Tenable Vulnerability Management User Guide

Last Revised: August 29, 2025

Table of Contents

Welcome to Tenable Vulnerability Management

Tenable Vulnerability Management® (formerly known as Tenable.io) allows security and audit teams to share multiple Tenable Nessus, Tenable Agent, and Tenable Network Monitor scanners, scan schedules, scan policies, and scan results among an unlimited set of users or groups.

Note: Tenable Vulnerability Management can be purchased alone or as part of the Tenable One package. For more information, see Tenable One.

For additional information on Tenable Vulnerability Management, review the following customer education course:

- Tenable Vulnerability Management Introduction (Tenable University)

Tenable One Exposure Management Platform

Tenable One is an Exposure Management Platform to help organizations gain visibility across the modern attack surface, focus efforts to prevent likely attacks and accurately communicate cyber risk to support optimal business performance.

The platform combines the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps, and identity systems, builds on the speed and breadth of vulnerability coverage from Tenable Research, and adds comprehensive analytics to prioritize actions and communicate cyber risk. Tenable One allows organizations to:

- Gain comprehensive visibility across the modern attack surface
- Anticipate threats and prioritize efforts to prevent attacks
- Communicate cyber risk to make better decisions

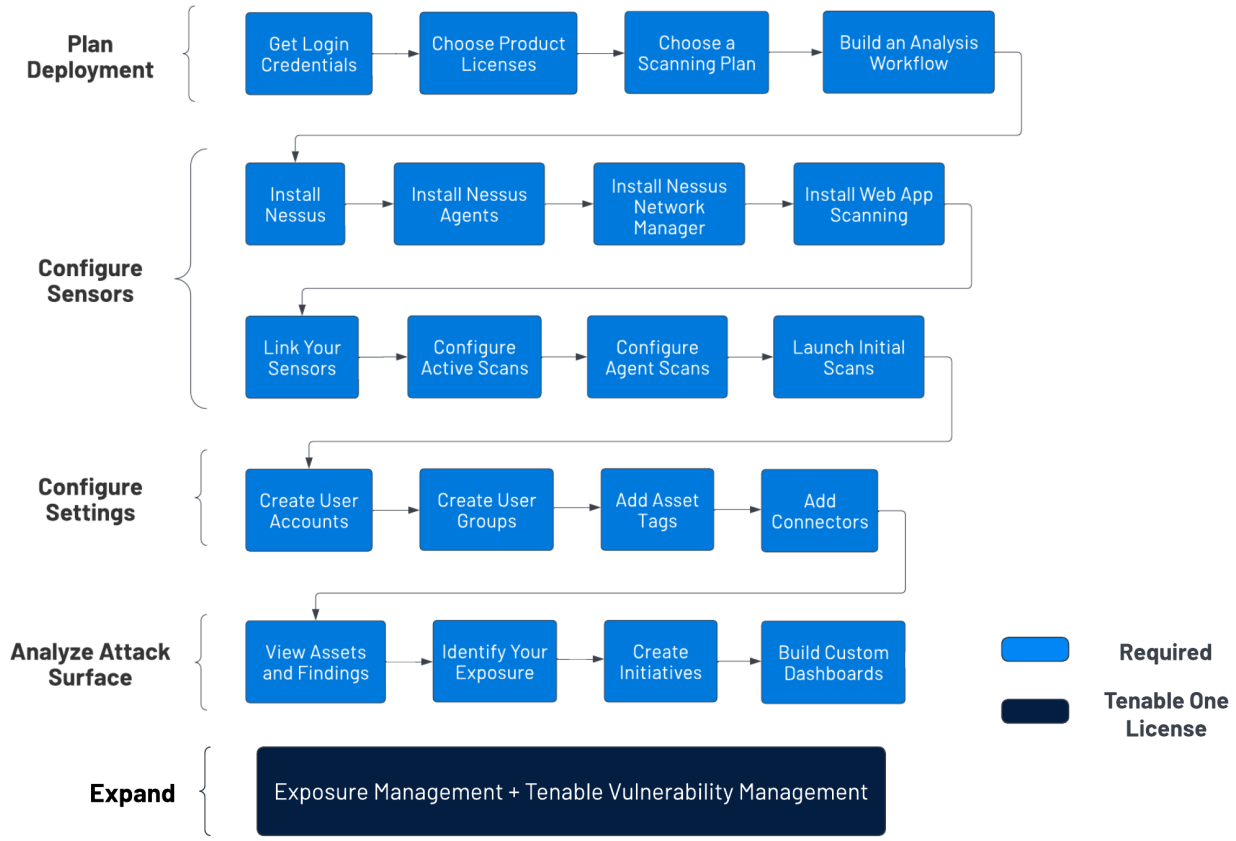
Tenable Vulnerability Management exists as a standalone product, or can be purchased as part of the Tenable One Exposure Management platform.

