your SAML or LDAP identity provider. For more information, see SAML User Provisioning or LDAP User Provisioning.

To delete a user:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Users**.

   The **Users** page appears.

3. Select the user you want to delete:

   To delete a single user:

   a. In the table, right-click the row for the user you want to delete.

      The actions menu appears.

   b. Click **Delete**.

   To delete multiple users:

   a. In the table, select the check box for each user you want to delete.

      The available actions appear at the top of the table.

   b. At the top of the table, click **More** > **Delete**.

   A confirmation window appears.

4. (Optional) If you want to migrate the user's objects, click the toggle to migrate the user's objects to another user. Tenable Security Center supports migrating:

- Active scans, agent scans, and scan results

- Custom assets, credentials, audit files, and scan policies

- Freeze windows

- Queries

- Tickets and alerts

- ARCs

- Dashboards

- Reports, report images, report attributes, and report results

If you do not migrate the user's objects, Tenable Security Center deletes the user's objects.

> **Note:** The following are considerations for migrating objects:
>
> - You cannot migrate objects when deleting an Administrator user because all Administrator-created objects are shared across Tenable Security Center and remain accessible after user deletion.
>
> - If you delete a linked non-admin user, the user's objects can only be migrated to the linked Security Manager account. For more information about linked user accounts, see Linked User Accounts.
>
> - When you delete multiple users, you cannot migrate objects for the users unless you are logged in as an Administrator.

5. Click **Delete**.

Tenable Security Center deletes the user.

Linked User Accounts

You can create *linked user accounts* and *linked non-admin user accounts* to allow users to switch between accounts without logging out and logging back in to Tenable Security Center.

- **Linked User Account** - A Security Manager user account that is linked to an Administrator user account.

- **Linked Non-Admin User Account** - An SM-Linked user account that is linked to a Security Manager user account.

On the **Users** page, a tooltip appears next to linked and linked non-admin users that displays the username for the associated Administrator or Security Manager account.

Linked User

Users with linked user accounts can use a single set of login credentials to log in to Tenable Security Center as an Administrator, then switch to a linked Security Manager, from one linked Security Manager to another, or from a linked Security Manager to the linked Administrator. You do not need to re-authenticate to switch between linked user accounts after logging in as the linked Administrator.

The following restrictions apply to linked user accounts:

- Each Administrator can have one linked Security Manager per organization.

- Each linked Security Manager can be associated with only one Administrator user account.

- Linked Security Managers cannot log in to Tenable Security Center directly. You must log in to the Administrator account associated with the linked Security Manager, then switch users.

- You cannot convert a standalone user account to a linked user account.

- You cannot convert a linked user account to a standalone user account. To unlink a Security Manager user from an Administrator user, delete the linked Security Manager, then create a standalone Security Manager.

Linked Non-Admin User

Users with linked non-admin user accounts can use a single set of login credentials to log in to Tenable Security Center as a Security Manager, then switch to a linked SM-Linked account, from one SM-Linked account to another, or from an SM-Linked account to the linked Security Manager. You do not need to re-authenticate to switch between linked user accounts after logging in as the linked Security Manager.

> **Note:** You must have more than one organization to create a linked non-admin user. For more information about organizations, see Organizations.

The following restrictions apply to linked non-admin user accounts:

- Each Security Manager can have one linked SM-Linked user account per organization.

- Each SM-Linked user account can be associated with only one Security Manager user account.

- SM-Linked user accounts cannot create, edit, or delete user accounts in the organization.

- SM-Linked users do not have access to the **Profile** page to edit their own accounts.

- SM-Linked users cannot log in to Tenable Security Center directly. You must log in to the Security Manager account associated with the SM-Linked account, then switch users.

- You can only create linked non-admin user accounts for TNS user accounts. Linked non-admin user accounts are not supported for LDAP or SAML user accounts.

- You cannot convert a standalone user account to a linked non-admin user account.

- You cannot convert an SM-Linked user to a standalone user account. To unlink an SM-Linked user from a Security Manager user, delete the SM-Linked user account.

- You cannot create a standalone SM-Linked user account.

For more information about user accounts in Tenable Security Center, see User Access and User Roles.

For more information about linked user accounts, see:

- Add a Linked User

- Switch to a Linked User Account

- Edit a Linked User Account

- Delete a Linked User Account

Add a Linked User

You can create *linked user accounts* and *linked non-admin user accounts* to allow users to switch between accounts without logging out and logging back in to Tenable Security Center. You can add

a linked Security Manager to an Administrator account, or you can add an SM-Linked user to a Security Manager account. The following restrictions apply to linked accounts:

- You cannot convert a standalone user account to a linked user account.

- Each Administrator can have one linked Security Manager per organization.

- Each Security Manager can have one linked SM-Linked user per organization.

- Each linked Security Manager user can be associated with only one Administrator user account.

- Each SM-Linked user can be associated with only one Security Manager user account.

For more information about linked user accounts, see Linked User Accounts. For more information about user account configuration options, see User Account Options.

To add a linked Security Manager to an Administrator, or add an SM-Linked user to a Security Manager:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Users** > **Users**.

   The **Users** page appears.

3. Right-click the row for the Administrator or Security Manager to which you want to add a linked user.

   The actions menu appears.

   -or-

   Select the check box for the Administrator or Security Manager to which you want to add a linked user.

   The available actions appear at the top of the table.

4. Click **Add Linked User**.

   The **Add User** page appears. Tenable Security Center pre-populates the **First Name**, **Last Name**, and **Contact Information** fields with values from the Administrator or Security Manager user account.

5. Select an **Organization**. If you create a linked non-admin user, you can select more than one organization and Tenable Security Center will create one linked non-admin user for each organization.

6. (Optional) Modify the **First Name** and **Last Name** for the user.

7. Type a **Username** for the user. If you create a linked non-admin user, Tenable Security Center adds the orgID to the end of the username.

8. Select a **Time Zone**.

9. (Optional) Select a **Scan Result Default Timeframe**.

10. (Optional) Enable **Cached Fetching**.

11. (Optional) Enable or disable **Dark Mode** for the user.

12. (Optional) Modify the **Contact Information** for the user.

13. Click **Submit**.

    Tenable Security Center saves your configuration.

What to do next:

- Switch between a linked user account and its associated Administrator or Security Manager user account, as described in Switch to a Linked User Account.

Switch to a Linked User Account

You can create *linked user accounts* and *linked non-admin user accounts* to allow users to switch between accounts without logging out and logging back in to Tenable Security Center.

Linked users can switch from the linked Administrator to a linked Security Manager, from one linked Security Manager to another, or from a linked Security Manager to the linked Administrator user. Linked non-admin users can switch from the linked Security Manager to an SM-Linked user, from one SM-Linked user to another, or from an SM-Linked user to the linked Security Manager. For more information about linked user accounts, see Linked User Accounts.

Before you begin:

- Configure one or more linked user accounts, as described in Add a Linked User.

To switch to a linked user account:

1. Log in to Tenable Security Center via the user interface.

> **Note:** You must log in to the Administrator or Security Manager account associated with the linked user, then switch between linked users. Linked Security Managers and SM-Linked users cannot log in to Tenable Security Center directly.

2. Click your user profile **SC** icon > **Switch User**. This option appears only if the current logged-in user already has a linked user account.

   The **Switch To Linked Account** window appears.

3. Click the name of the linked user you want to switch to.

4. Click **Switch**.

   Tenable Security Center logs you in as the selected user.

   The username menu updates to show the linked user account name and associated organization.

Edit a Linked User Account

Administrators can edit linked user accounts. Linked Security Manager users and SM-Linked users can edit their own account details. For more information, see Linked User Accounts.

To edit a linked user account as an Administrator:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Users**.

   The **Users** page appears.

3. Filter the **Users** page to show user accounts for the linked user's organization, as described in Apply a Filter.

4. Right-click the row for the linked user account you want to edit.

   The actions menu appears.

   -or-

   Select the check box for the linked user account you want to edit.

The available actions appear at the top of the table.

5. Click **More** > **Edit**.

    The **Edit User** page appears.

6. Modify the user account settings. For more information, see [User Account Options](#).

7. Click **Submit**.

    Tenable Security Center saves your configuration.

To edit your linked user account as a linked user:

1. Log in to Tenable Security Center via the user interface.

2. Switch to a linked user account, as described in [Switch to a Linked User Account](#).

3. Click **Username** > **Profile**.

    The **Edit User Profile** page appears.

4. Modify the user account settings. For more information, see [User Account Options](#).

5. Click **Submit**.

    Tenable Security Center saves your configuration.

Delete a Linked User Account

> **Required Tenable Security Center User Role:** Administrator

If you want to remove a linked user account, you must delete the linked account. You cannot convert a linked user account into a standalone user account. For more information about linked user accounts, see [Linked User Accounts](#).

> **Note:** If you want to delete an Administrator or Security Manager with linked user accounts, you must delete the linked accounts associated with the Administrator or Security Manager before deleting the Administrator or Security Manager.

To delete a linked user account:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Users**.

   The **Users** page appears.

3. Apply a filter to view the organization for the user you want to delete, as described in Apply a Filter.

4. Select the linked user account you want to delete:

   ## To delete a single linked user account:

   a. In the table, right-click the row for the linked user account you want to delete.

      The actions menu appears.

   b. Click **Delete**.

   ## To delete multiple linked user accounts:

   a. In the table, select the check box for each linked user account you want to delete.

      The available actions appear at the top of the table.

   b. At the top of the table, click **Delete**.

   A confirmation window appears.

5. (Optional) If you want to migrate the user's objects, click the toggle to migrate the user's objects to another user. Tenable Security Center supports migrating:

   - Active scans, agent scans, and scan results

   - Custom assets, credentials, audit files, and scan policies

   - Freeze windows

   - Queries

   - Tickets and alerts

   - ARCs

- Dashboards

- Reports, report images, report attributes, and report results

If you do not migrate the user's objects, Tenable Security Center deletes the user's objects.

> **Note:** You cannot migrate objects when deleting an Administrator user because all Administrator-created objects are shared across Tenable Security Center and remain accessible after user deletion.

6. Click **Delete**.

   Tenable Security Center deletes the user.

Custom Group Permissions

When creating or editing a user account, you can customize a user's group permissions.

- Your selection in the **Group** field assigns the user to a group.

- Your selections in the **Group Permissions** section grant the user resource (user and object) permissions in their assigned group and other groups.

For more information about organizations and groups, see [Organizations and Groups](#).

In the **Group Permissions** section, the **Manage All Users** and **Manage All Objects** sliders enable or disable all of the settings in the **User Permission** and **Object Permission** columns, respectively. By default, the system enables all permissions for all groups. You can clear the check boxes in each group row to restrict the user's ability to perform the following actions on the resources within a group.

Resources Controlled by Manage Users/User Permissions	Resources Controlled by Manage Objects/Object Permissions
- Users (edit and delete) - Groups (edit and delete)	- Reports (launch, stop, copy, delete, and sometimes edit) > **Note:** A user can only edit reports within their assigned group, even if you grant them **Object Permissions** for another group.

Resources Controlled by Manage Users/User Permissions	Resources Controlled by Manage Objects/Object Permissions
	• Report results (publish, email, copy, and delete)
	• Report images (delete)
	• Report attributes (delete)
	• Scan results (launch, import, copy, send to report, stop, pause, and delete)
	• Policies (edit, copy, and delete)
	• Assets (edit, share, and delete)
	• Alerts (edit and delete)
	• Audit files (edit, share, and delete)
	• Credentials (edit, share, and delete)
	• Tickets (edit, resolve, and close)
	• Risk rules (delete)
	• Queries (edit, share, and delete)
	• ARCs (edit, share, copy, and delete)
	• Dashboards (edit, share, copy, and delete)

Examples

Consider the following examples for a user assigned to *Group1*.

Control Permissions to Resources in the User's Assigned Group

- If you select the **User Permissions** and/or **Object Permissions** check boxes in the *Group1* row, the user can perform actions for all resources in *Group1*, including the resources owned by other users.

- If you clear the **User Permissions** and/or **Object Permissions** check boxes in the *Group1* row, the user cannot perform actions on resources owned by other users in *Group1*.

Control Permissions to Resources in Other Groups

- If you select the **User Permissions** and/or **Object Permissions** check boxes in the *Group2* row, the user can perform actions for all resources in *Group2*, including the resources owned by other users.

> **Note:** Although the user receives many permissions for resources in *Group2*, the user cannot edit reports owned by *Group2* users. Users must be assigned to *Group2* and have **Object Permissions** selected in order to edit reports, active scans, and agent scans.

- If you clear the **User Permissions** and/or **Object Permissions** check boxes in the *Group2* row, the user cannot perform actions on resources owned by other users in *Group2*.

Generate API Keys

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

API keys allow you to authenticate as a specific user for Tenable Security Center API requests. Administrators can generate API keys for any user account. Other roles can generate API keys for user accounts with the same role. For more information, see API Key Authentication.

> **Note:** If you generate API keys for a user that already has API keys, the old keys will be replaced. If you delete existing keys or generate new API keys for a user, Tenable Security Center deauthorizes API requests attempted with the old keys.

Before you begin:

- Enable API keys to allow users to perform API key authentication, as described in Enable API Key Authentication.

To generate API keys:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Users**.

The **Users** page appears.

3. Right-click the row for the user for which you want to generate an API key.

   The actions menu appears.

   -or-

   Select the check box for the user for which you want to generate an API key.

   The available actions appear at the top of the table.

4. Click **API Keys > Generate API Key**.

   A confirmation window appears.

5. Click **Generate**.

   The **Your API Key** window appears, displaying the access key and secret key for the user.

6. Save the API keys in a safe location.

> **Note:** You cannot view API secret keys in the Tenable Security Center interface after initial generation. If you lose your existing secret key, you must generate new API keys.

What to do next:

- Use the API keys to perform API requests, as described in API Key Authorization in the *Tenable Security Center API Best Practices Guide*.

Delete API Keys

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

After you delete a user's API keys, the deleted keys cannot be used for authentication in Tenable Security Center API requests. To generate new API keys for a user, see Generate API Keys. For more information, see API Key Authentication.

To delete API keys:

1. Log in to Tenable Security Center via the user interface.

2. Click **Users** > **Users**.

   The **Users** page appears.

3. Right-click the row for the user for which you want to delete API keys.

   The actions menu appears.

   -or-

   Select the check box for the user for which you want to delete API keys.

   The available actions appear at the top of the table.

4. Click **API Keys** > **Delete API Key**.

   A confirmation window appears.

5. Click **Delete**.

   The system deletes the API keys.

User Account Options

You can configure the following options for Tenable Security Center user accounts. The available options depend on the user type, the user's role, and the role of the user adding or editing the user.

- TNS User Account Options

- LDAP User Account Options

- SAML User Account Options

For more information about user accounts in Tenable Security Center, see User Accounts.

TNS User Account Options

To add a TNS-authenticated user, see Add a TNS-Authenticated User.

Option	Description
First Name	The user's first name.

Last Name	The user's last name.
Type	(If LDAP or SAML are configured) The type of authentication you want to perform on the user: • Tenable (**TNS**) • Lightweight Directory Access Protocol (**LDAP**) • Security Assertion Markup Language (**SAML**) You must configure an LDAP server or SAML authentication in order to select **LDAP** or **SAML** from the **Type** drop-down box.
Username	(Required) The username for the user account. **Note:** The username value is case-sensitive.
Password	(Required) The password for the user account. **Tip:** Tenable recommends using passwords that meet stringent length and complexity requirements. For information about Tenable Security Center password data encryption, see [Encryption Strength](#). When editing a user, type a new password to change the password for the user account.
Confirm Password	(Required) When creating a user or changing a user's password, re-type the password for the user account.
Password Change	Click **Change Password** to change the password for the user account. To change a user password: 1. Begin editing a user account, as described in [Manage User Accounts](#) or [Edit Your User Account](#). 2. Click **Change Password**. 3. In the **Current Password** box, type your password. If you do not have

	a password (for example, you have a SAML-authenticated or LDAP-authenticated user account), type any string of characters in this field.
	4. In the **Password** box, type a new password.
	5. In the **Confirm Password** box, type the new password again.
	6. Click **Submit**.
	Tenable Security Center saves your configuration.
Current Password	(If you click **Change Password**) Type your password. If you do not have a password (for example, you have a SAML-authenticated or LDAP-authenticated user account), type any string of characters in this field.
User Must Change Password	When enabled, the user must change their password upon initial login.
Account Locked	When enabled, the user cannot log in to Tenable Security Center. An administrator must unlock the user's account to allow them to log in.
Time Zone	(Required) The time zone for the user.
Scan Result Default Timeframe	The default **Completion Time** filter applied when the user accesses or refreshes the scan results page.
Cached Fetching	When enabled, Tenable Security Center caches plugin policy information and performs plugin policy downloads once per page load.
Password Expiration	
Password Never Expires	When enabled, the user's password will never expire. Any password expiration settings at the user or organization level will not apply to this user.
Enable Password Expiration or	When enabled, the user's password will expire after the number of days specified in the **Expiration Days** box.

Custom Password Expiration	When disabled, the user's password expiration settings will default to the organization settings. For more information about organization options, see [Organizations](#). The user will receive daily password expiration notifications at login, starting 14 days before the password expires. After the password expires, the user must change their password at the next login. For more information about Tenable Security Center notifications, see [Notifications](#).
Expiration Days	The number of days before the user's password expires. You can enter a number between 1 and 365.
Membership	
Role	(Required) The role assigned to the user. For more information, see [User Roles](#). Administrator users can create **Administrator** or **Security Manager** user accounts. Organizational users can create **Auditor**, **Credential Manager**, **Executive**, **No Role**, **Security Analyst**, **Security Manager**, or **Vulnerability Analyst** accounts at their own privilege level or lower. For example: - If a user is an Auditor, they can create new Auditors or lesser roles. - If a custom user has the Create Policies privilege but not the Update Feeds privilege, that user can create users with the Create Policies privilege, but not the Update Feeds privilege.
Organization	(Required) The organization where you want to assign the user account.
Group	(Required) The group where you want to assign the user account. A user's group determines their access to Tenable Security Center resources. For more information about groups, see [Groups](#). To grant a user limited privileges to other groups' resources, see [Custom Group Permissions](#).
Group Permissions	
Manage All	When enabled, allows the user to manage users in all of the user's assigned

Users	groups. For more information, see [Custom Group Permissions](#).
Manage All Objects	When enabled, allows the user to manage objects in all of the user's assigned groups. For more information, see [Custom Group Permissions](#).
Responsibility	
Asset	Assigns a user to an asset list for which the user is responsible. Assigning a user to an asset list makes it easier to determine who in a group or organization should be assigned tickets, notifications, and other tasks to resolve particular issues. Selecting an asset updates the User Responsibility Summary in the [Vulnerability Analysis](#) section.
Display Options	
Dark Mode	When enabled, sets the Tenable Security Center user interface to dark mode for the user.
Use System Dark Mode Setting	When enabled, the Tenable Security Center user interface uses the operating system setting for light or dark mode. This setting overrides the **Dark Mode** setting. If you select the sun or moon icon in the top navigation bar, that will override the **Use System Dark Mode Setting** for the user account.
Contact Information	
Title	
Address	
City	
State	The contact information for the user.
Country	
Email	
Phone	

LDAP User Account Options

You must configure an LDAP server to add LDAP-authenticated users. For more information, see [LDAP Authentication](#).

To add an LDAP-authenticated user, see [Add an LDAP-Authenticated User](#).

Option	Description
First Name	The user's first name.
Last Name	The user's last name.
Type	(If LDAP or SAML are configured) The type of authentication you want to perform on the user: • Tenable (**TNS**) • Lightweight Directory Access Protocol (**LDAP**) • Security Assertion Markup Language (**SAML**) You must configure an LDAP server or SAML authentication in order to select **LDAP** or **SAML** from the **Type** drop-down box.
LDAP Server	The LDAP server you want to use to authenticate the user.
Search String	The LDAP search string you want to use to filter your user search. Use the format: *attribute=<filter text>*. You can use wildcards, and the option accepts up to 1024 characters. **Examples** sAMAccountName=* mail=a* displayName=C*
LDAP Users Found	A filtered list of LDAP user accounts retrieved by the **Search String**. Your selection in this option populates the **Username** option.
The Username for this account must match a user on the LDAP	If the user was created via LDAP user provisioning, the username on the LDAP server associated with the Tenable Security Center user account. If you select a username in the drop-down, Tenable Security Center overwrites the Tenable Security Center user account using information

server in order to authenticate.	from the new LDAP user you selected. By default, this option is blank. You do not need to configure this option to enable user provisioning or automatic synchronization of user data between your LDAP server and Tenable Security Center. For more information, see LDAP User Provisioning.
Username	(Required) The username, populated by your **LDAP Users Found** selection. This username must match a user on the LDAP server in order to authenticate successfully.
Time Zone	(Required) The time zone for the user.
Scan Result Default Timeframe	The default **Completion Time** filter applied when the user accesses or refreshes the scan results page.
Cached Fetching	When enabled, Tenable Security Center caches plugin policy information and performs plugin policy downloads once per page load.
Membership	
Role	(Required) The role assigned to the user. For more information, see User Roles. Administrator users can create **Administrator** or **Security Manager** user accounts. Organizational users can create **Auditor**, **Credential Manager**, **Executive**, **No Role**, **Security Analyst**, **Security Manager**, or **Vulnerability Analyst** accounts at their own privilege level or lower. For example: • If a user is an Auditor, they can create new Auditors or lesser roles. • If a custom user has the Create Policies privilege but not the Update Feeds privilege, that user can create users with the Create Policies privilege, but not the Update Feeds privilege.
Organization	(Required) The organization where you want to assign the user account.
Group	(Required) The group where you want to assign the user account. A user's group determines their access to Tenable Security Center resources. For

	more information about groups, see [Groups](#). To grant a user limited privileges to other groups' resources, see [Custom Group Permissions](#).
Group Permissions	
Manage All Users	When enabled, allows the user to manage users in all of the user's assigned groups. For more information, see [Custom Group Permissions](#).
Manage All Objects	When enabled, allows the user to manage objects in all of the user's assigned groups. For more information, see [Custom Group Permissions](#).
Responsibility	
Asset	Assigns a user to an asset list for which the user is responsible. Assigning a user to an asset list makes it easier to determine who in a group or organization should be assigned tickets, notifications, and other tasks to resolve particular issues. Selecting an asset updates the User Responsibility Summary in the [Vulnerability Analysis](#) section.
Display Options	
Dark Mode	When enabled, sets the Tenable Security Center user interface to dark mode for the user.
Contact Information	
Title	
Address	
City	
State	The contact information for the user.
Country	
Email	
Phone	

SAML User Account Options

You must configure SAML authentication to add SAML-authenticated users. For more information, see SAML Authentication.

To add a SAML-authenticated user, see Add a SAML-Authenticated User.

Option	Description
First Name	The user's first name.
Last Name	The user's last name.
Type	(If LDAP or SAML are configured) The type of authentication you want to perform on the user: • Tenable (**TNS**) • Lightweight Directory Access Protocol (**LDAP**) • Security Assertion Markup Language (**SAML**) You must configure an LDAP server or SAML authentication in order to select **LDAP** or **SAML** from the **Type** drop-down box.
Username	(Required) The user's SAML username. Type the username exactly as it appears in your identity provider SAML configuration for this user.
Time Zone	(Required) The time zone for the user.
Scan Result Default Timeframe	The default **Completion Time** filter applied when the user accesses or refreshes the scan results page.
Cached Fetching	When enabled, Tenable Security Center caches plugin policy information and performs plugin policy downloads once per page load.
Membership	
Role	(Required) The role assigned to the user. For more information, see User Roles. Administrator users can create **Administrator** or **Security Manager** user accounts. Organizational users can create **Auditor**, **Credential Manager**, **Executive**, **No Role**, **Security Analyst**, **Security Manager**, or **Vulnerability**

	Analyst accounts at their own privilege level or lower. For example: • If a user is an Auditor, they can create new Auditors or lesser roles. • If a custom user has the Create Policies privilege but not the Update Feeds privilege, that user can create users with the Create Policies privilege, but not the Update Feeds privilege.
Organization	(Required) The organization where you want to assign the user account.
Group	(Required) The group where you want to assign the user account. A user's group determines their access to Tenable Security Center resources. For more information about groups, see Groups. To grant a user limited privileges to other groups' resources, see Custom Group Permissions.
Group Permissions	
Manage All Users	When enabled, allows the user to manage users in all of the user's assigned groups. For more information, see Custom Group Permissions.
Manage All Objects	When enabled, allows the user to manage objects in all of the user's assigned groups. For more information, see Custom Group Permissions.
Responsibility	
Asset	Assigns a user to an asset list for which the user is responsible. Assigning a user to an asset list makes it easier to determine who in a group or organization should be assigned tickets, notifications, and other tasks to resolve particular issues. Selecting an asset updates the User Responsibility Summary in the Vulnerability Analysis section.
Display Options	
Dark Mode	When enabled, sets the Tenable Security Center user interface to dark mode for the user.
Contact Information	

Title	
Address	
City	
State	The contact information for the user.
Country	
Email	
Phone	

LDAP Authentication

Adding LDAP servers allows you to use one or more external LDAP servers for Tenable Security Center user account authentication. LDAP authentication enhances the security of Tenable Security Center by inheriting password complexity requirements from environments mandated by security policy.

> **Note:** Tenable Security Center does not support SHA1 certificates for connecting to LDAP servers. Tenable Security Center uses OpenSSL3, which requires SHA256 certificates for authentication.

After you configure an LDAP server, create Tenable Security Center user accounts for each LDAP user you want to grant access.

- To manually add LDAP-authenticated users in Tenable Security Center, see Add an LDAP-Authenticated User.

- To automatically add LDAP-authenticated users by importing users from your LDAP identity provider, see LDAP User Provisioning.

Then, users with LDAP-authenticated accounts can log in to Tenable Security Center using the **Sign In Using Identity Provider** button, as described in Log In to the Web Interface.

You can also use configured LDAP servers as LDAP query assets. For more information, see Assets.

> **Note:** Tenable Security Center does not support Microsoft Active Directory Lightweight Directory Services (AD LDS) servers for LDAP authentication.

Note: Tenable Security Center cannot retrieve more than one page of LDAP results. If Tenable Security Center asset list or user authentication queries are not retrieving all expected results, consider modifying your LDAP pagination control settings to increase the results per page.

For more information, see [Add an LDAP Server](#) and [Delete an LDAP Server](#).

LDAP Authentication Options

Configure the LDAP settings as directed by your LDAP server administrator. Click **Test LDAP Settings** to validate the connection.

Option	Description
Server Settings	
Name	(Required) A unique name for the LDAP server.
Description	A description for the LDAP server.
Hostname	(Required) The IP address or DNS name of the LDAP server.
Port	(Required) The remote LDAP port. Confirm the selection with your LDAP server administrators. • When **Encryption** is **None**, **Port** is typically **389**. • When **Encryption** is **TLS** or **LDAPS**, **Port** is typically **636**.
Encryption	If the LDAP server encrypts communications, the encryption method: Transport Layer Security (STARTTLS) or LDAP over SSL (LDAPS).
Username / Password	(Required) The username and password for an account on the LDAP server with credentials to search for user data. For example, Active Directory servers require an authenticated search. Format the username as provided by the LDAP server. **Tip:** It is recommended to use passwords that meet stringent length and complexity requirements.
User Provisioning	You can enable user provisioning to automatically create LDAP-authenticated users in Tenable Security Center by importing user

Option	Description

	accounts from your LDAP identity provider. When user provisioning is enabled, users who log in to your LDAP identity provider are automatically created in Tenable Security Center.
	
	Tenable Security Center supports the following LDAP authentication systems for user provisioning:
	
	    • Active Directory on Microsoft Server 2016 (on-premises)
	
	    • Active Directory on Microsoft Server 2019 (on-premises)
	
	For more information, see LDAP User Provisioning.
	
	Note: If you want to delete a Tenable Security Center user that was created via LDAP user provisioning, delete the user from your LDAP identity provider. If you delete a user in Tenable Security Center that was created via LDAP user provisioning without deleting the user in your LDAP identity provider, Tenable Security Center automatically re-creates the user in Tenable Security Center the next time they log in using your LDAP identity provider.

User Data Sync	If you enable **User Provisioning**, you can enable **User Data Sync** to allow Tenable Security Center to automatically synchronize contact information (first name, last name, email address, and phone number) from your LDAP identity provider for Tenable Security Center users created via LDAP user provisioning. For more information, see LDAP User Provisioning. **Note:** If you want to edit a Tenable Security Center user that was created via LDAP user provisioning and you enabled **User Data Sync**, edit the user in your LDAP identity provider. Otherwise, the Tenable Security Center user data synchronization overwrites your changes the next time the user logs in to Tenable Security Center using your LDAP identity provider.
LDAP Schema Settings	
Base DN	(Required) The LDAP search base used as the starting point to search for the user data.

Option	Description
User Object Filter	The string you want to use to create a search based on a location or filter other than the default search base or attribute.
User Schema Settings (Optional, if you plan to use the LDAP server only as an LDAP query asset.)	
Username Attribute	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 LDAP server administrator for the correct value.
E-mail Attribute	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 LDAP server administrator for the correct value.
Phone Attribute	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 LDAP server administrator for the correct value.
Name Attribute	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 LDAP administrator for the correct value.
Access Settings	
Organizations	The Tenable Security Center organizations you want to authenticate using this LDAP server.
Advanced Settings	
Lowercase	When enabled, Tenable Security Center modifies the usernames sent by the LDAP server to use only lowercase characters. Tenable recommends keeping this option disabled.

Option	Description
DNS Field	The LDAP server parameter used in LDAP server requests to filter the returned asset data. Tenable recommends using the default value provided by Tenable Security Center.
Time Limit	The number of seconds you want Tenable Security Center to wait for search results from the LDAP server. Tenable recommends using the default value provided by Tenable Security Center.

> **Note:** 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.

Add an LDAP Server

> **Required Tenable Security Center User Role:** Administrator

For more information about LDAP server options, see LDAP Authentication.

To add an LDAP server connection:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Resources** > **LDAP Servers**.

3. Click **Add**.

4. Configure the following settings as described in the Options table:

   • **Server Settings**

   • **LDAP Schema Settings**

- **User Schema Settings**

- **Access Settings**

5. If necessary, modify the default **Advanced Settings**.

6. Click **Test LDAP Settings** to validate the LDAP server connection.

7. Click **Submit**.

What to do next:

- Add LDAP-authenticated user accounts.

    - To manually add LDAP-authenticated users in Tenable Security Center, see Add an LDAP-Authenticated User.

    - To automatically add LDAP-authenticated users by importing users from your LDAP identity provider, see Configure LDAP User Provisioning.

LDAP User Provisioning

You can enable user provisioning to automatically create LDAP-authenticated users in Tenable Security Center by importing user accounts from your LDAP identity provider. When user provisioning is enabled, users who log in to your LDAP identity provider are automatically created in Tenable Security Center.

Tenable Security Center supports the following LDAP authentication systems for user provisioning:

- Active Directory on Microsoft Server 2016 (on-premises)

- Active Directory on Microsoft Server 2019 (on-premises)

For more information about LDAP authentication in Tenable Security Center, see LDAP Authentication.

If you enable user provisioning and a user who does not have a Tenable Security Center user account logs in using your LDAP identity provider, Tenable Security Center automatically creates a user account for them in Tenable Security Center.

Tenable Security Center creates users using data from attribute fields you map to the corresponding fields in your LDAP identity provider. If you enable **User Data Sync** for an LDAP server, each time a user logs into Tenable Security Center using your LDAP identity provider,

Tenable Security Center updates any mapped attribute fields in Tenable Security Center with values from the fields in your LDAP identity provider. For more information about **User Data Sync**, see [LDAP Authentication Options](#).

> **Note:** If you want to edit a Tenable Security Center user that was created via LDAP user provisioning and you enabled **User Data Sync**, edit the user in your LDAP identity provider. Otherwise, the Tenable Security Center user data synchronization overwrites your changes the next time the user logs in to Tenable Security Center using your LDAP identity provider.

> **Note:** If you want to delete a Tenable Security Center user that was created via LDAP user provisioning, delete the user from your LDAP identity provider. If you delete a user in Tenable Security Center that was created via LDAP user provisioning without deleting the user in your LDAP identity provider, Tenable Security Center automatically re-creates the user in Tenable Security Center the next time they log in using your LDAP identity provider.

For more information, see [Configure LDAP User Provisioning](#).

Configure LDAP User Provisioning

> **Required Tenable Security Center User Role:** Administrator

You can enable user provisioning to automatically create LDAP-authenticated users in Tenable Security Center by importing user accounts from your LDAP identity provider. When user provisioning is enabled, users who log in to your LDAP identity provider are automatically created in Tenable Security Center.

Tenable Security Center supports the following LDAP authentication systems for user provisioning:

- Active Directory on Microsoft Server 2016 (on-premises)

- Active Directory on Microsoft Server 2019 (on-premises)

For more information, see [LDAP User Provisioning](#).

To manually create LDAP-authenticated users in Tenable Security Center, see [Add an LDAP-Authenticated User](#).

For more information about user account configuration options, see [LDAP User Account Options](#).

Before you begin:

1. (Recommended) Create a backup of your user directory in your LDAP identity provider.

2. In Tenable Security Center, add an LDAP server, as described in Add an LDAP Server.

3. In your LDAP identity provider, create the following custom user attributes: tenableRoleID, tenableGroupID, and tenableOrgID.

4. In your LDAP identity provider, specify the role, group, and organization you want to assign the user in Tenable Security Center:

   a. In the tenableRoleID attribute field, type the ID for the Tenable Security Center role you want to assign to the user. To locate the ID for a role, see View User Role Details.

   b. In the tenableGroupID attribute field, type the ID for the Tenable Security Center group you want to assign to the user. To locate the ID for a group, see View Group Details.

   c. In the tenableOrgID attribute field, type the ID for the Tenable Security Center organization you want to assign to the user. To locate the ID for an organization, see View Organization Details.

To enable LDAP user provisioning for an LDAP server:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Resources** > **LDAP Servers**.

   The **LDAP Servers** page appears.

3. Right-click the row for the LDAP server where you want to enable user provisioning.

   The actions menu appears.

   -or-

   Select the check box for the LDAP server where you want to enable user provisioning.

   The available actions appear at the top of the table.

4. Click **Edit**.

   The **Edit LDAP Server** page appears.

5. In the **Server Settings** section, click the toggle to enable **User Provisioning**.

6. (Optional) To automatically update contact information (first name, last name, email address, and phone number) for users created via LDAP user provisioning, click the **User Data Sync** toggle. For more information about **User Data Sync**, see LDAP Authentication Options.

7. (Optional) In the **User Schema Settings** section, type the names of the attributes in your LDAP identity provider you want to use to populate the **Username**, **Email**, **Phone**, **First Name**, and **Last Name** for users created via LDAP user provisioning. For more information about user account options, see LDAP User Account Options.

> **Note:** If you enable **User Data Sync** and configure the options in the **User Schema Settings** section, Tenable Security Center automatically updates the attributes in the **User Schema Settings** section with values from your LDAP identity provider. For more information, see LDAP Authentication Options.

8. Click **Submit**.

Tenable Security Center saves your configuration.

Delete an LDAP Server

> **Required Tenable Security Center User Role:** Administrator

For more information, see LDAP Authentication.

To delete an LDAP server connection:

> **Note:** If you delete a connection to an LDAP server, the users associated with that server cannot log in to Tenable Security Center. Tenable recommends reconfiguring associated user accounts before deleting LDAP server connections.

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **LDAP Servers**.

3. Select the server connection you want to delete:

   To delete a single server connection:

   a. In the table, right-click the row for the server connection you want to delete.

      The actions menu appears.

b. Click **Delete**.

To delete multiple server connections:

a. In the table, select the check box for each server connection you want to delete.

The available actions appear at the top of the table.

b. At the top of the table, click **Delete**.

A confirmation window appears.

4. Click **Delete**.

Tenable Security Center deletes the LDAP server.

LDAP Servers with Multiple OUs

Tenable's Tenable Security Center LDAP configuration does not support the direct addition of multiple Organizational Units (OUs) in the LDAP configuration page. Two deployment options are possible for those with multiple OUs.

For general information about LDAP Servers, see LDAP Authentication.

Option 1 (Recommended)

When you complete these changes, new users who are members of this group can log in immediately. No restart is required.

Before you begin:

- In LDAP, add a new group for Tenable Security Center users.

- In LDAP, allow existing Active Directory users to become members of the new group.

To configure LDAP with multiple OUs (Option 1):

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **LDAP Servers**.

3. Add the LDAP server, as described in Add an LDAP Server.

> **Note:** Use the Distinguished Name (DN) of the new group as the **Search Base** (e.g., *CN=Tenablesc,DC=target,DC=example,DC=com*).

4. Log out of Tenable Security Center.

5. Log in to Tenable Security Center as the organizational user you want to manage the users.

6. Create a user account for each Active Directory user in the new group, as described in Add an LDAP-Authenticated User.

   In the **Search String** box, type **=***.

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. As another example, you might use this search string, when used in the configuration, applies to all LDAP searches:

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

> **Note:** This option is limited to 128 characters.

To configure LDAP with multiple OUs (Option 2):

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **LDAP Servers**.

3. Begin configuring the LDAP server, as described in Add an LDAP Server.

4. Click **Test LDAP Settings** to test configurations.

5. Log out of Tenable Security Center.

6. Log in to Tenable Security Center as the organizational user you want to manage the users.

7. Create a user account for each Active Directory user, as described in Add an LDAP-Authenticated User.

   In the **Search String** box, type **=***.

SAML Authentication

You can configure SAML authentication so that Tenable Security Center users can use identity provider-initiated single sign-on (SSO) when logging in to Tenable Security Center. Tenable Security Center supports SAML 2.0-based authentication (for example, Okta, OneLogin, Microsoft ADFS, or Shibboleth 2.0).

For more information, see:

- Tenable SAML Configuration Quick-Reference Guide

- Configure SAML Authentication Automatically via the User Interface

- Configure SAML Authentication Manually via the User Interface

- Configure SAML Authentication via the SimpleSAML Module

After you configure SAML authentication, create Tenable Security Center user accounts for each SAML user you want to grant access.

- To manually add SAML-authenticated users in Tenable Security Center, see Add a SAML-Authenticated User.

- To automatically add SAML-authenticated users by importing users from your SAML identity provider, see SAML User Provisioning.

Then, users with SAML-authenticated accounts can log in to Tenable Security Center using the **Sign In Using Identity Provider** button, as described in Log In to the Web Interface.

Considerations for Advanced SAML Features

Because Tenable Security Center cannot accept private keys to decrypt SAML assertions, Tenable Security Center does not support SAML assertion encryption. If you want to configure SAML authentication in Tenable Security Center, choose an identity provider that does not require assertion encryption and confirm that assertion encryption is not enabled.

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

> **Note:** Tenable Support does not assist with configuring or troubleshooting advanced SAML features.

SAML Authentication Options

Option	Description
SAML	Specifies whether SAML authentication is enabled or disabled. If you disable SAML, the system clears your SAML configuration settings and prevents SAML-authenticated user accounts from accessing Tenable Security Center.
Source	Specifies your SAML configuration method: • **Import** — Configure SAML authentication by uploading the metadata file provided by your identity provider, as described in Configure SAML Authentication Automatically via the User Interface. • **Entry** — Configure SAML authentication by manually configuring SAML options using data from the metadata file provided by your identity provider, as described in Configure SAML Authentication Manually via the User Interface.
Type	Specifies the identity provider you are using: **SAML 2.0** (e.g., Okta, OneLogin, Shibboleth 2.0, etc.).
Entity ID	The name of the Entity ID attribute. Type the attribute exactly as it appears in your identity provider SAML configuration. The Entity ID must be in URL format. **Tip:** This is the **Federation Service Identifier** value in Microsoft ADFS.
Identity Provider (IdP)	The identity provider identifier string. For example: • The **Identity Provider Issuer** value in Okta. • The **Federation Service Identifier** value in Microsoft ADFS.
Username Attribute	The name of the SAML username attribute. Type the attribute exactly as it appears in your identity provider SAML configuration. For example, if your SAML username attribute is **NameID**, specify **NameID** to instruct Tenable Security Center to recognize users who match the

Option	Description
	format `NameID=username`.
Single Sign-on Service	The identity provider URL where users log in via single sign-on. Type the URL exactly as it appears in your identity provider SAML metadata.
Single Logout Service	The identity provider URL where users log out. Type the URL exactly as it appears in your identity provider SAML metadata.
Certificate Data	The text of the identity provider's X.509 SSL certificate, without the `===BEGIN CERT===` and the `===END CERT===` strings.
User Provisioning	You can enable user provisioning to automatically create SAML-authenticated users in Tenable Security Center by importing user accounts from your SAML identity provider. When user provisioning is enabled, users who log into your SAML identity provider are automatically created in Tenable Security Center. For more information, see SAML User Provisioning. **Note:** If you want to delete a Tenable Security Center user that was created via SAML user provisioning, delete the user from your SAML identity provider. If you delete a user in Tenable Security Center that was created via SAML user provisioning without deleting the user in your SAML identity provider, Tenable Security Center automatically re-creates the user in Tenable Security Center the next time they log in using your SAML identity provider.
User Data Sync	If you enabled **User Provisioning**, you can enable **User Data Sync** to allow Tenable Security Center to automatically synchronize contact information from your SAML identity provider for Tenable Security Center users created via SAML user provisioning. For more information, see SAML User Provisioning. **Note:** If you want to edit a Tenable Security Center user that was created via SAML user provisioning and you enabled **User Data Sync**, edit the user in your SAML identity provider. Otherwise, the Tenable Security Center user data sync overwrites your changes the next time the user logs in to Tenable Security Center using your SAML identity provider.

Option	Description
	Note: Tenable Security Center does not update required fields (**Organization ID**, **Group ID**, and **Role ID**). To change the organization, group, or role for a user created via SAML user provisioning, see Manage User Accounts.

Configure SAML Authentication Automatically via the User Interface

Required Tenable Security Center User Role: Administrator

You can use this method to configure most types of SAML authentication via the Tenable Security Center user interface. If you encounter issues with this method (for example, when configuring Microsoft ADFS), try the module method described in Configure SAML Authentication via the SimpleSAML Module.

For more information about SAML authentication and SAML authentication options, see SAML Authentication.

Before you begin:

- Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center.

- Save your identity provider SAML metadata file to a directory on your local computer.

To automatically configure SAML authentication for Tenable Security Center users:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **SAML** button.

   The **SAML Configuration** page appears.

4. In the **General** section, confirm the **SAML** toggle is enabled.

   If you want to disable SAML authentication for Tenable Security Center users, click the toggle.

5. In the **Source** drop-down box, select **Import**.

The page updates to display additional options.

6. In the **Type** drop-down box, select **SAML 2.0** (e.g., Okta, OneLogin, Shibboleth 2.0, etc.).

7. Click **Choose File** and browse to the SAML metadata file from your identity provider.

> **Note:** The metadata file must match the **Type** you selected. If Tenable Security Center rejects the file, contact your identity provider for assistance.

8. Click **Submit**.

Tenable Security Center saves your configuration.

What to do next:

- Click **Download SAML Configuration XML**, save the `.xml` file locally, and use it to configure your identity provider SAML configuration. For more information, see SAML Authentication XML Configuration Examples.

- Add SAML-authenticated user accounts.

    - To manually add SAML-authenticated users in Tenable Security Center, see Add a SAML-Authenticated User.

    - To automatically add SAML-authenticated users by importing users from your SAML identity provider, see Configure SAML User Provisioning.

- Instruct users to log in to Tenable Security Center using the **Sign In Using Identity Provider** button, as described in Log In to the Web Interface.

Configure SAML Authentication Manually via the User Interface

> **Required Tenable Security Center User Role:** Administrator

You can use this method to configure most types of SAML authentication via the Tenable Security Center interface. However, you may prefer a more streamlined method:

- To configure SAML Authentication automatically, use the method described in Configure SAML Authentication Automatically via the User Interface.

- If you encounter issues with either method (for example, when configuring Microsoft ADFS),

try the module method described in [Configure SAML Authentication via the SimpleSAML Module](#).

For more information about SAML authentication and SAML authentication options, see [SAML Authentication](#).

Before you begin:

- Review the [Tenable SAML Configuration Quick-Reference](#) guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center.

- Save your identity provider SAML metadata file to a directory on your local computer.

To configure SAML authentication for Tenable Security Center users:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **SAML** button.

   The **SAML Configuration** page appears.

4. In the **General** section, confirm the **SAML** toggle is enabled.

   If you want to disable SAML authentication for Tenable Security Center users, click the toggle.

5. In the **Source** drop-down box, select **Entry**.

   The page updates to display additional options.

6. In the **SAML Settings** section, configure the options:

   a. In the **Type** drop-down box, select **SAML 2.0** (e.g., Okta, OneLogin, Shibboleth 2.0, etc.).

   b. In the **Entity ID** box, type the name of the Entity ID attribute exactly as it appears in your identity provider SAML configuration. The **Entity ID** must be in URL format.

   c. In the **Identity Provider (IdP)** box, type identity provider identifier string.

   d. In the **Username Attribute** box, type the SAML username attribute exactly as it appears in your identity provider SAML configuration. This field is case-sensitive.

e. In the **Single Sign-on Service** box, type the identity provider URL where users log in via single sign-on exactly as it appears in your identity provider SAML metadata.

f. In the **Single Logout Service** box, type the identity provider URL where users log out exactly as it appears in your identity provider SAML metadata.

g. In the **Certificate Data** box, paste the text of the identity provider's X.509 SSL certificate, without the `===BEGIN CERT===` and the `===END CERT===` strings.

7. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

- Click **Download SAML Configuration XML**, save the `.xml` file locally, and use it to configure your identity provider SAML configuration. For more information, see SAML Authentication XML Configuration Examples.

- Add SAML-authenticated user accounts.

  - To manually add SAML-authenticated users in Tenable Security Center, see Add a SAML-Authenticated User.

  - To automatically add SAML-authenticated users by importing users from your SAML identity provider, see Configure SAML User Provisioning.

- Instruct users to log in to Tenable Security Center using the **Sign In Using Identity Provider** button, as described in Log In to the Web Interface.

Configure SAML Authentication via the SimpleSAML Module

Required Tenable Security Center User Role: Administrator

Note: These instructions are not for general configuration. These steps should be used only by advanced users or for custom configuration. The recommended method for configuring SAML authentication is via the Tenable Security Center interface:

- Configure SAML Authentication Automatically via the User Interface

- Configure SAML Authentication Manually via the User Interface

If you encounter issues configuring SAML via the Tenable Security Center interface, you can use a hidden SimpleSAML module to automatically configure SAML authentication.

For general information, see SAML Authentication.

Before you begin:

- Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center.

- Save your identity provider SAML metadata file to a directory on your local computer.

To configure SAML authentication via the SimpleSAML module:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **SAML** button.

   The **SAML Configuration** page appears.

4. Type placeholder values into all SAML configuration options. You do not need to configure valid values.

5. Click **Submit**.

   Tenable Security Center saves your configuration.

6. Log in to Tenable Security Center via the command line interface (CLI).

7. Navigate to and open the `/opt/sc/support/etc/SimpleSAML/config/authsources.php` file.

8. Copy and paste the following text into the file, between the `),` line and the `);` line:

   ```
   // This is a authentication source which handles admin authentication.
   'admin' => array(
   // The default is to use core:AdminPassword, but it can be replaced with
   // any authentication source.
   ```

```
'core:AdminPassword',
),
```

9. Save the file.

10. In a browser, navigate to **https://<Tenable Security Center IP address or hostname>/saml/module.php/core/frontpage_config.php**.

    The **SimpleSAML.php installation** page appears.

11. On the **Configuration** tab, click **Login as administrator**.

    The **Enter your username and password** page appears.

12. In the **Username** box, type *admin*.

13. In the **Password** box, type *admin*.

14. Click **Login**.

15. On the **Federation** tab, in the **Tools** section, click **XML to SimpleSAML.php metadata converter**.

    The **Metadata parser** page appears.

16. Click **Choose File** and select your identity provider SAML metadata file.

17. Click **Parse**.

    Tenable Security Center validates the identity provider SAML metadata file. If the metadata file is supported, Tenable Security Center populates the XML metadata box with content from your metadata file. If the metadata file is not supported, you cannot use it for SAML authentication in Tenable Security Center.

18. In the **saml20-idp-remote** section, copy the text in the box.

19. Log in to Tenable Security Center via the command line interface (CLI).

20. Navigate to and open the `/opt/sc/support/etc/SimpleSAML/metadata/saml20-idp-remote.php` file (for SAML 2.0 or Shibboleth 2.0).

21. Paste the text into the file, after the `<?php` line.

22. Save the file.

23. Navigate to and open the `/opt/sc/support/etc/SimpleSAML/config/authsources.php` file again.

24. Confirm the **idp** URL in the `authsources.php` file matches the **$metadata** URL in the `saml20-idp-remote.php` or `shib13-idp-remote.php` file:

    Valid `authsources.php` syntax example:

    ```
    'idp' => 'http://www.okta.com/abcdefghijKLmnopQr0s1'
    ```

    Valid `saml20-idp-remote.php` or `shib13-idp-remote.php` syntax example:

    ```
    $metadata['http://www.okta.com/abcdefghijKLmnopQr0s1']
    ```

25. In a browser, navigate to **https://<Tenable Security Center IP address or hostname>/saml/module.php/core/frontpage_config.php**.

    The **SimpleSAML.php installation** page appears.

26. On the **Authentication** tab, click **Test configured authentication sources**.

    The **Test authentication sources** page appears.

27. Click **1**.

    Your identity provider login page appears.

28. Log in to your identity provider.

    The **SAML 2.0 SP Demo Example** page appears. If this page does not appear, the configuration did not succeed.

What to do next:

- In the Tenable Security Center interface, on the **SAML Configuration** page, click **Download SAML Configuration XML**, save the `.xml` file locally, and use it to configure your identity provider SAML configuration. For more information, see SAML Authentication XML Configuration Examples.

- Add SAML-authenticated user accounts.

  - To manually add SAML-authenticated users in Tenable Security Center, see Add a SAML-Authenticated User.

  - To automatically add SAML-authenticated users by importing users from your SAML identity provider, see Configure SAML User Provisioning.

- Instruct users to log in to Tenable Security Center using the **Sign In Using Identity Provider** button, as described in Log In to the Web Interface.

SAML User Provisioning

You can enable user provisioning to automatically create SAML-authenticated users in Tenable Security Center by importing user accounts from your SAML identity provider. When user provisioning is enabled, users who log into your SAML identity provider are automatically created in Tenable Security Center. For more information about SAML authentication in Tenable Security Center, see SAML Authentication.

> **Tip:** Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center.

If you enable user provisioning and a user who does not have a Tenable Security Center user account logs in using your SAML identity provider, Tenable Security Center automatically creates a user account for them in Tenable Security Center.

Tenable Security Center creates users using data from attribute fields you map to the corresponding fields in your SAML identity provider. If you enable **User Data Sync**, each time a user logs into Tenable Security Center using your SAML identity provider, Tenable Security Center updates any mapped attribute fields in Tenable Security Center with values from the fields in your SAML identity provider. For more information about **User Data Sync**, see SAML Authentication Options.

> **Note:** If you want to edit a Tenable Security Center user that was created via SAML user provisioning and you enabled **User Data Sync**, edit the user in your SAML identity provider. Otherwise, the Tenable Security Center user data sync overwrites your changes the next time the user logs in to Tenable Security Center using your SAML identity provider.

> **Note:** If you want to delete a Tenable Security Center user that was created via SAML user provisioning, delete the user from your SAML identity provider. If you delete a user in Tenable Security Center that was

created via SAML user provisioning without deleting the user in your SAML identity provider, Tenable Security Center automatically re-creates the user in Tenable Security Center the next time they log in using your SAML identity provider.

For more information, Configure SAML User Provisioning.

Configure SAML User Provisioning

Required Tenable Security Center User Role: Administrator

You can enable user provisioning to automatically create SAML-authenticated users in Tenable Security Center by importing user accounts from your SAML identity provider. When user provisioning is enabled, users who log into your SAML identity provider are automatically created in Tenable Security Center. For more information, see SAML User Provisioning.

To manually create SAML-authenticated users in Tenable Security Center, see Add a SAML-Authenticated User.

For more information about user account configuration options, see SAML User Account Options.

Before you begin:

- Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center.

- Configure SAML authentication, as described in Configure SAML Authentication Manually via the User Interface.

To import SAML-authenticated user accounts from your SAML identity provider:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **SAML** button.

   The **SAML Configuration** page appears.

4. In the **SAML Settings** section, click the toggle to enable **User Provisioning**.

5. (Optional) To automatically update contact information for imported SAML-authenticated users, click the **User Data Sync** toggle. For more information about **User Data Sync**, see SAML Authentication Options.

6. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

- In your SAML identity provider, map the required Tenable Security Center user attribute fields to the corresponding fields for users in your identity provider: **Organization ID**, **Group ID**, and **Role ID**.

  > **Note:** Tenable Security Center uses the fields listed in the **Attribute Mapping** section to create and update users in Tenable Security Center. Any Tenable fields that you map to corresponding fields in your SAML identity provider populate when Tenable Security Center imports SAML users into Tenable Security Center. If you enable **User Data Sync**, each time a user logs into Tenable Security Center using your SAML identity provider, Tenable Security Center updates any mapped attribute fields in Tenable Security Center with values from the corresponding fields in your SAML identity provider.

SAML Authentication XML Configuration Examples

> **Tip:** Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Security Center.

Identity provider SAML configurations vary widely, but you can use the following examples to guide your SAML-side configurations.

- OneLogin Example

- Okta Example

- Microsoft ADFS Example

OneLogin Example

In the OneLogin SAML configuration, paste data from your `.xml` download file.

OneLogin Field	Description
Relay State	Leave this field blank.
Audience	Type `https://tenable.sc`.
Recipient	Type `https://<Tenable Security Center host>/saml/module.php/saml/sp/saml2-acs.php/1`, where `<Tenable Security Center host>` is the IP address or hostname for Tenable Security Center.
ACS (Consumer) URL Validatior	Type `-*`.
ACS (Consumer) URL	Type `https://<Tenable Security Center host>/saml/module.php/saml/sp/saml2-acs.php/1`, where `<Tenable Security Center host>` is the IP address or hostname for Tenable Security Center.
Single Logout URL	Type `https://<Tenable Security Center host>/saml/module.php/saml/index.php?sls`, where `<Tenable Security Center host>` is the IP address or hostname for Tenable Security Center.

Okta Example

In the Okta SAML configuration, paste data from your `.xml` download file.

Okta Field	Description
General	
Single Sign On URL	Type `https://<Tenable Security Center host>/saml/module.php/saml/sp/saml2-acs.php/1`, where `<Tenable Security Center host>` is the IP address or hostname for Tenable Security Center.
Recipient URL	Type `https://<Tenable Security Center host>/saml/module.php/saml/sp/saml2-acs.php/1`, where `<Tenable Security Center host>` is the IP address or

Okta Field	Description
	hostname for Tenable Security Center.
Destination URL	Type `https://<Tenable Security Center host>/saml/module.php/saml/sp/saml2-acs.php/1`, where `<Tenable Security Center host>` is the IP address or hostname for Tenable Security Center.
Audience Restriction	Type `https://tenable.sc`.
Default Relay State	Leave this field blank.
Name ID Format	Set to `Unspecified`.
Response	Set to `Signed`.
Assertion Signature	Set to `Signed`.
Signature Algorithm	Set to `RSA_SHA256`.
Digest Algorithm	Set to `SHA256`.
Assertion Encryption	Set to `Unencrypted`.
SAML Single Logout	Set to `Disabled`.
authnContextClassRef	Set to `PasswordProtectedTransport`.
Honor Force Authentication	Set to `Yes`.
SAML Issuer ID	Type `http://www.okta.com/${org.externalKey}`.
Attribute Statements	
FirstName	Set to **Name Format:** `Unspecified` and **Value:** `user.firstName`.
LastName	Set to **Name Format:** `Unspecified` and **Value:** `user.lastName`.
Email	Set to **Name Format:** `Unspecified` and **Value:** `user.email`.
username	Set to **Name Format:** `Unspecified` and one of the following:

Okta Field	Description
	• **Value:** `user.displayName`, if your Tenable Security Center user account usernames are full names (e.g., Jill Smith). • **Value:** `user.email`, if your Tenable Security Center user account usernames are email addresses (e.g., jsmith@website.com). • **Value:** `user.login`, if your Tenable Security Center user account usernames are name-based text strings (e.g., jsmith).

Microsoft ADFS Example

In the Microsoft ADFS configuration, paste data from your `.xml` download file.

Microsoft ADFS Configuration	Description
Edit Authentication Methods window	
Extranet	Select, at minimum, the **Forms Authentication** check box.
Intranet	Select, at minimum, the **Forms Authentication** check box.
Add Relying Party Trust wizard	
Welcome section	• Select **Claims aware**. • Select **Import data about the relying party from a file**. • Browse to and select the SAML configuration `.xml` file you downloaded from Tenable Security Center. **Note:** If you see a warning that some content was skipped, click **Ok** to continue.
Specify Display Name section	In the **Display Name** box, type your Tenable Security Center FQDN.

Microsoft ADFS Configuration	Description
Configure Certificate section	Browse to and select the encryption certificate you want to use.
Choose Access Control Policy section	Select the **Permit everyone** policy.
Ready to Add Trust section	- On the **Advanced** tab, select **SHA256** or the value dictated by your security policy. - On the **Identifiers** tab, confirm the information is accurate. - On the **Endpoints** tab, confirm the information is accurate.
Finish section	Select the **Configure claims issuance policy for this application** check box.
Edit Claim Issuance Policy window	Add one or more claim rules to specify the ADFS value you want Tenable Security Center to use when authenticating SAML users. For example: **To transform an incoming claim:** 1. In **Incoming claim type**, select **Email address** or **UPN**. 2. In **Outgoing claim type**, select **Name ID**. 3. In **Outgoing name ID format**, select **Transient Identifier**. 4. Select the **Pass through all claim values** check box. **To send LDAP attributes as claim:** 1. In **Attribute store**, select **Active Directory**. 2. In **LDAP Attribute**, select **E-Mail Addresses**. 3. In **Outgoing Claim Type**, select **E-Mail Addresses**. > **Note:** Tenable Support does not assist with claim rules.

Certificate Authentication

> **Note:** Tenable has validated certificate support for Signature Algorithms up to SHA-384 and RSA key sizes of up to 4096 bits.

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. (Optional) If you want to validate client certificates against a certificate revocation list (CRL), configure CRLs or OCSP in Tenable Security Center, as described in Configure a CRL in Tenable Security Center or Configure OCSP Validation in Tenable Security Center.

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.
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.

Configure a CRL in Tenable Security Center

Required Tenable Security Center User Role: Root user

You can enable a certificate revocation list (CRL) in Tenable Security Center to prevent users from authenticating to Tenable Security Center if their certificate matches a revocation in the CRL.

Note: Tenable Support does not assist with CRL creation or configuration in Tenable Security Center.

Before you begin:

- Confirm that you have the `mod_ssl` Apache module installed on Tenable Security Center.

- Back up the `/opt/sc/data/CA/` directory in case you encounter issues and need to restore the current version.

To configure a CRL 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**, as described in SSLVerifyClient.

   b. Set the **SSLVerifyDepth** setting, as described in SSLVerifyDepth.

   c. Save the file.

      Tenable Security Center saves your configuration.

2. Restart Tenable Security Center, as described in Start, Stop, or Restart Tenable Security Center.

   Tenable Security Center restarts.

3. Confirm that your CA root configuration file contains the following parameters:

- `crl_dir`

- `database`

- `crl`

- `clr_extensions`

- `default_crl_days`

For example:

```
...
# Directory and file locations.
dir                = /opt/sc/data/CA
crl_dir            = /opt/sc/support/conf/crl
database            = /opt/sc/support/conf/index.txt
# The root key and root certificate.
private_key        = /opt/sc/support/conf/TenableCA.key
certificate        = /opt/sc/data/CA/TenableCA.crt
# For certificate revocation lists.
crl                = /opt/sc/support/conf/crl/ca.crl
crl_extensions     = crl_ext
default_crl_days   = 30
...
```

4. Save your CA root configuration file as *YourCAname*`.conf` in a subdirectory of `/opt/sc/support/conf/`.

5. Confirm the directories and files referenced in your *YourCAname*`.conf` file are present on Tenable Security Center in a subdirectory of `/opt/sc/support/conf/`.

6. Configure Tenable Security Center to trust your CA, as described in [Trust a Custom CA](#).

   Tenable Security Center processes your CA.

7. In the command line interface (CLI), run the following command to enable the CRL in Tenable Security Center:

```
$ openssl ca -config <CA root configuration file directory> -gencrl -out
<crl parameter value in the YourCAname.conf file>
```

For example:

```
$ openssl ca -config /opt/sc/support/conf/ca-root.conf -gencrl -out
/opt/sc/support/conf/crl/ca.crl
```

Tenable Security Center creates the CRL file.

8. In a text editor, open the **/opt/sc/support/conf/vhostssl.conf** file.

   a. Add the following content at the end of the file:

   ```
   SSLCARevocationCheck <value>
   SSLCARevocationFile "<filepath>"
   ```

   Where *<value>* and *<filepath>* are:

Content	Description
SSLCARevocationCheck *<value>*	
chain	Tenable Security Center checks all certificates in a chain against the CRL.
leaf	Tenable Security Center checks only the end-entity certificate in a chain against the CRL.
SSLCARevocationFile *<filepath>*	
Specifies the file path for the CRL file in Tenable Security Center. For example, /opt/sc/support/conf/crl/ca.crl.	

   b. Save the file.

   Tenable Security Center saves your configuration.

9. In the CLI, run the following command to create a symbolic link for the CRL file:

```
$ ln -s <crl parameter value in the YourCAname.conf file> `openssl crl -
hash -noout -in <crl parameter value in the YourCAname.conf file>`.r0
```

For example:

```
$ ln -s /opt/sc/support/conf/crl/ca.crl `openssl crl -hash -noout -in
/opt/sc/support/conf/crl/ca.crl`.r0
```

> **Caution:** Do not use a single quote character (') instead of a backtick character (`); this command requires the backtick.

Tenable Security Center creates a symbolic link for the CRL file.

10. Restart Tenable Security Center, as described in [Start, Stop, or Restart Tenable Security Center](#).

Tenable Security Center restarts.

Configure OCSP Validation in Tenable Security Center

> **Required Tenable Security Center 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**, as described in [SSLVerifyClient](#).

    b. Set the **SSLVerifyDepth** setting, as described in [SSLVerifyDepth](#).

    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, as described in [Start, Stop, or Restart Tenable Security Center](#).

    Tenable Security Center restarts.

Search

In Tenable Security Center, you can search for vulnerabilities (by CVE ID) and host assets (by IPv4 address) using the search box in the top navigation bar. Click the drop-down to change the category. A list of suggestions appears after you type at least five characters or the first octet of an IPv4 address.

> **Note:** To search for host assets, you must have the **View Host Assets** permission enabled. For more information, see [User Roles](#).

Tenable Security Center saves your search history. To view your search history, click the search box. To delete an item from your search history, click the ✕ icon next to the search term.

To view a search result, press **Enter** or click a suggestion in the drop-down box. The search results page appears, which displays widgets with details about the vulnerability or host asset:

Widget	Description
Vulnerabilities	
Vulnerability Information	A list of solutions for the vulnerability that correspond to the plugins currently visible in the **Tenable Coverage** widget. The top right corner displays the Vulnerability Priority Rating (VPR) for the vulnerability. For more information about VPRs, see CVSS vs. VPR.
VPR Key Drivers	Details about the history and severity of the vulnerability that contribute to the VPR. For more information about VPRs, see CVSS vs. VPR.
Risk Information	Details about the risk associated with the vulnerability, as determined by the National Vulnerability Database (NVD).
Hosts Impacted	A list of assets in your system that are affected by the vulnerability. When you scan your network, any discovered assets that are affected by the vulnerability will appear in this list. If you have a Tenable Security Center+ license, this widget also displays the Asset Exposure Score (AES) and Asset Criticality Rating (ACR) for the assets. Click **More Details** to see the **IP Summary** page, where you can view the list of hosts filtered by the CVE ID.
CPEs	A list of CPE names that are relevant to the vulnerability. Click **More Details** to open a dialog box with the full list of CPEs.
References	A list of links with information relevant to the vulnerability. Click **More Details** to open a dialog box with the full list of references.
Tenable Coverage	A list of Tenable plugins that address the vulnerability. You can sort this list by plugin ID.

Widget	Description
	When you sort plugins or navigate pages in the widget, the **Vulnerability Information** and **Related Links** widgets update to correspond to the visible plugins.
	Click **More Details** to see the **Vulnerability List** page, where you can view the list of plugins filtered by your assets. If none of the assets in your network are affected by the list of plugins, then this page will not display any plugins.
Related Links	A list of links with information relevant to the plugins currently visible in the **Tenable Coverage** widget.
	Click **More Details** to open a dialog box with the full list of related links.
Host Assets	
Repository	The repository associated with the host asset. If the host asset appears in more than one repository, click the drop-down to view the host asset in a different repository.
Host Information	Details about the host asset.
	If you have a Tenable Security Center+ license, this widget also displays the Asset Exposure Score (AES) and Asset Criticality Rating (ACR) for the assets.
	Click **More Details** to open a dialog box with the full list of host details.
Host Vulnerability Severity	A chart that displays a breakdown of vulnerabilities by severity level.
Assets	A list of assets associated with the host.
Findings	A list of vulnerabilities in your system that correspond to the asset. When you scan your network, any vulnerabilities associated with the host asset will appear in this list.
	Click **More Details** to see the **Vulnerability List** page, where you can view the list of vulnerabilities filtered by the host asset.

Certificates and Certificate Authorities in Tenable Security Center

Tenable Security Center includes the following defaults:

- a default Tenable Security Center server certificate (`SecurityCenter.crt`)

- a Tenable Security Center certificate authority (CA), which signs `SecurityCenter.crt`

- a DigiCert High Assurance EV Root CA

However, you may want to upload your own CAs or certificates for advanced configurations or to resolve scanning issues. For more information, see:

- [Tenable Security Center Server Certificates](#)

- [Trust a Custom CA](#)

- [Certificate Authentication](#)

- [Custom Plugin Packages for NASL and CA Certificate Upload](#)

- [Manual Tenable Nessus SSL Certificate Exchange](#)

Tenable Security Center Server Certificates

Tenable Security Center ships with a default Tenable Security Center server certificate and key: `SecurityCenter.crt` and `SecurityCenter.key`. In some cases, you must replace it or regenerate it.

If you replace the server certificate with a self-signed certificate, you may need to upload the CA for your server certificate to Tenable Nessus or your browser.

Problem	Solution
The default certificate for Tenable Security Center is untrusted.	Upload a certificate for theTenable Security Center server, as described in [Upload a Server Certificate for Tenable Security Center](#). If the new server certificate is self-signed, plugin 51192 may report that the Tenable Security Center server certificate is untrusted. To configure Tenable Nessus to trust the server certificate, upload the CA certificate to Tenable Nessus.
Your browser reports	Upload a CA certificate for the Tenable Security Center server

Problem	Solution
that the Tenable Security Center server certificate is untrusted.	certificate to your browser.
Plugin 51192 reports that the Tenable Security Center server certificate expired.	Regenerate the Tenable Security Center server certificate, as described in Regenerate the Tenable Security Center Server Certificate.

Upload a Server Certificate for Tenable Security Center

Required Tenable Security Center User Role: Root user

For information about Tenable Security Center server certificates, see Tenable Security Center Server Certificates.

Note: When uploading a certificate file to Tenable Security Center, you must use a PEM file. The custom certificate email address must not be **SecurityCenter@SecurityCenter** or subsequent upgrades cannot retain the new certificate.

Before you begin:

- Save your new server certificate and key files as `host.crt` and `host.key`.

To upload a server certificate for Tenable Security Center:

1. Log in to Tenable Security Center via the user interface.

2. Back up the existing `SecurityCenter.crt` and `SecurityCenter.key` files located in the `/opt/sc/support/conf` directory.

   For example:

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

3. To rename the `host.crt` and `host.key` files and copy them to the `/opt/sc/support/conf` directory, run:

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

If prompted, type **y** to overwrite the existing files.

4. To confirm the files have the correct permissions (640) and ownership (tns), run:

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

Note: If an intermediate certificate is required, it must also be copied to the system and given the correct permissions (640) and ownership (tns). Additionally, you must remove the # from the line in `/opt/sc/support/conf/vhostssl.conf` that begins with `#SSLCertificateChainFile` to enable the setting. Modify the path and filename to match the uploaded certificate.

If necessary, change the ownership or permissions.

a. To change the ownership, run:

```
# chown tns:tns /opt/sc/support/conf/SecurityCenter.crt\
```

```
# chown tns:tns /opt/sc/support/conf/SecurityCenter.key
```

b. To change the permissions, run:

```
# chmod 640 /opt/sc/support/conf/SecurityCenter.crt
# chmod 640 /opt/sc/support/conf/SecurityCenter.key
```

5. Restart the Tenable Security Center service:

```
# service SecurityCenter restart
```

6. In a browser, log in to the Tenable Security Center user interface as a user with administrator permissions.

7. When prompted, verify the new certificate details.

What to do next:

- If you uploaded a self-signed server certificate and plugin 51192 reports that the CA for your self-signed certificate is untrusted, upload the custom CA certificate to Tenable Nessus.

Regenerate the Tenable Security Center Server Certificate

Required Tenable Security Center User Role: `tns` user

Required Tenable Security Center User Role: Root user

Tenable Security Center ships with a default server certificate that is valid for two years. After the certificate expires, you must regenerate the SSL certificate.

To regenerate the Tenable Security Center SSL certificate:

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 to switch to the **tns** user:

   ```
   su - tns
   ```

3. As the **tns** user, run the following command:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/installSSLCertificate.php
   ```

   (Optional) If you want to suppress the self-signed warning or specify a Common Name, include an optional argument.

Argument	Description
-q	Suppresses the warning: `This script generates a self-signed SSL certificate, which is not recommended for production.`

Argument	Description
-h *<IP|host name>*	Specifies an IP address or hostname that will be used as the Common Name for the certificate.

Tenable Security Center generates a new certificate.

4. Run the following command to exit the `tns` user:

```
exit
```

5. As the root user, run the following command to restart the Tenable Security Center service:

```
# service SecurityCenter restart
```

The service restarts and Tenable Security Center applies the new certificate.

Trust a Custom CA

Required Tenable Security Center 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`.

   Note: If you upload multiple certificates, you must upload each certificate individually in PEM format.

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, as described in [Start, Stop, or Restart Tenable Security Center](#).

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. Administrator users can configure more options than organizational users.

- [Configuration Settings](#)

- [Tenable One Data](#)

- [Diagnostics Settings](#)

- [Job Queue Events](#)

- [System Logs](#)

- [Publishing Sites Settings](#)

- [Keys Settings](#)

- [User Profile Menu Settings](#)

Configuration Settings

The configuration menu includes the following settings:

- [Data Expiration Settings](#)

- [External Schedules Settings](#)

- [Mail Settings](#)

- [Miscellaneous Settings](#)

- [License Settings](#)

- [Plugins/Feed Settings](#)

- [SAML Settings](#)

- [Security Settings](#)

- [Tenable One Settings](#)

Data Expiration Settings

Data expiration determines how long Tenable Security Center retains closed tickets, scan results, and report results.

Option	Description
User Generated Object Lifetime	
Closed Tickets	The number of days you want Tenable Security Center to retain closed tickets. The default value of this option is *365* days.
Scan Results	The number of days you want Tenable Security Center to retain scan results. The default value of this option is *365* days.
Report Results	The number of days you want Tenable Security Center to retain report results. The default value of this option is *365* days.

> **Tip:** You can configure vulnerability data expiration for individual IPv4, IPv6, agent, and universal repositories. For more information, see [IPv4/IPv6 Repositories](#), [Agent Repositories](#), and [Universal Repositories](#).

External Schedules Settings

The Tenable Security Center external schedule settings determine the update schedule for the common tasks of pulling Tenable Network Monitor data, IDS signature updates, and IDS correlation updates.

Option	Description
Tenable Network Monitor	
Pull Interval	This option configures the interval that Tenable Security Center uses to pull results from the attached Tenable Network Monitor instances. The default setting is 1 hour. The timing is based from the start of the

Option	Description
	Tenable Security Center service on the host system.
Tenable Log Correlation Engine	
IDS Signatures	Specifies the frequency to update Tenable Security Center IDS signatures via third-party sources. The schedule appears along with the specified time zone.
Correlation Database	Specifies the frequency to push vulnerability information to the Log Correlation Engine for correlation. The schedule appears along with the specified time zone.
Triggered Agent Scans	
Pull Interval	Specifies how often Tenable Security Center checks the scanner for triggered agent scan results.

You can also configure each of the update schedule times to occur by time in a particular time zone using the **Time Zone** link next to each hour selection.

Mail Settings

The **Mail** option designates SMTP settings for all email-related Tenable Security Center functions. Available options include SMTP host, port, authentication method, encryption, and return address. In addition, you can use the Test SMTP Settings in the upper left corner of the page to validate the settings.

> **Note:** Type the **Username** in a format supported by your SMTP server (for example, *username@domain.com* or *domain\username*).

> **Note:** The **Return Address** defaults to *noreply@localhost*. Use a valid return email address for this option. If this option is empty or the email server requires emails from valid accounts, the email server cannot send the email.

Miscellaneous Settings

The **Miscellaneous Configuration** section offers options to configure settings for web proxy, syslog, notifications, and enable or disable some report types.

Web Proxy

> **Note:** These settings are not available in Tenable Enclave Security.

From this configuration page, you can configure a web proxy by entering the host URL (proxy hostname or IP address), port, authentication type, username, and password. The hostname used must resolve properly from the Tenable Security Center host.

Syslog

> **Note:** These settings are not available in Tenable Enclave Security.

In the **Syslog** section, you can configure options to allow Tenable Security Center to send administrative log events to the local syslog service. For more information about the types of Tenable Security Center logs, see the knowledge base article.

Option	Description
Enable Forwarding	Enables log forwarding options.
Facility	Type the facility you want to receive the log messages.
Severity	Specifies which syslog message levels you want to forward: **Informational**, **Warning**, or **Critical**.

Scanning

The **IP Randomization** option specifies how you want Tenable Security Center to send active scan target lists to Tenable Nessus and Tenable Vulnerability Management scanners.

You enable or disable IP randomization for all configured active scans; you cannot configure IP randomization on a per-scan basis.

- When enabled, Tenable Security Center randomizes the targets in the active scan before sending the target list to the scanners to reduce strain on network devices during large active scans.

Scan	Randomization
1,000 or fewer targets	Tenable Security Center randomizes all the IP addresses in the target list.
1,001 or more targets	Tenable Security Center randomizes all the IP addresses in the target list by: 1. Ordering the IP addresses numerically and splitting them into 100 groups. 2. Randomly selecting a group and choosing the lowest IP address from that group. 3. Selecting groups and IP addresses until all IP addresses in all groups are randomized in the target list.

If the active scan includes a Tenable Vulnerability Management scanner, Tenable Security Center breaks the target list into smaller lists (256 IP addresses each) before sending to Tenable Vulnerability Management.

> **Note:** Some randomized target lists (such as small target lists) may still contain sequences of increasing IP addresses. This is a possible outcome of randomization, not an indication that randomization failed.

- When disabled, Tenable Security Center organizes the target list by increasing IP address. Then, scanners scan targets, starting with the lowest IP address and finishing with the highest IP address.

> **Tip:** The **Max simultaneous hosts per scan** scan policy option specifies how many IP addresses Tenable Security Center sends to each scanner at a time. For more information, see Scan Policy Options.

Notifications

In the **Notifications** section, you can configure options for Tenable Security Center notifications. For more information, see Notifications.

Option	Description
Tenable Security Center Location	Defines the Tenable Security Center web address used when alerts and tickets generate notifications.
Bell Notifications	Enables notifications to appear in the 🔔 menu in the top navigation bar.

Report Generation

> **Note:** These settings are not available in Tenable Enclave Security.

If your organization requires specialized reporting formats, such as DISA or CyberScope, you can enable **Report Generation** options based on your organization's needs.

- Defense Information Systems Agency (DISA) reporting standards include the Assessment Summary Results (ASR), Assessment Results Format (ARF), and Consolidated Assessment Results Format (CARF) styles.

- CyberScope reports utilize Lightweight Asset Summary Results Schema (LASR) style reports, which are used by some segments of governments and industry.

To allow users to choose these reports during report creation, you must enable the corresponding toggles. For more information about reports in Tenable Security Center, see [Reports](#).

Option	Description
Enable DISA ARF	Enable the DISA ARF report format, which meets the standards of the Defense Information Systems Agency Assessment Results Format.
Enable DISA Consolidated ARF	Enable the DISA consolidated ARF report format, which meets the standards of the Defense Information Systems Agency Consolidated Assessment Results Format.
Enable DISA ASR	Enable the DISA ASR report format, which meets the standards of the Defense Information Systems Agency Assessment Summary Results.
Enable CyberScope	Enable the CyberScope report format, which meets CyberScope reporting standards to support FISMA compliance.

Risk Rule Comments

You can enable the **Recast and Accept Risk Rule Comments** option to display accept risk rule comments and recast risk rule comments in reports and vulnerability analysis views.

For more information about recast risk rules and accept risk rules, see Recast Risk Rules and Accept Risk Rules.

For more information about vulnerability analysis views, see View Vulnerability Instance Details and View Vulnerabilities by Plugin.

PostgreSQL Connection

If you have configured an external Postgres database, this section displays the connection information for the database.

Privacy

The **Enable Usage Statistics** option specifies whether Tenable collects anonymous telemetry data about your Tenable Security Center deployment.

When enabled, Tenable collects usage statistics that cannot be attributed to a specific user or customer. Tenable does not collect personal data or personally identifying information (PII).

Usage statistics include, but are not limited to, data about your visited pages, your used reports and dashboards, your Tenable Security Center license, and your configured features. Tenable uses the data to improve your user experience in future Tenable Security Center releases. You can disable this option at any time to stop sharing usage statistics with Tenable.

After you enable or disable this option, all Tenable Security Center users must refresh their browser window for the changes to take effect.

License Settings

> **Note:** These settings are not available in Tenable Enclave Security.

The **License Configuration** section allows you to configure licensing and activation code settings for Tenable Security Center and all attached Tenable products.

For information about the Tenable Security Center license count, see License Requirements. To add or update a license, see Apply a New License or Update an Existing License.

Plugins/Feed Settings

The **Plugins/Feed Configuration** page displays the **Plugin Detail Locale** for Tenable Security Center and the feed and plugin update (scanner update) schedules.

For more information, see Edit Plugin and Feed Settings and Schedules.

Update	Description
Tenable Security Center Feed	Retrieves the latest Tenable Security Center feed from Tenable. This feed includes data for general use, including templates (for example, dashboards, ARCs, reports, policies, assets, and audit files), template-required objects, some general plugin information, and updated VPR values.
Active Plugins	Retrieves the latest active plugins feed (for Tenable Nessus and Tenable Vulnerability Management scanners) from Tenable. Tenable Security Center pushes the feed to Tenable Nessus and Tenable Vulnerability Management scanners.
Passive Plugins	Retrieves the latest passive plugins feed from Tenable. Tenable Security Center pushes the feed to Tenable Network Monitor instances.
Event Plugins	Retrieves the latest event plugins feed from Tenable. Tenable Security Center uses the feed locally with Log Correlation Engine data but does not push the feed to Log Correlation Engine; Log Correlation Engine retrieves the feed directly from Tenable.
WAS Plugins	Retrieves the latest Tenable Web App Scanning plugins feed from Tenable. Tenable Security Center pushes the feed to Tenable Web App Scanning instances.

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

Plugin Detail Locale

The local language plugin feature allows you to display portions of plugin data in local languages. When available, translated text displays on all pages where plugin details appear.

Select **Default** to display plugin data in English.

> **Note:** Tenable Security Center cannot translate text within custom files. Upload a translated **Active Plugins.**xml file to display the file content in a local language.

For more information, see [Configure Plugin Text Translation](#).

Schedules

Tenable Security Center automatically updates Tenable Security Center feeds, active plugins, passive plugins, and event plugins. If you upload a custom feed or plugin file, the system merges the custom file data with the data contained in the associated automatically updating feed or plugin.

You can upload `tar.gz` files with a maximum size of 1500 MB.

For more information, see [Edit Plugin and Feed Settings and Schedules](#).

Security Center Software Updates

The **Security Center Software Updates** section includes options for applying updates and patches for Tenable Security Center.

In the **Authorization Token** box, enter your authorization token. You can generate an authorization token on the [Tenable Downloads API](#) page.

If you enable the **Automatically Update Through the Security Center Feed** option, then Tenable Security Center automatically applies any available Tenable Security Center patches during scheduled feed updates.

> **Note:** Some patches cannot be applied through the feed, and must be installed manually.

Available Software Updates

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

The **Install Now** tab displays available software updates for download. You can install them immediately by selecting the check box and clicking **Install Now**. If you enable the **Automatically Update Through the Security Center Feed** option in the **Security Center Software Updates**

section, then Tenable Security Center will automatically apply these updates and patches during scheduled feed updates.

The **Install Manually** tab includes software updates that must be installed manually. You can download the files for these updates and patches from the [Tenable Downloads](#) page.

If you install a software update but the installation fails, the update will appear in the **Available Software Updates** section with a warning icon. Click the software update in the table to view details about the error.

Installed Software Updates

When you install a software update, it moves from the **Available Software Updates** section to the **Installed Software Updates** section. If a software update requires a restart to finish installing, the status for the update in the **Installed Software Updates** section will be **Needs Restart**. After you complete a software update, the status for the update will be **Installed**.

SAML Settings

Use the SAML section to configure SAML 2.0-based SAML authentication (for example, Okta, OneLogin, Shibboleth 2.0, etc.) for Tenable Security Center users. For more information, see [SAML Authentication](#).

Security Settings

Use the Security section to define the Tenable Security Center user interface login parameters and options for account logins. You can also configure banners, headers, and classification headers and footers.

Option	Description
Authentication Settings	
Session Timeout	The web session timeout in minutes (default: *60*).
Maximum Login Attempts	The maximum number of user login attempts Tenable Security Center allows before locking out the account (default: *20*). To disable this feature, set the value to *0*.

Option	Description
Minimum Password Length	This setting defines the minimum number of characters for passwords of accounts created using the local TNS authentication access (default: 3).
Password Complexity	When enabled, user passwords must be at least 4 characters long and contain at least one of each of the following: • An uppercase letter • A lowercase letter • A numerical character • A special character **Note:** After you enable **Password Complexity**, Tenable Security Center prompts all users to reset their passwords the next time they log in to Tenable Security Center. **Note:** If you enable **Password Complexity** and set the **Minimum Password Length** to a value greater than 4, Tenable Security Center enforces the longer password requirement.
Startup Banner Text	Type the text banner that appears before to the login interface.
User Text	Adds custom text to the bottom of the user profile menu. You can use the text to identify a company, group, or other organizational information (maximum 128 characters).
Classification Type	Adds a header and footer banner to Tenable Security Center to indicate the classification of the data accessible via the software. Current options are **None**, **Custom, Unclassified**, **Confidential**, **Secret**, **Top Secret**, and **Top Secret – No Foreign**. If you select **Custom**, the following options appear: • **Custom Text** - Type the text that you want to appear in the banner (maximum 128 characters).

Option	Description
	• **Text Color** - Select the text color for the banner.
	• **Background Color** - Select the background color for the banner.
	Note: Custom banners in reports are supported only for Arial Regular font.
	Sample header:
	Sample footer:
	Note: If you set **Classification Type** to an option other than **None**, users can only see the plain report styles. The Tenable report styles do not support the classification banners.
Allow API Keys	When enabled, allows users to generate API keys as an authentication method for Tenable Security Center API requests. For more information, see Enable API Key Authentication.
Allow Session Management	This setting is disabled by default. When enabled, the **Session Limit** option appears. This feature displays the option that allows administrators to set a session limit for all users.
Disable Inactive Users	When enabled, Tenable Security Center disables user accounts after a set period of inactivity. You cannot use a disabled user account to log in to Tenable Security Center, but other users can use and manage objects owned by the disabled user account.
Days Users Remain Enabled	When you enable **Disable Inactive Users**, specify the number of inactive days you want to allow before automatically disabling a user
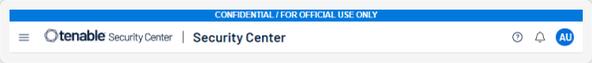
Option	Description
	account.
Session Limit	Specifies the maximum number of sessions a user can have open at once. If you log in and the session limit has already been reached, Tenable Security Center notifies you that the oldest session with that username will be logged out automatically. You can cancel the login or proceed with the login and end the oldest session. **Note:** This behavior is different for Common Access Cards (CAC) logins. Tenable Security Center does not check active sessions for CAC authentication.
Login Notifications	Sends notifications for each time a user logs in.
WebSeal	Allows you to enable or disable WebSEAL. WebSEAL supports multiple authentication methods, provides Security Access Authorization service, and single sign-on capabilities. **Caution:** Before the user that enabled WebSEAL logs out of Tenable Security Center, Tenable Security Center strongly recommends confirming, in a separate session, that at least one user (preferably an administrator user) is able to log in successfully via WebSEAL. Otherwise, if there is an issue, no one will be able to access Tenable Security Center to turn off WebSEAL. **Caution:** Any user created while WebSEAL is enabled will not have a password. An administrator must update the user account to establish a password. Any user that existed before enabling WebSEAL must revert to their old password.
PHP Serialization	
Operational Status	Summarizes your current setting.
PHP Serialization Mode	Specifies whether you want to allow or prevent PHP serialization in Tenable Security Center.

Option	Description

	• **PHP Serialization ON** — Tenable Security Center performs PHP serialization and Tenable Security Center features operate as expected.
	
	• **PHP Serialization OFF** — Tenable Security Center does not perform PHP serialization and prevents users from importing or exporting the following objects:
	
	    • Assets
	    • Scan policies
	    • Assurance Report Cards
	    • Reports
	    • Audit files
	    • Dashboards

Scanners	
Picture in Picture	When enabled, allows administrators to view and manage Tenable Nessus scanner configurations from the Tenable Security Center user interface. For more information, see Enable Picture in Picture. **Note:** You cannot use **Picture in Picture** with a Tenable Nessus scanner if you enabled **Use Proxy** for the scanner or if the scanner's **Authentication Type** is **SSL Certificate**. For more information, see Tenable Nessus Scanner Settings.
FIPS 140-2 Configuration	
Operational Status	Summarizes whether FIPS 140-2 mode is currently enabled or disabled.
FIPS 140-2 Mode	Specifies whether you want to enable or disable FIPS mode for communication. Switching from one mode to the other requires a restart. For more information, see Start, Stop, or Restart Tenable Security Center.

Tenable Lumin Settings

If you have a Tenable Vulnerability Management license to use Tenable Lumin with Tenable Security Center, you can configure your Tenable Security Center data to synchronize to Tenable Vulnerability Management for Tenable Lumin analysis.

For more information, see Tenable One Synchronization.

Edit Plugin and Feed Settings and Schedules

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Configuration Settings.

To view and edit plugin and feed settings and schedules as an administrator user:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **Plugins/Feed** tile.

   The **Plugins/Feed Configuration** page appears.

4. View the **Plugin Detail Locale** section to see the local language configured for Tenable Security Center.

5. Expand the **Schedules** section to show the settings for the **Tenable Security Center Feed**, **Active Plugins**, **Passive Plugins**, or **Event Plugins** schedule.

   a. If you want to update a plugin or feed on demand, click **Update**. You cannot update feeds with invalid activation codes.

      • If there is an update available, the **Update** link will be active.

      • If your plugins or feed are already up to date, the **Update** link will be inactive.

   b. If you want to upload a custom feed file, click **Choose File**.

c. Click **Submit**.

> Tenable Security Center saves your configuration.

To view and edit plugin and feed settings and schedules as an organizational user:

1. Log in to Tenable Security Center via the user interface.

2. In the top navigation bar, click your user profile **SC** icon > **Feeds**.

    The **Plugins/Feed Configuration** page appears.

3. View the **Plugin Detail Locale** section to see the local language configured for Tenable Security Center.

4. Expand the **Schedules** section to show the settings for the **Tenable Security Center Feed**, **Active Plugins**, **Passive Plugins**, or **Event Plugins** schedule.

5. If you want to update a plugin or feed on demand, click **Update**. You cannot update feeds with invalid activation codes.

6. If you want to upload a custom feed file, click **Choose File**.

7. Click **Submit**.

    Tenable Security Center saves your configuration.

Configure Plugin Text Translation

Required Tenable Security Center User Role: Administrator

For more information, see Configuration Settings.

To configure plugin text translation:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **System** > **Configuration**.

    The **Configuration** page appears.

3. Click the **Plugins/Feed** tile.

    The **Plugins/Feed Configuration** page appears.

4. If you want plugin text to display in a local language, select a language from the **Locale List** box.

5. Click **Apply**.

   Tenable Security Center saves your configuration.

6. In the **Schedules** section, in the **Active Plugins** row, click **Update**.

   Tenable Security Center updates active plugins to obtain available translations.

API Key Authentication

You can enable API key authentication to allow users to use API keys as an authentication method for Tenable Security Center API requests. Without API keys, users must use the `/token` endpoint to log in to the Tenable Security Center API and establish a token for subsequent requests, as described in Token in the *Tenable Security Center API Guide*.

Tenable Security Center attributes actions performed with API keys to the user account associated with the API keys. You can only perform actions allowed by the privileges granted to the user account associated with the API keys.

You can enable the **Allow API Keys** toggle in your Security Settings to allow users to perform API key authentication. Then, users can generate API keys for themselves or for other users. API keys include an access key and secret key that must be used together for API key authentication. For more information, see Enable API Key Authentication and Generate API Keys.

A user can use API keys for Tenable Security Center API request authentication by including the **x-apikey** header element in your HTTP request messages, as described in API Key Authorization in the *Tenable Security Center API Best Practices Guide*.

Deleting API keys prevents users from authenticating Tenable Security Center API requests with the deleted keys. For more information, see Delete API Keys.

For more information about the Tenable Security Center API, see the *Tenable Security Center API Guide* and the *Tenable Security Center API Best Practices Guide*.

Enable API Key Authentication

Required Tenable Security Center User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can enable API key authentication to allow users to use API keys as an authentication method for Tenable Security Center API requests. For more information, see API Key Authentication.

To allow users to authenticate to the Tenable Security Center API using API keys:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **Security** tile.

   The **Security Configuration** page appears.

4. In the **Authentication Settings** section, click **Allow API Keys** to enable the toggle.

5. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

- Generate API keys for a user, as described in Generate API Keys.

Disable API Key Authentication

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

> **Caution:** Disabling API keys prevents users from authenticating API requests with API keys. Disabling API keys does not delete existing API keys. If you re-enable API keys, Tenable Security Center reauthorizes any API keys they were active before you disabled API key authentication.

For more information, see API Key Authentication.

To disable API key authentication:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **Security** tile.

   The **Security Configuration** page appears.

4. In the **Authentication Settings** section, click **Allow API Keys** to disable the toggle.

5. Click **Submit**.

   Tenable Security Center saves your configuration.

Enable Picture in Picture

> **Required Tenable Security Center User Role:** Administrator

You can enable **Picture in Picture** to allow administrators to view and manage Tenable Nessus scanner configurations from the Tenable Security Center user interface.

> **Note:** You cannot use **Picture in Picture** with a Tenable Nessus scanner if you enabled **Use Proxy** for the scanner or if the scanner's **Authentication Type** is **SSL Certificate**. For more information, see Tenable Nessus Scanner Settings.

To enable **Picture in Picture**:

1. Log in to Tenable Security Center via the user interface.

2. Click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **Security** tile.

   The **Security Configuration** page appears.

4. In the **Scanners** section, click **Picture in Picture** to enable the toggle.

5. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

- View and manage your Tenable Nessus instances in Tenable Security Center, as described in View Tenable Nessus Instances in Tenable Security Center.

Disable Picture in Picture

> **Required Tenable Security Center User Role:** Administrator

For more information, see [Tenable Nessus Scanners](#).

To disable **Picture in Picture**:

1. Log in to Tenable Security Center via the user interface.

2. Click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **Security** tile.

   The **Security Configuration** page appears.

4. In the **Scanners** section, click **Picture in Picture** to disable the toggle.

5. Click **Submit**.

   Tenable Security Center saves your configuration.

Tenable One Data

After you configure Tenable Security Center data synchronization to Tenable One in Tenable Vulnerability Management, you can monitor information about your Tenable One metrics and past synchronizations. For general information about Tenable One synchronization, see [Configure Tenable One Synchronization](#).

Tenable Security Center logs all Tenable One synchronization activity. For more information about the log contents, see [View Tenable One Data Synchronization Logs](#).

Tenable Security Center retrieves your latest Cyber Exposure Score (CES), Assessment Maturity grade, and Remediation Maturity grade daily from Tenable One in Tenable Vulnerability Management. For more information about the metrics and timing, see [View Tenable One Metrics](#).

View Tenable One Metrics

> **Required Additional License:** Tenable Lumin

> **Required Tenable Security Center User Role:** Administrator

After you configure Tenable Security Center data synchronization to Tenable One in Tenable Vulnerability Management, you can view information about your Tenable One metrics.

Every day at 11:00 PM UTC, Tenable Security Center retrieves data from Tenable One in Tenable Vulnerability Management.

> **Note:** Newly transferred data does not immediately impact your Tenable Lumin metrics (for example, your CES). Tenable requires 4 to 6 hours to recalculate your metrics. Recalculated metrics appear in Tenable Security Center after the next daily retrieval.
>
> For more information, see How long does synchronization take to complete?.

> **Tip:** To view all Tenable Lumin data and take advantage of full Tenable Lumin functionality, see Tenable Lumin.

To view Tenable One metrics in Tenable Security Center:

1. Log in to Tenable Security Center via the user interface.

2. To view your Cyber Exposure Score, Assessment Maturity grade, and Remediation Maturity grade, do the following:

   a. In the left navigation, click **System** > **Tenable One Data**.

      The **Tenable One Data** page appears.

   b. In the **Metrics** section, view data about your Tenable One metrics.

      - An updated Cyber Exposure Score (CES) for the data you synchronized to Tenable One. High CES values indicate higher risk.

      - An updated Assessment Maturity grade for the data you synchronized to Tenable One. A high grade indicates you are assessing your assets frequently and thoroughly.

      - An updated Remediation Maturity grade for the data you synchronized to Tenable One. A high grade indicates you are remediating the vulnerabilities on your assets quickly and thoroughly.

      If a metric changed since the last retrieval, Tenable Security Center identifies if the value increased (⬆) or decreased (⬇).

> **Tip:** If you performed an initial synchronization, Tenable requires up to 48 hours to calculate your Tenable Lumin metrics. Then, metrics appear in Tenable Security Center after the next daily retrieval.
>
> For more information, see How long does synchronization take to complete?.

3. (Requires Tenable Security Center+ license) To view the Asset Criticality Rating for a host, view details for the host, as described in View Hosts. For more information, see Asset Criticality Rating in the *Tenable Vulnerability Management User Guide*.

4. (Requires Tenable Security Center+ license) To view the Asset Exposure Score for a host, view details for the host, as described in View Hosts. For more information, see Asset Exposure Score in the *Tenable Vulnerability Management User Guide*.

View Tenable One Data Synchronization Logs

> **Required Additional License:** Tenable Lumin

> **Required Tenable Security Center User Role:** Administrator

After you configure Tenable Security Center data synchronization to Tenable One in Tenable Vulnerability Management, you can view the logs for past synchronizations.

For information about monitoring Tenable One synchronization status, see View Tenable One Synchronization Status.

To view Tenable One synchronization logs:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **System** > **Tenable One Data**.

   The **Tenable One Data** page appears.

3. In the **History** section, view data about your logged activity.

Column	Description
Timestamp	The date and time of the logged activity, including the day of the week, the date, and the time.

Column	Description
	For example, *Tue, 05 Mar 2024 15:42:00.000*.
Object Type	The synchronization data type.
Sync Type	The repository or asset synchronization type: • **Cumulative** repository synchronization — The initial synchronization of this repository, which included all cumulative database data from the repository. • **Active** repository synchronization — A subsequent synchronization of this repository, which included only the new or modified scan result data imported to the repository. • **Static** asset — A synchronization of Static Assets. • **Dynamic** asset — A synchronization of Dynamic Assets. • **Delete** host - A synchronization of deleted Host Assets. • **Unknown** — Indicates an error occurred.
Object ID	The repository ID, asset ID, or host UUID. To locate the ID or UUID for an object, see View Repository Details, View Asset Details, or View Host Details.
Transfer Duration	For repository or asset synchronizations, the length of time it took Tenable Security Center to transfer your repository or asset data to Tenable Vulnerability Management. For host asset deletion synchronizations, the length of time it took Tenable Vulnerability Management to delete the host asset after the host was deleted in Tenable Security Center. **Note:** The transfer duration does not include the time required for all data and recalculated metrics to appear in Tenable One. For more information, see How long does synchronization take to complete?.

Column	Description
Status	The status of the repository or asset synchronization: • **Error** — Tenable Security Center failed to transfer your data to Tenable Vulnerability Management. • **Synchronized** — Tenable Security Center successfully transferred your data to Tenable Vulnerability Management. For more information about the time required for all data and recalculated metrics to appear in Tenable One, see How long does synchronization take to complete?.

4. To view additional details about your logged activity, click a row in the table.

Column	Description
Repository or asset **Message**	A message explaining the reason for the synchronization **Error** status.
Repository or asset **Organization ID**	The organization ID. To locate the ID for an organization, see View Organization Details.
Repository **Scan Result ID**	The scan result ID. To locate the ID for a scan result, see View Scan Result Details.

Edit an ACR Manually

Required License: Tenable Security Center+

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can customize an individual host's Asset Criticality Rating (ACR) value to reflect the unique infrastructure or needs of your organization.

For more information about ACR values, see Asset Criticality Rating in the *Tenable Vulnerability Management User Guide*.

> **Tip:** If you want to edit the ACR for a host you imported using a remote repository or by connecting a managed Tenable Security Center instance to Tenable Security Center Director, log in to the Tenable Security Center instance that contains the host's data.

> **Tip:** Changes to an ACR value (and recalculations for your ACR values) take effect within 24 hours.

To edit the ACR for a host:

1. Log in to Tenable Security Center via the user interface.

2. Click **Assets** > **Host Assets**.

   The **Host Assets** page appears.

3. In the host assets table, do one of the following:

   - Click the row for the host.

     The **Host Asset Details** page appears.

     In the **Asset Criticality Rating** section, click the ✎ button.

   - Right-click the row for the host for which you want to edit the ACR.

     The actions menu appears.

     Click **Edit ACR**.

   - Select the check box for the host for which you want to edit the ACR.

     The available actions appear at the top of the table.

     Click **Edit ACR**.

   The **Edit Asset Criticality Rating** plane appears.

4. Do one of the following:

   - To modify the ACR value, click the Asset Criticality Rating slider to increase or decrease the ACR.

   - To reset an existing ACR value to the Tenable-provided ACR value, click **Reset to Tenable ACR**.

5. In the **Overwrite Reasoning** section, select one or more options to include a justification for your ACR change. For example, if a host in your development lab environment received a Tenable-assigned ACR appropriate for a public host but not the development host, you can select **Dev Only**. If you modify the ACR from the Tenable-provided value, this option is required.

6. In the **Notes** box, type a note about your ACR change. If you select **Other** in the **Overwrite Reasoning** section, you must type a note for the change.

7. Click **Submit**.

   Tenable Security Center saves the ACR.

What to do next:

- View the ACR for each host, as described in [View Hosts](#).

Diagnostics 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. For more information, see [Before You Upgrade](#).
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. For more information, see [Hardware Requirements](#).
Correct RPM Package Installed	Indicates whether you have the correct Tenable Security Center RPM installed for your operating system.

System Function	Description
	For more information, see [System Requirements](#).
Debugging	Indicates whether debugging is enabled. You may experience performance and storage issues if you leave debugging enabled for extended periods of time.
	For more information, see [Debugging LogsDebugging Logs](#).
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.
PostgreSQL Connection Errors	Indicates whether any database connection errors have occurred.

Diagnostics File

You can use this section to generate a diagnostics file for troubleshooting with Tenable Support. For more information, see [Generate a Diagnostics File](#).

Debugging Logs

You can use this section to enable or disable debugging logs for troubleshooting with Tenable Support. For more information, see [Enable Debugging Logs](#) and [Disable Debugging Logs](#).

> **Note:** Tenable does not recommend leaving debugging enabled on Tenable Security Center after you send the log files to Tenable Support. You may experience performance and storage issues if you leave debugging enabled for extended periods of time.

Generate a Diagnostics File

> **Required Tenable Security Center 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](#).

For more information about Tenable Security Center diagnostics, see Diagnostics Settings.

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

For more information, see Diagnostics Settings and Generate a Diagnostics File.

Option	Description	Default
General		
Strip IPs from Chapters	When enabled, Tenable Security Center omits IP addresses from the following files: • `sc-configuration.txt`	Disabled

Option	Description	Default
	• `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`	
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`). For more information, see Active Scans, Agent Scanning, and Freeze Windows.	Enabled
Setup	Include information about the following Tenable Security Center resources in the diagnostic file (`sc-setup.txt`): • Active users • Tenable Nessus Scanners • Tenable Network Monitor Instances	Enabled

Option	Description	Default
	• Tenable Log Correlation Engines • Scan Zones • Schedules • Job Queue Events • Assets • Repositories • Organizations • User Roles • Reports • Report results • Audit Files	
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`). For more information, see Tenable Security Center Communications and Directories.	Enabled
Dependency	Include information about Tenable Security Center dependencies in the diagnostic file (`sc-depsinfo.txt`). For more information, see Dependencies.	Enabled
Upgrade Log	Include a log of Tenable Security Center upgrade events in	Enabled

Option	Description	Default
	the diagnostic file (`upgrade.log`).	
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 (`sc-users.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 For more information about ID values, see View User Details, View User Role Details, and View Group Details.	Enabled
Include Names	(If **User Information** is enabled) Include usernames and user display names for each user in the diagnostic file. For more information, see User Account Options. > **Tip**: The display name combine's the user's **First Name** and **Last Name**.	Disabled

Enable Debugging Logs

Required Tenable Security Center User Role: Administrator

You can enable debugging to generate logs for troubleshooting with Tenable Support.

> **Caution:** Tenable does not recommend enabling debugging logs unless instructed by Tenable Support.

To enable debugging:

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 **Debugging Logs** section, select one or more debugging logs Tenable Support asked you to enable.

4. Click **Save Debug Settings**.

   Tenable Security Center enables the debugging logs you selected and saves the corresponding log files to `/opt/sc/admin/logs`.

What to do next:

- Download the debugging logs, as described in Download Debugging Logs.

- Share the debugging log files with Tenable Support.

- Disable any unneeded debugging logs, as described in Disable Debugging Logs.

  > **Note:** Tenable does not recommend leaving debugging enabled on Tenable Security Center after you send the log files to Tenable Support. You may experience performance and storage issues if you leave debugging enabled for extended periods of time.

  > **Note:** Collected debug logs contained in the debug archive are automatically deleted during the scheduled nightly cleanup.

Download Debugging Logs

> **Required Tenable Security Center User Role:** Administrator

You can download debugging logs for troubleshooting with Tenable Support.

Before you begin:

- Enable debugging logs, as described in [Enable Debugging Logs](#).

To download debugging logs:

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 **Download Debugging Logs** section, click **Collect Log Files**.

   Tenable Security Center generates the debugging log files you selected.

4. Click **Download Debug File**.

   The debugging logs download.

What to do next:

- Share the files with Tenable Support.

- Disable any debugging logs as needed, as described in [Disable Debugging Logs](#).

> **Note:** Tenable does not recommend leaving debugging enabled on Tenable Security Center after you send the log files to Tenable Support. You may experience performance and storage issues if you leave debugging enabled for extended periods of time.

> **Note:** Collected debug logs contained in the debug archive are automatically deleted during the scheduled nightly cleanup.

Disable Debugging Logs

Required Tenable Security Center User Role: Administrator

Tenable does not recommend leaving debugging enabled on Tenable Security Center after you send the log files to Tenable Support. You may experience performance and storage issues if you leave debugging enabled for extended periods of time.

For more information about debugging logs, see [Debugging Logs](#).

To disable debugging:

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 **Debugging Logs** section:

   - To disable individual debugging logs, deselect the logs.

   - To disable all debugging logs, click **Deselect All**.

4. Click **Save Debug Settings**.

   Tenable Security Center disables the debugging logs you deselected.

What to do next:

- Follow Tenable Support's instructions to manually remove old debugging log files from `/opt/sc/admin/logs`.

Job Queue Events

Path: **System** > **Job Queue**

Job Queue is a Tenable Security Center feature that displays specified events in a list for review.

You can view and sort Job Queue notifications in several ways by clicking on the desired sort column. Using the ⚙ 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 Tenable Security Center processes.

System Logs

Tenable Security Center logs contain detailed information about functionality to troubleshoot unusual system or user activity. You can use the system logs for debugging and for maintaining an audit trail of users who access Tenable Security Center or perform basic functions (for example, changing passwords, recasting risks, or running Nessus scans).

To view system logs:

1. Log in to Tenable Security Center via the user interface.

2. Click **System** > **System Logs** (Administrator users) or **Username** > **System Logs** (Organizational users).

   The **System Logs** page appears.

3. To filter the logs, see Apply a Filter.

   The page updates to reflect the filter you applied.

View System Logs

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see System Logs.

To view system logs:

1. Log in to Tenable Security Center via the user interface.

2. Click **System** > **System Logs** (Administrator users) or **Username** > **System Logs** (Organizational users).

   The **System Logs** page appears and shows the 50 most recent system logs.

3. To filter the logs, see Apply a Filter.

   The page updates to reflect the filter you applied.

Publishing Sites Settings

Path: **System** > **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.

Option	Description
Name	Type a name for the publishing site.

Option	Description
Description	Type a description of the publishing site.
Type	The method Tenable Security Center uses to publish to the site. Available options are **HTTP Post** or **CMRS**. Use the selection appropriate for the configuration of the publishing site.
Max Chunk Size (MB)	If the target is a CMRS site, Tenable sends the report in chunks sized according to this value.
URI	The target address to send the report to when completed.
Use Proxy	When enabled, the publishing site leverages the web proxy defined in the [Web Proxy](#) settings.
Authentication	There are two methods of authentication available: **SSL Certificate** and **Password**.
Username / Password	If you select **Password** as the **Authentication** method, the credentials to authenticate to the target publishing server.
Certificate	If you selected **SSL Certificate** as the **Authentication** method, the certificate you want to use for authentication.
Organizations	Select the organization(s) that are allowed to publish to the configured site.
Verify Host	When enabled, Tenable Security Center verifies that the target address specified in the **URI** option matches the CommonName (CN) in the SSL certificate from the target publishing server.

Keys Settings

Keys allow administrator users to use key-based authentication with a remote Tenable Security Center (remote repository) or between a Tenable Security Center and a Tenable Log Correlation Engine server. This also removes the need for Tenable Security Center administrators to know the administrator login or password of the remote system.

Tenable Security Center uses Elliptic Curve Digital Signature Algorithm (ECDSA) keys to authenticate to other Tenable Security Center instances, and Rivest-Shamir-Adleman (RSA) keys to authenticate to Tenable Log Correlation Engine servers.

> **Note:** The ECDSA public key from the local Tenable Security Center must be added to the **Keys** section of the Tenable Security Center from which you wish to retrieve a repository. If the keys are not added properly, the remote repository add process prompts for the root username and password of the remote host to perform a key exchange before the repository add/sync occurs.

For more information, see Add a Key, Delete a Key, and Download the Tenable Security Center SSH Key.

Remote Tenable Log Correlation Engine Key Exchange

A manual key exchange between the Tenable Security Center and the Tenable Log Correlation Engine is normally not required; however, in some cases where remote root login is prohibited or key exchange debugging is required, you must manually exchange the keys.

For the remote Tenable Log Correlation Engine to recognize the Tenable Security Center, you need to copy the SSH public key of the Tenable Security Center and append it to the `/opt/lce/.ssh/authorized_keys` file. The `/opt/lce/daemons/lce-install-key.sh` script performs this function.

Add a Key

> **Required Tenable Security Center User Role:** Administrator

For more information, see Keys Settings.

To add a new key:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **System** > **Keys**.

   The **Keys** page appears.

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

   The **Add Key** page appears.

4. In the **Type** drop-down, select **DSA**,**RSA**, or **ECDSA**.

5. In the **Comment** box, add a description or note about the key.

6. In the **Public Key** box, type the text of your public key from your remote Tenable Security Center.

7. Click **Submit**.

   Tenable Security Center saves your configuration.

Delete a Key

Required Tenable Security Center User Role: Administrator

For more information, see Keys Settings.

To delete a key:

1. Log in to Tenable Security Center via the user interface.

2. Click **System** > **Keys**.

3. Select the key you want to delete:

   ### To delete a single key:

   a. In the table, right-click the row for the key you want to delete.

      The actions menu appears.

   b. Click **Delete**.

   ### To delete multiple keys:

   a. In the table, select the check box for each key you want to delete.

      The available actions appear at the top of the table.

   b. At the top of the table, click **Delete**.

   A confirmation window appears.

4. Click **Delete**.

   Tenable Security Center deletes the key.

Download the Tenable Security Center SSH Key

> **Required Tenable Security Center User Role:** Administrator

You can download the Tenable Security Center ECDSA key on the **Keys** page. For more information about keys, see [Keys Settings](#).

> **Note:** Tenable Security Center authenticates to Log Correlation Engine with RSA keys, and authenticates to Tenable Security Center with ECDSA keys. If your Tenable Security Center remote repository still uses an RSA key, it will continue to use the RSA key until you add the ECDSA key to the remote repository.

To download the Tenable Security Center SSH key:

1. Log in to Tenable Security Center via the user interface.

2. Click **System** > **Keys**.

3. At the top of the table, click **Download Tenable Security Center Key**.

   The Tenable Security Center ECDSA key downloads.

Notifications

To view your Tenable Security Center notifications, in the top navigation bar, click your user profile **SC** icon > **Notifications** *or* click the 🔔 icon > **Show More**. Notifications are cleared after 30 days.

> **Note:** If you upgrade from a previous version of Tenable Security Center to version 6.4.0 or later, all existing notifications will be deleted.

In Tenable Security Center, certain events can display a pop-up in the lower right-hand corner of the Tenable Security Center user interface. When you click on a notification, the **Notifications** page appears.

The **Notifications** page displays a list of notifications for your Tenable Security Center instance. You can filter these notifications by time frame. For general information about using filters, see [Filters](#).

User Profile Menu Settings

The user profile **SC** icon in the top navigation bar opens a menu with options to manage your user account.

> **Note:** Depending on the screen resolution, the username may not appear next to the user icon in the top navigation bar.

About

Path: Your user profile **SC** icon > **About**

The **About** menu item displays the Tenable Security Center version, Server Build ID, and copyright information.

System Logs (Organizational Users Only)

Path: Your user profile **SC** icon > **System Logs**

For a complete discussion about system logs, see System Logs.

Profile (Organizational Users Only)

Path: Your user profile **SC** icon > **Profile**

The **Profile** option launches the **Edit User Profile** page, where you can modify some of your user account information and permissions. For more information about user account options, see User Account Options.

Feeds (Organizational Users Only)

Path: Your user profile **SC** icon > **Feeds**

The **Feeds** option displays information about the Tenable Security Center feeds and plugin sets and, if permitted, a link to update the plugins either through Tenable Security Center or by manually uploading plugins. The displayed feeds are for Tenable Security Center Feed, Active Plugins, Passive Plugins, and Event Plugins. You can only update feeds with valid Activation Codes.

Plugins are scripts used by the Tenable Nessus, Tenable Network Monitor, and Log Correlation Engine servers to interpret vulnerability data. For ease of operation, Tenable Security Center centrally manages Tenable Nessus and Tenable Network Monitor plugins and pushes the plugins out

to their respective scanners. Log Correlation Engine servers download their own event plugins and Tenable Security Center downloads event plugins for its local reference. Tenable Security Center does not currently push event plugins to Log Correlation Engine servers.

For more information about plugin/feed settings, see Configuration Settings and Edit Plugin and Feed Settings and Schedules.

Notifications

Path: Your user profile SC icon > **Notifications** *or* 🔔 icon > **Show More**

In Tenable Security Center, specified events can display a pop-up in the lower right-hand corner of the Tenable Security Center user interface.

Some events in Tenable Security Center will cause a notification to appear in the 🔔 icon in the top navigation bar.

For more information, see Notifications.

Plugins

Path: Your user profile SC icon > **Plugins**

Plugins are scripts used by the Tenable Nessus, Tenable Network Monitor, and Log Correlation Engine servers to interpret vulnerability data. For ease of operation, Tenable Nessus and Tenable Network Monitor plugins are managed centrally by Tenable Security Center and pushed out to their respective scanners. Log Correlation Engine servers download their own event plugins and Tenable Security Center downloads event plugins for its local reference. Tenable Security Center does not currently push event plugins to Log Correlation Engine servers.

Within the Plugins interface, click the information icon next to the Plugin ID and search for specific plugins utilizing the filtering tools to view plugin details/source.

For more information about custom plugins, see Custom Plugin Packages for NASL and CA Certificate Upload.

Help

Path: Your user profile SC icon > **Help**

The **Help** option opens the *Tenable Security Center User Guide* section for your page. To access other Tenable documentation, see https://docs.tenable.com/.

Logout

To end your session in Tenable Security Center, click Your user profile 🆂🅲 icon > **Logout**. Tenable recommends closing your browser window after logging out.

Plugin Filter Components

For general information about using filters, see Filters.

Filter Component	Description
BID	Filters plugins based on the BID.
Cross References	Filters plugins based on a search against the cross reference information.
CVE ID	Displays plugins based on one or more CVE IDs. Type multiple IDs as a comma-separated list (e.g., *CVE-2011-3348,CVE-2011-3268,CVE-2011-3267*).
Exploit Prediction Scoring System (EPSS)	Filters results by the EPSS score, which predicts how likely a vulnerability is to be exploited.
Exploit Available	If set to yes, displays only plugins for vulnerabilities for which a known public exploit exists.
MS Bulletin ID	Displays plugins based on one or more Microsoft Bulletin IDs. Type multiple IDs as a comma-separated list (e.g., *MS10-012,MS10-054,MS11-020*).
Name	Type all or a portion of the actual plugin name. For example, entering **MS08-067** displays plugins named **MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)**. Similarly, entering the string **uncredentialed** displays a list of plugins with that string in the name.

Filter Component	Description
Patch Modified	Tenable plugins contain information about when a patch was last modified. This filter allows users to search based on when a particular patch was modified: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify)
Patch Published	Some plugins contain information about when a patch was published for a vulnerability. This filter allows the user to search based on when a vulnerability's patch became available: • **None** (displays plugins for vulnerabilities that do not have a patch available) • **Within the last day** • **Within the last 7 days** • **Within the last 30 days**

Filter Component	Description
	• **More than 7 days ago**
	• **More than 30 days ago**
	• **Current Month**
	• **Last Month**
	• **Current Quarter** (during the current calendar year quarter)
	• **Last Quarter** (during the previous calendar year quarter)
	• **Current Year**
	• **Last Year**
	• **Custom Range** (during a specific range you specify)
	• **Explicit** (at a specific time you specify)
Plugin ID	Type the plugin ID desired or range based on a plugin ID. Available operators are equal to (=), not equal to (!=), greater than or equal (>=) and less than or equal to (<=).
Plugin Modified	Tenable plugins contain information about when a plugin was last modified. This filter allows users to search based on when a particular plugin was modified:
	• **Within the last day**
	• **Within the last 7 days**
	• **Within the last 30 days**
	• **More than 7 days ago**
	• **More than 30 days ago**
	• **Current Month**
	• **Last Month**

Filter Component	Description
	• **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify)
Plugin Published	Tenable plugins contain information about when a plugin was first published. This filter allows users to search based on when a particular plugin was created: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify)
Plugin Type	Select whether to filter plugin types by active, compliance, event, passive,

Filter Component	Description
	or WAS plugins.
Vulnerability Published	When available, Tenable plugins contain information about when a vulnerability was published. This filter allows users to search based on when a particular vulnerability was published:
	• **Within the last day**
	• **Within the last 7 days**
	• **Within the last 30 days**
	• **More than 7 days ago**
	• **More than 30 days ago**
	• **Current Month**
	• **Last Month**
	• **Current Quarter** (during the current calendar year quarter)
	• **Last Quarter** (during the previous calendar year quarter)
	• **Current Year**
	• **Last Year**
	• **Custom Range** (during a specific range you specify)
	• **Explicit** (at a specific time you specify)
Security End of Life Date	When available, Tenable plugins contain information about software end of life dates. This filter allows users to search based on when a particular software is end of life:
	• **Within the last day**
	• **Within the last 7 days**
	• **Within the last 30 days**

Filter Component	Description
	• **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify)
Vulnerability Priority Rating (VPR)	Displays plugins for vulnerabilities within the chosen VPR range. For more information, see [CVSS vs. VPR](#). **Tip:** The **Vulnerabilities** page displays vulnerabilities by plugin. The VPR that appears is the highest VPR of all the vulnerabilities associated with that plugin.

Custom Plugin Packages for NASL and CA Certificate Upload

> **Note:** Tenable does not support troubleshooting custom plugin packages for NASL.

You can upload a custom plugin package as a `.tar.gz` or `.tgz` file. Depending on your needs, you must include a combination of the following files:

- A `custom_feed_info.inc` file. Always include this file to time stamp your upload to Tenable Security Center.

- (Optional) A `custom_nasl_archive.tar.gz` or `custom_nasl_archive.tgz` file. Include this file if you are uploading one or more custom plugins.

- (Optional) A `custom_CA.inc` file. Include this file if you are uploading one or more CA certificates to solve a Tenable Nessus scanning issue.

After you [Create the Custom Plugin Package](#) and [Upload the Custom Plugin Package](#), Tenable Security Center pushes the package to Tenable Nessus for use when scanning.

> **Note:** The system untars the files within your custom plugin package and overwrites any identically named files already in Tenable Security Center or Tenable Nessus.

custom_feed_info.inc Guidelines

Always include this file to time stamp your upload to Tenable Security Center. This text file must contain the following lines:

```
PLUGIN_SET = "YYYYMMDDHHMM";
PLUGIN_FEED = "Custom";
```

The `PLUGIN_SET` variable *YYYYMMDDHHMM* is the date and time 2 minutes in the future from when you plan to upload the file to Tenable Security Center.

custom_nasl_archive.tar.gz or custom_nasl_archive.tgz Guidelines

Include this file if you are uploading one or more custom plugins. This package must contain one or more custom plugin NASL files.

All custom plugins must have unique Plugin ID numbers and have family associations based on existing Tenable Security Center families.

> **Note:** Tenable Support does not assist with creating custom plugin NASL files.

custom_CA.inc Guidelines

Include this file if you are uploading one or more CA certificates to solve a Tenable Nessus scanning issue. This text file must contain PEM-encoded (Base64) CA certificate text.

For troubleshooting information, see [Troubleshooting Issues with the custom_CA.inc File](#).

One CA Certificate

If you need to include a single CA certificate, paste the PEM-encoded (Base64) certificate directly into the file.

```
-----BEGIN CERTIFICATE-----
certificatetext
certificatetext
certificatetext
certificatetext
-----END CERTIFICATE-----
```

Multiple CA Certificates

If you need to include two or more CA certificates, include the PEM-encoded (Base64) certificates back-to-back.

```
-----BEGIN CERTIFICATE-----
certificate1text
certificate1text
certificate1text
certificate1text
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
certificate2text
certificate2text
certificate2text
certificate2text
-----END CERTIFICATE-----
```

Create the Custom Plugin Package

Required Tenable Security Center User Role: Administrator

For complete information, see Custom Plugin Packages for NASL and CA Certificate Upload.

To create the `.tar.gz` or `.tgz` custom plugin package:

1. Prepare the individual text files you want to include in the custom plugins package.

    - `custom_nasl_archive.tar.gz` or `custom_nasl_archive.tgz`

    - `custom_feed_info.inc`

    - `custom_CA.inc`

    Confirm the files meet the requirements described in Custom Plugin Packages for NASL and CA Certificate Upload.

    > **Note:** After upload, the system untars the files within your custom plugin package and overwrites any identically named files already in Tenable Security Center or Tenable Nessus.

2. In the command line interface (CLI), tar and compress the files together. (7-Zip or running tar on a Mac does not work for this.) For example:

    ```
    # tar -zcvf upload_this.tar.gz custom_feed_info.inc custom_CA.inc
    ```

    The system generates a `.tar.gz` or `.tgz` file.

What to do next:

- Upload the `.tar.gz` or `.tgz` file, as described in Upload the Custom Plugin Package.

Upload the Custom Plugin Package

> **Required Tenable Security Center User Role:** Administrator

For complete information, see Custom Plugin Packages for NASL and CA Certificate Upload.

Before you begin:

- Create the `.tar.gz` or `.tgz` custom plugin file, as described in Create the Custom Plugin Package.

Upload the `.tar.gz` or `.tgz` file to Tenable Security Center:

1. Log in to Tenable Security Center via the user interface.

2. Click **Username** > **Plugins**.

The **Plugins** page appears.

3. Click **Upload Custom Plugins** and select the `.tar.gz` or `.tgz` file.

4. Click **Submit**.

   Tenable Security Center uploads the package and pushes it to Tenable Nessus.

What to do next:

- To verify the upload succeeded, click **System** > **System Logs**.

- To verify the upload resolved a validation issue, run another scan that includes plugin 51192. Verify that Nessus has the custom plugin bundle by checking its plugin directory.

Troubleshooting Issues with the custom_CA.inc File

If uploading a `custom_CA.inc` file does not resolve your issue, confirm your file meets the requirements described in [custom_CA.inc Guidelines](). Then, use these tips to continue troubleshooting.

The `/opt/sc/data/customNasl/custom_CA.inc` file

If the Tenable Security Center installation is not on the Appliance, check the uploaded custom_CA.inc with the following command: `# cat /opt/sc/data/customNasl/custom_CA.inc`.

The output should match the `custom_CA.inc` file that you checked in a text editor in step T1 above. If the file does not exist, the upload was not successful. If the file does not match, the most recent upload may not have been successful. Go over the steps above for creating and uploading `upload_this.tar.gz` and ensure it is done correctly.

The `/opt/nessus/lib/nessus/plugins/custom_CA.inc` or `\ProgramData\Tenable\Nessus\nessus\plugins\custom_CA.inc` file

If Nessus is not on the Appliance, navigate to the plugins folder and cat or type custom_CA.inc to verify it exists and matches the custom_CA.inc file contents verified in steps 1 and 2 above. If custom_CA.inc does not exist in the plugins folder, or does not match the most recent custom_CA.inc in Tenable Security Center, it has not propagated to the scanner. Check **Resources** > **Nessus Scanners** in Tenable Security Center to see if the scanner is still updating plugins. If it is in a

Working state, try updating the active plugins in Tenable Security Center to prompt a plugin push. For more information, see [Plugins/Feed Settings](#).

The plugin 51192 output details

Adding the custom CA certificate to custom_CA.inc does not resolve the issue if the service is missing intermediate certificate(s). If the service has a self-signed or default certificate (if not self-signed with the server name, it may be issued by a vendor name like Nessus Certification Authority) and not a certificate signed by their custom CA at all, the certificate is expired, etc.

Look at the detailed plugin output of 51192 to see exactly why the certificate is untrusted. If custom_CA.inc can fix it, the output states that the certificate at the top of the certificate chain is unrecognized, and the certificate it shows is either issued by the custom CA (matching the name exactly) or the actual custom CA self-signed certificate.

Backup and Restore

Tenable recommends performing regular backups of the Tenable Security Center data in your `/opt/sc` directory. When you restore a backup, the file overwrites the content in your `/opt/sc` directory.

Data backup requirements:

- You must restore a backup file to a Tenable Security Center running the same version. For example, you cannot restore a backup file created on version 6.0.0 to a Tenable Security Center running Tenable Security Center 6.1.0.

- You must restore a backup file to the same Tenable Security Center where you created the backup file. The hostname associated with the backup file must match the hostname on the receiving Tenable Security Center. For example, you cannot restore a backup file created on a Tenable Security Center with the hostname *Example1* to a Tenable Security Center with the hostname *Example2*.

For more information, see [Perform a Backup](#) and [Restore a Backup](#).

Configuration Backups

Tenable recommends performing regular backups of your Tenable Security Center configuration in addition to your Tenable Security Center data. You can restore a configuration backup to quickly resume normal Tenable Security Center operation as part of your disaster recovery plan.

Configuration backups do not include data (such as vulnerability data, trend data, licenses, or secure connection settings). When your repositories contain new vulnerability data, you can use your dashboards, reports, and analysis tools to assess your network.

> **Note:** After you restore a configuration backup, Tenable recommends performing discovery scans to re-populate your repositories with vulnerability data. For more information, see Scanning Overview.

Configuration backup requirements:

- You must restore a backup file to a Tenable Security Center running the same version. For example, you cannot restore a backup file created on version 5.20.0 to a Tenable Security Center running Tenable Security Center 5.21.0.

> **Note:** For best performance, after restoring a configuration backup, ensure the hostname associated with the configuration backup file matches the hostname on the receiving Tenable Security Center.

For more information, see Perform a Configuration Backup and Restore a Configuration Backup.

Configurations Included in a Configuration Backup

Category	Configurations
Users	User accounts, user roles, groups, and organizations
Resources	Tenable Nessus scanners, Tenable Network Monitor instances, Log Correlation Engines, LDAP servers, and scan zones
System	Configuration settings (including data expiration settings, external schedules settings, Tenable Lumin settings, mail settings, miscellaneous settings, license settings, plugins/feed settings, SAML settings, and security settings), publishing sites settings, keys settings, and schedules
Scanning	Active scans, agent synchronization jobs, agent scans, freeze windows, credentials, scan policies, audit files, assets, repositories, and compliance check plugin entries

Reporting	Dashboards, Assurance Report Cards, report definitions, report images, and CyberScope and DISA report attributes
Workflow	Alerts
Analysis	Queries

Automatic Backups

Tenable Security Center performs automatic nightly backups of the following databases:

- `/opt/sc/application.db`

- `/opt/sc/hosts.db`

- `/opt/sc/jobqueue.db`

- `/opt/sc/plugins.db`

- `/opt/sc/remediationHierarchy.db`

- `/opt/sc/orgs/<orgID>/organization.db` (for each organization in your Tenable Security Center)

- `/opt/sc/orgs/<orgID>/assets.db` (for each organization in your Tenable Security Center)

Automatic backups run nightly at 1:20 AM local time. This schedule cannot be changed.

Tenable Security Center stores backups in the same directory as the database.

Perform a Backup

Required Tenable Security Center User Role: Root user

For more information about the backup and restore process, see Backup and Restore.

To perform a backup of Tenable Security Center data:

1. Log in to Tenable Security Center via the command line interface (CLI).

2. Stop Tenable Security Center, as described in Start, Stop, or Restart Tenable Security Center.

   Tenable Security Center stops.

3. In the CLI in Tenable Security Center, run the following command to view all running processes:

```
# ps -fu tns
```

4. If any processes are listed, run the following commands to stop them:

```
# killall -u tns
```

```
# killall httpd
```

> **Note:** These commands stop all jobs (including scans) running on Tenable Security Center.

5. If necessary, repeat step 4 to confirm all processes stopped.

6. Run the following command to create a `.tar` file for your `/opt/sc` directory:

```
# tar -pzcf sc_backup.tar.gz /opt/sc
```

> **Note:** The `.tar` file switches are case-sensitive.

Tenable Security Center creates the backup file.

7. Run the following command to confirm the backup file is not corrupted:

```
# tar -tvf sc_backup.tar.gz
```

8. Move the backup file to a secure location.

9. Start Tenable Security Center, as described in Start, Stop, or Restart Tenable Security Center.

   Tenable Security Center starts.

What to do next:

- (Optional) Restore the backup file, as described in Restore a Backup.

Restore a Backup

> **Required Tenable Security Center User Role:** Root user

For more information about the backup and restore process, see [Backup and Restore](#).

Before you begin:

- Perform a backup of your Tenable Security Center, as described in [Perform a Backup](#).

- Confirm your receiving Tenable Security Center meets the requirements described in [Backup and Restore](#).

- Move the backup file to your receiving Tenable Security Center's `/tmp` directory.

To restore a backup file:

1. Log in to Tenable Security Center via the command line interface (CLI).

2. Stop Tenable Security Center, as described in [Start, Stop, or Restart Tenable Security Center](#).

   Tenable Security Center stops.

3. In the CLI in Tenable Security Center, run the following command to view all running processes:

   ```
   # ps -fu tns
   ```

4. If any processes are listed, run the following commands to stop them:

   ```
   # killall -u tns
   ```

   ```
   # killall httpd
   ```

   > **Note:** These commands stop all jobs (including scans) running on Tenable Security Center.

5. If necessary, repeat step 4 to confirm all processes are stopped.

6. Run the following commands to decompress the `.tar` file and overwrite the existing /opt/sc directory:

```
# cd /
```

```
# tar -xvf /tmp/sc_backup.tar.gz
```

> **Note:** The `.tar` file switches are case-sensitive.

The restore finishes.

7. Start Tenable Security Center, as described in [Start, Stop, or Restart Tenable Security Center](#).

   Tenable Security Center starts.

Perform a Configuration Backup

> **Required Tenable Security Center User Role:** Root user

For more information about the backup and restore process and the configurations included in a configuration backup, see [Backup and Restore](#).

Before you begin:

- If you uploaded custom plugins, save a copy of your custom plugins in a safe location.

To perform a backup of your Tenable Security Center configuration:

1. Log in to Tenable Security Center via the command line interface (CLI).

2. Stop Tenable Security Center, as described in [Start, Stop, or Restart Tenable Security Center](#).

   Tenable Security Center stops.

3. In the CLI in Tenable Security Center, do one of the following:

   - To save the configuration backup file to a local directory, run the following command, where [*local directory path*] is the local directory where you want to save the backup file:

```
/opt/sc/support/bin/php /opt/sc/src/tools/backupSCConfiguration.php -l [local
directory path]
```

For example:

```
/opt/sc/support/bin/php /opt/sc/src/tools/backupSCConfiguration.php -l /tmp/
```

- To save the configuration backup file to a remote directory, run the following command, where [*remote directory absolute path*] is the absolute path to the remote directory where you want to save the backup file:

```
/opt/sc/support/bin/php /opt/sc/src/tools/backupSCConfiguration.php -r
[user]@[host]:[remote absolute path to configuration backups directory]
```

For example:

```
/opt/sc/support/bin/php /opt/sc/src/tools/backupSCConfiguration.php -r
tns@100.100.100.100:/tmp/
```

Tenable Security Center creates the configuration backup file and saves it to the specified directory.

> **Tip:** The configuration backup file name includes the backup date and time, the Tenable Security Center hostname, and the Tenable Security Center version (for example, `SC-config-20211101-165111-sc-hostname-5_20_0.tar.gz`).

4. Start Tenable Security Center, as described in Start, Stop, or Restart Tenable Security Center.

   Tenable Security Center starts.

What to do next:

- (Optional) Restore the configuration backup file, as described in Restore a Configuration Backup.

Restore a Configuration Backup

Required Tenable Security Center User Role: Root user

For more information about the backup and restore process and the configurations included in a configuration backup, see Backup and Restore.

> **Note:** For best performance, after restoring a configuration backup, ensure the hostname associated with the configuration backup file matches the hostname on the receiving Tenable Security Center.

Before you begin:

1. Perform a configuration backup of your Tenable Security Center, as described in Perform a Configuration Backup.

2. Confirm your receiving Tenable Security Center meets the requirements described in Backup and Restore.

To restore a configuration backup file:

1. Log in to Tenable Security Center via the command line interface (CLI).

2. Stop Tenable Security Center, as described in Start, Stop, or Restart Tenable Security Center.

   Tenable Security Center stops.

3. In the CLI in Tenable Security Center, run the following command to restore the configuration backup, where [*path to backup file*] is the path to the backup file you want to restore:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/restoreSCConfiguration.php -l [path to
   backup file]
   ```

   For example:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/restoreSCConfiguration.php -l /tmp/SC-
   config-20211101-165111-sc-hostname-5_20_0.tar.gz
   ```

   Tenable Security Center restores the configuration backup.

4. Start Tenable Security Center, as described in Start, Stop, or Restart Tenable Security Center.

   Tenable Security Center starts.

What to do next:

1. If you uploaded custom plugins before restoring your Tenable Security Center configuration, re-upload the custom plugins. For more information, see [Custom Plugin Packages for NASL and CA Certificate Upload](#).

2. Perform discovery scans to re-populate your repositories with vulnerability data. For more information, see [Scanning Overview](#).

Tenable One Synchronization

You can use Tenable One to quickly and accurately assess your Cyber Exposure risk and compare your health and remediation performance to other Tenable customers in your Salesforce industry and the larger population. Tenable Lumin correlates raw vulnerability data with asset business criticality and threat context data to support faster, more targeted analysis workflows than traditional vulnerability management tools. For more information about Tenable One, see [Tenable One](#).

After you acquire a Tenable Lumin license for use with Tenable Security Center, you can configure Tenable Security Center synchronization to send limited Tenable Security Center data to Tenable Vulnerability Management for use in Tenable One analysis. Tenable Security Center communicates with Tenable Vulnerability Management using an encrypted connection, as described in [Encryption Strength](#).

When you send data to Tenable Vulnerability Management, the system does not remove the data from your Tenable Security Center. You can continue normal operation of Tenable Security Center.

For more information, see:

- [Plan Your Tenable One Synchronization](#)

- [Configure Tenable One Synchronization](#)

- [View Tenable One Synchronization Status](#)

- [View Tenable One Data Synchronization Logs](#)

- [View Tenable One Metrics](#)

- [Disable Tenable One Synchronization](#)

Tenable One Synchronization Options

Option	Description
Access Key	The Tenable Vulnerability Management API access key for a Tenable Vulnerability Management user with Administrator permissions.
Secret Key	The Tenable Vulnerability Management API secret key for a Tenable Vulnerability Management user with Administrator permissions.
Network Support	Supports accurate tracking of assets in repositories with overlapping IPv4 addresses.

Tip: The default setting for **Network Support** depends on the Tenable Security Center version where you configured Tenable Lumin synchronization. For the purpose of determining the default setting for **Network Support**, Tenable Lumin synchronization is configured if you have configured the **Tenable Connection Settings** and selected at least one repository to synchronize.

- Tenable Security Center 5.18.x or earlier — Disabled by default if Tenable Lumin is already configured.

- Tenable Security Center 5.19.x or later — Enabled by default and cannot be disabled.

- **Enabled** — Tenable Security Center synchronizes each IPv4 repository, agent repository, and universal repository to its own network in Tenable Vulnerability Management, named **TSC-*Repository Name***. You do not need to resolve repository overlaps if you enable **Network Support**.

    Note: Once enabled, you cannot disable **Network Support**.

- **Disabled** — Tenable Security Center synchronizes all repository data to the Default network in Tenable Vulnerability Management. You must resolve all repository overlaps before synchronizing your Tenable Security Center data to Tenable Vulnerability Management.

For more information, see Networks in the *Tenable Vulnerability Management User Guide*.

Contact your Tenable representative to enable **Network Support**.

Plan Your Tenable One Synchronization

Tenable recommends planning your synchronization strategy to accommodate synchronization limitations and limit data duplication in Tenable Vulnerability Management.

Can I communicate with Tenable Vulnerability Management through a proxy?

To use a proxy configured for your Tenable Security Center instance for communications with your Tenable Vulnerability Management instance, configure the Web Proxy settings.

Can I synchronize multiple Tenable Security Center instances?

You can synchronize data from multiple Tenable Security Center instances or managed Tenable Security Center instances to a single Tenable Vulnerability Management instance.

The following are some prerequisites and considerations for syncing more than one Tenable Security Center to Tenable Vulnerability Management.

- Every repository that you sync with Tenable Vulnerability Management must have a unique name, across all Tenable Security Center instances.

  If two repositories in different Tenable Security Center instances have the same name, and you sync both repositories with Tenable Vulnerability Management, the second repository sync will fail when Tenable Security Center attempts to create the network, because there will already be a network in Tenable Vulnerability Management with the same name.

- Every asset list that you sync with Tenable Vulnerability Management must have a unique name, across all Tenable Security Center instances.

  If two asset lists in different Tenable Security Center instances have the same name, and you sync both asset lists with Tenable Vulnerability Management, the second asset list sync will fail due to duplicate tag names.

  Note: Unique asset list names are important because every organization in Tenable Security Center comes with the same default set of dynamic asset lists.

- You cannot sync a Tenable Security Center Director instance with Tenable Vulnerability Management. However, you can sync multiple managed Tenable Security Center instances with Tenable Vulnerability Management.

- To prevent sync issues due to overlapping IP addresses across repositories, enable **Network Support** in each Tenable Security Center instance. **Network Support** is enabled by default in Tenable Security Center. For more information, see [Network Support and Repository Overlap](#).

What data does synchronization include?

Tenable Security Center supports synchronizing:

- IPv4 addresses within dynamic assets and IPv4 addresses within static assets.

  > **Note:** You cannot synchronize IPv6 addresses within static assets. If an asset contains a mix of IPv4 and IPv6 addresses, Tenable Security Center synchronizes only the IPv4 addresses.

  > **Note:** You cannot synchronize non-IPv4 assets within dynamic assets. If a dynamic asset contains other asset types, Tenable Security Center synchronizes only the IPv4 addresses.

  > **Note:** You cannot synchronize DNS name list assets, LDAP query assets, combination assets, watchlist assets, or import assets.

- Active or agent cumulative database and scan result vulnerability data stored in IPv4, IPv6, agent, and universal repositories.

  The initial synchronization includes all cumulative database data from the repository. All subsequent synchronizations include only the new or modified scan result data imported to the repository.

  > **Note:** You cannot synchronize passive scan result vulnerability data. Tenable Security Center identifies vulnerability data by plugin family and excludes Tenable Network Monitor and LCE plugin families from synchronization.

  > **Caution:** To avoid data merge issues in Tenable Vulnerability Management, Tenable recommends enabling **Network Support** or resolving all repository overlaps before synchronizing data to Tenable Vulnerability Management. You cannot resolve data merge issues after synchronizing a repository with Tenable Vulnerability Management; you must enable **Network Support** or resolve overlapping repositories in Tenable Security Center before synchronizing a repository for the first time. For more information, see [Network Support and Repository Overlap](#).

Do I need to synchronize both data types (repositories and assets)?

Yes. In order to accurately assess your Cyber Exposure risk with Tenable Lumin, you must synchronize one or more asset lists and one or more repositories containing vulnerability data for those assets.

Should I resolve repository overlaps or enable **Network Support**?

If you first configured Tenable Lumin synchronization in Tenable Security Center 5.19.x or later, **Network Support** is enabled by default and cannot be disabled.

If you first configured Tenable Lumin synchronization in Tenable Security Center 5.18.x or earlier and upgraded to Tenable Security Center 5.19.x or later, you can decide to enable **Network Support** instead of resolving repository overlaps in the Tenable Security Center repositories you synchronize with Tenable Vulnerability Management. Contact your Tenable representative to enable **Network Support**.

> **Tip:** For the purpose of determining the default setting for **Network Support**, Tenable Lumin synchronization is configured if you have configured the **Tenable Connection Settings** and selected at least one repository to synchronize.

For more information, see [Network Support and Repository Overlap](#) and [Tenable One Synchronization](#).

How long does synchronization take to complete?

Vulnerability and asset data synchronize differently to Tenable Vulnerability Management.

Data	Synchronization Method	Timing
Vulnerability data	• Manual initial synchronization. • Automatic subsequent synchronizations when new scan result data imports to your synchronized	After you initiate a synchronization, Tenable Security Center immediately begins transferring data to Tenable Vulnerability Management. After 10-15 minutes, data begins appearing in Tenable Vulnerability Management. Newly transferred data does not immediately impact your Tenable Lumin

Data	Synchronization Method	Timing
	repositories.	metrics (for example, your CES). Tenable requires 4 to 6 hours to recalculate your metrics.
Asset data (*tags* in Tenable Vulnerability Management)	• Manual initial synchronization. • On-demand, automatic, or scheduled subsequent synchronizations, depending on your synchronization configuration.	All data and recalculated Tenable Lumin metrics appear in Tenable Vulnerability Management within 4 to 6 hours. Recalculated metrics appear in Tenable Security Center after the next daily retrieval.

To monitor the success or failure of synchronizations, see View Tenable One Synchronization Status and View Tenable One Data Synchronization Logs.

Which of my synchronized assets count toward my Tenable Vulnerability Management license?

Synchronized assets that count toward your Tenable Security Center license also count toward your Tenable Vulnerability Management license. For more information about Tenable Security Center asset counting, see License Requirements.

Where will I see synchronized data in Tenable Vulnerability Management?

You can view your synchronized data in both the Vulnerability Management and Tenable Lumin areas of Tenable Vulnerability Management.

Vulnerability Management

View your synchronized data on the **Assets** page. For more information, see View Assets in Tenable Vulnerability Management.

Tenable One

View your synchronized data on any Tenable One page. For more information, see [Tenable Lumin](#).

> **Tip:** To view limited metrics Tenable Security Center retrieves from Tenable Lumin in Tenable Vulnerability Management, see [View Tenable One Metrics](#).

Network Support and Repository Overlap

Two or more IPv4 repositories *overlap* if their specified **IP Ranges** contain intersecting IP addresses. To avoid data merge issues in Tenable Vulnerability Management, Tenable recommends enabling **Network Support** or resolving all repository overlaps before synchronizing data to Tenable Vulnerability Management.

While both methods avoid data merge issues, Tenable recommends enabling **Network Support** to support accurate tracking of assets in repositories with overlapping IPv4 addresses without manually resolving repository overlaps.

Synchronize Repositories to Individual Tenable Vulnerability Management Networks

> **Tip:** The default setting for **Network Support** depends on the Tenable Security Center version where you configured Tenable Lumin synchronization. For the purpose of determining the default setting for **Network Support**, Tenable Lumin synchronization is configured if you have configured the **Tenable Connection Settings** and selected at least one repository to synchronize.
>
> - Tenable Security Center 5.18.x or earlier — Disabled by default if Tenable Lumin is already configured.
>
> - Tenable Security Center 5.19.x or later — Enabled by default and cannot be disabled.

Because **Network Support** synchronizes each IPv4 and agent repository to its own individual network in Tenable Vulnerability Management, repositories with overlap do not cause data merge issues in Tenable Vulnerability Management.

For more information, see [Tenable One Synchronization Options](#).

Resolve Repository Overlaps

If **Network Support** is disabled and you do not plan to enable it, you must resolve repository overlaps before synchronizing new repositories to Tenable Vulnerability Management.

To resolve an overlap between two repositories, edit the repository configurations and reconfigure the **IP Ranges** to avoid intersecting IP addresses, as described in [IPv4/IPv6 Repositories](#).

> **Caution:** You cannot resolve data merge issues after synchronizing a repository with Tenable Vulnerability Management; you must enable **Network Support** or resolve overlapping repositories in Tenable Security Center before synchronizing a repository for the first time.

If you cannot resolve all overlaps and you do not want to enable **Network Support**, plan to synchronize a limited number of repositories to avoid conflicts. For example, to avoid a conflict between two repositories, synchronize one repository but not the other repository.

Configure Tenable One Synchronization

> **Required Additional License:** Tenable Lumin

> **Required Tenable Security Center User Role:** Administrator
>
> **Required Tenable Vulnerability Management User Role:** Administrator

You can configure Tenable Security Center to send limited Tenable Security Center data to Tenable Vulnerability Management for use in Tenable One analysis. For more information, see [Tenable One Synchronization](#).

Before you begin:

- License and enable Tenable Lumin in Tenable Vulnerability Management, as described in [License and Enable Tenable Lumin](#) in the *Tenable Vulnerability Management User Guide*.

- Plan your synchronization strategy and review known limitations and dependencies, as described in [Plan Your Tenable One Synchronization](#).

- Note that Tenable Security Center repositories are not case-sensitive, but networks in Tenable Vulnerability Management are case-sensitive. When you synchronize a repository, ensure that the name is unique from any existing Tenable Vulnerability Management networks.

- Plan your strategy for avoiding data merge issues and perform any required cleanup, as described in [Network Support and Repository Overlap](#).

> **Caution:** You cannot resolve data merge issues after synchronizing a repository with Tenable Vulnerability Management; you must enable **Network Support** or resolve overlapping repositories in Tenable Security Center before synchronizing a repository for the first time.

- Generate Tenable Vulnerability Management API keys for a Tenable Vulnerability Management user with Administrator permissions, as described in Generate API Keys in the *Tenable Vulnerability Management User Guide*.

- Share assets that you want to synchronize with the **Full Access** group, as described in Groups. You cannot synchronize assets that are not shared with the Full Access group.

To configure data synchronization between Tenable Security Center and Tenable One in Tenable Vulnerability Management:

1. Log in to Tenable Security Center via the user interface.

2. Click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **Tenable One** tile.

   The **Tenable One Configuration** page appears.

4. In the **Tenable Vulnerability Management Connection Settings** section, type an **Access Key** and **Secret Key** for the Tenable Vulnerability Management user you want to have full access to your data in Tenable Vulnerability Management. For more information, see Tenable One Synchronization Options.

   Tenable Security Center validates the connection to Tenable Vulnerability Management and locks the key configuration.

5. (Optional) To test the connection to Tenable Vulnerability Management, click **Test Connection**.

   Tenable Security Center tests the connection to Tenable Vulnerability Management using the access key and secret key you provided.

   Tenable Security Center displays a notification indicating the status of the connection to Tenable Vulnerability Management.

6. (Optional) In the **Tenable One URL** box, modify the URL for Tenable One. By default, the URL is *cloud.tenable.com*.

7. In the **Vulnerability Data Synchronization** section:

   a. (Optional) If you did not enable **Network Support** and you want to synchronize each Tenable Security Center repository to its own network in Tenable Vulnerability Management, contact your Tenable representative to enable **Network Support**. For more information, see Tenable One Synchronization Options.

   > **Note:** Once enabled, you cannot disable **Network Support**.

   b. Select one or more repositories that contain the scan result data you want to synchronize with Tenable Vulnerability Management.

      The initial synchronization includes all cumulative database data from the repository. All subsequent synchronizations include only the new or modified scan result data imported to the repository.

   > **Note:** You cannot synchronize passive scan result vulnerability data. Tenable Security Center identifies vulnerability data by plugin family and excludes Tenable Network Monitor and LCE plugin families from synchronization.

   > **Caution:** To avoid data merge issues in Tenable Vulnerability Management, Tenable recommends enabling **Network Support** or resolving all repository overlaps before synchronizing data to Tenable Vulnerability Management. You cannot resolve data merge issues after synchronizing a repository with Tenable Vulnerability Management; you must enable **Network Support** or resolve overlapping repositories in Tenable Security Center before synchronizing a repository for the first time. For more information, see Network Support and Repository Overlap.

   > **Tip:** Hover over the ⓘ to view details for a repository (including information about unresolved repository overlaps).

   c. Click **Synchronize**.

      A confirmation window appears.

   d. Click **Synchronize**.

Tenable Security Center begins synchronizing your vulnerability data to Tenable Vulnerability Management.

8. In the **Asset to Tag Synchronization** section:

   a. If you want to synchronize asset data at a scheduled time:

      i. Click to enable the **Custom Schedule** slider.

      ii. Next to the schedule link, click the ✎ button.

      iii. Modify the **Time** and **Timezone** options to specify when you want synchronizations to occur.

      > **Tip:** You cannot modify the **Frequency** or **Repeat Every** options; all Tenable One synchronizations occur once daily.

      If you do not schedule your asset synchronizations, Tenable Security Center automatically synchronizes once daily, after business hours for your local time zone.

   b. If you want to filter the assets that appear in the **Unstaged Assets** section, do any of the following:

      - Select an organization from the **Organization Filter** drop-down list and click **Apply Filters**.

      - Select an asset type from the **Asset Type Filter** drop-down list and click **Apply Filters**.

      - Type an asset name in the **Search Name** box and press **Enter**.

      > **Note:** You can only synchronize assets shared with the **Full Access** group. You cannot synchronize assets with more limited sharing.

      Tenable Security Center applies your filter to the **Unstaged Assets** section.

   c. To stage one or more assets for synchronization, do one of the following:

- Click the **Add All** button to stage all visible assets for synchronization.

  Tenable Security Center stages all visible assets for synchronization and displays them in the **Staged Assets** section.

- In the rows for individual assets you want to stage for synchronization, click the ✚ button.

  Tenable Security Center stages your selected assets for synchronization and displays them in the **Staged Assets** section.

> **Note:** You cannot synchronize IPv6 addresses within static assets. If an asset contains a mix of IPv4 and IPv6 addresses, Tenable Security Center synchronizes only the IPv4 addresses.

> **Note:** You cannot synchronize non-IPv4 assets within dynamic assets. If a dynamic asset contains other asset types, Tenable Security Center synchronizes only the IPv4 addresses.

> **Note:** You cannot synchronize DNS name list assets, LDAP query assets, combination assets, watchlist assets, or import assets.

> **Tip:** Click an asset row to view details for an asset.

d. Click **Synchronize Staged Assets**.

A confirmation window appears.

e. Click **Synchronize**.

Tenable Security Center begins synchronizing your assets to Tenable Vulnerability Management.

9. Wait for data transfer and Tenable One data calculations to complete. For more information, see How long does synchronization take to complete?.

10. Monitor the synchronization and confirm there were no errors, as described in View Tenable One Synchronization Status or View Tenable One Data Synchronization Logs.

What to do next:

- Begin using Tenable Vulnerability Management and Tenable One, as described in Where will I see synchronized data in Tenable Vulnerability Management?.

- View Tenable One metrics information within Tenable Security Center, as described in View Tenable One Metrics.

- By default, synchronized data is visible to the Tenable Vulnerability Management Administrator account used for synchronization and to all other users in Tenable Vulnerability Management. If you want to restrict privileges for synchronized data, configure access groups as described in Access Groups in the *Tenable Vulnerability Management User Guide*.

View Tenable One Synchronization Status

Required Additional License: Tenable Lumin

Required Tenable Security Center User Role: Administrator

After you configure Tenable Security Center data synchronization to Tenable One in Tenable Vulnerability Management, you can view the status of your synchronizations.

For information about viewing logs for past synchronizations, see View Tenable One Data Synchronization Logs.

Before you begin:

- Configure Tenable One synchronization, as described in Configure Tenable One Synchronization.

To monitor the status of your data synchronization between Tenable Security Center and Tenable One in Tenable Vulnerability Management:

1. Log in to Tenable Security Center via the user interface.

2. Click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the Tenable One tile.

   The **Tenable One Configuration** page appears.

4. In the **Vulnerability Data Synchronization** section:

- View the **Last Successful Sync** date and time for data from any repository.

- View details for a repository by hovering over the ⓘ that appears when you hover over a repository name:

Data	Description
Name	The repository name.
Format	The repository type: **IPv4/IPv6**, **Agent**, or **Universal**.
First Successful Synchronization	The date and time of the first synchronization of this repository.
Last Successful Synchronization	The date and time of the most recent synchronization of this repository.
Error Status	If the most recent synchronization of this repository failed, a description of the failure.
Last Failed Synchronization	The date and time of the most recent failed synchronization of this repository.
Repositories Overlapping with *<Repository Name>*	The names of other repositories with **IP Ranges** that overlap this repository. For more information, see Network Support and Repository Overlap.

5. In the **Asset to Tag Synchronization** section:

- In the **Unstaged Assets** or **Staged Assets** section, click an asset row to view details for an asset:

Data	Description
Description	The asset description.
First Sync Success	The date and time of the first synchronization of this asset.
Last Sync Success	The date and time of the most recent synchronization of this asset.
Last Sync Failure	The date and time of the most recent failed synchronization of this asset.
Sync Error	If the most recent synchronization of this asset failed, a description of the failure.

- View the **Last Successful Sync** date and time for any asset data.

Disable Tenable One Synchronization

Required Additional License: Tenable Lumin

Required Tenable Security Center User Role: Administrator

When you disable Tenable One synchronization, Tenable Security Center stops synchronizing new or updated scan result and asset data with Tenable One in Tenable Vulnerability Management. Existing Tenable Security Center data remains visible in Tenable Vulnerability Management.

To stop synchronizing data with Tenable One in Tenable Vulnerability Management:

1. Log in to Tenable Security Center via the user interface.

2. Click **System** > **Configuration**.

   The **Configuration** page appears.

3. Click the **Tenable One** tile.

   The **Tenable One Configuration** page appears.

4. In the **Vulnerability Data Synchronization** section:

   a. Deselect all of your repositories.

   b. Click **Synchronize**.

      Tenable Security Center stops synchronizing vulnerability data to Tenable Vulnerability Management. Existing Tenable Security Center data remains visible in Tenable Vulnerability Management.

5. In the **Asset to Tag Synchronization** section:

   a. In the **Staged Assets** section, click **Remove All**.

      All staged assets move to the **Unstaged Assets** section.

   b. Click **Synchronize Staged Assets**.

      Tenable Security Center stops synchronizing asset data to Tenable Vulnerability Management. Existing Tenable Security Center data remains visible in Tenable Vulnerability Management.

Configure Scans

See the following sections to configure Tenable Security Center scans.

- [Scanning Overview](#)

- [Resources](#)

- [Repositories](#)

- [Active Scans](#)

- [Active Scan Objects](#)

- [Agent Scans](#)

- [Agent Scanning](#)

- [Freeze Windows](#)

- [Patch Management](#)

Scanning Overview

You can perform two types of scans using Tenable products: *discovery scans* and *assessment scans.* Tenable recommends performing discovery scans to get an accurate picture of the assets on your network and assessment scans to understand the vulnerabilities on your assets.

Configuring both methods provides a comprehensive view of the organization's security posture and reduces false positives. For more information about Tenable Security Center scanning strategies, see the [Tenable Security Center Scan Tuning Guide](#).

Scan Type	Description	Licensing
Discovery Scan	Find assets on your network. For example: • a scan configured with the **Host Discovery** template. • a scan configured to use only discovery plugins. • an [Tenable Network Monitor instance in discovery mode](#).	Assets identified by discovery scans do not count toward your license.

Assessment Scan	Find vulnerabilities on your assets. For example:	In general, assets assessed by assessment scans count toward your license.
	• an *authenticated* or *unauthenticated* [active scan](#) using a Tenable Nessus or Tenable Vulnerability Management scanner.	
	• an [agent scan](#) using an agent-capable Tenable Vulnerability Management or Tenable Nessus Manager scanner.	
	Authenticated Active Scans	
	Configure authenticated scans, also known as credentialed scans, by adding access credentials to your assessment scan configuration.	
	Credentialed scans can perform a wider variety of checks than non-credentialed scans, which can result in more accurate scan results. This facilitates scanning of a very large network to determine local exposures or compliance violations.	
	Credentialed scans can perform any operation that a local user can perform. The level of scanning depends on the privileges granted to the user account. The more privileges the scanner has via the login account (e.g., root or administrator access), the more thorough the scan results.	
	For more information, see [Credentials](#).	
	Unauthenticated Active Scans	
	If you do not add access credentials to your assessment scan configuration, Tenable Vulnerability Management performs a limited number of checks when scanning your assets.	

For more information about how discovered and assessed assets are counted towards your license, see [License Requirements](#).

Resources

Administrator users can configure supporting resources.

- Tenable Nessus Scanners

- Tenable Network Monitor Instances

- Tenable Log Correlation Engines

- Tenable Log Correlation Engine Clients

- Tenable Log Correlation Engine Client Policies

- OT Security Instances

Scan zone resources are considered active scan objects. For more information, see Active Scan Objects and Scan Zones.

LDAP server resources are part of user account configuration. For more information, see User Accounts and LDAP Authentication.

Tenable Nessus Scanners

For high level information about active and agent scanning, see Active Scans and Agent Scans.

In the Tenable Security Center framework, the Tenable Nessus scanner behaves as a server, while Tenable Security Center serves as a client that schedules and initiates scans, retrieves results, reports results, and performs a wide variety of other important functions.

You can add one or more Tenable Nessus or Tenable Vulnerability Management deployments to Tenable Security Center as Tenable Nessus scanners in Tenable Security Center:

- Managed or unmanaged Tenable Nessus scanners

  > **Note:** Tenable Security Center cannot perform scans with or update plugins for scanners running unsupported versions of Tenable Nessus. For minimum Tenable Nessus scanner version requirements, see the Tenable Security Center Release Notes for your version.

- Tenable Nessus Manager instances

Note: If you enabled clustering on Tenable Nessus Manager, add the parent node of the cluster to Tenable Security Center. For more information, see Clustering in the *Tenable Nessus User Guide*.

- Tenable Vulnerability Management instances

For more information, see:

- Add a Tenable Nessus Scanner

- Add a Tenable Vulnerability Management Scanner

- Manage Nessus Scanners

- View Your Nessus Scanners

- View Details for a Nessus Scanner

- Delete a Nessus Scanner

- View Tenable Nessus Instances in Tenable Security Center

For information about Tenable Security Center-Tenable Nessus and Tenable Security Center-Tenable Vulnerability Management communications encryption, see Encryption Strength.

Tenable Nessus Scanner Settings

Option	Description
General	
Name	A descriptive name for the scanner.
Description	A scanner description, location, or purpose.
Host	The hostname or IP address of the scanner.
Port	The TCP port that the scanner listens on for communications from Tenable Security Center. The default is port 8834.
Enabled	A scanner may be **Enabled** or **Disabled** within Tenable Security Center to allow or prevent access to the scanner.
Verify Hostname	Adds a check to verify that the hostname or IP address entered in the **Host** option matches the CommonName (CN) presented in the SSL

Option	Description
	certificate from the Nessus server. **Note:** Confirm that the correct CA certificate is configured for use by Tenable Security Center. If you are using a custom CA, configure Tenable Security Center to trust your custom CA, as described in Trust a Custom CA. You do not need to perform this step when using the default certificates for Tenable Nessus servers.
Use Proxy	Instructs Tenable Security Center to use its configured proxy for communication with the scanner.
Authentication	
Type	Select **Password**, **SSL Certificate**, or **API Keys** for the authentication type to connect to the scanner. For complete information about Tenable Nessus SSL certificate authentication, see Manual Tenable Nessus SSL Certificate Exchange.
Username	Username generated during the install for daemon to client communications. This must be an administrator user in order to send plugin updates to the scanner. If the scanner is updated by a different method, such as through another Tenable Security Center, a standard user account may be used to perform scans. This option is only available if the **Authentication Type** is set to **Password**.
Password	The login password must be entered in this option. This option is only available if the **Authentication Type** is set to **Password**.
Certificate	If you set **Authentication Type** to **SSL Certificate**, specifies the `nessuscert.pem` file you want to use for authentication to the scanner. For complete information about Tenable Nessus SSL certificate authentication, see Manual Tenable Nessus SSL Certificate Exchange.
Certificate Passphrase	If you selected **SSL Certificate** as the **Authentication Type** and the private key that decrypts your SSL certificate is encrypted with a passphrase, the passphrase for the private key.

Option	Description
Active Scans	
Zones	The scan zones that can use this scanner. For more information, see Scan Zones.
Agents	
Agent Capable	Specifies whether you want this scanner to provide Tenable Agent scan results to Tenable Security Center. Agent capable scanners must be either Tenable Vulnerability Management or Nessus Manager 6.5 or later. When using Nessus Manager, you must use an organizational user account to connect from Tenable Security Center.
Organizations	When the **Agent Capable** option is enabled, or you select **API Keys** as the **Authentication Type**, specifies one or more organizations that you want to grant access to import Tenable Agent data into Tenable Security Center.
API Keys	When the **Agent Capable** option is enabled, specifies whether you want to use secure API keys when importing agent scan data from Tenable Nessus or Tenable Vulnerability Management scanners. For more information about retrieving your access key and secret key from Tenable Nessus and Tenable Vulnerability Management, see Generate a Nessus API Key in the *Tenable Nessus User Guide* and Generate a Tenable Vulnerability Management API Key in the *Tenable Vulnerability Management User Guide*.
Access Key	When the **API Keys** option is enabled, specifies the access key for the Tenable Nessus or Tenable Vulnerability Management scanner. When you select **API Keys** as the **Authentication Type**, specifies the access key for the Tenable Agent.
Secret Key	When the **API Keys** option is enabled, specifies the secret key for the Tenable Nessus or Tenable Vulnerability Management scanner.

Option	Description
	When you select **API Keys** as the **Authentication Type**, specifies the secret key for the Tenable Agent.
Web Application Scanning	
Capable	Specifies whether you want this scanner to provide Tenable Web App Scanning scan results to Tenable Security Center.

Add a Tenable Nessus Scanner

Required Tenable Security Center User Role: Administrator

For more information, see Tenable Nessus Scanners.

Note: Tenable Security Center cannot perform scans with or update plugins for scanners running unsupported versions of Tenable Nessus. For minimum Tenable Nessus scanner version requirements, see the Tenable Security Center Release Notes for your version.

Note: Tenable Security Center does not send plugins to linked Nessus Managers. Nessus Manager pulls plugins directly from Tenable's plugin sites. Therefore, to update plugin sets, Nessus Manager needs access to the internet and Tenable's plugin sites (for more information, see the Which Tenable sites should I allow? community article). If your Nessus Manager does not have internet access, you can manually update its version and plugins offline (for more information, see Manage Nessus Offline in the *Nessus User Guide*).

To add a Tenable Nessus scanner to Tenable Security Center:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, 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, as described in Tenable Nessus Scanners.

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.

I. If you want this scanner to provide Tenable 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 Agent data into Tenable Security Center.

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

        a. Click **API Keys** to enable the toggle.

        b. In the **Access Key** box, type the access key.

        c. 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, as described in [Active Scans](#).

Add a Tenable Vulnerability Management Scanner

> **Required Tenable Security Center User Role:** Administrator

> **Required Tenable Vulnerability Management User Role:** VM Scan Operator, VM Standard, VM Scan Manager, or Administrator

Tenable Security Center supports the use of Tenable Vulnerability Management as a Tenable Nessus scanner within Tenable Security Center. Tenable Vulnerability Management is an enterprise-class remote vulnerability scanning service you can use to audit internet-facing IP addresses for both network and web application vulnerabilities from the cloud. While Tenable Security Center does not manage Tenable Vulnerability Management scanners (for example, Tenable Security Center does not push plugins to the scanner), you can add Tenable Vulnerability Management scanners to Tenable Security Center the same way you add internal, local, or remote Tenable Nessus scanners.

Before you begin:

- Confirm that you have a valid, active Tenable Vulnerability Management subscription.

To add Tenable Vulnerability Management to Tenable Security Center as a Tenable Nessus scanner:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Tenable Nessus Scanners**.

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

Add Nessus Scanner

General

Name*   Nessus Cloud

Description

Host*   cloud.tenable.com

Port*   443

Enabled

Verify Hostname

Use Proxy

Authentication

Type   Password ▾

Username*   username@example.com

Password*   ••••••••••••••

Active Scans

Zones   Search 🔍

    ☐ Default Scan Zone

Agents

Agent Capable

Submit   Cancel

4. Configure Tenable Nessus scanner options, as described in Tenable Nessus Scanners. You use Tenable Vulnerability Management-specific values for some settings.

Option	Value for a Tenable Vulnerability Management Configuration
Host	• Commercial Tenable Vulnerability Management: *cloud.tenable.com* • Tenable Vulnerability Management FedRAMP: *fedcloud.tenable.com*
Port	443
Username	The username for an active Tenable Vulnerability Management user account.
Password	The password for an active Tenable Vulnerability Management user account.
Zones	The zones within Tenable Security Center that use Tenable Vulnerability Management as a scanner.

5. Click **Submit**.

> **Note:** Existing scan reports from Tenable Vulnerability Management are not automatically available in Tenable Security Center. However, you can manually download and import them into Tenable Security Center.

> **Note:** By default, Tenable Vulnerability Management selects the regional scanner that corresponds with the location of your Tenable Vulnerability Management user account. For example, if you run a scan from a user account located in the United States, Tenable Vulnerability Management selects the United States scanner. If you run a scan from a user account in Germany, Tenable Vulnerability Management selects the Germany scanner.

What to do next:

• Configure a scan zone, repository, and active scan objects, as described in Active Scans.

Tenable Nessus Scanner Statuses

You can view the status for scanners, as described in View Your Nessus Scanners.

Status	Description	Recommended Action
Authentication Error	Tenable Security Center could not authenticate to the scanner	Check your scanner configuration settings and confirm the **Username**

	using the credentials you provided.	and **Password** options specify valid login credentials for the scanner.
Certificate Mismatch	Tenable Security Center could not confirm the validity of the SSL certificate presented by the scanner.	Do one of the following: • [Edit your scanner configuration](#) and select a different authentication type. • (Tenable Nessus scanners only) Check your [scanner configuration settings](#) and confirm the **Certificate** option specifies the correct `nessuscert.pem` file. For more information about managing SSL certificates in Nessus, see [Manage SSL Certificates](#) in the *Tenable Nessus User Guide*.
Connection Error	Tenable Security Center cannot connect to the scanner because the scanner is unreachable or does not exist at the IP address or hostname provided.	Do one or both of the following: • [Check your scanner configuration](#) and confirm the **Host** option specifies the correct IP address or hostname for the scanner. • Confirm the network devices and firewalls between Tenable Security Center and the scanner are configured to permit network traffic.
Connection Timeout	Tenable Security Center connected to the scanner but timed out waiting for a reply.	Contact your network administrator for troubleshooting assistance.

Invalid Configuration	The scanner attempted to connect to a scanner on port 0, or the provided API key is for a scanner that does not support agent scans.	Do one or both of the following: • Check your scanner configuration and confirm the **Port** option specifies a valid TCP port to connect to your scanners. For more information, see Port Requirements. • Check your scanner configuration and confirm the **Access Key** and **Secret Key** options specify valid keys for a Tenable Nessus Manager or cloud scanner.
Permission Error	The provided API keys do not have the correct permissions to run agent scans.	Check your scanner configuration and confirm the **Access Key** and **Secret Key** options specify valid keys for the scanner.
Plugins Out of Sync	The plugin sets on the scanner do not match the plugin sets in Tenable Security Center.	For troubleshooting assistance, see the knowledge base article.
Protocol Error	Tenable Security Center connected to the scanner but the scanner returned an HTTPS protocol negotiation error.	Contact your network administrator for troubleshooting assistance.
Reloading Scanner	The scanner is temporarily unable to run scans because Tenable Nessus is restarting on the scanner.	None.
Updating Plugins	Tenable Security Center is performing a plugin update on	You may want to schedule plugin updates to run a few hours before

	the scanner.	your scheduled scans. For more information, see Edit Plugin and Feed Settings and Schedules.
		If a scanner has a persistent **Updating Plugins** status, the plugin update have been interrupted. For troubleshooting assistance, see the knowledge base article.
Updating Status	Tenable Security Center is refreshing the status of the scanner. Scanners can continue to run scans while Tenable Security Center refreshes the status. **Note:** Tenable Security Center automatically refreshes scanner statuses every 15 minutes. If you create a new scanner, edit a scanner, or manually refresh the status using the **Update Status** option, Tenable Security Center refreshes the status of the scanner on demand.	None.
Upgrade Required	The version of Tenable Nessus on the scanner is unsupported and requires an upgrade. Tenable Security Center cannot perform scans with or update plugins for scanners running unsupported versions of Tenable Nessus. For minimum Tenable	Upgrade to a supported version of Tenable Nessus, as described in Upgrade Nessus in the *Tenable Nessus User Guide*.

	Nessus scanner version requirements, see the [Tenable Security Center Release Notes](#) for your version.	
User Disabled	A Tenable Security Center user disabled the scanner.	[Edit your scanner configuration](#) and click the **Enabled** toggle to re-enable the scanner. For more information about scanner options, see [Tenable Nessus Scanners](#).
Working	The scanner is connected to Tenable Security Center and able to run scans.	None.

Manage Nessus Scanners

> **Required Tenable Security Center User Role:** Administrator

For more information, see [Tenable Nessus Scanners](#).

To manage your Tenable Nessus scanners:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Tenable Nessus Scanners**.

   The **Tenable Nessus Scanners** page appears.

3. To filter the scanners that appear on the page, apply a filter as described in [Apply a Filter](#).

4. To view the list of configured scanners, see [View Your Nessus Scanners](#).

5. To view details for a scanner, see [View Details for a Nessus Scanner](#).

6. To edit a scanner:

a. Right-click the row for the scanner.

The actions menu appears.

-or-

Select the check box for the scanner.

The available actions appear at the top of the table.

b. Click **More** > **Edit**.

The **Edit Tenable Nessus Scanner** page appears.

c. Modify the scanner options. For more information about scanner options, see Tenable Nessus Scanners.

d. Click **Submit**.

7. To download logs for a scanner, see Download Tenable Nessus Scanner Logs.

8. To delete a scanner, see Delete a Nessus Scanner.

View Your Nessus Scanners

Required Tenable Security Center User Role: Administrator

For more information, see Tenable Nessus Scanners.

To view a list of configured Tenable Nessus scanners:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Tenable Nessus Scanners**.

The **Tenable Nessus Scanners** page appears.

3. View details about each Tenable Nessus scanner.

- **Name** — The name for the scanner.

- **Features** — Specifies whether the scanner is a **Standard** scanner or an **Agent Capable** scanner. Agent capable scanners provide Tenable Agent scan results to Tenable Security Center.

- **Status** — The status of the scanner. For more information, see [Tenable Nessus Scanner Statuses](#).

- **Host** — The IP address or hostname of the scanner.

- **Version** — The scanner's Tenable Nessus version.

- **Type** — The type of scanner connection.

Type	Description
Unknown	Tenable Security Center could not identify the scanner.
Nessus (Unmanaged Plugins)	Tenable Security Center accesses the scanner using a Tenable Nessus user account with **Standard** permissions. Tenable Security Center cannot send plugin updates to the scanner or manage the scanner's activation code.
Nessus (Managed Plugins)	Tenable Security Center manages the scanner and authenticates via a Tenable Nessus user account. Tenable Security Center sends plugin updates to the scanner and manages the scanner's activation code.
Tenable (Unmanaged Plugins)	Tenable Security Center accesses the instance using a Tenable Vulnerability Management user account with **Standard** permissions. Tenable Security Center cannot send plugin updates to the instance or manage the instance's activation code.

- **Uptime** — The length of time, in days, that the scanner has been running.

- **Last Modified** — The date and time the scanner was last modified.

4. To view details of a specific Tenable Nessus scanner, see [View Details for a Nessus Scanner](#).

5. To filter the scanners that appear on the page, apply a filter as described in [Apply a Filter](#).

6. To manually refresh the **Status** data, at the top of the table, click **Update Status**.

   Tenable Security Center refreshes the **Status** data.

View Details for a Nessus Scanner

> **Required Tenable Security Center User Role:** Administrator

For more information, see [Tenable Nessus Scanners](#).

To view details for a Tenable Nessus scanner:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Tenable Nessus Scanners**.

   The **Tenable Nessus Scanners** page appears.

3. Right-click the row for the scanner you want to view.

   The actions menu appears.

   -or-

   Select the check box for the scanner you want to view.

   The available actions appear at the top of the table.

4. Click **View**.

   The **View Tenable Nessus Scanner** page appears.

Section	Action
Options drop-down box	• To edit the scanner, click **Edit**. • To delete the scanner, click **Delete**, as described in [Delete a Nessus Scanner](#). • To download logs for the scanner, click **Download Logs**. For more information, see [Download Tenable Nessus Scanner Logs](#).
General	View general information about the scanner.
Authentication	View authentication information for the scanner.
Active Scans	View active scan information for the scanner.
Agents	View agent information for the scanner.

Section	Action
	• **Agent Capable** — Specifies whether the scanner is agent capable: **Yes** or **No**. • **Organizations** — If the scanner is agent capable, the organization configured for the scanner. • **API Keys Set** — If the scanner is agent capable, specifies whether API keys are configured for the scanner: **Yes** or **No**.
Data summary	View metadata and performance metrics for the scanner. **Note:** Tenable Security Center refreshes the load information every 15 minutes.
Nessus Scanner Health	If you are viewing details for a managed Tenable Nessus scanner running version 8.2.0 or later, view scanner health summary data: • **Running Scans** — The number of scans currently running on the scanner. • **Hosts Being Scanned** — The number of hosts currently being scanned by the scanner. • **CPU Load** — The percent of the total CPU currently in use by the scanner. • **Total Memory** — The total memory installed on the scanner. • **Memory Used** — The percent of the total memory currently in use by the scanner. • **Total Disk Space** — The total disk space installed on the scanner. • **Disk Space Used** — The percent of the total disk space currently in use by the scanner. • **Last Updated** — The date and time Tenable Security Center

Section	Action
	last updated the scanner data.
	Tenable Security Center refreshes the data when you load the **View Nessus Scanner** page. To force a manual refresh, click the ⟳ button.

View Tenable Nessus Instances in Tenable Security Center

Required Tenable Security Center User Role: Administrator

Administrators can view and manage Tenable Nessus scanner configurations from the Tenable Security Center user interface. For more information about Tenable Nessus scanners in Tenable Security Center, see Tenable Nessus Scanners.

Note: You cannot use **Picture in Picture** with a Tenable Nessus scanner if you enabled **Use Proxy** for the scanner or if the scanner's **Authentication Type** is **SSL Certificate**. For more information, see Tenable Nessus Scanner Settings.

Before you begin:

- Enable **Picture in Picture**, as described in Enable Picture in Picture.

To view Tenable Nessus instances inside the Tenable Security Center user interface:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Tenable Nessus Scanners**.

    The **Tenable Nessus Scanners** page appears.

3. Right-click the row for the Tenable Nessus scanner.

    The actions menu appears.

    -or-

    Select the check box for the Tenable Nessus scanner.

    The available actions appear at the top of the table.

4. Click **Manage System**.

   The Tenable Nessus instance opens inside the Tenable Security Center user interface.

What to do next:

- Manage your Tenable Nessus scanner configurations using the picture in picture window in Tenable Security Center. For more information about Tenable Nessus and Tenable Nessus settings, see the *Tenable Nessus User Guide.*

- To exit the Picture in Picture view, in the upper-right corner, click **Back**.

Download Tenable Nessus Scanner Logs

Required Tenable Security Center User Role: Administrator

You can download a log file for Tenable Nessus scanners managed by Tenable Security Center. The Tenable Nessus scanner must be running version 8.0.0 or later to send logs to Tenable Security Center for download.

All Tenable Nessus scanner logs include:

- Recent Tenable Nessus log data

- System information (operating system version, CPU statistics, available memory, available disk space, etc.)

- Troubleshooting data

If you include extended logs, the system also downloads recent Tenable Nessus web server log records, system log data, and network configuration information.

To download logs for a Tenable Nessus scanner:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Nessus Scanners**.

   The **Nessus Scanners** page appears.

3. Right-click the row for the scanner for which you want to download logs.

   The actions menu appears.

-or-

Select the check box for the scanner for which you want to download logs.

The available actions appear at the top of the table.

4. Click **Download Logs**.

   The **Download Nessus Scanner Logs** window appears.

5. To include recent Tenable Nessus web server log records, system log data, and network configuration information, click to enable the **Extended Logs** toggle.

6. To hide the first two octets of IPv4 addresses within the logs, click to enable the **Sanitize IPs** toggle.

7. Click **Download**.

   Tenable Security Center downloads the `tar.gz` file in your browser.

   > **Tip:** If you use 7-Zip to extract the `tar.gz` file, you may see the following error message: `There are some data after the end of the payload data.` You can safely ignore this error.

Delete a Nessus Scanner

> **Required Tenable Security Center User Role:** Administrator

For more information, see [Tenable Nessus Scanners](#).

To delete a Tenable Nessus scanner:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Nessus Scanners**.

   The **Nessus Scanners** page appears.

3. Select the scanner you want to delete:

   ### To delete a single scanner:

a. In the table, right-click the row for the scanner you want to delete.

The actions menu appears.

b. Click **Delete**.

To delete multiple scanners:

a. In the table, select the check box for each scanner you want to delete.

The available actions appear at the top of the table.

b. At the top of the table, click **More** > **Delete**.

A confirmation window appears.

4. Click **Delete**.

Tenable Security Center deletes the scanner.

Web Application Scanners

For high level information about web application scanning, see [Web App Scans](#).

To view your web application scanners, in the left navigation, click **Resources** > **Web Application Scanners**. If your deployment includes Web Application Scanning, you can add and configure web app scanners on the **Web Application Scanners** tab.

For more information, see:

- [Add a Web Application Scanner](#)

Add a Web Application Scanner

Required Tenable Security Center User Role: Administrator

Before you begin

- Add a [Sensor Proxy](#).

To add a Tenable Web App Scanning instance to Tenable Security Center:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Resources** > **Web Application Scanners**.

   The **Web Application Scanners** page appears.

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

   The **Add Web Application Scanner** panel appears.

4. Configure the Web Application Scanner.

   a. In the **Linking Key** section, click **Copy** to copy the linking key to your clipboard.

   b. Configure the Web Application Scanner, as described in [Web App Scans](#).

   c. Start the Docker container using the following command, where:

      - **<scanner_name>** is a unique name for the scanner.

      - **<SP_URL>** is the Sensor Proxy URL.

      - **<linking_key>** is the linking key you copied in step 4a.

      ```
      docker run -d -e WAS_SCANNER_NAME=<scanner_name> -e WAS_PLATFORM_URL=<SP_URL> -e WAS_
      LINKING_KEY=<linking_key> tenable/was-scanner:latest
      ```

   Additional Docker variables

   The following are some helpful variables you can set in your Docker container.

   - ```
     -e SCANNER_MEM_REQUEST=<docker_memory>
     ```

     Where **<docker_memory>** is the amount of memory the Docker container can use (for example, *5G* or *256M*).

   - ```
     -e WAS_LOG_TO_STDOUT=true -e WAS_LOG_LEVEL=debug
     ```

     These variables produce more detailed logs when you run a web app scan.

5. The scanner appears in the Web Application Scanners table.

What to do next:

- Before you use a Web Application Scanner, add the scanner to a [Scan Zones](#).

Tenable Network Monitor Instances

Tenable Network Monitor (Tenable Network Monitor) 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. Tenable Network Monitor 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, Tenable Network Monitor behaves like a security motion detector on the network.

Tenable Security Center communicates with Tenable Network Monitor utilizing the XMLRPC protocol on port 8835 by default. For information about Tenable Security Center-Tenable Network Monitor communications encryption, see [Encryption Strength](#).

> **Note:** It is important for you to restrict the data Tenable Network Monitor collects to only the desired IP address ranges. For example, if your attached Tenable Network Monitor collects information on 1100 hosts and Tenable Security Center is licensed for 1000 hosts, Tenable Security Center imports all of the Tenable Network Monitor data and indicates that you exceeded your host count. For more information, see [License Requirements](#).

Tenable Security Center will ask Tenable Network Monitor 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.

To fully configure passive scan data retrieval from Tenable Network Monitor:

1. Configure Tenable Network Monitor, as described in [Get Started](#) in the *Tenable Network Monitor User Guide*.

2. Add your Tenable Network Monitor license to Tenable Security Center, as described in [Apply a New License](#).

3. Add an IPv4, IPv6, or Universal repository for Tenable Network Monitor data in Tenable Security Center, as described in [Add a Repository](#).

4. Add an Tenable Network Monitor instance in Tenable Security Center, as described in [Add a Tenable Network Monitor Instance](#).

5. (Optional) Configure Tenable Network Monitor plugin import schedules, as described in [Edit Plugin and Feed Settings and Schedules](#). By default, Tenable Security Center checks for new

passive vulnerability plugins every 24 hours and pushes them to your attached Tenable Network Monitor instances.

What to do next:

- View vulnerability data filtered by your Tenable Network Monitor repository, as described in [Vulnerability Analysis](#).

Considerations for Licensing

If you want Tenable Security Center to push plugin updates to Tenable Network Monitor, you must add the product activation code to Tenable Security Center. For more information, see [Apply a New License](#).

For detailed information about plugins counted toward the Tenable Security Center license count, see [License Requirements](#).

Considerations for Tenable Network Monitor Discovery Mode

Your Tenable Network Monitor instances can run in two modes: discovery mode disabled and discovery mode enabled. For more information, see [NNM Settings](#) in the *Tenable Network Monitor User Guide*.

If discovery mode is enabled on an Tenable Network Monitor instance, Tenable Security Center stores discovery mode asset data to Tenable Security Center repositories. Since discovery mode only discovers limited asset data, the repository data appears incomplete.

Tenable Security Center does not count IP addresses present only from Tenable Network Monitor instances in discovery mode toward your license count.

Add a Tenable Network Monitor Instance

Required Tenable Security Center User Role: Administrator

Before you begin:

- Confirm you understand the complete scanning configuration process, as described in [Tenable Network Monitor Instances](#).

To add an Tenable Network Monitor instance to Tenable Security Center:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Resources** > **Tenable Network Monitors**.

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

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

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

4. Configure the settings, as described in [Tenable Network Monitor Instance Settings](#).

   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 Network Monitor server, click **Verify Hostname** to enable the toggle.

   g. If you want to use the proxy configured in Tenable 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 Network Monitor installation for daemon-to-client client communications.

      ii. In the **Password** box, type the password for the account generated during the Tenable Network Monitor installation for daemon-to-client client communications

   j. If you selected **SSL Certificate** as the **Type**, click **Choose File** to upload a certificate.

   k. 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.

l. 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.

View Your Tenable Network Monitor Instances

Required Tenable Security Center User Role: Administrator

For more information, see Tenable Network Monitor Instances.

To view your Tenable Network Monitor instances in Tenable Security Center:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Nessus Network Monitors**.

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

3. View details about each Tenable Network Monitor instance.

   - **Name** — The name for the instance.

   - **Status** — The status of the instance.

   - **Host** — The IP address of the instance.

   - **Version** — The instance's Tenable Network Monitor version.

   - **Uptime** — The length of time, in days, that the instance has been running.

   - **Last Report** — The date and time Tenable Network Monitor most recently reported data to Tenable Security Center.

4. (Optional) To manually refresh the **Status** data, at the top of the table, click **Update Status**.

   Tenable Security Center refreshes the **Status** data.

Tenable Network Monitor Instance Settings

Use the following options to configure Tenable Network Monitor instances in Tenable Security Center, as described in [Add a Tenable Network Monitor Instance](#).

Option	Description
Name	Descriptive name for the Tenable Network Monitor instance.
Description	Instance description, location, or purpose.
Host	Hostname or IP address of the instance.
Port	TCP port that the Tenable Network Monitor instance listens on for communications from Tenable Security Center. The default is port 8835.
State	A instance may be marked as **Enabled** or **Disabled** within Tenable Security Center to allow or prevent access to the instance.
Authentication Type	Select Password or SSL Certificate for the authentication type to connect to the Tenable Network Monitor instance.
Username	Username generated during the Tenable Network Monitor install for daemon to client communications. This must be an administrator user in order to send plugin updates to the Tenable Network Monitor instance. This option is only available if the **Authentication Type** is set to **Password**.
Password	The login password must be entered in this option. This option is only available if the **Authentication Type** is set to **Password**.
Certificate	This option is available if the **Authentication Type** is **SSL Certificate**. Click the **Browse** button, choose a SSL Certificate file to upload, and upload to the Tenable Security Center.
Certificate Passphrase	If you selected **SSL Certificate** as the **Authentication Type** and the private key that decrypts your SSL certificate is encrypted with a passphrase, the passphrase for the private key.
Verify Hostname	Adds a check to verify that the hostname or IP address entered in the **Host** option matches the CommonName (CN) presented in the SSL

Option	Description
	certificate from the Tenable Network Monitor server.
Use Proxy	Instructs Tenable Security Center to use its configured proxy for communication with the instance.
Repositories	The repositories which this Tenable Network Monitor instance will save its data to. If Tenable Network Monitor will be reporting IPv4 and IPv6 data, at least two repositories (one for IPv4 and one for IPv6 data) must be selected.

Tenable Log Correlation Engines

Note: Tenable Enclave Security does not support Tenable Log Correlation Engine.

Tenable Tenable Log Correlation Engine (Log Correlation Engine) is a software module that aggregates, normalizes, correlates, and analyzes event log data from the myriad of devices within the infrastructure. Log Correlation Engine also has the ability to analyze logs for vulnerabilities.

Tenable Security Center performs vulnerability, compliance, and event management, but without Log Correlation Engine integration it does not directly receive logs or IDS/IPS events. With Log Correlation Engine integration, Log Correlation Engine processes the events and passes the results to Tenable Security Center.

Log Correlation Engine's close integration with Tenable Security Center allows you to centralize log analysis and vulnerability management for a complete view of your organization's security posture.

Note: If you add an Log Correlation Engine server to Tenable Security Center and enable **Import Vulnerabilities**, Log Correlation Engine data counts against your Tenable Security Center license. For more information, see License Requirements.

For more information, see Add a Tenable Log Correlation Engine Server.

If remote root or root equivalent user login is prohibited in your environment, you can add the Log Correlation Engine server using SSH key authentication. For more information, see Manual Log Correlation Engine Key Exchange.

For information about Tenable Security Center-Tenable Log Correlation Engine communications encryption, see Encryption Strength.

Tenable Log Correlation Engine Options

Option	Description
Name	Name for the integrated Tenable Log Correlation Engine.
Description	Descriptive text for the integrated Tenable Log Correlation Engine.
Host	IP address of the integrated Tenable Log Correlation Engine.
Check Authentication	Whether Tenable Security Center checks the status of authentication between itself and the Log Correlation Engine server.
Organizations	Organizations that can access data from the integrated Tenable Log Correlation Engine.
Repositories	The repositories where you want Tenable Security Center to store the imported Log Correlation Engine data.
Port	The port where the Log Correlation Engine reporter is listening on the Log Correlation Engine server.
Username and Password	The username and password you want Tenable Security Center to use for authentication to the Log Correlation Engine server to retrieve vulnerability information.
	This user account must be able to make changes on the remote system to enable the SSH key exchange between Tenable Security Center and Log Correlation Engine. The appropriate permissions level is typically root, root equivalent, or other high-level user permissions on the Log Correlation Engine system. Tenable Security Center uses these credentials a single time to exchange SSH keys for secure communication between Tenable Security Center and Log Correlation Engine.

Add a Tenable Log Correlation Engine Server

Note: Tenable Enclave Security does not support Tenable Log Correlation Engine.

Required Tenable Security Center User Role: Administrator

> **Tip:** You can configure more than one Tenable Log Correlation Engine to work with Tenable Security Center.

Before you begin:

- Confirm you understand the complete scanning configuration process, as described in [Tenable Log Correlation Engines](#).

To add an Log Correlation Engine server to Tenable Security Center:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Resources** > **Log Correlation Engines**.

   The **LCE Servers** page appears.

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

   The **Add LCE Server** window appears.

4. Configure the **General** options, as described in [Tenable Log Correlation Engines](#).

   a. In the **Name** box, type a name for the Log Correlation Engine server.

   b. In the **Description** box, type a description for the Log Correlation Engine server.

   c. In the **Host** box, type the hostname or IP address for the Log Correlation Engine server.

   d. In the **Port** box, view the default **(1243)** and modify, if necessary.

5. (Optional) To allow Tenable Security Center to log in to the Log Correlation Engine server and retrieve vulnerability information:

   a. Enable **Import Vulnerabilities**.

   > **Note:** If you use an Log Correlation Engine server with Tenable Security Center, Tenable Security Center counts the IP addresses associated with each imported instance against your license. For more information, see [License Requirements](#).

   b. Select a **Repository** for the event vulnerability data.

   c. Type a **Username** and **Password** you want Tenable Security Center to use for access to the Log Correlation Engine server.

6. Click **Submit**.

   Tenable Security Center saves your configuration.

7. (Optional) If you enabled the **Check Authentication** option above, Tenable Security Center checks its ability to authenticate with the Log Correlation Engine server.

   - If authentication is successful, Tenable Security Center displays a message to acknowledge that fact.

   - If authentication fails, Tenable Security Center prompts you for credentials to the Log Correlation Engine server:

      a. Type a username and password.

      b. Click **Push Key** to initiate the transfer of the SSH Key.

         If the transfer is successful, Tenable Security Center displays a message to acknowledge that fact.

         > **Note:** Tenable Security Center connections use ECDSA keys, but Log Correlation Engine connections use RSA keys. When you use the **Push Key** option, Tenable Security Center sends an RSA key. For more information about Tenable Security Center keys, see Keys Settings.

Tenable Log Correlation Engine Clients

> **Note:** Tenable Enclave Security does not support Tenable Log Correlation Engine.

The Log Correlation Engine server manages configuration files for Log Correlation Engine 5.x clients remotely from the command line. Tenable Security Center manages the configuration files for Tenable Log Correlation Engine 5.x clients via a graphical interface.

The default view for the Log Correlation Engine Clients page displays all of the available clients for the selected Tenable Log Correlation Engine server in the **Filters** section, and may be changed by updating the Log Correlation Engine Server filter. Use the other filter options, to narrow down the displayed clients for the selected server by a mix of criteria based on combinations of the displayed columns.

Current Log Correlation Engine Client versions 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. Log Correlation Engine Client configurations can be managed from Tenable Security Center.

> **Tip:** Configured clients prior to version 5.x appear in the list without OS and policy information. However, these clients cannot have their policy files centrally managed from Tenable Security Center.

Each client may have a name assigned to it to help easily identify the client. The currently assigned name appears in the **Name** column. To change the name, click on the client to edit from the list, and type the name. Client names may not contain spaces. Click the **Submit** button to save the change.

Log Correlation Engine Clients are initially configured to send their data to a particular Log Correlation Engine server, but must be authorized by the Log Correlation Engine sever for the server to accept the data. The client's authorization status appears in the left-side column. If there is no icon, the client is authorized to send data to the Log Correlation Engine server. If there is a broken link icon, the client is not authorized to send data to the Log Correlation Engine server. To do this, right-click the row for the client or select the check box for the client, then click **Authorize** or **Revoke Authorization**.

Each client must have a policy assigned to it that specifies the appropriate data to send. The currently assigned policy appears in the **Policy** column. To change the assigned policy, select the client to edit and click the appropriate policy from the drop-down box. Search client policies by name by entering text into the Policy box. Click the **Submit** button to save the change. The policy updates on the client on its next connection.

Tenable Log Correlation Engine Client Policies

> **Note:** Tenable Enclave Security does not support Tenable Log Correlation Engine.

The **Log Correlation Engine Client Policies** page contains a list of all the client policies currently available for use by Log Correlation Engine clients. The list contains the name of the policy, the operating system 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-**. You can use these policy files as is or export them to be used as a basis for custom policy files. Tenable may update or change these example policy files without notice, so using them as is may return different results at a later time.

Use the **Add** button to add customized Log Correlation EngineClient policy files to the Log Correlation Engine server and make them available for use. The **Name** option is appended to the

beginning of the file name and offers 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** option is used to select and upload the custom policy file or type the policy file into the box. Click the **Submit** button to save the policy file and send it to the Log Correlation Engine server.

> **Note:** The default and **TNS** prefixes should only be used by policies supplied by Tenable. If you use default or **TNS** as a prefix for custom policy files, they may be overwritten or manipulated.

Right-click or select the check box for a policy, then click **Export** to save the policy to a local drive. The file is in XML format, which you can edit with standard text or XML editors.

Right-click or select the check box for a policy, then click **View** to display the policy name and source of the policy in a window within Tenable Security Center. You cannot edit the information from within this window.

> **Note:** For more information on creating Log Correlation Engine Client policy files, see the *Tenable Log Correlation Engine Client Guide*.

Sensor Proxies

The **Sensor Proxies** page contains a list of all the sensor proxies currently available for use.

Sensor Proxy provides an on-premises cache and single point of traffic between Tenable Web App Scanning and Tenable Security Center. Sensors send communication to Sensor Proxy, not to Tenable Security Center directly. As a result, large numbers of sensors can communicate with Tenable Security Center with less bandwidth usage. For more information about Sensor Proxy, see the Sensor Proxy user guide.

> **Note:** If you migrate your Sensor Proxy, both the old and new Sensor Proxies will appear on the **Sensor Proxies** page in Tenable Security Center. After you migrate your Sensor Proxy, a Tenable Security Center administrator should delete the old Sensor Proxy instance from the **Sensor Proxies** page in Tenable Security Center

Add a Sensor Proxy to Tenable Security Center

1. In the **Linking Key** section, click **Copy** to copy the linking key to your clipboard. You will use the linking key in step 4.

2. Install Sensor Proxy using the following command, replacing the rpm file name with the Sensor Proxy package you downloaded:

```
# dnf install SensorProxy-<version number>.<os>.<architecture>.rpm
```

3. Copy the Tenable Security Center CA certificate from your Tenable Security Center instance, and paste the CA certificate in any location on the Sensor Proxy instance. The following command is an example for how to copy the CA certificate, where:

   - **</path/to/security_center/TenableCA.crt>** is the path to the CA certificate on your Tenable Security Center instance.

     - The path to the default Tenable Security Center certificate is **/opt/sc/data/CA/TenableCA.crt**.

     - If your organization has a custom certificate, use the path and filename for the custom certificate.

   - **</path/to/sensor_proxy/TenableCA.crt>** is the new path to the CA certificate on your Sensor Proxy instance.

```
# scp root@sc_host:</path/to/security_center/TenableCA.crt> </path/to/sensor_
proxy/TenableCA.crt>
```

4. Link Sensor Proxy to Tenable Security Center using the following command, where:

   - **<linking_key>** is the linking key you copied in step 1.

   - **<sensor_proxy_name>** is a name for the Sensor Proxy.

   - **<security_center_ip>** is the IP address for the Tenable Security Center.

   - **<security_center_sensor_proxy_port>** is the inbound port. Sensor Proxy uses port 8837.

   - **</path/to/sensor_proxy/TenableCA.crt>** is the path to your Tenable Security Center CA certificate on the Sensor Proxy instance. Use the path where you pasted the CA certificate in the previous step.