Tip: For additional information on getting started with Tenable One products, check out the Tenable One Deployment Guide.

Get Started with Tenable Vulnerability Management

This topic explains how to plan a Tenable Vulnerability Management deployment. It includes high-level guidance to build a deployment plan, configure scanners and application settings, start analyzing vulnerability data, and—when ready—expand into Tenable One.

Tip: Click a box to view the relevant task.



Plan Your Deployment

Establish a deployment plan:

1. Contact your Tenable representative and get your product access information and account credentials.
2. Analyze your network topology, considering Tenable-recommended best practices, as described in the General Requirements Guide.
3. Choose additional Tenable product licenses based on your organizational needs:

- If you want to assess your exposure, obtain a Tenable Lumin license.
- If you want to scan web applications, obtain a Tenable Web App Scanning license.
- If you want to evaluate risk on your containers, obtain a Tenable Container Security license.

4. Choose a scanning plan, including the scans to run, consulting the Professional Services Scan Strategy guide if needed.
5. Design an analysis workflow, identifying key stakeholders and considering what data you intend to share.

Install and Configure Sensors

To install and configure sensors:

1. Install the sensors chosen in your deployment plan:
   - Install Tenable Nessus as described in the *Tenable Nessus User Guide*.
   - Install Tenable Agents as described in the *Tenable Agent Deployment and User Guide*.
   - Install Tenable Network Monitor and then configure your installation as described in in the *Tenable Agent Deployment and User Guide*.
   - Install Tenable Core and Tenable Web App Scanning as described in the *Tenable Core User Guide*.
2. Link sensors to Tenable Vulnerability Management, as described in Link a Sensor.
3. Configure your first active scan using the **Basic Network Scan** template:
   a. Create a scanner group, as described in Create a Scanner Group.
   b. Create a scan using the **Basic Network Scan** template, as described in Create a Scan.
4. Configure your first agent scan using the **Basic Agent Scan** template:
   a. Create an agent group, as described in Create an Agent Group.
   b. Create an agent scan using the **Basic Agent Scan** template, as described in Create a Scan.
5. Launch your first Tenable Nessus scan and agent scan, as described in Launch a Scan.

6. Confirm that scans completed, accessing all targeted areas of your network. Review discovered assets.

Configure Application Settings

Configure other settings in Tenable Vulnerability Management:

1. Create user accounts for the users in your organization.
2. Create user groups to control user permissions for the resources in Tenable Vulnerability Management.
3. Add asset tags to organize and identify the assets to scan.
4. Set up asset discovery with connectors, Professional Services integrations, or integrated products (as described in the **Integration Guides** section of the Tenable Vulnerability Management Documentation page).
5. Configure managed credentials, scan-specific credentials, or policy-specific credentials for a Tenable Nessus scan, as described in Credentials. For more information about configuring and troubleshooting credentialed scans, see Tenable Nessus Credentialed Checks.
    a. Launch your credentialed Tenable Nessus scan and credentialed agent scan, as described in Launch a Scan.
    b. Confirm your credentialed scan completed, accessing all targeted areas of your network.

Analyze Your Attack Surface

Use the following features in Tenable Vulnerability Management to understand your vulnerabilities:

1. View your scans and scan details.
2. View scanned assets and vulnerabilities on the Findings and Assets workbenches.
3. With Vulnerability Intelligence, view known vulnerabilities by category and compare them to your own exposure.
4. With Exposure Response, create initiatives to track remediation projects.