```
# /opt/sensor_proxy/sbin/configure --link --key=<linking_key> --host=<security_center_ip> --
port=<security_center_sensor_proxy_port> --ca-path=</path/to/sensor_proxy/TenableCA.crt> [--
name=<sensor_proxy_name>]
```

5. Enable and start the Sensor Proxy service using the following command:

```
# systemctl enable --now sensorproxy
```

What to do next

- Save the Sensor Proxy server certificate files in case you need to recover Sensor Proxy.

- Link sensors to Sensor Proxy.

OT Security Instances

OT Security protects industrial networks by providing industrial and critical infrastructure operations with visibility, security, and control to ensure safe facility operation while reducing overall risk. You can use Tenable Security Center to analyze OT Security asset and vulnerability data alongside your data from other scanners.

When you configure data synchronization from OT Security to Tenable Security Center, OT Security sends asset and vulnerability data to an agent repository in Tenable Security Center. OT Security communicates with Tenable Security Center using the Tenable Security Center API.

> **Note:** It is important to restrict the data OT Security collects to only the desired host IP address ranges. For example, if OT Security collects information on 1100 hosts and Tenable Security Center is licensed for 1000 hosts, OT Security sends all of the data to Tenable Security Center and Tenable Security Center will indicate that you exceeded your host count. For more information, see License Requirements.

Before you begin:

- Deploy OT Security, as described in the *OT Security User Guide*.

- Begin vulnerability assessment in OT Security, as described in the *OT Security User Guide*.

To fully configure data synchronization from OT Security to Tenable Security Center:

1. Add a designated agent repository for OT Security data in Tenable Security Center, as described in [Add a Repository](#).

2. Using the OT Security API, configure the Tenable Security Center integration to specify the sync schedule, import repository, and authentication.

What to do next:

- View scan results from OT Security, as described in [View Scan Results](#).

- View vulnerability data filtered by your OT Security repository, as described in [Vulnerability Analysis](#).

Repositories

Repositories are databases within Tenable Security Center that contain vulnerability data. You can share repositories with users and organizations based on admin-defined assets. Repositories provide scalable and configurable data storage. Optionally, you can share repository data between multiple Tenable Security Centers.

> **Note:** The maximum repository size is 64 GB. For best performance, Tenable recommends splitting repositories larger than 32 GB.

When adding a *local repository*, you designate storage within Tenable Security Center for different types of vulnerability data (identified by IPv4 addresses, IPv6 addresses, agents, or mobile scanners). Scanners attached to a Tenable Security Center populate your local repositories with vulnerability data. For more information, see [Local Repositories](#).

When adding an *external repository*, you access a local repository from another Tenable Security Center:

- Remote repositories allow you to share repository data from one Tenable Security Center deployment to your primary Tenable Security Center deployment via an SSH session. By default, Tenable Security Center uses ECDSA keys for remote repository authentication.

> **Note:** When you upgrade to Tenable Security Center 6.6.x from version 6.4.x or earlier, benchmark results will not appear until after the next repository sync.

- Offline repositories allow you to share repository data from one Tenable Security Center deployment to your primary Tenable Security Center deployment via manual export and import (a `.tar.gz` archive file). You can combine data from several repository files into a single offline repository by importing multiple files to the offline repository.

External repository data is static and used solely for reporting purposes. For more information, see External Repositories.

For more information, see Add a Repository and Manage Repositories. For information about Tenable Security Center repository data encryption, see Encryption Strength.

> **Tip:** If you need to remove data from a repository (for example, to remove retired asset data or to resolve a license issue), see the knowledge base article.

Manage Repositories

> **Required Tenable Security Center User Role:** Administrator

For more information, see Repositories.

To manage your repositories:

1. Log in to Tenable Security Center via the user interface.

2. Click **Repositories** > **Repositories**.

   The **Repositories** page appears.

3. To filter the repositories that appear on the page, apply a filter as described in Apply a Filter.

4. To view details for a repository:

   a. Right-click the row for the repository you want to view.

      The actions menu appears.

      -or-

      Select the check box for the repository you want to view.

      The available actions appear at the top of the table.

b. Click **View**.

   The **View Repository** page appears. For more information, see [Repository Details](#).

5. To edit a repository:

   a. Right-click the row for the repository you want to edit.

      The actions menu appears.

      -or-

      Select the check box for the repository you want to edit.

      The available actions appear at the top of the table.

   b. Click **More** > **Edit**.

      The **Edit Repository** page appears.

   c. Modify the repository options, as described in [IPv4/IPv6 Repositories](#), [Mobile Repositories](#), [Agent Repositories](#), [Universal Repositories](#), [Remote Repositories](#), or [Offline Repositories](#).

   d. Click **Submit**.

      Tenable Security Center saves your configuration.

6. To export a repository, see [Export a Repository](#).

7. To import a repository file into an offline repository, see [Import a Repository](#).

8. To delete a repository, see [Delete a Repository](#).

Add a Repository

Required Tenable Security Center User Role: Administrator

For more information about repositories, see [Repositories](#).

Note: By default, Tenable Security Center uses ECDSA keys for remote repository authentication regardless of FIPS mode settings.

To add a repository:

1. Log in to Tenable Security Center via the user interface.

2. Click **Repositories** > **Repositories**.

   The Repositories page appears.

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

   The **Add Repository** page appears.

4. Click the tile for the repository type you want to add.

   The **Add Repository** page appears.

5. Configure the options for your repository type:

   - [IPv4/IPv6 Repositories](#)

   - [Mobile Repositories](#)

   - [Agent Repositories](#)

   - [Universal Repositories](#)

   - [Remote Repositories](#)

   - [Offline Repositories](#)

6. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

- If you added an offline repository, export one or more repositories from your other Tenable Security Center as described in [Export a Repository](#).

- If you added an offline repository, import one or more exported repository files as described in [Import a Repository](#).

View Your Repositories

Required Tenable Security Center User Role: Administrator

You can view a list of all repositories on your Tenable Security Center. For more information, see [Repositories](#).

To view a list of your repositories:

1. Log in to Tenable Security Center via the user interface.

2. Click **Repositories** > **Repositories**.

   The **Repositories** page appears.

3. View details about each repository.

   - **Name** — The name of the repository.

   - **Vulnerability Count** — The total number of vulnerability instances in the repository.

     > **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

   - **IP/Device Count** — The total number of assets for which the repository contains vulnerability data.

   - **Type** — The repository type.

   - **Capacity** — (IPv4, IPv6, Agent, and Universal repositories only) The percentage of maximum available repository space you are currently using. The maximum repository size is 64 GB.

     > **Tip:** For best performance, Tenable recommends splitting repositories larger than 32 GB.

   - **Last Updated** — The date and time the repository was last updated.

View Repository Details

> **Required Tenable Security Center User Role:** Administrator

You can view details for any repository. For more information, see [Repositories](#).

To view repository details:

1. Log in to Tenable Security Center via the user interface.

2. Click **Repositories** > **Repositories**.

   The **Repositories** page appears.

3. Right-click the row for the repository you want to view.

   The actions menu appears.

   -or-

   Select the check box for the repository you want to view.

   The available actions appear at the top of the table.

4. Click **View**.

   The **View Repository** page appears.

Section	Repository Type	Action
General	All	View general information for the repository. • **Name** — The repository name. • **Description** — The repository description. • **IP Count** — The total number of assets for which the repository contains vulnerability data. • **Last Vuln Update** — The date and time the repository was last updated. • **Vulnerability Count** — The total number of vulnerability instances in the repository. **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

Section	Repository Type	Action
		• **Repository Capacity** — (IPv4, IPv6, Agent, and Universal repositories only) The percentage of maximum available repository space you are currently using. The maximum repository size is 64 GB. **Tip:** For best performance, Tenable recommends splitting repositories larger than 32 GB. • **Created** — The date the repository was created. • **Last Modified** — The date the repository was last modified. • **ID** — The repository ID.
MDM	Mobile	View a summary of your settings for the repository. For more information about a setting, see Mobile Repositories.
Data	IPv4/IPv6, Agent, Remote, Offline, Universal	View a summary of the repository data (for example, the IP address range). For more information, see: • IPv4/IPv6 Repositories • Agent Repositories • Universal Repositories • Remote Repositories • Offline Repositories
Access	All	View the name of the organizations with

Section	Repository Type	Action
		access to this repository.
Advanced Settings	IPv4/IPv6, Agent, Remote, Offline, Universal	View a summary of your settings for the repository. For more information about a setting, see: • [IPv4/IPv6 Repositories](#) • [Agent Repositories](#) • [Universal Repositories](#) • [Remote Repositories](#) • [Offline Repositories](#)

Tenable Synchronization Data	All supported for Tenable Lumin synchronization	View synchronization summary data:
		
		• **Status** — The status of the repository in Tenable Lumin synchronization:
		
		  • **Finished** — The most recent synchronization that included this repository succeeded.
		
		  • **Not Synced** — The repository is not configured for Tenable Lumin synchronization.
		
		  • **Error** — An error occurred. For more information, see [View Tenable One Data Synchronization Logs](#).
		
		• **First Synchronization** — The date and time of the first synchronization of this repository.

Section	Repository Type	Action
		• **Last Success** — The date and time of the most recent synchronization of this repository. • **Last Failure** — The date and time of the most recent failed synchronization of this repository. For more information about Tenable Lumin synchronization, see [Tenable One Synchronization](#).
Vulnerability Data Lifetime	IPv4/IPv6, Agent, Universal	View the data expiration settings for the repository. For more information, see: • [IPv4/IPv6 Repositories](#) • [Agent Repositories](#) • [Universal Repositories](#)

Export a Repository

Required Tenable Security Center User Role: Administrator

You can export a repository from one Tenable Security Center and import it as an offline repository on another Tenable Security Center. You can export repositories via the Tenable Security Center user interface or the CLI. For more information, see [Offline Repositories](#).

Note: 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.

Tip: If the repository you want to export has trend data enabled and you want to include trend data in your repository export, export the repository via the CLI. Repositories that you export via the user interface do not include trend data. For more information about trend data, see [IPv4/IPv6 Repositories](#), [Agent Repositories](#), and [Universal Repositories](#).

To export a repository via the user interface:

1. Log in to Tenable Security Center via the user interface.

2. Click **Repositories** > **Repositories**.

   The **Repositories** page appears.

3. Right-click the row for the repository you want to export.

   The actions menu appears.

   -or-

   Select the check box for the repository you want to export.

   The available actions appear at the top of the table.

4. Click **Export**.

   Tenable Security Center exports the repository.

To export a repository via the CLI:

1. Log in to Tenable Security Center via the command line interface (CLI).

2. Prepare the command you want to run.

   ```
   sh /opt/sc/customer-tools/exportRepository.sh [repID] [trendingDays]
   [trendWithRaw]
   ```

Variable	Description
repID	The repository ID of the repository you want to export. To locate the repository ID, view the details for the repository, as described in View Repository Details.
trendingDays	(IP, Agent, and Universal repositories only) The number of days of vulnerability trending data to include. To use the preconfigured repository setting, type **default**. **Note:** The number of days of trending data included in the

Variable	Description
	export cannot exceed the **Days Trending** setting for the repository or the number of days of trending data available for the repository. For example, if you request 30 days of trending data, but trending data has been enabled for only 15 days, then the export includes only 15 days of trending data. For more information about repository settings, see IPv4/IPv6 Repositories, Agent Repositories, and Universal Repositories.
trendWithRaw	(IP, Agent, and Universal repositories only) Specify whether you want the export to include plugin output data: **yes** or **no**. To use the preconfigured repository setting, type **default**.

(Optional) To automatically overwrite an existing repository file with the same name, include the optional argument -f.

3. In the CLI in Tenable Security Center, run the export command.

   For example:

   ```
   /opt/sc/customer-tools/exportRepository.sh -f 1 default default
   ```

   Tenable Security Center exports the repository.

What to do next:

- To import the repository to another Tenable Security Center, add an offline repository to that Tenable Security Center, as described in Add a Repository.

Import a Repository

Required Tenable Security Center User Role: Administrator

You can import one or more repository files to an offline repository. For more information, see Offline Repositories.

Note: 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.

Before you begin:

- Export one or more repository files from your other Tenable Security Center, as described in [Export a Repository](#).

- Add an offline repository, as described in [Add a Repository](#).

To import an exported repository to an offline repository:

1. Log in to Tenable Security Center via the user interface.

2. Click **Repositories** > **Repositories**.

   The **Repositories** page appears.

3. Right-click the row for the offline repository you created.

   The actions menu appears.

   -or-

   Select the check box for the offline repository you created.

   The available actions appear at the top of the table.

4. Click **Upload** and browse to the file you want to upload.

   Tenable Security Center imports the repository.

Delete a Repository

Required Tenable Security Center User Role: Administrator

To delete a repository:

1. Log in to Tenable Security Center via the user interface.

2. Click **Repositories** > **Repositories**.

   The **Repositories** page appears.

3. Select the repository you want to delete:

   To delete a single repository:

a. In the table, right-click the row for the repository you want to delete.

The actions menu appears.

b. Click **Delete**.

To delete multiple repositories:

a. In the table, select the check box for each repository you want to delete.

The available actions appear at the top of the table.

b. At the top of the table, click **More** > **Delete**.

A confirmation window appears.

4. Click **Delete**.

Tenable Security Center deletes the repository.

Local Repositories

When adding *local repositories*, you designate storage within Tenable Security Center for different types of vulnerability data. Scanners attached to a Tenable Security Center populate your local repositories with vulnerability data.

Tenable Security Center supports the following types of local repositories: IPv4/IPv6 Repositories, Mobile Repositories, Agent Repositories, and Universal Repositories.

For more information, see Repositories and Add a Repository.

IPv4/IPv6 Repositories

These are the most common types of repositories used with Tenable Security Center. They 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.

> **Caution:** When creating Tenable Security Center IPv4 or IPv6 repositories, Log Correlation Engine event source IP address ranges must be included along with the vulnerability IP address ranges or the event data and event vulnerabilities are not accessible from the Tenable Security Center user interface.

For more information, see Add a Repository.

IP Repository Options

Option	Description
General	
Name	The repository name.
Description	(Optional) A description for the repository.
Data	
IP Ranges	Specifies the IP address range of vulnerability data you want to store in the repository. Type the range as a comma-separated list of IP addresses, IP address ranges, and/or CIDR blocks.
Access	
Organizations	Specifies which organizations have access to the vulnerability data stored in the repository. If groups are configured for the organization, Tenable Security Center prompts you to grant or deny access to all of the groups in the organization. For more granular control, grant access within the settings for that group.
Advanced Settings	
Generate Trend Data	When enabled, Tenable Security Center generates trend data by taking periodic snapshots of the cumulative database. Trend data is displayed in some Tenable Security Center tools (e.g., trending line charts and trending area charts). Tenable Security Center also produces differential data (snapshot comparison data), which improves performance when displaying trend data in Tenable Security Center tools. **Tip:** Disable this option to reduce your disk space usage.
Days Trending	Specifies the number of days of cumulative vulnerability data that you want Tenable Security Center to display in dashboard and report

Option	Description
	vulnerability trending displays.
Enable Full Text Search	When enabled, Tenable Security Center includes vulnerability text in periodic snapshots of .nessus data for vulnerability trending purposes. For more information about the **Vulnerability Text** filter component, see [Vulnerability Analysis Filter Components](#).
Log Correlation Engine Correlation	Not supported for IPv6 repositories. The Log Correlation Engine server where you want Tenable Security Center to retrieve data. The data retrieved depends on the **Import Vulnerabilities** setting in your Log Correlation Engine server configuration: • If **Import Vulnerabilities** is enabled, Tenable Security Center retrieves vulnerability data and Log Correlation Engine events. • If **Import Vulnerabilities** is disabled, Tenable Security Center retrieves Log Correlation Engine events.
Vulnerability Data Lifetime (Data Expiration Settings)	
Active	The number of days you want Tenable Security Center to retain active scan vulnerability data stored in IP repositories. The default value of this option is *365* days.
Passive	The number of days you want Tenable Security Center to retain Tenable Network Monitor vulnerability data stored in IP repositories. The default value of this option is *7* days.
Event	(IPv4 repositories only) The number of days you want Tenable Security Center to retain Log Correlation Engine event data stored in IP repositories. The default value of this option is *365* days.
Compliance	The number of days you want Tenable Security Center to retain audit compliance data stored in IP repositories. The default value of this option is *365* days.

Option	Description
Mitigated	The number of days you want Tenable Security Center to retain mitigated vulnerability data. The default value of this option is *365* days.

Mobile Repositories

The mobile repository is a local type that stores data from various servers. For more information, see Add a Repository.

General Options

Configure the following options for all mobile repository types.

Option	Description	Default
Name	The repository name.	--
Description	(Optional) A description for the repository.	--
Type	The type of repository you want to configure. Your **Type** selection determines the type-specific options you must configure: • ActiveSync Options • AirWatch MDM Options • Apple Profile Manager Options • Blackberry UEM Options • Good MDM Options • MaaS360 Options • Microsoft Intune Options • MobileIron Options • Workspace ONE Options	--
Organizations	Specifies which organizations have access to	--

Option	Description	Default
	the vulnerability data stored in the repository. If groups are configured for the organization, Tenable Security Center prompts you to grant or deny access to all of the groups in the organization. For more granular control, grant access within the settings for that group.	

ActiveSync Options

The following table describes the additional options to configure when creating an **ActiveSync** mobile repository.

Option	Description	Default
Domain Controller	The domain controller for ActiveSync.	--
Domain	The Windows domain for ActiveSync.	--
Domain Username	The username for the domain administrator's account that Tenable Security Center uses to authenticate to ActiveSync.	--
Domain Password	The password for the domain administrator user.	--
Scanner	Specifies which Tenable Nessus scanner Tenable Security Center uses when scanning the server. Tenable Security Center can only use one Tenable Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable Security Center scans the server to update the mobile repository. On each scan, Tenable Security Center removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 -04:00

AirWatch MDM Options

The following table describes the additional options to configure when creating an **AirWatch MDM** mobile repository.

Option	Description	Default
AirWatch Environment API URL	The AirWatch API url endpoint. (For example, https://xxx.awmdm.com/api)	--
Port	The TCP port that AirWatch listens on for communications from Tenable.	443
Username	The username for the AirWatch user account Tenable uses to authenticate to Workspace ONE's API.	--
Password	The password for the AirWatch user.	--
API Key	The API key for the AirWatch API.	--
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	Enabled
Scanner	Specifies which Tenable Nessus scanner Tenable Security Center uses when scanning the server. Tenable Security Center can only use one Tenable Nessus scanner to add data to a mobile repository.	--

Option	Description	Default
Update Schedule	Specifies when Tenable Security Center scans the server to update the mobile repository. On each scan, Tenable Security Center removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 -04:00

Apple Profile Manager Options

The following table describes the additional options to configure when creating an **Apple Profile Manager** mobile repository.

Option	Description	Default
Server	The server URL Tenable Security Center uses to authenticate with Apple Profile Manager.	--
Port	The TCP port that Apple Profile Manager listens on for communications from Tenable Security Center.	443
Username	(Optional) The username for the Apple Profile Manager user account Tenable Security Center uses to authenticate to Apple Profile Manager.	--
Password	(Optional) The password for the Apple Profile Manager user.	--
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable verifies that the	Enabled

Option	Description	Default
	SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	
Scanner	Specifies which Tenable Nessus scanner Tenable Security Center uses when scanning the server. Tenable Security Center can only use one Tenable Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable Security Center scans the server to update the mobile repository. On each scan, Tenable Security Center removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 -04:00

Blackberry UEM Options

The following table describes the additional options to configure when creating a **Blackberry UEM** mobile repository.

Option	Description	Default
Hostname	The hostname for the Blackberry UEM server.	--
Port	The port you want Tenable Security Center to use for authenticating to the Blackberry UEM server.	--
Tenant	The SRP ID value in Blackberry UEM.	--
Domain	(Optional) The domain name value in Blackberry UEM.	--
Username	The username for the Blackberry UEM user account Tenable Security Center uses to authenticate to	--

Option	Description	Default
	Blackberry UEM.	
Password	The password for the Blackberry UEM user.	--
SSL	When enabled, Tenable Security Center uses an encrypted connection to authenticate with Blackberry UEM.	Disabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	Disabled
Scanner	Specifies which Tenable Nessus scanner Tenable Security Center uses when scanning the server. Tenable Security Center can only use one Tenable Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable Security Center scans the server to update the mobile repository. On each scan, Tenable Security Center removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 - 04:00

Good MDM Options

The following table describes the additional options to configure when creating a **Good MDM** mobile repository.

Option	Description	Default
Server	The server URL Tenable Security Center uses to authenticate with Good MDM.	--
Port	The TCP port that Good MDM listens on for communications from Tenable Security Center.	--

Option	Description	Default
Domain	The domain name for Good MDM.	--
Username	The username for the Good MDM user account Tenable Security Center uses to authenticate to Good MDM.	--
Password	The password for the Good MDM user.	--
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	Enabled
Scanner	Specifies which Tenable Nessus scanner Tenable Security Center uses when scanning the server. Tenable Security Center can only use one Tenable Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable Security Center scans the server to update the mobile repository. On each scan, Tenable Security Center removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 - 04:00

MaaS360 Options

The following table describes the additional options to configure when creating a **MaaS360** mobile repository.

Option	Description	Default
Username	The username for the MaaS360 user account Tenable Security Center uses to authenticate to MaaS360.	--
Password	The password for the MaaS360 user.	--
Root URL	The URL Tenable Security Center uses to authenticate to MaaS360.	--
Platform ID	The ID for the device platform.	--
Billing ID	The billing ID for the MaaS360 account.	--
App ID	The ID for the MaaS360 application.	--
App Version	The MaaS360 application version.	--
App Access Key	The access key for the MaaS360 application.	--
Collect All Device Data	When enabled, a mobile repository scan collects all data. When disabled, you can select which types of data a mobile repository scan collects: • **Collect Device Summary** • **Collect Device Applications** • **Collect Device Compliance** • **Collect Device Policies**	Enabled
Scanner	Specifies which Tenable Nessus scanner Tenable Security Center uses when scanning the server. Tenable Security Center can only use one Tenable Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable Security Center scans the server to update the mobile repository. On each scan, Tenable Security Center removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 - 04:00

Intune Options

The following table describes the additional options to configure when creating a **Microsoft Intune** mobile repository.

Option	Description	Default
Intune Tenant	The Microsoft Azure Directory value in your Microsoft Intune registration.	--
Intune Client	The Microsoft Azure Application value generated during your Microsoft Intune registration.	--
Intune Secret	The Microsoft Azure client secret key.	--
Intune Username	The username for the Microsoft Intune user account Tenable Security Center uses to authenticate to Microsoft Intune.	--
Intune Password	The password for the Microsoft Intune user.	--
Scanner	Specifies which Tenable Nessus scanner Tenable Security Center uses when scanning the server. Tenable Security Center can only use one Tenable Nessus scanner to add data to a mobile repository.	--
Update Schedule	Specifies when Tenable Security Center scans the server to update the mobile repository. On each scan, Tenable Security Center removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 - 04:00

MobileIron Options

The following table describes the additional options to configure when creating a **MobileIron** mobile repository.

Option	Description	Default
MobileIron VSP Admin Portal	The server URL Tenable Security Center uses	--

Option	Description	Default
URL	to authenticate to the MobileIron administrator portal.	
VSP Admin Portal Port	(Optional) The TCP port that the MobileIron administrator portal listens on for communications from Tenable Security Center.	--
MobileIron Port	The TCP port that MobileIron listens on for communications from Tenable Security Center.	443
Username	The username for the MobileIron administrator account Tenable Security Center uses to authenticate to MobileIron.	--
Password	The password for the MobileIron administrator user.	--
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	Enabled
Scanner	Specifies which Tenable Nessus scanner Tenable Security Center uses when scanning the server. Tenable Security Center can only use one Tenable Nessus scanner to add data	--

Option	Description	Default
	to a mobile repository.	
Update Schedule	Specifies when Tenable Security Center scans the server to update the mobile repository. On each scan, Tenable Security Center removes the current data in the repository and replaces it with data from the latest scan.	Every day at 12:30 -04:00

Workspace ONE Options

> **Note:** For the Workspace ONE integration to function properly, you must be assigned all the **Read-Only** permissions available for the role. For more information, see the VMware documentation.

Setting	Default Value	Description	Required
Workspace ONE Environment API URL	–	The Workspace ONE API url endpoint. (For example, https://xxx.awmdm.com/api)	yes
Port	443	The TCP port that Workspace ONE listens on for communications from Tenable.	yes
Workspace ONE Username	–	The username for the Workspace ONE user account Tenable uses to authenticate to Workspace ONE's API.	yes
Workspace ONE Password	–	The password for the Workspace ONE user.	yes
API Key	–	The API key for the VMware Workspace ONE API.	yes

HTTPS	Enabled	Enable for Tenable Security Center to authenticate over an encrypted (HTTPS) or an unencrypted (HTTP) connection.	no
Verify SSL Certificate	Enabled	(Appears when HTTPS is enabled) Enable for Tenable Security Center to verify if the SSL Certificate on the server is signed by a trusted CA.	no
Collect All Device Data	Yes	Collects all device data required for plugin checks.	no
Collect Device Applications	Yes	(Appears when Collect All Device Data is disabled) Collects applications installed on mobile devices.	no

Agent Repositories

Agent repositories can store data from Tenable Agents (identified by agent ID) or OT Security (identified by OT Security UUID).

An agent ID uniquely identifies agent-detected assets that may share a common IP address.

OT Security assigns UUIDs to assets to uniquely identify them, since not all operational technology assets have IP addresses. Then, Tenable Security Center uses the UUIDs to uniquely identify OT Security data in Tenable Security Center. For more information about viewing OT Security data in Tenable Security Center, see OT Security Instances.

For more information, see Add a Repository.

Agent Repository Options

Option	Description
General	

Option	Description
Name	The repository name.
Description	(Optional) A description for the repository.
Access	
Organizations	Specifies which organizations have access to the vulnerability data stored in the repository. If groups are configured for the organization, Tenable Security Center prompts you to grant or deny access to all of the groups in the organization. For more granular control, grant access within the settings for that group.
Advanced Settings	
Generate Trend Data	When enabled, Tenable Security Center generates trend data by taking periodic snapshots of the cumulative database. Trend data is displayed in some Tenable Security Center tools (e.g., trending line charts and trending area charts). Tenable Security Center also produces differential data (snapshot comparison data), which improves performance when displaying trend data in Tenable Security Center tools. **Tip:** Disable this option to reduce your disk space usage.
Days Trending	Specifies the number of days of cumulative vulnerability data that you want Tenable Security Center to display in dashboard and report vulnerability trending displays.
Enable Full Text Search	When enabled, Tenable Security Center includes vulnerability text in periodic snapshots of .nessus data for vulnerability trending purposes. For more information about the **Vulnerability Text** filter component, see Vulnerability Analysis Filter Components.
Vulnerability Data Lifetime (Data Expiration Settings)	

Option	Description
Active	The number of days you want Tenable Security Center to retain agent scan vulnerability data stored in agent repositories. The default value of this option is *365* days.
Compliance	The number of days you want Tenable Security Center to retain audit compliance data stored in repositories. The default value of this option is *365* days.
Mitigated	The number of days you want Tenable Security Center to retain mitigated vulnerability data. The default value of this option is *365* days.

Universal Repositories

Universal repositories can store data from Tenable Nessus, Tenable Agent, and Tenable OT Security scans, as well as IPv4 and IPv6 data from Tenable Network Monitor, and Log Correlation Engine scans.

Tenable Security Center assigns UUIDs to assets to uniquely identify vulnerability data in universal repositories, since not all operational technology assets have IP addresses or Tenable UUIDs.

For more information, see Add a Repository.

Universal Repository Options

Option	Description
General	
Name	The repository name.
Description	(Optional) A description for the repository.
Data	
IP Ranges	Specifies the IP address range of vulnerability data you want to store in the repository. Type the range as a comma-delimited list of IP addresses, IP address ranges, and/or CIDR blocks.

Option	Description
	Note: Agent scans and Tenable OT Security scans into universal repositories are not restricted by IP range.
Access	
Organizations	Specifies which organizations have access to the vulnerability data stored in the repository. If groups are configured for the organization, Tenable Security Center prompts you to grant or deny access to all of the groups in the organization. For more granular control, grant access within the settings for that group.
Advanced Settings	
Generate Trend Data	When enabled, Tenable Security Center generates trend data by taking periodic snapshots of the cumulative database. Trend data is displayed in some Tenable Security Center tools (e.g., trending line charts and trending area charts). Tenable Security Center also produces differential data (snapshot comparison data), which improves performance when displaying trend data in Tenable Security Center tools. **Tip:** Disable this option to reduce your disk space usage.
Days Trending	Specifies the number of days of cumulative vulnerability data that you want Tenable Security Center to display in dashboard and report vulnerability trending displays.
Enable Full Text Search	When enabled, Tenable Security Center includes vulnerability text in periodic snapshots of .nessus data for vulnerability trending purposes. For more information about the **Vulnerability Text** filter component, see Vulnerability Analysis Filter Components.
Vulnerability Data Lifetime (Data Expiration Settings)	

Option	Description
Active	The number of days you want Tenable Security Center to retain active scan vulnerability data stored in universal repositories. The default value of this option is *365* days.
Passive	The number of days you want Tenable Security Center to retain passive scan vulnerability data stored in universal repositories. The default value of this option is *7* days.
Event	The number of days you want Tenable Security Center to retain event data stored in universal repositories. The default value of this option is *365* days.
Compliance	The number of days you want Tenable Security Center to retain audit compliance data stored in universal repositories. The default value of this option is *365* days.
Mitigated	The number of days you want Tenable Security Center to retain mitigated vulnerability data stored in universal repositories. The default value of this option is *365* days.

External Repositories

When adding an *external repository*, you access a local repository from another Tenable Security Center:

- Offline repositories allow you to share repository data from one Tenable Security Center deployment to your primary Tenable Security Center deployment via manual export and import (a `.tar.gz` archive file). You can combine data from several repository files into a single offline repository by importing multiple files to the offline repository.

- Remote repositories allow you to share repository data from one Tenable Security Center deployment to your primary Tenable Security Center deployment via an SSH session. By default, Tenable Security Center uses ECDSA keys for remote repository authentication.

External repository data is static and used solely for reporting purposes. For more information, see Offline Repository Options and Remote Repositories.

For more information, see Repositories and Add a Repository.

Offline Repositories

Offline repositories allow you to share repository data from one Tenable Security Center deployment to your primary Tenable Security Center deployment via manual export and import (a `.tar.gz` archive file). You can combine data from several repository files into a single offline repository by importing multiple files to the offline repository.

Offline repositories are particularly useful to export data from air-gapped instances of Tenable Security Center. For more information, see Considerations for Air-Gapped Environments.

> **Note:** You cannot set an offline repository as the **Import Repository** for active scans. You can only use offline repository data for reporting purposes.

To fully configure an offline repository:

1. Add an offline repository to your primary Tenable Security Center deployment.

2. Export one or more repositories from your other Tenable Security Center deployment.

3. Import one or more repositories to the offline repository on your primary Tenable Security Center deployment.

Offline Repository Options

Option	Description
General	
Name	The repository name.
Description	(Optional) A description for the repository.
Access	
Data Type	The type of data in the other Tenable Security Center repository: **IPv4**, **IPv6**, **Mobile**, **Agent**, or **Universal**.
IP Ranges	If the **Data Type** is **IPv4** or **IPv6**, specifies the IP address range of vulnerability data that you want to view in the offline repository. For example, to view all data from the exported repository file, specify a range that includes all data in that repository.

Option	Description
	Type the range as a comma-delimited list of IP addresses, IP address ranges, and/or CIDR blocks. For more information, see IPv4/IPv6 Repositories.
Type	If the **Data Type** is **Mobile**, the type of mobile repository: **ActiveSync**, **AirWatch MDM**, **Apple Profile Manager**, **Blackberry UEM**, **Good MDM**, **Microsoft Intune**, or **Mobile Iron**. For more information, see Mobile Repositories.
Access	
Organizations	Specifies which organizations have access to the vulnerability data stored in the repository. If groups are configured for the organization, Tenable Security Center prompts you to grant or deny access to all of the groups in the organization. For more granular control, grant access within the settings for that group.
Advanced Settings	
Generate Trend Data	When enabled, Tenable Security Center generates trend data by taking periodic snapshots of the cumulative database. Trend data is displayed in some Tenable Security Center tools (e.g., trending line charts and trending area charts). Tenable Security Center also produces differential data (snapshot comparison data), which improves performance when displaying trend data in Tenable Security Center tools. **Tip:** Disable this option to reduce your disk space usage.
Days Trending	Specifies the number of days of cumulative vulnerability data that you want Tenable Security Center to display in dashboard and report vulnerability trending displays.

Option	Description
Enable Full Text Search	When enabled, Tenable Security Center includes vulnerability text in periodic snapshots of .nessus data for vulnerability trending purposes. For more information about the **Vulnerability Text** filter component, see Vulnerability Analysis Filter Components.

Remote Repositories

Remote repositories allow you to share repository data from one Tenable Security Center deployment to your primary Tenable Security Center deployment via an SSH session. By default, Tenable Security Center uses ECDSA keys for remote repository authentication.

> **Note:** You cannot set a remote repository as the **Import Repository** for active scans. You can use remote repository data only for reporting purposes.

> **Note:** Ensure all your Tenable Security Center deployments are running the same version. For example, if your remote repository exists on a Tenable Security Center running a later version than your primary Tenable Security Center deployment, upgrade your primary Tenable Security Center deployment to the same version.

For more information, see Add a Repository.

To use tiered remote repositories for large enterprise deployments of Tenable Security Center, see Tiered Remote Repositories.

Option	Description
General	
Name	The repository name.
Description	(Optional) A description for the repository.
Remote Tenable Security Center	
Host	The IP address for the host you want to synchronize with to obtain repository data. After you type the IP address: 1. Click **Request Repositories**.

Option	Description
	2. Type the username and password for an administrator account on the remote Tenable Security Center.
	The Tenable Security Center deployments exchange SSH keys, and the system populates the **Repository** list with all available repositories from the remote Tenable Security Center.
Repository	The remote repository you want to collect IP addresses and vulnerability data from.
Update Schedule	Sets the schedule for the remote server to be queried for updated information.
Access	
Organizations	Specifies which organizations have access to the vulnerability data stored in the repository.
	If groups are configured for the organization, Tenable Security Center prompts you to grant or deny access to all of the groups in the organization. For more granular control, grant access within the settings for that group.

Tiered Remote Repositories

Remote repositories allow you to share repository data from one Tenable Security Center deployment to your primary Tenable Security Center deployment via an SSH session. By default, Tenable Security Center uses ECDSA keys for remote repository authentication.

A *tiered remote repository* configuration uses remote repositories to share data between multiple Tenable Security Center instances.

- For environments that support more than 100,000 hosts or multiple Tenable Security Center consoles, Tenable recommends Tenable Security Center Director to provide additional operational insight to your Tenable environment.

- If you plan to support 100,000-249,999 hosts, Tenable recommends a tiered remote repository configuration.

- If you plan to support 250,000 or more hosts, Tenable **requires** a tiered remote repository configuration.

Tiered Tenable Security Center instances perform informal roles in your overall Tenable Security Center deployment. Tenable recommends at least one designated reporting Tenable Security Center and an additional Tenable Security Center instance for every 100,000 to 150,000 hosts on your network.

- A *scanning tier* Tenable Security Center optimizes scanning by managing scan jobs across your attached scanners. Scanning tier Tenable Security Center instances prioritize efficient collection of scan data.

- A *reporting tier* Tenable Security Center optimizes dashboards and reporting by centralizing the data collected by scanning tier Tenable Security Center instances. Tenable Security Center Director can serve as a reporting tier, bringing in data from scanning tiers as remote repositories and providing insight to operational activities such as active scan jobs, plugin updates, and scanner configurations.

> **Note:** Your scanning tier and reporting tier Tenable Security Center instances must be running the same Tenable Security Center version.

Without a tiered remote repository configuration, enterprise-scale scanning and analysis may cause performance issues on a single Tenable Security Center. Tiered remote repositories optimize your analysis and report generation without negatively impacting scanning performance.

For more information, see Configure Tiered Remote Repositories.

> **Tip:** Configuring tiered remote repositories does not allow you to monitor the status of scanning tier Tenable Security Center instances. To monitor the status of multiple Tenable Security Center instances, connect your Tenable Security Center instances to Tenable Security Center Director. For more information about Tenable Security Center Director, see the *Tenable Security Center Director User Guide*.

Configure Tiered Remote Repositories

You may want to configure tiered remote repositories in large deployments of Tenable Security Center. For more information, see Tiered Remote Repositories.

To configure a tiered remote repository deployment:

1. On the scanning tier Tenable Security Center instance, create one or more repositories for storing scan result data.

> **Note:** To view trend data for scanning tier Tenable Security Center instances on your reporting tier Tenable Security Center instance, enable the **Generate Trend Data** option for each repository on your scanning tier Tenable Security Center instances. For more information, see Agent Repositories and IPv4/IPv6 Repositories.

2. On the scanning tier Tenable Security Center instance, run scans to populate the repositories with data.

3. On the reporting tier Tenable Security Center instance, create a remote repository for each repository on your scanning tier Tenable Security Center instance.

   The reporting tier Tenable Security Center syncs scan result data from the scanning tier Tenable Security Center repositories.

Active Scans

In active scanning, the scanner sends packets to a remote target to provide a snapshot of network services and applications. Tenable Security Center compares this data to a plugin database to determine if any vulnerabilities are present. Tenable Security Center can also use a scanner located outside the local network to simulate what an external entity might see.

For more information about supported active scanner types (Tenable Nessus and Tenable Vulnerability Management deployments) in Tenable Security Center, see Tenable Nessus Scanners.

You can use credentialed Tenable Nessus scans, a type of active scanning, to perform highly accurate and rapid patch, configuration, and vulnerability audits on Unix, Windows, Cisco, and database systems by actually logging in to the target system with provided credentials. Credentialed scans can also enumerate all UDP and TCP ports in just a few seconds. Tenable Security Center can manage these credentials securely across thousands of different systems and also share the results of these audits only with users who need to access them.

For more information, see Manage Active Scans and Active Scan Settings.

To fully configure active scans using a Tenable Nessus or Tenable Vulnerability Management scanner:

1. If you are configuring a Tenable Nessus scanner (not a Tenable Vulnerability Management deployment), configure scanning in Tenable Nessus, as described in Scans in the *Tenable Nessus User Guide.*

> **Note:** For information about credentialed scanning in Tenable Nessus, see Credentialed Checks in the *Tenable Nessus User Guide.*

2. Add the Tenable Nessus scanner or your Tenable Vulnerability Management deployment in Tenable Security Center, as described in Tenable Nessus Scanners.

3. Add a scan zone in Tenable Security Center, as described in Add a Scan Zone.

4. Add a repository for the scan data in Tenable Security Center, as described in Add a Repository.

5. Create active scan objects in Tenable Security Center, as described in:

    a. Add a Template-Based Asset or Add a Custom Asset.

    b. Add Credentials.

    c. Add a Template-Based Audit File or Add a Custom Audit File.

    d. Add a Scan Zone.

    e. Add a Scan Policy.

6. Add an active scan in Tenable Security Center, as described in Add an Active Scan.

What to do next:

- View scan results, as described in Scan Results.
- View vulnerability data by IP address, as described in Vulnerability Analysis.

Special Active Scans

Diagnostic Scans

If you experience issues with an active scan, Tenable Support may ask you to run a diagnostic scan to assist with troubleshooting. After Tenable Security Center runs the diagnostic scan, download the diagnostic file and send it to Tenable Support.

For more information, see Run a Diagnostic Scan.

Remediation Scans

You can run a remediation scan to run a followup active scan against existing active scan results. A remediation scan evaluates a specific plugin against a specific target or targets where the related vulnerability was present in your earlier active scan.

For more information, see Launch a Remediation Scan.

Add an Active Scan

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For more information about active scan options, see Active Scan Settings.

Note: If you are scanning a Linux machine with Tenable Security Center, the Linux machine's shell configuration file must have a `PS1` variable of four or more characters (for example, `PS1='\u@\h:~\$ '`). Having a `PS1` variable of less than four characters (for example, `PS1='\$ '`) can drastically increase the overall scan time.

Before you begin:

- Confirm you are running Tenable Nessus 6.3.6 or later.

- Confirm you understand the complete scanning configuration process, as described in Active Scans.

To add an active scan:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Scans** > **Active Scans**.

   The **Active Scans** page appears.

3. Click **Add**.

   The **Add Active Scan** page appears.

4. Click **General**.

5. Type a **Name** for the scan.

6. (Optional) Type a **Description** for the scan.

7. Select a **Policy** for the scan.

8. (Optional) If you want to schedule the scan to run automatically, select a **Schedule** for the scan.

9. Click **Settings**.

   The **Settings** tab appears.

10. If prompted, select a preconfigured **Scan Zone** for the scan.

11. Select an **Import Repository** for the scan.

12. Select a **Scan Timeout Action** for the scan.

13. Select a **Rollover Schedule** for the scan.

14. Enable or disable the **Advanced** options.

15. Click **Targets**.

    The **Targets** tab appears.

16. Select a **Target Type** for the scan.

17. Select one or more **Assets** and **IPs / DNS Names** for the scan.

18. (Optional) To configure credentialed scanning, do the following:

    a. Click **Credentials**.

       The **Credentials** tab appears.

    b. Click **Add Credential**.

    c. In the drop-down boxes, select a credential type and a preconfigured credential.

    d. Click the check mark to save your selection.

19. (Optional) If you want to configure multiple credentials for the active scan, repeat step 19.

> **Note:** When running an active scan, Tenable Security Center attempts authentication using the newest credentials added by an Administrator user. If the newest Administrator-

added credentials do not match, Tenable Security Center attempts authentication with older Administrator-added credentials.

Then, if no Administrator-added credentials match, Tenable Security Center attempts to authenticate using the newest credentials added by an organizational user. If the newest organizational user-added credentials do not match, Tenable Security Center attempts authentication with older organizational user-added credentials.

If no credentials match, the scan runs without credentialed access.

20. (Optional) To configure post-scan options, do the following:

   a. Click **Post Scan**.

      The **Post Scan** tab appears.

   b. To configure automatic report generation, click **Add Report**.

   c. Select the report you want to run after the scan completes, as described in Add a Report to a Scan.

21. Click **Submit**.

   Tenable Security Center saves your configuration.

Configure vSphere Scanning

Required Tenable Security Center User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can configure a scan policy to scan the following virtual environments:

- ESXi/vSphere that vCenter manages

- ESXi/vSphere that vCenter does not manage

- Virtual machines

Note: You must provide an IPv4 address when scanning an ESXi host. Otherwise, the scan fails.

About VMware Credentialed Checks

Configuring the vCenter API or ESXi API credentials enables the collection of VMware Installation Bundle (VIB) package details for ESXi servers, which are used in the ESX Local

Security Checks plugin family. Both of these credentials enable the collection of ESXi VIBs. Configuring an SSH credential to a targeted ESXi server also enables the collection of VIBs.

In addition to collection of ESXi VIBs, the vCenter credential enables auto-discovery of ESXi servers and vCenter compliance checks. In the case of vCenter compliance checks, the vCenter server must be configured as a target.

These credentials do not collect any host-level data about the vCenter server. To collect host-level data, configure an additional credential to the vCenter server (for example, SSH or Windows).

Tenable also collects ESXi and vCenter versions by detecting the software on the targeted hosts using remote, unauthenticated checks. Current vCenter and ESXi vulnerability results are based on this data.

For more information on VMware/vCenter, refer to the [VMware integration documentation](#).

Scanning ESXi/vSphere Not Managed by vCenter

To configure an ESXi/vSphere scan that vCenter does not manage:

1. Begin configuring a scan policy that supports credentialed access, as described in [Add a Scan Policy](#). For more information about authentication options in scan policies, see [The Authentication tab specifies authentication options during a scan.](#).

2. In the left navigation menu, click **Authentication**.

   The **Authentication** tab appears.

3. Click **Add Authentication Settings**.

   The authentication options appear.

4. In the first **Type** drop-down box, select **Miscellaneous**.

5. In the second **Type** drop-down box, select **VMware ESX SOAP API**.

6. Click **Select**.

   The VMware ESX SOAP API options appear. For more information, see [VMware ESX SOAP API](#).

7. In the **Username** box, type the username associated with the local ESXi account.

8. In the **Password** box, type the password associated with the local ESXi account.

9. If your vCenter host includes an SSL certificate (not a self-signed certificate), disable the **Do not verify SSL Certificate** toggle.

10. Click the ✔ button.

   Tenable Security Center applies the VMware ESX SOAP API authentication options to the scan policy.

What to do next:

- Reference the scan policy in an active scan configuration, as described in <u>Add an Active Scan</u>.

Scanning vCenter-Managed ESXi/vSpheres

> **Note:** The SOAP API requires a vCenter admin account with read and write permissions. The REST API requires a vCenter admin account with read permissions, and a VMware vSphere Lifecycle manager account with read permissions.

To configure an ESXi/vSphere scan managed by vCenter:

1. Begin configuring a scan policy that supports credentialed access, as described in <u>Add a Scan Policy</u>. For more information about authentication options in scan policies, see <u>The Authentication tab specifies authentication options during a scan.</u>.

2. In the left navigation menu, click **Authentication**.

   The **Authentication** tab appears.

3. Click **Add Authentication Settings**.

   The authentication options appear.

4. In the first **Type** drop-down box, select **Miscellaneous**.

5. In the second **Type** drop-down box, select **VMware vCenter SOAP API**.

6. Click **Select**.

   The VMware vCenter SOAP API options appear. For more information, see <u>VMware vCenter SOAP API</u>.

7. In the **vCenter Host** box, type the IP address of the vCenter host.

8. In the **vCenter Port** box, type the port for the vCenter host.

9. In the **Username** box, type the username associated with the local vCenter account.

10. In the **Password** box, type the password associated with the local vCenter account.

11. If the vCenter host is not SSL enabled, disable the **HTTPS** toggle.

12. If your vCenter host includes an SSL certificate (not a self-signed certificate), enable the **Verify SSL Certificate** toggle.

13. Click the ✔ button.

    Tenable Security Center applies the VMware vCenter SOAP API authentication options to the scan policy.

> **Note:** When scanning vCenter-managed ESXis with API credentials, the Nessus Scan information plugin always shows `Credentialed Checks: No` in the vCenter scan results. To verify that the authentication was successful, check to see that the Nessus Scan Information plugin shows `Credentialed Checks: Yes` in the scan results of the ESXis.

What to do next:

- Reference the scan policy in an active scan configuration, as described in Add an Active Scan.

Scanning Virtual Machines

You can scan virtual machines just like any other host on the network. Be sure to include the IP addresses of virtual machines you want to scan in your scan targets. For more information, see Add an Active Scan.

VMware vCenter Support Matrix

Feature	Requires Authentication	Supported vCenter Version
Vulnerability Management	No	7.x, 8.x
Auto Discovery	Yes	7.0.3+, 8.x
Audit / Compliance	Yes	6.x, 7.x, 8.x

VIB Enumeration	Yes	7.0.3+, 8.x
Active / Inactive VMs	Yes	7.0.3+, 8.x

Manage Active Scans

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information about active scans, see Active Scans.

To manage active scans:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Active Scans**.

   The **Active Scans** page appears.

3. To filter the scans that appear on the page, apply a filter as described in Apply a Filter.

4. To start or pause a scan, see Start or Pause a Scan.

5. To suspend or resume a scheduled scan, see Suspend or Resume a Scheduled Active Scan.

6. To view details for a scan:

   a. Right-click the row for the scan.

      The actions menu appears.

      -or-

      Select the check box for the scan.

      The available actions appear at the top of the table.

   b. Click **View**.

      The **View Active Scan** page appears.

7. To edit a scan:

a. Right-click the row for the scan.

The actions menu appears.

-or-

Select the check box for the scan.

The available actions appear at the top of the table.

b. Click **Edit**.

The **Edit Active Scan** page appears.

c. Modify the scan options.

d. Click **Submit**.

Tenable Security Center saves your configuration.

8. To copy a scan:

a. Right-click the row for the scan.

The actions menu appears.

-or-

Select the check box for the scan.

The available actions appear at the top of the table.

b. Click **Copy**.

Tenable Security Center creates a copy of the scan.

To copy multiple scans:

a. In the table, select the check box for each scan you want to copy.

The available actions appear at the top of the table.

b. At the top of the table, click **Copy**.

A confirmation window appears.

c. Click **Copy**.

Tenable Security Center creates a copy of the scan.

9. To run a diagnostic scan, see [Run a Diagnostic Scan](#).

10. To delete a scan:

    a. In the table, right-click the row for the scan.

       The actions menu appears.

    b. Click **Delete**.

       A confirmation window appears.

    c. Click **Delete**.

       Tenable Security Center deletes the scan.

    To delete multiple scans:

    a. In the table, select the check box for each scan you want to delete.

       The available actions appear at the top of the table.

    b. At the top of the table, click **Delete**.

       A confirmation window appears.

    c. Click **Delete**.

       Tenable Security Center deletes the scans.

Start or Pause a Scan

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see [User Roles](#).

To start or pause a scan or synchronization job:

1. Log in to Tenable Security Center.

2. Click one of the following:

- **Scans** > **Active Scans** (to manage active scans)

- **Scans** > **Agent Synchronization Jobs** (to manage agent synchronization jobs)

- **Scans** > **Agent Scans** (to manage agent scans)

  > **Note:** You cannot pause agent scans in Tenable Security Center.

- **Scans** > **Scan Results** (to manage a scan from the results page).

3. Do one of the following:

   - To pause the scan or synchronization job, select the check box for the scan or synchronization job, and click **Pause** at the top of the table.

   - To start the scan or synchronization job, select the check box for the scan or synchronization job, and click **Launch** at the top of the table.

Suspend or Resume a Scheduled Active Scan

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

If you suspend a scheduled active scan, Tenable Security Center stops launching new scans for that active scan configuration. Tenable Security Center does not disrupt scans already in progress or prevent users from launching scans on demand.

If you resume a suspended active scan, Tenable Security Center resumes launching scans on the schedule configured for that active scan.

For more information, see Active Scans.

Before you begin:

- Configure a scheduled active scan, as described in Add an Active Scan.

To suspend or resume a scheduled active scan:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Active Scans**.

   The **Active Scans** page appears.

3. Right-click the row for the scheduled scan you want to suspend or resume.

   The actions menu appears.

   -or-

   Select the check box for the scheduled scan you want to suspend or resume.

   The available actions appear at the top of the table.

4. Click **Suspend Schedule** or **Resume Schedule**.

   The page updates to reflect the scan schedule status. When a scan is suspended, Tenable Security Center displays a line through the **Start Time** and **Schedule** values.

Run a Diagnostic Scan

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

If you experience issues with an active scan, Tenable Support may ask you to run a diagnostic scan to assist with troubleshooting. After Tenable Security Center runs the diagnostic scan, download the diagnostic file and send it to Tenable Support.

Before you begin:

- Add an active scan, as described in Add an Active Scan.

- Confirm the scanner associated with the active scan is running a supported version of Tenable Nessus. For minimum Tenable Nessus scanner version requirements, see the Tenable Security Center Release Notes for your version.

To run a diagnostic scan:

1. Click **Scans** > **Active Scans**.

2. Right-click the row for the scan where you want to run a diagnostic scan.

   The actions menu appears.

   -or-

   Select the check box for the scan where you want to run a diagnostic scan.

The available actions appear at the top of the table.

3. Click **Run Diagnostic Scan**.

> **Note:** You must resolve repository errors before running a diagnostic scan.

4. In the **Diagnostic Target** box, type a target as a single IPv4 address, IPv6 address, or hostname. The target must also be specified in the active scan's **Targets**.

5. In the **Diagnostic Password** box, type a password to secure the diagnostic file.

6. Click **Submit**.

   The diagnostic scan runs and finishes.

7. Click **Scans** > **Scan Results**.

8. Locate the diagnostic scan and confirm that the scan finished without errors.

9. Right-click the row for the diagnostic scan result.

   The actions menu appears.

   -or-

   Select the check box for the diagnostic scan result.

   The available actions appear at the top of the table.

10. Click **Download Diagnostic Info**.

    The diagnostic scan file downloads.

Active Scan Settings

For more information, see Add an Active Scan.

- Parameter

- Parameter

- The Targets section identifies the devices Tenable Security Center scans.

- The Credentials section allows users to select pre-configured credential sets for authenticated scanning. For more information, see Credentials.

- [These options determine what actions occur immediately before and after the active scan completes.](#)

General Options

Parameter	Description
General	
Name	The scan name that is associated with the scan's results and may be any name or phrase (for example, *SystemA*, *DMZ Scan*, or *Daily Scan of the Web Farm*).
Description	Descriptive information related to the scan.
Policy	The policy on which you want to base the scan. You can scroll through the list, or search by entering text in the search box at the top of the list of available policies.
Schedule	
Schedule	The frequency you want to run the scan. • **Now** specifies that you want Tenable Security Center to launch the scan immediately without saving the configuration for later. **Note:** Scans configured to run **Now** do not appear on the **Active Scans** page. • **Once** specifies that you want Tenable Security Center to launch the scan at the specified time without saving the configuration for later. **Note:** Scans configured to run **Once** do not appear on the **Active Scans** page. • **Daily**, **Weekly**, or **Monthly** specifies that you want Tenable Security Center to launch the scan at a scheduled interval. **Note:** If you schedule your scan to repeat monthly, Tenable recommends setting a start date no later than the 28th day. If you select a start date

Parameter	Description
	that does not exist in some months (e.g., the 29th), Tenable Security Center cannot run the scan on those days.
	• **On Demand** specifies that you want to manually launch the scan at any time.
	• **Dependent** specifies that you want Tenable Security Center to launch the scan every time Tenable Security Center finishes a scheduled run of the dependent scan you select.

Settings Options

Parameter	Description
Basic	
Scan Zone	**Note:** If your organization's **Distribution Method** setting is **Locked Zone**, you cannot modify this setting. If your organization's **Distribution Method** setting is **Automatic Distribution Only**, Tenable Security Center automatically chooses one or more scan zones and hides this setting.
	Specifies the scan zone you want to use to run the scan. Depending on your organization's **Distribution Method** setting, you can select one of the following:
	• An available zone — use a single scan zone to run the scan.
	Note: If you select a single scan zone, Tenable Security Center ignores the ranges in the scan zone and scans all of the targets you specify in the scan configuration.
	• **Automatic Distribution** — allow Tenable Security Center to choose the best scan zone to run the scan.
	For more information, see Organizations and Scan Zones.
Import Repository	Specifies the repository where Tenable Security Center imports the scan results. Select a IPv4, IPv6, or Universal repository to receive IPv4 or IPv6

Parameter	Description
	results appropriate to the scan.
Scan Timeout Action	The action you want Tenable Security Center to perform in the event a scan is incomplete: • **Import Completed Results With Rollover** — (Default) The system imports the results from the scan into the database and creates a rollover scan that you can launch manually to complete the scan. • **Import Completed Results** — The system imports the results of the current scan and discards the information for the unscanned hosts. • **Discard Results** — The system does not import any of the results obtained by the scan to the database.
Rollover Schedule	If you set the Scan Timeout Action to **Import results with Rollover**, this option specifies how to handle the rollover scan. You can create the rollover scan as a template to launch manually, or to launch the next day at the same start time as the just-completed scan.
Advanced	
Scan Virtual Hosts	Specifies whether the system treats a new DNS entry for an IP address as a virtual host as opposed to a DNS name update. When Tenable Security Center finds a new DNS name for an IP address: • If **Scan Virtual Hosts** is enabled, vulnerability data for the two DNS names appears as two entries with the same IP address in the IP Summary analysis tool. • If **Scan Virtual Hosts** is disabled, vulnerability data for the two DNS names merge into a single IP address entry in the IP Summary analysis tool. If you import scan results from a Universal repository, this option does not appear. Universal repositories treat hosts with the same IP address but unique FQDNs as different hosts. For more information, see Universal

Parameter	Description
	Repositories.
Track hosts which have been issued new IP address	This option uses the DNS name, NetBIOS name, Agent ID, and MAC address (if known), in that order, to track a host when its IP address changes. Once Tenable Security Center finds a match, Tenable Security Center does not search further for matches.
	For example, if Tenable Security Center does not match a DNS name, but it does match a NetBIOS name, the system does not check the MAC address. Networks using DHCP require that you set this option to properly track hosts.
	If you import scan results from a Universal repository, this option does not appear. Universal repositories do not rely on IP addresses to track hosts. For more information, see Universal Repositories.
Immediately remove vulnerabilities from scanned hosts that do not reply	If a previously responsive host does not reply to a scan, Tenable Security Center removes the host's vulnerabilities from the cumulative database. If the host has vulnerabilities in the mitigated database, they remain in the mitigated database.
	• If you enable this option, the system removes the vulnerabilities immediately after the scan completes.
	• If you disable this option, the system removes the vulnerabilities according to the interval set in the **Number of days to wait before removing dead hosts** option.
Number of days to wait before removing dead hosts	If you disable **Immediately remove vulnerabilities from scanned hosts that do not reply**, this value specifies how many days the system waits to remove vulnerabilities.
Max scan duration (hours)	Specifies the maximum number of hours you want a scan to run.
	If a scan reaches this threshold, Tenable Security Center automatically creates a rollover scan that you can launch manually to complete the

Parameter	Description
	scan. Tenable Security Center creates a rollover scan regardless of your **Scan Timeout Action** setting. **Note**: If there is a scan window set, the **Max scan duration** setting must be longer than the scan window to allow time to generate the scan results.
Inactivity timeout duration (hours)	This setting specifies the maximum number of hours a scan will wait for a plugin to run before switching to a different scanner. The default value is 12 hours. You can specify a value from 1 to 120 hours. The value for **Inactivity timeout duration** must be less than the value for **Max scan duration**.

Targets Options

The **Targets** section identifies the devices Tenable Security Center scans.

Option	Description
Target Type	Specifies the target type for the scan: • **Assets** — Scan one or more assets. For more information, see [Assets](#). • **IP / DNS Name** — Scan one or more IP addresses or DNS names. • **Mixed**—Scan a combination of asset lists, IP addresses, and DNS names.
Assets	(Available if **Target Type** is **Assets** or **Mixed**) The list of assets to scan. Click to select or deselect the assets you want to scan.
IPs / DNS Names	(Available if **Target Type** is **IP / DNS Name** or **Mixed**) The IP addresses or DNS names you want to scan. Specify IP addresses and DNS names using the following valid formats: • A single IPv4 address (for example, 192.0.2.202) • A single IPv6 address (for example,

	2001:db8:d54e:cca6:4109:ac02:2fbe:134e)
	• An IP address range in dot-decimal or CIDR notation (for example, 192.0.2.0-192.0.2.255 or 192.0.2.0/24)
	• A resolvable hostname (for example, www.yourdomain.com)
	Note: You can only scan IPv4 and IPv6 addresses when using Universal Repositories.

Credentials Options

The **Credentials** section allows users to select pre-configured credential sets for authenticated scanning. For more information, see Credentials.

Tenable Security Center active scans support the following credential types:

- Windows Credentials
- SSH Credentials
- SNMP Credentials
- Database Credentials
- API Gateway Credentials
- Miscellaneous Credentials

Post Scan Options

These options determine what actions occur immediately before and after the active scan completes.

Option	Description
Reports to Run on Scan Completion	
Add Report	This option provides a list of reports available to the user to run when the scan completes. For more information, see Add a Report to a Scan.

Launch a Remediation Scan

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can run a remediation scan to run a followup active scan against existing active scan results. A remediation scan evaluates a specific plugin against a specific target or targets where the related vulnerability was present in your earlier active scan.

Remediation scans allow you to validate whether your vulnerability remediation actions on the targets have been successful. If a remediation scan cannot identify a vulnerability on targets where it was previously identified, the system changes the status of the vulnerability to mitigated. For more information, see Cumulative vs. Mitigated Vulnerabilities.

Note the following:

- You can perform remediation scans only for active scan results.

- You cannot perform remediation scans for agent repository scan results.

- You cannot perform remediation scans for Tenable OT Security scan results.

- If the selected plugin requires dependent plugins, the system automatically includes those plugins in the remediation scan.

- Remediation scans only evaluate plugins against the port you specify. Keep this in mind when launching a remediation scan for a plugin that typically targets multiple ports.

- See the Understanding Tenable Security Center Mitigations knowledge base article for more information on mitigation logic.

- When you launch a remediation scan from a vulnerability in the **Vulnerability List** or **Vulnerability Detail List** views under **Analysis > Vulnerabilities**, the remediation scan will pre-populate the *Repository*, *Target IP Address*, and *Port* fields with those of the finding being viewed.

- When you launch a remediation scan from a vulnerability in the **Vulnerability Summary** view under **Analysis > Vulnerabilities**, the *Repository*, *Target IP Address*, and *Port* fields will be set to the default values or will be empty, because there could be multiple repositories, IPs, and ports in use.

> **Note:** If you are scanning a Linux machine with Tenable Security Center, the Linux machine's shell configuration file must have a `PS1` variable of four or more characters (for example, `PS1='\u@\h:~\$ '`).

Having a `PS1` variable of less than four characters (for example, `PS1='\$ '`) can drastically increase the overall scan time.

To launch a remediation scan:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.

3. In the analysis tools drop-down box, select **Vulnerability Summary**.

   The page refreshes to show the analysis tool view you selected.

4. Right-click the row for the vulnerability for which you want to launch a remediation scan and click **Launch Remediation Scan**.

   The **Launch Remediation Scan** page appears.

   > **Note:** A remediation scan inherits certain settings from the vulnerability or vulnerability instance you selected. The **Launch Remediation Scan** page:
   >
   > - Automatically populates the relevant plugin information.
   >
   > - Provides an editable scan name in the format "Remediation Scan of Plugin # *number*".
   >
   > - Populates the target IP address based on the asset where the previous scan identified the vulnerability.

5. Configure the settings for the scan, as described in [Active Scan Settings](#).

   > **Note:** You do not need to associate the remediation scan with a scan policy.

   > **Note:** You cannot schedule a remediation scan. The scan launches as soon as you submit it.

6. Click **Submit**.

   Tenable Security Center launches the remediation scan.

Attack Surface Domain Discovery

On the **Attack Surface Domain Discovery** page, you can manage your domains. When you add a domain, Tenable Security Center identifies internet-accessible assets associated with the domain that may not otherwise be visible to your organization. Tenable Security Center uses DNS records, IP addresses, and Autonomous System Numbers (ASN) to identify assets.

To view a list of assets identified on your domain, see the **Domain Inventory Assets** page.

For more information about domain inventory assets, see:

- View Domain Inventory Assets

- Export Domain Inventory Assets

To view your domains:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Scans** > **Attack Surface Domain Discovery**.

   The **Attack Surface Domain Discovery** page appears.

3. (Optional) Add your organization's domain to begin identifying assets.

4. Click **Submit**.

   Tenable Security Center saves your configuration.

Add a Domain

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

Note: You can add a maximum of two domains across your system.

When you add a domain, Tenable Security Center identifies internet-accessible assets associated with the domain. For more information, see Attack Surface Domain Discovery.

To add a domain:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Scans** > **Attack Surface Domain Discovery**.

The **Attack Surface Domain Discovery** page appears.

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

    The **Add Domain** panel appears.

4. In the **Add a Domain to Your Inventory** box, type your organization's domain.

5. Click **Submit**.

    Tenable Security Center saves your configuration.

What to do next:

- View the assets associated with your domain, as described in View Domain Inventory Assets.

- Export a CSV file of the assets associated with your domain, as described in Export Domain Inventory Assets.

View Domain Details

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information about domains, see Attack Surface Domain Discovery.

To view domain details:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Scans** > **Attack Surface Domain Discovery**.

    The **Attack Surface Domain Discovery** page appears.

3. In the table, select the domain you want to view.

    The **View Domain** panel appears, with details about the domain:

    - **Domain Name** — The name of the domain.

    - **Created Time** - When the domain was added to Tenable Security Center.

    - **Last Refresh** - The last time the list of domain assets was updated.

4. (Optional) Delete the domain.

Delete a Domain

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information about domains, see Attack Surface Domain Discovery.

To delete a domain:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Scans** > **Attack Surface Domain Discovery**.

    The **Attack Surface Domain Discovery** page appears.

3. In the table, select the domain you want to delete.

    The **View Domain** panel appears.

4. Click **Delete Domain**.

    A dialog box appears, confirming your selection to delete the domain.

5. Click **Delete**.

    The domain and related domain inventory assets are deleted.

Active Scan Objects

Complete Tenable Security Center scan configurations rely on the following scan objects. For information about active scans, see Active Scans.

Scan Object	Description
assets	Assets are lists of devices (for example, laptops, servers, tablets, or phones) within a Tenable Security Center organization. You can share assets with one or more users based on local security policy requirements.
	You can add an asset to group devices that share common attributes. Then, you can use the asset during scan configuration to target the devices in the asset.
	For more information, see Assets.

credentials	Credentials are reusable objects that facilitate a login to a scan target. You can configure various types of credentials with different authentication methods for use within scan policies. You can also share credentials between users for scanning purposes.
	Tenable Security Center supports an unlimited number of SSH, Windows, and database credentials, and four SNMP credential sets per scan configuration.
	For more information, see Credentials.
audit files	During a configuration audit, auditors verify that your server and device configurations meet an established standard and that you maintain them with an appropriate procedure. Tenable Security Center can perform configuration audits on key assets by using local Tenable Nessus checks that can log directly on to a Unix or Windows server without an agent.
	Tenable Security Center supports several audit standards. Some of these come from best practice centers like the PCI Security Standards Council and the Center for Internet Security (CIS). Some of these are based on Tenable's interpretation of audit requirements to comply with specific industry standards such as PCI DSS or legislation such as Sarbanes-Oxley.
	In addition to base audits, you can create customized audits for the particular requirements of any organization. You can upload customized audits into Tenable Security Center and make them available to anyone performing configuration audits within an organization.
	You can upload and use NIST SCAP files in the same manner as an audit file. Navigate to NIST's SCAP website (http://scap.nist.gov) and under the SCAP Content section, download the desired SCAP security checklist zip file. You can then upload the file to Tenable Security Center and select it for use in Tenable Nessus scan jobs.
	Once you configure audit scan policies in Tenable Security Center, you can use them as needed. Tenable Security Center can also perform audits intended for specific assets. A Tenable Security Center user can use audit policies and asset lists to determine the compliance posture of any specified asset.

	For more information, see [Audit Files](#).
scan zones	Scan zones represent areas of your network that you want to target in an active scan, associating an IP address or range of IP addresses with one or more scanners in your deployment. Scan zones define the IP address ranges associated with the scanner along with organizational access. For more information, see [Scan Zones](#).
scan policies	Scan policies contain options related to performing an active scan. For example: • Options that control technical aspects of the scan such as timeouts, number of hosts, type of port scanner, and more. • Options that provide plugin family-based or individual plugin-based scan specifications. • Options that control compliance policy checks (Windows, Linux, Database, etc.), report verbosity, service detection scan settings, audit files, patch management systems, and more. For more information, see [Scan Policies](#).

Assets

Tenable Security Center *assets* are lists of devices (for example, laptops, servers, tablets, or phones) within a Tenable Security Center organization. Assets can be shared with one or more users based on local security policy requirements.

You can add an asset to group devices that share common attributes. Then, you can use the asset during scan configuration to target the devices in the asset. Examples of common attributes include:

- IP address ranges

- hardware types

- vulnerabilities

- outdated software versions

- operating systems

Tenable Security Center supports template-based and custom assets. For more information, see Add a Template-Based Asset and Add a Custom Asset. To view details for any of your assets, see View Asset Details.

To view details about individual hosts that appear in your assets, see View Hosts and View Host Details.

> **Note:** When a scan import completes, it queues a job to calculate all dynamic and combination assets for the import repository. The next scan import does not begin until the previous scan import asset job completes. Usually the asset job runs quickly, but delays can occur due to extremely large repositories, a large quantity of assets, a backlogged job queue, or other system issues. This does not affect running scans.
>
> Asset lists are calculated for each repository, and updating one repository does not affect other repositories.

Template-Based Assets

Tenable provides asset templates that you can customize for your environment. Tenable-provided asset templates are updated via the Tenable Security Center feed and visible depending on other configurations.

Custom Assets

Tenable Security Center supports the following custom assets types: Static Assets, DNS Name List Assets, LDAP Query Assets, Combination Assets, Dynamic Assets, Watchlist Assets, and Import Assets.

Static Assets

Static assets are lists of IP addresses. You can use static assets immediately after configuration.

For example, if your organization assigns laptops within a defined IP address range, you can create a custom static asset for laptops using that IP address range.

Option	Description
Name	A name for the asset.
Description	A description for the asset.
Tag	A tag for the asset. For more information, see Tags.
IP Addresses	IP addresses to include within the asset (50,000 character limit). • Type a comma-separated list of IP addresses, CIDR addresses, or ranges. • Upload a `.txt` file containing a comma-separated list of IP addressees, CIDR addresses, or ranges.

DNS Name List Assets

> **Note:** You cannot select a DNS name list asset as the target of an agent scan or an agent synchronization job.

Option	Description
Name	A name for the asset.
Description	A description for the asset.
DNS Names	The DNS hostnames for the asset to be based on.

LDAP Query Assets

> **Note:** You cannot select an LDAP query asset as the target of an agent scan or an agent synchronization job.

The LDAP query asset type appears if your organization includes a configured LDAP server.

Option	Description
Name	A name for the asset.

Option	Description
Description	A description for the asset.
LDAP Server	The LDAP server where you want to perform the query. **Note:** If the LDAP server uses a different DNS server than Tenable Security Center, Tenable Security Center cannot resolve hostnames retrieved from the LDAP server. **Note:** Tenable Security Center cannot retrieve more than one page of LDAP results. If Tenable Security Center asset or user authentication queries are not retrieving all expected results, consider modifying your LDAP pagination control settings to increase the results per page.
Search Base	The LDAP search base used as the starting point to search for specific LDAP data.
Search String	Modify this string to create a search based on a location or filter other than the default search base or attribute.
Generate Preview	Click to display a preview query in the **Results Preview** section. The preview lists the LDAP data that matches the defined search string.

Combination Assets

Combination assets allow you to create an asset based on existing assets and the AND, OR, and NOT operators.

Combination assets can include agent IDs if the asset contains exclusively dynamic assets. You may experience unexpected asset behavior if your combination asset contains other asset types and interacts with agent repository data.

Option	Description
Name	A name for the asset.
Description	A description for the asset.
Combination	This option accepts multiple existing assets utilizing the operators AND,

Option	Description
	OR, and NOT. You can use these operators and multiple existing assets to create new unique assets. If the source assets change, the **Combination** asset updates to match the new conditions. To configure the query: 1. Click inside the **Combination** box. A list of assets appears. 2. Click one of the options in the list to select it. 3. Press Space. 4. Continue selecting options and pressing space to describe the combination asset you want to configure. **Tip:** A red border around a combination option indicates there is a problem in the query logic.

Dynamic Assets

Dynamic assets are flexible groups of condition statements that Tenable Security Center uses to retrieve a list of devices meeting the conditions. Tenable Security Center refreshes dynamic asset lists using the results from Tenable Security Center scans. You cannot use dynamic assets until after Tenable Security Center performs an initial discovery scan and retrieves a list of devices.

Note: Before a scan can target a dynamic asset list, you must first run a host discovery scan in the associated repository. For more information, see the troubleshooting article.

Note: If a dependent scan uses a dynamic asset list, the asset list will update before the scan runs.

Dynamic assets can include agent IDs.

Add Dynamic Asset

For example, in the asset above, Tenable Security Center retrieves a list of Linux systems listening on TCP Port 80.

Option	Description
Name	A name for the asset.
Description	A description for the asset.
Asset Definition	Defines the rules for creating a dynamic asset list. Hover over an existing rule to display the options to add, edit, or delete a group or a rule.

Dynamic Asset Rule Logic

Valid Operators	Effect
Plugin ID	

Valid Operators	Effect
is equal to	Value must be equal to value specified.
not equal to	Value must be not equal to value specified.
is less than	Value must be less than the value specified.
is greater than	Value must be greater than the value specified.
Plugin Text	
is equal to	Value must be equal to value specified.
not equal to	Value must be not equal to value specified.
contains the pattern	Value must contain the text specified (for example, ABCDEF contains ABC).
Posix regex	Any valid Posix regex pattern contained within "/" and "/" (example: /.*ABC.*/).
Perl compatible regex	Any valid Perl compatible regex pattern.
Operating System	
is equal to	Value must be equal to value specified.
not equal to	Value must be not equal to value specified.
contains the pattern	Value must contain the text specified (for example, ABCDEF contains ABC).
Posix regex	Any valid Posix regex pattern contained within "/" and "/" (for example, /.*ABC.*/).
Perl compatible regex	Any valid Perl compatible regex pattern.
IP Address	
is equal to	Value must be equal to value specified.

Valid Operators	Effect
not equal to	Value must be not equal to value specified.
DNS, NetBIOS Host, NetBIOS Workgroup, MAC, SSH v1 Fingerprint, SSH v2 Fingerprint	
is equal to	Value must be equal to value specified.
not equal to	Value must be not equal to value specified.
contains the pattern	Value must contain the text specified (for example, 1.2.3.124 contains 124).
Posix regex	Any valid Posix regex pattern contained within "/" and "/" (for example, /.*ABC.*/).
Perl compatible regex	Any valid Perl compatible regex pattern.
Port, TCP Port, UDP Port	
is equal to	Value must be equal to value specified.
not equal to	Value must be not equal to value specified.
is less than	Value is less than value specified.
is greater than	Value is greater than the value specified.
Days Since Discovery, Days Since Observation	
is equal to	Value must be equal to value specified (maximum *365*).
not equal to	Value must be not equal to value specified (maximum *365*).
is less than	Value is less than value specified (maximum *365*).
is greater than	Value is greater than the value specified (maximum *365*).
where Plugin ID is	Any valid plugin ID number. You can enter multiple plugin IDs using a range or comma-separated plugin IDs (for example, *3, 10189, 34598, 50000-55000, 800001-800055*).

Valid Operators	Effect
Severity	
is equal to	Value must be equal to value specified: **Info**, **Low**, **Medium**, **High**, or **Critical**.
not equal to	Value must be not equal to value specified: **Info**, **Low**, **Medium**, **High**, or **Critical**.
is less than	Value must be less than the value specified: **Info**, **Low**, **Medium**, **High**, or **Critical**.
is greater than	Value must be greater than the value specified: **Info**, **Low**, **Medium**, **High**, or **Critical**.
where Plugin ID is	Any valid plugin ID number. You can enter multiple plugin IDs using a range or comma-separated plugin IDs (for example, *3*, *10189*, *34598*, *50000-55000*, *800001-800055*).
Exploit Available	
Is	Click **True** or **False** in the drop-down box.
Exploit Frameworks	
is equal to	Value must be equal to value specified.
Is not equal to	Value must not be equal to value specified.
contains the pattern	Value must contain the pattern entered.
XRef	
Value must be in the XRef option.	

Watchlist Assets

You can use a watchlist asset to maintain lists of IPs that are not in the user's managed range of IP addresses. You can filter for IPs from a watchlist regardless of your IP address range configuration to help analyze event activity originating outside of the user's managed range. For example, if a

block of IP addresses is a known source of malicious activity, you could add it to a Malicious IPs watchlist and added to a custom query.

> **Note:** Watchlists only use event data to create the asset list.

Option	Description
Name	A name for the asset.
Description	A description for the asset.
IP Addresses	IP addresses to include within the asset list (20,000 character limit). You can enter one address, CIDR address, or range per line. Click **Choose File** to import a list of IP addresses from a saved file.

Import Assets

Option	Description
Name	The asset name.
Asset	Click **Choose File** to choose the asset that was previously exported for import into Tenable Security Center.

Add a Template-Based Asset

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For information, see Assets.

To add an asset from a Tenable-provided template:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Assets** > **Assets**.

   The **Assets** page appears.

3. Click **Add**.

The **Asset Templates** page appears.

4. (Optional) If you want to search for a specific asset template, type a search phrase in the **Search Templates** box.

5. In the **Common** section, click a template type.

   The **Add Asset Template** page for the template type appears.

6. View the available templates.

   - The four square icon ( ) on the left side indicates a collection of several assets.

   - The data icons (PVS LCE   NS) on the right side indicate the data required to build the asset. The Tenable Network Monitor (PVS), Log Correlation Engine, and NS icons indicate you must have Tenable Network Monitor, Log Correlation Engine, or Tenable Nessus data. The key icon ( ) indicates you must have credentials for the device. The notepad icon ( ) indicates you must have compliance data.

7. (Optional) If you want to search for a specific asset template, type a search phrase in the **Search Templates** box or select a category from the **All** drop-down box.

8. Click the row for the template you want to use.

   The detail page for the template type appears.

9. Click **Add**.

   The **Assets** page appears.

10. Click the row for the asset you just added.

    The **Edit** page appears.

11. View the details for the asset.

12. (Optional) If necessary, edit the asset to customize it for your environment. For more information about asset options, see [Assets](#).

13. Click **Submit**.

    Tenable Security Center saves your configuration.

Add a Custom Asset

For information, see Assets.

To add a custom asset:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Assets** > **Assets**.

   The **Assets** page appears.

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

   The **Asset Templates** page appears.

4. In the **Other** section, click an asset type.

   The **Add Assets** page for the asset type appears.

5. Configure the required options for the asset type, as described in Assets.

6. Click **Submit**.

   Tenable Security Center saves your configuration.

View Asset Details

You can view details for any asset. For more information, see Assets.

To view asset details:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Assets** > **Assets**.

   The **Assets** page appears.

3. Right-click the row for the asset you want to view.

   The actions menu appears.

-or-

Select the check box for the asset you want to view.

The available actions appear at the top of the table.

4. Click **View**.

The **View Asset** page appears.

Section	Action
General	View general information for the asset. • **Name** — The asset name. • **Description** — The asset description. • **Tag** — The tag applied to the asset. For more information, see Tags. • **IP Addresses** (static assets only) — The IP addresses specified in the asset. For more information, see Assets. • **Created** — The date the asset was created. • **Last Modified** — The date the asset was last modified. • **Owner** — The username for the user who created the asset. • **Group** — The group in which the asset belongs. • **ID** — The asset ID.
TenableSynchronization Data	View synchronization summary data: • **Status** — The status of the asset in Tenable Lumin synchronization: • **Finished** — The most recent synchronization that included this asset succeeded.

Section	Action
	• **Not Synced** — The asset is not configured for Tenable Lumin synchronization.
	• **Error** — An error occurred. For more information, see [View Tenable One Data Synchronization Logs]().
	• **First Synchronization** — The date and time of the first synchronization of this asset.
	• **Last Success** — The date and time of the most recent synchronization of this asset.
	• **Last Failure** — The date and time of the most recent failed synchronization of this asset.
	• **Details** — If the **Status** is **Error**, details about the error.
	For more information about Tenable Lumin synchronization, see [Tenable One Synchronization]().

View Hosts

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles]().

You can view a list of hosts associated with asset lists. For more information, see [Assets]().

To view details for an individual host, see [View Host Details]().

To view the list of hosts:

1. Log in to Tenable Security Center via the user interface.

2. Click **Assets** > **Host Assets**.

   The **Host Assets** page appears.

3. (Optional) To show or hide columns on the **Host Assets** page:

a. In the table, click the ☰ button next to a column header.

A drop-down menu appears with a list of column names.

b. Check or uncheck the boxes to show or hide columns.

4. View details about each host asset.

- **Name** — The name of the host.

- **AES** — (Requires Tenable Security Center+ license) The host's Asset Exposure Score. For more information, see [Asset Exposure Score](#) in the *Tenable Vulnerability Management User Guide*.

- **ACR**— (Requires Tenable Security Center+ license) The host's Asset Criticality Rating. For more information, see [Asset Criticality Rating](#) in the *Tenable Vulnerability Management User Guide*.

- **IP Address** — The host's IP address, if available.

- **Repository** — The repository that contains vulnerability data associated with the host.

- **OS** — The operating system running on the host, if available.

- **System Type** — The host's device type, as determined by plugin 54615.

- **Net BIOS** — The host's NetBIOS name, if available.

- **DNS** — The host's DNS name, if available.

- **Last Seen** — The date and time last Tenable Security Center detected the host on your network.

- **Asset ID** — The ID of the host.

- **Source** — The type of scan that discovered the host on your network: **Tenable Nessus Scan**, **Tenable Network Monitor**, **Log Correlation Engine**, **Agent Scan**, or **Tenable OT Security Scan**.

> **Tip:** The following columns are hidden by default: **System Type**, **Net BIOS**, **DNS**, and **Asset ID**.

Export Hosts

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can export a list of hosts in a .csv file to share the data with others in your organization. For more information, see Assets.

To view details for an individual host, see View Host Details.

To view the list of hosts:

1. Log in to Tenable Security Center via the user interface.

2. Click **Assets** > **Host Assets**.

   The **Host Assets** page appears.

3. (Optional) To filter the list of hosts, apply a filter. For more information, see Host Asset Filter Components.

4. At the top of the table, click **Export**.

   Tenable Security Center exports the host assets in a CSV file.

Host Asset Filter Components

For general information about using filters, see Filters.

Filter Component	Description
Asset Criticality Rating (ACR)	(Requires Tenable Security Center+ license) Filters for hosts within the specified ACR range (for example, between 1 and 5). For more information, see Asset Criticality Rating in the *Tenable Vulnerability Management User Guide*. > **Tip:** To edit the ACR for a host asset, see Edit an ACR Manually.
Address	This filter specifies an IPv4 or IPv6 address, range, or CIDR block to limit the viewed hosts. For example, entering *198.51.100.28/24* and/or *2001:DB8::/32* limits any of the web tools to show only host data from the selected network(s). Addresses can be comma-separated or on separate

Filter Component	Description
	lines.
Asset Exposure Score (AES)	(Requires Tenable Security Center+ license) Filters for hosts within the specified AES range (for example, between 400 and 600).
DNS Name	This filter specifies a DNS name to limit the viewed hosts. For example, entering host.example.com limits any of the web tools to show only host data from that DNS name.
Name	Filters for hosts with names that include the specified text.
Operating System	Filters for hosts running the specified operating system.
Repositories	Filters for hosts with associated vulnerability data in the specified repository.
System Type	Filters for hosts with the specified device type, as determined by plugin 54615.

View Domain Inventory Assets

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can view a list of assets identified in your organization's domains. For more information, see Attack Surface Domain Discovery.

To view the list of domain inventory assets:

1. Log in to Tenable Security Center via the user interface.

2. Click **Assets** > **Domain Inventory**.

   The **Domain Inventory** page appears.

3. (Optional) To filter the list of domain inventory assets, apply a filter. For more information, see Domain Inventory Filter Components.

4. (Optional) To create a domain inventory asset list, see [Create a Domain Inventory Asset List](#).

5. (Optional) To show or hide columns on the **Domain Inventory** page:

   a. In the table, click the ☰ button next to a column header.

      A drop-down menu appears with a list of column names.

   b. Check or uncheck the boxes to show or hide columns.

6. View details about each domain inventory asset.

   - **Host** — The host associated with the asset.

   - **Record Type** - The asset type.

     > **Note:** The value in this column is determined by DNS messages associated with the asset.

   - **Record Value** - The name of the asset.

   - **IP** - The asset's IP address, if available.

   - **ASN** - The asset's Autonomous System Number.

   - **Ports** - The ports to which the asset connects.

Create a Domain Inventory Asset List

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can create an asset list from your domain inventory assets to use in active scans.

For more information about your domain inventory, see [Attack Surface Domain Discovery](#).

To create an asset list from your domain inventory assets:

1. Log in to Tenable Security Center via the user interface.

2. Click **Assets** > **Domain Inventory**.

   The **Domain Inventory** page appears.

3. (Optional) To filter the list of domain inventory assets, apply a filter. For more information, see Domain Inventory Filter Components.

4. Right-click the row for the domain inventory asset you want to include in the asset list.

   The actions menu appears.

   -or-

   Select the check box for the domain inventory asset you want to include in the asset list.

   The available actions appear at the top of the table.

5. Click **Create Asset**.

   The **Create Asset** pane appears.

6. In the **Name** box, type a name for the asset list.

7. (Optional) In the **Description** box, type a description for the asset list.

8. (Optional) In the **Tag** drop-down box, select a tag for the asset list. For more information about tags, see Tags.

9. Click **Submit**.

What to do next:

- Create an active scan using the domain inventory asset list. For more information, see Add an Active Scan.

Export Domain Inventory Assets

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can export a list of assets identified in your organization's domains. For more information, see Attack Surface Domain Discovery.

To export a list of domain inventory assets:

1. Log in to Tenable Security Center via the user interface.

2. Click **Assets** > **Domain Inventory**.

The **Domain Inventory** page appears.

3. (Optional) To the left of the table, click a domain to filter the list of assets.

4. At the top of the table, click **Export All**.

   Tenable Security Center exports the domain inventory assets in a CSV file.

Domain Inventory Filter Components

For general information about using filters, see [Filters](). For more information about domains, see [Attack Surface Domain Discovery]().

Filter Component	Description
Address	Filters by an IPv4 or IPv6 address, range, or CIDR block. You can enter IP addresses in a comma-separated list or on separate lines.
Domain	Filters by domain name. The drop-down includes a list of all available domains.
Host	Filters by the host associated with the domain inventory asset. In the drop-down, select **Exact Match**, **Should not Match**, **Contains**, or **Not Contains**. The **Exact Match** option supports single and comma-separated values.
Ports	Filters by ports associated with the domain inventory asset. In the drop-down, select = to match the specified ports, ≠ to exclude the specified ports, ≥ to match ports greater than or equal to the specified ports, or ≤ to match ports less than or equal to the specified ports. You can specify a single port, comma-separated list of ports, or range of ports (e.g., 8000-8080).
Record Type	The type of domain inventory asset. This value is determined by DNS messages associated with the asset. In the drop-down, select **Exact Match**, **Should not Match**, **Contains**, or **Not Contains**. The **Exact Match** option supports single and comma-separated values.

Credentials

Credentials are reusable objects that facilitate scan target login.

Administrators can add credentials available to all organizations. Organizational users can add credentials available to other users in the same organization. For information about user access in Tenable Security Center, see User Access.

Users can share credentials with other users, allowing them to scan remote hosts without knowing the credentials of the host. For information about Tenable Security Center credential data encryption, see Encryption Strength.

Tenable Security Center supports the following credential types:

- API Gateway Credentials

- Database Credentials

- Miscellaneous Credentials

- SNMP Credentials

- SSH Credentials

- Web Authentication Credentials

- Windows Credentials

If a scan contains multiple instances of one type of credential, Tenable Security Center tries the credentials on each scan target in the order you added the credentials to Tenable Security Center.

> **Note:** Tenable Security Center uses the first credential that allows successful login to perform credentialed checks on the target. After a credential allows a successful login, Tenable Security Center does not try any of the other credentials in the list, even if a different credential has greater privileges.

> **Note:** If a Tenable Security Center scan contains multiple instances of one type of credential, Tenable Security Center attempts to log in to a valid target using each credential in sequence, in the order in which the credential objects were originally created in Tenable Security Center. The order in which credentials were added to the scan is irrelevant. Once Tenable Security Center is able to log in successfully with a credential set, it does not attempt to log in with any of the other credentials in the scan, regardless of their relative levels of access. Each stored credential set in Tenable Security Center has an object ID number, and credentials are attempted in ascending order of object ID. To check the ID of a credential, navigate to **Scans** > **Credentials**, right-click the row for a credential, and click **View**. The ID number is displayed on

the right-hand side:

CREATED	Mar 06, 2019 13:51
LAST MODIFIED	Mar 06, 2019 13:51
OWNER	Administrator
GROUP	Administrator
ID	8

To add credentials, see Add Credentials.

Add Credentials

Required Tenable Security Center User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information about credentials, see Credentials.

Note: You can add up to 1000 SSH credentials in a single scan. For best performance, Tenable recommends adding no more than 10 SSH credentials per scan.

To add credentials:

1. Log in to Tenable Security Center.

2. In the left navigation, click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   The **Credentials** page appears.

3. Click **Add**.

   The **Credential Templates** page appears.

4. In the **Miscellaneous**, **API Gateway**, **Database**, **SNMP**, **SSH**, **Windows**, or **Web Authentication** sections, click the tile for the specific method you want to configure.

   The **Add Credentials** configuration page appears.

5. In the **Name** box, type a name for the credentials.

6. In the **Description** box, type a description for the credentials.

7. (Optional) Type or select a **Tag**. For more information, see Tags.

8. Configure the options, as described in:

   - Miscellaneous Credentials

   - API Gateway Credentials

   - Database Credentials

   - SNMP Credentials

   - SSH Credentials

   - Windows Credentials

   - Web Authentication Credentials

9. Click **Submit**.

   Tenable Security Center saves your configuration.

API Gateway Credentials

Configure the following options for all API gateway credentials.

Option	Description
Name	(Required) A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see Tags.

IBM DataPower Options

The following table describes the additional options to configure for **IBM DataPower** credentials.

Option	Description
Client Certificate	The file that contains the PEM certificate used to communicate with the IBM DataPower host.
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
Custom Header Key	If your IBM DataPower configuration uses custom HTTP headers, the custom HTTP header key.
Custom Header Value	If your IBM DataPower configuration uses custom HTTP headers, the custom HTTP header value.
Enable for Hashicorp Vault	When enabled, allows Tenable Security Center to use the IBM DataPower credential with a Hashicorp Vault credential. **Tip:** If you want to run a test that does not use IBM DataPower credentials without having to delete the credential, you can temporarily disable this option to prevent Tenable Security Center from using IBM DataPower credentials.

Database Credentials

The following topic describes the available **Database** credentials.

> **Note:** Aspects of credential options are based on Nessus plugin options. Therefore, specific credential options may differ from the descriptions documented here.

Configure the following options for all database credentials:

Options	Description
Name (Required)	A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see Tags.

Apache Cassandra

Option	Description
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault • Wallix Bastion For descriptions of the options for your selected authentication type, see Database Credentials Authentication.
Database Port	The port the database listens on. The default is port 9042.

Delinea Secret Server Auto-Discovery

Option	Description	Required
Delinea Host	The Delinea Secret Server host to pull the secrets from.	Yes

Option	Description	Required
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	Yes
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, **Credentials** is selected.	Yes
Delinea Login Name	The username to authenticate to the Delinea server.	Yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the provided Delinea Login Name.	Yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the API Key authentication method is selected.	Yes
Query Mode	Choose to query accounts using pre-set fields or by constructing a string of URL query parameters. By default, **Simple** is selected.	Yes
Folder ID	Query accounts with the given folder ID. This option is only available if query mode is set to **Simple**.	No
Search Text	Query accounts matching the given search text. This option is only available if query mode is set to **Simple**.	No
Search Field	The field to search using the given search text. If not specified, the query will search the name field. This option is only available if query mode is set to **Simple**.	No
Exact Match	Perform an exact match against the search text. By default, this is unselected. This option is only available if query mode is set to **Simple**.	No
Query String	Provide a string of URL query parameters. This option is only available if query mode is set to **Advanced**, and in that case it is required.	Yes

Option	Description	Required
Use Private Key	Use key-based authentication for SSH connections instead of password authentication.	No
Use SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Verify the Delinea Secret Server SSL certificate.	No

IBM DB2

The following table describes the additional options to configure for **IBM DB2** credentials.

Options	Description
Source	The method for providing the required credential details: **Entry** or **Import**. • **Entry** — Specifies you want to use a single SID value or SERVICE_NAME value for the credential. You must also configure the remaining options on the **Add Credential** page, as described in Add Credentials. • **Import** — Specifies you want to use multiple SID values for the credential, uploaded as a `.csv` file. For more information about the required `.csv` file format, see Database Credentials Authentication.
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault • Wallix Bastion

Options	Description
	For descriptions of the options for your selected authentication type, see Database Credentials Authentication.
Port	The TCP port that the IBM DB2 database instance listens on for communications from Tenable Security Center. The default is port 50000.
Database Name	The name for your database (not the name of your instance).

Informix/DRDA

The following table describes the additional options to configure for **Informix/DRDA** credentials.

Options	Description
Username	The username for a user on the database.
Password	The password associated with the username you provided.
Port	The TCP port that the Informix/DRDA database instance listens on for communications from Tenable Security Center. The default is port 1526.

MongoDB

Option	Description
Username	The username for the database.
Password	The password for the supplied username.
Database	The name of the database to authenticate to. **Tip:** To authenticate via LDAP or saslauthd, type **$external**.
Port	(Required) The TCP port that the MongoDB database instance listens on for communications from Tenable Security Center.

MySQL

The following table describes the additional options to configure for **MySQL** credentials.

Options	Description
Source	The method for providing the required credential details: **Entry** or **Import**. • **Entry** — Specifies you want to use a single SID value or SERVICE_NAME value for the credential. You must also configure the remaining options on the **Add Credential** page, as described in [Add Credentials](#). • **Import** — Specifies you want to use multiple SID values for the credential, uploaded as a `.csv` file. For more information about the required `.csv` file format, see [Database Credentials Authentication](#).
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault • Wallix Bastion For descriptions of the options for your selected authentication type, see [Database Credentials Authentication](#).
Username	The username for a user on the database.
Password	The password associated with the username you provided.
Port	The TCP port that the MySQL database instance listens on for communications from Tenable Security Center. The default is port 3306.
SID	The name for your database instance.

Oracle Database

The following table describes the additional options to configure for **Oracle Database** credentials.

Options	Description
Source	The method for providing the required credential details: **Entry** or **Import**. • **Entry** — Specifies you want to use a single SID value or SERVICE_NAME value for the credential. You must also configure the remaining options on the **Add Credential** page, as described in Add Credentials. • **Import** — Specifies you want to use multiple SID values for the credential, uploaded as a `.csv` file. For more information about the required `.csv` file format, see Database Credentials Authentication.
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault • Wallix Bastion For descriptions of the options for your selected authentication type, see Database Credentials Authentication.
Port	The TCP port that the Oracle database instance listens on for communications from Tenable Security Center. The default is port 1521.
Authentication	The type of account you want Tenable Security Center to use to access the database instance: • **Normal** • **System Operator**

Options	Description
	• **System Database Administrator**
Service Type	The Oracle parameter you want to use to specify the database instance: **SID** or **Service Name**.
Service	The SID value or SERVICE_NAME value for your database instance. The **Service** value you enter must match your parameter selection for the **Service Type** option.

PostgreSQL

The following table describes the additional options to configure for **PostgreSQL** credentials.

Options	Description
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault For descriptions of the options for your selected authentication type, see Database Credentials Authentication.
Port	The TCP port that the PostgreSQL database instance listens on for communications from Tenable Security Center. The default is port 5432.
Database Name	The name for your database instance.

SQL Server

The following table describes the additional options to configure for **SQL Server** credentials.

Options	Description
Source	The method for providing the required credential details: **Entry** or **Import**. • **Entry** — Specifies you want to use a single SID value or SERVICE_NAME value for the credential. You must also configure the remaining options on the **Add Credential** page, as described in Add Credentials. • **Import** — Specifies you want to use multiple SID values for the credential, uploaded as a `.csv` file. For more information about the required `.csv` file format, see Database Credentials Authentication.
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault • Wallix Bastion For descriptions of the options for your selected authentication type, see Database Credentials Authentication.
Username	The username for a user on the database.
Password	The password associated with the username you provided.
Port	The TCP port that the SQL Server database instance listens on for communications from Tenable Security Center. The default is port 1433.
Authentication	The type of account you want Tenable Security Center to use to access the database instance: **SQL** or **Windows**.
Instance Name	The name for your database instance.

Sybase ASE

The following table describes the additional options to configure for **Sybase ASE** credentials.

Options	Description
Authentication Method	The authentication method for providing the required credentials. • CyberArk • Password • Lieberman • Hashicorp Vault • Wallix Bastion For descriptions of the options for your selected authentication type, see Database Credentials Authentication.
Port	The TCP port that the Sybase ASE database instance listens on for communications from Tenable Security Center. The default is port 3638.
Sybase ASE Auth Type	The type of authentication used by the Sybase ASE database: **RSA** or **Plain Text**.

Database Credentials Authentication Method Settings

Depending on the authentication type you select for your database credentials, you must configure the following options. For more information about database credential settings, see Database Credentials.

- Import Credentials

- Arcon Options

- CyberArk Options

- CyberArk (Legacy) Options

- CyberArk Database Auto-Discovery Options

- [Hashicorp Vault Options](#)

- [Lieberman Options](#)

- [Password Options](#)

- [WALLIX Bastion Options](#)

Import

Upload a `.csv` file with the credentials entered in the specified format. For descriptions of valid values to use for each item, see [Database Credentials](#).

You must configure either CyberArk or Hashicorp credentials for a database credential in the same scan so that Tenable Security Center can retrieve the credentials.

Database Credential	CSV Format
IBM DB2	`target, port, database_name, username, cred_manager, accountname_or_secretname`
MySQL	`target, port, database_name, username, cred_manager, accountname_or_secretname`
Oracle	`target, port, service_type, service_ID, username, auth_type, cred_manager, accountname_or_secretname`
SQL Server	`target, port, instance_name, username, auth_type, cred_manager, accountname_or_secretname`

Note: Include the required data in the specified order, with commas between each value, without spaces. For example, for Oracle with CyberArk: `192.0.2.255,1521,SID,service_id,username,SYSDBA,CyberArk,Database-Oracle-SYS`.

Note: The value for `cred_manager` must be either *CyberArk* or *Hashicorp*.

Arcon Options

The following table describes the additional options to configure when using Arcon as the **Authentication Method** for **IBM DB2**, **SQL Server**, **MySQL**, **Oracle Database**, **PostgreSQL**, or **Sybase**

ASE database credentials.

Option	Description
Arcon Host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon Port	(Required) The port on which Arcon listens. By default, Tenable Security Center uses port 444.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	(Required) The URL Tenable Security Center uses to access Arcon.
Password Engine URL	(Required) The URL Tenable Security Center uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Security Center scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Tip:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Security Center scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.

CyberArk Options

The following table describes the additional options to configure when using CyberArk as the **Authentication Method** for **Apache Cassandra**, **IBM DB2**, **MySQL**, **Oracle Database**, **PostgreSQL**, **SQL Server**, or **Sybase ASE** database credentials.

> **Note:** You must be running Tenable Nessus 7.0.0 or later to configure CyberArk credentials.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the CyberArk AIM Web Service. This can be the host, or the host with a custom URL added on in a single string.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk API connection.	yes
Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied
Get credential	The method with which your CyberArk API credentials are	yes

Option	Description	Required
by	retrieved. Can be **Username**, **Identifier**, or **Address**. **Note:** The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier.	
Username	(If **Get credential by** is **Username**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.	no
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no

CyberArk (Legacy) Options

The following table describes the additional options to configure when using CyberArk (Legacy) as the **Authentication Method** for **Apache Cassandra**, **IBM DB2**, **MySQL**, **Oracle Database**, **PostgreSQL**, **SQL Server**, or **Sybase ASE** database credentials.

Note: You must be running Tenable Nessus 7.0.0 or later to configure CyberArk credentials.

Option	Database Types	Description	Required
Username	All	The target system's username.	yes
Central	All	The CyberArk Central Credential Provider	yes

Option	Database Types	Description	Required
Credential Provider Host		IP/DNS address.	
Central Credential Provider Port	All	The port on which the CyberArk Central Credential Provider is listening.	yes
CyberArk AIM Service URL	All	The URL of the AIM service. By default, this field uses `/AIMWebservice/v1.1/AIM.asmx`.	no
Central Credential Provider Username	All	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.	no
Central Credential Provider Password	All	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.	no
CyberArk Safe	All	The safe on the CyberArk Central Credential Provider server that contained the authentication information you would like to retrieve.	no
CyberArk Client Certificate	All	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
CyberArk Client Certificate Private Key	All	The file that contains the PEM private key for the client certificate.	no

Option	Database Types	Description	Required
CyberArk Client Certificate Private Key Passphrase	All	The passphrase for the private key, if your authentication implementation requires it.	no
CyberArk AppId	All	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.	yes
CyberArk Folder	All	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.	no
CyberArk Account Details Name	All	The unique name of the credential you want to retrieve from CyberArk.	yes
PolicyId	All	The PolicyID assigned to the credentials that you want to retrieve from the CyberArk Central Credential Provider.	no
Use SSL	All	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.	no
Verify SSL Certificate	All	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate, select this option. Refer to the custom_CA.inc documentation for how to use self-signed certificates.	no

Option	Database Types	Description	Required
Database Port	All	The port on which Tenable Security Center communicates with the database.	yes
Database Name	DB2 PostgreSQL	The name of the database.	no
Auth type	Oracle SQL Server Sybase ASE	SQL Server values include: • Windows • SQL Oracle values include: • **Normal** • **System Operator** • **System Database Administrator** Sybase ASE values include: • RSA • Plain Text	yes
Instance Name	SQL Server	The name for your database instance.	no
Service type	Oracle	Valid values include: • SID • SERVICE_NAME	yes
Service	Oracle	The SID value for your database instance or a SERVICE_NAME value. The **Service** value you enter must match your parameter selection for the **Service Type** option.	no

CyberArk Database Auto-Discovery Options

The following table describes the additional options to configure when using CyberArk Database Auto-Discovery as the **Authentication Method** for **Apache Cassandra**, **IBM DB2**, **MySQL**, **Oracle Database**, **PostgreSQL**, **SQL Server**, or **Sybase ASE** database credentials.

> **Note:** You must be running Tenable Nessus 7.0.0 or later to configure CyberArk credentials.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the user's CyberArk Instance.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk API connection.	yes
Safe	Users may optionally specify a Safe to gather account information and request passwords.	no
AIM WebService Authentication Type	There are two authentication methods established in the feature. IIS Basic Authentication and Certificate Authentication. Certificate Authentication can be either encrypted or unencrypted.	yes
Client Certificate	The file that contains the PEM-formatted certificate used to communicate with the host.	no
Client Certificate Private Key	The file that contains the PEM-formatted private key for the client certificate.	no
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	no
CyberArk PVWA Web UI Login	Username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather	yes

Option	Description	Required
Name	bulk account information.	
CyberArk PVWA Web UI Login Password	Password for the username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk Platform Search String	String used in the PVWA REST API query parameters to gather bulk account information. For example, the user can enter `Oracle Admin TestSafe`, to gather all Oracle platform accounts containing a username `Admin` in a Safe called `TestSafe`. **Note:** This is a non-exact keyword search. A best practice would be to create a custom platform name in CyberArk and enter that value in this field to improve accuracy.	yes
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.	yes
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no

Password Options

The following table describes the additional options to configure when using Password as the **Authentication Method** for **Apache Cassandra**, **IBM DB2**, **SQL Server**, **MySQL**, **Oracle Database**, **PostgreSQL**, or **Sybase ASE** database credentials.

Option	Database Types	Description
Username	All	The username for a user on the database.
Password	All	The password associated with the username you

Option	Database Types	Description
		provided.
Port	All	The port the database is listening on.
Database Name	IBM D2 PostgreSQL	The name for your database instance.
Authentication	Oracle Database SQL Server	The type of account you want Tenable Security Center to use to access the database instance.
Service Type	Oracle Database	The Oracle parameter you want to use to identify the database instance: **SID** or **Service Name**.
Service	Oracle Database	The SID value for your database instance or a SERVICE_NAME value. The **Service** value you enter must match your parameter selection for the **Service Type** option.
Instance Name	SQL Server	The name for your database instance.

Hashicorp Vault Options

The following table describes the additional options to configure when using Hashicorp Vault as the **Authentication Method** for **Apache Cassandra**, **IBM DB2**, **SQL Server**, **MySQL**, **Oracle Database**, **PostgreSQL**, or **Sybase ASE** database credentials.

Option	Credential	Description	Required
Port	Oracle Database IBM DB2 MySQL	The port on which Tenable Security Center communicates with the database.	yes

	PostgreSQL SQL Server		
SID	MySQL	The security identifier used to connect to the database.	yes
Database Name	IBM DB2 PostgreSQL	The name of the database.	no
Instance Name	SQL Server	The SQL server name.	yes
Hashicorp Host	All	The Hashicorp Vault IP address or DNS address. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.	yes
Hashicorp Port	All	The port on which Hashicorp Vault listens.	yes
Service Type	Oracle Database	The unique **SID** or **Service Name** that identifies your database.	yes
Service	Oracle Database	The **SID** or **Service Name** value for your database instance. **Note:** The **Service** value must match the **Service Type** option parameter selection.	yes
Authentication Type	All	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**.	yes
Client Cert	All	If **Authentication Type** is	yes

		Certificates, the client certificate file you want to use to authenticate the connection.	
Private Key	All	If **Authentication Type** is **Certificates**, the private key file associated with the client certificate you want to use to authenticate the connection.	yes
Role ID	All	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	All	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	All	The path/subdirectory to the authentication endpoint. This is not the full URL. For example: `/v1/auth/approle/login`	yes
Namespace	All	The name of a specified team in a multi-team environment.	no
Hashicorp Vault Type	All	The type of Hashicorp Vault secrets engine: • **KV1** — Key/Value Secrets Engine Version 1 • **KV2** — Key/Value Secrets Engine Version 2 • **AD** — Active Directory • **LDAP** - LDAP secrets engine	yes

KV1 Engine URL **KV2 Engine URL** **AD Engine URL** **LDAP Engine URL**	All	The engine URL combines with the secret name to form the API request URL. For example, a secret name of `creds` and a KV v1 engine url of `/v1/secret` would result in a GET request to `/v1/secret/creds` (for KV v2, `/v1/secret/data/creds`).	yes
Username Source	All	(Appears when **Hashicorp Vault Type** is **KV1** or **KV2**) Specifies if the username is input manually or pulled from Hashicorp Vault.	yes
Username key	All	(Appears when **Hashicorp Vault Type** is **KV1** or **KV2**) The name in Hashicorp Vault that usernames are stored under.	no
Username	All	(Appears when **Username Source** is **Manual Entry**) The name in Hashicorp Vault that usernames are stored under.	yes
Password key	All	(Appears when **Hashicorp Vault Type** is **KV1** or **KV2**) The key in Hashicorp Vault that passwords are stored under.	no
Secret Name	All	The key secret you want to retrieve values for.	yes
Use SSL	All	When enabled, Tenable Security Center uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no

| Verify SSL | All | When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option. | no |

Lieberman Options

The following table describes the additional options to configure when using Lieberman as the **Authentication Method** for **Apache Cassandra**, **IBM DB2**, **SQL Server**, **MySQL**, **Oracle Database**, **PostgreSQL**, or **Sybase ASE** database credentials.

> **Note:** You must meet the version requirements specified in [Tenable Integrated Product Compatibility](#).

Option	Database Types	Description
Username	All	The username for a user on the database.
Port	All	The port the database is listening on.
Database Name	IBM DB2 PostgreSQL	The name for your database instance.
Authentication	Oracle Database SQL Server	The type of account you want Tenable Security Center to use to access the database instance.
Service Type	Oracle Database	The Oracle parameter you want to use to identify the database instance: **SID** or **Service Name**.
Service	Oracle Database	The SID value for your database instance or a SERVICE_NAME value. The **Service** value you enter must match your parameter selection for the **Service Type** option.
Instance Name	SQL Server	The name for your database instance.

Option	Database Types	Description
Lieberman Host	All	The Lieberman IP address or DNS address.
Lieberman Port	All	The port Lieberman is listening on.
Lieberman User	All	The username for the Lieberman explicit user you want Tenable Security Center to use for authentication to the Lieberman Rapid Enterprise Defense (RED) API.
Lieberman Password	All	The password for the Lieberman explicit user.
Use SSL	All	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Lieberman before enabling this option.
Verify SSL Certificate	All	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Lieberman before enabling this option.
System Name	All	The name for the database credentials in Lieberman.

WALLIX Bastion Options

The following table describes the additional options to configure when using WALLIX Bastion as the **Authentication Method** for **Apache Cassandra**, **IBM DB2**, **MySQL**, **Oracle Database**, **SQL Server**, or **Sybase ASE** database credentials.

Option	Description	Required
Port	The port the database is listening on.	no
WALLIX Host	The IP address for the WALLIX Bastion host.	yes
WALLIX Port	The port on which the WALLIX Bastion API communicates. By default, Tenable uses 443.	yes

Option	Description	Required
Authentication Type	**Basic** authentication (with WALLIX Bastion user interface username and Password requirements) or **API Key** authentication (with username and WALLIX Bastion-generated API key requirements).	no
WALLIX User	Your WALLIX Bastion user interface login username.	yes
WALLIX Password	Your WALLIX Bastion user interface login password. Used for **Basic** authentication to the API.	yes
WALLIX API Key	The API key generated in the WALLIX Bastion user interface. Used for **API Key** authentication to the API.	yes
Get Credential by Device Account Name	The account name associated with a **Device** you want to log in to the target systems with. **Note:** If your device has more than one account you must enter the specific device name for the account you want to retrieve credentials for. Failure to do this may result in credentials for the wrong account returned by the system.	Required only if you have a target and/or device with multiple accounts.
HTTPS	This is enabled by default. **Caution:** The integration fails if you disable **HTTPS**.	yes
Verify SSL Certificate	This is disabled by default and is not supported in WALLIX Bastion PAM integrations.	no

Miscellaneous Credentials

Configure the following options for all miscellaneous credentials, including options specific for your authentication method:

- [The following table describes the additional options to configure for Citrix credentials.](#)

- [The following table describes the additional options to configure for Nutanix Prism Central credentials.](#)

- [The following table describes the additional options to configure for OpenShift Container Platform credentials.](#)

- [The following table describes the additional options to configure for VMware vCenter API credentials.](#)

Option	Description
Name (Required)	A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see [Tags](#).

Citrix Options

The following table describes the additional options to configure for **Citrix** credentials.

Option	Description	Default
Port	(Required) The TCP port that Citrix listens on for communications from Tenable Security Center.	443
Username	(Required) The username for the scanning Citrix account that Tenable Security Center uses to perform checks on the target system.	--
Password	(Required) The password for the Citrix user.	--
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA.	enabled

Option	Description	Default
	Tip: If you are using a self-signed certificate, disable this setting.	

Nutanix Prism Central Options

The following table describes the additional options to configure for **Nutanix Prism Central** credentials.

Option	Description	Default
Nutanix Host	(Required) The hostname or IP address for the Nutanix Prism Central host.	--
Nutanix Port	(Required) The port for the Nutanix Prism Central host.	9440
Username	(Required) The username for the Nutanix Prism Central account.	--
Password	(Required) The password for the Nutanix Prism Central user.	--
Discover Hosts	When enabled, Tenable Security Center adds all discovered Nutanix hosts to the list of scan targets.	enabled
Discover Virtual Machines	When enabled. Tenable Security Center adds all discovered Nutanix Virtual Machines to the list of scan targets.	enabled
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	disabled

OpenShift Container Platform Options

The following table describes the additional options to configure for **OpenShift Container Platform** credentials.

Option	Description	Default
Token	(Required) The authentication token for the Service Account in OpenShift.	--
Port	(Required) The port for the OpenShift Container Platform host.	6443
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	enabled

VMware vCenter API Options

The following table describes the additional options to configure for **VMware vCenter API** credentials.

Note: The SOAP API requires a vCenter account with read permissions and settings privileges. The REST API requires a vCenter admin account with general read permissions and required Lifecycle Manager privileges to enumerate VIBs.

Option	Description	Default
vCenter Host	(Required) The hostname or IP address for the VMware vCenter API host.	--
vCenter Port	(Required) The port for the VMware vCenter API host.	443

Option	Description	Default
Username	(Required) The username for the VMware vCenter API account.	--
Password	(Required) The password for the VMware vCenter API user.	--
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	disabled
Auto Discover Managed VMware ESXi Hosts	When enabled, Tenable Security Center adds all discovered managed VMware ESXi hosts to the list of scan targets.	disabled
Auto Discover Managed VMware ESXi Virtual Machines	When enabled, Tenable Security Center adds all discovered managed VMware ESXi virtual machines to the list of scan targets.	disabled

SNMP Credentials

Configure the following options for SNMP credentials. Tenable Security Center supports SNMPv1 for authentication via a community string.

Options	Description
Name	(Required) A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see Tags.

Options	Description
Community	The SNMP community string used for authentication.

SSH Credentials

Use SSH credentials for host-based checks on Unix systems and supported network devices. Tenable Security Center uses these credentials to obtain local information from remote Unix systems for patch auditing or compliance checks. Tenable Security Center uses Secure Shell (SSH) protocol version 2 based programs (e.g., OpenSSH, Solaris SSH, etc.) for host-based checks.

Tenable Security Center encrypts the data using the AES-256-CBC algorithm to protect it from being viewed by sniffer programs.

> **Note:** Non-privileged users with local access on Linux systems can determine basic security issues, such as patch levels or entries in the /etc/passwd file. For more comprehensive information, such as system configuration data or file permissions across the entire system, an account with root privileges is required.

> **Note:** You can add up to 1000 SSH credentials in a single scan. For best performance, Tenable recommends adding no more than 10 SSH credentials per scan.

Configure the following options for SSH credentials, including options specific for your authentication method:

- Arcon Options

- BeyondTrust Options

- Centrify Options

- Certificate Options

- CyberArk Windows Auto-Discovery Options

- CyberArk Vault Options

- CyberArk Vault (Legacy) Options

- Delinea Secret Server Options

- Hashicorp Vault Options

- Kerberos Options

- [Lieberman Options](#)

- [Password Options](#)

- [Public Key Options](#)

- [QiAnXin Options](#)

- [Senhasegura Options](#)

- [Thycotic Secret Server Options](#)

- [WALLIX Bastion Options](#)

General Option	Description
Name	(Required) A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see [Tags](#).

Arcon Options

The following table describes the additional options to configure when using **Arcon** as the authentication method for SSH credentials.

Option	Description
Arcon Host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon Port	(Required) The port on which Arcon listens. By default, Tenable Security Center uses port 444.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication	(Required) The URL Tenable Security Center uses to access Arcon.

URL	
Password Engine URL	(Required) The URL Tenable Security Center uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Arcon Target Type	(Optional) The name of the target type. Depending on the Arcon PAM version you are using and the system type the SSH credential has been created with, this is set to **linux** by default. Refer to the Arcon PAM Specifications document (provided by Arcon) for target type/system type mapping for the correct target type value.
Checkout Duration	(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Security Center scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Tip:** Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Security Center scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **Privilege Escalation** selection determines the specific options you must configure. For more information, see Privilege Escalation.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list.

Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

BeyondTrust Options

The following table describes the additional options to configure when using **BeyondTrust** as the authentication method for SSH credentials.

Option	Description
Username	The username to log in to the hosts you want to scan.
BeyondTrust Host	The BeyondTrust IP address or DNS address.
BeyondTrust Port	The port BeyondTrust is listening on.
BeyondTrust API User	The API user provided by BeyondTrust.
BeyondTrust API Key	The API key provided by BeyondTrust.
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in BeyondTrust. Configure the **Checkout duration** to exceed the typical duration of your Tenable Security Center scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Tip:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable Security Center scans. If BeyondTrust changes a password during a scan, the scan fails.
Use SSL	If enabled, Tenable Security Center uses SSL through IIS for secure

Option	Description
	communications. You must configure SSL through IIS in BeyondTrust before enabling this option.
Verify SSL Certificate	If enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.
Use Private Key	If enabled, Tenable Security Center uses key-based authentication for SSH connections instead of password authentication.
Use Privilege Escalations	If enabled, Tenable Security Center uses BeyondTrust for privilege escalation.

Centrify Options

The following table describes the additional options to configure when using **Centrify** as the authentication method for SSH credentials.

Option	Description
Centrify Host	(Required) The Centrify IP address or DNS address. **Note:** If your Centrify installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Centrify Port	(Required) The port on which Centrify listens. By default, Tenable Security Center uses port 443.
API User	(Required) The API user provided by Centrify.
API Key	(Required) The API key provided by Centrify.
Tenant	(Required) The Centrify tenant associated with the API. By default, Tenable Security Center uses *centrify*.
Authentication URL	(Required) The URL Tenable Security Center uses to access Centrify. By default, Tenable Security Center uses */Security*.

Password Query URL	(Required) The URL Tenable Security Center uses to query the passwords in Centrify. By default, Tenable Security Center uses */RedRock*.
Password Engine URL	(Required) The URL Tenable Security Center uses to access the passwords in Centrify. By default, Tenable Security Center uses */ServerManage*.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	(Required) The length of time, in minutes, that you want to keep credentials checked out in Centrify. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Security Center scans so that password changes do not disrupt your Tenable Security Center scans. If Centrify changes a password during a scan, the scan fails. If a password from a previous scan is still checked out when a new scan begins, the new scan fails.
Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.

Certificate Options

The following table describes the additional options to configure when using **Certificate** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for a user on the host system.
User Certificate	(Required) The RSA, DSA, ECDSA, or ED25519 OpenSSH certificate file for the user.

Option	Description
Private Key	(Required) The RSA, DSA, ECDSA, or ED25519 OpenSSH private key file for the user.
Passphrase	The passphrase for the private key, if required.
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **Privilege Escalation** selection determines the specific options you must configure. For more information, see [Privilege Escalation]().

CyberArk SSH Auto-Discovery Options

The following table describes the additional options to configure when using **CyberArk SSH Auto-Discovery** as the authentication method for SSH credentials.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the user's CyberArk Instance.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk API connection.	yes
Safe	Users may optionally specify a Safe to gather account information and request passwords.	no
AIM Web Service Authentication Type	There are two authentication methods established in the feature. **IIS Basic Authentication** and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	yes
Username	(Appears if **AIM Web Service Authentication Type** is **IIS Basic Authentication**) The username for a user on the CyberArk server.	no

Option	Description	Required
Password	(Appears if **AIM Web Service Authentication Type** is **IIS Basic Authentication**) The password associated with the username you provided.	no
Client Certificate	(Appears if **AIM Web Service Authentication Type** is **Certificate Authentication**) The file that contains the PEM certificate used to communicate with the CyberArk host.	no
Client Certificate Private Key	(Appears if **AIM Web Service Authentication Type** is **Certificate Authentication**) The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	(Appears if **AIM Web Service Authentication Type** is **Certificate Authentication**) The passphrase for the private key, if required.	yes, if private key is applied
CyberArk PVWA Web UI Login Name	Username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk PVWA Web UI Login Password	Password for the username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk Platform Search String	String used in the PVWA REST API query parameters to gather bulk account information. For example, the user can enter `UnixSSH Admin TestSafe`, to gather all UnixSSH platform accounts containing a username `Admin` in a Safe called `TestSafe`. **Note:** This is a non-exact keyword search. A best practice would be to create a custom platform name in CyberArk and enter that value in this field to improve accuracy.	yes
Use SSL	If enabled, the scanner uses SSL through IIS for secure	yes

Option	Description	Required
	communications. Enable this option if CyberArk is configured to support SSL through IIS.	
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	no
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **Privilege Escalation** selection determines the specific options you must configure. For more information, see Privilege Escalation.	no

CyberArk Vault Options

The following table describes the additional options to configure when using **CyberArk Vault** as the authentication method for SSH credentials.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the CyberArk AIM Web	yes

Option	Description	Required
	Service.	
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk API connection.	yes
Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	(Required if Kerberos Target Authentication is enabled.) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	yes
KDC Transport	(Required if Kerberos Target Authentication is enabled.) The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the	yes

Option	Description	Required
	KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target (for example, example.com). By default, Tenable Security Center uses 443.	yes
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Username**, **Identifier**, or **Address**. **Note:** The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier.	yes
Username	(If **Get credential by** is **Username**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Address	The option should only be used if the Address value is unique to a single CyberArk account credential.	no
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.	no
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support	no

Option	Description	Required
	SSL through IIS and you want to validate the certificate.	

CyberArk Vault (Legacy) Options

The following table describes the additional options to configure when using **CyberArk Vault (Legacy)** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for the target system.
CyberArk elevate privileges with	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **CyberArk elevate privileges with** selection determines the specific options you must configure. For more information, see Privilege Escalation.
Central Credential Provider URL Host	(Required) The CyberArk Central Credential Provider IP/DNS address.
Central Credential Provider URL Port	(Required) The port the CyberArk Central Credential Provider is listening on.
CyberArk Address	The domain for the CyberArk account. You must configure SSL through IIS in CyberArk Central Credential Provider before configuring this option.
Vault Username	The username for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Vault Password	The password for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Safe	(Required) The safe on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.

Option	Description
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
AppID	(Required) The AppID with CyberArk Central Credential Provider permissions to retrieve the target password.
Folder	(Required) The folder on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.
PolicyID	The PolicyID assigned to the credentials you want to retrieve.
Vault Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option.
Vault Verify SSL	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option.
CyberArk Escalation Account Details Name	The unique name of the credential you want to retrieve from CyberArk.
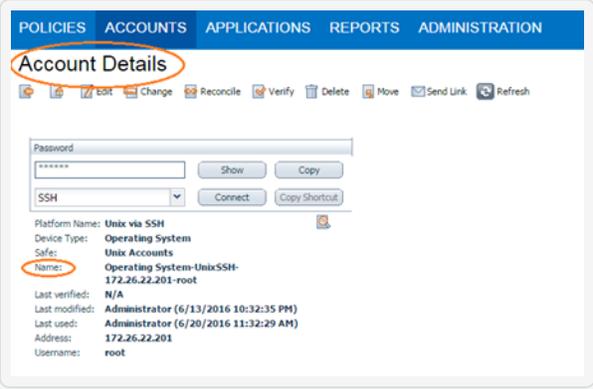
Option	Description
CyberArk AIM Service URL	The URL for the CyberArk AIM web service. By default, Tenable Security Center uses */AIMWebservice/v1.1/AIM.asmx*.

Delinea Secret Server Options

The following table describes the additional options to configure when using **Delinea Secret Server** as the authentication method for SSH credentials.

Option	Description	Required
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled **Secret Name** on the Delinea server.	yes
Delinea Host	The Delinea Secret Server host to pull the secrets from.	yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Use Private Key	If enabled, uses key-based authentication for SSH connections instead of password authentication.	no

Checkout Duration	The duration Tenable should check out the password from Delinea. Duration time is in hours and should be longer than the scan time.	yes
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target.	yes
Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no
Verify SSL Certificate	If enabled, verifies the SSL Certificate on the Delinea server.	no
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Multiple options for privilege escalation are supported, including su, su+sudo and sudo. Your selection determines the specific options you must configure.	no
Custom password prompt	Some devices are configured to prompt for a password with a non-standard string (for example, "secret-passcode"). This setting allows recognition of these	no

prompts. Leave this blank for most standard password prompts.	

Hashicorp Vault Options

The following table describes the additional options to configure when using **Hashicorp Vault** as the authentication method for SSH credentials.

Option	Default Value	Required
Hashicorp Host	The Hashicorp Vault IP address or DNS address. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.	yes
Hashicorp Port	The port on which Hashicorp Vault listens.	yes
Authentication Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate** (Required) and **Hashicorp Client Certificate Private Key** (Required) appear. Select the appropriate files for the client certificate and private key.	yes
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication URL	The path/subdirectory to the authentication endpoint. This is not the full URL. For example: /v1/auth/approle/login	yes
Namespace	The name of a specified team in a multi-team	no

	environment.	
Hashicorp Vault Type	The type of Hashicorp Vault secrets engine: • **KV1** — Key/Value Secrets Engine Version 1 • **KV2** — Key/Value Secrets Engine Version 2 • **AD** — Active Directory • **LDAP** - LDAP secrets engine	yes
KV1 Engine URL **KV2 Engine URL** **AD Engine URL** **LDAP Engine URL**	The engine URL combines with the secret name to form the API request URL. For example, a secret name of `creds` and a KV v1 engine url of `/v1/secret` would result in a GET request to `/v1/secret/creds` (for KV v2, `/v1/secret/data/creds`).	yes
Username Source	(Appears when **Hashicorp Vault Type** is **KV1** or **KV2**) Specifies if the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(Appears when **Hashicorp Vault Type** is **KV1** or **KV2**) The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	(Appears when **Hashicorp Vault Type** is **KV1** or **KV2**) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	The key secret you want to retrieve values for.	yes
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	(Required if Kerberos Target Authentication is enabled) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	yes

KDC Transport	(Required if Kerberos Target Authentication is enabled) The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	yes
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target (for example, example.com). By default, Tenable Security Center uses 443.	yes
Use SSL	When enabled, Tenable Security Center uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	no
Privilege	The privilege escalation method you want to use to	no

Escalation	increase users' privileges after initial authentication. Your **Privilege Escalation** selection determines the specific options you must configure. For more information, see Privilege Escalation.

Kerberos Options

The following table describes the additional options to configure when using **Kerberos** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for a user on the target system.
Password	(Required) The password associated with the username you provided.
KDC Host	(Required) The host supplying the session tickets.
KDC Port	(Required) The port you want to use for the KDC connection. By default, Tenable Security Center uses port 88.
KDC Transport	(Required) The method you want to use to connect to the KDC server. **Note:** If you select UDP, you may need to edit the KDC Port. The KDC UDP protocol uses either port 88 or port 750.
Realm	(Required) The authentication domain, typically the domain name of the target (e.g., *example.com*).
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **Privilege Escalation** selection determines the specific options you must configure. For more information, see Privilege Escalation.

Lieberman Options

The following table describes the additional options to configure when using **Lieberman** as the authentication method for SSH credentials.

Option	Description
Username	The username for a user on the database.
Lieberman Host	The Lieberman IP address or DNS address. **Note:** If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Lieberman Port	The port Lieberman is listening on.
Lieberman User	The username for the Lieberman explicit user you want Tenable Security Center to use for authentication to the Lieberman Rapid Enterprise Defense (RED) API.
Lieberman Password	The password for the Lieberman explicit user.
Use SSL	When enabled, Tenable Security Centeruses SSL through IIS for secure communications. You must configure SSL through IIS in Lieberman before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Lieberman before enabling this option.
System Name	The name for the database credentials in Lieberman.

Password Options

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`.

The following table describes the additional options to configure when using **Password** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for a user on the target system.
Password (Unsafe!)	(Required) The password associated with the username you provided.
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **Privilege Escalation** selection determines the specific options you must configure. For more information, see Privilege Escalation.

Public Key Options

The following table describes the additional options to configure when using **Public Key** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for a user on the host system.
Private Key	(Required) The RSA, DSA, ECDSA, or ED25519 OpenSSH key file for the user.
Passphrase	The passphrase for the private key, if required.
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **Privilege Escalation** selection determines the specific options you must configure. For more information, see Privilege Escalation.

QiAnXin Options

The following table describes the additional options to configure when using **QiAnXin** as the authentication method for SSH credentials.

Option	Description	Required
QiAnXin Host	The IP address or url for the QiAnXin host.	yes
QiAnXin Port	The port on which the QiAnXin API communicates.	yes

Option	Description	Required
	By default, Tenable uses 443.	
QiAnXin API Client ID	The Client ID for the embedded account application created in QiAnXin PAM.	yes
QiAnXin API Client Secret	The Secret ID for the embedded account application created in QiAnXin PAM.	yes
QiAnXin Username	The username to log in to the hosts you want to scan.	yes
QiAnXin Asset Address	Specify the host IP of the asset containing the account to use. If not specified, the scan target IP is used.	no
QiAnXin Asset Platform	Specify the platform (based on asset type) of the asset containing the account to use. If not specified, a default target is used based on credential type (for example, for Windows credentials, the default is WINDOWS). Possible values: • **ACTIVE_DIRECTORY** — Windows Domain Account • **WINDOWS** — Windows Local Account • **LINUX** — Linux Account • **SQL_SERVER** — SQL Server Database • **ORACLE** — Oracle Database • **MYSQL** — MySQL Database • **DB2** — DB2 Database • **HP_UNIX** — HP Unix • **SOLARIS** — Solaris	no

Option	Description	Required
	• **OPENLDAP** — OpenLDAP • **POSTGRESQL** — PostgreSQL	
QiAnXin Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target.	yes
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To	no

Option	Description	Required
	specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	
Privilege Escalation	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **Privilege Escalation** selection determines the specific options you must configure. For more information, see Privilege Escalation.	no

Senhasegura Options

The following table describes the additional options to configure when using **Senhasegura** as the authentication method for SSH credentials.

Option	Description	Required
Senhasegura Host	The IP address or url for the Senhasegura host.	yes
Senhasegura Port	The port on which the Senhasegura API communicates. By default, Tenable uses 443.	yes
Senhasegura API Client ID	The Client ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes

Option	Description	Required
Senhasegura API Client Secret	The Secret ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura Credential ID or Identifier	The credential ID or identifier for the credential that you are requesting to retrieve.	yes
Use SSH Key for Target Authentication	The user can select this option to retrieve the SSH Key to authenticate to the target if configuration is applicable in Senhasegura.	Required if authenticating to target with SSH Key.
Private Key File	The Private Key used to decrypt encrypted sensitive data from A2A. **Note:** You can enable encryption of sensitive data in the A2A Application Authorizations. If enabled, you must provide a private key file in the scan credentials. This can be downloaded from the applicable A2A application in Senhasegura.	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
Use SSL	When enabled, Tenable Security Center uses SSL for secure communications. This setting is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. This setting is disabled by default.	no
Privilege Escalation	The Private Key used to decrypt encrypted sensitive data from A2A. **Note:** Tenable supports multiple options for privilege escalation, including su, su+sudo and sudo. For example, if you select sudo, more fields for sudo user, Escalation Account Name, and Location of su and sudo (directory) are provided	no

Option	Description	Required
	and can be completed to support authentication and privilege escalation through Senhasegura. The Escalation Account Name field is then required to complete your privilege escalation. **Note:** For more information about supported privilege escalation types and their accompanying fields, see [Privilege Escalation](#).	

Thycotic Secret Server Options

The following table describes the additional options to configure when using **Thycotic Secret Server** as the authentication method for SSH credentials.

Option	Description
Username	(Required) The username for a user on the target system.
Thycotic elevate privileges with	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your selection for this setting determines the specific options you must configure. For more information, see [Privilege Escalation](#).
Thycotic Secret Name	The Secret Name value on the Thycotic server.
Thycotic Secret Server URL	(Required) The value you want Tenable Security Center to use when setting the transfer method, target, and target directory for the scanner. Find the value on the Thycotic server, in **Admin > Configuration > Application Settings > Secret Server URL**. For example, if you type *https://pw.mydomain.com/SecretServer*, Tenable Security Center determines it is an SSL connection, that *pw.mydomain.com* is the target address, and that */SecretServer* is the root directory.
Thycotic Login Name	(Required) The username for a user on the Thycotic server.

Option	Description
Thycotic Password	(Required) The password associated with the **Thycotic Login Name** you provided.
Thycotic Organization	In cloud instances of Thycotic, the value that identifies the organization you want Tenable Security Center to target.
Thycotic Domain	The domain, if set for the Thycotic server.
Verify SSL Certificate	If enabled, Tenable Security Center verifies the SSL Certificate on the Thycotic server. For more information about using self-signed certificates, see the Nessus custom_CA.inc documentation.
Use Private Key	If enabled, Tenable Security Center uses key-based authentication for SSH connections instead of password authentication.

WALLIX Bastion Options

The following table describes the additional options to configure when using **WALLIX Bastion** as the authentication method for SSH credentials.

Option	Description	Required
WALLIX Host	The IP address for the WALLIX Bastion host.	yes
WALLIX Port	The port on which the WALLIX Bastion API communicates. By default, Tenable uses 443.	yes
Authentication Type	**Basic** authentication (with WALLIX Bastion user interface username and Password requirements) or **API Key** authentication (with username and WALLIX Bastion-generated API key requirements).	no
WALLIX User	Your WALLIX Bastion user interface login username.	yes

Option	Description	Required
WALLIX Password	Your WALLIX Bastion user interface login password. Used for **Basic** authentication to the API.	yes
WALLIX API Key	The API key generated in the WALLIX Bastion user interface. Used for **API Key** authentication to the API.	yes
Get Credential by Device Account Name	The account name associated with a **Device** you want to log in to the target systems with. **Note:** If your device has more than one account you must enter the specific device name for the account you want to retrieve credentials for. Failure to do this may result in credentials for the wrong account returned by the system.	Required only if you have a target and/or device with multiple accounts.
HTTPS	This is enabled by default. **Caution:** The integration fails if you disable **HTTPS**.	yes
Verify SSL Certificate	This is disabled by default and is not supported in WALLIX Bastion PAM integrations.	no
Privilege Escalation	This enables WALLIX Bastion Privileged Access Management (PAM). Use the drop-down menu to select the privilege elevation method. To bypass this function, leave this field set to **Nothing**. **Caution:** In your WALLIX Bastion account, the WALLIX Bastion super admin must have enabled "credential recovery" on your account for PAM to be enabled. Otherwise, your scan may not return any results. For more information, see your WALLIX Bastion documentation.	Required if you wish to escalate privileges.

Option	Description	Required
	Note: Multiple options for privilege escalation are supported, including *su*, *su+sudo* and *sudo*. For example, if you select **sudo**, more fields for **sudo user**, **Escalation Account Name**, and **Location of su and sudo** (directory) are provided and can be completed to support authentication and privilege escalation through WALLIX Bastion PAM. The **Escalation Account Name** field is then required to complete your privilege escalation.	
	Note: For more information about supported privilege escalation types and their accompanying fields, see [Privilege Escalation]().	
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	no

Privilege Escalation

Some SSH credential types support privilege escalation.

Note: BeyondTrust's PowerBroker (pbrun) and Centrify's DirectAuthorize (dzdo) are proprietary root task delegation methods for Unix and Linux systems.

> **Tip:** 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.

> **Note:** 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. For more information, see https://www.sudo.ws/docs/man/sudo.man/.

The following table describes the additional options to configure for privilege escalation.

Option	SSH Types	Description
Escalation Username	Arcon Checkpoint Gaia 'Expert' Kerberos Password Public Key WALLIX Bastion	The username for the account with elevated privileges.
Escalation Password	Kerberos Password Public Key WALLIX Bastion	The password for the account with elevated privileges.
Escalation Path	Arcon Kerberos Password Public Key WALLIX Bastion	The directory path for the privilege escalation commands.
Escalation Su User	Arcon	The username for the account with su privileges.

Option	SSH Types	Description
	CyberArk	
	Kerberos	
	Password	
	Public Key	
	WALLIX Bastion	
Escalation Account Name	Arcon Checkpoint Gaia 'Expert' CyberArk Delinea Secret Server	The name parameter for the account with elevated privileges. **Note:** For CyberArk credentials, the system uses the password associated with the CyberArk account name you provide for all scanned hosts.
CyberArk Escalation Account Details Name	Checkpoint Gaia 'Expert' CyberArk	The name parameter for the account with elevated privileges. **Note:** For CyberArk credentials, the system uses the password associated with the CyberArk account name you provide for all scanned hosts.
Escalation Account	CyberArk	The username for the account with elevated privileges.
Escalation Account Credential ID or Identifier	Senhasegura	The credential ID or identifier for the account with elevated privileges.
Escalation Account Secret Name	Hashicorp Vault	The key secret for the Hashicorp account with elevated privileges.
Escalation sudo	CyberArk	The username for the account with sudo privileges.

Option	SSH Types	Description
user		
Escalation Credential ID	Checkpoint Gaia 'Expert' Delinea Secret Server	The secret name for the account with elevated privileges.
Expert Password	Checkpoint Gaia 'Expert'	The password for Expert mode in Gaia.
Location of dzdo (directory)	CyberArk Delinea Secret Server Hashicorp Vault Senhasegura	The directory path for the dzdo command.
Location of pbrun (directory)	CyberArk Delinea Secret Server Hashicorp Vault Senhasegura	The directory path for the pbrun command.
Location of su (directory)	CyberArk Delinea Secret Server Hashicorp Vault Senhasegura	The directory path for the su command.
Location of su and sudo (directory)	CyberArk Delinea Secret Server	The directory path for the su and sudo commands.

Option	SSH Types	Description
	Hashicorp Vault	
	Senhasegura	
Location of sudo (directory)	CyberArk Delinea Secret Server Hashicorp Vault	The directory path for the sudo command.
su user	Delinea Secret Server Hashicorp Vault Senhasegura	The username for the account with su privileges.
su login	CyberArk Hashicorp Vault Senhasegura	The username for the account with su privileges.
sudo user	Hashicorp Vault Senhasegura	The username for the account with sudo privileges.
sudo login	CyberArk	The username for the account with sudo privileges.
Thycotic Escalation Account	Checkpoint Gaia 'Expert' Thycotic Secret Server	The name parameter for the account with elevated privileges. **Note:** For Thycotic credentials, the system uses the password associated with the Thycotic account name you provide for all scanned hosts.

Web Authentication Credentials

Required Additional License: Tenable Web App Scanning

Required Tenable Nessus Version: 10.6.1 or later

Configure the following options for Web Authentication credentials, including options specific for your authentication method: Client Certificate Authentication Options, HTTP Server Authentication Options, and Web Application Authentication Options.

For information about web app scans, see Web App Scans.

General Options	Description
Name	(Required) A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see Tags.

Client Certificate Authentication Options

The following table describes the additional options to configure when using **Client Certificate Authentication** as the authentication method for Web Authentication credentials.

Option	Description
Client Certificate	The file that contains the PEM-formatted certificate used to communicate with the host.
Client Certificate Private Key	The file that contains the PEM-formatted private key for the client certificate.
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
Page to Verify Successful Authentication	The URL that Tenable Security Center can access to validate the authenticated session.
Pattern to Verify Successful Authentication	A word, phrase, or regular expression that appears on the website only if the authentication is successful (for example, Welcome, *your username*!). Leading slashes are escaped and .* is not required at the beginning or end of the pattern.

HTTP Server Authentication Options

The following table describes the additional options to configure when using **HTTP Server Authentication** as the authentication method for Web Authentication credentials.

Option	Description
Username	(Required) The username that Tenable Security Center uses to authenticate to the HTTP server.
Password	(Required) The password that Tenable Security Center uses to authenticate to the HTTP server.
Authentication Type	The method used to authenticate to the HTTP server: • **Basic/Digest** • **NTLM** • **Kerberos**
Kerberos Realm	(Required when enabling the Kerberos Authentication Type) The realm to which Kerberos Target Authentication belongs, if applicable.
Key Distribution Center (KDC)	(Required when enabling the Kerberos Authentication Type) The host that supplies the session tickets for the user.

Web Application Authentication Options

The following table describes the additional options to configure when using **Web Application Authentication** as the authentication method for Web Authentication credentials.

Option	Description
Authentication Method	The method used to authenticate to the HTTP server: • **Login Form** • **Cookie Authentication** • **API Key** • **Selenium Authentication** • **Bearer Authentication**

Option	Description
Login Form	
Login Page	The URL of the login page for the web application you want to scan.

Login Parameters	For each field in the target's login form (for example, username, password, domain, etc.) enter one login parameter in each row:
	
	  a. In the left box, type the login field's name or id HTML DOM attribute.
	
	  b. In the right box, type the value to insert in that text field at login.
	
	  c. (Optional) Click **Add** to add additional login parameters.

Pattern to Verify Successful Auth	A word, phrase, or regular expression that appears on the website only if the authentication is successful (for example, *Welcome, your username*). Note that leading slashes are escaped and .* is not required at the beginning or end of the pattern.
Page to Verify Active Session	The URL that Tenable Security Center can continually access to validate the authenticated session.
Pattern to Verify Active Session	A word, phrase, or regular expression that appears on the website only if the session is still active (for example, *Hello, your username*). Note that leading slashes are escaped and .* is not required at the beginning or end of the pattern.
Cookie Authentication	

Cookies	Enter one cookie authentication credential in each row:
	
	  a. In the left box, type the name of the cookie authentication credential.
	
	  b. In the right box, type the value of the cookie authentication credential.
	
	  c. (Optional) Click **Add** to add additional cookie authentication credentials.

Page to Verify	The URL that Tenable Security Center can continually access to validate

Option	Description
Active Session	the authenticated session.
Pattern to Verify Active Session	A word, phrase, or regular expression that appears on the website only if the session is still active (for example, *Hello, your username*). Note that leading slashes are escaped and .* is not required at the beginning or end of the pattern.
API Key	
Headers	Enter one HTTP header in each row: a. In the left box, type the name of the HTTP header. b. In the right box, type the value of the HTTP header. c. (Optional) Click **Add** to add additional headers.
Page to Verify Active Session	The URL that Tenable Security Center can continually access to validate the authenticated session.
Pattern to Verify Active Session	A word, phrase, or regular expression that appears on the website only if the session is still active (for example, *Hello, your username*). Note that leading slashes are escaped and .* is not required at the beginning or end of the pattern.
Selenium Authentication	
Selenium Script (.side)	Use the following steps to add a `.side` file: a. In the Selenium IDE extension, record your authentication credentials. b. Click **Add File**. The file manager for your operating system appears. c. Navigate to and select your Selenium credentials `.side` file. Tenable Security Center imports the credentials file.
Page to Verify	The URL that Tenable Security Center can continually access to validate

Option	Description
Active Session	the authenticated session.
Pattern to Verify Active Session	A word, phrase, or regular expression that appears on the website only if the session is still active (for example, *Hello, your username*). Note that leading slashes are escaped and .* is not required at the beginning or end of the pattern.
Bearer Authentication	
Bearer Token	The value of the bearer token.
Page to Verify Active Session	The URL that Tenable Security Center can continually access to validate the authenticated session.
Pattern to Verify Active Session	A word, phrase, or regular expression that appears on the website only if the session is still active (for example, *Hello, your username*). Note that leading slashes are escaped and .* is not required at the beginning or end of the pattern.

Windows Credentials

Tenable Security Center has vulnerability checks that can use a Microsoft Windows account to find local information from a remote Windows host. For example, using credentials enables Tenable Security Center to determine if important security patches have been applied.

> **Tip:** Using a non-administrator account will greatly affect the quality of the scan results. Tenable recommends you create a Nessus user account with local administrative privileges specifically for scheduled scanning.

Configure the following options for Windows credentials, including options specific for your authentication method:

- [The following table describes the additional options to configure when using Arcon as the authentication method for Windows credentials.](#)

- [The following table describes the options to configure when using BeyondTrust as the authentication method for Windows credentials.](#)

- [Centrify Options](#)

- [The following table describes the options to configure when using CyberArk Vault (Legacy) as the authentication method for Windows credentials.](#)

- [The following table describes the additional options to configure when using CyberArk Windows Auto-Discovery as the authentication method for Windows credentials.](#)

- [The following table describes the additional options to configure when using CyberArk Vault as the authentication method for Windows credentials.](#)

- [The following table describes the additional options to configure when using Delinea Secret Server as the authentication method for Windows credentials.](#)

- [The following table describes the additional options to configure when using Hashicorp Vault as the authentication method for Windows credentials.](#)

- [The following table describes the options to configure when using Kerberos as the authentication method for Windows credentials.](#)

- [The following table describes the additional options to configure when using Lieberman as the authentication method for Windows credentials.](#)

- [The following table describes the options to configure when using LM Hash as the authentication method for Windows credentials.](#)

- [The following table describes the options to configure when using NTLM Hash as the authentication method for Windows credentials.](#)

- [The following table describes the options to configure when using Password as the authentication method for Windows credentials.](#)

- [QiAnXin Options](#)

- [The following table describes the options to configure when using Senhasegura as the authentication method for Windows credentials.](#)

- [The following table describes the options to configure when using Thycotic Secret Server as the authentication method for Windows credentials.](#)

- [The following table describes the additional options to configure when using WALLIX Bastion as the authentication method for Windows credentials.](#)

General Options	Description
Name	(Required) A name for the credential.
Description	A description for the credential.
Tag	A tag for the credential. For more information, see Tags.

Arcon Options

The following table describes the additional options to configure when using **Arcon** as the authentication method for Windows credentials.

Option	Description
Arcon Host	(Required) The Arcon IP address or DNS address. **Note:** If your Arcon installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Arcon Port	(Required) The port on which Arcon listens. By default, Tenable Security Center uses port 444.
API User	(Required) The API user provided by Arcon.
API Key	(Required) The API key provided by Arcon.
Authentication URL	(Required) The URL Tenable Security Center uses to access Arcon.
Password Engine URL	(Required) The URL Tenable Security Center uses to access the passwords in Arcon.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	(Required) The length of time, in hours, that you want to keep credentials checked out in Arcon. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Security Center scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails.

	Tip: Configure the password change interval in Arcon so that password changes do not disrupt your Tenable Security Center scans. If Arcon changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Arcon before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Arcon before enabling this option.

BeyondTrust Options

The following table describes the options to configure when using **BeyondTrust** as the authentication method for Windows credentials.

Option	Description
Username	The username to log in to the hosts you want to scan.
Domain	The domain of the username, if required by BeyondTrust.
BeyondTrust Host	The BeyondTrust IP address or DNS address.
BeyondTrust Port	The port BeyondTrust is listening on.
BeyondTrust API User	The API user provided by BeyondTrust.
BeyondTrust API Key	The API key provided by BeyondTrust.
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in BeyondTrust. Configure the **Checkout duration** to exceed the typical duration of your Tenable Security Center scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Tip:** Configure the password change interval in BeyondTrust so that

Option	Description
	password changes do not disrupt your Tenable Security Center scans. If BeyondTrust changes a password during a scan, the scan fails.
Use SSL	If enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option.
Verify SSL Certificate	If enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.

Centrify Options

The following table describes the additional options to configure when using **Centrify** as the authentication method for Windows credentials.

Option	Description
Centrify Host	(Required) The Centrify IP address or DNS address. **Note:** If your Centrify installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.
Centrify Port	(Required) The port on which Centrify listens. By default, Tenable Security Center uses port 443.
API User	(Required) The API user provided by Centrify.
API Key	(Required) The API key provided by Centrify.
Tenant	(Required) The Centrify tenant associated with the API. By default, Tenable Security Center uses *centrify*.
Authentication URL	(Required) The URL Tenable Security Center uses to access Centrify. By default, Tenable Security Center uses */Security*.
Password Query	(Required) The URL Tenable Security Center uses to query the

URL	passwords in Centrify. By default, Tenable Security Center uses */RedRock*.
Password Engine URL	(Required) The URL Tenable Security Center uses to access the passwords in Centrify. By default, Tenable Security Center uses */ServerManage*.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	(Required) The length of time, in minutes, that you want to keep credentials checked out in Centrify. Configure the **Checkout Duration** to exceed the typical duration of your Tenable Security Center scans so that password changes do not disrupt your Tenable Security Center scans. If Centrify changes a password during a scan, the scan fails. If a password from a previous scan is still checked out when a new scan begins, the new scan fails.
Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.

CyberArk Vault (Legacy) Options

The following table describes the options to configure when using **CyberArk Vault (Legacy)** as the authentication method for Windows credentials.

Option	Description
Username	The username for the target system.
Domain	The domain, if the username is part of a domain.
Central Credential	The CyberArk Central Credential Provider IP/DNS address.

Option	Description
Provider URL Host	
Central Credential Provider URL Port	The port the CyberArk Central Credential Provider is listening on.
Vault Username	The username for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Vault Password	The password for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Safe	The safe on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
AppID	The AppID with CyberArk Central Credential Provider permissions to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.
PolicyID	The PolicyID assigned to the credentials you want to retrieve.
Vault Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure

Option	Description
	communications. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option.
Vault Verify SSL	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option. For more information about using self-signed certificates, see Custom Plugin Packages for NASL and CA Certificate Upload.
CyberArk Escalation Account Details Name	The unique name of the credential you want to retrieve from CyberArk.
CyberArk AIM Service URL	The URL for the CyberArk AIM web service. By default, Tenable Security Center uses */AIMWebservice/v1.1/AIM.asmx*.

CyberArk Windows Auto-Discovery Options

The following table describes the additional options to configure when using **CyberArk Windows Auto-Discovery** as the authentication method for Windows credentials.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the user's CyberArk Instance.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes

Option	Description	Required
AppID	The Application ID associated with the CyberArk API connection.	yes
Safe	Users may optionally specify a Safe to gather account information and request passwords.	no
AIM Web Service Authentication Type	There are two authentication methods established in the feature. **IIS Basic Authentication** and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	yes
Username	(Appears if **AIM Web Service Authentication Type** is **IIS Basic Authentication**) The username for a user on the CyberArk server.	no
Password	(Appears if **AIM Web Service Authentication Type** is **IIS Basic Authentication**) The password associated with the username you provided.	no
Client Certificate	(Appears if **AIM Web Service Authentication Type** is **Certificate Authentication**) The file that contains the PEM certificate used to communicate with the CyberArk host.	no
Client Certificate Private Key	(Appears if **AIM Web Service Authentication Type** is **Certificate Authentication**) The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	(Appears if **AIM Web Service Authentication Type** is **Certificate Authentication**) The passphrase for the private key, if required.	yes, if private key is applied
CyberArk PVWA Web UI Login Name	Username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk PVWA	Password for the username to log in to CyberArk web	yes

Option	Description	Required
Web UI Login Password	console. This is used to authenticate to the PVWA REST API and gather bulk account information.	
CyberArk Platform Search String	String used in the PVWA REST API query parameters to gather bulk account information. For example, the user can enter `UnixSSH Admin TestSafe`, to gather all Windows platform accounts containing a username `Admin` in a Safe called `TestSafe`. **Note:** This is a non-exact keyword search. A best practice would be to create a custom platform name in CyberArk and enter that value in this field to improve accuracy.	yes
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.	yes
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no

CyberArk Vault Options

The following table describes the additional options to configure when using **CyberArk Vault** as the authentication method for Windows credentials.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the CyberArk AIM Web Service. This can be the host, or the host with a custom URL added on in a single string.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk	yes

Option	Description	Required
	API connection.	
Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	(Required if Kerberos Target Authentication is enabled) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	yes
KDC Transport	(Required if Kerberos Target Authentication is enabled) The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	yes
Domain	(Required if Kerberos Target Authentication is enabled) The domain to which Kerberos Target Authentication	yes

Option	Description	Required
	belongs, if applicable.	
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Address**, **Identifier**, **Parameters**, or **Username**. **Note:** For more information about the **Parameters** option, refer to the **Parameters Options** table. **Note:** The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier.	yes
Username	(If **Get credential by** is set to **Username**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Address	The option should only be used if the Address value is unique to a single CyberArk account credential.	no
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.	no
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no

Delinea Secret Server Options

The following table describes the additional options to configure when using **Delinea Secret Server** as the authentication method for Windows credentials.

Option	Description	Required
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled **Secret Name** on the Delinea server.	yes
Delinea Host	The Delinea Secret Server IP address for API requests.	yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Checkout Duration	The duration Tenable should check out the password from Delinea. Duration time is in hours and should be longer than the scan time.	yes
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Windows target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	no
Domain	(Required if Kerberos Target Authentication is enabled) The Kerberos Domain is the authentication domain,	yes

	usually noted as the domain name of the target.	
Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no
Verify SSL Certificate	If enabled. verifies the SSL Certificate on the Delinea server.	no

Hashicorp Vault Options

The following table describes the additional options to configure when using **Hashicorp Vault** as the authentication method for Windows credentials.

Option	Default Value	Required
Hashicorp Host	The Hashicorp Vault IP address or DNS address. **Note:** If your Hashicorp Vault installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/subdirectory path*.	yes
Hashicorp Port	The port on which Hashicorp Vault listens.	yes
Authenticaton Type	Specifies the authentication type for connecting to the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate** (Required) and **Hashicorp Client Certificate Private Key** (Required) appear. Select the appropriate files for the client certificate and private key.	yes
Role ID	The GUID provided by Hashicorp Vault when you configured your App Role.	yes
Role Secret ID	The GUID generated by Hashicorp Vault when you configured your App Role.	yes
Authentication	The path/subdirectory to the authentication endpoint.	yes

URL	This is not the full URL. For example: `/v1/auth/approle/login`	
Namespace	The name of a specified team in a multi-team environment.	no
Hashicorp Vault Type	The type of Hashicorp Vault secrets engine: • **KV1** — Key/Value Secrets Engine Version 1 • **KV2** — Key/Value Secrets Engine Version 2 • **AD** — Active Directory • **LDAP** - LDAP secrets engine	yes
KV1 Engine URL **KV2 Engine URL** **AD Engine URL** **LDAP Engine URL**	The engine URL combines with the secret name to form the API request URL. For example, a secret name of `creds` and a KV v1 engine url of `/v1/secret` would result in a GET request to `/v1/secret/creds` (for KV v2, `/v1/secret/data/creds`).	yes
Username Source	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) Specifies if the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	(Only displays if **Hashicorp Vault Type** is **KV1** or **KV2**) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	The key secret you want to retrieve values for.	yes
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes

KDC Port	(Required if Kerberos Target Authentication is enabled) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	yes
KDC Transport	(Required if Kerberos Target Authentication is enabled) The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	yes
Domain	(Required if Kerberos Target Authentication is enabled) The domain to which Kerberos Target Authentication belongs, if applicable.	yes
Use SSL	When enabled, Tenable Security Center uses SSL for secure communications. You must configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no

Kerberos Options

The following table describes the options to configure when using **Kerberos** as the authentication method for Windows credentials.

Option	Description
Username	The username for a user on the target system.
Password	The password associated with the username you provided.
Domain	The authentication domain, typically the domain name of the target (e.g., *example.com*).
KDC Host	The host supplying the session tickets.

Option	Description
KDC Port	The port you want to use for the KDC connection. By default, Tenable Security Center uses port 88.
KDC Transport	The method you want to use to connect to the KDC server. > **Note:** If you select UDP, you may need to edit the **KDC Port**. The KDC UDP protocol uses either port 88 or port 750.

Lieberman Options

The following table describes the additional options to configure when using **Lieberman** as the authentication method for Windows credentials.

Option	Description
Username	The username for a user on the database.
Domain	The domain of the username, if required by Lieberman.
Lieberman Host	The Lieberman IP address or DNS address. > **Note:** If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type `IP address or hostname/subdirectory path`.
Lieberman Port	The port Lieberman is listening on.
Lieberman User	The username for the Lieberman explicit user you want Tenable Security Center to use for authentication to the Lieberman Rapid Enterprise Defense (RED) API.
Lieberman Password	The password for the Lieberman explicit user.
Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Lieberman before enabling this option.

Option	Description
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Lieberman before enabling this option. For more information about using self-signed certificates, see Custom Plugin Packages for NASL and CA Certificate Upload.
System Name	The name for the database credentials in Lieberman.

LM Hash Options

The following table describes the options to configure when using **LM Hash** as the authentication method for Windows credentials.

Option	Description
Username	The username for a user on the target system.
Hash	The LM hash you want to use.
Domain	The domain of the username, if required.

NTLM Hash Options

The following table describes the options to configure when using **NTLM Hash** as the authentication method for Windows credentials.

Option	Description
Username	The username for a user on the target system.
Hash	The NTLM hash you want to use.
Domain	The domain of the username, if required.

Password Options

The following table describes the options to configure when using **Password** as the authentication method for Windows credentials.

Option	Description
Username	The username for a user on the target system.
Password	The password associated with the username you provided.
Domain	The domain of the username, if required.

QiAnXin Options

The following table describes the options to configure when using **QiAnXin** as the authentication method for Windows credentials.

Option	Description	Required
QiAnXin Host	The IP address or URL for the QiAnXin host.	yes
QiAnXin Port	The port on which the QiAnXin API communicates. By default, Tenable uses 443.	yes
QiAnXin API Client ID	The Client ID for the embedded account application created in QiAnXin PAM.	yes
QiAnXin API Client Secret	The Secret ID for the embedded account application created in QiAnXin PAM.	yes
QiAnXin Username	The username to log in to the hosts you want to scan.	yes
Domain	The domain to which the username belongs.	no
QiAnXin Asset Address	Specify the host IP of the asset containing the account to use. If not specified, the scan target IP is used.	no
QiAnXin Asset Platform	Specify the platform (based on asset type) of the asset containing the account to use. If not specified, a default target is used based on credential type (for example, for Windows credentials, the default is WINDOWS). Possible	no

Option	Description	Required
	values:	
	- **ACTIVE_DIRECTORY** — Windows Domain Account - **WINDOWS** — Windows Local Account - **LINUX** — Linux Account - **SQL_SERVER** — SQL Server Database - **ORACLE** — Oracle Database - **MYSQL** — MySQL Database - **DB2** — DB2 Database - **HP_UNIX** — HP Unix - **SOLARIS** — Solaris - **OPENLDAP** — OpenLDAP - **POSTGRESQL** — PostgreSQL	
QiAnXin Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions.
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Windows target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If	no

Option	Description	Required
	you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	
Domain	(Required if Kerberos Target Authentication is enabled) The Kerberos Domain is the authentication domain, usually noted as the domain name of the target.	yes
Use SSL	When enabled, Tenable uses SSL for secure communication. This is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable verifies that the SSL Certificate on the server is signed by a trusted CA.	no

Senhasegura Options

The following table describes the options to configure when using **Senhasegura** as the authentication method for Windows credentials.

Option	Description	Required
Senhasegura Host	The IP address or url for the Senhasegura host.	yes
Senhasegura Port	The port on which the Senhasegura API communicates. By default, Tenable uses 443.	yes
Senhasegura API Client ID	The Client ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura API Client Secret	The Secret ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Domain	The domain to which the username belongs.	no

Option	Description	Required
Senhasegura Credential ID or Identifier	The credential ID or identifier for the credential that you are requesting to retrieve.	yes
Private Key File	The Private Key used to decrypt encrypted sensitive data from A2A. **Note:** You can enable encryption of sensitive data in the A2A Application Authorizations. If enabled, you must provide a private key file in the scan credentials. This can be downloaded from the applicable A2A application in Senhasegura.	Required if you have enabled encryption of sensitive data in A2A Application Authorizations.
Use SSL	When enabled, Tenable Security Center uses SSL for secure communications. This setting is enabled by default.	no
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. This setting is disabled by default.	no

Thycotic Secret Server Options

The following table describes the options to configure when using **Thycotic Secret Server** as the authentication method for Windows credentials.

Option	Description
Username	(Required) The username for a user on the target system.
Domain	The domain of the username, if set on the Thycotic server.
Thycotic Secret Name	The Secret Name value on the Thycotic server.
Thycotic Secret Server URL	(Required) The value you want Tenable Security Center to use when setting the transfer method, target, and target directory for the scanner. Find the

Option	Description
	value on the Thycotic server, in **Admin > Configuration > Application Settings > Secret Server URL**. For example, if you type *https://pw.mydomain.com/SecretServer*, Tenable Security Center determines it is an SSL connection, that *pw.mydomain.com* is the target address, and that */SecretServer* is the root directory.
Thycotic Login Name	(Required) The username for a user on the Thycotic server.
Thycotic Password	(Required) The password associated with the **Thycotic Login Name** you provided.
Thycotic Organization	In cloud instances of Thycotic, the value that identifies which organization the Tenable Security Center query should target.
Thycotic Domain	The domain, if set for the Thycotic server.
Use Private Key	If enabled, Tenable Security Center uses key-based authentication for SSH connections instead of password authentication.
Verify SSL Certificate	If enabled, Tenable Security Center verifies the SSL Certificate on the Thycotic server. For more information about using self-signed certificates, see Custom Plugin Packages for NASL and CA Certificate Upload.

WALLIX Bastion Options

The following table describes the additional options to configure when using **WALLIX Bastion** as the authentication method for Windows credentials.

Option	Description	Required
WALLIX Host	The IP address for the WALLIX Bastion host.	yes
WALLIX Port	The port on which the WALLIX Bastion API	yes

Option	Description	Required
	communicates. By default, Tenable uses 443.	
Authentication Type	**Basic** authentication (with WALLIX Bastion user interface username and Password requirements) or **API Key** authentication (with username and WALLIX Bastion-generated API key requirements).	no
WALLIX User	Your WALLIX Bastion user interface login username.	yes
WALLIX Password	Your WALLIX Bastion user interface login password. Used for **Basic** authentication to the API.	yes
WALLIX API Key	The API key generated in the WALLIX Bastion user interface. Used for **API Key** authentication to the API.	yes
Get Credential by Device Account Name	The account name associated with a **Device** you want to log in to the target systems with. **Note:** If your device has more than one account you must enter the specific device name for the account you want to retrieve credentials for. Failure to do this may result in credentials for the wrong account returned by the system.	Required only if you have a target and/or device with multiple accounts.
HTTPS	This is enabled by default. **Caution:** The integration fails if you disable **HTTPS**.	yes
Verify SSL Certificate	This is disabled by default and is not supported in WALLIX Bastion PAM integrations.	no

Audit Files

The Tenable Nessus vulnerability scanner allows you 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. For more information, see Manage Audit Files.

After you create an audit file, you can reference the audit file in a template-based Policy Compliance Auditing scan policy or a custom scan policy. For more information about compliance options in custom scan policies, see The Compliance tab specifies compliance the audit files to reference in a scan policy. The options available depend on the type of audit file selected..

For more information on compliance checks and creating custom audits, see the Compliance Checks Reference.

> **Note:** The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements.

Template-Based Audit Files

You can add template-based audit files using templates embedded within Tenable Security Center. Tenable updates these templates regularly through the Tenable Security Center feed.

For more information, see Add a Template-Based Audit File.

Custom Audit Files

You can add custom audit files to upload any of the following:

- a Tenable-created audit file downloaded from the Tenable downloads page.

- a Security Content Automation Protocol (SCAP) Data Stream file downloaded from a SCAP repository (e.g., https://nvd.nist.gov/ncp/repository).

  The file must contain full SCAP content (Open Vulnerability and Assessment Language (OVAL) and Extensible Configuration Checklist Description Format (XCCDF) content) or OVAL standalone content.

> **Note:** XCCDF standalone content audit files lack automated checks and do not return scan results in Tenable Security Center.

- a custom audit file created or customized for a specific environment. For more information, see the knowledge base article.

For more information, see Add a Custom Audit File.

Add a Template-Based Audit File

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can add template-based audit files using templates embedded within Tenable Security Center. Tenable updates these templates regularly through the Tenable Security Center feed.

For more information, see Audit Files.

> **Note:** The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements.

To add a template-based audit file:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Audit Files** (administrator users) or **Scans** > **Audit Files** (organizational users).

   The **Audit Files** page appears.

3. Click **Add**

   The **Audit File Templates** page appears.

4. In the **Common** section, click a template category tile.

   The **Add Audit Template** page appears.

5. In the **Name** box, type a name for the audit file.

6. (Optional) In the **Description** box, type a description for the audit file.

7. (Optional) Edit the template-specific options if you do not want to use the default values.

8. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

- Reference the audit file in a template-based Policy Compliance Auditing scan policy or a custom scan policy. For more information about compliance options in custom scan policies, see The Compliance tab specifies compliance the audit files to reference in a scan policy. The options available depend on the type of audit file selected..

Add a Custom Audit File

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can add custom audit files to upload any of the following:

- a Tenable-created audit file downloaded from the Tenable downloads page.

- a Security Content Automation Protocol (SCAP) Data Stream file downloaded from a SCAP repository (e.g., https://nvd.nist.gov/ncp/repository).

  The file must contain full SCAP content (Open Vulnerability and Assessment Language (OVAL) and Extensible Configuration Checklist Description Format (XCCDF) content) or OVAL standalone content.

  > **Note:** XCCDF standalone content audit files lack automated checks and do not return scan results in Tenable Security Center.

- a custom audit file created or customized for a specific environment. For more information, see the knowledge base article.

For more information, see Audit Files.

> **Note:** The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements.

Before you begin:

- Download or prepare the file you intend to upload.

To add a custom audit file or SCAP Data Stream file:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Scanning** > **Audit Files** (administrator users) or **Scans** > **Audit Files** (organizational users).

   The **Audit Files** page appears.

3. Click **Add**

   The **Audit File Templates** page appears.

4. In the **Other** section, click the **Advanced** tile.

5. In the **Name** box, type a descriptive name for the audit file.

6. In the **Description** box, type a description for the audit file.

7. Click **Choose File** and browse to the **Audit File** you want to upload.

   The system uploads the file. If you uploaded a SCAP Data Stream file, additional options appear.

8. If you uploaded a Data Stream file with full SCAP content, continue configuring options for the file:

   a. If you uploaded SCAP 1.2 content or later, in the **Data Stream Name** box, select the Data Stream identifier found in the SCAP 1.2 Data Stream content.

   b. In the **Benchmark Type** box, select the operating system that the SCAP content targets.

   c. In the **Benchmark Name** box, select the benchmark identifier found in the SCAP XCCDF component.

   d. In the **Profile** box, select the benchmark profile identifier found in the SCAP XCCDF component.

9. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

- Reference the audit file in a template-based Policy Compliance Auditing scan policy or a custom scan policy. For more information about compliance options in custom scan policies, see The Compliance tab specifies compliance the audit files to reference in a scan policy. The options available depend on the type of audit file selected..

Manage Audit Files

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Audit Files.

To manage your audit files:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Audit Files**.

   The **Audit Files** page appears.

3. To filter the audit files that appear on the page, apply a filter as described in Apply a Filter.

4. To add an audit file, see Add a Template-Based Audit File or Add a Custom Audit File.

5. To view details for an audit file:

   a. Right-click the row for the audit file.

   The actions menu appears.

   -or-

   Select the check box for the audit file.

   The available actions appear at the top of the table.

   b. Click **View**.

   The **View Audit File** page appears.

6. To edit or replace an audit file:

a. Right-click the row for the audit file.

   The actions menu appears.

   -or-

   Select the check box for the audit file.

   The available actions appear at the top of the table.

b. Click **Edit**.

   The **Edit Audit File** page appears.

c. To edit the name or description, type a new **Name** or **Description**.

d. To replace the audit file, click the delete button (✖) next to the file and upload a new audit file.

e. Click **Submit**.

   Tenable Security Center saves your configuration.

7. To share or revoke access to an audit file:

a. Right-click the row for the audit file.

   The actions menu appears.

   -or-

   Select the check box for the audit file.

   The available actions appear at the top of the table.

b. Click **Share**.

c. Share or revoke access for each group in your organization.

d. Click **Submit**.

   Tenable Security Center saves your configuration.

8. To export an audit file:

a. Right-click the row for the audit file.

The actions menu appears.

-or-

Select the check box for the audit file.

The available actions appear at the top of the table.

b. Click **Export**.

Tenable Security Center exports the audit file.

9. To delete an audit file:

a. Right-click the row for the audit file.

The actions menu appears.

-or-

Select the check box for the audit file.

The available actions appear at the top of the table.

b. Click **Delete**.

A confirmation window appears.

c. Click **Delete**.

Tenable Security Center deletes the audit file.

Scan Zones

Scan zones are areas of your network that you want to target in an active scan, associating an IP address or range of IP addresses with one or more scanners in your deployment. You must create scan zones in order to run active scans in Tenable Security Center.

For more information, see Add a Scan Zone, View Your Scan Zones, Edit a Scan Zone, and Delete a Scan Zone.

Option	Description
Name	A name for the scan zone.

Description	(Optional) A description for the scan zone.
Ranges	One or more IP addresses that you want the scan zone to target. Supported formats: • a comma-separated list of IP addresses and/or CIDR addresses. • a newline-separated list of IP addresses and/or CIDR addresses. • a hyphenated range of IP addresses (e.g., 192.0.2.0-192.0.2.25).
Scanners	One or more scanners that you want to use to scan the **Ranges** in this scan zone. **Note:** Do not choose scanners that cannot reach the areas of your network identified in the **Ranges**. Similarly, consider the quality of the network connection between the scanners you choose and the **Ranges**.

Best Practices

Tenable recommends pre-planning your scan zone strategy to efficiently target discrete areas of your network. If configured improperly, scan zones prevent scanners from reaching their targets. Consider the following best practices:

- It is simplest to configure and manage a small number of scan zones with large ranges.

- It is simplest to target ranges (versus large lists of individual IP addresses).

- If you use Nessus Manager for agent management, do not target Nessus Manager in any scan zone ranges.

Overlapping Scan Zones

In some cases, you may want to configure overlapping scan zones to ensure scanning coverage or redundancy.

Note: Do not configure overlapping scan zones without pre-planning your scan zone and **Distribution Method** strategy.

Two or more scan zones are redundant if they target the same area of your network. If Tenable Security Center executes a scan with redundant scan zones, it first attempts the scan using the narrowest, most specific scan zone.

In this example, the red numbers represent specific IP addresses on your network. The grey circles represent the network coverage of individual scan zones.
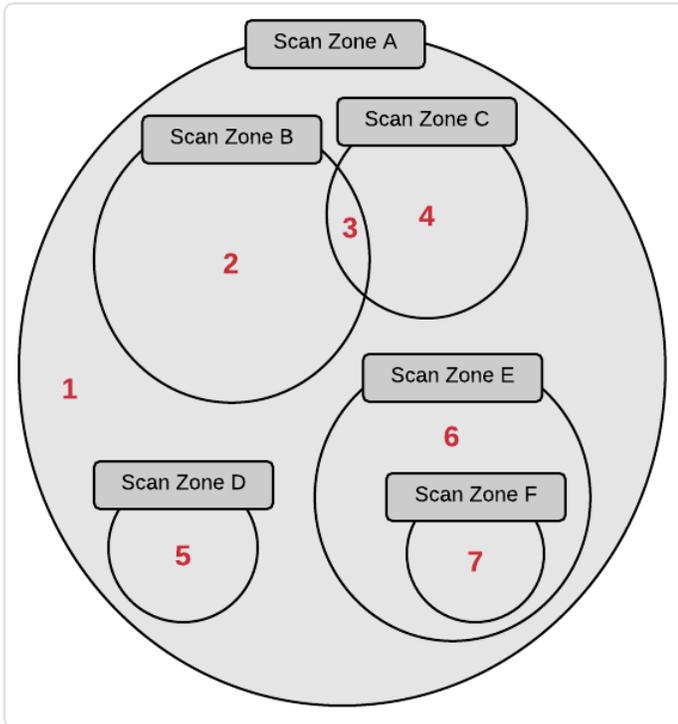
See the following table to understand the primary and redundant scan zones for the IP addresses in this example.

IP Address	Primary Scan Zone	Redundant Scan Zones
1	Scan Zone A	None.
2	Scan Zone B	Scan Zone A.
3	Scan Zone C	Scan Zone B, then Scan Zone A.
4	Scan Zone C	Scan Zone A.
5	Scan Zone D	Scan Zone A.
6	Scan Zone E	Scan Zone A.

| 7 | Scan Zone F | Scan Zone E, then Scan Zone A. |

Add a Scan Zone

Required Tenable Security Center User Role: Administrator

For more information about scan zone options, see Scan Zones.

To add a scan zone:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Scan Zones**.

   The **Scan Zones** page appears.

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

   The **Add Scan Zone** page appears.

4. In the **Name** box, type a name for the scan zone.

5. In the **Description** box, type a description for the scan zone.

6. In the **Ranges** box, type one or more IP addresses, CIDR addresses, or ranges to target with the scan zone.

7. In the **Scanners** box, choose one or more scanners to associate with the scan zone.

8. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

- Configure scan zone-related organization settings, as described in Organizations.

- Configure an active scan that targets your scan zone, as described in Add an Active Scan.

View Your Scan Zones

Required Tenable Security Center User Role: Administrator

For more information, see Scan Zones.

To view a list of configured scan zones:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Scan Zones**.

   The **Scan Zones** page appears.

3. View details about each scan zone.

   - **Name** — The name of the scan zone.

   - **Status** — The status of the scan zone.

Scan Zone Status	Description
All Scanners Available	All of the scanners in the scan zone are **Working**.
x/y Scanners Available	Only some of the scanners in the scan zone are **Working**.
No Scanners Available	None of the scanners in the scan zone are **Working**.

     For information about **Working** and other scanner statuses, see Tenable Nessus Scanner Statuses.

   - **Scanners** — The number of Tenable Nessus scanners in the scan zone.

   - **Last Modified** — The date and time the scan zone was last modified.

Edit a Scan Zone

Required Tenable Security Center User Role: Administrator

For more information about scan zone options, see Scan Zones.

To edit a scan zone:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Scan Zones**.

   The **Scan Zones** page appears.

3. Right-click the row for the scan zone you want to edit.

The actions menu appears.

-or-

Select the check box for the scan zone you want to edit.

The available actions appear at the top of the table.

4. Click **Edit**.

   The **Edit Scan Zone** page appears.

5. Modify the following scan zone options. For more information, see Scan Zones.

   - **Name**

   - **Description**

   - **Ranges**

   - **Scanners**

6. Click **Submit**.

   Tenable Security Center saves your configuration.

Delete a Scan Zone

Required Tenable Security Center User Role: Administrator

For more information, see Scan Zones.

Before you begin:

- Confirm that no scans target the scan zone you want to delete. Tenable Security Center scans may fail if you delete an actively targeted scan zone.

To delete a scan zone:

1. Log in to Tenable Security Center via the user interface.

2. Click **Resources** > **Scan Zones**.

   The **Scan Zones** page appears.

3. Select the scan zone you want to delete:

To delete a single scan zone:

   a. In the table, right-click the row for the scan zone you want to delete.

   The actions menu appears.

   b. Click **Delete**.

To delete multiple scan zones:

   a. In the table, select the check box for each scan zone you want to delete.

   The available actions appear at the top of the table.

   b. At the top of the table, click **Delete**.

A confirmation window appears.

4. Click **Delete**.

Tenable Security Center deletes the scan zone.

Scan Policies

Scan policies contain plugin settings and advanced directives for active scans.

When an administrator user creates a scan policy, the policy is available to all organizations. When an organizational user creates a scan policy, the scan policy is available only to their organization. Users with the appropriate permissions can use scan policies in an active scan, modify policy options, and more. For more information about user permissions, see User Roles.

For more information, see:

- Add a Scan Policy

- Scan Policy Templates

- Scan Policy Options

- View Your Scan Policies

- View Scan Policy Details

- Edit a Scan Policy

- [Share or Revoke Access to a Scan Policy](#)

- [Export a Scan Policy](#)

- [Import a Scan Policy](#)

- [Copy a Scan Policy](#)

- [Delete a Scan Policy](#)

Add a Scan Policy

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

You can create template-based or custom scan policies for your active scans. When you create a custom scan policy, you can configure any scan policy option. When you configure a template-based scan policy, you can configure the options included for the template type. For more information about Tenable-provided scan policy templates, see [Scan Policy Templates](#).

For more information, see [Scan Policies](#) and [Active Scans](#).

To add a template-based scan policy:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   The **Policies** page appears.

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

   The **Add Policy** page appears.

4. In the **Template** section, click a policy template. For more information, see [Scan Policy Templates](#).

   The policy template page appears.

5. Configure the options described in [Scan Policy Options](#).

6. Click **Submit**.

   Tenable Security Center saves your configuration.

To add a custom scan policy:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   The **Policies** page appears.

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

   The **Add Policy** page appears.

4. In the **Custom** section, click **Advanced Scan**.

   The **Advanced Scan** page appears.

5. Configure the options described in Scan Policy Options.

6. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

- Reference the scan policy in an active scan configuration, as described in Add an Active Scan.

Scan Policy Templates

Tenable Security Center provides scan policy templates with pre-configured plugin settings and advanced directives for active scans. You can configure a Tenable-provided template or you can create a fully customized scan policy from all of the available scan policy options in Tenable Security Center.

Each Tenable-provided scan policy template contains a different set of scan policy options. You can only modify the settings included for that scan policy template type.

Custom scan policies, such as Advanced Scan, contain all scan policy options. You can modify any scan policy options for custom scans.

For more information, see Scan Policies and Scan Policy Options.

> **Note:** If there is a Tenable-provided template that does not appear in this list, it may be a scan policy that is not supported by Tenable Security Center.

Template	Description
Common	
Advanced Agent Scan	The most configurable scan type. You can configure this scan template to match any policy. This template has the same default settings as the basic scan template, but it allows for additional configuration options. **Note:** Advanced scan templates allow you to scan more deeply using custom configuration, such as faster or slower checks, but misconfigurations can cause asset outages or network saturation. Use the advanced templates with caution.
Advanced Scan	The most configurable scan type. You can configure this scan template to match any policy. This template has the same default settings as the basic scan template, but it allows for additional configuration options. **Note:** Advanced scan templates allow you to scan more deeply using custom configuration, such as faster or slower checks, but misconfigurations can cause asset outages or network saturation. Use the advanced templates with caution. **Note:** Tenable automatically updates this template with any newly-released plugin families in which plugins rely on network traffic for detection.
Basic Network Scan	Performs a full system scan that is suitable for any host. Use this template to scan an asset or assets with all of Nessus's plugins enabled. For example, you can perform an internal vulnerability scan on your organization's systems.
Credentialed Patch Audit	Authenticates hosts and enumerates missing updates. Use this template with credentials to give Tenable Security Center direct access to the host, scan the target hosts, and enumerate missing patch updates.
Web Application Tests	Scan for published and unknown web vulnerabilities.

Compliance Configuration	
Internal PCI Network Scan	Performs an internal PCI DSS (11.2.1) vulnerability scan.
	This template creates scans that you can use to satisfy internal (PCI DSS 11.2.1) scanning requirements for ongoing vulnerability management programs that satisfy PCI compliance requirements. You can use these scans for ongoing vulnerability management and to perform rescans until passing or clean results are achieved. You can provide credentials to enumerate missing patches and client-side vulnerabilities.
	Note: While the PCI DSS requires you to provide evidence of passing or "clean" scans on at least a quarterly basis, you must also perform scans after any significant changes to your network (PCI DSS 11.2.3).
PCI Quarterly External Scan	Performs quarterly external scans as required by PCI.
	You can use this template to simulate an external scan (PCI DSS 11.2.2) to meet PCI DSS quarterly scanning requirements. However, you cannot submit the scan results from this template to Tenable for PCI Validation. Only Tenable Vulnerability Management customers can submit their PCI scan results to Tenable for PCI ASV validation.
Policy Compliance Auditing	Audits system configurations against a known baseline.
	Note: The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements.
	The compliance checks can audit against custom security policies, such as password complexity, system settings, or registry values on Windows operating systems. For Windows systems, the compliance audits can test for a large percentage of anything that can be described in a Windows policy file. For Unix systems, the compliance audits test for running processes, user security policy, and content of files.

SCAP and OVAL Auditing	Audits systems using SCAP and OVAL definitions.
	The National Institute of Standards and Technology (NIST) Security Content Automation Protocol (SCAP) is a set of policies for managing vulnerabilities and policy compliance in government agencies. It relies on multiple open standards and policies, including OVAL, CVE, CVSS, CPE, and FDCC policies.
	- SCAP compliance auditing requires sending an executable to the remote host. - Systems running security software (for example, McAfee Host Intrusion Prevention), may block or quarantine the executable required for auditing. For those systems, you must make an exception for either the host or the executable sent. - When using the **SCAP and OVAL Auditing** template, you can perform Linux and Windows **SCAP CHECKS** to test compliance standards as specified in NIST's Special Publication 800-126.
Other	
Active Directory Starter Scan	Scans for misconfigurations in Active Directory.
	Use this template to check Active Directory for Kerberoasting, Weak Kerberos encryption, Kerberos pre-authentication validation, non-expiring account passwords, unconstrained delegation, null sessions, Kerberos KRBTGT, dangerous trust relationships, Primary Group ID integrity, and blank passwords.
Credential Validation	A lightweight scan template used to verify that host credential pairs for Windows and Unix successfully authenticate to scan targets. Use this scan template to quickly diagnose credential pair issues in your network.
Find AI	Scans for artificial intelligence (AI), large language model (LLM), and machine learning (ML) related detections and vulnerabilities.
Host Discovery	Performs a simple scan to discover live hosts and open ports.
	Launch this scan to see what hosts are on your network and associated

	information such as IP address, FQDN, operating systems, and open ports, if available. After you have a list of hosts, you can choose what hosts you want to target in a specific vulnerability scan.
	Tenable recommends that organizations who do not have a passive network monitor, such as Nessus Network Monitor, run this scan weekly to discover new assets on your network.
	Note: Assets identified by discovery scans do not count toward your license.
Malware Scan	Scans for malware on Windows and Unix systems.
	Tenable Security Center detects malware using a combined allow list and block list approach to monitor known good processes, alert on known bad processes, and identify coverage gaps between the two by flagging unknown processes for further inspection.
Nessus 10.8.0 / 10.8.1 Agent Reset	Scan to find, reset, and update Tenable Agents on versions 10.8.0 and 10.8.1. For more information, see the upgrade notes of the [[[Undefined variable Agent.Agent]]] 10.8.2 release notes.
Ping-only Discovery	A simple scan to discover live hosts with minimal network traffic.

Web Application Scanning

Required Additional License: Tenable Web App Scanning

Required Tenable Nessus Version: 10.6.1 or later

API	A scan that checks an API for vulnerabilities. This scan analyzes RESTful APIs described via an OpenAPI (Swagger) specification file.
Log4Shell	Detects the Log4Shell vulnerability (CVE-2021-44228) in Apache Log4j.
PCI	A scan that assesses web applications for compliance with Payment Card Industry Data Security Standards (PCI DSS) for PCI ASV.
Quick Scan	A high-level scan similar to the **Config Audit** scan policy template that

	analyzes HTTP security headers and other externally facing configurations on a web application to determine if the application is compliant with common security industry standards. Does not include scheduling.
	If you create a scan using the **Quick Scan** scan policy template, Tenable Security Center analyzes your web application only for plugins related to security industry standards compliance.
Scan	A comprehensive scan that assesses web applications for a wide range of vulnerabilities.
	The **Scan** scan policy template provides plugin family options for all active web application plugins.
	If you create a scan using the **Scan** scan policy template, Tenable Security Center analyzes your web application for all plugins that the scanner checks for when you create a scan using the **Web App Config Audit**, **Web App Overview**, or **SSL_TLS** scan policy templates, as well as additional plugins to detect specific vulnerabilities.
	A scan run with this scan template provides a more detailed assessment of a web application and take longer to complete that other web app scans.
SSL_TLS	A scan to determine if a web application uses SSL/TLS public-key encryption and, if so, how the encryption is configured.
	When you create a scan using the **SSL_TLS** scan policy template, Tenable Security Center analyzes your web application only for plugins related to SSL/TLS implementation. The scanner does not crawl URLs or assess individual pages for vulnerabilities.
Web App Config Audit	A high-level scan that analyzes HTTP security headers and other externally facing configurations on a web application to determine if the application is compliant with common security industry standards.
	If you create a scan using this scan policy template, Tenable Security Center analyzes your web application only for plugins related to security industry standards compliance.
Web App	A high-level preliminary scan that determines which URLs in a web

Overview	application Tenable Security Center scans by default.
	This scan template does not analyze the web application for active vulnerabilities. Therefore, this scan policy template does not offer as many plugin family options as the **Scan** template.

Scan Policy Options

Scan policy options specify granular configurations for your active scans.

When you create a custom scan policy, you can configure any scan policy option. When you configure a template-based scan policy, you can configure the options included for the template type. For more information about Tenable-provided scan policy templates, see Scan Policy Templates.

- Setup Options

- Advanced Options

- Host Discovery Options

- Port Scanning Options

- Service Discovery Options

- Assessment Options

- Brute Force Options

- Malware Options

- SCADA Options

- Web Applications Options

- Windows Options

- Report Options

- Authentication Options

- Compliance Options

- Plugins Options

Setup Options

Option	Description
General	
Name	A unique name for the policy.
Description	(Optional) A description for the policy.
Tag	A tag for the policy. For more information, see Tags.

Advanced Options

Option	Description
General Settings	
Enable safe checks	Tenable Nessus attempts to identify remote vulnerabilities by interpreting banner information and attempting to exercise a vulnerability. When **Enable safe checks** is enabled, Tenable Nessus does not attempt to exercise any vulnerabilities. This is not as reliable as a full probe, but is less likely to negatively impact a targeted system.
Scan for unpatched vulnerabilities (no patches or mitigations available)	Determines whether the scan searches for unpatched vulnerabilities. This includes CVEs marked as "Will Not Fix" by the related vendor. Enabling this setting may increase your overall findings count; each platform and package combination results in an individual plugin. If additional CVEs are found to affect a platform and package combination, the CVEs are added to the existing plugin. This setting is disabled by default. **Note:** If you configure a scan to produce findings for unpatched vulnerabilities and then the setting is unchecked, Tenable Security Center remediates unpatched findings in the next scan. Additionally, if multiple scans target the same device and one has enabled findings for unpatched vulnerabilities and another does not, the findings results may vary per scan.

Option	Description
Custom Red Hat repository mapping	Upload a .json file that maps internal custom or mirrored repositories to their official Red Hat repository counterparts. For more information on how this works, see How Red Hat Local Vulnerability Checks Use Repositories To Determine Scope. By default, this setting is disabled and requires you to upload a .json file.
Stop scanning hosts that become unresponsive during the scan	During a scan, hosts may become unresponsive after a period of time. Enabling this setting stops scan attempts against hosts that stop sending results.
Automatically accept detected SSH disclaimer prompts	When enabled, if a credentialed scan tries to connect via SSH to a host that presents a disclaimer prompt, the scanner provides the necessary text input to accept the disclaimer prompt and continue the scan. When disabled, credentialed scans on hosts that present a disclaimer prompt fail because the scanner cannot connect to the device and accept the disclaimer. The error appears in the plugin output.
Scan targets with multiple domain names in parallel	When disabled, to avoid overwhelming a host, Tenable Nessus prevents against simultaneously scanning multiple targets that resolve to a single IP address. Instead, Tenable Nessus scanners serialize attempts to scan the IP address, whether it appears more than once in the same scan task or in multiple scan tasks on that scanner. Scans may take longer to complete. When enabled, a Tenable Nessus scanner can simultaneously scan multiple targets that resolve to a single IP address within a single scan task or across multiple scan tasks. Scans complete more quickly, but hosts could potentially become overwhelmed, causing timeouts and incomplete results.
Create unique identifier on hosts	When enabled, the scanner creates a unique identifier (Tenable UUID). Tenable Vulnerability Management and Tenable Security Center use the

Option	Description
scanned using credentials	Tenable UUID to merge incoming scan data with historical results for the asset and ensure that license counts are accurately reflected. For more information, see [Why Tenable Tags and Agent IDs are created during authenticated scans]().
Performance Options	
Slow down the scan when network congestion is detected	When Tenable 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).
Network timeout (in seconds)	Determines the amount of time, in seconds, to determine if there is an issue communicating over the network.
Max simultaneous checks per host	This setting limits the maximum number of checks a Tenable Nessus scanner performs against a single host at one time. The default value of this option is 5 simultaneous checks per host. Type an integer greater than 0. If you enter **0**, enter a negative integer, or delete the value in the field, Tenable Security Center does not perform any checks and scans will not complete.
Max simultaneous hosts per scan	This setting limits the maximum number of hosts that a single Tenable Nessus scanner scans at the same time. The default value of this option is *30* hosts per scan. If the scan is using a zone with multiple scanners, each scanner will accept up to the amount specified in the **Max simultaneous hosts per scan** option. For example, if the **Max simultaneous hosts per scan** is set to 5 and there are 5 scanners per zone, each scanner will accept 5 hosts to scan, allowing a total of 25 hosts to be scanned between the 5 scanners. If you set **Max Simultaneous hosts per scan** to more than the Nessus

Option	Description
	scanner's **max_hosts** value, the following message appears in the scanner's `nessusd.messages`: *Tried to raise the maximum hosts number - 150. Using 100. Change 'max_hosts' in the server configuration if you believe this is incorrect.* You can ignore this message; Tenable Security Center send scans to the scanner into scan chunks of up to eight IPs and will not reach the scanner's **max_hosts**, which must be nine or greater.
Max number of concurrent TCP sessions per host	Specifies the maximum number of established TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner sends, which is 10 times the number of TCP sessions. For example, if this option is set to 15, the SYN scanner sends 150 packets per second at most. Type an integer between 1-2000. If you leave the box empty or enter **0**, Tenable Security Center does not enforce a limit.
Max number of concurrent TCP sessions per scan	This setting limits the maximum number of TCP sessions established by any of the active scanners during a scan. Type an integer between 1-2000. If you leave the box empty or enter **0**, Tenable Security Center does not enforce a limit.
Unix find command Options	
Command Timeout	The maximum number of seconds the find command is allowed to run on Unix systems. Not all **Find** commands use this timeout. Default value is 240. **Note:** For all **Find** command executions in the plugin to complete, and to prevent the plugin from timing out, its plugin timeout should be adjusted with `timeout_<plugin ID>` in the scanner's **Advanced Settings**,
Exclude Filepath	A plain text file containing a list of filepaths to exclude from all plugins that search using the `find` command on Unix systems.

Option	Description
	In the file, enter one filepath per line, formatted per patterns allowed by the Unix `find` command `-path` argument. For more information, see the `find` command [man page]().
Exclude Filesystem	A plain text file containing a list of filesystems to exclude from all plugins that search using the `find` command on Unix systems.
	In the file, enter one filesystem per line, using filesystem types supported by the Unix `find` command `-fstype` argument. For more information, see the `find` command [man page]().
Include Filepath	A plain text file containing a list of filepaths to include from all plugins that search using the `find` command on Unix systems.
	In the file, enter one filepath per line, formatted per patterns allowed by the Unix `find` command `-path` argument. For more information, see the `find` command [man page]().
	Including filepaths increases the locations that are searched by plugins, which extends the duration of the scan. Make your inclusions as specific as possible.
	Tip: Avoid having the same filepaths in **Include Filepath** and **Exclude Filepath**. This conflict may result in the filepath being excluded from the search, though results may vary by operating system.
Agent Performance Options	
Use Tenable supplied binaries for 'find' and 'unzip'	When enabled, instead of running native operating system commands of `find` and `unzip`, plugins use binaries included within the plugin feed for agent-based scanning. This allows CPU consumption to be controlled for the Tenable Agent `find` command. Another benefit to enabling this setting is that if `find` or `unzip` are not found natively on the operating system, using the commands from the feed allows full plugin execution with these commands to continue.
	This setting works in tandem with the [Scan Performance]() setting, which

Option	Description
	you can set locally on the agent. If you enable this setting and have adjusted the **Scan Performance** to a setting other than the default (**High**), the resulting scan findings may be different than previous scans with the same configuration. This is because the scan may experience timeouts in finding files due to the lower CPU resources. **Note:** Due to the need for thorough and complete results, audits do not leverage the `find` or `unzip` binaries from the Tenable feed. **Note:** With this setting enabled, CPU usage may spike up or close to 100% when the plugin requests a batch of results to process. The CPU then drops down to a lower level until the next batch is requested for processing.
Windows file search Options	
Windows Exclude Filepath	A plain text file containing a list of filepaths to exclude from all plugins that search using Tenable's unmanaged software directory scans. In the file, enter one absolute or partial filepath per line, formatted as the literal strings you want to exclude. You can include absolute or relative directory names, examples such as `E:\`, `E:\Testdir\`, and `\Testdir\`. **Tip:** The default exclusion paths include `\Windows\WinSxS\` and `\Windows\servicing\` if you do not configure this setting. If you configure this setting, Tenable recommends adding those two paths to the file; those directories are very slow and do not contain unmanaged software.
Windows Include Filepath	A plain text file containing a list of filepaths to include in all plugins that search using Tenable's unmanaged software directory scans. In the file, enter one absolute or partial filepath per line, formatted as the literal strings you want to exclude. You can only include absolute directory names, examples such as `E:\`, `E:\Testdir\`, and `C:\`. **Caution:** Avoid having the same filepaths in the **Windows Include Filepath**

Option	Description
	and **Windows Exclude Filepath** settings. This conflict results in the filepath being excluded from the search.
Compliance Output Settings	
Maximum Compliance Output Length in KB	Controls the maximum output length in kilobytes for each individual compliance check value that the target returns. If a compliance check value that is greater than this setting's value, Tenable Security Center truncates the result. The default value is 128000.
Maximum Compliance Check Timeout in Seconds	Controls the maximum timeout duration for compliance checks. This setting is used by checks with long run times, especially checks that run commands on remote targets for Windows and Unix audits. This timeout setting overrides all other timeout settings when it is available. The default value is 300 seconds.
Generate Gold Image Audit	Attaches a compliance gold image .audit established by generated compliance scan results. For more information, see Compliance Export Gold Image.
Generate XCCDF Result File	Attaches XCCDF result files generated from compliance .audit scans. For more information, see Compliance Export XCCDF Results.
Generate JSON Result File	Attaches .audit JSON result files. For more information, see Compliance Export JSON Results. **Note:** You cannot download the JSON file directly from Tenable Security Center.
Debug Settings	

Note: Tenable does not recommend enabling debug settings in production environments. Debug settings generate a substantial amount of data, and can alter the overall scan time and performance. Tenable only recommends the settings for specific debugging instances, and not for constant use.

Option	Description
Always Report SSH Commands	When enabled, Tenable Security Center generates a report of all the commands run over SSH on the host in a machine-readable format. You can view the reported commands under plugin 168017. **Note:** The setting does not function correctly if you disable plugin 168017.
Enumerate Launched Plugins	Shows a list of plugins that were launched during the scan. You can view the list in scan results under plugin 112154.
Stagger scan start	
Maximum delay (minutes)	(Agents 8.2 and later) If set, each agent in the agent group delays starting the scan for a random number of minutes, up to the specified maximum. Staggered starts can reduce the impact of agents that use a shared resource, such as virtual machine CPU. If the maximum delay you set exceeds your scan window, Tenable shortens your maximum delay to ensure that agents begin scanning at least 30 minutes before the scan window closes.
Agent Performance	
Use Tenable supplied binaries for 'find' and 'unzip'	When enabled, Tenable agent utilities will perform find and unzip functions.

Host Discovery Options

Option	Description
Ping the remote host	When enabled, Tenable Nessus attempts to ping the hosts in the scan to determine if the host is alive or not.
General Settings (available when **Ping the remote host** is enabled)	
Test the local Tenable Nessus host	This option allows you to include or exclude the local Tenable Nessus host from the scan. This is used when the Tenable Nessus host falls within the target network range for the scan.

Option	Description
Use fast network discovery	When Tenable Nessus pings a remote IP address 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 **Use fast network discovery** is enabled, Tenable Nessus does not perform these checks.
Ping Methods (available when **Ping the remote host** is enabled)	
ARP	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.
TCP	Ping a host using TCP.
Destination ports	Destination ports can be configured to use specific ports for TCP ping. This option specifies the list of ports that are checked via TCP ping. Type one of the following: • a single port • a comma-separated list of ports • `built-in` For more information about which ports `built-in` specifies, see the [knowledge base](#) article.
ICMP	Ping a host using the Internet Control Message Protocol (ICMP).
Assume ICMP unreachable means the host is down	When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When enabled, this option considers this to mean the host is dead. This is to help speed up discovery on some networks. 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 leads to the scan considering the host is down when it is indeed up.

Option	Description
Maximum number of retries	(If you enabled **ICMP**) Allows you to specify the number of attempts to try to ping the remote host. The default is two attempts.
UDP	Ping a host using the User Datagram Protocol (UDP). **Tip:** 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	
Scan Network Printers	Instructs the Tenable Nessus scanner not to scan network printers if unselected. Since many printers are prone to denial of service conditions, Tenable Nessus can skip scanning them once identified. This is recommended if scanning is performed on production networks.
Scan Novell Netware hosts	Instructs the Tenable Nessus scanner not to scan Novel Netware hosts if unselected. Since many Novell Netware hosts are prone to denial of service conditions, Tenable Nessus can skip scanning them once identified. This is recommended if scanning is performed on production networks.
Scan Operational Technology devices	When enabled, Tenable Security Center performs a full scan of Operational Technology (OT) devices such as programmable logic controllers (PLCs) and remote terminal units (RTUs) that monitor environmental factors and the activity and state of machinery. When disabled, Tenable Security Center uses ICS/SCADA Smart Scanning to identify OT devices cautiously and stops scanning them once they are discovered.
Wake-on-LAN	
List of MAC addresses	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.

Option	Description
Boot time wait (in minutes)	The number of minutes Tenable Nessus will wait to attempt a scan of hosts sent a WOL packet.

Port Scanning Options

Option	Description
Ports	
Consider unscanned ports as closed	If a port is not scanned with a selected port scanner (for example, out of the range specified), the scanner will consider it closed.
Port scan range	Specifies the range of ports to be scanned. The supported ranges are: • `default` — Instructs the scanner to scan approximately 4,790 commonly used ports specified in the `nessus-services` file. You can also combine the `default` keyword with other ports and port ranges. **Note:** You can convert the `nessus-services` file to a custom list of ports by performing four consecutive regular expression (regex) replace-all operations in a text editor that supports such operations: • `.*\s+(\d+)\/(tcp|udp)(\r\n|\r|\n)` to `$1\/$2`, • `(\d+)\/(tcp|udp)` to `$2:$1` • `tcp` to `T` • `udp` to `U` You can find the `nessus-services` file in the following directories, depending on your operating system: • Linux — /opt/nessus/var/nessus/nessus-services • Windows —

Option	Description
	C:\ProgramData\Tenable\Nessus\nessus\nessus-services • macOS — /Library/Nessus/run/var/nessus/nessus-services • `all` — Instructs the scanner to scan all 65,536 ports, excluding port 0. You cannot combine the `all` keyword with other ranges. • A comma-separated list of ports (for example, **21,23,25,80,110**), port ranges (for example, **1-1024,9000-9200** or **1-65535** to scan all ports but 0 and **T:1-1024,U:300-500** or **1-1024,T:1024-65535,U:1025** to scan separate or overlapping TCP and UDP port ranges), or combinations thereof. If you disable the UDP, SYN, or TCP port scanner settings in the scan policy **Discovery** settings, those ports are not scanned despite what range of ports you specify. The UDP and TCP port scanner settings are disabled by default; the SYN port scanner setting is enabled by default.
Local Port Enumerators	
SSH (netstat)	When enabled, the scanner uses netstat to check for open ports from the local machine. It relies on the netstat command being available via an SSH connection to the target. This scan is intended for Linux-based systems and requires authentication credentials. To use this setting, you must first configure SSH Credentials.
WMI (netstat)	When enabled, the scanner uses netstat to determine open ports while performing a WMI-based scan. In addition, the scanner: • Ignores any custom range specified in the **Port Scan Range** setting. • Continues to treat unscanned ports as closed if the **Consider unscanned ports as closed** setting is enabled. If any port enumerator (netstat or SNMP) is successful, the port range becomes *all*. To use this setting, you must first configure Windows

Option	Description
	Credentials.
SNMP	When enabled, if the appropriate credentials are provided by the user, the scanner can 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	When this setting is enabled, the scanner relies on local port enumeration before relying on network port scans. If a local port enumerator runs, all network port scanners are disabled for the asset. When this setting is disabled, the scanner performs network port scans regardless of the local port enumeration status.
Verify open TCP ports found by local port enumerators	When enabled, if a local port enumerator (for example, WMI or netstat) finds a port, the scanner also verifies that the port is open remotely. This approach helps determine if some form of access control is being used (for example, TCP wrappers or a firewall).
Network Port Scanners	
TCP	Use the built-in Tenable Nessus TCP scanner to identify open TCP ports on the targets, using a full TCP three-way handshake. If you enable this option, you can also set the **Override Automatic Firewall Detection** option. **Note:** On some platforms (for example, Windows and macOS), if the operating system is causing serious performance issues using the TCP scanner, Tenable Nessus launches the SYN scanner instead.
SYN	Use the built-in Tenable Nessus SYN scanner to identify open TCP ports on the target hosts. SYN scans do not initiate a full TCP three-way handshake. The scanner sends a SYN packet to the port, waits for SYN-ACK reply, and determines the port state based on a response or lack of response. If you enable this option, you can also set the **Override Automatic Firewall**

Option	Description
	Detection option.
Override automatic firewall detection	Rely on local port enumeration first before relying on network port scans.
UDP	This option engages the built-in Tenable Nessus UDP scanner to identify open UDP ports on the targets. Due to the nature of the protocol, it is generally not possible for a port scanner to tell the difference between open and filtered UDP ports. Enabling the UDP port scanner may dramatically increase the scan time and produce unreliable results. Consider using the netstat or SNMP port enumeration options instead if possible.

Service Discovery Options

The **Service Discovery** tab specifies how the scanner looks for services running on the target's ports.

Option	Description
Probe all ports to find services	When enabled, the scanner attempts to map each open port with the service that is running on that port, as defined by the **Port scan range** option. **Caution:** In some rare cases, probing might disrupt some services and cause unforeseen side effects.
Search for SSL/TLS services	Controls how the scanner tests SSL-based services. **Caution:** Testing for SSL capability on all ports may be disruptive for the tested host.
Search for	Specifies which ports on target hosts the scanner searches for SSL/TLS

Option	Description

SSL/TLS on	services.
	
	This setting has two options:
	
	    • **Known SSL/TLS ports**
	
	    • **All ports**

Search for DTLS on	Specifies which ports on target hosts the scanner searches for DTLS services.
	
	This setting has the following options:
	
	    • **None**
	
	    • **Known DTLS ports**
	
	    • **All ports**

Identify certificates expiring within x days	Identifies SSL certificates that age out within the specified timeframe. Type a value to set a timeframe (in days).
Enumerate all SSL/TLS ciphers	When Tenable Security Center 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 Tenable Nessus to check SSL certificates against known Certificate Revocation Lists (CRL). Enabling this option makes a connection and query one or more servers on the internet.

Assessment Options

The **Assessment** tab specifies how the scanner tests for information during the scan.

Value	Description
Accuracy	
Override normal accuracy	In some cases, Tenable Nessus cannot remotely determine whether a flaw is present or not. If report paranoia is set to **Paranoid** then a flaw is 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 Tenable Nessus to not report any flaw whenever there is a hint of uncertainty about the remote host. **Normal** is a middle ground between these two settings.
Perform thorough tests (may disrupt your network or impact scan speed)	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.
Antivirus	
Antivirus definition grace period (in days)	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.
SMTP	
Third party domain	Tenable Nessus attempts to send spam through each SMTP device to the address listed in this option. 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.
From address	The test messages sent to the SMTP server(s) will appear as if they originated from the address specified in this option.
To Address	Tenable Nessus attempts to send messages addressed to the mail recipient listed in this option. The postmaster address is the default value since it is a valid address on most mail servers.

Brute Force Options

The **Brute Force** tab specifies options for brute force login testing.

Additionally, if Hydra is installed on the same host as a Tenable Nessus server linked to Tenable Security Center, the Hydra section is enabled. Hydra extends brute force login testing for the following services: Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, S7-300, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP.

Option	Description
General Settings	
Only use credentials provided by the user	In some cases, Tenable 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 Tenable Nessus from performing these tests.
Oracle Database	
Test default Oracle accounts (slow)	Test for known default accounts in Oracle software.
Hydra	
Always enable Hydra (slow)	Enables Hydra whenever the scan is performed.
Logins file	A file that contains user names that Hydra will use during the scan.
Passwords file	A file that contains passwords for user accounts that Hydra will use during the scan.

Option	Description
Number of parallel tasks	The number of simultaneous Hydra tests that you want to execute. By default, this value is *16*.
Timeout (in seconds)	The number of seconds per login attempt.
Try empty passwords	If enabled, Hydra will additionally try user names without using a password.
Try login as password	If enabled, Hydra will additionally try a user name as the corresponding password.
Stop brute forcing after the first success	If enabled, Hydra will stop brute forcing user accounts after the first time an account is successfully accessed.
Add accounts found by other plugins to the login file	If disabled, only the user names specified in the logins file will be used for the scan. Otherwise, additional user names discovered by other plugins will be added to the logins file and used for the scan.
PostgreSQL database name	The database that you want Hydra to test.
SAP R3 Client ID (0 – 99)	The ID of the SAP R3 client that you want Hydra to test.
Windows accounts to test	Can be set to **Local accounts**, **Domain Accounts**, or **Either**.
Interpret passwords as NTLM hashes	If enabled, Hydra will interpret passwords as NTLM hashes.
Cisco login	This password is used to login to a Cisco system before brute forcing enable

Option	Description
password	passwords. If no password is provided here, Hydra will attempt to login using credentials that were successfully brute forced earlier in the scan.
Web page to brute force	Type a web page that is protected by HTTP basic or digest authentication. If a web page is not provided here, Hydra will attempt to brute force a page discovered by the Tenable Nessus web crawler that requires HTTP authentication.
HTTP proxy test website	If Hydra successfully brute forces an HTTP proxy, it will attempt to access the website provided here via the brute forced proxy.
LDAP DN	The LDAP Distinguish Name scope that Hydra will authenticate against.

Malware Options

The **Malware** tab specifies options for DNS Resolution, hash, and allowlist files and file system scanning.

Option	Description
Malware Scan Settings	
Malware scan	When enabled, displays the **General Settings**, **Hash and Allowlist Files**, and **File System Scanning** sections.
Hash and Allowlist Files (available when **Malware scan** is enabled)	
Provide your own list of known bad MD5/SHA1/SHA256 hashes	Additional known bad MD5 hashes can be uploaded via a text file that contains one MD5 hash per line. If you want to add a description for each hash, type 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.
Provide your own list of known good MD5/SHA1/SHA256	Additional known good MD5 hashes can be uploaded via a text file that contains one MD5 hash per line.

hashes	If you want to add a description for each hash, type 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.
Hosts file allowlist	Tenable Nessus checks system hosts files for signs of a compromise (e.g., Plugin ID 23910). This option allows you to upload a file containing a list of IPs and hostnames that will be ignored by Tenable Nessus during a scan. Include one IP address and hostname (formatted identically to your hosts file on the target) per line in a regular text file.
File System Scanning (available when **Malware scan** is enabled)	
Scan file system	Turning on this option allows you to scan system directories and files on host computers. **Caution:** Enabling this setting in scans targeting 10 or more hosts could result in performance degradation.
Directories (available when **File System Scanning** is enabled)	
Scan %Systemroot%	Enable file system scanning to scan %Systemroot%.
Scan %ProgramFiles%	Enable file system scanning to scan %ProgramFiles%.
Scan %ProgramFiles (x86)%	Enable file system scanning to scan %ProgramFiles(x86)%.
Scan %ProgramData%	Enable file system scanning to scan %ProgramData%.
Scan User Profiles	Enable file system scanning to scan user profiles.
Custom Filescan Directories	A custom file that lists directories for malware file scanning. List each directory on one line. **Caution:** Root directories such as C:\ or D:\ are not accepted.
Yara Rules Files	A `.yar` file containing the YARA rules to be applied in the scan. You

can only upload one file per scan, so include all rules in a single file. For more information, see yara.readthedocs.io.

SCADA Options

The **SCADA** tab specifies how the scanner tests for information against SCADA systems.

Option	Description
Modbus/TCP Coil Access	
Start at register **End at register**	These options are available for commercial users. This drop-down box item is dynamically generated by the SCADA plugins available with the commercial version of Tenable Nessus. Modbus uses a function code of 1 to read coils in a Modbus slave. Coils represent binary output settings and are typically mapped to actuators. The ability to read coils may help an attacker profile a system and identify ranges of registers to alter via a write coil message. The defaults for this are *0* for the **Start at register** value and *16* for the **End at register** value.
ICCP/COTP TSAP Addressing Weakness	
Start COTP TSAP **Stop COTP TSAP**	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.

Web Applications Options

The **Web Applications** tab specifies how the scanner tests for information against web server applications.

Value	Description
Web Application Settings	
Scan web applications	When enabled, displays the **General Settings**, **Web Crawler**, and **Application Test Settings** sections.

Value	Description
Use a custom User-Agent	Specifies which type of web browser Tenable Nessus will impersonate while scanning.
Web Crawler (available when **Scan web applications** is enabled)	
Start crawling from	The URL of the first page that will be tested. If multiple pages are required, use a colon delimiter to separate them (e.g., */:/php4:/base)*.
Excluded pages (regex)	Enable exclusion of portions of the web site from being crawled. For example, to exclude the /manual directory and all Perl CGI, set this option to: *(^/manual)|(\.pl(\?.*)?$)*. Tenable Nessus supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).
Maximum pages to crawl	The maximum number of pages to crawl.
Maximum depth to crawl	Limit the number of links Tenable Nessus will follow for each start page.
Follow dynamically generated pages	When enabled, Tenable Nessus will follow dynamic links and may exceed the parameters set above.
Application Test Settings (available when **Scan web applications** is enabled)	
Enable generic web application tests	Enables the **Application Test Settings** options.
Abort web application tests if HTTP login fails	If Tenable Nessus cannot login to the target via HTTP, then do not run any web application tests.
Try all HTTP	This option will instruct Tenable Nessus to also use POST requests for

Value	Description
Methods	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, Tenable 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.
Attempt HTTP Parameter Pollution	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 `/target.cgi?a='&b=2`. With HTTP Parameter Pollution (HPP) enabled, the request may look like `/target.cgi?a='&a=1&b=2`.
Test embedded web servers	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.
Test more than one parameter at a time per form	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 non-attack variations for additional parameters. For example, Tenable Nessus attempts `/test.php?arg1=XSS&`*b*`=1&`*c*`=1` where *b* and *c* allows other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. This drop-down box has five selections: **One value** — This tests one parameter at a time with an attack string, without trying non-attack variations for additional parameters. For example, Tenable Nessus attempts `/test.php?arg1=XSS&`*b*`=1&`*c*`=1` where *b* and *c* allows other values, without testing each combination.

Value	Description
	This is the quickest method of testing with the smallest result set generated. • **Some pairs** — This form of testing will randomly check a combination of random pairs of parameters. This is the fastest way to test multiple parameters. • **All pairs** (slower but efficient) — This form of testing is slightly slower but more efficient than the one value test. While testing multiple parameters, it will test an attack string, variations for a single variable and then use the first value for all other variables. For example, Tenable Nessus attempts `/test.php?arg1=XSS&`*b*`=1&`*c*`=1` and then cycles 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, Tenable Nessus will never test for `/test.php?a=XSS&b=3&c=3&d=3` when the first value of each variable is *1*. • **Some combinations** — This form of testing will randomly check a combination of 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** (extremely slow) — This method of testing will do a fully exhaustive test of all possible combinations of attack strings with valid input to variables. Where All-pairs testing seeks to create a smaller data set as a tradeoff for speed, all combinations makes no compromise on time and uses a complete data set of tests. This testing method may take a long time to complete.
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

Value	Description
	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 CGI** — As soon as a flaw is found on a CGI by a script, Tenable Nessus switches to the next known CGI on the same server, or if there is no other CGI, to the next port/server. This is the default option. • **Per port** (faster) — As soon as a flaw is found on a web server by a script, Tenable 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), Tenable 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** (slower) — 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, Tenable 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.

Windows Options

The **Windows** tab specifies basic Windows SMB domain options.

Option	Description
General Settings	
Request information about the SMB Domain	When enabled, Tenable Nessus queries domain users instead of local users.
User Enumeration Methods	
SAM Registry	When enabled, Tenable Nessus enumerates users via the Security Account Manager (SAM) registry.
ADSI Query	When enabled, Tenable Nessus enumerates users via Active Directory Service Interfaces (ADSI). To use ADSI, you must also configure [ADSI authentication](#) options.
WMI Query	When enabled, Tenable Nessus enumerates users via Windows Management Interface (WMI).
RID Brute Forcing	When enabled, Tenable Nessus enumerates users via relative identifier (RID) brute forcing. Enabling this setting enables the **Enumerate Domain User** and **Enumerate Local User** options.
Enumerate Domain Users (available when **RID Brute Forcing** is enabled)	
Start UID	*1000*
End UID	*1200*
Enumerate Local Users (available when **RID Brute Forcing** is enabled)	
Start UID	*1000*
End UID	*1200*

Report Options

The **Report** tab specifies information to include in the scan's report.

Option	Description
Processing	
Override normal verbosity	Determines the verbosity of the detail in the output of the scan results: • **Normal** — Provides the standard level of plugin activity in the report. • **Quiet** — Provides less information about plugin activity in the report to minimize impact on disk space. • **Verbose** — Provides more information about plugin activity in the report. When this option is selected, the output includes the informational plugins 56310, 64582, and 58651.
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.
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.
Display Unicode characters	When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information.

Option	Description
	Note: Plugin output may sometimes incorrectly parse or truncate strings with Unicode characters. If this issue causes problems with regular expressions in plugins or custom audits, disable this setting and scan again.
Generate SCAP XML Results	Generate a SCAP XML results file as a part of the report output for the scan.

Authentication Options

The **Authentication** tab specifies authentication options during a scan.

Option	Description
Authentication	
Type	Specifies the type of authentication you want scanners to use for credentialed access to scan targets. Credentialed access gathers more complete data about a target. • Host • Database Credentials • Miscellaneous • Plaintext Authentication • Patch Management
SNMP	
UDP Port **Additional UDP port #1** **Additional UDP port #2** **Additional UDP**	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*.

Option	Description
port #3	
SSH	
known_hosts file	If an SSH known_hosts file is provided for the scan policy, Tenable Nessus will only attempt to log in to 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.
Preferred port	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.
Client version	Specifies which type of SSH client to impersonate while performing scans.
Attempt least privilege (experimental)	Enables or disables dynamic privilege escalation. When enabled, if the scan target credentials include privilege escalation, Tenable Nessus first attempts to run commands without privilege escalation. If running commands without privilege escalation fails, Tenable Nessus retries the commands with privilege escalation. Plugins 102095 and 102094 report whether plugins ran with or without privilege escalation. **Note:** Enabling this option may increase the time required to perform scans by up to 30%.
Windows	
Never send credentials in the clear	By default, Windows credentials are not sent to the target host in the clear.
Do not use NTLMv1 authentication	When disabled, it is theoretically possible to trick Tenable Nessus into attempting to log in to a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the

Option	Description
	ability to use a hash obtained from Tenable Nessus. This hash can be potentially cracked to reveal a username or password. It may also be used to directly log in to other servers. Because NTLMv1 is an insecure protocol, this option is enabled by default.
Start the Remote Registry service during the scan	This option tells Tenable Nessus to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Tenable Nessus to execute some Windows local check plugins.
Enable administrative shares during the scan	This option will allow Tenable Nessus to access certain registry entries that can be read with administrator privileges.
Start the Server service during the scan	When enabled, the scanner temporarily enables the Windows Server service, which allows the computer to share files and other devices on a network. The service is disabled after the scan completes. By default, Windows systems have the Windows Server service enabled, which means you do not need to enable this setting. However, if you disable the Windows Server service in your environment, and want to scan using SMB credentials, you must enable this setting so that the scanner can access files remotely.
Plaintext Authentication	
Perform patch audits over telnet	When enabled, Tenable Security Center uses telnet to connect to the host device for patch audits. **Note:** This protocol is sent in cleartext and could contain unencrypted usernames and passwords.
Perform patch audits over rsh	When enabled, Tenable Security Center permits patch audits over a rsh connection.

Option	Description
	Note: This protocol is sent in cleartext and could contain unencrypted usernames and passwords.
Perform patch audits over rexec	When enabled, Tenable Security Center permits patch audits over a rexec connection. **Note:** This protocol is sent in cleartext and could contain unencrypted usernames and passwords.
HTTP	
Login method	Specify whether the login action is performed via a GET or POST request.
Re-authenticate delay (seconds)	The delay between authentication attempts, in seconds. **Tip:** A time delay can help prevent triggering brute force lockout mechanisms.
Follow 30x redirections (# of levels)	If a 30x redirect code is received from a web server, this directs Tenable Nessus to follow the link provided or not.
Invert authenticated regex	The regex pattern you want Tenable Security Center to look for on the login page that, if found, denies authentication. **Tip:** Tenable Security Center can attempt to match a given string, such as `Authentication failed`.
Use authenticated regex on HTTP headers	When enabled, Tenable Security Center searches the HTTP response headers for a given regex pattern instead of searching the body of a response to better determine authentication state.
Case insensitive authenticated regex	When enabled, Tenable Security Center ignores case in regex.

Compliance Options

The **Compliance** tab specifies compliance the audit files to reference in a scan policy. The options available depend on the type of audit file selected.

For more information, see [Audit Files](#) and [Configure Compliance Options](#).

Option	Description
Generic SSH Escalation command	(Generic SSH audits only) The command to use for accomplishing the privilege escalation. This is similar to the enable command for Cisco devices.
Generic SSH Escalation success check	(Generic SSH audits only) A regular expression that must match after the escalation has succeeded. This can be the prompt or any other message notifying the success of privilege escalation.

Plugins Options

The **Plugins** tab specifies which plugins are used during the policy's Tenable Nessus scan. You can enable or disable plugins in the plugin family view or in the plugin view for more granular control.

For more information, see [Configure Plugin Options](#).

> **Caution:** The Denial of Service plugin family contains plugins that could cause outages on network hosts if the **Safe Checks** option is not enabled, but it also contains useful checks that do not cause any harm. The Denial of Service plugin family can be used in conjunction with **Safe Checks** to ensure that any potentially dangerous plugins are not run. However, Tenable does not recommend enabling the Denial of Service plugin family in production environments.

Configure Compliance Options

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see [User Roles](#).

You can configure compliance options within a scan policy to reference one or more audit files in a template-based **Policy Compliance Auditing** scan policy or a custom scan policy.

For more information, see [Audit Files](#), [Scan Policies](#), and [Scan Policy Options](#).

> **Note:** The maximum number of audit files you can include in a single **Policy Compliance Auditing** scan is limited by the total runtime and memory that the audit files require. Exceeding this limit may lead to

> incomplete or failed scan results. To limit the possible impact, Tenable recommends that audit selection in your scan policies be targeted and specific for the scan's scope and compliance requirements.

To configure compliance options for a scan policy:

1. Begin configuring a scan policy, as described in Add a Scan Policy.

2. In the left navigation bar, click **Compliance**.

   The **Compliance** options appear.

3. Click **+ Add Audit File**.

   The **Select a Type** drop-down box appears.

4. In the **Select a Type** drop-down box, select the type of audit file you want to reference in the scan policy.

   The **Select an Audit File** drop-down box appears.

5. In the **Select an Audit File** drop-down box, select the name of the audit file you want to reference in the scan policy.

6. Click the ✔ button.

   Tenable Security Center applies the audit file to the scan policy.

7. If required, configure additional options for the audit file you applied to the scan policy. For more information, see The Compliance tab specifies compliance the audit files to reference in a scan policy. The options available depend on the type of audit file selected..

Configure Plugin Options

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can configure plugin options within a scan policy to enable or disable plugins at the plugin family level or individual plugin level.

> **Note:** When Tenable adds new plugins to Tenable Security Center, Tenable Security Center automatically enables the new plugins if the entire plugin family they belong to is enabled in your scan policy template.

To configure plugin options at the plugin family level:

1. Begin configuring a scan, policy as described in [Add a Scan Policy](#).

2. In the left navigation bar, click **Plugins**.

   The **Plugins** page appears with the plugin family view displayed.

3. In the **Status** column, view the plugin family status and the number of enabled plugins within the plugin family:

   - **Enabled** — All plugins in the family are enabled. The scan targets the parameters in the plugins.

   - **Disabled** — All plugins in the family are disabled. The scan does not target the parameters in the plugins.

   - **Mixed** — The plugin family contains a combination of **Enabled** and **Disabled** plugins. Mixed plugin families have a padlock icon that is locked or unlocked:

     - **Locked** - New plugins added to the plugin family via plugin feed updates will be *disabled* automatically in the policy.

     - **Unlocked** - New plugins added to the plugin family via plugin feed updates will be *enabled* automatically in the policy.

4. In the **Total** column, view the number of plugins in the family.

5. To enable or disable all plugins in the family, select the **Enabled** or **Disabled** slider in the **Status** column.

6. To filter the plugin families listed on the page, use the **Select a Filter** drop-down box to build and apply a filter.

   The **Total** column becomes the **Matched** column and indicates the number of plugins in the family that match the current filter.

7. To view only enabled or disabled plugin families, click the **Enabled** or **Disabled** tab above the table.

8. To sort the plugin families listed on the page, click the **Status**, **Plugin Family**, or **Total** column title.

9. To lock or unlock all mixed plugin families displayed on the page, click **Lock All Mixed** or **Unlock All Mixed**.

10. To enable or disable all of the plugin families displayed on the page, click **Enable Shown** or **Disable Shown**.

    Tenable Security Center enables or disables all plugins within the plugin families shown on the page, not just the number of plugins in the **Total** or **Matched** column. For more granular control, set plugin statuses in the plugin view.

11. To enable or disable individual plugins within a family, click the plugin family name to access the plugin view.

    The plugin view appears.

To configure plugin options at the individual plugin level:

1. Begin configuring a scan policy as described in [Add a Scan Policy](#).

2. Click **Plugins** in the left navigation bar.

    The **Plugins** page appears.

3. Click the plugin family name.

    The plugin view appears.

4. In the **Status** column, view the plugin status:

    - **Enabled** — The plugin is enabled. The scan targets the parameters in the plugins.

    - **Disabled** — The plugin is disabled. The scan does not target the parameters in the plugins.

5. In the **Plugin ID** column, click the information icon to display the plugin details.

6. To enable or disable a plugin, click the **Status** box.

7. To filter the plugins listed on the page, use the **Select a Filter** drop-down box to build and apply a filter.

8. To view only enabled or disabled plugins, click the **Enabled** or **Disabled** tab above the table.

9. To sort the plugins listed on the page, click the **Status**, **Plugin Name**, or **Plugin ID** column title.

10. To enable or disable all of the plugins displayed on the page, click **Enable Shown** or **Disable Shown**.

   Tenable Security Center enables or disables all plugins shown on the page.

11. To return to the plugin family view, click the **Back** option.

12. To view the plugins in a different family, click the drop-down box and select a different plugin family.

Host

Tenable Security Center can use SNMPv3 credentials to scan remote systems that use an encrypted network management protocol (including network devices). Tenable Security Center uses these credentials to scan for patch auditing or compliance checks.

You can configure SNMPv3 options in scan policies, as described in Authentication Options and Add a Scan Policy.

SNMPv3 Options

Option	Description	Default
Username	The username for the SNMPv3 account that Tenable Security Center uses to perform checks on the target system.	-
Port	(Required) The TCP port that SNMPv3 listens on for communications from Tenable Security Center.	161
Security level	The security level for SNMP: • **No authentication and no privacy** • **Authentication without privacy** • **Authentication and privacy**	Authentication and privacy
Authentication algorithm	The algorithm the remove service supports: **MD5** or **SHA1**.	SHA1
Authentication	The password associated with the **Username**.	-

Option	Description	Default
password		
Privacy algorithm	The encryption algorithm to use for SNMP traffic: **AES** or **DES**.	AES-192
Privacy password	A password used to protect encrypted SNMP communication.	–

Miscellaneous

Tenable Security Center supports the following additional authentication methods:

- ADSI

- F5

- IBM iSeries

- Red Hat Enterprise Virtualization (RHEV)

- Netapp API

- Palo Alto Networks PAN-OS

- VMware ESX SOAP API

- VMware vCenter SOAP API

- X.509

You can configure these authentication methods in scan policies, as described in The Authentication tab specifies authentication options during a scan. and Add a Scan Policy.

ADSI

ADSI allows Tenable Security Center to query an ActiveSync server to determine if any Android or iOS-based devices are connected. Using the credentials and server information, Tenable Security Center authenticates to the domain controller (not the Exchange server) to directly query it for device information. These settings are required for mobile device scanning.

Tenable Security Center supports obtaining the mobile information from Exchange Server 2010 and 2013 only.

Option	Description	Default
Domain Controller	(Required) The name of the domain controller for ActiveSync.	-
Domain	(Required) The name of the NetBIOS domain for ActiveSync.	-
Domain Admin	(Required) The domain administrator's username.	-
Domain Password	(Required) The domain administrator's password.	-

F5

Option	Description	Default
Username	(Required) The username for the scanning F5 account that Tenable Security Center uses to perform checks on the target system.	-
Password	(Required) The password for the F5 user.	-
Port	(Required) The TCP port that F5 listens on for communications from Tenable Security Center.	443
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	enabled

IBM iSeries

Option	Description	Default
Username	(Required) The username for the IBM iSeries account that Tenable Security Center uses to perform checks on the target system.	-
Password	(Required) The password for the IBM iSeries user.	-

Red Hat Enterprise Virtualization (RHEV)

Option	Description	Default
Username	(Required) The username for RHEV account that Tenable Security Center uses to perform checks on the target system.	-
Password	(Required) The password for the RHEV user.	-
Port	(Required) The TCP port that the RHEV server listens on for communications from Tenable Security Center.	443
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	enabled

Netapp API

Option	Description	Default
Username	(Required) The username for the Netapp API account with HTTPS access that Tenable Security Center uses to perform checks on the target system.	-
Password	(Required) The password for the Netapp API user.	-
vFiler	The vFiler nodes to scan for on the target systems. To limit the audit to a single vFiler, type the name of the vFiler. To audit for all discovered Netapp virtual filers (vFilers) on	-

	target systems, leave the field blank.	
Port	(Required) The TCP port that Netapp API listens on for communications from Tenable Security Center.	443

Palo Alto Networks PAN-OS

Option	Description	Default
Username	(Required) The username for the PAN-OS account that Tenable Security Center uses to perform checks on the target system.	-
Password	(Required) The password for the PAN-OS user.	-
Port	(Required) The TCP port that PAN-OS listens on for communications from Tenable Security Center.	443
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	enabled

VMware ESX SOAP API

For more information about configuring VMWare ESX SOAP API, see [Configure vSphere Scanning](#).

Tenable can access VMware servers through the native VMware SOAP API.

Option	Description	Default
ESX SOAP API Authentication Method	(Required) The user can choose from a list of authentication methods: • Username and Password (manual entry) • PAM Integration (Use a specific PAM to gather vCenter API Authentication Credentials from the available list.)	Username and Password

Option	Description	Default
Do not verify SSL Certificate	Do not validate the SSL certificate for the ESXi server.	disabled

VMware vCenter SOAP API

For more information about configuring VMWare vCenter SOAP API, see Configure vSphere Scanning.

Tenable can access vCenter through the native VMware vCenter SOAP API. If available, Tenable uses the vCenter REST API to collect data in addition to the SOAP API.

> **Note:** Tenable supports VMware vCenter/ESXi versions 7.0.3 and later for authenticated scans. This does not impact vulnerability checks for VMware vCenter/ESXi, which do not require authentication.

> **Note:** The SOAP API requires a vCenter account with read permissions and settings privileges. The REST API requires a vCenter admin account with general read permissions and required Lifecycle Manager privileges to enumerate VIBs.

Option	Description	Default
vCenter Host	(Required) The name of the vCenter host.	–
vCenter Port	(Required) The TCP port that vCenter listens on for communications from Tenable.	443
Username	(Required) The username for the vCenter server account with admin read/write access that Tenable uses to perform checks on the target system.	–
Password	(Required) The password for the vCenver server user.	–
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA.	enabled

Option	Description	Default
	Tip: If you are using a self-signed certificate, disable this setting.	

X.509

Option	Description	Default
Client Certificate	(Required) The client certificate.	-
Client Key	(Required) The client private key.	-
Password	(Required) The passphrase for the client private key.	-
CA Certificate to Trust	(Required) The trusted Certificate Authority's (CA) digital certificate.	-

Plaintext Authentication

Caution: Tenable does not recommend plaintext credentials. Instead, use encrypted authentication methods when possible.

If a secure method of performing credentialed checks is not available, you can configure Tenable Security Center to perform checks over unsecure protocols using plaintext authentication settings.

Tenable Security Center supports the following plaintext authentication methods:

- [telnet/rsh/rexec](#)
- [NNTP](#)
- [FTP](#)
- [POP2](#)
- [POP3](#)
- [IMAP](#)
- [IPMI](#)
- [HTTP](#)

You can configure plaintext authentication options in scan policies, as described in [The Authentication tab specifies authentication options during a scan.](#) and [Add a Scan Policy](#).

telnet/rsh/rexec

Tenable Security Center performs patch auditing on non-Windows targets only.

Setting	Description	Default
Username	(Required) The username for the telnet, rsh, or rexec account that Tenable Security Center uses to perform checks on the target system.	-
Password (Unsafe!)	(Required) The password for the telnet, rsh, or rexec user.	-

NNTP

Setting	Description	Default
Username	(Required) The username for the NNTP account that Tenable Security Center uses to perform checks on the target system.	-
Password	(Required) The password for the NNTP user.	-

FTP

Setting	Description	Default
Username	(Required) The username for the FTP account that Tenable Security Center uses to perform checks on the target system.	-
Password	(Required) The password for the FTP user.	-

POP2

Setting	Description	Default
Username	(Required) The username for the POP2 account that Tenable	-

	Security Center uses to perform checks on the target system.	
Password	(Required) The password for the POP2 user.	-

POP3

Setting	Description	Default
Username	(Required) The username for the POP3 account that Tenable Security Center uses to perform checks on the target system.	-
Password	(Required) The password for the POP3 user.	-

IMAP

Setting	Description	Default
Username	(Required) The username for the IMAP account that Tenable Security Center uses to perform checks on the target system.	-
Password	(Required) The password for the IMAP user.	-

IPMI

Setting	Description	Default
Username	(Required) The username for the IMPI account that Tenable Security Center uses to perform checks on the target system.	-
Password (Sent in Clear)	(Required) The password for the IPMI user.	-

HTTP

Setting	Description	Default
Authentication Method	(Required) The authentication method. • **Automatic authentication**	HTTP Login Form

Setting	Description	Default
	• **Basic/Digest authentication** • **HTTP login form** — Controls the start location of authenticated testing of a custom web-based application. • **HTTP cookies import** — Tenable Security Center uses cookies imported from another piece of software (such as a web browser or web proxy) to facilitate web application testing by using when attempting to access a web application.	
Username	(Required) The username for the HTTP account that Tenable Security Center uses to perform checks on the target system.	–
Password	(Required) The password for the HTTP user.	–
Login page	(Required) The absolute path to the application login page. For example, `/login.html`.	–
Login submission page	(Required) The action parameter for the form method. For example, for `<form method="POST" name="auth_form" action="/login.php">`, use `/login.php`.	–
Login parameters	(Required) The authentication parameters (for example, `login=%USER%&password=%PASS%`). Tenable Security Center replaces the `%USER%` and `%PASS%` keywords with values supplied on the Login configurations drop-down menu. **Tip:** If needed, you can provide additional parameters, such as a group name or other information required for authentication.	–
Check	(Required) The absolute path of a protected web page	–

Setting	Description	Default
authentication on page	that requires authentication. For example, `/admin.html`.	
Regex to verify successful authentication	(Required) The regex pattern you want Tenable Security Center to look for on the login page to validate authentication. **Tip:** Tenable Security Center can attempt to match a given string, such as `Authentication successful`.	–
Cookies file	(Required) A cookie file in Netscape `cookies.txt` format.	–

Patch Management

Tenable Security Center can leverage credentials for patch management systems to perform patch auditing on systems for which credentials may not be available.

Tenable Security Center supports:

- Dell KACE K1000

- HCL BigFix

- Microsoft System Center Configuration Manager (SCCM)

- Microsoft Windows Server Update Services (WSUS)

- Red Hat Satellite Server

- Symantec Altiris

You can configure patch management options in scan policies, as described in Authentication Options and Add a Scan Policy.

IT administrators are expected to manage the patch monitoring software and install any agents required by the patch management system on their systems.

Note: If the credential check sees a system but it is unable to authenticate against the system, it uses the data obtained from the patch management system to perform the check. If Tenable Security Center is able

o connect to the target system, it performs checks on that system and ignores the patch management system output.

> **Note:** The data returned to Tenable Security Center by the patch management system is only as current as the most recent data that the patch management system has obtained from its managed hosts.

Scanning with Multiple Patch Managers

If you provide multiple sets of credentials to Tenable Security Center for patch management tools, Tenable Security Center uses all of them.

If you provide credentials for a host and for one or more patch management systems, Tenable Security Center compares the findings between all methods and report on conflicts or provide a satisfied finding. Use the Patch Management Windows Auditing Conflicts plugins to highlight patch data differences between the host and a patch management system.

Dell KACE K1000

KACE K1000 is available from Dell to manage the distribution of updates and hotfixes for Linux, Windows, and macOS systems. Tenable Security Center can query KACE K1000 to verify whether or not patches are installed on systems managed by KACE K1000 and display the patch information through the Tenable Security Center user interface.

Tenable Security Center supports KACE K1000 versions 6.x and earlier.

KACE K1000 scanning uses the following Tenable plugins: 76867, 76868, 76866, and 76869.

Option	Description	Default
Server	(Required) The KACE K1000 IP address or system name.	–
Database Port	(Required) The TCP port that KACE K1000 listens on for communications from Tenable Security Center.	3306
Organization Database Name	(Required) The name of the organization component for the KACE K1000 database (e.g., ORG1).	ORG1
Database Username	(Required) The username for the KACE K1000 account that Tenable Security Center uses to perform checks on the target system.	R1

Option	Description	Default
K1000 Database Password	(Required) The password for the KACE K1000 user.	-

HCL BigFix

HCL Bigfix is available to manage the distribution of updates and hotfixes for desktop systems.Tenable Security Center can query HCL Bigfix to verify whether or not patches are installed on systems managed by HCL Bigfix and display the patch information.

Package reporting is supported by RPM-based and Debian-based distributions that HCL Bigfix officially supports. This includes Red Hat derivatives such as RHEL, CentOS, Scientific Linux, and Oracle Linux, as well as Debian and Ubuntu. Other distributions may also work, but unless HCL Bigfix officially supports them, there is no support available.

For local check plugins to trigger, only RHEL, CentOS, Scientific Linux, Oracle Linux, Debian, Ubuntu, and Solaris are supported. Plugin 160250 must be enabled.

Tenable Security Center supports HCL Bigfix 9.5 and later and 10.x and later.

HCL Bigfix scanning uses the following Tenable plugins: 160247, 160248, 160249, 160250, and 160251.

Option	Description	Default
Web Reports Server	(Required) The name of HCL Bigfix Web Reports server.	-
Web Reports Port	(Required) The TCP port that the HCL Bigfix Web Reports server listens on for communications from Tenable Security Center.	-
Web Reports Username	(Required) The username for the HCL Bigfix Web Reports administrator account that Tenable Security Center uses to perform checks on the target system.	-
Web Reports Password	(Required) The password for the HCL Bigfix Web Reports administrator user.	-
HTTPS	When enabled, Tenable connects using secure communication	Enabled

Option	Description	Default
	(HTTPS). When disabled, Tenable connects using standard HTTP.	
Verify SSL certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	Enabled

HCL Bigfix Server Configuration

In order to use these auditing features, you must make changes to the HCL Bigfix server. You must import a custom analysis into HCL Bigfix so that detailed package information is retrieved and made available to Tenable Security Center.

From the HCL BigFix Console application, import the following `.bes` files.

BES file:

```
<?xml version="1.0" encoding="UTF-8"?>
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd">
    <Analysis>
        <Title>Tenable</Title>
        <Description>This analysis provides SecurityCenter with the data it needs for vulnerability reporting. <
        <Relevance>true</Relevance>
        <Source>Internal</Source>
        <SourceReleaseDate>2013-01-31</SourceReleaseDate>
        <MIMEField>
            <Name>x-fixlet-modification-time</Name>
            <Value>Thu, 13 May 2021 21:43:29 +0000</Value>
        </MIMEField>
        <Domain>BESC</Domain>
        <Property Name="Packages - With Versions (Tenable)" ID="74"><![CDATA[if (exists true whose (if true then
repository) else false)) then unique values of (lpp_name of it & "|" & version of it as string & "|" & "fileset"
architecture of operating system) of filesets of products of object repository else if (exists true whose (if tr
debianpackage) else false)) then unique values of (name of it & "|" & version of it as string & "|" & "deb" & "|
architecture of it & "|" & architecture of operating system) of packages whose (exists version of it) of debianp
(exists true whose (if true then (exists rpm) else false)) then unique values of (name of it & "|" & version of
"|" & "rpm" & "|" & architecture of it & "|" & architecture of operating system) of packages of rpm else if (exi
(if true then (exists ips image) else false)) then unique values of (full name of it & "|" & version of it as st
"pkg" & "|" & architecture of operating system) of latest installed packages of ips image else if (exists true w
then (exists pkgdb) else false)) then unique values of(pkginst of it & "|" & version of it & "|" & "pkg10") of p
pkgdb else "<unsupported>"]]></Property>
        <Property Name="Tenable AIX Technology Level" ID="76">current technology level of operating system</Prop
        <Property Name="Tenable Solaris - Showrev -a" ID="77"><![CDATA[if ((operating system as string as lowerc
"SunOS 5.10" as lowercase) AND (exists file "/var/opt/BESClient/showrev_patches.b64")) then lines of file
"/var/opt/BESClient/showrev_patches.b64" else "<unsupported>"]]></Property>
    </Analysis>
</BES>
```

BES file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<BES xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="BES.xsd">
    <Task>
        <Title>Tenable - Solaris 5.10 - showrev -a Capture</Title>
        <Description><![CDATA[&lt;enter a description of the task here&gt; ]]></Description>
        <GroupRelevance JoinByIntersection="false">
            <SearchComponentPropertyReference PropertyName="OS" Comparison="Contains">
                <SearchText>SunOS 5.10</SearchText>
                <Relevance>exists (operating system) whose (it as string as lowercase contains "SunOS
5.10" as lowercase)</Relevance>
            </SearchComponentPropertyReference>
        </GroupRelevance>
        <Category></Category>
        <Source>Internal</Source>
        <SourceID></SourceID>
        <SourceReleaseDate>2021-05-12</SourceReleaseDate>
        <SourceSeverity></SourceSeverity>
        <CVENames></CVENames>
        <SANSID></SANSID>
        <MIMEField>
            <Name>x-fixlet-modification-time</Name>
            <Value>Thu, 13 May 2021 21:50:58 +0000</Value>
        </MIMEField>
        <Domain>BESC</Domain>
        <DefaultAction ID="Action1">
            <Description>
                <PreLink>Click </PreLink>
                <Link>here</Link>
                <PostLink> to deploy this action.</PostLink>
            </Description>
            <ActionScript MIMEType="application/x-sh"><![CDATA[#!/bin/sh
/usr/bin/showrev -a > /var/opt/BESClient/showrev_patches
/usr/sfw/bin/openssl base64 -in /var/opt/BESClient/showrev_patches -out /var/opt/BESClient/showrev_
patches.b64

]]></ActionScript>
        </DefaultAction>
    </Task>
</BES>
```

Microsoft System Center Configuration Manager (SCCM)

Microsoft System Center Configuration Manager (SCCM) is available to manage large groups of
Windows-based systems. Tenable Security Center can query the SCCM service to verify whether or
not patches are installed on systems managed by SCCM and display the patch information through
the scan results.

Tenable Security Center connects to the server that is running the SCCM site (e.g., credentials must
be valid for the SCCM service, so the selected user must have privileges to query all the data in the
SCCM MMC). This server may also run the SQL database, or the database and the SCCM repository

can be on separate servers. When leveraging this audit, Tenable Security Center must connect to the SCCM server via WMI and HTTPS.

> **Note:** Initial configuration of SCCM with Tenable Security Center requires the **Domain Administrator** role.

> **Note:** SCCM scanning with Tenable products requires one of the following roles: **Read-only Analyst**, **Operations Administrator**, or **Full Administrator**. For more information, see Setting Up SCCM Scan Policies.

SCCM scanning uses the following Tenable plugins: 57029, 57030, 73636, and 58186.

> **Note:** SCCM patch management plugins support versions from SCCM 2007 up to and including Configuration Manager version 2309.

Credential	Description	Default
Server	(Required) The SCCM IP address or system name.	-
Domain	(Required) The name of the SCCM server's domain.	-
Username	(Required) The username for the SCCM user account that Tenable Security Center uses to perform checks on the target system. The user account must have privileges to query all data in the SCCM MMC.	-
Password	(Required) The password for the SCCM user with privileges to query all data in the SCCM MMC.	-

Windows Server Update Services (WSUS)

Windows Server Update Services (WSUS) is available from Microsoft to manage the distribution of updates and hotfixes for Microsoft products. Tenable Security Center can query WSUS to verify whether or not patches are installed on systems managed by WSUS and display the patch information through the Tenable Security Center user interface.

WSUS scanning uses the following Tenable plugins: 57031, 57032, and 58133.

Option	Description	Default
Server	(Required) The WSUS IP address or system name.	-

Option	Description	Default
Port	(Required) The TCP port that Microsoft WSUS listens on for communications from Tenable Security Center.	8530
Username	(Required) The username for the WSUS administrator account that Tenable Security Center uses to perform checks on the target system.	-
Password	(Required) The password for the WSUS administrator user.	-
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	Enabled

Red Hat Satellite 6 Server

Red Hat Satellite 6 is a systems management platform for Linux-based systems. Tenable Security Center can query Satellite to verify whether or not patches are installed on systems managed by Satellite and display the patch information.

Although not supported by Tenable, the Red Hat Satellite 6 plugin also works with Spacewalk Server, the Open Source Upstream Version of Red Hat Satellite. Spacewalk can manage distributions based on Red Hat (RHEL, CentOS, Fedora) and SUSE. Tenable supports the Satellite server for Red Hat Enterprise Linux.

Red Hat Satellite 6 scanning uses the following Tenable plugins: 84236, 84235, 84234, 84237, 84238, 84231, 84232, and 84233.

Option	Description	Default
Satellite Server	(Required) The Red Hat Satellite 6 IP address or system	-

Option	Description	Default
	name.	
Port	(Required) The TCP port that Red Hat Satellite 6 listens on for communications from Tenable Security Center.	443
Username	(Required) The username for the Red Hat Satellite 6 account that Tenable Security Center uses to perform checks on the target system.	-
Password	(Required) The password for the Red Hat Satellite 6 user.	-
HTTPS	When enabled, Tenable connects using secure communication (HTTPS). When disabled, Tenable connects using standard HTTP.	Enabled
Verify SSL Certificate	When enabled, Tenable verifies that the SSL certificate on the server is signed by a trusted CA. **Tip:** If you are using a self-signed certificate, disable this setting.	Enabled

Symantec Altiris

Altiris is available from Symantec to manage the distribution of updates and hotfixes for Linux, Windows, and macOS systems. Tenable Security Center has the ability to use the Altiris API to verify whether or not patches are installed on systems managed by Altiris and display the patch information through the Tenable Security Center user interface.

Tenable Security Center connects to the Microsoft SQL server that is running on the Altiris host. When leveraging this audit, if the MSSQL database and Altiris server are on separate hosts, Tenable Security Center must connect to the MSSQL database, not the Altiris server.

Altiris scanning uses the following Tenable plugins: 78013, 78012, 78011, and 78014.

Credential	Description	Default
Server	(Required) The Altiris IP address or system name.	-

Credential	Description	Default
Database Port	(Required) The TCP port that Altiris listens on for communications from Tenable Security Center.	5690
Database Name	(Required) The name of the MSSQL database that manages Altiris patch information.	Symantec_ CMDB
Database Username	(Required) The username for the Altiris MSSQL database account that Tenable Security Center uses to perform checks on the target system. Credentials must be valid for a MSSQL databas account with the privileges to query all the data in the Altiris MSSQL database.	-
Database Password	(Required) The password for the Altiris MSSQL database user.	-
Use Windows Authentication	When enabled, use NTLMSSP for compatibility with older Windows Servers. When disabled, use Kerberos.	Enabled

View Your Scan Policies

Required Tenable Security Center User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Scan Policies.

To view a list of configured scan policies:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   The **Policies** page appears.

3. View details about each scan policy.

- **Name** — The name of the scan policy.

- **Tag** — The tag applied to the scan policy.

- **Type** — The name of the template used to add the scan policy.

- **Group** — The group associated with the scan policy.

- **Owner** — The username for the user associated with the scan policy.

- **Last Modified** — The date and time the scan policy was last modified.

View Scan Policy Details

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can view details for individual scan policies. For more information, see Scan Policies.

To view details of a scan policy:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   The **Policies** page appears.

3. Right-click the row for the scan policy you want to view.

   The actions menu appears.

   -or-

   Select the check box for the scan policy you want to view.

   The available actions appear at the top of the table.

4. Click **View**.

   The **View Policy** page appears.

Section	Action
General	View general information for the scan policy. • **Name** — The name of the scan policy. • **Description** — The description for the scan policy. • **Tag** — The tag applied to the scan policy. • **Type** — The name of the template used to add the scan policy. • **Created** — The date and time the scan policy was added. • **Last Modified** — The date and time the scan policy was last modified. • **Owner** — The username for the user associated with the scan policy. • **Group** — The group associated with the scan policy. • **ID** — The scan policy ID.
Configuration	(Template-based policies only) View a summary of options configured for the scan policy. For more information, see Scan Policy Options.
Options tabs	View all of the options configured for the scan policy. The tabs displayed depend on the scan policy type. For more information, see Scan Policy Options.

Edit a Scan Policy

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Scan Policies.

To edit a scan policy:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   The **Policies** page appears.

3. Right-click the row for the scan policy you want to edit.

   The actions menu appears.

   -or-

   Select the check box for the scan policy you want to edit.

   The available actions appear at the top of the table.

4. Click **More** > **Edit**.

   The **Edit Policy** page appears.

5. Modify the scan policy. For more information, see Scan Policy Options.

6. Click **Submit**.

   Tenable Security Center saves your configuration.

Share or Revoke Access to a Scan Policy

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can share or revoke access to a scan policy to allow or restrict access to a user group. When you share a scan policy with a user group, users in the group with the appropriate permissions can use the policy in an active scan, modify policy options, and more.

For more information, see Scan Policies. For more information about user groups, see Groups.

To share or revoke access to a scan policy:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   The **Policies** page appears.

3. Right-click the row for the scan policy for which you want to share or revoke access.

   The actions menu appears.

   -or-

   Select the check box for the scan policy for which you want to share or revoke access.

   The available actions appear at the top of the table.

4. Click **Share**.

   The **Share Policy** window appears.

5. In the **Share Policy** window, select the groups for which you want to share or revoke access to the scan policy.

6. Click **Submit**.

   Tenable Security Center saves your configuration.

Export a Scan Policy

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

> **Note:** Exported scan policies are not backwards-compatible. For example, If you are running Tenable Security Center 6.1.0 or later and you export a scan policy, you can only import the scan policy into another instance of Tenable Security Center 6.1.0 or later.

You can export a scan policy as a `.nessus` file and import it to another Tenable Security Center to use in an active scan configuration.

In some cases, Tenable Support may also ask you to export a scan policy for troubleshooting.

> **Note:** Exported scan policy files do not include audit files or credentials. You can re-configure audit files and credentials you want to use with the scan policy on the Tenable Security Center where you import the scan policy. For more information, see Audit Files and Credentials.

For more information, see Scan Policies.

Before you begin:

- Add a scan policy, as described in [Add a Scan Policy](#).

- Confirm your **PHP Serialization Mode** setting is set to **PHP Serialization ON**. For more information, see [Use the Security section to define the Tenable Security Center user interface login parameters and options for account logins. You can also configure banners, headers, and classification headers and footers.](#).

To export a scan policy:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   The **Policies** page appears.

3. To export a single scan policy:

   a. In the table, right-click the row for the scan policy you want to export.

      The actions menu appears.

   To export multiple scan policies:

   a. In the table, select the check box for each scan policy you want to export.

      The available actions appear at the top of the table.

4. Click **Export**.

   Tenable Security Center exports the scan policy as a `.xml` file.

What to do next:

- Do any of the following:

  - Import the scan policy into another Tenable Security Center, as described in [Import a Scan Policy](#).

  - If Tenable Support requested a scan policy file for troubleshooting, share the scan policy file with Tenable Support.

Import a Scan Policy

Required Tenable Security Center User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can import a `.nessus` scan policy file from Tenable Nessus or from another Tenable Security Center to use in an active scan configuration. For more information, see Scan Policies.

Note: Imported scan policies do not include audit files or credentials. For more information, see Audit Files and Credentials.

Before you begin:

- Ensure your **PHP Serialization Mode** setting is **PHP Serialization ON**. For more information, see Use the Security section to define the Tenable Security Center user interface login parameters and options for account logins. You can also configure banners, headers, and classification headers and footers..

- Do one of the following:

  ○ Export a scan policy from another Tenable Security Center, as described in Export a Scan Policy.

  ○ Export a scan policy from Tenable Nessus. For more information, see Policies in the *Tenable Nessus User Guide*.

To import a scan policy:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   The **Policies** page appears.

3. At the top of the table, click **Upload Policy**.

   The **Upload Policy** page appears.

4. In the **Name** box, type a name for the scan policy.

5. (Optional) In the **Description** box, type a description for the scan policy.

6. (Optional) In the **Tag** box, type or select a tag for the scan policy.

7. Click **Choose File** and browse to the `.nessus` scan policy file you want to import.

8. Click **Submit**.

   Tenable Security Center imports the scan policy.

What to do next:

- (Optional) Modify the scan policy settings, as described in Edit a Scan Policy.

- (Optional) Configure audit files and credentials you wish to reference with the scan policy, as described in Add a Custom Audit File and Add Credentials.

- Reference the scan policy in an active scan configuration, as described in Add an Active Scan.

Copy a Scan Policy

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Scan Policies.

To create a copy of a scan policy:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   The **Policies** page appears.

3. To copy a single scan policy:

   a. In the table, right-click the row for the scan policy you want to copy.

      The actions menu appears.

   To copy multiple scan policies:

   a. In the table, select the check box for each scan policy you want to copy.

      The available actions appear at the top of the table.

4. Click **Copy**.

   Tenable Security Center copies the scan policy. The copy appears, named **Copy of PolicyName**.

Delete a Scan Policy

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Scan Policies.

> **Note:** If you delete a scan policy referenced by an active scan, Tenable Security Center disables the scan. For more information, see Scan Result Statuses.

Before you begin:

- If any active scans reference the scan policy you intend to delete, update the active scans to use a different scan policy, as described in Manage Active Scans.

To delete a scan policy:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   The **Policies** page appears.

3. In the table, right-click the row for the scan policy you want to delete.

   The actions menu appears.

4. Click **Delete**.

   A confirmation window appears.

5. Click **Delete**.

   Tenable Security Center deletes the scan policy.

To delete multiple scan policies:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   The **Policies** page appears.

3. In the table, select the check box for each scan policy you want to delete.

   The available actions appear at the top of the table.

4. At the top of the table, click **Delete**.

   A confirmation window appears.

5. Click **Delete**.

   Tenable Security Center deletes the scan policies.

Agent Scanning

To perform agent scanning, Tenable Security Center fetches agent scan results from agent-capable Tenable Nessus Manager or Tenable Vulnerability Management instances. Using Tenable Agents for scanning reduces network usage and allows devices to maintain their scan schedules even when disconnected from the network. Tenable Security Center fetches these results for review with other acquired information about the host and network.

You can configure one or both methods of fetching agent scan results in Tenable Security Center:

- *Agent scans* fetch results from agent scans you add and launch in Tenable Security Center. When you add an agent scan in Tenable Security Center, Tenable Security Center creates a corresponding agent scan in an instance of Tenable Nessus Manager or Tenable Vulnerability Management that you linked to Tenable Security Center. When you launch an agent scan in Tenable Security Center, Tenable Security Center launches the corresponding scan in Tenable Nessus Manager or Tenable Vulnerability Management, then imports the results into Tenable Security Center.

  You can create agent scans in Tenable Security Center using the Advanced Agent Scan template. For more information, see Scan Policy Templates.

  For more information, see Agent Scans.

- *Agent synchronization jobs* fetch results from agent scans you previously created and launched in Tenable Nessus Manager or Tenable Vulnerability Management.

  Agent synchronization jobs can fetch results from agent scans configured in Tenable Nessus Manager or Tenable Vulnerability Management using any agent scan template.

  For more information, see Agent Synchronization Jobs.

To configure agent scanning:

1. Configure Tenable Agents in either Tenable Nessus Manager or Tenable Vulnerability Management, as described in Deployment Workflow in the *Tenable Agent Deployment and User Guide*.

2. Add your agent-capable Tenable Nessus Manager or Tenable Vulnerability Management instance as a Tenable Nessus scanner in Tenable Security Center, as described in Tenable Nessus Scanners.

3. Add one or more agent repositories in Tenable Security Center, as described in Add a Repository.

4. Do one or both of the following:

   - Add an agent scan using the Basic Agent Scan or Advanced Agent Scan template in Tenable Security Center, as described in Add an Agent Scan.

   - Add an agent synchronization job in Tenable Security Center, as described in Add an Agent Synchronization Job.

What to do next:

- View scan results, as described in Scan Results.

- View vulnerability data by unique Agent ID, as described in Vulnerability Analysis.

Agent Scans

Agent scans fetch results from agent scans you add and launch in Tenable Security Center. When you add an agent scan in Tenable Security Center, Tenable Security Center creates a corresponding agent scan in an instance of Tenable Nessus Manager or Tenable Vulnerability Management that you linked to Tenable Security Center. When you launch an agent scan in Tenable Security Center, Tenable Security Center launches the corresponding scan in Tenable Nessus Manager or Tenable Vulnerability Management, then imports the results into Tenable Security Center.

You can create agent scans in Tenable Security Center using the Advanced Agent Scan template. For more information, see Scan Policy Templates.

For more information about agent scanning in Tenable Security Center, see Agent Scanning.

The **Agent Scans** page displays a list of all available agent scans. Tenable Security Center shares newly created agent scan import schedules to everyone within the same user group when users have the appropriate permissions.

When more than one agent scan result is ready on Tenable Vulnerability Management or Tenable Nessus Manager, the scan results queue for import to Tenable Security Center.

For more information about agent scans, see:

- Add an Agent Scan

- Agent Scan Settings

- Manage Agent Scans

Add an Agent Scan

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can create agent scans in Tenable Security Center using the Advanced Agent Scan template. For more information, see Scan Policy Templates.

For more information, see Agent Scans and Agent Scan Settings.

> **Note:** If you are scanning a Linux machine with Tenable Security Center, the Linux machine's shell configuration file must have a `PS1` variable of four or more characters (for example, `PS1='\u@\h:~\$ '`). Having a `PS1` variable of less than four characters (for example, `PS1='\$ '`) can drastically increase the overall scan time.

Before you begin:

- Confirm you understand the complete agent scanning configuration process, as described in Agent Scanning.

- (Optional) Configure an Advanced Agent Scan policy template, as described in Add a Scan Policy.

To add an agent scan:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Scans** > **Agent Scans**.

   The **Agent Scans** page appears.

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

   The **Add Agent Scan** page appears.

4. Click **General**.

5. Type a **Name** for the scan.

6. (Optional) Type a **Description** for the scan.

7. (Optional) To reference an Advanced Agent Scan policy in the scan:

   a. Click **Custom Policy** to enable the toggle.

   b. In the **Policy** drop-down menu, select the Advanced Agent Scan policy.

8. Select an **Agent Scanner**.

9. Select one or more **Agent Groups**.

10. Select a **Scan Type**:

Scan Type	Description
Scan Window	A Scan Window is the duration of time that an agent has from the scheduled scan start time to receive the scan job, run the scan, and upload the results. If you select this scan type, the following options appear: • **Scan Window** - Specify the amount of time Tenable Security Center waits before fetching the results of the agent scan: **15 minutes**, **30 minutes**, **1 hour**, **3 hours**, **6 hours**, **12 hours**, or **1 day**. If Tenable Security Center fetches results for the scan before the scan completes, Tenable Security Center displays the results available at the time the scan window expired. The agent scan continues to run in Tenable Vulnerability Management or Tenable

Scan Type	Description
	Nessus Manager during the scan window specified in Tenable Vulnerability Management or Tenable Nessus Manager, even if the scan window in Tenable Security Center expires.

> **Note:** To view complete agent scan result data in Tenable Security Center, Tenable recommends setting a **Scan Window** value that allows your agent scans to complete before Tenable Security Center fetches the results.

- **Schedule** - Specify the frequency you want Tenable Security Center to fetch agent scan results: **Now**, **Remediation**, **Once**, **Daily**, **Weekly**, **Monthly**, or **On Demand**.

> **Note:** If you schedule your scan to repeat monthly, Tenable recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (e.g., the 29th), Tenable Security Center cannot run the scan on those days.

> **Tip:** Retrieve agent scan results as close to the completion time of the scan as possible to most accurately display within Tenable Security Center when the scan discovered the vulnerability results.

Scan Type	Description
Triggered	A Triggered scan configuration allows the agent or agent group to launch the scan without user intervention. If you select this scan type, the following options appear: • **Interval** - Enable this option to trigger the scan at a set time interval, in days or hours. • **Filename** - Enable this option to trigger the scan when a file with a specific file name is added to the agent trigger directory. The trigger file disappears after the scan begins. The agent trigger directory location varies by operating system:

Scan Type	Description

Operating System	Location
Windows	`C:\ProgramData\Tenable\Nessus Agent\nessus\triggers`
macOS	`/Library/NessusAgent/run/var/nessus/triggers`
Linux	`/opt/nessus_agent/var/nessus/triggers`

If you enable both the *Interval* and *Filename* options, the scan searches for triggers in order. In other words, if the first trigger does not trigger the scan, the scan searches for the second trigger.

> **Note:** Agents perform triggered scans automatically, and do not require an admin to launch or schedule them to launch at a particular time. Triggered scans also do not generate a scan DB or UUID.

> **Note:** After you create a triggered agent scan, a background agent synchronization job begins. This agent synchronization job downloads triggered agent scan results and imports them into the repository selected for the triggered agent scan. When the last triggered agent scan for that scanner is deleted, the background agent synchronization job is deleted. This agent synchronization job does not appear on the **Agent Synchronization Jobs** page.

11. Click **Settings**.

12. Select an **Import Repository** for the scan.

13. (Optional) Click **Post Scan**. The **Post Scan** section does not appear if the agent scan type is **Triggered**.

    - If you want to configure automatic report generation, click **Add Report**. For more information, see Add a Report to a Scan.

14. Click **Submit**.

Tenable Security Center saves your configuration.

What to do next:

- View scan results, as described in Scan Results.

- View vulnerability data by unique Agent ID, as described in Vulnerability Analysis.

Manage Agent Scans

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information about agent scans, see Agent Scans.

To manage agent scans:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Agent Scans**.

   The **Agent Scans** page appears.

3. To filter the scans that appear on the page, apply a filter as described in Apply a Filter.

4. To start an agent scan, see Start or Pause a Scan.

5. To view details for a scan:

   a. Right-click the row for the scan.

      The actions menu appears.

      -or-

      Select the check box for the scan.

      The available actions appear at the top of the table.

   b. Click **View**.

      The **View Agent Scan** page appears.

6. To edit a scan:

a. Right-click the row for the scan.

The actions menu appears.

-or-

Select the check box for the scan.

The available actions appear at the top of the table.

b. Click **Edit**.

The **Edit Agent Scan** page appears.

c. Modify the scan options. For more information, see Agent Scan Settings.

d. Click **Submit**.

Tenable Security Center saves your configuration.

7. To delete a scan:

a. Right-click the row for the scan.

The actions menu appears.

-or-

Select the check box for the scan.

The available actions appear at the top of the table.

b. Click **Delete**.

Tenable Security Center deletes the scan.

8. To delete multiple scans:

a. In the table, select the check box for each scan you want to delete.

The available actions appear at the top of the table.

b. At the top of the table, click **Delete**.

A confirmation window appears.

c. Click **Delete**.

Tenable Security Center deletes the scans.

Agent Scan Settings

For more information, see [Agent Scans](#).

- [General Options](#)

- [Settings Options](#)

- [Post Scan Options](#)

General Options

Parameter	Description	Default
General		
Name	The scan name associated with the scan's results. This may be any name or phrase (for example, **SystemA**, **DMZ Scan**, or **Daily Scan of the Web Farm**).	--
Description	Descriptive information related to the scan.	--
Custom Policy	When enabled, select an agent scan policy to apply to the scan. For more information, see [Scan Policy Templates](#). When disabled, the scan uses a Tenable Nessus or Tenable Vulnerability Management Basic Agent Scan template. For more information, see [Agent Scan and Policy Templates](#) in the *Tenable Agent Deployment and User Guide* and [Tenable-Provided Agent Templates](#) in the *Tenable Vulnerability Management User Guide*.	Disabled
Policy	(If **Custom Policy** is enabled) The name of the agent scan policy.	--
Agent Scanner	The Agent-enabled scanner from which to retrieve agent results.	--
Agent Groups	Specifies the agent group or groups in Tenable Nessus Manager you want the scan to target. For more information, see [Agent Groups](#) in	--

Parameter	Description	Default
	the *Tenable Nessus User Guide*.	
Scan Type	Specifies the type of schedule for the agent scan: **Scan Window** or **Triggered**. A Scan Window is the duration of time that an agent has from the scheduled scan start time to receive the scan job, run the scan, and upload the results. A Triggered scan configuration allows the agent or agent group to launch the scan without user intervention.	
Scan Window	Specifies the amount of time Tenable Security Center waits before fetching the results of the agent scan: **15 minutes**, **30 minutes**, **1 hour**, **3 hours**, **6 hours**, **12 hours**, or **1 day**. If Tenable Security Center fetches results for the scan before the scan completes, Tenable Security Center displays the results available at the time the scan window expired. The agent scan continues to run in Tenable Vulnerability Management or Tenable Nessus Manager during the scan window specified in Tenable Vulnerability Management or Tenable Nessus Manager, even if the scan window in Tenable Security Center expires. **Note:** To view complete agent scan result data in Tenable Security Center, Tenable recommends setting a **Scan Window** value that allows your agent scans to complete before Tenable Security Center fetches the results.	1 hour
Triggered	Specifies the frequency you want Tenable Security Center to launch the scan and fetch results. • **Interval** – Enable this option to trigger the scan at a set time interval, in days or hours. • **Filename** - Enable this option to trigger the scan when a file with a specific file name is added to the agent trigger directory. The trigger file disappears after the scan begins. The agent trigger directory location varies by operating system:	

Parameter	Description	Default
	Operating System / **Location**	
	Windows: `C:\ProgramData\Tenable\Nessus Agent\nessus\triggers`	
	macOS: `/Library/NessusAgent/run/var/nessus/triggers`	
	Linux: `/opt/nessus_agent/var/nessus/triggers`	
	If you enable both the *Interval* and *Filename* options, the scan searches for triggers in order. In other words, if the first trigger does not trigger the scan, the scan searches for the second trigger. **Note:** Agents perform triggered scans automatically, and do not require an admin to launch or schedule them to launch at a particular time. Triggered scans also do not generate a scan DB or UUID. **Note:** After you create a triggered agent scan, a background agent synchronization job begins. This agent synchronization job downloads triggered agent scan results and imports them into the repository selected for the triggered agent scan. When the last triggered agent scan for that scanner is deleted, the background agent synchronization job is deleted. This agent synchronization job does not appear on the **Agent Synchronization Jobs** page.	
Schedule		
Schedule	The frequency you want Tenable Security Center to fetch agent scan results: **Now**, **Remediation**, **Once**, **Daily**, **Weekly**, **Monthly**, or **On Demand**. This setting appears only when you select *Scan Window* in the **Scan Type** drop-down.	On Demand

Parameter	Description	Default
	Note: If you schedule your scan to repeat monthly, Tenable recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (e.g., the 29th), Tenable Security Center cannot run the scan on those days. **Tip:** Retrieve agent scan results as close to the completion time of the scan as possible to most accurately display within Tenable Security Center when the scan discovered the vulnerability results.	

Settings Options

Parameter	Description	Default
Import Repository	Specifies the repository where you want the agent scan results to import. Select an agent repository to receive scan data. **Note:** You cannot import agent scan data to a non-agent repository.	--

Post Scan Options

These options determine what actions occur immediately before and after the agent scan completes.

Option	Description	Default
Add Report	This option provides a list of reports available to the user to run when the agent scan data import completes. For more information, see Add a Report to a Scan.	--

Agent Synchronization Jobs

Agent synchronization jobs fetch results from agent scans you previously created and launched in Tenable Nessus Manager or Tenable Vulnerability Management. Agent synchronization jobs can fetch results from agent scans configured in Tenable Nessus Manager or Tenable Vulnerability

Management using any agent scan template. For more information about agent scanning in Tenable Security Center, see Agent Scanning.

The **Agent Synchronization Jobs** page displays a list of all available agent synchronization jobs. Tenable Security Center shares newly created agent scan import schedules to everyone within the same user group when users have the appropriate permissions.

When more than one agent scan result is ready on Tenable Nessus Manager, the scan results queue for import to Tenable Security Center.

For more information about agent synchronization jobs, see:

- Add an Agent Synchronization Job

- Agent Synchronization Job Settings

- Manage Agent Synchronization Jobs

Add an Agent Synchronization Job

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information about agent synchronization jobs, see Agent Synchronization Jobs. For more information about agent synchronization job options, see Agent Synchronization Job Settings.

Before you begin:

- Confirm you understand the complete agent scanning configuration process, as described in Agent Scanning.

To add an agent synchronization job:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Scans** > **Agent Synchronization Jobs**.

   The **Agent Synchronization Jobs** page appears.

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

   The **Add Agent Synchronization Job** page appears.

4. Click **General**.

5. Type a **Name** for the agent synchronization job.

6. (Optional) Type a **Description** for the agent synchronization job.

7. Select an **Agent Scanner**.

8. Type an **Agent Scan Name Filter**.

9. (Optional) If you want to limit the scan results fetched by Tenable Security Center, enable **Scan Result Threshold** and select a date and time to specify the oldest scan results you want Tenable Security Center to fetch.

10. (Optional) Select a **Schedule** for the agent synchronization job.

11. Click **Settings**.

12. Select an **Import Repository** for the agent synchronization job.

13. (Optional) Click **Post Scan**.

    - If you want to configure automatic report generation, click **Add Report**. For more information, see Add a Report to a Scan.

    - If you previously added an email address to your account profile and you want to configure email notifications, enable or disable **E-Mail Me on Launch** or **E-Mail Me on Completion**.

14. Click **Submit**.

    Tenable Security Center saves your configuration.

What to do next:

- View scan results, as described in Scan Results.

- View vulnerability data by unique Agent ID, as described in Vulnerability Analysis.

Manage Agent Synchronization Jobs

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Agent Synchronization Jobs.

To manage agent synchronization jobs:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Agent Synchronization Jobs**.

   The **Agent Synchronization Jobs** page appears.

3. To filter the agent synchronization jobs that appear on the page, apply a filter as described in Apply a Filter.

4. To start or pause an agent synchronization job, see Start or Pause a Scan.

5. To view details for an agent synchronization job:

   a. Right-click the row for the agent synchronization job.

      The actions menu appears.

      -or-

      Select the check box for the agent synchronization job.

      The available actions appear at the top of the table.

   b. Click **View**.

      The **View Agent Synchronization Job** page appears.

6. To edit an agent synchronization job:

   a. Right-click the row for the agent synchronization job.

      The actions menu appears.

      -or-

      Select the check box for the agent synchronization job.

      The available actions appear at the top of the table.

   b. Click **Edit**.

      The **Edit Agent Synchronization Job** page appears.

c. Modify the agent synchronization job options. For more information, see [Agent Synchronization Job Settings](#).

d. Click **Submit**.

    Tenable Security Center saves your configuration.

7. To copy an agent synchronization job:

    a. Right-click the row for the agent synchronization job.

        The actions menu appears.

        -or-

        Select the check box for the agent synchronization job.

        The available actions appear at the top of the table.

    b. Click **Copy**.

        Tenable Security Center creates a copy of the agent synchronization job.

    To copy multiple agent synchronization jobs:

    a. In the table, select the check box for each agent synchronization job you want to copy.

        The available actions appear at the top of the table.

    b. At the top of the table, click **Copy**.

        Tenable Security Center creates a copy of the agent synchronization job.

8. To delete an agent synchronization job:

    a. Right-click the row for the agent synchronization job.

        The actions menu appears.

        -or-

        Select the check box for the agent synchronization job.

        The available actions appear at the top of the table.

    b. Click **Delete**.

Tenable Security Center deletes the agent synchronization job.

To delete multiple agent synchronization jobs:

a. In the table, select the check box for each agent synchronization job you want to delete.

The available actions appear at the top of the table.

b. At the top of the table, click **Delete**.

A confirmation window appears.

c. Click **Delete**.

Tenable Security Center deletes the scans.

Agent Synchronization Job Settings

For more information, see [Agent Synchronization Jobs](#).

- [General Options](#)
- [Settings Options](#)
- [Post Scan Options](#)

General Options

Option	Description
Name	The agent synchronization job name associated with the scan's results. This may be any name or phrase (e.g., **SystemA**, **DMZ Scan**, **Daily Scan of the Web Farm**, etc.).
Description	A description for the agent synchronization job.
Agent Scanner	The agent-capable scanner from which you want Tenable Security Center to retrieve agent results.
Agent Scan Name Filter	A filter for agent scan results to retrieve from the Tenable Agent-enabled scanner. Filters can use the specific name of the result(s) to retrieve or an asterisk (*) or question mark (?) for all or part of the scan result name(s) to retrieve. You can find the available agent scans retrieved from the selected

Option	Description
	scanner on the Scan page of the user logged in to the Nessus server.
	You can click the **Preview Filter** button to view results that match the filter.
Scan Result Threshold	Specifies whether Tenable Security Center fetches all or some agent scan results from the agent-capable scanner. • When disabled, Tenable Security Center fetches all agent scan results. • When enabled, Tenable Security Center restricts the agent scan results it fetches. **Note:** You cannot modify the Scan Result Threshold after initial creation of the agent synchronization job. After you create the agent synchronization job, the **Edit Agent Synchronization Job** and **View Agent Synchronization Job** pages display the **Last Fetched** date to indicate when Tenable Security Center performed the most recent successful agent synchronization job.
Import Triggered Agent Scans	Specifies whether the job includes triggered agent scan results.
Select Date and Time	When **Scan Result Threshold** is enabled, specifies the oldest agent scan results you want Tenable Security Center to fetch.
Schedule	The frequency you want Tenable Security Center to fetch agent scan results. Select **Now**, **Once**, **Daily**, **Weekly**, **Monthly**, **On Demand**, or **Dependent** to create an agent scan result retrieval template that you can launch manually at any time. The other time frames allow you to retrieve agent scan results at specified times and intervals. Tenable recommends retrieving agent scan results as close to the completion time of the scan as possible to most accurately display within Tenable Security Center when the scan discovered the vulnerability results. For more information about how Tenable Security Center determines vulnerability discovery dates, see Vulnerability Discovered.

Option	Description
	Note: If you schedule your scan to repeat monthly, Tenable recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (e.g., the 29th), Tenable Security Center cannot run the scan on those days.

Settings Options

Parameter	Description
Import Repository	Specifies the agent repository where you want the agent scan results to import. **Note:** You can only import agent scan data to a Universal or Agent repository.

Post Scan Options

These options determine what actions occurs immediately before and after the agent synchronization job completes. The table below describes the post agent synchronization job options available to users:

Option	Description
Add Report	This option provides a list of reports available to the user to run when the agent scan data import completes. The initial choices are to click the group and owner of the report to present a list of valid report options. Next, click the report from the list that can be searched using the text search box. When hovering over a report name, you can select the information icon to display the name and description of the report. You can base the generated report on the current scan's results or the results in the Cumulative database. Selecting the check mark causes the report to launch once the agent synchronization job completes. Selecting the **X** removes the changes. Once added, you can modify or delete the report information.

Web App Scans

> **Required Additional License:** Tenable Web App Scanning for Tenable Security Center

Web application scanning in Tenable Security Center allows you to scan and address web application vulnerabilities that traditional scanners cannot accurately assess.

Web app scans in Tenable Security Center are configured using Tenable Core + Tenable Web App Scanning or Tenable Web App Scanning in a Docker deployment routed through Sensor Proxy. For more information about Tenable Core + Tenable Web App Scanning, see Welcome to Tenable Core + Tenable Web App Scanning. For more information about using Tenable Web App Scanning as a Docker image, see Deploy Tenable Web App Scanning as a Docker Image.

For instructions on how to configure web app scans, see the following:

- Configure web app scans with Tenable Security Center using Tenable Core or Docker image
- Configure web app scans using a Tenable Nessus scanner

For more information about web app scans in Tenable Security Center, see Manage Web App Scans and Web App Scan Settings.

For more information about your Tenable Web App Scanning for Tenable Security Center license, see License Requirements.

To fully configure web app scans with Tenable Security Center using Tenable Core or Docker image:

> **Note:** Tenable Security Center allows four concurrent web app scans per configured Tenable Core + Tenable Web App Scanning or Docker image at a time.

1. Apply the Tenable Web App Scanning for Tenable Security Center license, as described in Update an Existing License.

2. Ensure the Tenable Web App Scanning plugins are updated, as described in Plugin/Feed Settings. The plugins automatically update when the license is updated.

3. Add a Sensor Proxy to Tenable Security Center if there is not one added or if a new one is required due to network architecture.

4. Add a [Tenable Core + Tenable Web App Scanning](#) or a [Tenable Web App Scanning as a Docker image](#) to your environment.

5. [Add a Web Application Scanner](#) to your Sensor Proxy.

6. Add a scan zone in Tenable Security Center, as described in [Add a Scan Zone](#).

7. Add a universal repository for the scan data in Tenable Security Center, as described in [Add a Repository](#).

8. Configure your Tenable Web App Scanning credentials, as described in [Add Credentials](#).

9. Create a Web App Scanning scan policy, as described in [Add a Scan Policy](#).

10. Add a web app scan in Tenable Security Center, as described in [Add a Web App Scan](#).

To fully configure web app scans using a Tenable Nessus scanner:

> **Note:** You can use a Tenable Nessus scanner to perform web app scans, however this will be deprecated in a future release. For more information about Tenable Nessus scanners, see [Tenable Nessus Scanners](#).

> **Note:** Tenable Security Center allows only one concurrent web app scan per configured Tenable Nessus scanner at a time.

1. Apply the Tenable Web App Scanning for Tenable Security Center license, as described in [Update an Existing License](#).

2. Ensure the Tenable Web App Scanning plugins are updated, as described in [Plugin/Feed Settings](#). The plugins automatically update when the license is updated.

3. If you are configuring a Tenable Nessus scanner:

   a. Ensure you are running Docker version 20.0.0 or later on your Tenable Nessus host. Tenable recommends the [official Docker builds and install packages](#).

   > **Note:** If your scanner is configured to connect through a proxy, ensure that you configure the proxy settings directly in Docker.

   b. Ensure you are running Tenable Nessus version 10.6.1 or later.

c. Ensure your system meets the [hardware requirements](#) for Tenable Nessus with Tenable Web App Scanning enabled.

> **Note:** The following platforms do not support web app scanning in Tenable Nessus:
>
> - Any host system that does not support official Docker builds.
>
> - Any host that uses an ARM-based processor (for example, AArch64 Linux distributions and macOS M1 and M2 systems).
>
> - Tenable Core + Tenable Nessus, or any instance of Tenable Nessus that already runs within a Docker image.
>
> For more information about Docker support on virtualized hosts, see the [Docker documentation](#).

4. Enable the Tenable Web App Scanning **Capable** option for the Tenable Nessus scanner in Tenable Security Center, as described in [Tenable Nessus Scanners](#).

5. Add a scan zone in Tenable Security Center, as described in [Add a Scan Zone](#).

6. Add a universal repository for the scan data in Tenable Security Center, as described in [Add a Repository](#).

7. Configure your Tenable Web App Scanning credentials, as described in [Add Credentials](#).

8. Create a Web App Scanning scan policy, as described in [Add a Scan Policy](#).

9. Add a web app scan in Tenable Security Center, as described in [Add a Web App Scan](#).

What to do next:

- View scan results, as described in [Scan Results](#).

- View web app scan vulnerability data, as described in [Web App Scanning Analysis](#).

Add a Web App Scan

Required Additional License: Tenable Web App Scanning

Required Tenable Nessus Version: 10.6.1 or later

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can create web app scans in Tenable Security Center using Web Application Scanning templates. For more information, see Scan Policy Templates.

For more information, see Web App Scans and Web App Scan Settings.

Before you begin:

- Confirm you understand the complete web app scanning configuration process, as described in Web App Scans.

- Configure a Web App Scanning scan policy, as described in Add a Scan Policy.

To add a web app scan:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Web App Scans**.

   The **Web App Scans** page appears.

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

   The **Add Web App Scan** page appears.

4. Click **General**.

   a. Type a **Name** for the scan.

   b. (Optional) Type a **Description** for the scan.

   c. In the **Policy** drop-down menu, select the Web App Scanning scan policy.

   d. (Optional) Select a **Schedule** for the scan.

5. Click **Settings**.

   a. Select a **Scan Zone** for the scan.

   b. Select an **Import Repository** for the scan.

6. Click **Targets**.

a. Type a target **URL** for the scan.

7. Click **Credentials**.

   a. Click **Add Credential**.

   b. In the drop-down boxes, select a credential type and a preconfigured credential.

   c. Click the check mark to save your selection.

8. (Optional) Click **Post Scan**.

   a. If you want to configure automatic report generation, click **Add Report**. For more information, see [Add a Report to a Scan](#).

9. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

- View scan results, as described in [Scan Results](#).

- View web app scan vulnerability data, as described in [Web App Scanning Analysis](#).

Manage Web App Scans

Required Additional License: Tenable Web App Scanning

Required Tenable Nessus Version: 10.6.1 or later

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information about web app scans, see [Web App Scans](#).

To manage web app scans:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Web App Scans**.

   The **Web App Scans** page appears.

3. To filter the scans that appear on the page, apply a filter as described in Apply a Filter.

4. To start a scan, see Start or Pause a Scan.

> **Note:** Pausing is not supported for web app scans.

5. To view details for a scan:

   a. Right-click the row for the scan.

      The actions menu appears.

      -or-

      Select the check box for the scan.

      The available actions appear at the top of the table.

   b. Click **View**.

      The **View Web App Scan** page appears.

6. To edit a scan:

   a. Right-click the row for the scan.

      The actions menu appears.

      -or-

      Select the check box for the scan.

      The available actions appear at the top of the table.

   b. Click **Edit**.

      The **Edit Web App Scan** page appears.

   c. Modify the scan options. For more information, see Web App Scan Settings.

   d. Click **Submit**.

      Tenable Security Center saves your configuration.

7. To delete a scan:

a. Right-click the row for the scan.

The actions menu appears.

-or-

Select the check box for the scan.

The available actions appear at the top of the table.

b. Click **Delete**.

Tenable Security Center deletes the scan.

8. To delete multiple scans:

a. In the table, select the check box for each scan you want to delete.

The available actions appear at the top of the table.

b. At the top of the table, click **Delete**.

A confirmation window appears.

c. Click **Delete**.

Tenable Security Center deletes the scans.

Web App Scan Settings

Required Additional License: Tenable Web App Scanning

Required Tenable Nessus Version: 10.6.1 or later

For more information, see Web App Scans.

- Parameter

- Parameter

- Option

- The Credentials section allows users to select pre-configured credential sets for authenticated scanning. For more information, see Credentials.

- [These options determine what actions occur immediately before and after the web app scan completes.](#)

General Options

Parameter	Description	Default
General		
Name	The scan name that is associated with the scan's results. This can be any name or phrase (for example, *SystemA*, *DMZ Scan*, or *Daily Scan of the Web Farm*).	--
Description	Descriptive information related to the scan.	--
Policy	The policy on which you want to base the scan. You can scroll through the list, or search by entering text in the search box at the top of the list of available policies. For more information, see [Scan Policy Templates](#).	--
Schedule		
Schedule	The frequency you want to run the scan.	On Demand
	• **Now** specifies that you want Tenable Security Center to launch the scan immediately without saving the configuration for later.	
	> **Note:** Scans configured to run **Now** do not appear on the **Active Scans** page.	
	• **Once** specifies that you want Tenable Security Center to launch the scan at the specified time without saving the configuration for later.	
	> **Note:** Scans configured to run **Once** do not appear on the **Active Scans** page.	
	• **Daily**, **Weekly**, or **Monthly** specifies that you want	

Parameter	Description	Default
	Tenable Security Center to launch the scan at a scheduled interval. **Note:** If you schedule your scan to repeat monthly, Tenable recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (e.g., the 29th), Tenable Security Center cannot run the scan on those days. • **On Demand** specifies that you want to launch the scan manually at any time. • **Dependent** specifies that you want Tenable Security Center to launch the scan every time Tenable Security Center finishes a scheduled run of the dependent scan you select.	

Settings Options

Parameter	Description
Basic	
Scan Zone	**Note:** If your organization's **Distribution Method** setting is **Locked Zone**, you cannot modify this setting. If your organization's **Distribution Method** setting is **Automatic Distribution Only**, Tenable Security Center automatically chooses one or more scan zones and hides this setting. Specifies the scan zone you want to use to run the scan. Depending on your organization's **Distribution Method** setting, you can select one of the following: • An available zone — use a single scan zone to run the scan. **Note:** If you select a single scan zone, Tenable Security Center ignores the ranges in the scan zone and scans all of the [targets](#) you specify in the scan configuration.

Parameter	Description
	• **Automatic Distribution** — allow Tenable Security Center to choose the best scan zone to run the scan. For more information, see [Organizations](#) and [Scan Zones](#).
Import Repository	Specifies the repository where Tenable Security Center imports the scan results. Select a Universal repository to receive IPv4 or IPv6 results appropriate to the scan. For more information about repositories, see [Repositories](#).
Advanced	
Immediately remove vulnerabilities from scanned hosts that do not reply	If a previously responsive host does not reply to a scan, Tenable Security Center removes the host's vulnerabilities from the cumulative database. If the host has vulnerabilities in the mitigated database, they remain in the mitigated database. • If you enable this option, the system removes the vulnerabilities immediately after the scan completes. • If you disable this option, the system removes the vulnerabilities according to the interval set in the **Number of days to wait before removing dead hosts** option.
Max scan duration (hours)	Specifies the maximum number of hours you want a scan to run. If a scan reaches this threshold, the scan stops and Tenable Security Center discards the scan results.
Inactivity timeout duration (hours)	Specifies the maximum number of hours you want a scan to be inactive before it times out. The value for **Inactivity timeout duration** must be less than the value for **Max scan duration**.

Targets Options

Option	Description	Default
URLs	One or more URL targets for the scan. Type multiple targets as a comma-separated list of URLs.	--

Credentials Options

The **Credentials** section allows users to select pre-configured credential sets for authenticated scanning. For more information, see Credentials.

Tenable Security Center web app scans support Web Authentication Credentials.

> **Note:** You cannot add credentials to web app scans that have multiple targets.

Post Scan Options

These options determine what actions occur immediately before and after the web app scan completes.

Option	Description	Default
Notifications		
E-mail Me on Launch	When enabled, Tenable Security Center sends a notification to the email address associated with your user account when the scan launches.	disabled
E-mail Me on Completion	When enabled, Tenable Security Center sends a notification to the email address associated with your user account when the scan completes.	disabled
Reports to Run on Scan Completion		
Add Report	This option provides a list of reports available to the user to run when the web app scan data import completes. For more information, see Add a Report to a Scan.	--

Freeze Windows

You can set a freeze window in Tenable Security Center to specify a time frame when you do not want Tenable Security Center to scan specific targets. This prevents remediation or ad-hoc scans from scanning assets during undesired time frames, such as during production hours. For more information about what happens to in-progress scans at the start of a freeze window, see the [knowledge base](#) article.

Freeze windows are organizational and affect all scans in the creating user's organization. Only users with the Manage Freeze Windows permission can add, edit, or delete freeze windows.

> **Note**: If a freeze window becomes active in Tenable Security Center after an Agent scan or a web app scan launches, the freeze window will not stop any Agent scans or web app scans that are currently in progress. However, if you launch a web app scan while a freeze window is already active, and the freeze window applies to any of the web app scan targets, then those web app scan targets will not be scanned.
>
> To stop Agent scans, configure a freeze window in each Tenable Nessus Manager.

For more information, see [Add a Freeze Window](#), [Edit a Freeze Window](#), and [Delete a Freeze Window](#).

Option	Description
Name	A name for the freeze window.
Description	(Optional) A description for the freeze window.
Enabled	When enabled, Tenable Security Center does not scan any assets that are affected by the freeze window. If a scan does not include any assets outside of the freeze window, then the scan will abort. When disabled, Tenable Security Center scans all assets as scheduled.
Targets	Specifies the targets you do not want to scan during the freeze window. • **All Systems** — Tenable Security Center does not scan any assets. • **Assets** — Tenable Security Center does not scan specific Tenable-provided or user-defined asset lists. • **IPs** — Tenable Security Center does not scan specific

Option	Description
	IP addresses.
	• **Mixed** — Tenable Security Center does not scan a combination of IP addresses and/or Tenable-provided or user-defined asset lists.
	Note: If you select an **Import Repository** later in the configuration, Tenable Security Center applies your **Target** selections only to scans configured with that import repository. Scans configured with other import repositories still run and scan targeted assets, regardless of your freeze window **Targets** selection.
Assets	If you selected **Assets** or **Mixed** as the **Targets**, specifies one or more Tenable-provided or user-defined asset lists that you do not want to scan during the freeze window.
IPs	If you selected **IPs** or **Mixed** as the **Targets**, specifies one or more asset IP addresses that you do not want to scan during the freeze window.
ImportRepository	(Optional) If you selected **Assets**, **IPs**, or **Mixed** as your **Targets**, specifies whether you want to restrict the freeze window to apply to scans configured with a specific import repository. • If you select a repository, Tenable Security Center applies the freeze window to scans with the repository configured. • If you do not select a repository, Tenable Security Center does not restrict the freeze by repository.
Starts On **Frequency** **Repeat Every** **Repeat On**	Specifies a schedule for the freeze window.

Add a Freeze Window

For more information about configuration options, see Freeze Windows.

To add a freeze window:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Scans** > **Freeze Windows**.

   The **Freeze Windows** page appears.

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

   The **Add Freeze Window** page appears.

4. In the **Name** box, type a name for the freeze window.

5. In the **Description** box, type a description for the freeze window.

6. Confirm the **Enabled** toggle is enabled.

7. In the **Targets** drop-down box, select a target: **All Systems**, **Assets**, **IPs**, or **Mixed**.

   Additional options appear based on the targets you specified.

8. In the **Assets** and/or **IPs** boxes, select or type targets for the freeze window.

9. (Optional) If you selected **Assets** or **Mixed** as the **Targets** and you want to restrict the freeze window by scan repository, in the **Repository** section, select a repository.

10. Modify the **Starts On**, **Frequency**, **Repeat Every**, and **Repeat On** options to set the schedule for the freeze window.

11. Click **Submit**.

    Tenable Security Center saves your configuration.

Edit a Freeze Window

For more information, see Freeze Windows.

To edit a freeze window:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Freeze Windows**.

   The **Freeze Windows** page appears.

3. Right-click the row for the freeze window you want to edit.

   The actions menu appears.

   -or-

   Select the check box for the freeze window you want to edit.

   The available actions appear at the top of the table.

4. Click **Edit**.

   The **Edit Freeze Window** page appears.

5. To disable the freeze window, click the **Enabled** slider.

6. To edit the freeze window settings, modify options described in Edit a Freeze Window.

7. Click **Submit**.

   Tenable Security Center saves your configuration.

Delete a Freeze Window

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Freeze Windows.

To delete a freeze window:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Freeze Windows**.

   The **Freeze Windows** page appears.

3. To delete a single freeze window:

a. In the table, right-click the row for the freeze window you want to delete.

The actions menu appears.

To delete multiple freeze windows:

a. In the table, select the check box for each freeze window you want to delete.

The available actions appear at the top of the table.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

Tenable Security Center deletes the freeze window.

Tags

You can use tags in Tenable Security Center to label assets, policies, credentials, or queries with a custom descriptor to improve filtering and object management. For example, you could add a tag named **East Coast Employees** to label all of your assets in that geographic area.

After you create a tag and apply it to an object, the tag is visible to all users who can view or modify that object. However, tags are not shared across object types.

For instructions on creating a new tag or adding an existing tag, see Add a Tag. For instructions on how to delete a tag, see Remove or Delete a Tag.

Add a Tag

Required Tenable Security Center User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Tags.

To add a tag:

1. Log in to Tenable Security Center.

2. Navigate to the assets, policies, credentials, or queries page:

- Click **Assets** > **Assets**. Tags are available on the **Assets** tab, not the **Host Assets** tab.

  > **Note:** The **Assets** page is available only to Security Manager users.

- Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

- Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

- Click **Analysis** > **Queries**.

3. Right-click the row for the asset, policy, credential, or query you want to tag.

   The actions menu appears.

   -or-

   Select the check box for the asset, policy, credential, or query you want to tag.

   The available actions appear at the top of the table.

4. Click **Edit**.

5. In the **Tag** drop-box, select an existing tag or type a new tag.

6. Click **Submit**.

   The tag appears, applied to the asset, policy, credential, or query.

Remove or Delete a Tag

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can remove a tag from an asset, policy, credential, or query to stop associating that object with the tag. To completely delete a tag from Tenable Security Center, you must remove the tag from all assets, policies, credentials, or queries. For more information, see Tags.

To remove a tag or completely delete a tag from Tenable Security Center:

1. Log in to Tenable Security Center via the user interface.

2. Navigate to the assets, policies, credentials, or queries page:

   - Click **Assets** > **Assets**.

   - Click **Scanning** > **Policies** (administrator users) or **Scans** > **Policies** (organizational users).

   - Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   - Click **Analysis** > **Queries**.

3. In the table, right-click the row for the asset, policy, credential, or query where you want to remove the tag.

   The actions menu appears.

4. Click **Edit**.

5. In the **Tag** drop-box, remove the tag from the asset, policy, credential, or query.

6. Click **Submit**.

   Tenable Security Center removes the tag from the asset, policy, credential, or query.

7. (Optional) If you want to delete the tag from Tenable Security Center, repeat steps 2 through 6 until you have removed all uses of the tag for the object type.

   Tenable Security Center deletes the tag.

Analyze Data

> **Note**: To enable cumulative vulnerability data analysis, add the repositories of your managed Tenable Security Center instances as Remote Repositories.

See the following sections to analyze and respond to Tenable Security Center data.

Analysis Tool	Description
Scan Results	View a table of scan results from active and agent scans.
Dashboards	View graphical summaries of scans, scan results, and system activity.
Solutions Analysis	View recommended solutions for all vulnerabilities on your network.
Vulnerability Analysis	View a table of cumulative or mitigated vulnerability data.
Event Analysis	View a table of Tenable Log Correlation Engine security event data.
Mobile Analysis	View a table of vulnerability data discovered by scanning an ActiveSync, Apple Profile Manager, AirWatch, Good, or MobileIron MDM server.
Reports	Create custom or template-based reports to export Tenable Security Center data for further analysis.
Assurance Report Cards	Create ARCs to develop security program objectives and assess your organization's security posture.

You can use Filters and Queries to manipulate the data you see in analysis tools and save views for later access. You can perform Workflow Actions (alerting, ticketing, accepting risk, recasting risk) from some analysis tools.

If you are licensed for Tenable Lumin, you can synchronize Tenable Security Center with Tenable Lumin to take advantage of Cyber Exposure features, as described in Tenable One Synchronization. For more information, contact your Tenable representative.

Dashboards

Required Tenable Security Center User Role: Administrator or organizational user with appropriate permissions. For more information, see User Roles.

Administrator users can view Tenable-provided **Overview** , **LCE Overview**, and **Health Overview** dashboards. For more information, see Overview Dashboard , LCE Overview Dashboard, and Health Overview Dashboard.

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). For a complete index of Tenable-provided dashboard templates, see the Tenable Security Center Dashboards blog.

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. For more information, see Scanning Overview.

Tip: Tenable Security Center automatically refreshes dashboard data once per day. To refresh all dashboard components on demand as an organizational user, click **Refresh All**.

For more information, see:

- View a Dashboard

- Add a Template-Based Dashboard

- Add a Custom Dashboard

- Import a Dashboard

- Manage Dashboards

- Manage Dashboard Components

Dashboard Options

Option	Description
General	
Name	The name of the dashboard.
Description	(Optional) A description for the dashboard.
Layout	The number and arrangement of dashboard columns.

View a Dashboard

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Dashboards.

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, as described in Add a Template-Based Dashboard Component or Add a Custom Dashboard Component.

      - Manage dashboard components on the dashboard in view, as described in Manage Dashboard Components.

- Edit the dashboard settings for the dashboard in view, as described in [Edit Settings for a Dashboard](#).

- Share or revoke access to the dashboard in view, as described in [Share or Revoke Access to a Dashboard](#).

- Create a report from the dashboard in view:

   a. In the upper-right corner of the page, click the **Options** drop-down box.

   b. Click **Send to Report**.

   For more information about reports, see [Reports](#).

- Delete the dashboard in view, as described in [Delete a Dashboard](#).

- Customize the table, as described in [Interact with a Customizable Table](#).

Overview Dashboard

Tenable provides the **Overview** dashboard to administrator users by default. For more information, see [View a Dashboard](#).

Widget	Action
Licensing Status How close am I to hitting my license limit?	View a graph of your total license size compared to your total currently active IP addresses.
Web App Scanning FQDNs How close am I to hitting my license limit?	View a graph of your total license size compared to your total currently active FQDNs. For more information about web app scans, see [Web App Scans](#).
Repository Statistics How am I using my repositories?	View information about your repositories: • **Name** — The name of the repository. • **Vuln Count** — The number of vulnerability instances in the repository. **Tip:** A vulnerability instance is a single instance of a

Widget	Action
	vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol. • **Last Update** — The date and time of the most recent scan that updated the repository data. • **IP/Device Count** — The number of IP addresses in the repository counting toward your Tenable Security Center license. • **Type** — The repository type. • **Data Format** — The type of data stored in the repository: **IPv4**, **IPv6**, **Mobile**, or **Agent**.
System Status Is the Tenable Security Center job daemon running?	• View the status of the job daemon, which powers the job queue. • To change the status of the job daemon, click **Start** or **Stop**. Tenable Security Center changes the status of the job daemon.
Scanner Status What is the status of my scanners?	View information about your scanners: • **Name** — The name of the scanner or instance. • **Type** — The type of connection: **Passive** or **Active**. • **Status** — The status of the scanner or instance.
Latest Plugins What plugins were most recently changed in a feed update?	View information about the latest plugin changes in feed updates. • **ID** — The plugin ID. • **Name** — The name of the plugin. • **Family** — The plugin family.

Widget	Action
	• **Type** — The plugin type. • **Date** — The date and time of the feed update that contained the plugin change.

Health Overview Dashboard

Tenable provides the **Health Overview** dashboard to administrator users by default. For more information, see View a Dashboard.

Widget	Action
Application Configuration Health What is the health of my application configuration?	View information about the health of your application with the following checks: • **License Expiration Warning** — When a Tenable Security Center license expires, you may not be able to update plugins, receive Feed updates or access the tool. • **Percent Licenses Used** — When a Tenable Security Center console reaches it's license limit, scans of additional assets will not be imported. • **SMTP Configured** — If misconfigured, invalid SMTP settings will prevent Tenable Security Center from being able to send emails notifying users of events. • **Maximum Recommended LCE Imports Per Day (200)** — Tenable Log Correlation Engine job imports should be managed to reduce impact on other scan imports. • **Maximum Recommended NNM Imports Per Day (200)** — Nessus Network Monitor job imports should be managed to reduce impact on other scan imports. • **Maximum Recommended Nessus Scanners (250)** — You may experience degraded performance when a large quantity of Nessus Scanners are attached to Tenable Security Center.

Widget	Action
	• **Maximum Recommended Repositories (200)** — You may experience degraded performance when a large quantity of Repositories are configured in Tenable Security Center. See the [Tenable Security Center Large Enterprise Deployment Guide](#) for more information. • **Maximum Recommended Scan Zones (100)** — You may experience degraded performance when a large quantity of Scan Zones are configured in Tenable Security Center. See the [Tenable Security Center Large Enterprise Deployment Guide](#) for more information. • **Passive Activation Code Configured** (Requires Tenable Security Center+ license) — Tenable Security Center+ consoles should have a passive activation code applied. This allows usage of Nessus Network Monitor Sensors for more than Asset Discovery.
Repository Size Warning What is the size of each of my repositories?	View information about the size of your repositories.
Job Queue Health Summary What is the health of my job queue?	View information about the health of your job queue: • **Job Delay** — Jobs that have been delayed by more than an hour since their scheduled run time. • **Pending Jobs** — Jobs that are scheduled to run in the future. If too many jobs are scheduled, you may experience delays in processing vulnerability data, generating reports, or other processes.
Refine Scan Zone Scope	View information about the size of your scan zones.

Widget	Action
What is the size of each of my scan zones?	
Job Queue Delay Details Why were there delays in the job queue?	View information about delays in the job queue.
Scan Zones with Overlap Do I have scan zones that overlap each other?	View information about the size of your scan zones, and whether they have overlapping boundaries.
Non-Working Scanners Are there any non-working scanners in my configuration?	View information about non-working scanners in your scan zones.
Maximum Recommended Scanners in a Zone What is the maximum number of scanners I should have in my scan zones?	View information about the maximum suggested number of scanners for each of your scan zones.
Nessus Agent Managers as Network Scanners Are there any Nessus	View a list of Nessus Agent Managers currently configured to use as Network Scanners.

Widget	Action
Agent Managers being used as Network Scanners?	
Degraded Scan Zones Which scan zones have non-working scanners?	View information about scan zones with non-working scanners.
Nessus Agent Managers Not Using API Authentication Are there any Nessus Agent Managers not configured to use API authentication?	View a list of Nessus Agent Managers not configured to use API keys.
Large Asset Lists Are there any large asset lists that may contribute to performance issues?	View lists of assets with more than 20,000 characters.

LCE Overview Dashboard

Tenable provides the **LCE Overview** dashboard to administrator users by default. For more information, see <u>View a Dashboard</u>.

Widget	Action
LCE Status What is the status of my Tenable Log Correlation Engine servers?	View information about your Tenable Log Correlation Engine server: • **Name** — The name of the Tenable Log Correlation Engine server. • **Status** — The status of the Tenable Log Correlation

Widget	Action
	Engine server.
LCE Client Status What is the status of my Tenable Log Correlation Engine clients?	View information about your Tenable Log Correlation Engine clients: • **Client IP** — The IP address of the Tenable Log Correlation Engine client. • **LCE** — The Tenable Log Correlation Engine server associated with the Tenable Log Correlation Engineclient. • **Last Update** — The date and time of the most recent Tenable Log Correlation Engine client import to Tenable Security Center. • **Status** — The status of the Tenable Log Correlation Engine client.

Set a Dashboard as Your Default Dashboard

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Dashboards.

To set a dashboard as your default 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.

4. In the upper-right corner of the page, click the **Options** drop-down box.

5. Click **Set as Default**.

The system sets the dashboard as your default.

Add a Template-Based Dashboard

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can add a dashboard by configuring a Tenable-provided dashboard template. To add a custom dashboard instead, see Add a Custom Dashboard. To import a dashboard, see Import a Dashboard.

For more information, see Dashboards and Dashboard and Component Templates.

To add a template-based dashboard:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Dashboard** > **Dashboard**.

   The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Options** drop-down button.

4. Click **Add Dashboard**

   The **Dashboard Templates** page appears.

5. In the **Common** section, click a template category tile.

   The **Add Dashboard Template** page appears.

6. Click a template.

   The **Add Dashboard Template** page updates to reflect the template you selected.

7. Modify the dashboard template:

- To edit the dashboard name, click the name box and edit the name.

- To edit the dashboard description, click the **Description** box and edit the description.

- To restrict the target data displayed in the dashboard, click the **Targets** drop-down box.

- To edit the dashboard refresh schedule, click the **Schedule** link.

8. Click **Add**.

   Tenable Security Center saves your configuration and the **Dashboards** page appears.

9. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.

10. Click the name of the dashboard you just created.

    The page for the dashboard appears.

What to do next:

- Add dashboard components, as described in Add a Template-Based Dashboard Component or Add a Custom Dashboard Component.

Add a Custom Dashboard

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can add a fully customized dashboard. To add a dashboard from a Tenable-provided template instead, see Add a Template-Based Dashboard.

For more information, see Dashboards.

To add a custom dashboard:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Dashboard** > **Dashboard**.

   The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Options** drop-down button.

4. Click **Add Dashboard**

The **Dashboard Templates** page appears.

5. In the **Other** section, click the **Advanced** tile.

6. In the **Name** box, type a name for the dashboard.

7. In the **Description** box, type a description for the dashboard.

8. In the **Layout** section, select the layout you want to use for the dashboard.

9. Click **Submit**.

   Tenable Security Center saves your configuration and the **Dashboards** page appears.

10. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.

11. Click the name of the dashboard you just created.

   The page for the dashboard appears.

What to do next:

- Add dashboard components, as described in Add a Template-Based Dashboard Component or Add a Custom Dashboard Component.

Dashboard and Component Templates

Tenable Security Center provides a selection of dashboards and dashboard component templates. You can configure a Tenable-provided dashboard template or you can create a fully customized dashboard. For more information, see Dashboards and Custom Dashboard Component Options.

For a complete index of Tenable-provided report templates, see the Tenable Security Center Dashboards blog.

Template	Description
Common	
Compliance & Configuration Assessment	Dashboards that aid with configuration, change, and compliance management.
Discovery & Detection	Dashboards that aid in trust identification, rogue detection, and new device discovery.

Executive	Dashboards that provide operational insight and metrics geared towards executives.
Monitoring	Dashboards that provide intrusion monitoring, alerting, and analysis.
Security Industry Trends	Dashboards related to trends, reports, and analysis from industry leaders.
Threat Detection & Vulnerability Assessments	Dashboards that aid with identifying vulnerabilities and potential threats.
Other (Dashboards)	
Advanced	A custom dashboard with no pre-configured settings.
Import	Import a dashboard. For more information, see Import a Dashboard.
Other (Dashboard Components)	
Table	Add a table to your dashboard.
Bar Chart	Add a bar chart to your dashboard.
Pie Chart	Add a pie chart to your dashboard.
Matrix	Add a matrix to your dashboard.
Line Chart	Add a line chart to your dashboard.
Area Chart	Add an area chart to your dashboard.

Import a Dashboard

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Dashboards.

To import a dashboard:

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard**.

   The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Options** drop-down button.

4. Click **Add Dashboard**

   The **Dashboard Templates** page appears.

5. In the **Other** section, click **Import**.

   The **Import Dashboard** page appears.

6. In the **Name** box, type a name for the dashboard.

7. Click **Choose File** and browse to the dashboard file you want to import.

8. Click **Submit**.

   Tenable Security Center imports the dashboard.

Manage Dashboards

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Dashboards.

To manage dashboards:

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard** > **Dashboard**.

   The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Options** drop-down button.

4. Click **Manage Dashboards**

   The **Manage Dashboards** page appears.

5. To add a dashboard, click **Add**. For more information, see [Add a Template-Based Dashboard](#) or [Add a Custom Dashboard](#).

6. To filter the dashboards in the table, see [Apply a Filter](#).

7. To manage a single dashboard, right-click the dashboard.

   -or-

   To manage multiple dashboards, select the check box for the dashboard.

   The actions menu appears.

   From this menu, you can:

   - Click **View** to view details for the dashboard.

   - Click **Share** to share or revoke access to the dashboard.

   - Click **Export** to download an XML version of the dashboard.

   - Click **Copy** to copy the dashboard.

   - Click **Edit** to edit the dashboard.

   - Click **Hide from Dashboard** to hide the dashboard from the **Switch Dashboard** drop-down on the **Dashboards** page.

   - Click **Show on Dashboard** to show the dashboard on the **Switch Dashboard** drop-down on the **Dashboards** page.

   - Click **Delete** to delete the dashboard.

To export the dashboard as an XML file:

a. Click **Export**.

b. Then, identify how you want Tenable Security Center to handle object references:

   - **Remove All References** – all object references are removed, altering the definitions of the components. Importing users do not need to make any changes for components to be useable.

- **Keep All References** – object references are kept intact. Importing users must be in the same organization and have access to all relevant objects for the components to be useable.

- **Replace With Placeholders** – object references are removed and replaced with their respective names. Importing users see the name of the reference object, but need to replace it with an applicable object within their organization before the component is useable.

Note: Due to version-specific changes in dashboard XML file formats, exported dashboards are not always compatible for import between Tenable Security Center versions.

Edit Settings for a Dashboard

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Dashboards.

To edit the settings for 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.

4. In the upper-right corner of the page, click the **Options** drop-down box.

5. Click **Edit Dashboard**.

   The **Edit Dashboard** page appears.

6. Edit the **Name**, **Description**, or **Layout**.

7. Click **Submit**.

   Tenable Security Center saves your configuration.

Share or Revoke Access to a Dashboard

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can share access to a dashboard to give users in a group the ability to view the dashboard. The user's role and custom permissions determine if they can drill down into other pages with more information. For more information, see Dashboards.

To share or revoke access to 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.

4. In the upper-right corner of the page, click the **Options** drop-down box.

5. Click **Share**.

   The **Share Dashboard** window appears.

6. In the box, search for and select the groups for which you want to share or revoke access.

7. Click **Submit**.

   Tenable Security Center saves your configuration.

Delete a Dashboard

For more information, see Dashboards.

To delete 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.

4. In the upper-right corner of the page, click the **Options** drop-down box.

5. Click **Delete**.

    A confirmation window appears.

6. Click **Delete**.

    The system deletes the dashboard.

Manage Dashboard Components

For more information, see Dashboards.

To manage dashboard components:

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard** > **Dashboard**.

    The **Dashboards** page appears.

To edit a dashboard component:

1. Hover over the dashboard component.

2. Click the ••• menu.

   The actions menu appears.

3. Click **Edit**.

4. Edit the dashboard component options. For more information, see Custom Dashboard Component Options.

To view the data behind a dashboard component:

1. Hover over the dashboard component.

2. In the lower right corner, click **View Data**.

   The analysis page appears.

   > **Note:** Only dashboard components that display vulnerability analysis or event analysis data support viewing the data behind a dashboard component.

To reorder a dashboard component:

1. Click the title of a dashboard component.

2. Drag the dashboard component around the page.

To copy a dashboard component to the dashboard in view or a different dashboard:

1. Hover over the dashboard component.

2. Click the ••• menu.

   The actions menu appears.

3. Click **Copy**.

4. In the **Name** box, edit the name for the copied dashboard component.

5. In the **Dashboard** drop-down box, click the name of the dashboard where you want to copy the dashboard component.

6. Click **Copy**.

Tenable Security Centercopies the dashboard component.

To refresh the dashboard component data:

1. Hover over the dashboard component.

2. Click the ••• menu.

   The actions menu appears.

3. Click **Refresh**.

   Tenable Security Centerrefreshes the dashboard component data.

To delete the dashboard component:

1. Hover over the dashboard component.

2. Click the ••• menu.

   The actions menu appears.

3. Click **Delete**.

   A confirmation window appears.

4. Click **Delete**.

   Tenable Security Center deletes the dashboard component.

Add a Template-Based Dashboard Component

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions.
> For more information, see User Roles.

You can add a dashboard component by configuring a Tenable-provided dashboard component template. To add a custom dashboard component instead, see Add a Custom Dashboard Component.

For more information, see Dashboards and Dashboard and Component Templates.

Before you begin:

- Add a dashboard, as described in <u>Add a Template-Based Dashboard</u>, <u>Add a Custom Dashboard</u>, or <u>Import a Dashboard</u>.

To add a template-based dashboard component to a dashboard:

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard**.

   The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.

4. Click the name of the dashboard for which you want to add a component.

   The dashboard appears.

5. In the upper-right corner of the page, click the **Options** drop-down box.

6. Click **Add Component**.

   The **Component Templates** page appears.

7. In the **Common** section, click the template you want to use for the dashboard component.

   The **Add Component Template** page updates to reflect the template you selected.

8. Modify the dashboard component template:

   - To edit the dashboard component name, click the name box and edit the name.

   - To edit the dashboard component description, click the **Description** box and edit the description.

   - To restrict the target data displayed in the dashboard component, click the **Targets** drop-down box.

   - To edit the dashboard component refresh schedule, click the **Schedule** link.

9. Click **Add**.

   Tenable Security Center saves your configuration and the **Dashboards** page appears.

Add a Custom Dashboard Component

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can configure a custom dashboard component to add a table, bar chart, pie chart, line chart, area chart, or matrix to a dashboard. For more information, see Dashboards and Dashboard and Component Templates.

For an example matrix component configuration, see Configure a Simple Matrix Dashboard Component.

Before you begin:

- Add a dashboard, as described in Add a Template-Based Dashboard, Add a Custom Dashboard, or Import a Dashboard.

To add a custom dashboard component to a dashboard:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Dashboard**.

   The **Dashboards** page appears.

3. In the upper-right corner of the page, click the **Switch Dashboard** drop-down box.

4. Click the name of the dashboard for which you want to add a component.

   The dashboard page appears.

5. In the upper-right corner of the page, click the **Options** drop-down box.

6. Click **Add Component**.

   The **Component Templates** page appears.

7. In the **Other** section, click the type of component you want to configure.

   The component configuration page appears.

8. Configure the options for your component type, as described in Custom Dashboard Component Options.

9. Click **Submit**.

   Tenable Security Center saves your configuration.

Custom Dashboard Component Options

Use the following options to configure custom dashboard components. For more information about dashboard component types, see Dashboard and Component Templates.

Tenable Security Center supports the following custom dashboard components:

- Table Component Options

- Bar Chart Component Options

- Pie Chart Component Options

- Matrix Component Options

- Line and Area Chart Component Options

General Options

Configure the following options for all custom dashboard component types.

Option	Description	Default
Name	(Required) A name for the dashboard component.	--
Description	A description for the dashboard component. The description appears on the **Dashboards** page when you hover over a dashboard component.	--
Schedule	(Required for all except **Matrix** components) Specifies how often the component polls the data source to obtain updates: • **Never** — The component never polls the data source. • **Minutely** — Polls every 15, 20, or 30 minutes. • **Hourly** — Polls every 1, 2, 4, 6, or 12 hours. • **Daily** — Polls daily or every specified number of days at the specified time. • **Weekly** — Polls weekly or every specified number of weeks at the specified time.	Daily

Option	Description	Default
	• **Monthly** — Polls monthly or every specified number of months at the specified day and time.	
	Caution: Excessively frequent updates may cause the application to become less responsive due to the added processing load imposed on the host OS.	

Table Component Options

Option	Description	Default
Data		
Type	The type of data: **Vulnerability**, **Event**, **Mobile**, **User**, **Ticket**, or **Alert**.	Vulnerability
Query	Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or as a template on which to base the **Filters** option.	--
Source	(If **Type** is **Vulnerability** or **Event**) Specifies the data source. For vulnerability data, select **Cumulative** or **Mitigated**. For event data, the data source is **Active**. Tenable Security Center can use only active event data for event-based components.	Cumulative
Tool	The analysis tool to use for creating the chart. For more information, see Vulnerability Analysis Tools and Event Analysis Tools.	Vulnerability Summary
Filters	Additional filters to use on the data source. For more information, see Filters.	--
Display		

Option	Description	Default
Results Displayed	The number of displayed results. You can choose to display up to 999 results. If the **Viewport Size** setting is smaller than this setting, the results display is limited to the **Viewport Size** setting with a scrollbar to display the additional results.	10
Viewport Size	The number of records (maximum: 50) to display along with a scrollbar to handle additional records. For example, if **Results Displayed** is set to **100** and **Viewport Size** is **15**, 15 records are displayed with a scrollbar to view the additional 85 records.	10
Sort Column	(Not available if **Type** is **Event**) The column Tenable Security Center uses to sort the results.	Plugin ID
Sort Direction	(Not available if **Type** is **Event**) The sort direction: **Descending** or **Ascending**.	Descending
Display Columns	The columns to display in the component output.	--

Bar Chart Component Options

Option	Description	Default
Data		
Type	The type of data: **Vulnerability**, **Event**, **Mobile**, or **Ticket**.	Vulnerability
Query	Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or as a template on which to base the **Filters** option.	--
Source	(If **Type** is **Vulnerability** or **Event**) Specifies the data source.	Cumulative

Option	Description	Default
	For vulnerability data, select **Cumulative** or **Mitigated**. For event data, the data source is **Active**. Tenable Security Center can use only active event data for event-based components.	
Tool	The analysis tool to use for creating the chart. For more information, see Vulnerability Analysis Tools and Event Analysis Tools.	Vulnerability Summary
Filters	Additional filters to use on the data source. For more information, see Filters.	--
Display		
Results Displayed	The number of displayed results. You can choose to display up to 100 results.	10
Sort Column	(If **Type** is **Vulnerability** or **Ticket**) The column Tenable Security Center uses to sort the results.	Plugin ID
Sort Direction	(If **Type** is **Vulnerability** or **Ticket**) The sort direction: **Descending** or **Ascending**.	Descending
Display Column	The columns to display in the component output.	--

Pie Chart Component Options

Option	Description	Default
Data		
Type	The type of data: **Vulnerability**, **Event**, **Mobile**, or **Ticket**.	Vulnerability
Query	Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or as a template on which to base the **Filters** option.	--

Option	Description	Default
Source	(If **Type** is **Vulnerability** or **Event**) Specifies the data source.	Cumulative
	For vulnerability data, select **Cumulative** or **Mitigated**.	
	For event data, the data source is **Active**. Tenable Security Center can use only active event data for event-based components.	
Tool	The analysis tool to use for creating the chart. For more information, see [Vulnerability Analysis Tools](#) and [Event Analysis Tools](#).	Vulnerability Summary
Filters	Additional filters to use on the data source. For more information, see [Filters](#).	--
Display		
Results Displayed	The number of displayed results.	10
Sort Column	The column Tenable Security Center uses to sort the results.	Plugin ID
Sort Direction	The sort direction: **Descending** or **Ascending**.	Descending
Display Column	The columns to display in the component output.	--

Matrix Component Options

For information about configuring matrix components and to download samples, visit the [Tenable Security Center Dashboards](#) blog. For an example matrix component, see [Configure a Simple Matrix Dashboard Component](#).

When you create a matrix component, you define rules to determine what displays in each cell in a table of customizable columns and rows.

- Use columns to define a group of vulnerability, mobile, event, ticket, user, or alert data. For example, you could create columns for critical, high, medium, low, and informational vulnerabilities.

- Use rows to define the operations performed against each column element for that row. For example, if each column determines the vulnerability type (critical, high, medium, low, and informational), you can create a row to calculate the ratio of the particular vulnerability type count against the total vulnerability count.

By default, each cell definition includes a single customizable rule that defines what appears in the cell if no other conditions have been defined or triggered.

Tenable Security Center reviews each rule in a cell from top to bottom and triggers the display rule on the first rule match. Once a rule triggers, Tenable Security Center stops reviewing rules for the cell. If none of the added rules match, Tenable Security Center performs the default rule.

Option	Action
Cells	
Size	Use the drop-down menus to select the number of columns and rows for the matrix. Tenable Security Center supports matrices from 1x1 to 10x10. Click **Generate Cells** create a blank matrix with customizable cells.
••• icon	Click the ••• icon in a row or column header cell to manage the column or row. • To edit the header name or refresh frequency, click **Edit Header**. **Tip:** You can choose to refresh the data more often to see the most current view. However, frequent refreshes can cause slow system performance. • To delete the row or column, click **Delete Cells**. Tenable Security Center deletes the row or column. • To copy the row or column, click **Copy**. Tenable Security Center copies the row or column.
✏ icon	Click the ✏ icon inside a cell to configure rules for the cell. For more information, see Matrix Component Query Options.

Matrix Component Query Options

Option	Description	Default
Data		
Data Type	The type of data: **Vulnerability**, **Mobile**, **Event**, **User**, **Alert**, or **Ticket**. The **Data Type** determines which query values are available in the **Condition** option.	Vulnerability
Type	The matrix component display type: **Count** or **Ratio**	Count
Source	(If **Data Type** is **Vulnerability** or **Event**) Specifies the data source. For vulnerability data, select **Cumulative** or **Mitigated**. For event data, the data source is **Active**. Tenable Security Center can use only active event data for event-based components.	Cumulative
Filters	(If **Type** is **Count**) Additional filters to use on the data source. For more information, see Filters.	--
Numerator Filters	(If **Type** is **Ratio**) The filters to apply to the ratio numerator. For more information, see Filters.	--
Denominator Filters	(If **Type** is **Ratio**) The filters to apply to the ratio denominator. For more information, see Filters.	--
Rules		
Condition	Specifies the conditions for the matrix component. Use the drop-down menus to define the quantity and query value to use for the rule. Quantities: **Less than or equal to**, **Greater than or equal to**, **Exactly**, or **Not Equal to**. Query values: **Events**, **Hosts**, **Vulnerabilities**, **Ports**,	--

Option	Description	Default
	Devices, **Users**, **Alerts**, or **Tickets**. **Note:** The available query values depend on the **Data Type**.	
Display	Specifies the appears of the matrix component when the rule **Condition** is met. • **Text** — Displays the **Query Value** or custom **User-Defined** text. • **Icon** — Displays the selected indicator icon. • (If **Type** is **Ratio**) **Indicator** — Displays a percentage.	Text
Text Color	(If **Display** is **Text**) The matrix component text color.	#1a1a40
Background	(If **Display** is **Text**) The matrix component background color.	#333333 or #ffffff

Line and Area Chart Component Options

Option	Description	Default
Data		
Date Type	The date type: • **Relative** — A date relative to the current time when the chart is loaded. • **Absolute** — An absolute time frame that is the same on each page visit.	Relative
Date Range	The date range for the line or area chart. If **Date Type** is **Relative**, select from the following options: • **Within x Minutes** — Display data within the last 15, 20, or 30	Within 24 Hours

Option	Description	Default
	minutes. • **Within *x* Hours** — Display data within the last 1, 2, 4, 6, 12, 24, 48, or 72 hours. • **Within *x* Days** — Display data within the last 5, 7, 25, or 50 days. • **Within *x* Months** — Display data within the last 3 or 6 months. • **Within 1 Year** — Display data within the last year. If **Date Type** is **Absolute**, select a date and time for the beginning and end of the range.	
Series	Click to add a series to the line or area chart. For more information, see [Line and Area Chart Series Options](#).	--

Line and Area Chart Series Options

Option	Description	Default
Name	The name of the series.	--
Data		
Data Type	The type of data: **Vulnerability** or **Event**. > **Note:** For line/area charts, vulnerability data analysis often requires that the underlying repository be a trending repository. If the selected repository is not a trending repository, no historical analysis is available.	Vulnerability
Query	Predefined query used to further narrow down the data source options. If a query does not exist or is not desired, it may be left unselected. The query may be used as is or as a template on which to base the **Filters** option.	--
Filters	Additional filters to use on the data source. For more	--

	information, see Filters.	
Display		
Series Data	Data to display in the chart: **Total**, **Info**, **Low**, **Medium**, **High**, or **Critical**.	All

Configure a Simple Matrix Dashboard Component

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Dashboards and Matrix Component Options.

Before you begin:

- Begin adding a custom matrix dashboard component, as described in Add a Custom Dashboard Component.

To construct a simple matrix dashboard component:

1. On the **Add Matrix Component** page, in the **Name** box, type a name for the dashboard component.

2. Type a **Description** for the dashboard component.

3. In the **Cells** section, select the number of **Columns** and **Rows** for the matrix.

Add Matrix Component

Name*   Exectuive 7 Day - Exploitable Vulnerability

Description   Percentages of hosts with exploitable
vulnerabilities over the last 7 day and
the frameworks that can be used to
exploit them.

Cells

Size*   5 ▼   Columns x   3 ▼   Rows   Generate Cells

Submit   Cancel

For example, 5 columns and 3 rows.

4. Click **Generate Cells**.

   The matrix editor appears.

5. Next to the header label, click the ••• menu.

   The actions menu appears.

6. Click **Edit Header**.

7. Type a **Label** for the column or row header.

8. Click **Submit**.

   The matrix editor appears, with the new header label displayed.

Cells

	Exploit %	Metasploit	Core Impact	Canvas	Malware
Critical					
High					
Medium					

Submit   Cancel

9. Repeat the header label steps for the other header cells.

10. Hover over the body cells and click the edit icon.

    The **Add Matrix Component** page appears.

11. Customize the matrix component options.

    For example, this matrix component displays Vulnerability data by a ratio from the Cumulative database. The numerator filters are looking for vulnerabilities that have an exploit available with a Critical severity discovered within the last 7 days. The Denominator filters are for vulnerabilities that have a Critical severity discovered within the last 7 days. The rules are looking for percentages of the vulnerabilities that match and designate the ratio value with the corresponding color based on the percentages found.

Add Matrix Component

Data

Data Type	Vulnerability ▾
Type	Ratio ▾
Source*	Cumulative ▾

Numerator Filters

Exploit Available	Yes
Severity	Critical
Vulnerability Discovered	Within the last 7 days

+ Add Filter

Denominator Filters

Severity	Critical
Vulnerability Discovered	Within the last 7 days

+ Add Filter

Rules

Greater than or equal to 50 % of Vulnerabilities match	Display	Ratio Value: Vulnerabilities
Greater than or equal to 10 % of Vulnerabilities match	Display	Ratio Value: Vulnerabilities
Greater than or equal to 1 % of Vulnerabilities match	Display	Ratio Value: Vulnerabilities
Default	Display	Ratio Value: Vulnerabilities

+ Add Rule

Submit   Cancel

12. Repeat the body cell steps for the other body cells.

In the example above, the other cells are similar with many of the same rules. The differences are adding a Numerator filter to include the Exploit Framework we are looking for and a Denominator filter for the Exploit Available option.

Cells

	Exploit %	Metasploit	Core Impact	Canvas	Malware
Critical	▼≡	▼≡	▼≡	▼≡	▼≡
High	▼≡	▼≡	▼≡	▼≡	▼≡
Medium	▼≡	▼≡	▼≡	▼≡	▼≡

Submit   Cancel

13. Click **Submit**.

The matrix element appears.

Interact with a Customizable Table

To interact with a customizable table:

1. Log in to Tenable Security Center via the user interface.

2. View a customizable table.

3. Do any of the following:

Navigate the table:

- To adjust the sort order, click a column title.

  Tenable Security Center sorts all pages of the table by the data in the column that you selected.

- To view all action buttons available in a single row, right-click the row:

  A drop-down menu appears with all the available actions.

- To navigate to another page of the table, click the arrows:

Button	Action
«	Navigate to the first page of the table.
»	Navigate to the last page of the table.
›	Navigate to the next page of the table.
‹	Navigate to the previous page of the table.

  ○ Click any row to navigate to another page to view more details.

  ○ On the **Dashboard** page, click any plugin ID to view the **Plugin ID** pane.

- To change the column order, drag and drop a column header to another position in the table.

- Remove or add columns:

    1. Roll over any column.

       The ☰ appears in the header.

    2. Click the ☰ button.

       A column selection box appears.

    3. Select or clear the check box for any column you want to show or hide in the table.

       Tenable Security Center updates the table based on your selection.

- Adjust column width:

    a. Roll over the header between two columns until the resize cursor appears.

       Click and drag the column width to the desired width.

- To sort data in the table, click a column header.

  Tenable Security Center sorts all pages of the table by the data in the column you selected.

Scan Results

The **Scan Results** page displays scan results and statuses from active scans, agent scans, and agent synchronization jobs .

> **Note:** Tenable Security Center does not include all agent scans in the scan results table. If an agent scan imports scan results identical to the previous agent scan, Tenable Security Center omits the most recent agent scan from the scan results table.

> **Note:** If you added the parent node of a Tenable Nessus Manager cluster as a scanner in Tenable Security Center, Tenable Security Center displays scan results for all child nodes. For more information, see Clustering in the *Tenable Nessus User Guide*.

> **Note:** For each agent synchronization job result for a child node, Tenable Security Center imports a metadata record containing no vulnerability data. This metadata record appears as a

second result on the **Scan Results** page. To prevent Tenable Security Center from importing the metadata file, configure and launch agent scans from Tenable Security Center, as described in Agent Scans.

For more information, see Manage Scan Results and Scan Result Statuses.

Scan Result Statuses

You can view the scan status and the import status for all scan results, as described in View Scan Result Details.

- Scan Status

- Import Status

Scan Status

The scan status specifies the status of the scan.

Status	Description
Active Scans	
Queued	The scan is queued.
Preparing	Tenable Security Center is preparing to run the scan.
Resolving Hostnames	Tenable Security Center is resolving hostnames before running the scan.
Verifying Targets	Tenable Security Center is verifying targets before running the scan.
Initializing Scanners	Tenable Security Center is initializing scanners before running the scan.
Running	The scan is running.
Pausing	You paused the scan and Tenable Security Center is pausing the scan.
Paused	The scan is paused.
Resuming	You resumed the scan and Tenable Security Center is resuming the scan.

Status	Description
Stopping	Tenable Security Center is stopping the scan.
Completed	The scan finished successfully.
Partial	The scan finished and some results are available.
Error	The scan did not finish.
Agent Scans	
Queued	The scan is queued.
Running	The scan is running.
Completed	The scan finished successfully.
Error	The scan did not finish.

Import Status

The scan status specifies the status of the scan result import to Tenable Security Center.

Status	Description
Active and Agent Scans	
No Results	The scan finished successfully but yielded no results.
Import Pending	Tenable Security Center is preparing to start the import.
Importing	Tenable Security Center is importing the scan result data.
Finished	The import finished successfully.
Blocked	Tenable Security Center did not import the scan result for one of the following reasons: • You have exceeded your license limit. • The scan result import would cause you to exceed your license.

Status	Description
	For more information about license limits, see [License Requirements](#).
Error	The import did not finish.

Manage Scan Results

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

Depending on the state of a scan result, you can perform different management actions (for example, you cannot download results for a scan with errors).

For more information, see [Scan Results](#).

To manage scan results:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Scan Results**.

   The **Scan Results** page appears.

3. Manage the results:

   To filter the scan results:

   - Click the filter icon.

     Filters allow you to view only desired scan results. Filter parameters include:

     - **Access** – filters by whether the scan is manageable or usable.

     - **Group** – filters by the groups that can access the scans.

     - **Name** – filters by the scan name.

     - **Owner** – filters by the scan owner.

     - **Scan Policy** – filters by the scan policy.

     - **Status** – filters by the scan status.

- **Time (Created)** - filters by when the scan result was created.

- **Time (Finished)** - filters by when the scan finished running.

- **Type** - filters by the type of scan.

To remove all filters:

- Under the filter options, click **Clear Filters**.

> **Note:** To return to the default filter for your user account, refresh your browser window. The number in grey next to the filter displays how many filters are currently in use.

To view a set of scan results:

a. Right-click the row for the scan.

The actions menu appears.

-or-

Select the check box for the scan.

The available actions appear at the top of the table.

b. Select **Browse**.

The Vulnerability Summary analysis tool appears, populated with data from the scan.

To view scan result details for a set of scan results:

a. Right-click the row for the scan.

The actions menu appears.

-or-

Select the check box for the scan.

The available actions appear at the top of the table.

b. Click **View**.

The **View Scan Result** page appears. For more information, see Scan Result Details.

To download the results of a scan:

a. Right-click the row for the scan.

    The actions menu appears.

    -or-

    Select the check box for the scan.

    The available actions appear at the top of the table.

b. Select **Download**.

> **Tip:** On a standard scan, you can download a Tenable Nessus results file. If the scan contains SCAP results, you can use an additional option to download the SCAP results.

To manually import scans listed on the scan results page:

a. Right-click the row for the scan.

    The actions menu appears.

    -or-

    Select the check box for the scan.

    The available actions appear at the top of the table.

b. Select **Import**.

> **Tip:** This option is useful for cases where a scan may have not fully imported after completion. For example, if Tenable Security Center blocked a scan because importing it would have exceeded the licensed IP address count, you can increase the IP address count, then import the scan results previously not imported.

To share scan results with other users:

a. Right-click the row for the scan.

    The actions menu appears.

    -or-

Select the check box for the scan.

The available actions appear at the top of the table.

b. Select **Copy**.

Selecting a **Group** from the drop-down box displays a list of users from that group. You can select one or more users from the list.

To send a copy of the scan results to users without access to Tenable Security Center:

a. Right-click the row for the scan.

The actions menu appears.

-or-

Select the check box for the scan.

The available actions appear at the top of the table.

b. Select **Email**.

To generate a report for the scan results based off a preconfigured report:

a. Right-click the row for the scan.

The actions menu appears.

-or-

Select the check box for the scan.

The available actions appear at the top of the table.

b. Select **Send to Report**.

Tenable Security Center sends the scan results to a report.

To upload Tenable Nessus scan results performed by other systems:

- See Upload Scan Results.

To pause or resume a running scan:

- In the row for the scan, click the pause or play button, as described in [Start or Pause a Scan](#).

To delete a set of scan results from Tenable Security Center:

a. Right-click the row for the scan.

   The actions menu appears.

   -or-

   Select the check box for the scan.

   The available actions appear at the top of the table.

b. Select **Delete**.

   Tenable Security Center deletes the scan results.

View Scan Results

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information, see [Scan Results](#).

> **Note:** Tenable Security Center does not include all agent scans in the scan results table. If an agent scan imports scan results identical to the previous agent scan, Tenable Security Center omits the most recent agent scan from the scan results table.

> **Note:** If you added the parent node of a Tenable Nessus Manager cluster as a scanner in Tenable Security Center, Tenable Security Center displays scan results for all child nodes. For more information, see [Clustering](#) in the *Tenable Nessus User Guide*.

> **Note:** For each agent synchronization job result for a child node, Tenable Security Center imports a metadata record containing no vulnerability data. This metadata record appears as a second result on the **Scan Results** page. To prevent Tenable Security Center from importing the metadata file, configure and launch agent scans from Tenable Security Center, as described in [Agent Scans](#).

To view a list of scan results:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Scan Results**.

   The **Scan Results** page appears.

3. View details about each scan result.

   - **Name** — The name for the scan associated with the result.

   - **Type** — The type of scan that generated the scan result.

   - **Scan Policy** — The name of the scan policy that generated the scan result.

   - **Scanned IPs** — The number of IP addresses scanned.

   - **Group** — The group associated with the scan.

   - **Owner** — The username for the user who added the scan.

   - **Duration** — The total time elapsed while running the scan.

   - **Import Time** — The date and time Tenable Security Center completed the scan result import.

   - **Status** — The status of the scan that generated the scan result. For more information, see Scan Status.

4. To view additional details for a scan result, see View Scan Result Details.

View Scan Result Details

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can view details for any scan result. For more information, see Scan Results.

To view scan result details:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Scan Results**.

   The **Scan Results** page appears.

3. Right-click the row for the scan result.

The actions menu appears.

-or-

Select the check box for the scan result.

The available actions appear at the top of the table.

4. Click **View**.

The **View Scan Result** page appears.

Section	Action
General	View general information for the scan result. • **Name** — The scan result name. • **Type** — The type of scan that generated the scan result. • **Scan Policy** — The name of the scan policy that generated the scan result. • **Repository** — The name of the repository associated with the scan policy that generated the scan result. • **Scanned IPs / Total IPs** — The number of IP addresses scanned compared to the total number of IP addresses targeted in the scan. • **Status** — The scan status. For more information, see Scan Status. • **Start Time** — The date and time Tenable Security Center started the scan. • **Finish Time** — The date and time Tenable Security Center completed the scan. • **Status** — The scan status. For more information, see Scan Status.

Section	Action
	• **Duration** — The total time elapsed while running the scan.
	• **Import Start** — The date and time Tenable Security Center started the scan result import.
	• **Import Finish** — The date and time Tenable Security Center completed the scan result import.
	• **Import Status** — The scan result import status. For more information, see Import Status.
	• **Import Duration** — The total time elapsed during scan result import.
	• **Owner** — The username for the user who added the scan.
	• **Group** — The group associated with the scan.
	• **ID** — The scan result ID.
Tenable Synchronization Data	View synchronization summary data:
	• **Status** — The status of the Tenable Lumin synchronization containing this scan result data:
	• **Not Synced** — The repository containing this scan result data is not configured for Tenable Lumin synchronization.
	• **Syncing** — The Tenable Lumin synchronization containing this scan result data is in progress.
	• **Finished** — The most recent synchronization that included this scan result data succeeded.
	• **Error** — An error occurred. For more information, see View Tenable One Data Synchronization Logs.
	• **Start Time** — The date and time Tenable Security Center

Section	Action
	started the most recent transfer of data to Tenable Vulnerability Management. • **Finish Time** — The date and time Tenable Security Center finished the most recent transfer of data to Tenable Vulnerability Management. • **Duration** — The total time elapsed during the most recent transfer of data to Tenable Vulnerability Management. • **Details** — If the **Status** is **Error**, details about the error. For more information about Tenable Lumin synchronization, see Tenable One Synchronization.

Upload Scan Results

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can upload active or agent scan results from scans performed by other systems. Tenable Security Center supports either raw (.nessus) or compressed (.zip) files, with one .nessus file per archive before uploading. This allows you to import scan results from scans run in remote locations without network connectivity to Tenable Security Center.

Note: To upload files greater than 300 MB to Tenable Security Center, you must modify `upload_max_filesize` in `/opt/sc/support/etc/php.ini` to accommodate the larger uploads.

Scan Result-Repository Incompatibility

Caution: Tenable does not recommend importing scan results to incompatible repositories since data may be omitted.

If you upload agent scan results to a non-agent repository, Tenable Security Center omits all vulnerabilities without **IP Address** data for the host. Non-agent repositories cannot uniquely identify hosts without **IP Address** data for the host.

If you upload non-agent scan results to an agent repository, Tenable Security Center omits all vulnerabilities without **Agent ID** data for the host. Agent repositories cannot uniquely identify hosts without **Agent ID** data for the host.

To upload scan results:

1. Log in to Tenable Security Center via the user interface.

2. Click **Scans** > **Scan Results**.

   The **Scan Results** page appears.

3. At the top of the table, click **Upload Scan Results**.

4. In the **Scan File** option, click **Choose File**.

   The file uploads to Tenable Security Center.

5. In the **Import Repository** drop-down box, select a repository.

6. If you selected an IPv4, IPv6, or Universal repository, enable or disable the **Advanced** options: **Track hosts which have been issued new IP address**, **Scan Virtual Hosts**, and **Immediately remove vulnerabilities from scanned hosts that do not reply**.

   For more information about the advanced options, see [Active Scan Settings](#).

7. Click **Submit**.

   Tenable Security Center saves your configuration.

Solutions Analysis

Tenable provides recommended solutions for all vulnerabilities on your network. You can perform the recommended action in a solution to lower the risk on your network.

For more information, see:

- [View Solutions](#)

- [View Solution Details](#)

View Solutions

You can use the **Solutions** page to view solutions for specific assets on your network or drill into solution details.

To view solutions for assets on your network:

1. Log in to Tenable Security Center via the user interface.

2. Click **Solutions**.

   The **Solutions** page appears.

3. To filter the solutions in the table by an asset list, in the **Targeted Assets** drop-down box, click an asset list name.

   The system refreshes the page and filters the table by the asset list you selected. For more information about asset lists, see Assets.

4. To customize the table, see Interact with a Customizable Table.

5. View information about each solution.

   - **Solution** — A description for the solution.

   - **Risk Reduction** — The percent you would reduce your risk by addressing the vulnerability in the solution. Tenable Security Center calculates the risk reduction percentage by dividing the score of the vulnerabilities in the solution by the score of all of the vulnerabilities on your network.

   - **Hosts Affected** — The number of devices affected by the solution.

   - **Vulnerabilities** — The number of vulnerability instances included in the solution.

     > **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

   - **VPR** — The highest VPR for a vulnerability included in the solution.

   - **EPSS** — The EPSS score for the vulnerability.

- **CVSSv3 Base Score** — The highest CVSSv3 or CVSS 4 score for a vulnerability included in the solution. If only CVSSv2 or CVSS v4 is available, the column is blank.

- **CVSSv4 Base Score** — The CVSSv4 score for the vulnerability included in the solution. If only CVSSv2 or CVSSv3 is available, the column is blank.

6. To view details for a solution, click a row.

   The **Solution Details** page appears. For more information, see Solution Details.

View Solution Details

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can use the **Solution Details** page to view details for a specific solution. To export the details for a solution, see Export Hosts Affected by a Solution.

To view details for a specific solution:

1. Log in to Tenable Security Center via the user interface.

2. Click **Solutions**.

   The **Solutions** page appears.

3. Click a solution row.

   The **Solution Details** page appears.

Section	Action
Metrics summary	View summary statistics for the recommended solution. • **Hosts Affected** — The number of devices affected by the solution. • **Vulnerabilities** — The total number of vulnerability instances included in the solution. > **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and

Section	Action
	protocol.
	• **VPR** — The highest VPR for a vulnerability included in the solution.
	• **CVSSv3 Base Score** — The highest CVSSv3 score for a vulnerability included in the solution. If only CVSSv2 is available, the column is blank.
Vulnerabilities Included table	View all vulnerabilities related to the recommended solution, sorted by decreasing VPR.
	• **Plugin** — The plugin ID.
	• **Hosts Affected** — The number of devices affected by the solution.
	• **VPR** — The VPR for the vulnerability.
	• **EPSS** — The EPSS score for the vulnerability.
	• **CVSSv3 Base Score** — The CVSSv3 score for the vulnerability included in the solution. If only CVSSv2 or CVSS v4 is available, the column is blank.
	• **CVSSv4 Base Score** — The CVSSv4 score for the vulnerability included in the solution. If only CVSSv2 or CVSSv3 is available, the column is blank.
Hosts Affected table	View device information.
	• **IP Address** — The IP address for the device.
	• **NetBIOS** — The NetBIOS name, if known.
	• **DNS** — The DNS name, if known.
	• **OS CPE** — The operating system common platform enumeration (CPE) name.

Section	Action
	• **Repository** — The repository name where device's scan data is stored. A device appears in multiple rows if the device's scan data is stored in multiple repositories.

What to do next:

- (Optional) Export the hosts affected by the solution to share with others in your organization, as described in Export Hosts Affected by a Solution.

Export Hosts Affected by a Solution

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can export a list of hosts affected by a solution as a `.csv` file to share the data with others in your organization. For more information, see Solutions Analysis.

To export hosts affected by a solution:

1. Log in to Tenable Security Center via the user interface.

2. Click **Solutions**.

   The **Solutions** page appears.

3. Click the row for the solution for which you want to export a list of affected hosts.

   The **Solution Details** page appears.

4. In the upper-right corner, click **Export as CSV**.

   A confirmation window appears.

   > **Note:** If the number of affected hosts is greater than 1,000, Tenable Security Center prompts you to type a name for the CSV report result you want to generate. After generation, you can download the report result, as described in Download a Report Result.

5. Select or clear the check boxes to indicate which columns you want to appear in the exported file.

Column Name	Description
Solution ID	The plugin ID associated with the recommended solution.
Solution	A description for the solution.
Tenable UUID	The Tenable UUID, if applicable. A Tenable UUID uniquely identifies: • Agent-detected assets that may share a common IP address. • OT Security assets that may not have an IP address. For more information, see OT Security Instances.
DNS	The DNS name of the device, if known.
IP Address	The IP address for the device.
OS	The operating system running on the device.
CVEs	The number of unique CVEs associated with vulnerabilities on the affected host that are addressed by the solution.
CVE Instances	The total number of CVE instances associated with vulnerabilities on the affected host that are addressed by the solution. **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.
OS CPE	The operating system common platform enumeration (CPE) name of the device.
Repository	The name of the repository that stores the device's scan data.
MAC	The MAC address of the device, if known.
NetBIOS	The NetBIOS name of the device, if known.

Vulnerabilities	The total number of vulnerability instances on the affected host addressed by the solution.
	Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.
Vulnerability Percentage	The number of vulnerability instances on the affected host addressed by the solution as a percentage of total vulnerability instances.
	Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.
Score	The sum of the weighted CVSS score across vulnerability instances on the affected host addressed by the solution.
	Note: Tenable Security Center uses either CVSSv2 or CVSSv3 to assess the severity of vulnerabilities, depending on your configuration. For more information, see Organizations.
	Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.
Risk Reduction	The percent you would reduce your risk across all solutions and affected hosts by addressing the vulnerabilities on this affected host associated with the solution. Tenable Security Center calculates the risk reduction percentage by dividing the total CVSS score of the vulnerabilities on the affected host addressed by the solution by the total CVSS score of all of the vulnerabilities on your network.
	Note: Tenable Security Center uses either CVSSv2 or CVSSv3 to assess the severity of vulnerabilities, depending on your configuration. For

	more information, see Organizations.
MS Bulletins	The number of unique MS Bulletins associated with vulnerabilities on the affected host that are addressed by the solution.
MS Bulletin Instances	The total number of vulnerabilities with associated MS Bulletins on the affected host that are addressed by the solution.
VPR	The highest VPR of all vulnerabilities on the affected host that are addressed by the solution. If no VPR is available, the column is blank.
CVSS v3	The highest CVSSv3 score of all vulnerabilities on the affected host that are addressed by the solution. If only a CVSSv2 score is available, the column is blank.

6. Click **Download**.

   Tenable Security Center exports the list of hosts affected by the solution.

Vulnerability Analysis

The **Vulnerabilities** page displays vulnerabilities from either the cumulative or mitigated vulnerability database. For more information, see Cumulative vs. Mitigated Vulnerabilities.

> **Note:** If multiple vulnerabilities share the same **IP Address** or **Agent ID** data, Tenable Security Center assumes they are from the same host.

To perform a common type of vulnerability analysis, see View Vulnerabilities by Plugin or View Vulnerabilities by Host.

To view a specific vulnerability analysis tool, see Vulnerability Analysis Tools.

Cumulative vs. Mitigated Vulnerabilities

Tenable Security Center stores vulnerabilities in two databases: the cumulative database and the mitigated database. You can choose to view cumulative vulnerabilities or mitigated vulnerabilities in any vulnerability analysis tool. For more information, see View Cumulative or Mitigated Vulnerabilities.

Cumulative Vulnerabilities

The cumulative database contains currently vulnerable vulnerabilities, including recast, accepted, or previously mitigated vulnerabilities.

Mitigated Vulnerabilities

The mitigated database contains vulnerabilities that Tenable Security Center determines are not vulnerable, based on the scan definition, the results of the scan, the current state of the cumulative view, and authentication information.

A vulnerability is mitigated if:

- The IP address of the vulnerability was in the target list of the scan.

- The plugin ID of the vulnerability was in the list of scanned plugins.

- The port of the vulnerability was in the list of scanned ports.

- The vulnerability with that IP address/port/plugin ID combination was not in the scan result.

To start, the vulnerability must appear in the cumulative view to be considered for mitigation. The import process then looks at each vulnerability in the import repository. The import process also verifies that authentication was successful before mitigating any local check vulnerabilities that meet the above criteria.

> **Note:** Mitigation logic works with scans using policies defined by templates, advanced policies, and remediation scans. These policies are set up to take advantage of this new mitigation logic.

For more information about mitigation, see the knowledge base article.

View Cumulative or Mitigated Vulnerabilities

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For general information about cumulative vulnerabilities and mitigated vulnerabilities, see Cumulative vs. Mitigated Vulnerabilities.

To switch between viewing mitigated or cumulative vulnerabilities:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.

3. In the upper-right corner, click **Cumulative** or **Mitigated**.

   The page updates to display data from the mitigated or cumulative vulnerability database.

CVSS vs. VPR

Tenable uses CVSS scores and a dynamic Tenable-calculated Vulnerability Priority Rating (VPR) to quantify the risk and urgency of a vulnerability.

> **Note:** When you view these metrics on an analysis page organized by plugin (for example, the **Vulnerabilities** page), the metrics represent the highest value assigned or calculated for a vulnerability associated with the plugin.

CVSS

Tenable uses and displays third-party Common Vulnerability Scoring System (CVSS) values retrieved from the National Vulnerability Database (NVD) to describe risk associated with vulnerabilities.

Tenable assigns all vulnerabilities a severity (**Info**, **Low**, **Medium**, **High**, or **Critical**) based on the vulnerability's static CVSS score (the CVSS version depends on your configuration). For more information, see Organizations.

Tenable Security Center analysis pages provide summary information about vulnerabilities using the following CVSS categories.

Severity	CVSSv2 Range	CVSSv3 Range
Critical	The plugin's highest vulnerability CVSSv2 score is 10.0.	The plugin's highest vulnerability CVSSv3 score is between 9.0 and 10.0.
High	The plugin's highest vulnerability CVSSv2 score is between 7.0 and 9.9.	The plugin's highest vulnerability CVSSv3 score is between 7.0 and 8.9.
Medium	The plugin's highest vulnerability CVSSv2 score is between 4.0 and 6.9.	The plugin's highest vulnerability CVSSv3 score is between 4.0 and 6.9.

| Low | The plugin's highest vulnerability CVSSv2 score is between 0.1 and 3.9. | The plugin's highest vulnerability CVSSv3 score is between 0.1 and 3.9. |
| Info | The plugin's highest vulnerability CVSSv2 score is 0.

- or -

The plugin does not search for vulnerabilities. | The plugin's highest vulnerability CVSSv3 score is 0.

- or -

The plugin does not search for vulnerabilities. |

Vulnerability Priority Rating

Tenable calculates a dynamic VPR for most vulnerabilities. The VPR is a dynamic companion to the data provided by the vulnerability's CVSS score, since Tenable updates the VPR to reflect the current threat landscape. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploit.

VPR Category	VPR Range
Critical	9.0 to 10.0
High	7.0 to 8.9
Medium	4.0 to 6.9
Low	0.1 to 3.9

Note: Vulnerabilities without CVEs (for example, many vulnerabilities with the **Info** severity) do not receive a VPR. Tenable recommends remediating these vulnerabilities according to their CVSS-based severity.

Note: You cannot edit VPR values.

Tenable Security Center provides new and updated VPR values through the Tenable Security Center feed. For more information, see Edit Plugin and Feed Schedules.

Tenable recommends resolving vulnerabilities with the highest VPRs first. You can view VPR scores and summary data in:

- The Tenable-provided **Vulnerability Priority Rating (VPR) Summary** dashboard, described in [Dashboards](#).

- The **Vulnerability Summary**, **Vulnerability List**, and **Vulnerability Detail List** tools, described in [View Vulnerabilities by Plugin](#).

VPR Key Drivers

Some key drivers that you can view to explain a vulnerability's VPR include, but are not limited to:

> **Note:** Tenable does not customize these values for your organization; VPR key drivers reflect a vulnerability's global threat landscape.

Key Driver	Description
Vulnerability Age	The number of days since the National Vulnerability Database (NVD) published the vulnerability.
CVSSv3 Impact Score	The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable Security Center displays a Tenable-predicted score.
Exploit Code Maturity	The relative maturity of a possible exploit for the vulnerability based on the existence, sophistication, and prevalence of exploit intelligence from internal and external sources (e.g., Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (**High**, **Functional**, **PoC**, or **Unproven**) parallel the CVSS Exploit Code Maturity categories.
Product Coverage	The relative number of unique products affected by the vulnerability: **Low**, **Medium**, **High**, or **Very High**.
Threat Sources	A list of all sources (e.g., social media channels, the dark web, etc.) where [threat events](#) related to this vulnerability occurred. If the system did not observe a related threat event in the past 28 days, the system displays **No recorded events**.
Threat Intensity	The relative intensity based on the number and frequency of recently observed [threat events](#) related to this vulnerability: **Very Low**, **Low**, **Medium**, **High**, or **Very High**.

Threat Recency	The number of days (0-180) since a [threat event](#) occurred for the vulnerability.

Threat Event Examples

Common threat events include:

- An exploit of the vulnerability

- A posting of the vulnerability exploit code in a public repository

- A discussion of the vulnerability in mainstream media

- Security research about the vulnerability

- A discussion of the vulnerability on social media channels

- A discussion of the vulnerability on the dark web and underground

- A discussion of the vulnerability on hacker forums

Vulnerability Analysis Tools

On the **Vulnerabilities** page, you can use the drop-down box to select the vulnerability analysis tool you want to view.

To perform a common type of vulnerability analysis, see [View Vulnerabilities by Plugin](#) or [View Vulnerabilities by Host](#).

Analysis Tool	Description
Asset Summary	This tool summarizes the scores and counts of vulnerabilities for all dynamic or static asset lists.
	A breakdown of each asset's specific vulnerabilities and counts for each severity level is also included.
	You can click a count to view the **IP Summary** tool, filtered by the asset list you selected.
CCE Summary	This displays a summary of hosts which have Common Configuration Enumeration (CCE) vulnerabilities.

Analysis Tool	Description
	You can click a count to view the **Vulnerability Summary** tool, filtered by the CCE vulnerability you selected.
Class A Summary **Class B Summary** **Class C Summary**	Summarizes host information. The vulnerability score for an address is computed by adding up the number of vulnerabilities at each severity level and multiplying it with the organization's severity score. Starting out with a Class A or Class B summary can identify more active network ranges for networks with a large number of active IP addresses. You can click a **Class A** or **Class B** row to view the **Class B** or **Class C** tool, filtered by the asset list you selected. You can click a **Class C** row to view the **IP Summary** tool, filtered by the asset list you selected.
CVE Summary	This view groups vulnerabilities based on their CVE ID, severity, and vulnerability count.
DNS Name Summary	Tenable Security Center includes the ability to summarize information by vulnerable DNS name. The DNS Name Summary lists the matching hostnames, the repository, vulnerability count, and a breakdown of the individual severity counts. You can click a DNS name to view the **Vulnerability List** tool, filtered by the DNS name you selected.
IAVM Summary	This view groups vulnerabilities based on their IAVM ID, severity, and vulnerability count.
IP Summary	Summarizes host information, organized by IP address/agent ID. You can click the **IP Address** to view host details, as described in View Host Details. For more information, see View Vulnerabilities by Host.
List Mail Clients	Tenable Security Center uses Tenable Network Monitor to determine a unique list of email clients. The list contains the email client name, count of detections, and the detection method.

Analysis Tool	Description
	You can click a count to view the **IP Summary** tool, filtered by the email client you selected.
List OS	Tenable Security Center understands both actively and passively fingerprinted operating systems. This tool lists what has been discovered. The method (active, passive, or event) of discovery is also indicated. You can click a count to view the **IP Summary** tool, filtered by operating system.
List Services	Tenable Security Center processes information from scans and creates a summary of unique services discovered. The service discovered, count of hosts, and detection method are listed. You can click a service to view the **IP Summary** tool, filtered by the service you selected.
List Software	Tenable Security Center processes information from scans and creates a summary of unique software packages discovered. The software name, count of hosts, and detection method are listed. You can click a software name to view the **IP Summary** tool, filtered by the software you selected.
List SSH Servers	This tool utilizes active and passive scan results to create a unique list of known SSH servers. The list contains the ssh server name, count of detections, and the detection method. **Tip:** Not all SSH servers run on port 22. Do not be surprised if you encounter SSH servers running on unexpected ports. You can click a count to view the **IP Summary** tool, filtered by the SSH server you selected.
List Web Clients	Tenable Security Center understands Tenable Network Monitor plugin ID 1735, which passively detects the web client in use. This tool lists the unique web clients detected. The list contains the user-agents, count of

Analysis Tool	Description
	detections, and the detection method.
	You can click a count to view the **IP Summary** tool, filtered by the web client you selected.
List Web Servers	This tool takes the passive output from passive and active scans to create a unique list of known web servers. The list contains the web server name, count of detections, and the detection method.
	Tip: Not all web servers run on port 80 or 443. Do not be surprised if you encounter web servers running on unexpected ports.
	You can click a count to view the **IP Summary** tool, filtered by the web server you selected.
MS Bulletin Summary	This tool filters vulnerabilities based on Microsoft Bulletin ID. Displayed are the IDs, Vulnerability Totals, Host Total, and Severity. This view is particularly useful in cases where Microsoft releases a new bulletin and a quick snapshot of vulnerable hosts is required.
Plugin Family Summary	This tool charts the Nessus, Tenable Network Monitor, or Event plugin family as well as their relative counts based on severity level for all matching vulnerabilities.
	You can click a count to view the **Vulnerability List** tool, filtered by the plugin family you selected.
Port Summary	A summary of the ports in use is displayed for all matched vulnerabilities. Each port has its count of vulnerabilities as well as a breakdown for each severity level.
	You can click a port to view the **IP Summary** tool, filtered by the port you selected.
Protocol Summary	This tool summarizes the detected IP protocols such as TCP, UDP, and ICMP. The tool also breaks out the counts for each protocol's severity levels.

Analysis Tool	Description
	You can click a count to view the **IP Summary** tool, filtered by the count you selected.
Remediation Summary	The Remediation Summary tool provides a list of remediation actions that may be taken to prioritize tasks that have the greatest effect to reduce vulnerabilities in systems. This list provides a solution to resolve a particular CPE on a given OS platform. The data provided includes: • **Risk Reduction** — The percent you would reduce your risk by addressing the vulnerability in the solution. Tenable Security Center calculates the risk reduction percentage by dividing the score of the vulnerabilities in the solution by the score of all of the vulnerabilities on your network. • **Hosts Affected** — The number of unique hosts that would be affected by performing the remediation action. • **Vulnerabilities** — The count of vulnerabilities (Tenable Nessus plugins) that would be remediated by performing the remediation action. • **Score** — This is calculated by adding up the score for each vulnerability that would be remediated by performing the remediation action. • **CVE** — The number of distinct CVEs that would be remediated by performing the remediation action. • **MS Bulletin** — The number of unique MS Bulletins that would be remediated by performing the remediation action. • **Vulnerability %** — The count of vulnerabilities (Tenable Nessus plugins) that would be remediated by performing the remediation action over the total vulnerability count returned by the query as a percentage.
Severity Summary	This tool considers all of the matching vulnerabilities and then charts the total number of info, low, medium, high, and critical vulnerabilities.

Analysis Tool	Description
	You can click a count to view the **Vulnerability Summary** tool, filtered by the severity you selected.
User Responsibility Summary	This displays a list of the users who are assigned responsibility for the vulnerability based on the user's assigned asset list. Multiple users with the same responsibility are displayed on the same line. Users without any assigned responsibilities are not displayed in the list. Tenable Security Center populates this list after you assign an asset to a user account.
Vulnerability Detail List	Displays the details for a specific vulnerability instance on your network.
	Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.
	Important options include CVSS v2/CVSS v3 score, CVSS v2/CVSSv3 temporal score, VPR, VPR key drivers, availability of public exploit, CVE, BID, synopsis, description, and solution.
	For more information, see View Vulnerability Instance Details.
Vulnerability List	Displays a table of all vulnerability instances found on your network, organized by plugin ID.
	Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.
	For more information, see View Vulnerabilities by Plugin.
Vulnerability Summary	Displays a table of all plugins associated with vulnerabilities on your network, organized by plugin ID.
	For more information, see View Vulnerabilities by Plugin.

Vulnerability Analysis Filter Components

For general information about using filters, see Filters.

Filter Component	Availability	Description
Accept Risk	Cumulative View	Displays vulnerabilities based on their Accepted Risk workflow status. Available choices include **Accepted Risk** or **Non-Accepted Risk**. Choosing both options displays all vulnerabilities regardless of acceptance status.
Address	All	This filter specifies an IPv4 or IPv6 address, range, or CIDR block to limit the viewed vulnerabilities. For example, entering *198.51.100.28/24* and/or *2001:DB8::/32* limits any of the web tools to show vulnerability data from the specified networks. You can enter addresses in a comma-separated list or on separate lines.
Agent ID	All	Displays results matching the specified agent UUID (Tenable UUID). An agent UUID uniquely identifies: • Agent-detected assets that may share a common IP address. • OT Security assets that may not have an IP address. For more information, see OT Security Instances.
Application CPE	All	Allows a text string search to match against available CPEs. The filter may be set to search based on a **contains**, **Exact Match**, or **Regex Filter** filter. The **Regex Filter** is based on Perl-compatible regular expressions (PCRE).
Asset	All	This filter displays systems from the assets you select. If more than one asset contains the systems from the primary asset (i.e., there is an intersect between the asset lists), those assets are displayed as well. **Tip:** Use NOT, OR, and AND operators to exclude

Filter Component	Availability	Description
		unwanted assets from the view.
Asset Criticality Rating (ACR)	All	(Requires Tenable Security Center+ license) Filters for vulnerabilities on hosts within the specified ACR range, between 0 and 10. For more information, see Asset Criticality Rating in the *Tenable Vulnerability Management User Guide*. **Tip:** To edit the ACR for an asset, see Edit an ACR Manually.
Asset Exposure Score (AES)	All	(Requires Tenable Security Center+ license) Filters for hosts within the specified AES range, between 0 and 1000. For more information, see Asset Exposure Score in the *Tenable Vulnerability Management User Guide*.
AES Severity	All	(Requires Tenable Security Center+ license) Filters for hosts with the specified AES severity. For more information, see Asset Exposure Score in the *Tenable Vulnerability Management User Guide*.
Audit File	All	Filters vulnerabilities by plugin IDs associated with the audit file used to perform a scan.
CCE ID	All	Displays results matching the entered CCE ID.
CVE ID	All	Displays vulnerabilities based on one or more CVE IDs. Type multiple IDs as a comma-separated list (e.g., **CVE-2011-3348,CVE-2011-3268,CVE-2011-3267**).
CVSS v2 Score	All	Displays vulnerabilities within the chosen Common Vulnerability Scoring System version 2 (CVSS v2) score range.

Filter Component	Availability	Description
CVSS v2 Vector	All	Filters results based on a search against the CVSS v2 vector information.
CVSS v3 Score	All	Displays vulnerabilities within the chosen CVSS v3 score range.
CVSS v3 Vector	All	Filters results based on a search against the CVSS v3 vector information.
CVSS v4 Score	All	Displays vulnerabilities within the chosen CVSS v4 score range.
CVSS v4 Supplemental	All	Filters results based on a search against the CVSS v4 supplemental information.
CVSS v4 Threat Score	All	Displays vulnerabilities within the chosen CVSS v4 threat score range.
CVSS v4 Threat Vector	All	Filters results based on a search against the CVSS v4 threat vector information.
CVSS v4 Vector	All	Filters results based on a search against the CVSS v4 vector information.
Cross References	All	Filters results based on a search against the cross reference information in a vulnerability.
Data Format	All	Displays results matching the specified data type: **IPv4**, **IPv6**, or **Agent**.
DNS Name	All	This filter specifies a DNS name to limit the viewed vulnerabilities. For example, entering host.example.com limits any of the web tools to only show vulnerability data from that DNS name.
Exploit Prediction Scoring System	All	Filters results by the EPSS score, which predicts how likely a vulnerability is to be exploited.

Filter Component	Availability	Description
(EPSS)		
Exploit Available	All	If set to yes, displays only vulnerabilities for which a known public exploit exists.
Exploit Frameworks	All	When set, the text option can be equal to or contain the text entered in the option.
IAVM ID	All	Displays vulnerabilities based on one or more IVAM IDs. Type multiple IDs as a comma-separated list (e.g., *2011-A-0005,2011-A-0007,2012-A-0004*).
MS Bulletin ID	All	Displays vulnerabilities based on one or more Microsoft Bulletin IDs. Type multiple IDs as a comma-separated list (e.g., *MS10-012,MS10-054,MS11-020*).
Mitigated	All	Displays vulnerabilities for a specific mitigation status: **Previously Mitigated** — the vulnerability was previously mitigated but it reappeared in a scan and is currently vulnerable **Never Mitigated** — the vulnerability is currently vulnerable and has never been mitigated For more information about mitigation, see [Mitigated Vulnerabilities](#).
Nessus Web Tests	All	Displays vulnerabilities that are detected by a scan with Nessus Web Tests enabled in the scan policy.
NetBIOS Name	All	Displays vulnerabilities that match the specified NetBIOS name. In the drop-down, select **Exact Match**, **Contains**, or **Regex Match**. **Regex Match** is based on Perl-compatible regular expressions (PCRE).

Filter Component	Availability	Description
		Note: You cannot filter NetBIOS Name by UNKNOWN. The NetBIOS workgroup is labeled UNKNOWN when a workgroup or domain cannot be detected.
Output Assets	Asset Summary Analysis Tool	This filter displays only the desired asset list systems.
Patch Published	All	Some plugins contain information about when a patch was published for a vulnerability. This filter allows the user to search based on when a vulnerability's patch became available:

- **None** (displays vulnerabilities that do not have a patch available)

- **Within the last day**

- **Within the last 7 days**

- **Within the last 30 days**

- **More than 7 days ago**

- **More than 30 days ago**

- **Current Month**

- **Last Month**

- **Current Quarter** (during the current calendar year quarter)

- **Last Quarter** (during the previous calendar year quarter)

- **Current Year**

- **Last Year**

- **Custom Range** (during a specific range you

Filter Component	Availability	Description
		specify)
		• **Explicit** (at a specific time you specify)
Plugin Family	All	This filter chooses a Nessus or Tenable Network Monitor plugin family. Only vulnerabilities from that family display.
Plugin ID	All	Type the plugin ID desired or range based on a plugin ID. Available operators are equal to (=), not equal to (!=), greater than or equal (>=) and less than or equal to (<=).
Plugin Modified	All	Tenable plugins contain information about when a plugin was last modified. This filter allows users to search based on when a particular plugin was modified: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you

Filter Component	Availability	Description
		specify) • **Explicit** (at a specific time you specify)
Plugin Name	All	Using the **Contains** option, type all or a portion of the actual plugin name. For example, entering **MS08-067** in the plugin name filter displays vulnerabilities using the plugin named **MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)**. Similarly, entering the string **uncredentialed** displays a list of vulnerabilities with that string in the plugin name. Use the **Regex Match** option to filter plugin names based on Perl-compatible regular expressions (PCRE).
Plugin Published	All	Tenable plugins contain information about when a plugin was first published. This filter allows users to search based on when a particular plugin was created: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter)

Filter Component	Availability	Description
		• **Current Year**
		• **Last Year**
		• **Custom Range** (during a specific range you specify)
		• **Explicit** (at a specific time you specify)
Plugin Type	All	Select whether to view all plugin types or passive, active, event, or compliance vulnerabilities.
Port	All	This filter is in two parts. First the equality operator is specified to allow matching vulnerabilities with the same ports, different ports, all ports less than or all ports greater than the port filter. The port filter allows a comma separated list of ports. For the **larger than** or **less than** filters, only one port may be used.
		Note: All host-based vulnerability checks are reported with a port of 0 (zero).
Protocol	All	This filter provides boxes to select TCP, UDP, or ICMP-based vulnerabilities.
Recast Risk	Cumulative View	Displays vulnerabilities based on their Recast Risk workflow status. Available choices include **Recast Risk** or **Non-Recast Risk**. Choosing both options displays all vulnerabilities regardless of recast risk status.
Repositories	All	Displays vulnerabilities from the chosen repositories.
STIG Severity	All	Displays vulnerabilities with the chosen STIG severity in the plugins database.
Scan Accuracy	All	Displays vulnerabilities that are detected by scans with the chosen scan accuracy:
		• **Not Paranoid** — the vulnerability was detected by

Filter Component	Availability	Description
		a scan with the scan accuracy set to Not Paranoid in the scan policy. • **Paranoid** — the vulnerability was detected by a scan with the scan accuracy set to Paranoid in the scan policy.
Scan Policy Plugins	All	Displays vulnerabilities found by the currently enabled plugins in the scan policy. For more information, see [The Plugins tab specifies which plugins are used during the policy's Tenable Nessus scan. You can enable or disable plugins in the plugin family view or in the plugin view for more granular control.]().
Security End of Life Date	All	When available, Tenable plugins contain information about software end of life dates. This filter allows users to search based on when a particular software is end of life: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year**

Filter Component	Availability	Description
		• **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify)
Severity	All	Displays vulnerabilities with the selected severity. For more information, see CVSS vs. VPR.
Thorough Tests	All	Displays vulnerabilities that are detected by scans with Thorough Tests enabled in the scan policy.
Users	All	Allows selection of one or more users who are responsible for the vulnerabilities.
Vulnerability Discovered	All	Tenable Security Center tracks when each vulnerability was first discovered. This filter allows you to see when vulnerabilities were discovered: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year**

Filter Component	Availability	Description
		- **Last Year** - **Custom Range** (during a specific range you specify) - **Explicit** (at a specific time you specify) **Note:** The discovery date is based on when the vulnerability was first imported into Tenable Security Center. For Tenable Network Monitor, this date does not match the exact vulnerability discovery time as there is normally a lag between the time that Tenable Network Monitor discovers a vulnerability and the import occurs. **Note:** Days are calculated based on 24-hour periods prior to the current time, not calendar days. For example, if the report run time was 1/8/2019 at 1:00 PM, using a 3-day count would include vulnerabilities starting 1/5/2019 at 1:00 PM and not from 12:00 AM.
Vulnerability Last Observed	Cumulative View	This filter allows the user to see when the vulnerability was last observed by Tenable Nessus, Tenable Log Correlation Engine, or Tenable Network Monitor: - **Within the last day** - **Within the last 7 days** - **Within the last 30 days** - **More than 7 days ago** - **More than 30 days ago** - **Current Month** - **Last Month** - **Current Quarter** (during the current calendar year quarter)

Filter Component	Availability	Description
		• **Last Quarter** (during the previous calendar year quarter)
		• **Current Year**
		• **Last Year**
		• **Custom Range** (during a specific range you specify)
		• **Explicit** (at a specific time you specify)
		Note: The observation date is based on when the vulnerability was most recently imported into Tenable Security Center. For Tenable Network Monitor, this date does not match the exact vulnerability discovery as there is normally a lag between the time that Tenable Network Monitor discovers a vulnerability and the import occurs.
Vulnerability Mitigated	Mitigated View	This filter allows the user to filter results based on when the vulnerability was mitigated:
		• **Within the last day**
		• **Within the last 7 days**
		• **Within the last 30 days**
		• **More than 7 days ago**
		• **More than 30 days ago**
		• **Current Month**
		• **Last Month**
		• **Current Quarter** (during the current calendar year quarter)
		• **Last Quarter** (during the previous calendar year quarter)

Filter Component	Availability	Description
		• **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify)
Vulnerability Priority Rating (VPR)	All	Displays vulnerabilities within the chosen VPR range. For more information, see CVSS vs. VPR. **Tip:** The **Vulnerabilities** page displays vulnerabilities by plugin. The VPR that appears is the highest VPR of all the vulnerabilities associated with that plugin.
Vulnerability Published	All	When available, Tenable plugins contain information about when a vulnerability was published. This filter allows users to search based on when a particular vulnerability was published: • **All** • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year

Filter Component	Availability	Description
		quarter)
		• **Current Year**
		• **Last Year**
		• **Custom Range** (during a specific range you specify)
		• **Explicit** (at a specific time you specify)
Vulnerability Text	All	Displays vulnerabilities containing the entered text (e.g., php 5.3) or regex search term.
Web App Scanning	All	**Required Additional License:** Tenable Web App Scanning **Required Tenable Nessus Version:** 10.6.1 or later Select whether to display web app scan results in the list: • **Exclude Web App Results** - do not display web app scan results in the list of vulnerabilities. • **Include Web App Results** - include web app scan results in the list of vulnerabilities. • **Only Web App Results** - filter the list to display only web app scans results.
Web App URL	All	**Required Additional License:** Tenable Web App Scanning **Required Tenable Nessus Version:** 10.6.1 or later The URL for the discovered web application associated with the vulnerability.

View Vulnerabilities by Host

You can drill into analysis views, filtering by host, to view vulnerabilities and vulnerability instances on a host.

To view vulnerabilities and vulnerability instances associated with a host:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.

3. In the drop-down box, click **IP Summary**.

   The **IP Summary** tool appears.

4. Filter the tool to locate the host where you want to view vulnerability instance details, as described in Filters and Vulnerability Analysis Filter Components.

5. To customize the table, see Interact with a Customizable Table.

6. To view details of a vulnerability instance:

   a. Click the row for the vulnerability instance for which you want to view the details.

      The **Vulnerability List** tool appears, filtered by the vulnerability instance you selected.

      In this tool, you can:

Options	Actions
Jump to Vulnerability Detail	View the **Vulnerability Detail List** page. This page displays the synopsis, description, solution, and the plugin output of the vulnerability.
Export	Export data as a .csv or a .pdf file, as described in Export Vulnerability Data.
Save	• **Save Query** — Save a query, as described in Add or Save a Query.

	• **Save Asset** — Save an asset, as described in [Assets].
More	• **Open Ticket** — Open a ticket, as described in [Open a Ticket].
	• **Set as Default View** — Set this view as your default view.
Cumulative	Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in [View Cumulative or Mitigated Vulnerabilities].
Mitigated	Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in [View Cumulative or Mitigated Vulnerabilities].
Filters side bar	Apply a filter, as described in [Apply a Filter] and [Vulnerability Analysis Filter Components].
Vulnerability row	• Click the **Plugin ID** to view the plugin details associated with the vulnerability, as described in [View Plugin Details].
	• Click the **IP Address** to view the host details for the vulnerability, as described in [View Host Details].
	Click the row to view the vulnerability instance details in the **Vulnerability Detail List** tool, as described in [View Vulnerability Instance Details].

7. To view the host details of an instance:

   a. Click the **IP Address** link.

      The **System Information** pane appears. For more information, see [View Host Details].

View Vulnerabilities by Plugin

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see [User Roles].

You can drill into analysis views, filtering by plugin, to view vulnerabilities and vulnerability instances related to that plugin.

To view vulnerabilities and vulnerability instances associated with a plugin:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.

3. In the drop-down box, click **Vulnerability Summary**.

   The **Vulnerability Summary** tool appears.

   In this tool, you can:

Options	Actions
Jump to Vulnerability Detail	View the **Vulnerability Detail List** page. This page displays the synopsis, description, solution, and the plugin output of the vulnerability.
Export	Export data as a .csv or a .pdf file, as described in Export Vulnerability Data.
Save	• **Save Query**: Save a query, as described in Add or Save a Query. • **Save Asset**: Save an asset, as described in Assets.
More	• **Open Ticket**: Open a ticket, as described in Open a Ticket. • **Set as Default View**: Set this view as your default view.
Cumulative	Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.
Mitigated	Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.
Table	Customize the table, as described in Interact with a Customizable Table.
Filters side bar	Apply a filter, as described in Apply a Filter and Vulnerability Analysis

	[Filter Components]().
Plugin row	• Click the **Plugin ID** to view the plugin details for the plugin, as described in [View Plugin Details](). • Click the row to view the vulnerability details in the **Vulnerability List** tool.
Plugin row	You can right-click any row to do the following: • View **Asset Summary** tool, **DNS Summary** tool, or **IP Summary** tool. • Create an accept risk rule, as described in [Add an Accept Risk Rule](). • Create a recast risk rule, as described in [Add a Recast Risk Rule](). • Launch a remediation scan, as described in [Launch a Remediation Scan]().

4. Click the row for the plugin where you want to view vulnerability instance details.

    The **Vulnerability List** tool appears, filtered by the plugin you selected.

    In this tool, you can:

Options	Actions
Jump to Vulnerability Detail	View the **Vulnerability Detail List** page. This page displays the synopsis, description, solution, and the plugin output of the vulnerability.
Export	Export data as a .csv or a .pdf file, as described in [Export Vulnerability Data]().
Save	• **Save Query** — Save a query, as described in [Add or Save a Query](). • **Save Asset** — Save an asset, as described in [Assets]().

More	• **Open Ticket** — Open a ticket, as described in [Open a Ticket](#). • **Set as Default View** — Set this view as your default view.
Cumulative	Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in [View Cumulative or Mitigated Vulnerabilities](#).
Mitigated	Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in [View Cumulative or Mitigated Vulnerabilities](#).
Filters side bar	Apply a filter, as described in [Apply a Filter](#) and [Vulnerability Analysis Filter Components](#).
Vulnerability row	• Click the **Plugin ID** to view the plugin details associated with the vulnerability, as described in [View Plugin Details](#). • Click the **IP Address** to view the host details for the vulnerability, as described in [View Host Details](#). Click the row to view the vulnerability instance details in the **Vulnerability Detail List** tool, as described in [View Vulnerability Instance Details](#).

View Vulnerability Instance Details

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can drill into analysis views to view details for a specific instance of a vulnerability found on your network.

> **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

To view vulnerability instance details:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.

3. In the drop-down box, click **Vulnerability Detail List**.

   The **Vulnerability Detail List** tool appears.

   In this tool, you can:

Section	Actions
Options menu	• Export data as a `.csv` or a `.pdf` file, as described in Export Vulnerability Data. • Save a query, as described in Add or Save a Query. • Save an asset. • Open a ticket, as described in Open a Ticket. • Set this view as your default view. • Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities.
arrows	Click the arrows to view other vulnerability instances related to the plugin.
toolbar	• Launch a remediation scan, as described in Launch a Remediation Scan. • Create an accept risk rule, as described in Add an Accept Risk Rule. • Create a recast risk rule, as described in Add a Recast Risk Rule.
Synopsis and **Description**	View information about the plugin, vulnerability instance, and affected assets.

Solution	View the Tenable-recommended action to remediate the vulnerability.
See Also	View related links about the plugin or vulnerability.
Discovery	View details about when the vulnerability was discovered and last seen on your network.
Host Information	View details about the asset.
Risk Information	View metrics (for example, CVSS score, VPR, and EPSS) about the risk associated with the vulnerability.
Exploit Information	View details about the exploit.
Plugin Details	View details about the plugin.
VPR Key Drivers	View the key drivers Tenable used to calculate the VPR score. For more information, see CVSS vs. VPR.
Vulnerability Information	View Common Platform Enumeration (CPE) details.
Reference Information	View related links to the CVE, BID, MSFT, CERT, and other industry materials about the vulnerability.

View Host Details

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can drill into analysis views to view details for a specific host on your network.

To view host details from the **Vulnerabilities** page:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Vulnerabilities**.

The **Vulnerabilities** page appears.

3. In the drop-down box, click **Vulnerability List**.

   The **Vulnerability List** tool appears.

4. In the **IP Address** column, click the IP address link to view host details for a specific vulnerability instance.

> **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

The host details panel appears.

Section	Actions
System Information	View information about the host system. • **IP Address** — The host's IP address, if available. • **UUID** — The host's UUID, if available. • **NetBIOS Name** — The host's NetBIOS name, if available. • **DNS Name** — The host's DNS name, if available. • **MAC Address** — The host's MAC address, if available. • **OS** — The operating system running on the host, if available. • **CPE** — The host's application common platform enumeration (CPE). • **Score** — The cumulative score for all vulnerability instances on the host. For more information about vulnerability scoring, see [CVSS vs. VPR](#). > **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol. • **Repository** — The repository that contains vulnerability data

	associated with the host.
	• **Last Scan** — The date and time Tenable Security Center last scanned the host.
	• **Passive Data** — Indicates whether a passive scan detected the vulnerability.
	• **Compliance Data** — Indicates whether the scan that detected the vulnerability included compliance plugins.
Vulnerabilities	View the number of vulnerabilities on the host, organized by severity category. For more information, see CVSS vs. VPR.
Links	• View SANS and ARIN links for the host. If configured, this section also displays custom resource links.
	• Click a resource link to view details for the current IP address/agent IDs. For example, if the current IP address was a publicly registered address, click the ARIN link to view the registration information for that address.
Assets	View the asset lists containing the asset. For more information, see Assets.

To view host details from the **Host Assets** page:

1. Log in to Tenable Security Center via the user interface.

2. Click **Assets** > **Host Assets**.

   The **Host Assets** page appears.

3. Click the row for the host.

   The **Host Asset Details** page appears.

Section	Action
Host Information	View general information about the host.
	• **Name** — The name of the host.

Section	Action
	• **System Type** — The host's device type, as determined by plugin 54615. • **Operating System** — The operating system running on the host, if available. • **IP Addresses** — The host's IP address, if available. • **MAC Addresses** — The host's MAC address, if available. • **Host ID** — The ID of the host. • **Repository** — The repository that contains vulnerability data associated with the host.
Asset Exposure Score	(Requires Tenable Security Center+ license) View the host's AES. For more information, see Asset Exposure Score in the *Tenable Vulnerability Management User Guide*.
Asset Criticality Rating	(Requires Tenable Security Center+ license) View the host's ACR and details about modifications to the ACR. • **Overwrite Reasoning** — The justification for overwriting the host's ACR. • **Notes** — Notes associated with overwriting the host's ACR. • **Overwritten By** — The user that overwrote the host's ACR. • **ACR By Key Drivers** — The key drivers used to calculate the host's ACR. For more information, see Asset Criticality Rating and ACR Key Drivers in the *Tenable Vulnerability Management User Guide*. To edit the host's ACR, see Edit an ACR Manually.
OT Properties	View the Tenable OT Security properties for the host. This section appears only for hosts discovered by Tenable OT Security scans.

Section	Action
	• **Additional Names** - Any additional names for the asset in the network.
	• **Additional IP Addresses** - Any additional IP addresses for the asset.
	• **Segment** - The network segment that the IP address(es) of this asset are assigned to.
	• **Slot** - For assets that are on backplanes, shows the number of the slot to which the asset is attached.
	• **Family** - The family name of the product as defined by the asset vendor.
	• **State** - The device state:
	• **Backup** – the controller is running as a backup to a primary controller.
	• **Fault** – the controller is in fault mode.
	• **NoConfig** – no configuration has been set for the controller.
	• **Running** – the controller is running.
	• **Stopped** – the controller is not running.
	• **Unknown** – the state is unknown.
	• **Category** - The type of asset identified by Tenable OT Security. For more information about categories, see Asset Types in the *Tenable OT Security user guide*.
	• **Purdue** - The Purdue level of the asset:
	• **0** - Physical process
	• **1** - Intelligent devices

Section	Action
	• **2** - Control systems
	• **3** - Manufacturing operations systems
	• **4** - Business logistics systems
	• **Last Update** - The date and time that the asset was last updated.
	• **Risk Score** - A measure of the degree of risk related to this asset on a scale from 0 (no risk) to 100 (extremely high risk). For an explanation of how the Risk score is calculated, see Risk Assessment in the *Tenable OT Security user guide*.
	• **Description** - A brief description of the asset, as configured by the user in the Tenable OT Security asset details. For more information, see Inventory in the *Tenable OT Security user guide*.
	• **Back Plane** - The backplane unit that the asset is connected to.
	• **System Type** - A brief description of the asset, as configured by the user in the OT Security asset details.
	• **Model** - The model name of the asset.
	• **Firmware** - The firmware version currently installed on the asset.
	• **Location** - The location of the asset as input by the user in the Tenable OT Security asset details.
	• **Vendor** - The asset vendor.
	• **Criticality** - A measure of the importance of this asset to the proper functioning of the system. A value is assigned automatically to each asset based on the asset type. You can

Section	Action
	manually adjust the value.
Scan Information	View scan information related to the host. • **First Seen** — The date and time Tenable Security Center first detected the host on your network. • **Last Seen** — The date and time last Tenable Security Center detected the host on your network. • **Source** — The type of scan that discovered the host on your network: **Tenable Nessus Scan**, **Tenable Network Monitor**, **Log Correlation Engine**, **Agent Scan**, or **Tenable OT Security Scan**.
Findings tab	• View the vulnerabilities detected on the host. For more information, see CVSS vs. VPR. • Customize the table, as described in Interact with a Customizable Table.
Installed Software tab	View the software packages installed on the host, if available. Customize the table, as described in Interact with a Customizable Table.

View Plugin Details

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can drill into analysis views to view details for a specific instance of a vulnerability found on your network.

Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

To view plugin details:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.

3. In the drop-down box, click **Vulnerability Summary**.

   The **Vulnerability Summary** tool appears.

4. To customize the table, see Interact with a Customizable Table.

5. In the **Plugin ID** column, click the plugin ID to view plugin details for a specific plugin.

   The **Plugin Details** panel appears.

   In this panel, you can:

Section	Actions
Description	View information about the plugin, vulnerability instance, and affected assets.
Solution	View the Tenable-recommended action to remediate the vulnerability.
Vulnerability Priority Rating (VPR) Key Drivers	View the key drivers Tenable used to calculate the vulnerability VPR. For more information, see CVSS vs. VPR.
CVE and **BID**	View related links to the CVE and BID materials about the vulnerability.
Cross-References	View related documentation for the vulnerability.
See Also	View related links about the plugin or vulnerability.

Export Vulnerability Data

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can export data from the **Vulnerabilities** page as a `.csv` or a `.pdf` file.

To export data from the Vulnerabilities page:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.

3. In the **Export** drop-down box, click **Export** > **Export as CSV** or **Export as PDF**.

   > **Note:** If the record count (rows displayed) of any CSV export is greater than 1,000, Tenable Security Center prompts you for the name of the CSV report you want to generate. After generation, you can download the report from the **Report Results** page.

4. Select or clear the check boxes to indicate which columns you want to appear in the exported file.

5. Click **Submit**.

   Tenable Security Center exports the vulnerability data.

Vulnerability Intelligence

> **Note:** If you have more than 100,000 assets or a non-rpm installation, you must connect an external PostgreSQL server to use Vulnerability Intelligence.

In the **Vulnerability Intelligence** section, you can review all vulnerabilities known to Tenable without leaving Tenable Security Center.

The vulnerabilities come from Tenable's database, which draws on sources such as internal expertise, vendor advisories, the GitHub Advisory Database, and the National Vulnerability Database (NVD).

The **Vulnerability Intelligence** section also holds curated categories that blend known risk indicators with insights from the Tenable Research Team to surface the most crucial vulnerabilities.

Once you have chosen which vulnerabilities to focus on, you compare them to your own findings and build a list to take action on. To do this, use the query builder to refine the results and save your searches to re-use or share.

The following topics explain how to use the tools in the **Vulnerability Intelligence** section to: 1) search Tenable's vulnerability database, 2) view vulnerability profiles, and 3) identify your exposure when compared to known vulnerabilities.

Search Known Vulnerabilities

On the **Vulnerability Intelligence Overview** page, you can search all vulnerabilities known to Tenable by *Common Vulnerabilities and Exposures* (CVE) ID.

To search for a vulnerability:

1. In the left navigation, click ⓘ **Vulnerability Intelligence**.

   The **Vulnerability Intelligence Overview** page appears.

2. In the header, in the search box, type a complete or partial search (for example, *CVE-2014-0160* or *2014*).

3. Press the **Enter** key.

4. In the list of results, click a vulnerability.

   The **Vulnerability Profile** page appears.

View Vulnerability Profiles

On the **Vulnerability Intelligence Overview** page, when you click a search result or a row in the **CVEs** tab, the **Vulnerability Profile** page appears.

The **Vulnerability Profile** page breaks down a single vulnerability in detail and includes an event timeline, your affected assets and products, the sources, and metrics such as risk profile and severity.

The **Vulnerability Profile** page has four sections.

In this Section	You Can...
Vulnerability Information	View the Common Vulnerability Scoring System (CVSS), Vulnerability Priority Rating (VPR), and Exploit Prediction Scoring System (EPSS) scores. In tabs, review an event timeline, VPR and EPSS trends, identifying plugins, all known products affected, and a summary.

How Does This Affect Me?	View affected assets and products in your environment and build queries to refine the results.
Sources	View contextual intelligence such as security advisories on the external websites where they appear.
Vulnerability Metrics	In a right-hand pane, review metrics broken down by general information, risk profile, severity, and plugin coverage.

Vulnerability Information

On the **Vulnerability Profile** page, the **Vulnerability Information** section provides a short summary along the vulnerability's Vulnerability Priority Rating (VPR), Common Vulnerability Scoring System (CVSS), and Exploit Prediction Scoring System (EPSS) scores.

It also contains four tabs, within which you can view an event timeline, VPR and EPSS widgets, plugin details, known affected products, and a full summary.

Events

The **Events** tab appears by default and contains a timeline for the vulnerability. Use the horizontal scroll bar or click an *event marker* to go to that event. Click event links to open them in your web browser.

The timeline can contain the following events.

Event	Description
Discovery Date	Indicates the date Tenable first observed the vulnerability.
NVD Published	Indicates the date that the National Vulnerability Database (NVD) disclosed the vulnerability.
First Tenable Coverage	Indicates the first time Tenable provided coverage for the vulnerability.
First Proof of Concept	Indicates the date Tenable first observed a proof of concept for the vulnerability.
First Functional	Indicates the date the first functional exploit for the vulnerability was

Exploit	released.
Consec Plugin Published	Appears when a new Container Security Scanner plugin for the vulnerability is released.
LCE Plugin Published	Appears when a new Log Correlation Engine plugin for the vulnerability is released.
Nessus Plugin Published	Appears when a new Tenable Nessus plugin for the vulnerability is released.
NNM Plugin Published	Appears when a new Tenable Network Monitor plugin for the vulnerability is released.
WAS Plugin Published	Appears when a new [[[Undefined variable WebApplicationScanning.WAS]]] plugin for the vulnerability is released.
Ransomware	Indicates the first time Tenable observed ransomware events for the vulnerability.
Malware	Indicates the first time Tenable observed malware events for the vulnerability.
Emerging Threats	Indicates that Tenable is actively monitoring the vulnerability since it is being publicly discussed, has a viable proof of concept, and/or is widely used.
Exploited in the Wild	Indicates that the vulnerability has been used in a cyberattack.
Persistently Exploited	Appears each time Tenable observes that the vulnerability is being persistently exploited.
CISA Known Exploits	Indicates the date that the Cybersecurity and Infrastructure Security Agency (CISA) added the vulnerability to their Known Exploited Vulnerabilities catalog.
CISA Due-Date	Indicates the date by which federal agencies must fix vulnerabilities on the CISA Known Exploited Vulnerabilities (KEV) list.
Cyber Exposure	Appears when Tenable publishes a Cyber Exposure Alert for the

Alert	vulnerability.
EPSS Increased	Appears when the Exploit Prediction Scoring System (EPSS) increases (for example, *EPSS Increased to 65%*).
EPSS Decreased	Appears when the EPSS decreases.
EPSS Assigned	Appears when an EPSS score is assigned.
VPR Increased	Appears when the Vulnerability Priority Rating (VPR) increases (for example, *VPR Increased to 6.1*).
VPR Decreased	Appears when the VPR decreases.
VPR Assigned	Appears when a VPR score is assigned.

Scores

The **Scores** tab contains ring charts for VPR and EPSS along with trend charts to track how these scores have changed over time.

In addition, you can review the following **VPR Key Drivers**.

VPR Driver	Description
Age of Vulnerability	Indicates the number of days since the vulnerability was discovered.
CVSSv3 Impact Score	Indicates the NVD-provided CVSSv3 impact score from 0–10. If NVD did not provide a score, Tenable generates one.
Exploit Code Maturity	The highest level of exploit maturity for the vulnerability: **Unproven**, **PoC**, **Functional**, or **High**. Drawn from Tenable's research, as well as key external sources.
Product Coverage	Indicates the relative number of unique products affected. Values are **Low**, **Medium**, **High**, or **Very High**.
Threat Intensity	Indicates the number and frequency of recent threat events. Values are **Very Low**, **Low**, **Medium**, **High**, or **Very High**.
Threat Sources	Lists sources where relevant threat events occurred (for example, social

	media or the dark web). If no events were observed in the past 28 days, **No recorded events** appears.
Threat Recency	Indicates the number of days since a threat event occurred, from 0–180.

Plugins

The **Plugins** tab lists plugins that detected findings for the vulnerability.

Column	Description
Plugin ID	Indicates the ID of the Tenable plugin that detected the finding.
Name	Indicates the name of the Tenable plugin that detected the finding.
Family	Indicates the plugin family. For example, with a Tenable Nessus plugin, *Backdoors*. Or, with a Tenable Web App Scanning plugin, *Code Execution*. To learn more, see About Plugin Families on the Tenable website.
Severity	Indicates severity for the detected vulnerability as **Low**, **Medium**, or **High**.
Type	Indicates the type of plugin: **Active**, **Compliance**, **Event**, **Passive**, or **WAS**.

Products

In the **Products** tab, view affected products by vendor. Next to a vendor, click the drop-down **>** to view a list of products.

For example, a vulnerability might have the **Vendor** *canonical* with the **Product** *linux*.

> **Tip**: Tenable curates this data. It represents all known affected products for a vulnerability, not only yours.

Summary

In the **Summary** tab, read a summary and **Copy** it to your clipboard.

How Does This Affect Me?

On the **Vulnerability Profile** page, view your affected assets and products that relate to the current vulnerability in the **How Does This Affect Me?** section. You can build queries to refine the results.

Affected Assets

The table of results in the **Affected Assets** tab has the following columns, which you can show or hide as described in Interact with a Customizable Table.

Column	Description
Asset ID	Indicates the asset's Universally Unique Identifier (UUID).
Name	The asset identifier, assigned based on the availability of specific attributes in logical order.
Operating System	The operating system for the affected asset.
IP Address	The IPv4 or IPv6 address for the affected asset.
Severity	The severity level of the vulnerabilities on the affected asset.

Sources

In the **Sources** section, search for and review contextual intelligence such as security advisories on the external websites where they appear.

This section contains a table with the following columns.

Column	Description
Source	Links to contextual intelligence about a vulnerability.
Authoritative	Indicates if the source is authoritative with a label such as *Tenable Research* or *NVD* (for the National Vulnerability Database).
Source Details	Provides more information about the source via labels added by the Tenable Research Team (for example, *Third Party Advisory*).

Vulnerability Metrics

In the right-hand **Vulnerability Metrics** pane, review key details in the following sections.

General Information

In the **General Information** section, review when a vulnerability was first discovered, how exploitable it is, and other details.

Field	Description
Tenable Discovery Date	Indicates the date Tenable first discovered the vulnerability.
NVD Published Date	Indicates the date that the National Vulnerability Database (NVD) added the vulnerability.
Exploitability	Describes how easy it is to exploit the vulnerability (for example, *Low Complexity*, *Network Exploitability*).
Exploit Maturity	The highest level of exploit maturity for the vulnerability: **Unproven**, **PoC**, **Functional**, or **High**. Drawn from Tenable's research, as well as key external sources.
First Proof of Concept	Indicates the date the first proof of concept for the vulnerability was released.
First Functional Exploit	Indicates the date the first functional exploit for the vulnerability was released.

Risk Profile

In the **Risk Profile** section, see if the Tenable Research Team is tracking a vulnerability, learn which categories it belongs to, and find out if it can be exploited from a remote network.

Field	Description
Categories	Indicates the categories the vulnerability belongs to, as described in [Vulnerability Categories](). Most vulnerabilities do not have a category.
Tenable Research Watchlist	Indicates that Tenable is actively monitoring the vulnerability since it is being publicly discussed, has a viable proof of concept, and/or is widely used.

Remotely Exploitable	Indicates if the vulnerability can be exploited from a remote network.
Proof of Concept Available	Indicates if Tenable has identified a proof of concept for this vulnerability.

Severity Metrics

In the **Severity Metrics** section, view Common Vulnerability Scoring System (CVSS) v2, v3, or v4, depending on which are available, along with their vector strings.

Field	Description
CVSSv4 Base Score	Indicates the CVSSv4 score. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
CVSSv4 Vector	Lists a vector string with the values used to calculate the CVSSv4 score, for example: *CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H*. To learn more, see the CVSSv4 calculator on the FIRST website.
CVSSv3 Base Score	Indicates the CVSSv3 score. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
CVSSv3 Vector	Lists a vector string with the values used to calculate the CVSSv3 score, for example: *CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H*. To learn more, see the CVSSv3 calculator on the FIRST website.
CVSSv2 Base Score	Indicates the CVSSv2 score. When not available from NVD, Tenable determines this score.
CVSSv2 Vector	Lists a vector string with the values used to calculate the CVSSv2 score.

Latest Plugin Coverage

In the **Latest Plugin Coverage** section, view the most recent Tenable Nessus and Tenable Web App Scanning plugins to detect the vulnerability. Click the links to view plugin details on Tenable's website.

Field	Description
Nessus	Lists the release date of the newest Tenable Nessus plugin to identify the vulnerability.
Web App Scanning	Lists the release date of the newest [[[Undefined variable WebApplicationScanning.WAS]]] plugin to identify the vulnerability.

Identify Your Exposure

On the **Vulnerability Intelligence** page, you can review all vulnerabilities known to Tenable or only those in crucial categories such as **Recently Actively Exploited**. Then, you can compare the list of vulnerabilities to findings in your environment. This process has two parts: 1) review known vulnerabilities and, 2) compare them to your findings.

Review Known Vulnerabilities

First, build a list of known vulnerabilities to compare with your own findings.

To review vulnerabilities known to Tenable:

1. In the left navigation, click ⓘ **Vulnerability Intelligence**.

   The **Vulnerability Intelligence Overview** page appears.

2. (Optional) Click a hexagon tile to choose a [vulnerability category](#). If you want to search all vulnerabilities, click the default category to deselect it.

   In the **CVEs** tab in the lower half of the page, a table of results appears.

   > **Tip**: Under **How Does This Affect Me?** click **Findings** or **Affected Assets** to open those tabs and start reviewing your vulnerabilities.

3. (Optional) Use the *Query Builder* to refine the results, as described in [Use the Query Builder](#).

4. (Optional) In a table row, click the dropdown **>** to view affected assets for the CVE.

5. (Optional) Click a row in the table.

   The **[Vulnerability Intelligence Profile](#) page** for the CVE appears.

Compare Known Vulnerabilities to Your Findings

Once you have built a list of known vulnerabilities, compare them with your findings in the **My Findings** tab or the **My Affected Assets** tab as follows.

Click the **My Findings** tab and do one of the following:

- Refine your results with the Query Builder.

- In a row, click the number in the **Affected Assets** column.

  The **Assets** page appears. It is grouped by **Asset** and lists findings for that Tenable plugin.

- Click the dropdown **>** to display a list of assets with that finding. Then, click an **Asset Name**.

  The **Asset Details** page appears.

Click the **My Affected Assets** tab and do one of the following:

- Refine your results with the Query Builder.

  In a row, click the number in the **Plugin Count** column.

- The **Assets** page appears. It is grouped by **Plugin** and lists findings for that asset.

- Click the dropdown **>** to display a list of assets with that finding. Then, click an **Asset Name**.

  A list of plugins that identified findings on that asset appears.

Use the Query Builder

In the three tabs on the lower part of the **Vulnerability Intelligence** page, use the *Query Builder* to refine your search results with contextual filters.

How Queries Work

Queries are joined by *Conditions* (for example, AND). They have three components:

- **Filter** — The search criteria (for example, for a vulnerability, *Common Name*).

- **Operator** — The condition to filter on (for example, *is not equal to*).

- **Value** — The value to search (for example, a CVE ID of *CVE-2024-3272*).

> **Tip**: You can nest queries with parentheses. For example, to search for CISA Known Exploited vulnerabilities where the VPR is greater than five or the EPSS is greater than 50, use:

Category is equal to CISA Known Exploited AND (VPR is greater than 5 OR EPSS Score is greater than 50).

Build a Query

To build a query with the Query Builder:

1. In the left navigation, click ⓘ **Vulnerability Intelligence**.

   The **Vulnerability Intelligence Overview** page appears.

2. Build a list of CVEs, findings, or affected assets, as described in [Identify Your Exposure](#).

3. Click the query box.

   The **Filters** list appears. To review the filters you can use, see [Query Builder Filters](#).

4. In the **Filters** list, choose a filter.

   The **Operators** list appears.

5. In the **Operators** list, choose an operator.

   For a filter where the value is text or a number, the **Value Hint** box appears. Otherwise, the **Value Options** list appears.

6. Type a Value or select one from the list.

7. (Optional) Add another query (that is, type a Condition and then add a Filter, an Operator, and a Value).

8. Click **Search** or press **Enter**.

   A table of results appears.

Edit a Query

To edit a query, do one of the following.

Action	Description
Replace a query component	In the query box, click the component to replace. A list of options appears.

Delete a query component	On the query component, click the **X**.
Clear a query	On the right side of the query box, click **Clear**.

Keyboard Shortcuts

Use the following keyboard shortcuts in the Query Builder.

Shortcut	Description
Up Arrow or **Down Arrow**	Navigate lists of open-ended values such as text or numbers.
Right Arrow or **Left Arrow**	Move the cursor in your query or choose a date in the date picker.
Enter	Select a query component or date. If no component is selected, apply the query.
Esc	Close a list (for example, the **Filters** list).
Ctrl-C	Copy the highlighted text.
Ctrl-V	Paste your clipboard contents into the Query Builder.
Ctrl-Z	Undo the last action.
Ctrl-Y	Redo the last action.

Query Builder Filters

On the **Vulnerability Intelligence** page and the **Vulnerability Profile** page, use the Query Builder to refine your results. Show only the CVEs, findings, or affected assets you want to take action on.

The following table lists the filters you can use with the Query Builder and the tabs they appear in.

Filter	Description	Appears In...
ACR	Filter by Tenable-defined Asset Criticality Rating (ACR) as a number from 1 to 10.	My Findings, My Affected Assets

AES	Filter by Tenable-defined [Asset Exposure Score](#) (AES) as a number from 0 to 1000.	My Findings, My Affected Assets
Asset ID	Filter by the UUID of the asset. This value is unique to Tenable Security Center.	My Findings, My Affected Assets
Asset Name	Filter by asset name, for example the IPv4 address *206.206.136.40*.	My Findings, My Affected Assets
Category	Filter by category, as described in [Vulnerability Categories](#).	CVEs, My Findings, My Affected Assets
CVE ID	Filter by Common Vulnerabilities and Exposures (CVE) ID, for example *CVE-2002-2024*.	CVEs
CVSSv2 Score	Filter by the CVSSv2 score for the vulnerability, for example *5.2*. When not available from NVD, Tenable determines this score. To learn more, see [CVSS vs. VPR](#).	CVEs
CVSSv3 Attack Complexity	Filter by attack complexity, which defines how difficult it is to use a vulnerability in an attack. Choose from **High** or **Low**.	CVEs
CVSSv3 Attack Vector	Filter by attack vector, which defines an attack's location. Choose from **Adjacent**, **Network**, **Local**, or **Physical**.	CVEs
CVSSv3 Availability	Filter by the affected asset's availability. Choose from **High**, **Low**, or **None**. For example, an affected asset with *High* is completely unavailable.	CVEs
CVSSv3 Score	Filter by the CVSSv3 score for the vulnerability, for example *4.3*. When not available from NVD, Tenable determines this score. To learn more, see [CVSS vs. VPR](#).	CVEs, My Findings, My Affected

		Assets
CVSSv3 Confidentiality	Filter by the expected impact of the affected asset's information confidentiality loss. Choose from **High**, **Low**, or **None**. For example, an affected asset with *High* may have a catastrophic adverse effect on your organization or customers.	CVEs
CVSSv3 Integrity	Filter by the expected impact of the affected asset's data integrity loss. Choose from **High**, **Low**, or **None**.	CVEs
CVSSv3 Privileges Required	Filter by the permission level attackers require to exploit the vulnerability. Choose from **High**, **Low**, or **None**. *None* means attackers need no permissions in your environment and can exploit the vulnerability while unauthorized.	CVEs
CVSSv3 Scope	Filter by whether a vulnerability allows attackers to compromise resources beyond an affected asset's normal authorization privileges. Choose from **Unchanged** or **Changed**. *Changed* means the vulnerability increases the affected asset's privileges.	CVEs
CVSSv3 User Interaction	Filter by whether a vulnerability requires other users (such as end users) for attackers to be able to use it. Choose from **Required** or **None**. *None* is more severe since it means that no additional user interaction is required.	CVEs
CVSSv4 Score	Filter by the CVSSv4 score for the vulnerability, for example, 4.3. When not available from NVD, Tenable determines this score. To learn more, see [CVSS vs. VPR]().	CVEs, My Findings, My Affected Assets
EPSS Score	Filter by the percentage likelihood that a vulnerability will be exploited, based on the third-party [Exploit Prediction Scoring System]() (EPSS). Type a number from 1 to 100 with up to three decimal places, for example,	CVEs

	50.5.	
Exploit Maturity	Filter by exploit maturity based on sophistication and availability. This information is drawn from Tenable's own research as well as key external sources. Choose from **High**, **Functional**, **PoC**, or **Unproven**.	CVEs
First Discovered	Filter for the date a vulnerability was first identified. Use Operators to get results based on a date range, a specific date, vulnerabilities older than a date, and others.	CVEs
First Functional Exploit	Filter for the date a vulnerability was first known to be exploited. Use Operators to get results based on a date range, a specific date, vulnerabilities older than a date, and others.	CVEs
First Proof of Concept	Filter for the date a vulnerability's first proof of concept was found. Use Operators to get results based on a date range, a specific date, vulnerabilities older than a date, and others.	CVEs
IP Address	Filter for affected asset IPv4 and IPv6 addresses as a single IP, an IP range, or an IP Classless Inter-Domain Routing (CIDR) block. For example, type *172.16.2.1–172.16.2.100, ::ffff:c0a8:102*.	My Findings, My Affected Assets
Last Seen	Filter for the date a finding affected or asset last appeared on a scan. Use Operators to get results based on a date range, a specific date, vulnerabilities older than a date, and others.	My Findings, My Affected Assets
Operating System	Filter by assets running the specified operating system.	My Findings, My Affected Assets
Plugins Available	Filter by whether or not a vulnerability currently has a Tenable plugin that detects it. Choose from **Yes** or **No**.	CVEs

Plugin Family	Filter by the family of the Tenable plugin that detected the vulnerability. For example, *Service detection*.	My Findings, My Affected Assets, Plugins
Plugin ID	Filter by the ID of the Tenable plugin that detected the vulnerability, for example *157288*. To look up plugin IDs, go to the [Tenable website](#).	CVEs, My Findings, My Affected Assets, Plugins
Plugin Name	Filter by the name of the Tenable plugin that detected the vulnerability, for example *TLS Version 1.1 Protocol Deprecated*.	My Findings, My Affected Assets, Plugins
Plugin Type	Filter by the type of Tenable plugin that detected the vulnerability. For example, *remote*.	My Findings, My Affected Assets, Plugins
Repository	Filter for assets with associated vulnerability data in the specified repository.	My Findings, My Affected Assets
Severity	Filters by the vulnerability's CVSS-based severity. To learn more, see [CVSS vs. VPR](#).	My Findings, My Affected Assets, Plugins
VPR	Filter by the Tenable-calculated [Vulnerability Priority Rating](#) (VPR) score, as a number from 1 to 10. **Note**: A finding's VPR is based on the VPR of the plugin that identified it. When plugins are associated with multiple vulnerabilities, the highest VPR appears.	CVEs, My Findings, My Affected Assets
VPR Threat	Filter for a vulnerability's Tenable-calculated threat	CVEs

Intensity	intensity based on the number and frequency of threat events. Choose from **Very Low**, **Low**, **Medium**, **High**, or **Very High**.	

CVEs

On the **Vulnerability Intelligence Overview page**, the **CVEs** tab shows vulnerabilities from Tenable's database. All vulnerabilities appear by default, but you can refine the results with vulnerability categories and the query builder.

The table in the **CVEs** tab has the following columns, which you can show or hide as described in Interact with a Customizable Table.

Column	Description
CVE ID	Indicates the Common Vulnerability and Exposure (CVE) identifier for the vulnerability, as assigned by the CISA-sponsored CVE Program.
Name	Indicates the informal name of the vulnerability (for example, *Log4Shell*). Not all vulnerabilities have a common name.
VPR	The Tenable-calculated Vulnerability Priority Rating (VPR) score from 0.1 to 10.
CVSS v2	Indicates the CVSS v2 score for the vulnerability. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
CVSS v3	Indicates the CVSS v3 score for the vulnerability. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
CVSS v4	Indicates the CVSS v4 score for the vulnerability. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
EPSS	Indicates the likelihood that the vulnerability will be actively exploited, based on the third-party Exploit Prediction Scoring System (EPSS).
Exploit Maturity	The highest level of exploit maturity for the vulnerability: **Unproven**, **PoC**, **Functional**, or **High**. Drawn from Tenable's research, as well as key external sources.
First	Indicates the date the vulnerability was first identified.

Discovered	
First Exploited	Indicates the date of the vulnerability's first-known exploitation.
POC	Indicates the date the vulnerability's first proof of concept was discovered.
Plugins	Lists the IDs for the Tenable plugins that detected the vulnerability.

My Findings

On the **Vulnerability Intelligence Overview** page, the **My Findings** tab shows all active, new, or resurfaced findings in your environment that are being tracked by Tenable Vulnerability Management. Refine the results with vulnerability categories and the query builder.

The **My Findings** tab has the following columns, which you can show or hide as described in Interact with a Customizable Table.

Column	Description
VPR	The Tenable-calculated Vulnerability Priority Rating (VPR) score from 0.1 to 10. **Note**: A finding's VPR is based on the VPR of the plugin that identified it. When plugins are associated with multiple vulnerabilities, the highest VPR appears.
Plugin Name	Indicates the name of the Tenable plugin that detected the finding.
Plugin ID	Indicates the ID of the Tenable plugin that detected the finding.
Affected Assets	Indicates the number of affected assets. Click the number to open the **Asset Details** page.
CVES	The CVE IDs associated with the finding.
CVSSv2	Indicates the Common Vulnerability Scoring System (CVSS) v2 score for the finding.
CVSSv3	Indicates the CVSS v3 score for the finding.
CVSSv4	Indicates the CVSS v4 score for the finding.

Affected Assets

In any findings row, click the dropdown **>** to reveal a table of assets on which that finding appears, with the following columns.

Column	Description
Asset Name	The asset identifier, assigned based on the availability of specific attributes in logical order.
Operating System	Indicates the operating system the asset is running.
IP Address	Indicates the IPv4 or IPv6 address for the asset.
Repository	Indicates the repository associated with the asset.
Plugin Count	Indicates the number of plugins that discovered findings on the asset.
ACR	The Asset Criticality Rating for the asset.
AES	The Asset Exposure Score for the affected asset.
Last Seen	Indicates the date when the asset last appeared on a scan.

My Affected Assets

On the **Vulnerability Intelligence Overview** page, the **My Affected Assets** tab shows all assets in your environment with a finding that has not yet been fixed. Refine the results with vulnerability categories and the query builder.

The **My Affected Assets** tab has the following columns, which you can show or hide as described in Interact with a Customizable Table.

Column	Description
Name	The asset identifier, assigned based on the availability of specific attributes in logical order.
Operating System	Indicates the operating system the asset is running.
IP Address	Indicates the IPv4 or IPv6 address for the asset.

Repository	Indicates the repository associated with the asset.
Plugin Count	Indicates the number of Tenable plugins that identified findings on the asset. Click the number to review details on the **Assets** page.
ACR	The Asset Criticality Rating for the asset.
AES	The Asset Exposure Score for the affected asset.
CVES	The CVE IDs associated with the asset.

Plugins

In any asset row, click the dropdown **>** to reveal a table of plugin results for the findings on that asset, with the following columns.

Column	Description
VPR	The Tenable-calculated Vulnerability Priority Rating (VPR) score from 0.1 to 10. **Note**: A finding's VPR is based on the VPR of the plugin that identified it. When plugins are associated with multiple vulnerabilities, the highest VPR appears.
Severity	Indicates the vulnerability's severity based on the Common Vulnerability Scoring System (CVSS).
Plugin Name	Indicates the name of the Tenable plugin that detected the finding.
Plugin ID	Indicates the ID of the Tenable plugin that detected the finding.
Findings	Indicates the number of findings detected on the asset.
CVSSv2	Indicates the CVSSv2 score for the finding.
CVSSv3	Indicates the CVSSv3 score for the finding.
CVSSv4	Indicates the CVSSv4 score for the finding.

Vulnerability Categories

The **Vulnerability Intelligence** page breaks down key vulnerabilities from Tenable's database into curated categories that you select from hexagon-shaped tiles.

While most vulnerabilities do not belong to categories, the ones that do require quick action when found in your environment! To learn how to compare your findings to one of these categories, see [Identify Your Exposure](#).

You can choose from the following categories.

Category	Description
Emerging Threats	Vulnerabilities being actively monitored by Tenable in three areas: • **Vulnerabilities Being Monitored** — Publicly discussed, but no exploit or proof of concept has been disclosed. • **Vulnerabilities of Interest** — Publicly discussed and have a proof of concept that could lead to widespread use by attackers. • **Vulnerabilities of Concern** — Widely discussed and large-scale abuse by attackers is being observed.
CISA Known Exploited	Vulnerabilities that appear in the [CISA Known Exploited Vulnerabilities Catalog](#). CISA suggests that you prioritize remediation efforts for these vulnerabilities since they are known to cause immediate harm.
In the News	Vulnerabilities being widely reported in the press with notable coverage over the past 30 days.
Recently Actively Exploited	Vulnerabilities with notable coverage in the press over the past 30 days, and for which Tenable has evidence of active exploitation.
Ransomware	Vulnerabilities used in current or historical ransomware attacks, as determined from evidence gathered by the Tenable Research team.
Persistently Exploited	Vulnerabilities being leveraged by threat actors over an extended period of time in targeted attacks, ransomware, or malware campaigns. These vulnerabilities are manually curated by the Tenable Research team.
Top 50 VPR	The top 50 vulnerabilities by [Vulnerability Priority Rating](#) (VPR).

Web App Scanning Analysis

> **Required Additional License:** Tenable Web App Scanning

> **Required Tenable Nessus Version:** 10.6.1 or later

The **Web App Scanning** page displays vulnerabilities discovered by web app scans.

Web application scanning in Tenable Security Center allows you to scan and address web application vulnerabilities that traditional scanners cannot scan. For more information about web app scanning, see [Web App Scans](#).

For more information about the **Web App Scanning** analysis page, see:

[Web App Scanning Analysis Tools](#)

[Web App Scanning Analysis Filter Components](#)

[View Web App Scanning Vulnerability Details](#)

[Export Web App Scanning Data](#)

Web App Scanning Analysis Tools

> **Required Additional License:** Tenable Web App Scanning

> **Required Tenable Nessus Version:** 10.6.1 or later

On the **Web App Scanning** page, you can use the drop-down box to select the web app scanning analysis tool you want to view.

Analysis Tool	Description
Asset Summary	Summarizes the scores and counts of web app vulnerabilities for all dynamic or static asset lists.
	A breakdown of each asset's specific web app vulnerabilities and counts for each severity level is also included.
	You can click a count to view the **IP Summary** tool, filtered by the asset list you selected.
CCE Summary	Displays a summary of hosts which have Common Configuration

Analysis Tool	Description
	Enumeration (CCE) vulnerabilities.
	You can click a count to view the **Vulnerability Summary** tool, filtered by the CCE vulnerability you selected.
Class A Summary **Class B Summary** **Class C Summary**	Summarizes host information. The vulnerability score for an address is computed by adding up the number of vulnerabilities at each severity level and multiplying it with the organization's severity score. Starting out with a Class A or Class B summary can identify more active network ranges for networks with a large number of active IP addresses. You can click a **Class A** or **Class B** row to view the **Class B** or **Class C** tool, filtered by the asset list you selected. You can click a **Class C** row to view the **IP Summary** tool, filtered by the asset list you selected.
CVE Summary	Displays web app vulnerabilities grouped by CVE ID, severity, and vulnerability count.
DNS Name Summary	Tenable Security Center includes the ability to summarize information by vulnerable DNS name. The DNS Name Summary displays the matching hostnames, the repository, vulnerability count, and a breakdown of the individual severity counts. You can click a DNS name to view the **Vulnerability List** tool, filtered by the DNS name you selected.
IAVM Summary	Displays web app vulnerabilities grouped by IAVM ID, severity, and vulnerability count.
IP Summary	Summarizes host information, organized by IP address/agent ID. You can click the **IP Address** to view host details, as described in View Host Details. For more information, see View Vulnerabilities by Host.
List OS	Tenable Security Center understands both actively and passively

Analysis Tool	Description
	fingerprinted operating systems. This tool displays a list of discovered operating systems, including the method of discovery (for example, active, passive, or event). You can click a count to view the **IP Summary** tool, filtered by operating system.
Plugin Family Summary	Charts the Nessus, Tenable Network Monitor, or Event plugin family as well as their relative counts based on severity level for all matching vulnerabilities. You can click a count to view the **Vulnerability List** tool, filtered by the plugin family you selected.
Port Summary	Summarizes the ports in use for all matched vulnerabilities. Each port displays a count of vulnerabilities and a breakdown for each severity level. You can click a port to view the **IP Summary** tool, filtered by the port you selected.
Severity Summary	Displays the total number of info, low, medium, high, and critical vulnerabilities. You can click a count to view the **Vulnerability Summary** tool, filtered by the severity you selected.
User Responsibility Summary	Displays a list of the users who are assigned responsibility for the vulnerability based on the user's assigned asset list. Multiple users with the same responsibility are displayed on the same line. Users without any assigned responsibilities are not displayed in the list. Tenable Security Center populates this list after you assign an asset to a user account.
Vulnerability Summary	Displays a table of all plugins associated with vulnerabilities on your network, organized by plugin ID. For more information, see View Vulnerabilities by Plugin.
Web App URL Summary	Displays a list of all web apps associated with vulnerabilities on your network, organized by URL.

Analysis Tool	Description
Web App Vuln Detail List	Displays details for each web app vulnerability. For more information, see [View Web App Scanning Vulnerability Details]().
Web App Vuln List	Displays a list of all web app vulnerabilities discovered on your network, organized by plugin ID.

Web App Scanning Analysis Filter Components

> **Required Additional License:** Tenable Web App Scanning

> **Required Tenable Nessus Version:** 10.6.1 or later

Filters limit the results of the displayed web app vulnerability data and can be added, modified, or reset as desired. For more information, see [Filters]().

Filter Component	Description
Asset Criticality Rating (ACR)	(Requires Tenable Security Center+ license) Filters for vulnerabilities on hosts within the specified ACR range, between 0 and 10. For more information, see [Asset Criticality Rating]() in the *Tenable Vulnerability Management User Guide*. > **Tip:** To edit the ACR for an asset, see [Edit an ACR Manually]().
Asset Exposure Score (AES)	(Requires Tenable Security Center+ license) Filters for hosts within the specified AES range, between 0 and 1000. For more information, see [Asset Exposure Score]() in the *Tenable Vulnerability Management User Guide*.
AES Severity	(Requires Tenable Security Center+ license) Filters for hosts with the specified AES severity. For more information, see [Asset Exposure Score]() in the *Tenable Vulnerability Management User Guide*.

Filter Component	Description
Accept Risk	Displays web app vulnerabilities based on their Accepted Risk workflow status. Available choices include **Accepted Risk** or **Non-Accepted Risk**. Choosing both options displays all vulnerabilities regardless of acceptance status.
Address	This filter specifies an IPv4 or IPv6 address, range, or CIDR block to limit the viewed vulnerabilities. For example, entering *198.51.100.28/24* and/or *2001:DB8::/32* limits any of the web tools to show vulnerability data from the specified networks. You can enter addresses in a comma-separated list or on separate lines.
Agent ID	Displays results matching the specified agent UUID (Tenable UUID). An agent UUID uniquely identifies: • Agent-detected assets that may share a common IP address. • OT Security assets that may not have an IP address. For more information, see OT Security Instances.
Application CPE	Allows a text string search to match against available CPEs. The filter may be set to search based on a **contains**, **Exact Match**, or **Regex Filter** filter. The **Regex Filter** is based on Perl-compatible regular expressions (PCRE).
Asset	This filter displays systems from the assets you select. If more than one asset contains the systems from the primary asset (i.e., there is an intersect between the asset lists), those assets are displayed as well. **Tip:** Use NOT, OR, and AND operators to exclude unwanted assets from the view.
Audit File	Filters vulnerabilities by plugin IDs associated with the audit file used to perform a scan.
CCE ID	Displays results matching the entered CCE ID.
CVE ID	Displays vulnerabilities based on one or more CVE IDs. Type multiple IDs as

Filter Component	Description
	a comma-separated list (e.g., **CVE-2011-3348,CVE-2011-3268,CVE-2011-3267**).
CVSS v2 Score	Displays vulnerabilities within the chosen Common Vulnerability Scoring System version 2 (CVSS v2) score range.
CVSS v2 Vector	Filters results based on a search against the CVSS v2 vector information.
CVSS v3 Score	Displays vulnerabilities within the chosen Common Vulnerability Scoring System version 3 (CVSS v3) score range.
CVSS v3 Vector	Filters results based on a search against the CVSS v3 vector information.
Cross References	Filters results based on a search against the cross reference information in a vulnerability.
DNS Name	This filter specifies a DNS name to limit the viewed vulnerabilities. For example, entering host.example.com limits any of the web tools to only show vulnerability data from that DNS name.
Data Format	Displays results matching the specified data type: **IPv4**, **IPv6**, or **Agent**.
Exploit Available	If set to yes, displays only vulnerabilities for which a known public exploit exists.
Exploit Frameworks	When set, the text option can be equal to or contain the text entered in the option.
Host ID	Displays the host ID of the discovered asset.
IAVM ID	Displays vulnerabilities based on one or more IVAM IDs. Type multiple IDs as a comma-separated list (e.g., *2011-A-0005,2011-A-0007,2012-A-0004*).
Input Name	If the asset is vulnerable to injection attacks, this displays the name of the asset component where an attacker could inject malicious code.
Input Type	If the asset is vulnerable to injection attacks, this displays the component of the asset where an attacker could inject malicious code (for example, a

Filter Component	Description
	form or session cookie).
MS Bulletin ID	Displays vulnerabilities based on one or more Microsoft Bulletin IDs. Type multiple IDs as a comma-separated list (e.g., *MS10-012,MS10-054,MS11-020*).
Mitigated	Displays vulnerabilities for a specific mitigation status: • **Previously Mitigated** — the vulnerability was previously mitigated but it reappeared in a scan and is currently vulnerable • **Never Mitigated** — the vulnerability is currently vulnerable and has never been mitigated For more information about mitigation, see Mitigated Vulnerabilities.
NetBIOS Name	Displays vulnerabilities that match the specified NetBIOS name. In the drop-down, select **Exact Match**, **Contains**, or **Regex Match**. **Regex Match** is based on Perl-compatible regular expressions (PCRE). **Note:** This filter searches for exact matches only. Type the NetBIOS name as *workgroup \ NetBIOS name*.
Operating System	The operating system that a scan identified as installed on the asset.
Patch Published	Some plugins contain information about when a patch was published for a vulnerability. This filter allows the user to search based on when a vulnerability's patch became available: • **None** (displays vulnerabilities that do not have a patch available) • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago**

Filter Component	Description
	More than 30 days ago **Current Month** **Last Month** **Current Quarter** (during the current calendar year quarter) **Last Quarter** (during the previous calendar year quarter) **Current Year** **Last Year** **Custom Range** (during a specific range you specify) **Explicit** (at a specific time you specify)
Plugin Family	This filter chooses a Nessus or Tenable Network Monitor plugin family. Only vulnerabilities from that family display.
Plugin ID	Type the plugin ID desired or range based on a plugin ID. Available operators are equal to (=), not equal to (!=), greater than or equal (>=) and less than or equal to (<=).
Plugin Modified	Tenable plugins contain information about when a plugin was last modified. This filter allows users to search based on when a particular plugin was modified: **Within the last day** **Within the last 7 days** **Within the last 30 days** **More than 7 days ago** **More than 30 days ago** **Current Month** **Last Month**

Filter Component	Description
	Current Quarter (during the current calendar year quarter) **Last Quarter** (during the previous calendar year quarter) **Current Year** **Last Year** **Custom Range** (during a specific range you specify) **Explicit** (at a specific time you specify)
Plugin Name	Using the **Contains** option, type all or a portion of the actual plugin name. For example, entering **MS08-067** in the plugin name filter displays vulnerabilities using the plugin named **MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check)**. Similarly, entering the string **uncredentialed** displays a list of vulnerabilities with that string in the plugin name. Use the **Regex Match** option to filter plugin names based on Perl-compatible regular expressions (PCRE).
Plugin Published	Tenable plugins contain information about when a plugin was first published. This filter allows users to search based on when a particular plugin was created: **Within the last day** **Within the last 7 days** **Within the last 30 days** **More than 7 days ago** **More than 30 days ago** **Current Month** **Last Month**

Filter Component	Description
	• **Current Quarter** (during the current calendar year quarter)
	• **Last Quarter** (during the previous calendar year quarter)
	• **Current Year**
	• **Last Year**
	• **Custom Range** (during a specific range you specify)
	• **Explicit** (at a specific time you specify)
Plugin Type	Select whether to view all plugin types or passive, active, event, or compliance vulnerabilities.
Port	This filter is in two parts. First the equality operator is specified to allow matching vulnerabilities with the same ports, different ports, all ports less than or all ports greater than the port filter. The port filter allows a comma separated list of ports. For the **larger than** or **less than** filters, only one port may be used. **Note:** All host-based vulnerability checks are reported with a port of 0 (zero).
Protocol	This filter provides boxes to select TCP, UDP, or ICMP-based vulnerabilities.
Recast Risk	Displays vulnerabilities based on their Recast Risk workflow status. Available choices include **Recast Risk** or **Non-Recast Risk**. Choosing both options displays all vulnerabilities regardless of recast risk status.
Repositories	Displays vulnerabilities from the chosen repositories.
STIG Severity	Displays vulnerabilities with the chosen STIG severity in the plugins database.
Scan Policy Plugins	Displays vulnerabilities found by the currently enabled plugins in the scan policy. For more information, see The Plugins tab specifies which plugins are used during the policy's Tenable Nessus scan. You can enable or disable plugins in the plugin family view or in the plugin view for more

Filter Component	Description
	granular control..
Security End of Life Date	When available, Tenable plugins contain information about software end of life dates. This filter allows users to search based on when a particular software is end of life:
	• **Within the last day**
	• **Within the last 7 days**
	• **Within the last 30 days**
	• **More than 7 days ago**
	• **More than 30 days ago**
	• **Current Month**
	• **Last Month**
	• **Current Quarter** (during the current calendar year quarter)
	• **Last Quarter** (during the previous calendar year quarter)
	• **Current Year**
	• **Last Year**
	• **Custom Range** (during a specific range you specify)
	• **Explicit** (at a specific time you specify)
Severity	Displays vulnerabilities with the selected severity. For more information, see CVSS vs. VPR.
Users	Allows selection of one or more users who are responsible for the vulnerabilities.
Vulnerability Discovered	Tenable Security Center tracks when each vulnerability was first discovered. This filter allows you to see when vulnerabilities were discovered:

Filter Component	Description
	- **Within the last day** - **Within the last 7 days** - **Within the last 30 days** - **More than 7 days ago** - **More than 30 days ago** - **Current Month** - **Last Month** - **Current Quarter** (during the current calendar year quarter) - **Last Quarter** (during the previous calendar year quarter) - **Current Year** - **Last Year** - **Custom Range** (during a specific range you specify) - **Explicit** (at a specific time you specify) **Note:** The discovery date is based on when the vulnerability was first imported into Tenable Security Center. For Tenable Network Monitor, this date does not match the exact vulnerability discovery time as there is normally a lag between the time that Tenable Network Monitor discovers a vulnerability and the import occurs. **Note:** Days are calculated based on 24-hour periods prior to the current time, not calendar days. For example, if the report run time was 1/8/2019 at 1:00 PM, using a 3-day count would include vulnerabilities starting 1/5/2019 at 1:00 PM and not from 12:00 AM.
Vulnerability ID	The ID for the vulnerability. The authority that identifies a given vulnerability determines the vulnerability's ID format.
Vulnerability	This filter allows the user to see when the vulnerability was last observed

Filter Component	Description
Last Observed	by Tenable Nessus, Tenable Log Correlation Engine, or Tenable Network Monitor: • **Within the last day** • **Within the last 7 days** • **Within the last 30 days** • **More than 7 days ago** • **More than 30 days ago** • **Current Month** • **Last Month** • **Current Quarter** (during the current calendar year quarter) • **Last Quarter** (during the previous calendar year quarter) • **Current Year** • **Last Year** • **Custom Range** (during a specific range you specify) • **Explicit** (at a specific time you specify) **Note:** The observation date is based on when the vulnerability was most recently imported into Tenable Security Center. For Tenable Network Monitor, this date does not match the exact vulnerability discovery as there is normally a lag between the time that Tenable Network Monitor discovers a vulnerability and the import occurs.
Vulnerability Priority Rating (VPR)	Displays vulnerabilities within the chosen VPR range. For more information, see CVSS vs. VPR.
Vulnerability Published	When available, Tenable plugins contain information about when a vulnerability was published. This filter allows users to search based on

Filter Component	Description
	when a particular vulnerability was published:
	• **All**
	• **Within the last day**
	• **Within the last 7 days**
	• **Within the last 30 days**
	• **More than 7 days ago**
	• **More than 30 days ago**
	• **Current Month**
	• **Last Month**
	• **Current Quarter** (during the current calendar year quarter)
	• **Last Quarter** (during the previous calendar year quarter)
	• **Current Year**
	• **Last Year**
	• **Custom Range** (during a specific range you specify)
	• **Explicit** (at a specific time you specify)
Vulnerability Text	Displays vulnerabilities containing the entered text (e.g., php 5.3) or regex search term.
Web App URL	The URL for the discovered web application associated with the vulnerability. Separate multiple URLs with single quotations and commas.

View Web App Scanning Vulnerability Details

Required Additional License: Tenable Web App Scanning

Required Tenable Nessus Version: 10.6.1 or later

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can drill into web app scanning vulnerabilities to view details for each vulnerability instance found on your network.

Tip: A vulnerability instance is a single instance of a web app vulnerability appearing on an asset, identified uniquely by plugin ID, port, protocol, URL, input type, input name, and HTTP method.

To view web app scanning vulnerability instance details:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Web App Scanning**.

   The **Web App Scanning** page appears.

3. In the drop-down box, click **Web App Vuln Detail List**.

   The **Web App Vuln Detail List** tool appears.

   In this tool, you can:

Section	Actions
Options menu	• Export data as a `.csv` or a `.pdf` file, as described in Export Web App Scanning Data. • Set this view as your default view. • Switch between viewing cumulative vulnerabilities or mitigated vulnerabilities, as described in View Cumulative or Mitigated Vulnerabilities. • Save an asset. • Open a ticket, as described in Open a Ticket. • Save a query, as described in Add or Save a Query.
arrows	Click the arrows to view other vulnerability instances related to the plugin.

toolbar	• Create an accept risk rule, as described in [Add an Accept Risk Rule](). • Create a recast risk rule, as described in [Add a Recast Risk Rule]().
Synopsis and **Description**	View information about the plugin, vulnerability instance, and affected assets.
See Also	View related links about the plugin or vulnerability.
Affected Host Asset	View details about the affected host asset, as well as the plugin output.
Discovery	View details about when the vulnerability was first discovered and last observed on your network.
Asset Criticality Rating	View the ACR value for the vulnerability. For more information about ACR values, see [Asset Criticality Rating]() in the *Tenable Vulnerability Management User Guide*.
Asset Exposure Score	View the AES value for the vulnerability. For more information, about AES values, see [Asset Exposure Score]() in the *Tenable Vulnerability Management User Guide*.
Risk Information	View metrics (for example, CVSS score, VPR, and EPSS) about the risk associated with the vulnerability.
Exploit Information	View details about the exploit.
Plugin Details	View details about the plugin.
Attachments	View related attachments for the vulnerability, including the HTTP request and response.

Export Web App Scanning Data

Required Additional License: Tenable Web App Scanning

> **Required Tenable Nessus Version:** 10.6.1 or later

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can export data from the **Web App Scanning** page as a `.csv` or a `.pdf` file.

To export data from the **Web App Scanning** page:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Web App Scanning**.

   The **Web App Scanning** page appears.

3. In the **Export** drop-down box, click **Export** > **Export as CSV** or **Export as PDF**.

   > **Note:** If the record count (rows displayed) of any CSV export is greater than 1,000, Tenable Security Center prompts you for the name of the CSV report you want to generate. After generation, you can download the report from the **Report Results** page.

4. Select or clear the check boxes to indicate which columns you want to appear in the exported file.

5. Click **Submit**.

   Tenable Security Center exports the web app scanning data.

Event Analysis

The **Events** display page contains an aggregation of security events from Tenable Log Correlation Engine. Events can be viewed in a list format with options similar to the Vulnerability interface.

> **Note:** Log Correlation Engine events are not supported in Tenable Enclave Security.

Raw Syslog Events

Tenable Security Center's event filters includes a **Syslog Text** option to narrow down the scope of a set of events, and supports the use of keyword searches for active filters.

Active vs. Archived

In the upper-right corner, click **Active** or **Archived** to switch between the active and archived data. This selection determines whether the displayed events are pulled from the active or an archived event database. The Active view is the default that displays all currently active events. The Archived view prompts for the selection of the Log Correlation Engine and an Archive Silo from which the event data is displayed. In the example below, the Log Correlation Engine and Silo date range are displayed to help the user choose the correct archive data for analysis.

Analysis Tools

A wide variety of analysis tools are available for comprehensive event analysis.

When viewing the analysis tool results, clicking on result will generally take you to the next level of detail for the analysis. For instance, from the Type summary page clicking on a type will display the Normalized Event Summary. Clicking on an even in that list will display the List of Events page featuring that event. Along each progression a new drop-down menu will appear allowing for easy access to either pivot to another analysis tool based on the current view or to return to the previous view.

Additionally most results will have a gear icon next to them. This icon will provide summaries, normally based on time restrictions or a view of the vulnerability summary for the affected host, around that item's result.

For more information, see Event Analysis Tools.

Load Query

The **Load Query** option enables users to load a predefined query and display the current dataset against that query. Click on **Load Query** in the filters list to display a box with all available queries. The query names are displayed in alphabetical order. After clicking on an individual query, the vulnerability view is changed to match the query view for the current dataset.

Event Analysis Filters

For more information, see Event Analysis Filter Components.

Event Analysis Actions

You can use the **Options** drop-down menu to perform the following event analysis actions.

Save Query

You can save the current view as a query for reuse. For more information about queries, see Queries.

Save Asset

Event results can be saved to an asset list for later use. For more information, see Assets.

Save Watchlist

Event results can be saved to a watchlist asset list for later use. For more information, see Assets.

Open Ticket

Tickets are used within Tenable Security Center to assist with the assessment and remediation of vulnerabilities and security events. For more information, see Open a Ticket.

View Settings

When available, this setting controls the columns displayed in your view.

Switch to Archived / Switch Archive / Switch to Active

The **Switch to Archived** item is displayed when viewing active event data and when selected will present a dialog to choose the archived event data to display by Tenable Log Correlation Engine and date range.

The **Switch Archive** menu item is displayed when viewing archived event data. Selecting this option displays the same menu and selections as above to select a different archive silo for viewing.

The **Switch to Active** menu item is displayed when viewing archived data and when selected, changes the view to active event data for analysis.

Export as CSV

Event results can be exported to a comma-separated file for detailed analysis outside of Tenable Security Center by clicking on the Options drop-down menu and then the **Export as CSV** option. When selected, a window opens with an option to choose the columns to be included in the CSV file.

If the record count (rows displayed) of any CSV export is greater than 1,000 records, a note is displayed that prompts for the name of the CSV report to be generated. When complete, the report can be downloaded from the **Report Results** page. For CSV exports of under 1,000 records, the browser's standard **Save As** dialog window is displayed.

Once the appropriate selections are made, click the **Submit** button to create the CSV file or **Cancel** to abort the process.

Event Analysis Tools

> **Note:** Log Correlation Engine events are not supported in Tenable Enclave Security.

A wide variety of analysis tools are available for comprehensive event analysis. Clicking on the drop-down menu indicating the current view (Type Summary by default) displays a list of analysis tools to choose from.

When viewing the analysis tool results, clicking on result will generally take you to the next level of detail for the analysis. For instance, from the Type summary page clicking on a type will display the Normalized Event Summary. Clicking on an even in that list will display the List of Events page featuring that event. Along each progression a new drop-down menu will appear allowing for easy

access to either pivot to another analysis tool based on the current view or to return to the previous view.

Additionally most results will have a gear icon next to them. This icon will provide summaries, normally based on time restrictions or a view of the vulnerability summary for the affected host, around that item's result.

Tool	Description
Asset Summary	This tool can be used to see how certain types of activity, remote attackers, or non-compliant events have occurred across different asset groups. Clicking on the **Total** count for the listed asset displays a Type Summary analysis tool.
Connection Summary	This tool lists connections made between two different hosts by source and destination IP address and the counts of connections between them. Clicking on a host will display the Type Summary analysis tool.
Date Summary	When analyzing large amounts of data, it is often useful to get a quick summary of how the data set manifests itself across several dates. For example, when analyzing a suspected attacker's IP address, creating a filter for that IP address and looking at the type of events is simple enough. However, displaying that same data over the last few days or weeks can paint a much more interesting picture of a potential attacker's activity. Selecting a date will display the Type Summary analysis tool.
Destination IP Summary	This tool displays events listed by the destination IP address recorded. The table lists the Tenable Log Correlation Engine it was discovered on, the IP address, and the count. Clicking on the information icon next to the IP address displays the system information pertaining to the host IP address. Clicking on one of the hosts displays the Type Summary analysis tool.
Detailed Event Summary	This tool displays a summary of the various events based on their full event name and count. Clicking on an event displays the List of Events analysis tool.
Event Trend	This analysis tool displays an event trend area graph with total events over

Tool	Description
	the last 24 hours. Modify the filters for this graph to display the desired event trend view.
IP Summary Class A Summary Class B Summary Class C Summary	Tenable Security Center provides the ability to quickly summarize matching IP addresses by single IP address, Class A, Class B, and Class C addresses. The IP Summary tool displays the associated Tenable Log Correlation Engine server along with the IP address of the reporting system and about the event count for that system. Clicking on an IP address displays a Host Detail window for that IP address. Clicking the information icon next to the IP address displays information about the NetBIOS Name (if known), DNS Name (if known), MAC address (if known), OS (if known), Score, Repository, Last Scan, Passive Data, Compliance Data, and Vulnerability severity counts. The Assets box displays which asset lists the IP address belongs to. The Useful Links box contains a list of resources that can be queried by IP address. Clicking on one of the Resource links causes the resource to be queried with the current IP address. For example, if the current IP address was a publicly registered address, clicking on the ARIN link causes the ARIN database to be queried for the registration information for that address. If custom resources have been added by an administrative user (via the **Manage IP Address Information Links** selection under the **Customization** tab), they will be displayed here. The Sum by Class A, B, and C tools work by displaying matching addresses. Clicking on the number displayed in the Total column will display the Type Summary for that IP address range.
List of Events	This tool displays a line of data for each matching event. The line includes many pieces of information such as time, event name, number of correlated vulnerabilities involved IP addresses, and sensor.
Normalized Event Summary	This tool summarizes a listing of all normalized events and their count for the chosen time period. Normalized events are lower-level events that have been assigned a Tenable name based on Tenable Log Correlation Engine

Tool	Description
	scripts parsing of the log records (e.g., Snort-HTTP_Inspect). Clicking on the event name displays the List of Events analysis tool.
Port Summary	A port summary can be invoked. This tool produces a table of the top used ports and combines counts for source and destination ports into one overall count. Clicking on the port will display a Type Summary of events filtered for that port. **Note:** Port 0 events are host-based events that are not specific to any particular TCP/UDP port.
Protocol Summary	This tool summarizes counts of events based on IP protocols. Clicking on the event total displays a Type Summary view of events filtered by the selected protocol.
Raw Syslog Events	Users can choose to view the original log message or IDS event for full forensic analysis. It is recommended that users attempt some sort of filtering match first before attempting to find their desired event. Users will typically sort their results and drill into the list until they find what they are looking for before attempting to view the raw data.
Sensor Summary	This tool displays the unique event counts for any query from unique sensor types. When a sensor is clicked on, the Type Summary analysis tool is displayed for events from the selected sensor.
Source IP Summary	This tool displays events listed by the source IP address recorded. The table lists the Tenable Log Correlation Engine it was discovered on, the IP address, and the count. Clicking on the information icon next to the IP address displays the system information pertaining to the host IP address. Clicking on one of the hosts displays the Type Summary analysis tool.

Tool	Description
Type Summary	This tool displays the matching unique event types and the number of corresponding events for each.
	The unique event types are based on normalized logs or events such as firewall, system, correlated, network and IDS. These types are high-level types used to describe event types (e.g., login or Ice).
	Clicking on any of the event counts displays the Normalized Event Summary for the type.
User Summary	This tool displays the matching unique event types and the number of corresponding events for each user when user tracking is enabled in Tenable Log Correlation Engine.
	The unique event types are based on normalized logs such as firewall, system, correlated, network, and IDS.
	Clicking on any of the event counts under the **Total** column will display the Type Summary analysis tool.

Event Analysis Filter Components

> **Note:** Log Correlation Engine events are not supported in Tenable Enclave Security.

Filters limit the results of the event data displayed and can be added, modified, or reset as desired. For more information, see Filters.

The **Events** page also supports using a filter bar for filtering. To display the filter bar, in the toolbar, click **More** > **Show Filter Bar**.

> **Note:** The filter bar does not display or adjust the timeframe filter.

Filter Component	Description
Address	Specifies an IP address, range, or CIDR block to limit the displayed events. For example, entering 198.51.100.64/24 limits any of the web tools to show only the event data from that network. You can enter addresses on

Filter Component	Description
	separate lines or comma separated.
Asset	Filter the event by the specified asset list. **Tip:** Use NOT, OR, and AND operators to exclude unwanted assets from the view.
Destination Address	Specifies an IP address or CIDR block to limit the displayed events based on destination. For example, entering 198.51.100.64/24 limits any of the analysis tools to show only the event data with destination IPs in that block. Addresses can be comma-separated.
Destination Asset	Filter the destination address of the event data by the specified asset list. **Tip:** Use NOT, OR, and AND operators to exclude unwanted assets from the view.
Destination Port	This filter is in two parts. Specify the type of filter to allow matching events with the same ports (=) or different ports (≠). The port filter may specify a single, comma separated list of ports or range of ports (for example, 8000-8080).
Detailed Event	This is the detailed event name given by the IDS vendor. For example, an event received from a Snort sensor can have a detailed event name of DOUBLE DECODING ATTACK, which means that HTTP_INSPECT 119:2:1 fired and was sent to the Log Correlation Engine.
Direction	Filter by event direction of All by default or select Inbound, Outbound, or Internal.
Log Correlation Engines	Specify one or more Log Correlation Engines to obtain events from by checking the box next to the choices. **Note:** Log Correlation Engine events are not supported in Tenable Enclave Security.

Filter Component	Description
Normalized Event	The name given to the event by the Log Correlation Engine after the Log Correlation Engine runs its PRM and TASL scripts against it.
Port	This filter is in two parts. Specify the type of filter to allow matching vulnerabilities with the specified ports (=), excluding ports (≠), ports greater than or equal to (≥), or ports less than or equal to (≤). The specified and excluding port filter may specify a single port, comma-separated list of ports, or range of ports (for example, 8000-8080). **Note:** Tenable Security Center reports all host-based vulnerability checks with a port of 0 (zero).
Protocol	Specify the protocol of the event TCP, UDP, or ICMP.
Repositories	Specify the Repositories to obtain events from. You can search the repositories using the search filter at the top. You can select multiple repositories from the list.
Sensor	Filter the events by sensor using the equal (=) or not equal (!=) operators.
Source Address	Specifies an IP address or CIDR block to limit the displayed events based on source. For example, entering 198.51.100.64/24 limits any of the analysis tools to show only the event data with source IPs in that block. Addresses can be comma separated.
Source Asset	Filter the source address of the event data by asset list and select an asset list from those available or the NOT operator to exclude asset lists. After you add each list, the AND or OR operators are available to customize the combining of asset lists.
Source Port	This filter is in two parts. Specify the type of filter to allow matching events with the same ports (=) or different ports (≠). The port filter may specify a single port, comma-separated list of ports, or range of ports (for example, 8000-8080).
Syslog Text	(Raw Syslog Events Analysis Tool) String to search for within the filtered

Filter Component	Description
	event.
Targeted IDS Events	This filter box selects IDS events that have targeted systems and ports with vulnerabilities likely to be exploited by the detected attack. This is determined by comparing the host's vulnerabilities (CVE, etc.) against those tied to the actual IDS event.
Timeframe	**Tip:** Tenable Security Center always uses this filter. By default, it is set for the last 24 hours, based on the time of the page load. By default, Tenable Security Center displays an explicit timeframe using the last 24 hours. Specify either an explicit or relative timeframe for the event filter. Choosing explicit allows for selecting dates and times from a calendar and time sliders for the start and end time. Relative timeframes, available from the drop-down box, range using various time periods from the last 15 minutes to the last 12 months and All.
Type	Use this to filter by the event type (for example, error, Ice, login, or intrusion).
User	Specify only events tied to a particular username.

Note: Clicking on **Clear Filters** causes the filters to return to the default settings.

Mobile Analysis

The **Mobile** page displays lists of vulnerabilities discovered by scanning an ActiveSync, Apple Profile Manager, AirWatch, Good, and/or MobileIron MDM servers.

For information about mobile analysis filtering, see Mobile Analysis Filter Components.

Mobile Analysis Actions

You can use the options in the toolbar to perform the following mobile analysis actions:

- Save Query

- Export as CSV or PDF

Save Query

You can save the current view as a query for reuse. For more information about queries, see [Queries](#).

Export as CSV or PDF

You can export mobile results in the current view to a comma-separated file or a PDF for detailed analysis outside of Tenable Security Center.

> **Note:** If the record count (rows displayed) of any CSV export is greater than 1,000 records, a note is displayed that prompts for the name of the CSV report to be generated. When complete, the report can be downloaded from the **Report Results** page. For CSV exports of under 1,000 records, the browser's standard **Save As** dialog window is displayed.

Select the columns of data you want exported, then click **Submit**.

Mobile Analysis Filter Components

For general information about using filters, see [Filters](#).

Option	Description
Analysis Tool Filter	
Analysis Tool	This drop-down box is used to choose the analysis tool used by the filter. This is the same as selecting the desired analysis tool from the **Analysis** > **Mobile** dialog.
Active Filters	Displays the existing filters and allows the user to selectively remove filters as needed.
Filters	
Identifier	A text based search filter that looks at the **Identifier** option in the repository.
MDM Type	A drop-down box to select the MDM server type of ActiveSync, Apple

Option	Description
	Profile Manager, Good, AirWatch, and MobileIron MDM server.
Model	A text based search filter that looks at the **Model** option in the repository.
Operating System CPE	A text based search filter that looks at the **Operating System CPE** option in the repository.
Plugin ID	Type the Plugin ID to filter results on.
Plugin Output	Filter results based on a text search of plugin output.
Repositories	Display vulnerabilities from the chosen repositories.
Serial Number	This is a text based search filter that looks at the **Serial Number** option in the repository.
Severity	Displays vulnerabilities with the selected severity (**Info**, **Low**, **Medium**, **High**, **Critical**).
Username	This is a text based search filter that looks at the **User** option in the repository.
Version	This is a text based search filter that looks at the **OS Version** option in the repository.
Vulnerability Last Observed (Cumulative only)	This filter allows the user to see when the vulnerability was last observed.

Reports

You can create reports in Tenable Security Center to share data with users in other organizations. For more information about which users can access what data, see Tenable Security Center Architecture.

Tenable provides reporting through an assortment of report templates and customizable report formats, including PDF and CSV.

Custom CyberScope, DISA ASR, and DISA ARF reports are also available for specialized needs. An administrator user must enable report generation options before organizational users can generate reports with CyberScope, DISA ASR, or DISA ARF data.

Custom CyberScope, DISA ASR, DISA ARF, and DISA Consolidated ARF reports are also available for specialized needs. An administrator user must enable report generation options before organizational users can generate reports with CyberScope, DISA ASR, DISA ARF, or DISA Consolidated ARF data.

In Tenable Security Center, organizational users can create custom reports or template-based reports, as described in Create a Custom Report or Create a Template Report.

> **Note:** To create custom PDF reports and template-based reports, you must install either the Oracle Java JRE or OpenJDK (along with their accompanying dependencies) on the system hosting the Tenable Security Center.

> **Tip:** Tenable provides report templates through the Tenable Security Center feed. For a complete index of Tenable-provided report templates, see the Tenable Security Center Report Templates blog.

For more information, see:

- Manage Reports

- Manage Report Results

- CyberScope and DISA Report Attributes

- Report Images

Manage Reports

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

On the **Reports** page of Tenable Security Center, you can manage report definitions and launch reports. For more information, see Reports.

To manage reports:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. Do any of the following:

   - Filter existing report definitions in the reports table.

   - Create a custom report.

   - Create a template report.

   - Edit a report definition.

   - Edit a report outline.

   - Manage filters for a chapter report.

   - Manage filters for a non-chapter report.

   - View a report definition.

   - Copy a report definition.

   - Export a report definition.

   - Import a report definition.

   - Delete a report definition.

   - Launch a report on demand.

   - Add a report to a scan.

Create a Custom Report

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Reports.

Before you begin:

- If you want to create a CyberScope, DISA ASR, DISA ARF, or DISA Consolidated ARF report, confirm an administrator user enabled the corresponding report generation options, as

described in Configuration Settings.

- If you want to create a CyberScope, DISA ARF, or DISA Consolidated ARF report, create report attributes as described in CyberScope and DISA Report Attributes.

To create a custom report definition:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

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

   The **Report Template** page appears.

4. In the **Other** section, click a report tile. For more information, see Report Templates.

5. Configure the options for the report.

   Tenable Security Center displays options relevant to the report format you selected.

6. (Optional) Edit the report outline.

7. Click **Submit** to save your report.

   Tenable Security Center saves your configuration.

Create a Template Report

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

Template reports are formatted reports that can be customized using chapter and target selections. For more information, see Reports.

To create a template report:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

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

   The **Report Template** page appears.

4. Do one of the following to locate a specific template:

   - In the **Search Templates** box in the top right corner of the page, search for a specific template by keyword.

     > **Tip:** After the initial search, you can limit search results by template category.

   - In the **Common** section, click a template category to view the related templates. For more information, see Report Templates.

5. Click a template report.

   > **Note:** Each template description specifies which Tenable Security Center data must be available to obtain a complete report. For more information, see Data Required for Template-Based Reports.

6. (Optional) In the **Chapters** section, select which chapters from the template you want to include in your report. By default, the report includes all chapters from the template.

7. In the **Focus** section, do one of the following:

   Target all systems in the report.

   > **Note:** This is the default setting.

   To return to this setting, click **All Systems** in the **Targets** drop-down box.

   Target specific assets in the report.

   a. In the **Targets** drop-down box, click **Assets**.

   b. Select **Assets** and **Repositories**.

   Target specific IP addresses in the report.

a. In the **Targets** drop-down box, click **IP Addresses**.

b. In the **IP Addresses** box, type the IP address or addresses where you want the report to focus. Use commas to separate multiple addresses.

c. In the **Repositories** box, select a target repository or repositories.

Target specific repositories in the report.

a. In the **Targets** drop-down box, click **Repositories**.

b. In the **Repositories** box, select a target repository or repositories.

8. (Optional) Edit the default text in the **Description** box.

> **Note:** You cannot modify any information in the **Details** section of the page.

9. Click **Add**.

Tenable Security Center creates a report based on the template and displays the **Reports** page. The new report appears as the last entry in reports table.

10. (Optional) Modify report options that are common to both custom and template reports. For more information, see Report Options.

For example, the default value for the **Schedule** option for all template-based reports is **On Demand**. If you want to run the report automatically, modify the **Schedule** option for the report.

11. (Optional) Customize the report outline, as described in Edit a Report Outline.

For example, you might want to use text elements to add your business context to template-based chapters.

Data Required for Template-Based Reports

Each report template description contains icons that represent which types of data must be available on Tenable Security Center to obtain a complete report.

Hover the cursor over the icon to display the label.

Icon	Label	Action Required

🏷️	Asset Required	Configure an IPv4/IPv6 repository and store scan results in the repository; see [Local Repositories](#) and [IPv4/IPv6 Repositories](#).
📋	Audit File Required	Upload audit files and add them to your scan policy; see [Audit Files](#) and [Scan Policies](#).
	Compliance Data Required	
🗝️	Local Checks Required	Configure and run credentialed scans; see [Active Scans](#).
📱	Mobile Data Required	Configure a mobile repository and store scan results in the repository; see [Mobile Repositories](#).
NS	Active Data Required	Configure a Tenable Nessus scanner and run active scans. For more information, see [Tenable Nessus Scanners](#) and [Active Scans](#).
PVS	Passive Data Required	Configure a Tenable Network Monitor (NNM) scanner; see [Tenable Network Monitor Instances](#).
LCE	Event Data Required	Configure a Tenable Log Correlation Engine server; see [Tenable Log Correlation Engines](#).

Report Templates

Tenable Security Center provides a selection of report templates and customizable report formats. You can configure a Tenable-provided report template or you can create a fully customized report from one of the available formats. For more information, see [Reports](#).

For a complete index of Tenable-provided report templates, see the [Tenable Security Center Report Templates](#) blog.

Template	Description
Common	
Compliance & Configuration Assessment	Reports that aid with configuration, change, and compliance management.

Discovery & Detection	Reports that aid in trust identification, rogue detection, and new device discovery.
Executive	Reports that provide operational insight and metrics geared towards executives.
Monitoring	Reports that provide intrusion monitoring, alerting, and analysis.
Security Industry Trends	Reports related to trends, reports, and analysis from industry leaders.
Threat Detection & Vulnerability Assessments	Reports that aid with identifying vulnerabilities and potential threats.
Other	
PDF	Create a Portable Document Format (PDF) report that can be viewed universally.
CSV	Create a Comma Separated Values (CSV) report that can be imported into spreadsheets or databases.
DISA ARF	(Requires [Report Generation](#) configuration) Create a report that meets the standards of the Defense Information Systems Agency Assessment Results Format (DISA ARF).
DISA Consolidated ARF	(Requires [Report Generation](#) configuration) Create a report that meets the standards of the Defense Information Systems Agency Consolidated Assessment Results Format (DISA Consolidated ARF).
DISA ASR	(Requires [Report Generation](#) configuration) Create a report that meets the standards of the Defense Information Systems Agency Assessment Summary Results (DISA ASR).
CyberScope	(Requires [Report Generation](#) configuration) Create a report that meets CyberScope reporting standards to support FISMA compliance.

Edit a Report Definition

In Tenable Security Center, you can edit both custom reports and reports based on templates.

To edit a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

4. Modify the report options.

   > **Note:** Tenable Security Center displays options relevant to the report type.

5. (PDF and template reports only) Edit the report outline.

6. Click **Submit** to save your changes to the report.

Report Options

In Tenable Security Center, you can configure the options described below for both custom and template reports. For information on how to create reports, see Create a Custom Report and Create a Template Report.

The option descriptions on this page are grouped as they appear on the **Add Report** and **Edit Report** pages. In the options tables, the **Relevant Reports** column specifies which report types use each option.

> **Note:** Tenable Security Center classifies a template-based report as a PDF report. You can configure the same options for that report as you can for a PDF report.
>
> During template report creation, Tenable Security Center set these options to default values. You can change these options for a template report only after creation is complete.

- [General Options](#)
- [Report Options](#)
- [Definition Options](#)
- [Display Options](#)
- [Distribution Options](#)

General Options

Option	Description	Relevant Reports
Name	Name assigned to the report.	Any
Description	Descriptive text for the report.	Any
Schedule	Determines how often the report runs. Options are **On Demand**, **Now**, **Once**, **Daily**, **Weekly**, or **Monthly**. When you select a frequency from the drop-down box, Tenable Security Center displays additional options for the selected time frame.	Any
Attribute Sets	Predefined operational attributes that add required information to DISA ARF, DISA Consolidated ARF, or CyberScope report types. The drop-down box displays only the attribute set defined for the report you are currently creating.	DISA ARF, DISA Consolidated ARF, CyberScope
ASR Content	When creating a report, this drop-down box offers a selection of Benchmark, IAVM, CVE, or Plugin ID to be included.	DISA ASR, DISA Consolidated ARF

Option	Description	Relevant Reports
ASR Record Format	This drop-down box determines the format (Summary or Detail) of the DISA ASR report.	DISA ASR
Include ARF	When enabled, allows for the inclusion of a DISA attribute set for the report.	DISA ASR
Benchmarks	Benchmarks are generated after a scan using certain audit files that have been successfully run against at least one target system.	DISA ASR, DISA Consolidated ARF, CyberScope

Report Options

Option	Description	Relevant Reports
Style	A compound value that specifies the report style, paper size, and orientation. For example, **Plain, Letter**	PDF

Report styles include:

- **Plain** — a report with basic graphs

- **Tenable** — a report with basic graphs and a [footer logo](#) on the cover page

- **Tenable 3D** — a report with enhanced 3D graphs and a [footer logo](#) on the cover page

> **Note:** If an administrator configured a Classification Type banner, plain report styles are the only options listed.

Paper sizes include:

- **Letter** — the standard 8.5 inches x 11 inches letter size

> **Note:** Letter size is the default paper size, used by

Option	Description	Relevant Reports
	options that do not explicitly state a paper size. For example, the paper size for **Plain, Landscape** is letter size.	
	• **A4** — the standard 8.27 inches x 11.69 inches A4 size Orientation options include: • **Portrait** — vertical Note: Portrait is the default orientation, used by options that do not explicitly state an orientation. For example, the orientation for **Plain, Letter** is vertical. • **Landscape** — horizontal	
Include Cover Page	Include a cover page in the report. Cover pages include: • a cover logo • the scan **Name** • the date and time you generated the report • the date and time Tenable Security Center imported the scan results, if you generated the report from scan results • the scan result **ID**, if you generated the report from scan results	PDF
Include Header	Include a predefined header in the report.	PDF
Include Footer	Include a predefined footer in the report.	PDF
Include Table of Contents	Include a table of contents with the report.	PDF

Option	Description	Relevant Reports
Include Index	Include an Index with the report.	PDF
Cover Logo	Specifies which image to use for the lower-left footer logo on the cover page of the report. The default logo is the Tenable logo. To add a custom logo, see Report Images. **Note:** The Plain report style suppresses this footer logo on the cover page.	PDF
Footer Logo	Specifies which image to use for the lower-left footer logo on all pages *except* the cover page. The default logo is the Tenable logo. To add a custom logo, see Report Images.	PDF
Watermark	Specifies a watermark for each page of the report. The default is no watermark. To add a custom watermark, see Report Images.	PDF
Encrypt PDF	Protect the PDF with a password and 256-bit Advanced Encryption Standard (AES) encryption. When enabled, the **Password** text box appears. Enter a password to use to open the report and view its contents.	PDF

Definition Options

Tenable Security Center displays definition options relevant to the report or report element type.

Option	Description	Relevant Reports
Add Chapter	The primary component in the report organization. Chapters are listed in the table of contents for the report and consist of sections and elements. For more information, see Add a Custom Chapter to a Report and Edit a Report Outline.	PDF
Add Template Chapter	A predefined chapter from a Tenable-provided report template. For more information, see Add a	PDF

Option	Description	Relevant Reports
	[Template Chapter to a Report](#).	
Query	A list of predefined queries you can use to retrieve data for the report. For more information, see [Queries](#).	CSV, DISA ARF, DISA Consolidated ARF, DISA ASR, CyberScope; Iterator, Table, and Chart elements in PDF
Type	The type of data to include in the report.	CSV; Iterator, Table, and Chart elements in PDF
Source	The source of the data to include in the report. For CSV reports, valid values for this field differ based on the setting of the **Type** option: • If **Type** is set to **Vulnerability**, valid **Source** values are: ◦ **Cumulative**—All vulnerabilities, regardless of whether the vulnerabilities have been remediated or not ◦ **MItigated**—Remediated vulnerabilities ◦ **Individual Scan**—Vulnerabilities identified in a specific scan **Note:** If you select **Individual Scan**, Tenable Security Center displays the **Selected Scan** option, which allows you to select a scan to use as the basis of the report:	CSV, DISA ARF, DISA Consolidated ARF, DISA ASR, CyberScope; Iterator, Table, and Chart elements in PDF

Option	Description	Relevant Reports

	a. Click one of the predefined date ranges, or click **Custom Range** and enter starting and ending days for the range.
	
	    b. Click **Fetch Scans** to view a list of possible scans within the date range.
	
	    c. Click the scan you want to use in the drop-down box.
	
	• If **Type** is set to **Event**, valid **Source** values are:
	
	    ◦ **Active**—Currently active events
	
	    ◦ **Archive**—Archived events
	
	        Note: If you select **Archive**, Tenable Security Center displays additional options, allowing you to select the **LCE** that collected the events and the **Silo** that stores the archived events.
	
	• If **Type** is set to **Mobile**, Ticket, or Alert, this option is absent.
	
	For DISA ARF, DISA Consolidated ARF, and DISA ASR reports, you do not set the **Type** option. Valid **Source** values are limited to **Cumulative** and **Individual Scan**, which operate in the same way as they do for CSV reports.	

Tool	Select the tool Tenable Security Center uses to analyze the data in the report.	CSV; Iterator, Table, and Chart elements in PDF
Filters	Specifies additional criteria to refine report data.	CSV, DISA ARF, DISA

Option	Description	Relevant Reports
	For more information, see Manage Filter Components for a Non-Chapter Report.	Consolidated ARF, DISA ASR, CyberScope; Iterator, Table, and Chart elements in PDF
Find/Update Filters	This option appears after you add at least one chapter to the report. For more information, see Manage Filter Components for Multiple Elements.	PDF

Display Options

These options allow you to specify column format information format. A selection to define the columns and number of results to appear in the report is then available for configuration.

Option	Description	Relevant Reports
Results Displayed	The number of results included in the CSV file.	CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF
Sort Column	The column that Tenable Security Center uses to sort results in the CSV file. Available columns depend on: • the **Type** you selected in the **Definition** options • the **Display Columns** value you select in the **Display** options	CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF
Sort Direction	The sort direction for results in the CSV file.	CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF

Option	Description	Relevant Reports
Display Columns	The columns included in the results file. Available columns depend on **Definition** options you select. **Tip:** The **Display Columns** appear in the results file in the order in which you select them.	CSV; Iterator, Table, Bar Chart, and Pie Chart elements in PDF

Distribution Options

Distribution options specify the actions Tenable Security Center takes when a report run completes.

Option	Description	Relevant Reports
Email Users	Select Tenable Security Center users to whom Tenable Security Center emails the completed report. The drop-down list includes only users with defined email addresses.	Any
Email Addresses (cc)	Add CC email addresses where Tenable Security Center emails the completed report. You can specify multiple email addresses, separated by commas.	Any
Email Addresses (bcc)	Add Bcc email addresses where Tenable Security Center emails the completed report. You can specify multiple email addresses, separated by commas.	Any
Share	Allows you to select which Tenable Security Center users within your organization can view the completed report in Tenable Security Center. Use this option if organizational policies prohibit emailing potentially sensitive data.	Any
Publishing Sites	Allows you to select predefined publishing sites where Tenable Security Center uploads the completed report. For more information, see Publishing Sites Settings.	Any

Edit a Report Outline

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

In Tenable Security Center, the report outline allows you to modify the structure of a PDF or template-based report.

The outline consists of the following components:

Component	Outline Level	Description
chapter	primary	Highest-level component. Can contain any type of element (grouping, text, chart).
element	subordinate	A grouping, text, or chart element. Can be nested in a chapter or grouping component.

To edit a report outline:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. The outline is, by default, expanded.

4. In the report outline, you can:

   - Expand or collapse elements nested in the outline by clicking **Collapse All** or **Expand All** at the top of the outline.

   - Expand or collapse elements nested in an individual chapter or element by clicking the arrow next to the element.

   - Add a custom chapter.

- [Add a template chapter](#).

- [Add or edit a report element](#).

- [Reorder chapters and elements in a report](#).

- Delete a report element by clicking the delete icon next to the element.

  > **Note:** Tenable Security Center does not ask you to confirm this deletion. However, the deletion is not final until you save all changes to the report.

5. Click **Submit** to save your changes to the report.

Add a Custom Chapter to a Report

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

In Tenable Security Center, you can add custom chapters to PDF or template-based reports.

To add a custom chapter to a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. At the bottom of the report outline, click **Add Chapter**

> **Tip:** If the report contains multiple chapters or sections, scroll down to locate the bottom navigation bar. It can also be helpful to click **Collapse All** on the top navigation bar to collapse the outline to its highest-level components.

The **Add Chapter** page appears.

5. In the **Name** box, enter a title for the chapter.

6. In the **Location** box, select a relative location for the chapter within the report.

7. In the **Style** box, select a style for the report.

8. Click **Submit**.

   Tenable Security Center adds the chapter to the report and displays the **Edit Report** page.

9. Click **Submit** to save your changes to the report.

Add a Template Chapter to a Report

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

In Tenable Security Center, you can add template chapters to template reports and custom PDF reports.

To add a template-based chapter to a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. At the bottom of the outline, click **Add Template Chapter**.

5. Do one of the following:

   - In the **Search Templates** box in the top right corner of the page, search for a specific template by keyword.

     > **Tip:** After the initial search, you can limit search results by template category.

   - Click a template category icon to view the related templates.

6. Click the report template that contains chapters you want to include in your custom report.

7. (Optional) Modify the default options for the report template:

   a. In the **Chapters** section, select which chapters from the template you want to include in your report. By default, the report includes all chapters from the template.

   b. Do one of the following:

      - In the **Focus** section, target all systems in the report.

        This is the default setting. To return to this setting, click **All Systems** in the **Targets** drop-down box.

      - Target specific assets in the report.

        i. In the **Targets** drop-down box, click **Assets**.

        ii. Select **Assets** and **Repositories**.

      - Target specific IP addresses in the report.

        i. In the **Targets** drop-down box, click **IP Addresses**.

        ii. In the **IP Addresses** box, type the IP address or addresses where you want the report to focus. Use commas to separate multiple addresses.

        iii. In the **Repositories** box, select a target repository or repositories.

      - Target specific repositories in the report.

i. In the **Targets** drop-down box, click **Repositories**.

ii. In the **Repositories** box, select a target repository or repositories.

c. (Optional) Edit text in the **Description** box.

> **Note:** You cannot modify any information in the **Details** section.

8. Click **Add**.

Tenable Security Center adds the template chapter or chapters to your custom report and displays the **Add Report** page again.

9. (Optional) Change the template chapter options.

a. Click the edit icon next to the chapter you added.

b. In the **Name** box, edit the chapter title.

c. In the **Location** box, change the relative location for the chapter within the report.

d. In the **Style** box, select a style for the chapter.

e. Click **Submit** to save your changes to the chapter.

10. Click **Submit** to save your changes to the report.

Add or Edit a Report Element

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can add or edit elements within chapters or grouping elements in Tenable Security Center reports.

To add or edit a report element:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

Right-click the row for the report you want to edit, and click **Edit**.

The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see
   Edit a Report Outline.

4. Do one of the following:

   • Click **Add Element** next to the element where you want to add the element.

   • Click the edit icon next to the element you want to change.

     > **Tip:** To display **Add Element** or the edit icon, hover the cursor over the element.

5. Configure any of the following types of elements:

   • **Grouping**

   • **Text**

   • **Charts**

6. Click **Submit** to save your changes to the report.

Configure a Grouping Element in a Report

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions.
> For more information, see User Roles.

Grouping elements in Tenable Security Centerreports include:

Type	Description	Relevant Reports
Group	Groups associated elements on the same page.	PDF
Section	Allows you to organize content within chapters.	PDF
Iterator	Allows you to specify how the report groups its data. For example, if an **Iterator Type** of **Port Summary** is chosen for a vulnerability report, vulnerability data in the report is grouped by	PDF

Type	Description	Relevant Reports
	detected ports. If you do not configure an iterator, hosts and vulnerabilities are listed in the report individually.	

To configure a grouping element:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.

4. Click **Add Element**.

   > **Tip:** To display **Add Element**, hover the cursor over the element.

5. Do one of the following:

   - Add a group to the report.

     a. In the **Grouping** section, click the **Group** icon.

     b. Configure the following options:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.

- Add a section to the report.

  a. In the **Grouping** section, click the **Section** icon.

  b. Configure the following options:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.

- Add an iterator to the report.

  a. In the **Grouping** section, click the **Iterator** icon.

  b. Configure the following options:

Option	Action
General	
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.
Definition	
Query	Select a predefined query to define the data included in the element. For more information, see Queries.
Type	Select the type of data to include in the element. Iterator elements support vulnerability or event data only.
Source	Select the source of the data included in the element. Valid values for this field differ based on the setting of the **Type** option:

- If **Type** is set to **Vulnerability**, valid **Source** values are:

  - **Cumulative**—All vulnerabilities, regardless of whether the vulnerabilities have been remediated or not

  - **MItigated**—Remediated vulnerabilities

  - **Individual Scan**—Vulnerabilities identified in a specific scan

    > **Note:** If you select **Individual Scan**, Tenable Security Center displays the **Selected Scan** option, which allows you to select a scan to use as the basis of the report:
    >
    > a. Click one of the predefined date ranges, or click **Custom Range** and enter starting and ending days for the range.
    >
    > b. Click **Fetch Scans** to view a list of possible scans within the date range.
    >
    > c. Click the scan you want to use in the drop-down box.

- If **Type** is set to **Event**, valid **Source** values are:

  - **Active**—Currently active events

  - **Archive**—Archived events

    > **Note:** If you select **Archive**, Tenable Security Center displays additional options, allowing you to select the **LCE** that collected the events and the **Silo** that stores the archived events.

Filters	Specify additional criteria to refine element data. See

	Manage Filters for a Chapter Report
Iterator Type	Select a grouping method for iteration data: • **IP Summary**—Group vulnerability or event data by the IP addresses of detected hosts. • **Port Summary**—Group vulnerability or event data by the detected ports. • **Type Summary**—Group event data by event type. • **User Summary**—Group event data by user. • **Vulnerability Summary**—Group vulnerability data by individual vulnerability.
Results Displayed	Select the number of results you want to include in the iteration.
Sort Column	Select the column that Tenable Security Center uses to sort the iteration data.
Sort Direction	Select the sort direction for the iteration data.
Header Information	Select the columns you want to include in the iteration data. Available columns depend on the settings of the **Type** and **Source** options.

6. Click **Submit** to save the element.

7. Click **Submit** to save your changes to the report.

Configure a Text Element in a Report

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

Text elements in Tenable Security Center reports include:

Type	Description	Relevant Reports
Matrix	Data in a chart layout.	PDF
Table	Data in a table layout (max results displayed: 999). The underlying data set determines the report display. The default view for most reports is host-centric and Tenable Security Center presents the user with the ability to choose a vulnerability-centric report (a listing of vulnerabilities with all associated hosts).	PDF
Paragraph	Descriptive text that can be inserted anywhere in the report. Use this option to describe table elements or report output for the viewer.	PDF
Assurance Report Card	An element based on the results of a selected Assurance Report Card.	PDF

To configure a text element in a report:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   –or–

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.

4. Do one of the following:

- Click **Add Element** to add an element.

- Click the edit icon next to the element to edit an existing element.

> **Tip:** To display **Add Element** and the edit icon, hover the cursor over the element.

5. Do one of the following:

   - [Add a matrix to the report](#).

   - [Add a table to the report](#).

   - Add a paragraph to the report.

     a. In the **Text** section, click the **Paragraph** icon.

     b. Configure the following options:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.
Text	Type the text of the paragraph.

     c. Click **Submit** to save your changes to the element.

   - Add an Assurance Report Card to the report.

     a. In the **Text** section, click the **Assurance Report Card** icon.

b. Configure the following options:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.
Assurance Report Card	Select the Assurance Report Card (ARC) you want to add to the report. For more information on ARCs, see Assurance Report Cards.

c. Click **Submit** to save your changes to the element.

6. Click **Submit** to save your changes to the report.

Configure a Matrix Element in a Report

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

A matrix element is a type of text element you can insert into a Tenable Security Center report definition. For more information on text elements, see Configure a Text Element in a Report.

To configure a matrix element in a report:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.

4. Do one of the following:

   • Add a new element.

      a. Click **Add Element**.

      b. In the **Text** section, click the **Matrix** icon.

      • Click the edit icon next to the element you want to change.

   > **Tip:** To display **Add Element** and the edit icon next to an element, hover the cursor over the element.

5. Configure the **General** options:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.

6. In the **Cells** section, select the number of columns and rows you want the matrix to include. By default, the matrix is 4 cells by 4 cells.

7. Click **Generate Cells**.

   Tenable Security Center displays the empty matrix for configuration.

8. Do one of the following:

   • Edit a row or column header.

      a. Click the header for the row or column you want to edit.

      b. Next to the header label, click the ⚙ menu.

         The actions menu appears.

      c. Click **Edit Header**.

d. In the **Label** box, type a new header.

e. Click **Submit**.

- Add a matrix component.

    a. Click the matrix cell where you want to add the component.

    b. In the **Data Type** drop-down box, select the type of data for the component.

    c. In the **Type** drop-down box, select the type of calculation you want the component to perform.

    d. In the **Source** drop-down box, select a data source.

    e. (Optional) In the **Filter** box, add or edit a filter using the same steps you would to add a filter to a report element; see Manage Filter Components for a Single Element.

    f. In the **Rules** section, click **Add Rule** to add a rule.

    -or-

    Click the edit icon next to a rule to edit an existing rule.

    g. Click **Submit** to save your changes to the component.

- Copy a row or column.

    a. Click the header for the row or column you want to copy.

    b. Next to the header label, click the ⚙ menu.

    The actions menu appears.

    c. Click **Copy**.

    For columns, Tenable Security Center inserts the copied column to the right of the original column

    For rows, Tenable Security Center inserts the copied row under the original row.

- Delete a row or column.

a. Click the header for the row or column you want to delete.

b. Next to the header label, click the ⚙ menu.

The actions menu appears.

c. Click **Delete Cells**.

9. Click **Submit** to save your changes to the element.

10. Click **Submit** to save your changes to the report.

Example

Current Vulnerabilities

	New IP's	Info	Low	Medium	High	Critical
< 7 Days	895	895	62	67	24	21
8 - 14 Days	43	43	7	20	11	9
15 - 21 Days	5	5	12	21	13	4
22 - 30 Days	1	1	2	2	2	2

Configure a Table Element in a Report

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

A table element is a type of text element you can insert into a Tenable Security Center report definition. For more information on text elements, see Configure a Text Element in a Report.

To configure a table element in a report:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

The report outline appears. This outline is, by default, expanded. For more information, see [Edit a Report Outline](#).

4. Do one of the following:

   - Add a new element.

     a. Click **Add Element**.

     b. In the **Text** section, click the **Table** icon.

   - Click the edit icon next to the element you want to change.

   > **Tip:** To display **Add Element** and the edit icon next to an element, hover the cursor over the element.

5. Configure the **General** options:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.

6. Configure the **Data** options:

Option	Description
Type	
Query	
Source	Equivalent to the **Definition** option of the same name in [Report Options](#).
Tool	
Filters	

7. Configure the **Display** options:

Option	Description
Results Displayed	Equivalent to the **Display** option of the same name in Report Options.
Sort Column	
Sort Direction	
Display Columns	

8. Click **Submit** to save your changes to the element.

9. Click **Submit** to save your changes to the report.

Example

Highest Ranked Asset Vulnerability Index [Scan Result #23]

Asset	Score	Total	Med.	High	Crit.
All Defined Assets	13593	1423	541	777	105
Linux Hosts	4189	476	193	257	26
Linux Kernel 2.6	4092	453	174	253	26
CentOS	3625	386	115	252	19
Linux Kernel 64-Bit	1294	141	68	61	12
Ubuntu Linux	380	48	40	2	6
Debian Linux	74	10	8	1	1
Linux Kernel 3.1	9	3	3	0	0
Linux Kernel 3.2	6	2	2	0	0
Linux Kernel 3.3	6	2	2	0	0

Configure a Charts Element in a Report

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

Charts elements in Tenable Security Center reports include:

Option	Description	Relevant Reports
Bar Chart	Click to add a bar chart element to the report.	PDF
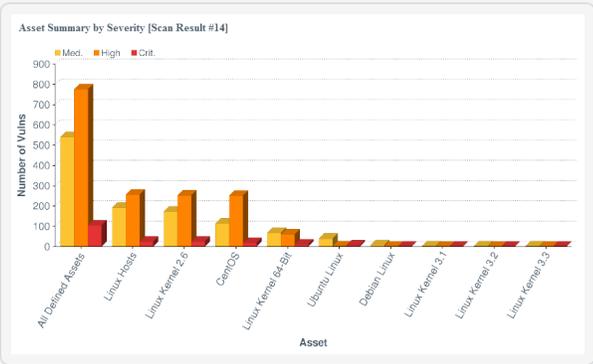
Option	Description	Relevant Reports
Pie Chart	Click to add a pie chart element to the report. 	PDF
Line Chart	Click to add a line chart element to the report. Line charts are defined by time (x-axis) and series data (y-axis). When selecting the time, available options include Relative time and Absolute time. One or more series data elements can be	PDF
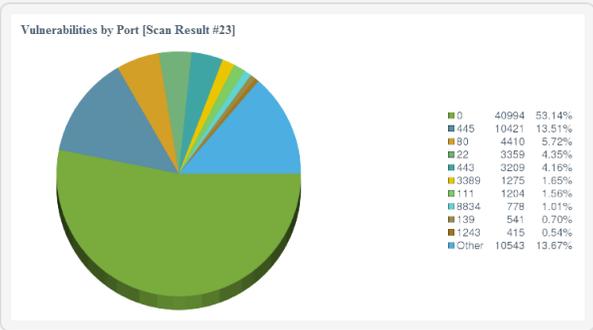
Option	Description	Relevant Reports
	chosen and displayed as discrete lines for easy comparison.	
Area Chart	Click to add an area chart element to the report. Area charts are defined by time (x-axis) and series data (y-axis). When selecting the time, available options include Relative time and Absolute time. One or more series data elements can be chosen and displayed as a stackable view for easy comparison.	PDF
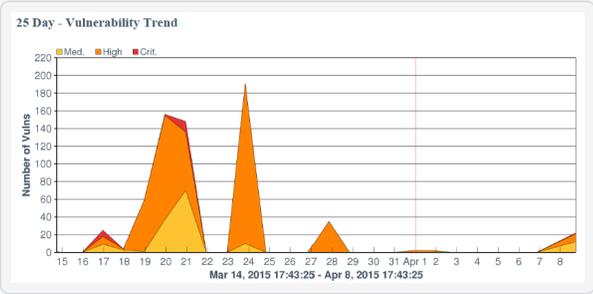
To configure a chart element in a report:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.

4. Do one of the following:

- Add a chart element

  a. Click **Add Element** to add an element.

  b. In the **Charts** section, click the icon for the type of chart you want to add.

- Click the edit icon next to an existing chart element.

> **Tip:** To display **Add Element** and the edit icon, hover the cursor over the element.

5. For all charts, configure the **General** options:

Option	Action
Name	Type a name for the element.
Location	Select a location for the element in the report.
Style	Select a style for the element.

6. For bar charts and pie charts, configure the following **Data** options:

Option	Action
Type	
Query	
Source	Equivalent to the option the **Definition** option of the same name in Report Options.
Tool	
Filters	

7. For line charts and area charts, configure the following **Data** options:

Option	Action
Data Type	Valid values are **Relative** and **Absolute**. Use to configure the x-axis of the chart.

Data Range	Use to configure the x-axis of the chart:
	• If you select **Relative** for **Data Type**, select a relative date range.
	• If you select **Absolute** for **Data Type**, select a specific start and end date for the data.
Series	Use to configure the y-axis of the chart. Line charts and area charts require that you configure at least one series.

8. For bar charts and pie charts, configure the following **Display** options:

Option	Action
Results Displayed	
Sort Column	Equivalent to the **Display** option of the same name in Report Options.
Sort Direction	
Display Columns	

9. Click **Submit** to save your changes to the element.

10. Click **Submit** to save your changes to the report.

Reorder Report Chapters and Elements

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

In Tenable Security Center, you can reorder chapters and elements in a PDF, CSV, or template-based report.

To reorder report chapters and elements:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

-or-

Right-click the row for the report you want to edit, and click **Edit**.

The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see
   Edit a Report Outline.

4. Do one of the following:

   - In the report outline, click the report element, then drag and drop it to its new location.

   - Click the edit icon for the component, and select a new location in the **Location** drop-
     down box.

5. Click **Submit** to save your changes to the report.

Manage Filters for a Chapter Report

In Tenable Security Center, PDF and template-based reports use a chapter structure, so you can
specify different filters for individual chapter elements of those reports.

You can manage filters for a single element or for multiple elements at the same time. For more
information, see:

- Manage Filter Components for a Single Element

- Manage Filter Components for Multiple Elements

Manage Filter Components for a Single Element

Required Tenable Security Center User Role: Organizational user with appropriate permissions.
For more information, see User Roles.

Tip: You can build filters using one or more *filter components* with defined *filter component criteria*. Filter
components are types of data (e.g., **CVE ID** or **Severity**). After you select a filter component, you specify
the filter component criteria (e.g., a specific CVE ID or a specific severity level).

To manage filter components for a single element in a chapter report in Tenable Security
Center:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.

4. Click the edit icon next to the element you want to edit.

   > **Tip:** To display icons next to a element, hover the cursor over the element.

5. Do one of the following:

   - Add a filter component.

     Use these steps to add one or more filter components to a single element. For information about the filter components available for vulnerability analysis data or event analysis data, see Vulnerability Analysis Filter Components or Event Analysis Filter Components.

     a. In the **Data** section, click **Add Filter**.

     b. Select a filter component from the drop-down box.

     c. Set the filter component criteria, as prompted.

        Depending on the filter component you selected, Tenable Security Center prompts you to type the value you want to filter for or to select from valid values and operators.

> **Note:** If Tenable Security Center does not prompt you to specify an operator, the unstated operator is equivalent to **is equal to** or **is set to**.

    d. Click the check mark next to the filter component to stop editing it.

> **Note:** The new filter component is not saved until you click **Submit**.

- Edit a filter component.

  a. In the **Data** section, click the pencil icon next to the filter component.

  b. Edit the filter component criteria.

  c. Click the check mark next to the filter component to stop editing it.

  > **Note:** Your changes to the filter are not saved until you click **Submit**.

- Delete a filter component.

  In the **Data** section, click the delete icon next to the filter component.

  > **Note:** Tenable Security Center does not prompt you to confirm the deletion. However, the deletion is not final until you click **Submit** to save your changes.

6. Click **Submit**.

Manage Filter Components for Multiple Elements

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

When managing filter components for a chapter report in Tenable Security Center, you can search the report for elements that use certain filter components, then update the filter component criteria for all matching elements in that report at the same time.

> **Tip:** You can build filters using one or more *filter components* with defined *filter component criteria*. Filter components are types of data (e.g., **CVE ID** or **Severity**). After you select a filter component, you specify the filter component criteria (e.g., a specific CVE ID or a specific severity level).

You can use the following filter components to search and update: **Address**, **Audit File**, **Asset**, **CVE ID**, **DNS Name**, **IAVM ID**, **Repositories**, **Scan Policy**, and **Severity**.

For example, if you search a report definition for all elements where the **Severity** filter component is set to **Info**, you can update the **Severity** filter component to **Medium** for all elements, and add an **Audit File** filter component to the elements at the same time.

To manage filter components for multiple elements in a chapter report:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. On the left side of the page, click **Definition**.

   The report outline appears. This outline is, by default, expanded. For more information, see Edit a Report Outline.

4. At the top of the outline, click **Find/Update Filters**.

To search for specific elements in the report:

1. In the **Search Filters** section, click **Add Search Filter**.

2. Select a filter component from the drop-down box.

3. Select an operator from the drop-down box.

   a. If you selected **is equal to** or **contains** as operator, type filter component criteria or select a value from the list of valid filter component criteria, as appropriate to the filter component you selected.

4. Click the check mark at the end of the filter box.

   Tenable Security Center searches the report outline for elements that match your search criteria and displays the results in the **Matching Filters** box.

To specify the filter updates you want to make:

1. In the **Update Actions** section, click **Add Search Filter**.

2. Select a filter component from the drop-down box.

3. Select an operator from the drop-down box.

4. Type filter component criteria or select a value from the list of valid filter values, as appropriate to the filter component and operator you selected.

5. Click the check mark at the end of the filter box.

To review and update the filter updates:

1. In the **Matching Filters** box, review the list to verify that you want to apply the update to all the listed elements.

   > **Tip:** If you do not want to apply the current update to all the listed elements, it may be more appropriate to manage filter components by individual element. For more information, see Manage Filter Components for a Single Element.

2. Click **Update Filters**.

   Tenable Security Center applies the updates to the matching elements and returns you to the report outline.

3. Click **Submit** to save your changes to the report.

Manage Filter Components for a Non-Chapter Report

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

In Tenable Security Center, CSV, DISA ARF, DISA ASR, and Cyberscope reports do not use a chapter structure, so you can create a set of filter components that apply to every element of the report.

> **Tip:** You can build filters using one or more *filter components* with defined *filter component criteria*. Filter components are types of data (e.g., **CVE ID** or **Severity**). After you select a filter component, you specify the filter component criteria (e.g., a specific CVE ID or a specific severity level).

To manage filter components for a non-chapter report:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the reports table, click the name of the report you want to edit.

   -or-

   Right-click the row for the report you want to edit, and click **Edit**.

   The **Edit Report** page appears.

3. Do one of the following:

   - Add a filter component.

     Use these steps to add one or more filter components to a single element. For information about the filter components available for vulnerability analysis data or event analysis data, see Vulnerability Analysis Filter Components or Event Analysis Filter Components.

     a. In the **Definition** section, click **Add Filter**.

     b. Select a filter component from the drop-down box.

     c. Set the filter component criteria, as prompted.

        Depending on the filter component you selected, Tenable Security Center prompts you to type the value you want to filter for or to select from valid values and operators.

     d. Click the check mark next to the filter component to stop editing it.

     > **Note:** The new filter component is not saved until you click **Submit**.

   - Edit a filter component.

     a. In the **Definition** section, click the edit icon next to the filter component.

     b. Edit the filter criteria.

     c. Click the check mark next to the filter component to stop editing it.

> **Note:** Your changes to the filter component are not saved until you click **Submit**.

- Delete a filter component.

  In the **Definition** section, click the delete icon next to the filter component.

  > **Note:** Tenable Security Center does not prompt you to confirm the deletion. However, the deletion is not final until you click **Submit** to save your changes.

4. Click **Submit** to save your changes.

View a Report Definition

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

To view a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the row for the report definition you want to view, click the ⚙ menu.

   The actions menu appears.

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

   The actions menu appears.

4. Click **View**.

   Tenable Security Center displays a read-only version of the report definition.

   > **Note:** If you want to edit or delete the report definition from this page, see [Edit a Report Definition](#) or [Delete a Report Definition](#).

Copy a Report Definition

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can share a copy of a report definition with other users in your organization in Tenable Security Center. This feature is useful for maintaining consistency throughout your organization.

After you share the copy, the other users own their local copy and can edit or delete as with any report they create themselves. Later changes you make to the original do not synchronize automatically to the copy.

To copy a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the table, right-click the row for the report definition you want to copy.

   The actions menu appears.

3. Click **Copy**.

   The **Copy Report** page appears.

4. In the **Group** box, select the group you want to grant access to a copy of the report.

5. Specify the user(s) that you want to grant access to a copy of the report.

6. Click **Copy**.

   Tenable Security Center copies the report definition to the other accounts you specified. The copy appears, named **Copy of *DefinitionName***.

Export a Report Definition

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

In Tenable Security Center, you can export a report definition as an `.xml` file. This feature is useful for organizations running multiple Tenable Security Center deployments to provide consistent reports without duplicating the work needed to create definition templates.

To export a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the table, right-click the row for the report definition you want to export.

   The actions menu appears.

3. Click **Export**.

4. Click the export option you want to use:

Option	Description
Keep All References	Export the report definition with object references intact. Users who meet the following requirements can use an imported report definition with intact object references: • The user must be in the same organization as the user who exported the report definition. • The user must have access to all relevant objects in the report definition.
Remove All References	Export the report definition with object references removed, altering the definitions of the components. Any user can use an imported report definition with object references removed.
Replace With Placeholders	Export the report definition with object references replaced with their respective names. Users must replace the placeholder names with applicable objects available to their organization in order to use an imported report definition with placeholder names.

Tenable Security Center downloads the report definition to your computer.

Import a Report Definition

In Tenable Security Center, you can only import XML files in the same format used to export report definitions. This feature is useful for organizations running multiple Tenable Security Center deployments to provide consistent reports without duplicating the work needed to create definition templates.

To import a report definition:

1. Copy the report definition file to your local computer.

2. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

3. At the top of the table, click **Import Report**.

4. In the **Name** box, type a name for the report.

5. Click **Choose File** next to the **Report Definition** box.

6. Browse to the local copy of the report definition XML file.

7. Click **Import**.

   Tenable Security Center imports the report definition.

8. (Optional) Edit the report definition as desired.

Delete a Report Definition

To delete a report definition:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. To delete a single report definition:

a. In the table, right-click the row for the report definition you want to delete.

   The actions menu appears.

To delete multiple report definitions:

a. In the table, select the check box for each report definition you want to delete.

   The available actions appear at the top of the table.

3. Click **Delete**.

4. Click **Delete** to confirm the deletion.

   Tenable Security Center deletes the report definition.

   > **Note:** Tenable Security Center retains any report results associated with the deleted definition. You must manually delete results associated with the report.

Launch a Report on Demand

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

To launch a report on demand:

1. In the left navigation, click **Reporting** > **Reports**.

   The **Reports** page appears.

2. In the table, right-click the row for the report you want to launch.

   -or-

   Select the check box for the report you want to launch.

   The actions menu appears.

3. Click **Launch**.

4. (Optional) Monitor the status of the report in the **Report Results** page.

   To view this page, do one of the following:

- In the launch notification message, click **View Report Results**.

- In the left navigation, click **Reporting > Report Results**.

> **Note:** In the **Report Results** page, you can also stop the currently running report.

Add a Report to a Scan

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

After you create one or more on demand reports, you can add them to active scan, agent scan, or agent synchronization job configurations.

To add a preconfigured report to an active scan, agent scan, or agent synchronization job:

1. Do one of the following:

    - Begin configuring an active scan, as described in Add an Active Scan.

    - Begin configuring an agent scan, as described in Add an Agent Scan.

    - Begin configuring an agent synchronization job, as described in Add an Agent Synchronization Job.

2. In the **Post Scan** section, click **Add Report**.

    The page displays available on demand reports.

3. Select the report you want to add.

4. (Optional) If you want the report to include cumulative data in Tenable Security Center, enable the **Create report using cumulative data** option.

    If you disable this option, the report includes data only from the configured scan.

5. Click the checkmark icon to save the report.

6. (Optional) If you want to add multiple reports, repeat steps 2–5 for each additional report.

7. Click **Submit**.

    Tenable Security Center saves your configuration.

Manage Report Results

On the **Report Results** page of Tenable Security Center, you can manage both currently running reports and completed report results. Completed report results include successful and failed report runs, so you can access and distribute a successful report result or troubleshoot a report failure. For more information, see Reports.

To manage report results:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.

2. Do any of the following:

   - Filter existing report results in the report results table.

   - Stop a currently running report.

   - Download a successful report result to your computer.

   - View a successful report result.

   - Publish a successful result.

   - Email a copy of a successful result to specified users.

   - Share a copy of a successful result with other Tenable Security Center user accounts.

   - View error conditions for a failed report.

   - Delete a report result.

Stop a Running Report

If you want to stop a report that is currently running:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.

2. Right-click the row for the report you want to stop, and click **Stop**.

   Tenable Security Center stops the report run.

   > **Note:** You cannot restart a stopped report run. You can only launch the report again.

Download a Report Result

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

To download a successful report result to your computer:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.

2. Do one of the following:

   - In the Results table, click the name of the report.

   - Right-click the row for the report result.

     The actions menu appears.

     a. Click **Export**.

   - Select the check box for the report result.

     At the top of the table, click **Download**.

View a Report Result

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

To view a successful report result:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.

2. Right-click the row for the report result you want to view.

   The actions menu appears.

3. Click **View**.

   The report appears.

4. (Optional) To download the report result to your computer, click **Download**.

   The report result downloads.

5. (Optional) To delete the report result, click **Delete**.

   Tenable Security Center deletes the report result.

Publish a Report Result

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

To publish a successful report result:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.

2. Right-click the row for the report result you want to publish.

   The actions menu appears.

3. Click **Publish**.

   The **Publish Report Results** window appears.

4. Search for and select a publishing site.

5. Click **Publish**.

   Tenable Security Center publishes the report result.

Email a Report Result

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

To email a copy of a successful report result to specific users:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.

2. Right-click the row for the report result you want to email.

   The actions menu appears.

3. Click **Email**.

4. Do one of the following:

   - Use the **Group** and **User** boxes to select the Tenable Security Center user or users you want to receive the report result.

   - Type the email address of recipients who are not Tenable Security Center users.

5. Click **Submit**.

   Tenable Security Center sends the report result.

Copy a Report Result

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

To share a copy of a successful report result with other Tenable Security Center user accounts:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.

2. Right-click the row for the report result you want to copy.

   The actions menu appears.

3. Click **Copy**.

4. In the **Group** box, select the group you want to grant access to a copy of the report result.

5. Specify a user or users that you want to grant access to a copy of the report result.

6. Click **Copy**.

   Tenable Security Center copies the report result to the other accounts you specified. The copy appears, named **Copy of *ResultName***.

View Errors for a Failed Report

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

To view error conditions for a failed report:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.

2. Click the name of the failed result in the results table.

   The **View Report Results** page appears.

3. Review the **Error Details** section.

Delete a Report Result

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

To delete a report result:

1. Click **Reporting** > **Report Results**.

   The **Report Results** page appears.

2. Right-click the row for the report result you want to delete.

   The actions menu appears.

3. Click **Delete**.

   A confirmation window appears.

4. Click **Delete** to confirm the deletion.

    Tenable Security Center deletes the report result.

CyberScope and DISA Report Attributes

Report attributes are used for adding required information to CyberScope or DISA report types. After you create an attribute, you can select it during CyberScope, DISA ARF, or DISA Consolidated ARF report creation. For more information, see Create a Custom Report.

To filter the **Report Attributes** page, see Apply a Filter.

Configure the following options, including options specific for your attribute type: CyberScope Options or DISA Options.

General Option	Description
Name	A name for the attribute.
Description	(Optional) A description for the attribute.
Type	The type of attribute you want to create. Your **Type** selection determines the other options you must configure: CyberScope Options or DISA Options.

CyberScope Options

The following table describes the additional options to configure when configuring a **CyberScope** attribute.

Option	Description
Reporting Component	The CyberScope value for a reporting component (e.g., **Department of Justice**).
Component Bureau	The CyberScope value for a FISMA reporting entity within the **Reporting Component** (e.g., **Justice Management Division**).
Enclaves	The CyberScope value for an enclave associated with the **Reporting Component** or **Component Bureau**.

DISA Options

The following table describes the additional options to configure when configuring a **DISA** attribute.

Option	Description
Owning Unit	
Name	(Required) The Cyber Operational Attributes Management System (COAMS) fully qualified hierarchy name of the owning organization.
Owning Service	
Name	The COAMS fully qualified hierarchy name of the owning combatant command, service, or agency.
Current AOR	The COAMS fully qualified hierarchy name of the appropriate combatant command area of responsibility (COCOM AOR).
Region	A region for the owning service.
Administration Unit	
Name	The COAMS fully qualified hierarchy name of the administering organization.
Administration POC	
Any required information you need to provide about the administration unit's point of contact (POC). **Tip:** Tenable recommends leaving the **Generational Qualifier** option blank.	
CND Service Provider	
Name	The COAMS fully qualified hierarchy name of the Computer Network Defense Service Provider (CNDSP).
Por Managed	(Required) Specifies if the reported assets are centrally managed by a program management office (PMO): **true** or **false**.
System Affiliation	The COAMS **operationalacredit** value that specifies the fully qualified hierarchy name of the system affiliation.

Option	Description
Location	

> **Tip:** Tenable recommends leaving all options blank except the **Street Address**. The **Street Address** specifies the COAMS geolocation area.

Report Images

In Tenable Security Center, the **Report Images** interface allows a user with permissions to view details, add, edit, or delete PDF report images. From this interface, you can manage two types of images: logos and watermarks. Logos appear at the bottom of each page, while watermarks appear prominently across the center of the report page.

> **Note:** Image files must be of type .png or .jpg. Images used must be consistent when selecting the bit depth (8-bit, 16-bit, 24-bit, etc.). Otherwise, errors might be encountered when generating reports.

To filter the **Report Images** page, see Apply a Filter.

Report Image Options

Option	Description
Add	Add a new logo or watermark image. Note that only PNG and JPEG formats are supported. The default image sizes are as follows, all at 300 DPI: • default-cover-logo = 987x130 • default-footer-logo = 380x100 • default-page-logo = 579x84 • default-watermark = 887x610 While there are no set limitations on image size or resolution, using images that are different from these specifications can have a negative impact on report appearance. > **Note:** The image size must be set to 300 DPI to prevent image breaks.

Option	Description
Edit	Edit any of the selected image's options, including name, description, type and file.
Detail	View image details, including name, description, date uploaded, last modified, and type.
Delete	Delete the highlighted image.

Assurance Report Cards

Assurance Report Cards (ARCs) provide an overview of the security posture of your network. These configurable reports provide quick visible feedback using a pass or fail methodology for each policy statement in the ARC.

Organizational users with appropriate permissions can add a template-based ARC using Tenable-provided templates or you can add a custom ARC. For more information about Tenable-provided ARC templates, see the Assurance Report Cards blog. For more information about user permissions, see User Roles.

- Add a Template-Based Assurance Report Card

- Add a Custom Assurance Report Card

- Assurance Report Card Options

- Edit an Assurance Report Card

- View Your Assurance Report Cards

- View Details for an Assurance Report Card

- Share or Revoke Access to an Assurance Report Card

- Export an Assurance Report Card

- Copy an Assurance Report Card

- Delete an Assurance Report Card

Add a Template-Based Assurance Report Card

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can use a Tenable-provide template to add an Assurance Report Card (ARC). For more information about Tenable-provided ARC templates, see the Assurance Report Cards blog. To create a custom ARC, see Add a Custom Assurance Report Card.

For more information, see Assurance Report Cards.

To add a template-based Assurance Report Card:

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard** > **Assurance Report Cards**.

   The **Assurance Report Cards** page appears.

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

   The **Assurance Report Card Templates** page appears.

4. Click a template category tile.

   The list of templates for the selected category appears.

5. Click a template.

   The **Add Assurance Report Card Template** page updates to reflect the template you selected.

6. Modify the ARC template. For more information, see Assurance Report Card Options.

   - To edit the ARC name, click ARC template title.

   - To edit the ARC description, click the **Description** box.

   - To edit the required assets, click an item in the **Required Assets** section.

   - To restrict the target data displayed in the ARC, click the **Targets** drop-down box.

   - To set how often the ARC polls data sources to obtain updates, click **Schedule**.

7. Click **Add**.

   Tenable Security Center saves your configuration.

Add a Custom Assurance Report Card

You can create a fully customized Assurance Report Card (ARC). To add an ARC from a Tenable-provided template, see Add a Template-Based Assurance Report Card.

For more information, see Assurance Report Cards.

To add a custom Assurance Report Card:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Dashboard** > **Assurance Report Cards**.

   The **Assurance Report Cards** page appears.

3. In the **Options** drown-down box, click **Advanced Add**.

   The **Advanced Add Assurance Report Cards** page appears.

4. Configure the ARC options. For more information, see Assurance Report Card Options.

5. Click **Submit**.

   Tenable Security Center saves your configuration.

View Your Assurance Report Cards

You can view a summary that displays each Assurance Report Card (ARC), the overall status of the ARC, and the status of each policy statement in each ARC. To view details for an ARC, see View Details for an Assurance Report Card.

For more information, see Assurance Report Cards.

> **Tip:** To change the position of an ARC in the list, click the icon next to the ARC and drag it to a new position.

Before you begin:

- Add an ARC, as described in [Add a Template-Based Assurance Report Card](#) or [Add a Custom Assurance Report Card](#).

To view a summary of your Assurance Report Cards:

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard** > **Assurance Report Cards**.

   The **Assurance Report Cards** page appears.

3. Click the row for the ARC.

   The ARC expands to display each policy statement in the ARC.

4. View the status of each ARC and its policy statements.

   - A green icon (☑) next to an ARC indicates all policy statement in the ARC passed.

   - A red icon (☒) next to an ARC indicates one or more policy statements in the ARC failed.

   - A green check mark (✔) next to a policy statement indicates the policy statement passed.

   - A red x (✖) next to a policy statement indicates the policy statement failed.

What to do next:

- (Optional) Click a policy statement to view vulnerability analysis for the policy statement data. For more information, see [Vulnerability Analysis](#).

View Details for an Assurance Report Card

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

For more information, see [Assurance Report Cards](#).

Before you begin:

- Add an Assurance Report Card (ARC), as described in [Add a Template-Based Assurance Report Card](#) or [Add a Custom Assurance Report Card](#).

To view details for an Assurance Report Card:

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard** > **Assurance Report Cards**.

   The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

   The **Manage Assurance Report Cards** page appears.

4. Right-click the row for the ARC.

   The actions menu appears.

5. Click **View**.

   The **View Assurance Report Card** page appears. For more information, see Assurance Report Card Options.

Section	Action
Options drop-down box	• To edit the ARC, click **Edit**. • To delete the ARC, click **Delete**.
General	View general information about the ARC. • **Name** — The ARC name. • **Description** — The ARC description. • **Schedule** — TheARC schedule. • **Created** — The date the ARC was created. • **Last Modified** — The date the ARC was last modified. • **Owner** — The user who created or owns the ARC. • **Group** — The group associated with the **Owner**. • **ID** — The unique identifier for the ARC.
Policy Statements	View the policy statements in the ARC.
Focus	View the targets configured for the ARC.

Edit an Assurance Report Card

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Assurance Report Cards.

Before you begin:

- Add an Assurance Report Card (ARC), as described in Add a Template-Based Assurance Report Card or Add a Custom Assurance Report Card.

To edit an Assurance Report Card:

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard** > **Assurance Report Cards**.

   The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

   The **Manage Assurance Report Cards** page appears.

4. Right-click the row for the ARC.

   The actions menu appears.

5. Click **More** > **Edit**.

   The **Edit Report Card** page appears.

6. Modify the ARC options. For more information, see Assurance Report Card Options.

7. Click **Submit**.

   Tenable Security Center saves your configuration.

Share or Revoke Access to an Assurance Report Card

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can share access to an Assurance Report Card (ARC) to give users in a group the ability to view the ARC. The user's role and custom permissions determine if they can drill down into other pages with more information. For more information, see Assurance Report Cards.

Before you begin:

- Add an ARC, as described in Add a Template-Based Assurance Report Card or Add a Custom Assurance Report Card.

To share or revoke access to an Assurance Report Card:

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard** > **Assurance Report Cards**.

   The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

   The **Manage Assurance Report Cards** page appears.

4. Right-click the row for the ARC.

   The actions menu appears.

5. Click **Share**.

   The **Share Assurance Report Card** page appears.

6. In the box, search for and select the groups for which you want to share or revoke access.

7. Click **Submit**.

   Tenable Security Center saves your configuration.

Export an Assurance Report Card

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can export an Assurance Report Card (ARC) to share with other users in your organization. For more information, see Assurance Report Cards.

Before you begin:

- Add an ARC, as described in [Add a Template-Based Assurance Report Card](#) or [Add a Custom Assurance Report Card](#).

To export an Assurance Report Card:

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard** > **Assurance Report Cards**.

   The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

   The **Manage Assurance Report Cards** page appears.

4. To export a single ARC:

   a. In the table, right-click the row for the ARC you want to export.

      The actions menu appears.

   To export multiple ARCs:

   a. In the table, select the check box for each ARC you want to export.

      The available actions appear at the top of the table.

5. Click **Export**.

   The export options appear.

6. Click the export option you want to use:

Option	Description
Keep All References	Export the ARC with object references intact. Users who meet the following requirements can use an imported ARC with intact object references: • The user must be in the same organization as the user who exported the ARC. • The user must have access to all relevant objects in the ARC.
Remove All References	Export the ARC with object references removed, altering the definitions of the components. Any user can use an imported ARC with object references removed.
Replace With Placeholders	Export the ARC with object references replaced with their respective names. Users must replace the placeholder names with applicable objects available to their organization in order to use an imported ARC with placeholder names.
Template	Export the ARC as a template.

Tenable Security Center exports the ARC as an `.xml` file.

Copy an Assurance Report Card

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Assurance Report Cards.

Before you begin:

• Add an Assurance Report Card (ARC), as described in Add a Template-Based Assurance Report Card or Add a Custom Assurance Report Card.

To copy an Assurance Report Card:

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard** > **Assurance Report Cards**.

   The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

   The **Manage Assurance Report Cards** page appears.

4. Right-click the row for the ARC.

   The actions menu appears.

5. Click **Copy**.

   Tenable Security Center copies the ARC. The copy appears, named **Copy of *ARC Name***.

Delete an Assurance Report Card

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Assurance Report Cards.

To delete an Assurance Report Card (ARC):

1. Log in to Tenable Security Center via the user interface.

2. Click **Dashboard** > **Assurance Report Cards**.

   The **Assurance Report Cards** page appears.

3. In the **Options** drop-down menu, click **Manage ARCs**.

   The **Manage Assurance Report Cards** page appears.

4. To delete a single ARC:

   a. In the table, right-click the row for the ARC you want to delete.

      The actions menu appears.

   To delete multiple ARCs:

a. In the table, select the check box for each ARC you want to delete.

   The available actions appear at the top of the table.

5. Click **Delete**.

   A confirmation window appears.

6. Click **Delete**.

   Tenable Security Center deletes the ARC.

Assurance Report Card Options

You can configure the following options for Assurance Report Cards (ARCs). For more information, see Assurance Report Cards.

- Assurance Report Card Options

- Policy Statement Options

Assurance Report Card Options

Option	Description
General	
Name	The name of the ARC.
Description	(Optional) A description for the ARC.
Schedule	Specifies how often the ARC polls data sources to obtain updates. • **Daily** (default) — The ARC polls data sources every 1-20 days at the specified time. • **Weekly** — The ARC polls data sources every 1-20 weeks at the specified time and day of the week. • **Monthly** — The ARC polls data sources every 1-20 months at the specified time and day of the month. For example, *Every 2 months on the fourth Thursday at 15:00 -4:00* indicates the ARC will poll data sources to obtain updates every two months, on the

Option	Description
	fourth Thursday of the month, at 15:00 in the America/New York timezone.
Policy Statements	
Add Policy Statement	Click to add a custom policy statement to the ARC. For more information, see Policy Statement Options.
Focus	
Targets	Specifies the target hosts for the ARC to analyze: • **All Systems** — Targets all available hosts. • **Assets** — Targets the specified assets. For more information, see Assets. > **Tip:** Use NOT, OR, and AND operators to exclude unwanted assets from the view. • **IPs** — Targets the specified IP addresses. You can specify single addresses, IP addresses in CIDR notation, and IP ranges. • **Repositories** — Targets the specified repositories. For more information, see Repositories. If you want to match the specified assets or IP addresses against one or more repositories, select the repositories you want to match against. > **Note:** If an IP address you specified appears in two or more repositories you selected, the duplicated IP address negatively skews the ARC results.

Policy Statement Options

Option	Description
Basic	
Statement	Specifies pass/fail criteria for the policy statement.
Display	Specifies how the ARC displays the policy statement: **Ratio (x/y)**,

Option	Description
	Percentage (%), or **Compliant/Non-Compliant**.
Advanced	
Data Type	The type of data you want the ARC to analyze: **Vulnerabilities** or **Events**.
Base Filters	The filters used as the basis for data analysis. • If the **Data Type** is **Vulnerabilities**, you can select from the list of vulnerability analysis filter components. • If the **Data Type** is **Events**, you can select from a list of event analysis filter components.
Compliant Filters	The filters used to determine the compliance conditions for the data analysis. For more information, see Vulnerability Analysis and Event Analysis. • If the **Data Type** is **Vulnerabilities**, you can select from the list of vulnerability analysis filter components. • If the **Data Type** is **Events**, you can select from a list of event analysis filter components. **Note:** Filters set in **Base Filters** are not present in **Compliant Filters**, with exception of the Assets and Plugin IDs. All filters set in **Base Filters** are carried over into **Compliant Filters**.
Compliant Condition	Specifies the conditions to match for determining compliance. For more information, see Vulnerability Analysis and Event Analysis. Specify a quantity: **All**, **No**, **Any**, **>** (greater than), **<** (less than), **>=** (greater than or equal to), and **<=** (less than or equal to). Specify hosts: **Hosts**, **Vulnerabilities**, and **Ports**.
Drilldown Filters	The filters to apply when clicking on the ARC policy statement for more details. For more information, see Vulnerability Analysis and Event Analysis. • If the **Data Type** is **Vulnerabilities**, you can select from the list of vulnerability analysis filter components.

Option	Description
	• If the **Data Type** is **Events**, you can select from a list of [event analysis filter components]().

Filters

You can apply filters on many pages of the Tenable Security Center web interface to filter the data displayed on the page.

You can build filters using one or more *filter components* with defined *filter component criteria*. Filter components are types of data (e.g., **CVE ID** or **Severity**). After you select a filter component, you specify the filter component criteria (e.g., a specific CVE ID or a specific severity level).

If you want to save a filter for repeated use, create a query, as described in [Queries]().

For more information, see:

- [Apply a Filter]()

- [Filter Components]()

- [Vulnerability Analysis Filter Components]()

- [Event Analysis Filter Components]()

- [Mobile Analysis Filter Components]()

- [Host Asset Filter Components]()

- [Plugin Filter Components]()

Apply a Filter

Required Tenable Security Center User Role: Any

You can use filters to narrow the data displayed on specific pages.

Each filterable page in Tenable Security Center has a different set of filter components. On the **Vulnerabilities**, **Events**, and **Mobile** pages, you can add and remove filter components.

For more information, see [Filters]() and [Filter Components]().

To filter data:

1. Log in to Tenable Security Center via the user interface.

2. Navigate to any page that supports filtering.

3. On the left side of the page, click the ▽ button.

   The filter panel appears.

   ▽ ‹   **Apply**

   ＋ Customize　✕ Clear All

   Load Query ⌄
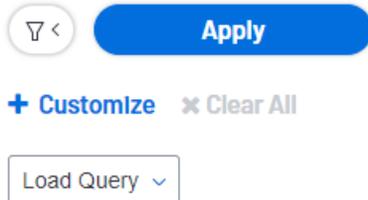
4. (Optional) To customize the filter components on an analysis page, do the following:

   a. Click **Customize**.

      The filter components selection window appears.

   b. Select one or more filter component check boxes. For more information about the components supported for your analysis view, see Vulnerability Analysis Filter Components, Event Analysis Filter Components, Mobile Analysis Filter Components, and Host Asset Filter Components.

   c. Click **Apply**.

      The filter panel updates to show the filter components you selected.

5. To modify the criteria for a filter component, click the box for the filter component.

   The filter component criteria selection window appears.

6. Modify the filter component criteria.

7. Click **OK**.

   The filter panel updates to show the filter component criteria you modified.

8. Click **Apply**.

   The page updates to reflect the filter you applied.

What to do next:

- (Optional) Save a filter on the **Vulnerabilities** page, **Events** page, and **Mobile** page as a reusable query, as described in [Add or Save a Query](#).

Filter Components

For general information about using filters, see [Filters](#).

Filter Component	Description

Access	The level of object access to include in the filter:
	
	• **Manageable** — Shows the objects your user account can modify.
	
	  For example, set the filter to show only the credentials you can edit.
	
	• **Usable** — Shows the objects your user account can view or use.
	
	  For example, set the filter to show only the credentials you can use in a scan.

Actions	The alert actions to include in the filter: **Email**, **Notify**, **Report**, **Scan**, **SysLog**, or **Ticket**. For more information, see [Alerts](#) and [Alert Actions](#).
Agent Scanner	The agent scanners to include in the filter. For more information, see [Agent Scanning](#).
Assignee	The ticket assignees to include in the filter. For more information, see [Tickets](#).
Authorized	The Log Correlation Engine Client authorization status to include in the filter: **yes** or **no**.
Client IP	The Log Correlation Engine Client IP addresses to include in the filter. For more information, see [Tenable Log Correlation Engine Clients](#).
Completion Time	The date range for scan results to include in the filter: • **Explicit** — Choose start and end dates and times to filter for a specific date range. • **Last *x* Minutes** — Filter for the last 15, 20, or 30 minutes.

Filter Component	Description
	• **Last x Hours** — Filter for the last 1, 2, 4, 6, 12, 24, 48, or 72 hours. • **Last x Days** — Filter for the last 5, 7, 15, 25, 30, 60, 90, 120, or 180 days. • **Last 12 Months** — Filter for the last year. • **All** — Show all results.
Creator	The ticket creators to include in the filter. For more information, see [Tickets](#).
Data Type	The repository data type to include in the filter: **Agent**, **IPv4**, **IPv6**, or **Mobile**. For more information, see [Repositories](#).
Date	The date range to include in the system log filter (for example, *Oct 2021*). For more information, see [System Logs](#).
Filter By	The type of plugin data to include in the plugin filter. For more information, see [Vulnerability Analysis Filter Components](#).
Finish Time	The date range for report results to include in the filter: • **Explicit** — Choose start and end dates and times to filter for a specific date range. • **Last x Minutes** — Filter for the last 15, 20, or 30 minutes. • **Last x Hours** — Filter for the last 1, 2, 4, 6, 12, 24, 48, or 72 hours. • **Last x Days** — Filter for the last 5, 7, 15, 25, 30, 60, 90, 120, or 180 days. • **Last 12 Months** — Filter for the last year. • **All** — Show all results.
Group	The groups to include in the filter. For more information, see [Groups](#).
Host	The name of the host to include in the filter. For more information, see

Filter Component	Description
	[Host]().
Initiator	The username for a user who initiated a job to include in the filter. For more information, see [Job Queue Events]().
Keywords	The keywords to include in the system logs filter (for example, *login*). For more information, see [System Logs]().
Log Correlation Engine Server	The Log Correlation Engine servers to include in the filter. For more information, see [Tenable Log Correlation Engines]().
Module	The type of logs to include in the system logs filter. For more information, see [System Logs]().
Name	The name of the object or user to include in the filter. For example, the name of a Tenable Nessus scanner or the name of a repository.
Organization	The organization to include in the filter. For more information, see [Organizations]().
OS	The operating systems to include in the filter. For more information, see [Tenable Log Correlation Engine Clients]() and [Tenable Log Correlation Engine Client Policies]().
Owner	The object owners to include in the filter. The object owner is the user who created an object or inherited objects from a deleted user.
Plugin	The plugin IDs to include in the filter.
Plugin Family	The plugin family to include in the plugin filter.
Repositories	The repositories to include in the filter. For more information, see [Repositories]().
Repository	The repository to include in the filter. For more information, see [Repositories]().
Role	The user roles to include in the filter. For more information, see [User]()

Filter Component	Description
	Roles.
Scan Policy	The scan policies to include in the filter. For more information, see Scan Policies.
Schedule	The schedules to include in the filter. For more information, see Active Scan Settings, Agent Scan Settings, Agent Synchronization Job Settings, and Report Options.
Severity	The severity to include in the filter. For more information, see CVSS vs. VPR.
State	The Log Correlation Engine Client state to include in the filter: **Alive** or **Dead**. For more information, see Tenable Log Correlation Engine Clients.
Status	The statuses to include in the filter.
Tags	The tags to include in the filter. For more information, see Tags.
Timeframe	The date range to include in the notification filter: **Last 24 Hours**, **Last 7 Days**, or **Last 30 Days**.
Type	The object type (for example, **Active** or **Agent** scan results).
Username	The username to include in the filter. For more information, see User Account Options.
Version	The Log Correlation Engine version to include in the filter. For more information, see Tenable Log Correlation Engines.

Queries

The **Queries** page displays a list of queries available for use. The information on this page includes **Name**, **Type**, **Group**, **Owner**, and the **Last Modified** time. You can use a filter to narrow the list by any of the columns (except **Last Modified**). For more information, see Filters.

For more information about queries, see:

- [Add or Save a Query](#)

- [Load a Query](#)

- [Query Options](#)

- [Edit a Query](#)

Add or Save a Query

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see [User Roles](#).

You can add queries from the **Queries** page or from the **Vulnerabilities** page, **Web App Scanning** page, **Events** page, or **Mobile** page. For more information about query options, see [Queries](#).

> **Note:** If you want to create a mitigated vulnerabilities query, you must add the query from the **Vulnerabilities** page.

To add a query from the **Queries** page:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Queries**.

   The **Queries** page appears.

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

4. Type a **Name** and **Description**.

5. (Optional) If you want to add a tag, type select a **Tag** from the drop-down. For more information, see [Tags](#).

6. Select a **Type**.

   The **Tool** drop-down updates with options for that type.

7. Select a **Tool**.

8. Click **Add Filter**.

   The **Filters** section expands. For more information, see [Filters](#).

9. Select a filter component from the **Select a Filter** drop-down.

   The filter component criteria box appears.

10. In the filter component criteria box, type or select filter component criteria.

11. Click the ✔ button.

   Tenable Security Center adds the filter component.

12. (Optional) To add other filter components, repeat step 8.

13. Click **Submit**.

   Tenable Security Center saves your configuration.

To save a query from an analysis page:

1. Log in to Tenable Security Center via the user interface.

2. Do one of the following to navigate to an analysis page:

   - Click **Analysis** > **Vulnerabilities**

   - Click **Analysis** > **Web App Scanning**

   - Click **Analysis** > **Events**

   - Click **Analysis** > **Mobile**

   The analysis page appears.

3. Apply a filter for the query, as described in Apply a Filter.

   The page updates to reflect the filter you applied.

4. Click **Save** > **Save Query**.

   The **Save Query** panel appears.

5. In the **Name** box, type a name for the query.

6. In the **Description** box, type a description for the query.

7. (Optional) If you want to add a tag, type or select a **Tag** from the drop-down. For more
   information, see Tags.

8. Click **Submit**.

    Tenable Security Center saves your configuration.

Load a Query

> **Required Tenable Security Center User Role:** Any

You can load queries from any page that supports filtering. For more information, see [Queries](#) and [Filters](#).

To load a query:

1. Log in to Tenable Security Center via the user interface.

2. Navigate to any page that supports filtering.

3. On the left side of the page, click the filter icon (› ▽).

    The filter panel appears.

4. Click **Load Query**.

5. Select the query you want to load.

6. Click **Apply**.

    The page updates, filtered by the query you selected.

Query Options

Queries provide the ability to save custom views of vulnerability, event, ticket, user, and alert data for repeated access.

Option	Description
Name	A name for the query.
Description	A description for the query.
Tag	A tag for the query. For more information, see [Tags](#).
Type	The type of data you want the query to use.

Option	Description
	For more information about the filter components for **Vulnerability**, **Event**, and **Mobile** data types, see Vulnerability Analysis Filter Components, Event Analysis Filter Components, and Mobile Analysis. For more information about the filter components for **Ticket**, **User**, and **Alert** data types, see Ticket-Specific Query Options, User-Specific Query Options, and Alert-Specific Query Options.
Tool	Chooses the analysis tool used by the query.

Ticket-Specific Query Options

Ticket queries are a useful way of determining what tickets to alert against. For example, if you want to be alerted when a specific user receives a ticket, you could create a query with a ticket filter where the **Assignee** value is the user's name. You could then create an alert to email you when the user receives a ticket. The table below contains a list of the ticket query options.

Option	Description
Name	Ticket name to filter against
Status	Ticket status to filter against.
Classification	The ticket classification to filter against.
Owner	The manager (owner) of the ticket assignee.
Assignee	The ticket assignee to filter against.
Created Timeframe	Ticket creation date/time to filter against. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.)
Assigned Timeframe	Ticket assigned date/time to filter against. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.)
Modified Timeframe	Ticket modified date/time to filter against. Either specify an explicit timeframe, including the start and end time or choose one of the

Option	Description
	predefined periods (e.g., last 15 minutes, last hour, etc.)
Resolved Timeframe	Ticket resolution date/time to filter against. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.)
Closed Timeframe	Ticket closed date/time to filter against. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.)

User-Specific Query Options

User queries are useful for reporting, dashboards and alerts based on user actions. For example, they can track user logins and locked accounts. They can also track user logins from accounts not authorized on the monitored systems.

Option	Description
First Name	User first name to filter against.
Last Name	User last name to filter against.
Username	Actual username to filter against.
Group	Filter against the group the user(s) belong to.
Role	Filters against users who have the specified role.
Email	Filters against users based on their email address.
Last Login Timeframe	Filters against users whose last login was that the timeframe specified. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.).
Account State	Filters against the user account state (locked vs. unlocked).

Alert-Specific Query Options

The alert query is useful for reporting, dashboards and alerting when an alert has triggered. This is useful for situations where you want a report, dashboard element, or conditional alert after the specified alert filter conditions have been met. For example, you can schedule a daily report containing a query of all active alerts and their details.

Option	Description
Name	Filter against alerts with the specified name.
Description	Filter against alerts with the specified description.
State	Choose from **All**, **Triggered**, or **Not Triggered**.
Created Timeframe	Filters against the alert creation timeframe specified. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.).
Modified Timeframe	Filters against the most recent alert modification timeframe specified. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.).
Last Triggered Timeframe	Filters against the most recent alert trigger timeframe specified. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.).
Last Evaluated Timeframe	Filters against the most recent alert evaluation timeframe specified. Either specify an explicit timeframe, including the start and end time or choose one of the predefined periods (e.g., last 15 minutes, last hour, etc.).

Edit a Query

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Query Options.

To edit a query:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Queries**.

   The **Queries** page appears.

3. In the table, right-click the row for the query you want to edit.

   The actions menu appears.

   -or-

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

   The available actions appear at the top of the table.

4. Click **Edit**.

   The **Edit Query** page appears.

5. Modify the query options.

6. Click **Submit**.

   Tenable Security Center saves the modified query.

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.

For more information, see Alerts, Tickets, Accept Risk Rules, and Recast Risk Rules.

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.

For more information, see:

- [Alert Actions](#)

- [Add an Alert](#)

- [View Alert Details](#)

- [Alert Options](#)

- [Edit an Alert](#)

- [Evaluate an Alert](#)

- [Delete an Alert](#)

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](#)

> **Tip:** Use email alerts to interface with third-party ticketing systems by adding variables in the message option.

For more information, see [Alerts](#).

Assign Ticket

When the alert triggers, Tenable Security Center creates a ticket and assigns the ticket to a user. For more information, see [Tickets](#).

Option	Description	Default
Name	(Required) The name of the ticket.	Ticket opened by alert

Description	A description for the ticket.	--
Assignee	(Required) The user who receives the ticket.	--

Email

When the alert triggers, Tenable Security Center sends an email.

Option	Description	Default
Email		
Subject	The alert email subject line.	Email Alert
Message	The body of the email message. You can include the following variables to customize the email: • **Alert ID** — Designated with the variable: %alertID%, this specifies the unique identification number assigned to the alert by Tenable Security Center. • **Alert name** — Designated with the variable: %alertName%, this specifies the name assigned to the alert (for example, "Test email alert"). • **Trigger Name** — Designated with the variable: %triggerName%, this specifies if the trigger is IP address count, Vulnerability count, or Port count. • **Trigger Operator** — Designated with the variable: %triggerOperator%, this specifies the operator used for the count: >=, =, >= or != • **Trigger value** — Designated with the variable: %triggerValue%, this specifies the specific threshold value set that triggers the alert. • **Calculated value** — Designated with the variable: %calculatedValue%, this specifies the actual value that triggered the alert.	(see description)

- **Alert Name** — Designated with the variable: %alertName%, this specifies the name given to the alert within Tenable Security Center.

- **Alert owner** — Designated with the variable: %owner%, this specifies the user that created the alert.

- **Tenable Security Center URL** — Designated with the variable: %url%, this specifies the URL that you use to access Tenable Security Center. This is useful where the URL that users use to access Tenable Security Center differs from the URL known by Tenable Security Center.

The following sample email alert contains some of these keywords embedded into an HTML email:

```
Alert <strong>%alertName%</strong> (id
#%alertID%) has triggered.

<strong>Alert Definition:</strong> %triggerName%
%triggerOperator% %triggerValue%
<strong>Calculated Value:</strong>
%calculatedValue%

Please visit your Tenable Security Center (<a
href="%url%">%url%</a>) for more information.
This e-mail was automatically generated by
Tenable Security Center as a result of alert
<strong>%alertName%</strong> owned by
<strong>%owner%</strong>.

If you do not wish to receive this email, contact
the alert owner.
```

Include Results	When enabled, Tenable Security Center includes the query results that triggered the alert (maximum of 500).	Disabled

Recipients		
Users	The users who receive the alert email. **Tip:** If you delete a user who receives alert emails, the action option for the alert turns red and Tenable Security Center displays a notification to the new alert owner with the new alert status. To resolve this, update the list of users in the alert email.	--
Email Addresses	Specifies additional email addresses to include in the alert email. For multiple recipients, add one email address per line or use a comma-separated list.	--

Generate Syslog

When the alert triggers, Tenable Security Center sends a custom message to a syslog server.

Option	Description	Default
Host	(Required) The host that receives the syslog alert.	--
Port	The UDP port used by the remote syslog server.	514
Severity	The severity level of the syslog messages (**Critical**, **Notice**, or **Warning**).	Critical
Message	(Required) The message Tenable Security Center sends with the syslog alert.	--

Launch Scan

When the alert triggers, Tenable Security Center launches an active scan from an existing active scan template. The active scan **Schedule** must be **On Demand**. For more information, see Active Scans and Active Scan Settings.

> **Note:** At this time, the **Launch Scan** alert action does not support web app scans, agent scans, or agent sync.

Option	Description	Default
Scan	(Required) The scan template Tenable Security Center uses for the alert scan. **Note:** Tenable Security Center scans the host that triggered the scan, not the host within the scan template. Tenable Security Center uses the top 100 IP results from the alert query for the scan targets.	--

Launch Report

When the alert triggers, Tenable Security Center generates a report from an existing report template. For more information, see Reports.

Option	Description	Default
Report Template	(Required) The report template Tenable Security Center uses to generate a report based on the triggered alert data.	--

Notify Users

When the alert triggers, Tenable Security Center displays a notification to the specified users.

Option	Description	Default
Message	(Required) The notification message Tenable Security Center sends when the alert triggers.	--
Users	(Required) The users who receive the notification message.	--

Add an Alert

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

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

For more information about the available options for alerts, see Alert Options.

To add an alert:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, 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. For more information, see Alert Actions.

13. Click **Submit**.
    Tenable Security Center creates the alert.

View Alert Details

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

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. For more information about the following fields, see Alert Options.

Section	Action
Options drop-down box	• To edit the alert, click **Edit**. For more information, see Edit an Alert. • To delete the alert, click **Delete**. For more information, see Delete an Alert.
General	View general information about the alert. • **Name** — Alert name. • **Description** — Descriptive text for the alert. • **Schedule** — The schedule for how often the alert checks for matching conditions. • **Behavior** — The setting for how the alert behaves once it is triggered. • **Last Evaluated** — The date on which the alert was last evaluated. • **Last Triggered** — The date on which the alert was last triggered.

Section	Action
	• **Status** — The status of the alert. • **Created** — The date on which the alert was created. • **Last Modified** — The date on which the alert was last modified. • **Owner** — The user who created or owns the alert. • **Group** — The group associated with the **Owner**. • **ID** — The unique identifier of the alert.
Condition	View the conditions specified for the alert: • **Type** — The type of the alert. For example, vulnerability, event, or ticket. • **Trigger** — The condition that triggers the alert. For example, IP count, unique vulnerability/event count, or port count. • **Query** — The dataset to which the trigger condition is compared. • **Filters** — The filters added for vulnerability or event data.
Actions	The actions performed once the alert is triggered.

Alert Options

The following options are available when you create or edit an alert in Tenable Security Center.

Option	Description
General	
Name	The name of the alert.
Description	A description for the alert.
Schedule	Specifies how often the alert checks for the conditions to be matched: **Minutely**, **Hourly**, **Daily**, **Weekly**, **Monthly**, or **Never**. Select **Never** to create an alert that you trigger manually on demand.

Option	Description
General	
Behavior	Specifies how many times Tenable Security Center performs the alert actions: • **Perform actions only on first trigger** — Tenable Security Center performs the alert actions only the first time the alert conditions match the trigger configuration. • **Perform action on every trigger** — Tenable Security Center performs the alert actions every time the alert conditions match the trigger configuration.
Condition	
Type	The type of data to use for the condition: **Vulnerability**, **Event**, or **Ticket**.
Trigger	• **IP Count** — Trigger on vulnerabilities or events whose IP address count matches the given parameters. • **Unique Vulnerability Count** — Trigger an alert when the unique vulnerability count matches the given parameters. This option appears when you select **Vulnerability** for the **Type** option. • **Event Count** — Trigger an alert when the event count matches the given parameters. This option appears when you select **Event** for the **Type** option. • **Port Count** — Trigger an alert when the events or vulnerabilities using a certain port number match the given parameters.
Query	The dataset Tenable Security Center uses to determine if trigger conditions have been met.
Filters	Apply advanced filters to the vulnerability or event data. For more information, see Filters.
Actions	

Option	Description
General	
Add Actions	Specifies the actions that occur when the alter triggers: **Assign Ticket**, **Email**, **Generate Syslog**, **Launch Scan**, **Launch Report**, or **Notify Users**. For more information, see Alert Actions.

Edit an Alert

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

For more information, see Alert Options.

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

You can submit an alert for evaluation to test whether the alert has met the configured time criteria or not.

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 evaluate.

   The actions menu appears.

   -or-

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

   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

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 delete.

The actions menu appears.

–or–

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

The available actions appear at the top of the table.

4. At the top of the table, click **More** > **Delete**.

   A confirmation window appears.

5. Click **Delete**.

   Tenable Security Center deletes the alert.

Tickets

In Tenable Security Center, you can create tickets manually or automatically using the Alerts feature. This section describes how to manage your tickets.

For more information, see:

- Open a Ticket

- View Ticket Details

- Ticket Options

- Edit a Ticket

- Resolve and Close a Ticket

Open a Ticket

Required Tenable Security Center User Role: Organizational user with appropriate permissions. For more information, see User Roles.

You can use tickets within Tenable Security Center to coordinate the assessment and remediation of vulnerabilities and security events.

You can configure a ticket from an analysis page, or from the **Tickets** page. For more information about the options to configure, see Tickets.

To open a ticket from an analysis page:

1. Log in to Tenable Security Center via the user interface.

2. Click **Analysis** > **Vulnerabilities** or **Analysis** > **Events**.

   The Vulnerabilities or **Events** page appears.

3. From the toolbar, click **More** > **Open Ticket**.

   The **Open Ticket** pane appears.

4. In the **Name** box, type a name.

5. (Optional) In the **Description** box, type a description.

6. (Optional) In the **Notes** box, type a note to the assignee.

7. In the **Assignee** drop-down box, select an assignee.

8. In the **Classification** drop-down box, select a classification.

9. Click **Submit**.

   Tenable Security Centercreates the ticket.

To open a ticket from the **Tickets** page:

1. Log in to Tenable Security Center via the user interface.

2. Click **Workflow** > **Tickets**.

   The **Tickets** page appears.

3. Click **Add**.

4. In the **Name** box, type a name.

5. (Optional) In the **Description** box, type a description.

6. (Optional) In the **Notes** box, type a note to the assignee.

7. In the **Assignee** drop-down box, select an assignee.

8. In the **Classification** drop-down box, select a classification.

9. (Optional) Click **Add Query View**.

10. Click **Submit**.

Tenable Security Center creates the ticket.

View Ticket Details

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

You can view the summary details of a ticket with the name, status, creator, assignee, history, queries, description, and ticket notes.

Before you begin:

- Add a ticket, as described in Open a Ticket.

To edit a ticket:

1. Log in to Tenable Security Center via the user interface.

2. Click **Workflow** > **Tickets**.

   The **Tickets** page appears.

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

   The actions menu appears.

   -or-

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

   The available actions appear at the top of the table.

4. Click **View**.

   The **View Ticket** page appears. For more information, see Ticket Options.

Section	Action
Options drop-down box	- To edit the ticket, click **Edit**. For more information, see Edit a Ticket.
General	View general information about the ticket. - **Name** — The ticket name.

Section	Action
	• **Description** — The ticket description. • **Notes** — The notes added for the ticket. • **Status** — The status of the ticket. • **Assignee** — The user assigned to the ticket. • **Classification** — The classification selected for the ticket. • **Created** — The date on which the ticket was created. • **Last Modified** — The date on which the ticket was last modified. • **Owner** — The user who created or owns the ticket. • **Group** — The group associated with the **Owner**. • **ID** — The unique identifier of the ticket.
Query Views	The query added to help provide context for coming up with a resolution.

Ticket Options

The following options are available when you create or edit a ticket in Tenable Security Center.

Option	Description
General	
Name	Name assigned to the ticket.
Description	Descriptive text for the ticket.
Notes	Notes for the ticket assignee.
Assignee	User that the ticket is assigned to. **Note:** If the ticket assignee is deleted, the ticket is automatically reassigned to the assignee's owner along with a notification message indicating that the

Option	Description
	ticket has been reassigned.
Status (Available during edit)	The following ticket statuses become available after a ticket has been created and are available from the **Edit Ticket** page: • **Assigned** • **Resolved** • **More Information** • **Not Applicable** • **Duplicate** • **Closed**
Classification	The ticket classification: **Information**, **Configuration**, **Patch**, **Disable**, **Firewall**, **Schedule**, **IDS**, **Accept Risk**, **Recast Risk**, **Re-scan Request**, **False Positive**, **System Probe**, **External Probe**, **Investigation Needed**, **Compromised System**, **Virus Incident**, **Bad Credentials**, **Unauthorized Software**, **Unauthorized System**, **Unauthorized User**, and **Other**.
Query Views	
Add Query View	Click to choose a query for the ticket assignee to help provide context for coming up with a resolution.

Edit a Ticket

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

Before you begin:

- Add a ticket, as described in Open a Ticket.

To edit a ticket:

1. Log in to Tenable Security Center via the user interface.

2. Click **Workflow** > **Tickets**.

   The **Tickets** page appears.

3. In the table, right-click the row for the ticket you want to edit.

   The actions menu appears.

   -or-

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

   The available actions appear at the top of the table.

4. Click **More** > **Edit**.

   The **Edit Ticket** page appears.

5. Modify the ticket options. For more information, see Ticket Options.

6. Click **Submit**.

   Tenable Security Center saves your configuration.

Resolve and Close a Ticket

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

When a ticket is mitigated, you can change the ticket status to **Resolved**. Once the ticket is resolved, you can change the status to **Closed**. Tickets in the **Resolved** or **Closed** state can always be reopened as needed.

Before you begin:

- Add a ticket, as described in Open a Ticket.

To resolve a ticket:

1. Log in to Tenable Security Center via the user interface.

2. Click **Workflow** > **Tickets**.

The **Tickets** page appears.

3. In the table, right-click the row for the ticket you want to resolve.

    The actions menu appears.

    -or-

    In the table, select the check box for the ticket you want to resolve.

    The available actions appear at the top of the table.

4. Click **Resolve**.

    The **Resolve Ticket** page appears.

5. Change the status to **Resolved**. Optionally, you can add notes to provide details of the resolution.

6. Click **Submit**.

7. To close the ticket, click the resolved ticket name and change the status to **Closed**.

Tenable Security Center updates the ticket status. Resolved tickets still show up in your ticket queue with an **Active** status. Closing a ticket removes the ticket from the **Active** status filter view, but does not provide the option to add notes similar to editing a ticket.

Accept Risk Rules

The **Accept Risk Rules** page displays a list of accept risk rules configured in Tenable Security Center. Organizational users must add accept risk rules before the rules appear on this page. For more information, see Add 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. For more information, see Filters.

Administrator and organizational users can manage accept risk rules. You can access information on what particular vulnerabilities or hosts have been declared to be accepted and, if noted in the comments, the reason.

To view details for a rule, click the row. To delete a rule, see Delete an Accept Risk Rule.

Add an Accept Risk Rule

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

If you create an accept risk rule, Tenable Security Center automatically accepts the risk associated with any vulnerabilities that match the rule. Risk-accepted vulnerabilities do not appear in a vulnerability search if your filter excludes **Accepted Risk** vulnerabilities.

For more information, see Accept Risk Rules.

To add an accept risk rule:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.

3. In the analysis tools drop-down box, select **Vulnerability Detail List**, **Vulnerability List**, or **Vulnerability Summary**.

   The page refreshes to show the analysis tool view you selected.

4. To accept risk, do one of the following:

Accept Risk Rule	Actions
To accept risk rule for a single vulnerability	• Right-click any row for which you want to accept risk and select **Accept Risk**. • Select the check box next to the vulnerability for which you want to accept risk and in the toolbar, click **Accept Risk**.
To accept risk rule for multiple vulnerabilities	• Select more than one row and in the toolbar, click **Accept Risk**.

   The **Accept Risk** pane appears.

5. (Optional) In the **Comment** box, add a comment.

6. (Optional) In the **Expires** box, select the date you want the accept risk rule to expire.

7. In the **Repository** section, select one or more repositories where you want to apply the rule.

8. Click **Submit**.

   Tenable Security Center saves your configuration.

   > **Note:** There can be a short delay between clicking on **Submit** and vulnerabilities showing the new risk acceptance. You may need to reload the filters to view the applied changes.

What to do next:

- (Optional) Enable **Recast and Accept Risk Rule Comments** to display contents of the **Comment** field in reports and vulnerability analysis views. For more information, see Risk Rule Comments.

Delete an Accept Risk Rule

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can delete an accept risk rule to stop accepting the risk associated with a vulnerability.

To delete an accept risk rule:

1. Log in to Tenable Security Center via the user interface.

2. Click **Workflow** > **Accept Risk Rules** (Organizational users) or **Repositories** > **Accept Risk Rules** (Administrator users).

   The **Accept Risk Rules** page appears.

3. To delete a single rule:

   a. In the table, right-click the row for the rule you want to delete.

      The actions menu appears.

   To delete multiple rules:

   a. In the table, select the check box for each rule you want to delete.

      The available actions appear at the top of the table.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

   Tenable Security Center deletes the rule.

   > **Note**: Tenable Security Center automatically deletes expired accept risk rules through an hourly scheduled job.

6. Click **Apply Rules**.

   Tenable Security Center stops accepting the risk associated with the vulnerability.

Recast Risk Rules

A list of recast rules configured in Tenable Security Center appears on the **Recast Risk Rules** page. Organizational users must add recast risk rules before the rules appear on this page. For more information, see Add a Recast Risk Rule.

Administrator and organizational users can manage recast risk rules. You can access information on what particular vulnerabilities or hosts have had risk levels recast, their new severity level and, if noted in the comments, the reason for the severity change. You can search for rules by Plugin ID or Repository.

You can set an expiration date for a recast risk rule. When a recast risk rule expires, the severity will reset based on the following criteria:

- If an administrator has configured Tenable Security Center to use CVSSv3 at the organization level, and there are CVSSv3 metrics available, the severity level of the vulnerability will return to the level determined by the CVSSv3 data.

- If an administrator has not configured Tenable Security Center to use CVSSv3, or there are no CVSSv3 metrics available, the vulnerability will retain the recast severity level. If Tenable Security Center finds the vulnerability again, the vulnerability will receive the severity level currently determined by the plugin.

To view details for a rule, click the row. To delete a rule, see Delete a Recast Risk Rule.

Add a Recast Risk Rule

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

If you create a recast risk rule, Tenable Security Center automatically updates the severity for any vulnerabilities that match the rule to the severity you specified in the rule.

For more information, see Recast Risk Rules.

To add a recast risk rule:

1. Log in to Tenable Security Center via the user interface.

2. In the left navigation, click **Analysis** > **Vulnerabilities**.

   The **Vulnerabilities** page appears.

3. In the analysis tools drop-down box, select **Vulnerability Detail List**, **Vulnerability List**, or **Vulnerability Summary**.

   The page refreshes to show the analysis tool view you selected.

4. To recast risk, do one of the following:

Recast Risk Rule	Actions
To recast risk rule for a single vulnerability	• Right-click any row that you want to recast and select **Recast Risk**. • Select the check box next to the vulnerability that you want to recast and in the toolbar, click **Recast Risk**.
To recast rule for multiple vulnerabilities	• Select more than one row and in the toolbar, click **Recast Risk**.

   The **Recast Risk** pane appears.

5. In the **New Severity** drop-down box, select a new severity for the vulnerability.

6. (Optional) In the **Comment** box, add a comment.

7. (Optional) In the **Expires** box, select the date you want the recast risk rule to expire.

8. In the **Repository** section, select one or more repositories where you want to apply the rule.

9. Click **Submit**.

   Tenable Security Center saves your configuration.

   > **Note:** There can be a short delay between clicking on **Submit** and vulnerabilities showing the new risk. It may be necessary to reload the filters to view the applied changes.

What to do next:

- (Optional) Enable **Recast and Accept Risk Rule Comments** to display contents of the **Comment** field in reports and vulnerability analysis views. For more information, see Risk Rule Comments.

Edit a Recast Risk Rule

> **Required Tenable Security Center User Role:** Organizational user with appropriate permissions. For more information, see User Roles.

If you create a recast risk rule, Tenable Security Center automatically updates the severity for any vulnerabilities that match the rule to the severity you specified in the rule. You can edit the expiration date of existing recast risk rules.

For more information, see Recast Risk Rules.

To edit the expiration date of a recast risk rule:

1. Log in to Tenable Security Center via the user interface.

2. Click **Workflow** > **Recast Risk Rules**.

   The **Recast Risk Rules** page appears.

3. To edit a single rule:

   a. In the table, right-click the row for the rule you want to edit.

      The actions menu appears.

   To edit multiple rules:

a. In the table, select the check box for each rule you want to edit.

The available actions appear at the top of the table.

4. Click **Edit**.

The **Edit Recast Rules** pane appears.

5. In the **Expires** box, select the date you want the recast risk rule to expire.

6. Click **Submit**.

Tenable Security Center saves your configuration.

Delete a Recast Risk Rule

> **Required Tenable Security Center User Role:** Administrator or organizational user with appropriate permissions. For more information, see User Roles.

You can delete a recast risk rule to remove your custom severity for a vulnerability. Then, if Tenable Security Center sees the vulnerability again, the vulnerability receives the severity currently associated with the plugin.

To delete a recast risk rule and remove your custom severity:

1. Log in to Tenable Security Center via the user interface.

2. Click **Workflow** > **Recast Risk Rules** (Organizational users) or **Repositories** > **Recast Risk Rules** (Administrator users).

The **Recast Risk Rules** page appears.

3. To delete a single rule:

a. In the table, right-click the row for the rule you want to delete.

The actions menu appears.

To delete multiple rules:

a. In the table, select the check box for each rule you want to delete.

The available actions appear at the top of the table.

4. Click **Delete**.

A confirmation window appears.

5. Click **Delete**.

   Tenable Security Center deletes the rule.

6. Click **Apply Rules**.

   If Tenable Security Center sees the vulnerability again, the vulnerability receives the severity currently associated with the plugin.

Additional Resources

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

- [Start, Stop, or Restart Tenable Security Center](#)

- [License Declarations](#)

- [Encryption Strength](#)

- [File and Process Allow List](#)

- [Manual Log Correlation Engine Key Exchange](#)

- [Manual Tenable Nessus SSL Certificate Exchange](#)

- [Offline Plugin and Feed Updates for Tenable Security Center](#)

- [Troubleshooting](#)

Start, Stop, or Restart Tenable Security Center

Required Tenable Security Center User Role: Root user

When Tenable Security Center is installed, the required services are started by default.

To change the status of 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 to check the status of your Tenable Security Center:

   ```
   # service SecurityCenter status
   ```

   The system indicates whether Tenable Security Center is running or stopped.

3. Run one of the following commands to change the status of your Tenable Security Center:

- To start Tenable Security Center, run:

```
# /bin/systemctl start SecurityCenter
```

- To stop Tenable Security Center, run:

```
# /bin/systemctl stop SecurityCenter
```

- To restart Tenable Security Center, run:

```
# /bin/systemctl restart SecurityCenter
```

4. If you are running Tenable Security Center 6.5.x or later with a managed PostgreSQL database on the same server, then run the following commands to start and stop the PostgreSQL database:

- To start the PostgreSQL database, run:

```
# su - tns -c "/opt/sc/support/bin/pg_ctl -D /opt/sc/data/postgresql/ -l
/opt/sc/admin/logs/postgresql.log start"
```

- To stop the PostgreSQL database, run:

```
# su - tns -c "/opt/sc/support/bin/pg_ctl -D /opt/sc/data/postgresql/ stop"
```

> **Note:** These commands assume the install path for the PostgreSQL database is `/opt/sc/`. Replace `/opt/sc/` with your install path if necessary. For more information about managed PostgreSQL databases, see Connect an External PostgreSQL Server.

License Declarations

Tenable Security Center's Software License Agreement can be found on Tenable Security Center in the `/opt/sc/docs` directory.

For a list of third-party software packages that Tenable utilizes with Tenable Security Center, see Tenable Third-Party License Declarations.

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, as described in Credentials.	AES-256-CBC
Storing scan data, as described in Repositories.	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, CLI program, or API program: EECDH+AESGCM, EDH+AESGCM, AES256+EECDH, or AES256+EDH. For more information about strong encryption, see Configure SSL/TLS Strong Encryption.
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	TLS 1.2 with the strongest encryption method supported by

Function	Encryption
between Tenable Security Center and: • Tenable Nessus or Tenable Nessus Manager • Tenable Vulnerability Management • Tenable Network Monitor • Tenable Log Correlation Engine	Tenable Security Center Apache and your browser, CLI program, or API program: ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-SHA384, or ECDHE-RSA-AES256-GCM-SHA384.
Synchronizations between Tenable Security Center and Tenable Vulnerability Management for Tenable Lumin.	TLS 1.2

Configure SSL/TLS Strong Encryption

You can configure SSL/TLS strong encryption for Tenable Security Center-client communications to meet the security needs of your organization. For more information about Tenable Security Center encryption, see Encryption Strength.

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-RSA-
AES256-SHA384:ECDHE-RSA-AES256-GCM-SHA384
```

3. Restart Tenable Security Center, as described in Start, Stop, or Restart Tenable Security Center.

   Tenable Security Center restarts.

4. In `/opt/sc/support/logs`, open `ssl_request_log`.

   The log file text appears.

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

If your organization requires that your instance of Tenable Security Center meets National Information Assurance Partnership (NIAP) standards, you can configure relevant settings to be compliant with NIAP standards.

You must run Tenable Security Center 5.15.0 or later to fully configure Tenable Security Center for NIAP compliance. If you are running Tenable Security Center 5.15.0, you must install a patch to configure Tenable Security Center for NIAP compliance. Contact Tenable Support for assistance with the required patch. For more information about upgrading Tenable Security Center, see Before You Upgrade and Upgrade Tenable Security Center.

For more information about Tenable Security Center storage and communications encryption, see Encryption Strength.

Before you begin:

- If you are running Tenable Security Center 5.15.0, contact Tenable Support for assistance with the required patch.

- 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 to Tenable Security Center via the command line interface (CLI).

2. In the CLI in Tenable Security Center, as the root or `tns` user, run the following commands to configure strong SSL/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-RSA-
AES128-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-
AES256-GCM-SHA384', 'false', 'false' )"
```

3. Configure the Tenable Security Center web server to use strong encryption for storage and communications, as described 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 Manager, Tenable Network Monitor, or Tenable Log Correlation Engine, you must use certificates to authenticate the connection. For more information, see Manual Tenable Nessus SSL Certificate Exchange and Manual Log Correlation Engine Key Exchange.

File and Process Allow List

If you use third-party endpoint security products such as anti-virus applications and host-based intrusion and prevention systems, Tenable recommends adding Tenable Security Center to the allow list.

If you configured supporting resources for Tenable Security Center, see the product documentation for each resource you added for more file and process allow list information. For more information about supporting resources in Tenable Security Center, see Resources.

Tenable recommends allowing the following Tenable Security Center files and processes.

Allow List
Files
/opt/sc/*
Processes
/opt/sc/bin/*
/opt/sc/src/*
/opt/sc/support/bin/*
/opt/sc/www/*

Asset Tracking in Tenable Security Center

Assets in Tenable Security Center are tracked by several attributes, depending on the asset repository and scan configuration of the sensors that identify the assets.

- Assets in universal repositories are tracked by asset attribute.

- Assets in IPv4 and IPv6 repositories are tracked by IP address.

- Assets in agent repositories are tracked by agent UUID.

When you import asset data, if Tenable Security Center cannot find an existing asset that matches the imported host, the asset is added to Tenable Security Center as a new asset.

For more information about repositories in Tenable Security Center, see Repositories.

Universal Repositories

The following identification attributes (IA) are considered in determining whether or not an imported asset matches an existing one, in descending order of priority:

1. Tenable UUID (from credentialed scans of managed hosts, Tenable Agents, or imported Tenable OT Security data)

2. BIOS UUID

3. MAC Address

4. NetBIOS Name

5. Fully Qualified Domain Name (FQDN)

6. IP Address (IPv4 and IPv6)

Similar to Tenable Vulnerability Management, Tenable Security Center verifies that there are no conflicting higher priority attributes when it finds a match. For example, if there is a MAC Address match, but the Tenable UUID is different, the assets will not merge. When a unique asset is discovered, the following informational message will appear in `/opt/sc/admin/logs/YYMMdd.log` (`sc-logs.txt` in a Tenable Security Center debug zip).

```
Scan Result #<Job ID> - <IP Address or Agent UUID> did not match any existing assets
```

Possible root causes for duplicate assets include, but are not limited to:

- different scan types for the same asset, such as Agent scans and non-credentialed Tenable Nessus scans or, similarly, credentialed Tenable Nessus scans with the **Create unique identifier on hosts scanned using credentials** (host_tagging) setting disabled in the Advanced settings of the scan policy. While Agent scans have access to the local Tenable UUID, the same is not true for a non-credentialed or equivalent scan. If an asset was duplicated as a result of a non-credentialed or equivalent scan after a credentialed one, the assets will not merge until the next credentialed or equivalent scan.

- different network interfaces of an asset scanned in one or more non-credentialed scans. Because each network interface is associated with a different MAC Address, and the Tenable UUID cannot be accessed in a non-credentialed scan, a unique asset will be created for each network interface.

For more information about universal repositories, see [Universal Repositories](#).

IPv4 and IPv6 Repositories

If the **Track hosts which have been issued new IP address** setting is enabled (default), assets are tracked using the following IAs in this order:

1. DNS Name

2. NetBIOS Name

3. Tenable UUID (from credentialed scans of managed hosts)

4. MAC Address

5. IP Address (IPv4 or IPv6, based on repository type)

If the **Track hosts which have been issued new IP address** setting is disabled, assets are tracked only by IP address.

During scan import, Tenable Security Center checks the targeted repository for the scan job for the above listed IAs.

- If the IP has the attributes mentioned above, Tenable Security Center migrates all of the vulnerabilities in the cumulative results to the IP seen in the scan result.

- If the IP does not have any of the attributes mentioned above, Tenable Security Center considers this a new asset.

- Once a match has been made, Tenable Security Center does not search for more matches.

For example, if Tenable Security Center does not match a DNS name, but it does match a NetBIOS name, the system does not check the Agent UUID or MAC address.

> **Note:** The **Track hosts which have been issued new IP address** setting is in the Advanced settings section, and is enabled by default in Active Scans. Tenable recommends that networks using DHCP enable this setting to properly track hosts.

For more information about IPv4 and IPv6 repositories, see [IPv4/IPv6 Repositories](#).

Agent Repositories

Assets in agent repositories are tracked by UUID, because all assets in agent repositories have UUIDs.

For more information about agent repositories, see [Agent Repositories](#).

Manual Log Correlation Engine Key Exchange

> **Required Tenable Security Center User Role:** Administrator

You are not normally required to make a manual key exchange between Tenable Security Center and the Log Correlation Engine; however, in some cases where you are prohibited from remote root login or required to do key exchange debugging, you must manually exchange the keys.

For the remote Log Correlation Engine to recognize Tenable Security Center, copy the SSH public key of Tenable Security Center and append it to the `/opt/lce/.ssh/authorized_keys` file. The `/opt/lce/daemons/lce-install-key.sh` script performs this function.

> **Note:** The Log Correlation Engine server must have a valid license key installed and the Log Correlation Engine daemon must be running before you perform the steps below.

To perform manual Log Correlation Engine key exchange:

1. Log in to Tenable Security Center via the user interface.

2. Download the Tenable Security Center key, as described in [Download the Tenable Security Center SSH Key](#).

3. Save the file locally as **SSHKey.pub**.

   > **Caution:** 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 (e.g., WinSCP) to copy the **SSHKey.pub** file to the Log Correlation Engine system.

   > **Note:** You must have the credentials of an authorized user on the Log Correlation Engine server to perform this step.

For example, if you have a user **username** configured on the Log Correlation Engine server (hostname **lceserver**) whose home directory is **/home/username**, the command on a Unix system is as follows:

```
# scp SSHKey.pub username@lceserver:/home/username
```

5. After you copy the file to the Log Correlation Engine server, in the CLI, run the following command to move the file to /opt/lce/daemons:

```
# mv /home/username/SSHKey.pub /opt/lce/daemons
```

6. On the Log Correlation Engine server, as the root user, run the following command to change the ownership of the SSH key file to lce:

```
# chown lce /opt/lce/daemons/SSHKey.pub
```

7. Run the following command to append the SSH public key to the **/opt/lce/.ssh/authorized_ keys** file:

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

8. To test the communication, as the user tns on the Tenable Security Center system, attempt to run the id command:

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

If you have not previously established a connection, a warning appears that is similar to the following:

```
The authenticity of host '198.51.100.28 (198.51.100.28)' can't be established.
RSA key fingerprint is 86:63:b6:c3:b4:3b:ba:96:5c:b6:d4:42:b5:45:37:7f.
Are you sure you want to continue connecting (yes/no)?
```

9. Answer yes to this prompt.

If the key exchange worked correctly, a message similar to the following appears:

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

10. You can add the IP address of Tenable Security Center to the Log Correlation Engine system's `/etc/hosts` file. This prevents the SSH daemon from performing a DNS lookup that can add seconds to your query times.

11. You can add the Log Correlation Engine to Tenable Security Center via the normal administrator process, described in Log Correlation Engines.

Manual Tenable Nessus SSL Certificate Exchange

If you want to use self-signed certificates for the Tenable Security Center-Tenable Nessus connection, you can perform 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
- Tenable Nessus Certificate Configuration for Unix
- Tenable Nessus Certificate Configuration for Windows

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 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 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 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 (Tenable Security Center)

The Nessus client, Tenable Security Center, communicates with the Nessus server via SSL. 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 SSL process on a Red Hat Linux system. This process creates the following files:

File Name Created	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,	/opt/nessus/com/nessus/CA on the initial Nessus server and any additional Nessus servers that need to authenticate using SSL.

File Name Created	Purpose	Where to Copy to
	this will be provided to you by the PKI and must be copied to this location.	
/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 SSL.
/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/var/nessus/CA on any additional Nessus servers that need to authenticate using SSL.

File Name Created	Purpose	Where to Copy to
/opt/nessus/var/nessus/CA/serverkey.pem	This is the private key of the Nessus server.	/opt/nessus/var/nessus/CA on any additional Nessus servers that need to authenticate using SSL.

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

File Name Created	Purpose
	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 SSL 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 appropriate 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. For more information, see Add a Tenable Nessus Scanner.

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.

Before you begin:

- Set up and configure all of your Tenable Nessus scanners.

- Add your Tenable Nessus scanners to Tenable Security Center, as described in Add a Tenable Nessus Scanner.

To duplicate the same authentication configuration on other Tenable Nessus scanners:

1. In the command line interface (CLI) on another Tenable Nessus server, run the following command to copy the certificate files onto your other Tenable Nessus server:

```
# 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
```

2. Run the following command to create a user directory on your second Tenable Nessus server, using the same name as [the user you created on the first Tenable Nessus server](). Replace *admin* with the user's name:

```
/opt/nessus/sbin/nessuscli adduser admin
```

A confirmation prompt appears.

3. Press **y** to confirm you want the user to have system administrator privileges.

Tenable Nessus creates the user.

4. Run the following command to copy the [the user you created on the first Tenable Nessus server]() to the directory you created in step 2. Replace *admin* 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"
```

5. Run the following command to force Tenable Nessus to authenticate via certificate:

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

6. 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
```

7. In Tenable Security Center, update all of your Tenable Nessus scanner configurations to use SSL certificate-based authentication. For more information, see Add a Tenable Nessus Scanner.

Tenable Nessus Certificate 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:

File Name Created	Purpose	Where to Copy to
C:\Program Files\Tenable\Nessus\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.	C:\Program Files\Tenable\Nessus\nessus\ CA\ on any additional Nessus servers that need to authenticate using SSL.
C:\Program Files\Tenable\Nessus\nessus\CA\servercert.pem	This is the public	C:\Program Files\Tenable\Nessus\nessus\ CA\ on any additional Nessus

File Name Created	Purpose	Where to Copy to
	certificate for the Nessus server that is sent in response to a CSR.	servers that need to authenticate using SSL.
C:\Program Files\Tenable\Nessus\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.	C:\Program Files\Tenable\Nessus\nessus\CA\ on any additional Nessus servers that need to authenticate using SSL.
C:\Program Files\Tenable\Nessus\nessus\CA\serverkey.pem	This is the private key of the Nessus server.	C:\Program Files\Tenable\Nessus\nessus\CA\ on any additional Nessus servers that need to authenticate using SSL.

Nessus Client Keys

The Nessus user, which in this case is the user ID that Tenable Security Center 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 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**.

The following files are created by this command:

File Name Created	Purpose
C:\Documents and Settings\<UserAccount>\Local Settings\Temp\nessus-xxxxxxxx\cert_<user>.pem	This is the public certificate for the specified user.
C:\Documents and Settings\<UserAccount>\Local Settings\Temp\nessus-xxxxxxxx\key_<user>.pem	This is the private key for the specified user.
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 options 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

To create the keys and user:

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

2. Provide the requested information.

> **Caution:** Critical: 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 policies.db from the Nessus Scanner to ensure the deployment finishes successfully.

3. To remove the `policies.db` on a Linux system issue this command as root:

   `rm /opt/nessus/var/nessus/users/<UserName>/policies.db`

4. To remove the `policies.db` on a Windows system, navigate to the `C:\Program Files\Tenable\Nessus` folder and remove the policies.db file. The actual location of the `policies.db` differs depending on the version of Windows that is running.

5. 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 using the following command:

   `C:\Program Files\Tenable\Nessus\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 certificates created contain the username entered previously, in this case **admin**, and are located in the directory as listed in the example 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 Tenable Security Center

Transfer the `cert_admin.pem` and `key_admin.pem` files to a desired location on Tenable Security Center, change into that directory and concatenate them as follows:

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

Note: The `nessuscert.pem` file will be 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:

```
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

In Tenable Security Center, update your Tenable Nessus scanner configuration to use SSL certificate-based authentication. For more information, see Add a Tenable Nessus Scanner.

Offline Plugin and Feed Updates for Tenable Security Center

You can perform offline plugin updates and feed updates in air-gapped Tenable Security Center environments.

[Perform an Offline Nessus Plugin Update](#)

[Perform an Offline Tenable Network Monitor Plugin Update](#)

[Perform an Offline Tenable Security Center Feed Update](#)

[Perform an Offline Tenable Web App Scanning Plugins Update](#)

[Configure Tenable Nessus + Tenable Web App Scanning for Tenable Security Center Offline](#)

> **Note:** Tenable Security Center does not manage plugins for Log Correlation Engine. However, Log Correlation Engine plugins are required for event analysis.

For general information about best practices in air-gapped environments, see [Considerations for Air-Gapped Environments](#).

Perform an Offline Nessus Plugin Update

> **Required Tenable Security Center User Role:** Administrator

Before you begin:

- If you installed Tenable Security Center in an environment other than Tenable Core, install a temporary Tenable Nessus scanner on the same host as Tenable Security Center. You will use this temporary Tenable Nessus scanner to generate a challenge code for offline Tenable Security Center registration. Do not start or otherwise configure the temporary Tenable Nessus scanner.

To perform an offline Tenable Nessus plugin update:

1. In the command line interface (CLI), run the following command to prevent the Tenable Nessus scanner from starting automatically upon restarting the system:

```
/usr/bin/systemctl disable nessusd
```

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

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

3. In your browser, navigate to https://plugins.nessus.org/offline.php.

> **Note:** Do not click **here**, even if you have a newer version of Tenable Nessus installed. You cannot use the https://plugins.nessus.org/v2/offline.php page for Tenable Security Center downloads.

4. Paste the challenge string from Step 3 and your Activation Code in the appropriate boxes on the web page.

5. Click **Submit**.

6. On the next page, copy the link that starts with **https://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.

> **Caution:** Do not click the link for nessus-fetch.rc.

7. Go to the favorite you created.

   The page prompts you to download a file.

8. Download the file, which is called `sc-plugins-diff.tar.gz`.

9. Verify the file using the MD5 checksum, as described in the knowledge base article.

10. Save the `sc-plugins-diff.tar.gz` on the system used to access your Tenable Security Center web interface.

11. Log in to Tenable Security Center via the user interface.

12. Click **System** > **Configuration**.

    The **Configuration** page appears.

13. Click **Plugins/Feed**.

The **Plugins/Feed Configuration** page appears.

14. In the **Schedules** section, expand the **Active Plugins** options.

15. Click **Choose File** and browse to the saved `sc-plugins-diff.tar.gz` file.

16. Click **Submit**.

After several minutes, the plugin update finishes and the page updates the **Last Updated** date and time.

What to do next:

- If you installed a temporary Tenable Nessus scanner on the same host as Tenable Security Center, uninstall the Tenable Nessus scanner.

Perform an Offline Tenable Network Monitor Plugin Update

Required Tenable Security Center User Role: Administrator

Before you begin:

- If you installed Tenable Security Center in an environment other than Tenable Core, install a temporary Tenable Nessus scanner on the same host as Tenable Security Center. You will use this temporary Tenable Nessus scanner to generate a challenge code for offline Tenable Security Center registration. Do not start or otherwise configure the temporary Tenable Nessus scanner.

To perform an offline Tenable Network Monitor plugin update:

1. In the command line interface (CLI), run the following command to prevent the Tenable Network Monitor scanner from starting automatically upon restarting the system:

   ```
   /usr/bin/systemctl disable nnm
   ```

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

   ```
   # /opt/nnm/bin/nnm --challenge
   ```

3. In your browser, navigate to the Tenable Network Monitor plugins page.

4. Paste the challenge string from Step 3 and your Activation Code in the appropriate boxes on the web page.

5. Click **Submit**.

6. On the next page, copy the link that starts with **https://plugins.nessus.org/v2/...** and bookmark it in your browser. The other information on the page is not relevant for use with Tenable Security Center.

7. Click the bookmarked link.

   The page prompts you to download a file.

8. Download the file, which is called `sc-passive.tar.gz`.

9. Verify the file using the MD5 checksum, as described in the [knowledge base](#) article.

10. Save the `sc-passive.tar.gz` on the system used to access your Tenable Security Center GUI.

    > **Note:** Access the Tenable Network Monitor feed setting and change the activation from offline to Tenable Security Center.

11. Log in to Tenable Security Center via the user interface.

12. Click **System** > **Configuration**.

    The **Configuration** page appears.

13. Click **Plugins/Feed**.

    The **Plugins/Feed Configuration** page appears.

14. In the **Schedules** section, expand the **Passive Plugins** options.

15. Click **Choose File** and browse to the saved `sc-passive.tar.gz` file.

16. Click **Submit**.

    After several minutes, the plugin update finishes and the page updates the **Last Updated** date and time.

What to do next:

- If you installed a temporary Tenable Nessus scanner on the same host as Tenable Security Center, uninstall the Tenable Nessus scanner.

Perform an Offline Tenable Security Center Feed Update

> **Required Tenable Security Center User Role:** Administrator

> **Note:** If you already performed a Tenable Nessus offline plugin update, start at step 7.

Before you begin:

- If you installed Tenable Security Center in an environment other than Tenable Core, install a temporary Tenable Nessus scanner on the same host as Tenable Security Center. You will use this temporary Tenable Nessus scanner to generate a challenge code for offline Tenable Security Center registration. Do not start or otherwise configure the temporary Tenable Nessus scanner.

To perform an offline Tenable Security Center feed update:

1. In the command line interface (CLI), run the following command to prevent the Tenable Nessus scanner from starting automatically upon restarting the system:

   ```
   /usr/bin/systemctl disable nessusd
   ```

2. To obtain the challenge code for an offline Tenable Security Center registration, do one of the following:

   - If you deployed Tenable Security Center + Tenable Core, navigate to the **Tenable Security Center** tab in Tenable Core and save the challenge code.

   - If you installed Tenable Security Center in an environment other than Tenable Core, run the following command and save the challenge code:

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

3. In your browser, navigate to https://plugins-customers.nessus.org/offline.php.

4. Paste the challenge code from Step 2 and your Activation Code in the appropriate boxes on the web page.

5. Click **Submit**.

6. On the next page, copy the link that starts with **https://plugins.nessus.org/get.php...** and save it as a favorite.

7. Within the saved link change **all-2.0.tar.gz** to **SecurityCenterFeed48.tar.gz**. This link is needed for future use.

> **Caution:** Do not click the link for nessus-fetch.rc as it is not needed.

8. Go to the favorite link you created.

   The page prompts you to download a file.

9. Download the file, which will be called `SecurityCenterFeed48.tar.gz`.

10. Verify the file using the MD5 checksum, as described in the knowledge base article.

11. Save the `SecurityCenterFeed48.tar.gz` on the system used to access your Tenable Security Center GUI.

12. Log in to Tenable Security Center via the user interface.

13. Click **System** > **Configuration**.

   The **Configuration** page appears.

14. Click **Plugins/Feed**.

   The **Plugins/Feed Configuration** page appears.

15. In the **Schedules** section, expand the **Tenable Security Center Feed** options.

16. Click **Choose File** and browse to the saved `SecurityCenterFeed48.tar.gz` file.

17. Click **Submit**.

   After several minutes, the plugin update finishes and the page updates the **Last Updated** date and time.

What to do next:

- If you installed a temporary Tenable Nessus scanner on the same host as Tenable Security Center, uninstall the Tenable Nessus scanner.

Perform an Offline Tenable Web App Scanning Plugins Update

Required Tenable Security Center User Role: Administrator

Note: If you have already updated Tenable Nessus plugins offline, or if you have updated plugins via the Tenable Security Center feed, skip to step 8.

Before you begin:

- If you installed Tenable Security Center in an environment other than Tenable Core, install a temporary Tenable Nessus scanner on the same host as Tenable Security Center. You will use this temporary Tenable Nessus scanner to generate a challenge code for offline Tenable Security Center registration. Do not start or otherwise configure the temporary Tenable Nessus scanner.

- Ensure that you are running Tenable Security Center 6.2 or later.

- Ensure that you have a Tenable Web App Scanning license to use with Tenable Security Center

To perform an offline Tenable Security Center feed update:

1. In the command line interface (CLI), run the following command to prevent the Tenable Nessus scanner from starting automatically upon restarting the system:

   ```
   /usr/bin/systemctl disable nessusd
   ```

2. To obtain the challenge code for an offline Tenable Security Center registration, do one of the following:

   - If you deployed Tenable Security Center + Tenable Core, in Tenable Core, click the **Tenable Security Center** tab and save the challenge code.

   - If you installed Tenable Security Center in an environment other than Tenable Core, run

the following command and save the challenge code:

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

3. In your browser, navigate to https://plugins-customers.nessus.org/offline.php.

4. Paste the challenge code from Step 2 and your Activation Code in the corresponding boxes.

5. Click **Submit**.

6. On the next page, copy the link that starts with `https://plugins.nessus.org/get.php...` and save it as a favorite.

7. In the saved link, change `all-2.0.tar.gz` to `sc-was-plugins.tar.gz` and change `/get.php` to `/v2/wasnessus.php`. The link should look like this: `https://plugins.nessus.org/v2/wasnessus.php?f=sc-was-plugins.tar.gz…` This link is needed for future use; save it in a secure location.

8. Go to the favorite link you created.

   The page prompts you to download the `sc-was-plugins.tar.gz` file.

9. Save the `sc-was-plugins.tar.gz` on the system used to access your Tenable Security Center UI.

10. Log in to Tenable Security Center via the UI.

11. Click **System** > **Configuration**.

   The **Configuration** page appears.

12. Click **Plugins/Feed**.

   The **Plugins/Feed Configuration** page appears.

13. In the Schedules section, expand the WAS Plugins options.

14. Click **Choose File** and browse to the saved `sc-was-plugins.tar.gz` file.

15. Click **Submit**.

   After several minutes, the plugin update finishes and the page updates the **Last Updated** date and time.

What to do next:

- If you installed a temporary Tenable Nessus scanner on the same host as Tenable Security Center, uninstall the Tenable Nessus scanner.

- Update the `was-scanner` Docker image on your Tenable Nessus scanners. When updating offline Tenable Web App Scanning plugins, always update the `was-scanner` Docker image and vice-versa.

Configure Tenable Nessus + Tenable Web App Scanning for Tenable Security Center Offline

Required Tenable Security Center User Role: Administrator

Note: If you already configured Tenable Nessus + Tenable Web App Scanning for Tenable Security Center offline, you only need to repeat steps 3-5.

Before you begin:

- Apply the Tenable Web App Scanning for Tenable Security Center license, as described in Update an Existing License.

- Update any Tenable Web App Scanning plugins, as described in Perform an Offline Tenable Web App Scanning Plugins Update.

To configure Tenable Nessus + Tenable Web App Scanning for Tenable Security Center offline:

1. On a system with Docker installed that is connected to the internet, run the following commands:

   ```
   docker pull tenable/was-scanner:latest
   ```

   ```
   docker save tenable/was-scanner:latest > was-scanner-image.tar
   ```

2. Transfer the `was-scanner-image.tar` file to the Tenable Nessus scanner you want to configure as a Tenable Web App Scanning scanner.

3. Ensure the Tenable Nessus scanner host you're configuring:

a. Install and run Docker version 20.0.0 or later on your Tenable Nessus host. Tenable recommends the [official Docker builds and install packages](#).

> **Note:** If your scanner is configured to connect through a proxy, ensure that you configure the proxy settings directly in Docker.

b. Ensure you are running Tenable Nessus version 10.6.1 or later.

c. Ensure Tenable Nessus meets the [Hardware Requirements](#).

d. Run `docker load < was-scanner-image.tar`.

e. Ensure `tenable/was-scanner` is visible when you run `docker image ls`.

4. Enable the Tenable Web App Scanning**Capable** option for the Tenable Nessus scanner in Tenable Security Center, as described in [Tenable Nessus Scanners](#).

5. Add a scan zone in Tenable Security Center, as described in [Add a Scan Zone](#).

6. Add a universal repository for the scan data in Tenable Security Center, as described in [Add a Repository](#).

7. Configure your Tenable Web App Scanning credentials, as described in [Add Credentials](#).

8. Create a Web App Scanning scan policy, as described in [Add a Scan Policy](#).

9. Add a web app scan in Tenable Security Center, as described in [Add a Web App Scan](#).

Migrate Data Between PostgreSQL Implementations

If you want to migrate Tenable Security Center data between PostgreSQL implementations, Tenable offers a script to simplify the process.

The script is supported for the following use cases:

- Existing Tenable Security Center installs that are licensed and configured. For new installs, follow the directions in [Connect an External PostgreSQL Server](#).

- Migrating from an internal to an external PostgreSQL.

- Migrating from an external PostgreSQL 16 to an internal or external PostgreSQL 16 or 17.

- Migrating from an external PostgreSQL 17 to an external PostgreSQL 17. In this scenario, the script will only modify the PostgreSQL configuration. You will need to migrate your data manually after running the script.

> **Note:** The following migration paths are not supported:
>
> - External PostgreSQL 17 to external PostgreSQL 16.
>
> - External PostgreSQL 17 to internal PostgreSQL.

This page includes two sets of instructions:

- [Migrate data from an internal PostgreSQL or a PostgreSQL version 16 implementation](#)

  Use these steps if you are migrating from an internal PostgreSQL to an external PostgreSQL, or if you are migrating from an external PostgreSQL 16 to an internal or external PostgreSQL 16 or 17.

- [Migrate data from a PostgreSQL version 17 implementation](#)

  Use these steps if you are migrating from an external PostgreSQL 17 to an external PostgreSQL 17.

> **Note:** In the following instructions, the *source server* is the PostgreSQL that you are migrating data from, and the *destination server* is the PostgreSQL that you are migrating data to.

Before you begin

- The destination PostgreSQL must be a supported version. For information about supported PostgreSQL versions, see [External PostgreSQL Requirements](#).

- For Tenable Security Center 6.5 and 6.6, download the script php file from the [Tenable downloads site](#) to the server where you have installed Tenable Security Center. Move the script file to `/opt/sc/src/tools`.

- Ensure that both the source PostgreSQL server and the destination PostgreSQL server are currently running.

- On the destination PostgreSQL server, you must have the permission to create a database. If the database is already created, then you must have read and write permissions.

Migrate data from an internal PostgreSQL or a PostgreSQL version 16 implementation

1. Stop Tenable Security Center with the following command:

   ```
   # /bin/systemctl stop SecurityCenter
   ```

2. Set the environment variables for the destination PostgreSQL server.

   > **Note:** You must set the environment variables with a `root` or `tns` user account. Use the same account to run the script in step 4. If you are using the `tns` user account to run the script, switch to the `tns` user using the command `su - tns`.

3. Run the following script on the server where you have installed Tenable Security Center:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/MovePostgresDB.php
   ```

   The data on the source server is copied to the destination server.

4. Start Tenable Security Center with the following command:

   ```
   # /bin/systemctl start SecurityCenter
   ```

Migrate data from a PostgreSQL version 17 implementation

1. Stop Tenable Security Center with the following command:

   ```
   # /bin/systemctl stop SecurityCenter
   ```

2. Set the environment variables for the destination PostgreSQL server.

   > **Note:** You must set the environment variables with a `root` or `tns` user account. Use the same account to run the script in step 4.

3. Run the following script on the server where you have installed Tenable Security Center:

   ```
   /opt/sc/support/bin/php /opt/sc/src/tools/MovePostgresDB.php config-only
   ```

4. Migrate your data from the source server to the destination server.

a. Log in to your source PostgreSQL server with the following command, where *<username>* is your PostgreSQL username:

```
sudo su - <username>
```

b. Dump the contents of the source server to a directory with the following command, where *<dbname>* is the name of the source PostgreSQL server, and *<backup_name>* is the name of the backup file:

```
pg_dump <dbname> -O -F d -f <backup_name> -j 5 2>&1
```

c. Restore the dumped contents to the destination server with the following command, where *<admin:admin@[IP address of new PG]:port/dbname>* is the path to the destination PostgreSQL server, and *<backup_name>* is the name of the backup file you created in the previous step:

```
pg_restore -d postgresql://<admin:admin@[IP address of new PG]:port/dbname> -O -F d
<backup_name> -j 5 2>&1
```

The data on the source server is copied to the destination server.

5. Start Tenable Security Center with the following command:

```
# /bin/systemctl start SecurityCenter
```

Troubleshooting

This troubleshooting section covers some of the common issues encountered with Tenable Security Center.

- General Tenable Security Center Troubleshooting

- Tenable Log Correlation Engine Troubleshooting

- Tenable Nessus Troubleshooting

- Tenable Network Monitor Troubleshooting

- Troubleshooting Issues with the custom_CA.inc File

Tenable Security Center does not appear to be operational

1. If a login page does not appear, close and reopen the web browser.

2. Ensure that the remote `httpd` service is running on the Tenable Security Center host:

```
# ps ax | grep httpd
1990 ?          Ss      0:01 /opt/sc/support/bin/httpd -k start
```

3. Ensure that sufficient drive space exists on the Tenable Security Center 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
```

4. If there is not enough drive space, recover sufficient space and restart the Tenable Security Center service:

```
# 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  ]
#
```

Locked out of all Tenable Security Center user accounts

Contact Tenable Support.

Invalid license error

If you receive an invalid license error while attempting to log in as a security manager or lower organizational user, an administrator user 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`. Obtain a license from Tenable and copy it 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. The system only supports OpenJDK and Oracle JRE. The existence of another type of Java on the system will likely break reporting.

Tenable Log Correlation Engine Troubleshooting

Tenable Log Correlation Engine server does not appear to be operational

1. Confirm that the Tenable Log Correlation Engine server state is **Working** along with all attached Tenable Log Correlation Engine clients.

2. Check that you can SSH from the Tenable Security Center host to the Tenable Log Correlation Engine host.

3. Check that the Tenable Log Correlation Engine daemon is running on its host and listening on the configured port (TCP port 31300 by default):

```
# ss -pan | grep lced


tcp        0        0 0.0.0.0:31300   0.0.0.0:*      LISTEN      30339/lced
```

4. Check that the listening ports can be reached from the network and are not blocked by a firewall.

5. If the Tenable Log Correlation Engine server is not operational, attempt to start the service:

```
# service lce start


Starting Log Correlation EngineLCE Daemon Configuration
LICENSE: Tenable Log Correlation Engine 3-Silo Key for [user]
 EXPIRE: 11-10-2011
 REMAIN: 30 days
MESSAGE: LCE (3-silo license)
MESSAGE: Valid authorization
---------------------------------------------------------
                                                      [  OK  ]
```

No events from an attached Tenable Log Correlation Engineserver

1. Confirm that theTenable Log Correlation Engine server state is **Working** along with all attached Tenable Log Correlation Engine clients.

2. Confirm connectivity by checking that heartbeat events show up in the Tenable Security Center UI.

3. Check the Tenable Log Correlation Engine configuration settings in accordance with the Tenable Log Correlation Engine documentation.

4. Check the individual Tenable Log Correlation Engine client configuration and authorization. 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 Tenable Log Correlation Engine documentation.

5. Check for NTP time synchronization between the Tenable Security Center, Tenable Log Correlation Engine, and Tenable Log Correlation Engine clients.

Invalid Tenable Log Correlation Engine license

1. Check that an up-to-date license exists on the Tenable Log Correlation Engine server.

Tenable Log Correlation Engine plugins fail to update

1. 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.

2. Ensure that the Tenable Security Center host is allowed outbound HTTPS connectivity to the Tenable Log Correlation Engine Plugin Update Site.

3. For all other Tenable Log Correlation Engine plugin update issues, contact Tenable Support.

Tenable Nessus Troubleshooting

Tenable Nessus server does not appear to be operational

1. Verify that the Tenable Nessus scanner **Status** is **Unable to Connect**.

2. SSH to the remote Tenable Nessus host to make sure the underlying operating system is operational.

3. Confirm that the Tenable Nessus daemon is running (Linux example below):

```
# service nessusd status
nessusd (pid 3853) is running...
```

4. If the Tenable Nessus service is not running, start the service:

```
# 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 Tenable Nessus server

1. Make sure the Tenable Nessus daemon was registered using the Tenable Security Center option for registration.

2. Check connectivity from Tenable Security Center to the port the Tenable Nessus system is running on (e.g., 8834). For example, run:

```
curl -k https://<scannerIPaddress>:<port>
```

Tenable Nessus scans fail to complete

1. Ensure that the Tenable Nessus service is running on the Tenable Nessus host.

2. Ensure that Tenable Nessus scanner is listed in Tenable Security Center under **Resources** > **Nessus Scanners** and that the status of the Tenable Nessus scanner is listed as **Working**. For more information, see Tenable Nessus Scanner Statuses.

3. Click **Edit** to ensure that the IP address or hostname, port, username, password, and selected repositories for the Tenable Nessus scanner are all correct.

4. Edit any incorrect entries to their correct state.

5. Click **Submit** to attempt to reinitialize the Tenable Nessus scanning interface.

6. 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 address count that has reached the limit. Either remove a repository to free up IP addresses or obtain a license for more IP addresses.

7. Ensure that scan targets are permitted within the configured scan zones.

8. Ensure the Tenable Nessus scanner is running a supported Tenable Nessus version. For minimum Tenable Nessus scanner version requirements, see the Tenable Security Center Release Notes for your version.

Tenable Nessus plugins fail to update

1. Click **System > Configuration**.

   The **Configuration** page appears.

2. Click **License** and ensure that the Tenable Nessus Activation Code is marked as **Valid**.

3. Ensure the Tenable Nessus scanner is running a supported Tenable Nessus version. For minimum Tenable Nessus scanner version requirements, see the [Tenable Security Center Release Notes](#) for your version.

4. Ensure that the user used to connect to the Tenable Nessus server is a Tenable Nessus administrator.

5. Ensure that the Tenable Security Center system is allowed outbound HTTPS connectivity to the Tenable Nessus Plugin Update Site.

6. Under **System**, **Configuration**, and **Update** in Tenable Security Center, ensure that Active Plugins is not set to **Never**.

7. Manually test a plugin update under **Plugins** with **Update Plugins**.

   If successful, the line **Active Plugins Last Updated** updates to the current date and time.

8. For all other Tenable Nessus plugin update issues, contact Tenable Support.

Tenable Network Monitor Troubleshooting

Tenable Network Monitor server does not appear to be operational

1. Verify that the Tenable Network Monitor server appears as **Unable to Connect** under **Status**.

2. SSH to the remote Tenable Network Monitor host to make sure the underlying operating system is operational.

3. Confirm that the Tenable Network Monitor is running (Linux example below):

```
# service pvs status

NNM is stopped
NNM Proxy (pid 3142) is running
#
```

4. If the Tenable Network Monitor service is not running, start the service:

```
# service nnm start
```

```
Starting NNM Proxy                                              [   OK   ]
Starting NNM                                                    [   OK   ]
#
```

Cannot add a Tenable Network Monitor server

1. Confirm that the Tenable Network Monitor proxy is listening on the same port as Tenable Security Center (port 8835 by default):

   ```
   # ss -pan | grep 8835
   tcp       0      0 0.0.0.0:8835    0.0.0.0:*     LISTEN      406/pvs
   ```

2. Check connectivity by telnetting from the Tenable Security Center console into the Tenable Network Monitor server on port 8835 (the Tenable Network Monitor listening port). If successful, the response includes: Escape character is '^]'.

No vulnerabilities are being received from the Tenable Network Monitor server

1. Ensure that the Tenable Network Monitor service is running on the Tenable Network Monitor host.

2. Ensure that the Tenable Network Monitor appears in Tenable Security Center under **Resources** > **Tenable Network Monitors** and that the status of the Tenable Network Monitor appears as **Working**.

3. Click **Edit** to ensure that the IP address or hostname, port, username, password, and selected repositories for the Tenable Network Monitor are correct.

4. Edit any incorrect entries to their correct state.

5. Click **Submit** to attempt to reinitialize the Tenable Network Monitor scanning interface.

Tenable Network Monitor plugins fail to update

1. Manually test a plugin update under **Plugins** with **Update Plugins**.

   If successful, **Passive Plugins Last Updated** updates to the current date and time.

2. Ensure that the Tenable Security Center host allows outbound HTTPS connectivity to the Tenable Network Monitor Plugin Update Site.

3. For all other Tenable Network Monitor plugin update issues, contact Tenable Support.

Error Messages

For Tenable Security Center API status codes, see the Tenable Security Center API Guide.

> **Note:** Some errors are dependent on internal processes. If the error code you received is not listed, it may not indicate a specific Tenable Security Center error.

Scanning

For more information about creating, modifying, and launching scans, see Configure Scans.

For more information about statuses, see Tenable Nessus Scanner Statuses, Scan Result Statuses, and View Your Scan Zones.

Code	Message	Recommended Action
14	Progress handler has died.	Your system processes may be overloaded during the scan. Confirm your available system resources and re-run the scan.
14	Error creating Email notifying User '<*username*'> of Scan launch.	Do any of the following: • Confirm the alert specifies one or more valid email addresses. For more information, see Email. • Confirm the job queue database is not locked.
14	Error creating Email notifying User '<*username*>' of Scan completion.	Do any of the following: • Confirm the alert specifies one or more valid email addresses. For more information, see Email. • Confirm the job queue database is not locked.
60	Available Zones do not	For troubleshooting assistance, see the knowledge

Code	Message	Recommended Action
	cover any accessible Scan IPs for Scan job #*<jobIDorPID>* ('*<scanDefinitionName>*' - #*<scanDefinitionID>*).	base article.
62	No scanners ready to scan	The scan may be using incorrect or insufficient credentials, or another issue is blocking the scan. For troubleshooting assistance, see the knowledge base article.
64	Scan #*<scanDefinitionID>* is disabled.	You may have insufficient permissions to run the scan. For troubleshooting assistance, see the knowledge base article.
64	Scan Policy #*<scanPolicyID>* in Scan #*<scanDefinitionID>* is disabled.	You may have insufficient permissions to run the scan. For troubleshooting assistance, see the knowledge base article.
70	Unable to launch Scan progress process	Tenable Security Center is unable to fork the running scan process. You may need to raise the stack size for the `tns` user. Contact your system administrator for assistance.
102	Could not open '*<nessusFile>*' for writing.	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the knowledge base article.
106	Error getting contents of AuditFile '*<auditFileName>*' for Scan job #*<scanJobID>*.	Tenable Security Center cannot access the audit file definition. Do any of the following: • Verify the specified audit file is valid. • Create a new audit file to use with the scan. For more information, see Audit Files.

Code	Message	Recommended Action
106	Error creating temp SCAP directory '*<scapDir>*'.	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Error creating temp OVAL directory '*<ovalDir>*'.	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Error creating temp directory '*<tempDir>*'.	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Error untaring SCAP results file '*<file>*' (rc = $rc).	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Error moving *<type>* result file '*<curFile>*' to '*<newFile>*'.	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Unable to get current working directory.	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Failed to change to the SCAP directory for zipping.	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Error building SCAP results file '*<scapFile>*' (rc = *<zipReturnCode>*).	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Failed to change back to originating directory.	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Unable to get current	Tenable Security Center may have insufficient disk

Code	Message	Recommended Action
	working directory.	space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Failed to change to the OVAL directory for zipping.	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Error building OVAL results file '$ovalFile' (rc = $rc).	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	Failed to change back to originating directory.	Tenable Security Center may have insufficient disk space. Free up disk space in Tenable Security Center, as described in the [knowledge base](#) article.
106	No results file found for Scan job #*<jobIDorPID>* ('*<scanDefinitionName>*' - #*<scanDefinitionID>*).	Tenable Security Center cannot locate `/opt/sc/data/scans/#jobID/results.xml`. Verify the following: • `/opt/sc/data/scans/#jobID/results.xml` is in the correct directory. • The `tns` user can access the file and directory.
106	Error creating new VDB directory for Scan job #*<jobIDorPID>* ('*<scanDefinitionName>*' - #*<scanDefinitionID>*).	Verify the `tns` user can access the following directory: `/opt/sc/orgs/#orgID/VDB/#dateOfScan/`.
106	Error moving results for Scan job #*<jobIDorPID>* ('*<scanDefinitionName>*' - #*<scanDefinitionID>*).	Verify the `tns` user can access the following directory: `/opt/sc/orgs/#orgID/VDB/#dateOfScan/`.
145	Error reading AuditFile '' for	Add an audit file to the scan policy, then re-run the

Code	Message	Recommended Action
	Scan job #<scanJobID>. Unable to retrieve AuditFile #<auditFileID>"	scan. For more information, see [Audit Files](#) and [Scan Policies](#).
146	Unable to find template maps for Policy template #*policyTemplateID*.	Check for any errors with the last plugin update. If needed perform another plugin update. For more information, see [Offline Plugin and Feed Updates for Tenable Security Center](#).
146	Diagnostic target is outside IPs of original Scan.	The scan target is not included in the scan configuration. If you want to include the target in the scan, update the scan settings and then re-run the scan.
146	Diagnostic target is not a single host.	The target of the diagnostic scan must be a single IP or FQDN. Update the scan configuration, then re-run the scan.
146	Zone Selection is locked but no Zone is specified.	You may have insufficient permissions to run the scan, or you may need to adjust your scan configuration. For troubleshooting assistance, see the [knowledge base](#) article.
146	Zone Selection is selectable but no Zone is specified.	You may have insufficient permissions to run the scan, or you may need to adjust your scan configuration. For troubleshooting assistance, see the [knowledge base](#) article.
146	Entered IPs and Assets are empty.	One or more scan targets do not exist in the selected import repository. For troubleshooting assistance, see the [knowledge base](#) article.
146	Scan IPs are restricted.	You may have insufficient permissions to run the

Code	Message	Recommended Action
		scan, or you may need to adjust your scan configuration. For troubleshooting assistance, see the [knowledge base](#) article.
146	Scan IPs are not within your accessible range.	You may have insufficient permissions to run the scan, or you may need to adjust your scan configuration. For troubleshooting assistance, see the [knowledge base](#) article.
146	The number of Scan IPs is too large (more than 2^24 unique IPs).	Reduce the number of scan targets and re-run the scan.
147	Job #*\<scanJobID\>* not found.	Confirm the job queue database is not locked, then re-run the scan.
201	Error Setting up Scan database. *\<details\>*	Do any of the following, then re-run the scan: • Confirm you have adequate disk space • Confirm the `tns` user can access `/opt/sc/data/scans/#jobID/`
201	Error creating Scan database tables. *\<details\>*	Do any of the following, then re-run the scan: • Confirm you have adequate disk space • Confirm the `tns` user can access `/opt/sc/data/scans/#jobID/` • Confirm there are no corrupted databases
201	Error: Search for CVE failed. Postgres is not currently operational.	There was a problem communicating with the PostgreSQL server. To use global search when your Tenable Security Center has more than 100,000

Code	Message	Recommended Action
		assets, you must [connect an external PostgreSQL server](). If your Tenable Security Center has fewer than 100,000 assets, please open a case with Tenable Support.
202	*Error message varies.*	Your system processes may be overloaded during the scan. Confirm your available system resources and re-run the scan. If the error persists, contact your Tenable representative.
400	Scan job #*<scanJobID>* stopped due to scanner inactivity.	Your system processes may be overloaded during the scan. Confirm your available system resources and re-run the scan.
65536	Failed to resolve *<numFailed>* scan target hostnames in Scan #job #*<jobIDorPID>* ('*<scanDefinitionName>*' - #*<scanDefinitionID>*)."	Tenable Security Center cannot resolve the specified scan target hostnames. For troubleshooting assistance, see the [knowledge base]() article.
65536	Unable to scan *<numRestrictedTargets>* Restricted target<plural> in Scan job #*<jobIDorPID>* ('*<scanDefinitionName>*' - #*<scanDefinitionID>*).	You may have insufficient permissions to run the scan, or you may need to adjust your scan configuration. For troubleshooting assistance, see the [knowledge base]() article.
65536	Unable to scan *<numInaccessibleTargets>* target(s) outside your accessible ranges in Scan #job #*<jobIDorPID>* ('*<scanDefinitionName>*' - #*<scanDefinitionID>*).	You may have insufficient permissions to run the scan, or you may need to adjust your scan configuration. For troubleshooting assistance, see the [knowledge base]() article.

Code	Message	Recommended Action
65536	Usable Zones fail to cover *<unscannableCount>* accessible Scan IP*<plural>* for Scan job #*<jobIDorPID>* ('*<scanDefinitionName>*' - #*<scanDefinitionID>*).	You may have insufficient permissions to run the scan, or you may need to adjust your scan configuration. For troubleshooting assistance, see the [knowledge base](#) article.
65536	Available Zones do not cover accessible Scan IPs for Scan job #*<jobIDorPID>* ('*<scanDefinitionName>*' - #*<scanDefinitionID>*).	You may have insufficient permissions to run the scan, or you may need to adjust your scan configuration. For troubleshooting assistance, see the [knowledge base](#) article.