5. With reports, share scan and vulnerability information with your organization.
6. Use custom dashboards to get visual overviews of your attack surface.

Expand into Tenable One

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

Integrate Tenable Vulnerability Management 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 VM 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 **Vulnerability Management** 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 Vulnerability Management Licenses

This topic breaks down the licensing process for Tenable Vulnerability Management as a standalone product. It also explains how assets are counted, lists add-on components you can purchase, explains how licenses are reclaimed, and notes plugins whose output is excluded from your license count.

Licensing Tenable Vulnerability Management

To use Tenable Vulnerability Management, you purchase licenses based on your organizational needs and environmental details. Tenable Vulnerability Management then assigns those licenses to your *assets*: assessed resources from the past 90 days, either identified on scans or imported with vulnerabilities (for example, servers, storage devices, network devices, virtual machines, or containers).

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.

Tip: To view your current license count and available assets, in the Tenable top navigation bar, click  and then click **License Information**. To learn more, see License Information Page.

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

How Assets Are Counted

When Tenable Vulnerability Management scans an asset, it compares it to previously discovered assets. In general, if the new asset does not match a previously discovered asset and has been assessed for vulnerabilities, it counts towards your license.

Tenable Vulnerability Management uses a complex algorithm to identify new assets without creating duplicates. The algorithm looks at the asset's BIOS UUID, MAC address, NetBIOS name, fully

qualified domain name (FQDN), and more. Authenticated scanners or agents also assign a Tenable UUID to each asset to mark it as unique. For more information, see the Tenable Vulnerability Management FAQ.

The following table describes when assets count towards your license.

Counted Towards Your License	Not Counted Towards Your License
• An asset identified by an active scan. • An asset identified by an agent scan. • An asset import containing vulnerabilities (for example, a scan result from Tenable Nessus Professional). • Host and Tenable Web App Scanning asset types, if the last licensed scan was within the past 90 days. • An asset identified by a scan with plugin debugging enabled. To prevent such assets from counting against your license, delete them.	• A scan configured with the Host Discovery template or configured to use only the discovery plugins. • An asset import containing no vulnerabilities (for example, ServiceNow data). • A linked instance of Tenable Network Monitor running in discovery mode. • A discovery-only connector, until and unless the asset is scanned for vulnerabilities Scanned Mobile Device Management assets. • Some plugin output, as described in Excluded Plugin Output.

Tenable Vulnerability Management Components

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

Included with Purchase	Add-on Component
• Unlimited Tenable Nessus scanners. • Unlimited Tenable Agents. • Unlimited Tenable Network Monitors with vulnerability detection.	• Tenable PCI ASV. • Tenable Attack Surface Management.

• Access to the Tenable Vulnerability Management API.	

Reclaiming Licenses

When you purchase licenses, your total license count is static for the length of your contract unless you purchase more licenses. However, Tenable Vulnerability Management reclaims licenses under some conditions—and then reassigns them to new assets so that you do not run out of licenses.

The following table explains how Tenable Vulnerability Management reclaims licenses.

Asset Type	License Reclamation Process
Deleted assets	Tenable Vulnerability Management removes deleted assets from the **Assets** workbench and reclaims their licenses within 24 hours.
Aged out assets	In **Settings** > **Sensors** > **Networks**, if you enable **Asset Age Out**, Tenable Vulnerability Management reclaims assets after they have not been scanned for a period you specify.
Assets from connectors	Tenable Vulnerability Management reclaims assets from connectors the day after they are terminated. You can observe this event in each connector.
All other assets	Tenable Vulnerability Management reclaims all other assets—such as those imported from other products or assets with no age-out setting—after they have not been scanned for 90 days.

Exceeding the License Limit

To allow for usage spikes due to hardware refreshes, sudden environment growth, or unanticipated threats, Tenable licenses are elastic. However, when you scan more assets than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages.

Scenario	Result
You scan more assets than are licensed for three consecutive days.	A message appears in Tenable Vulnerability Management.
You scan more assets than are	A message and warning about reduced functionality

licensed for 15+ days.	appears in Tenable Vulnerability Management.
You scan more assets than are licensed for 30+ days.	A message appears in Tenable Vulnerability Management; scan and export features are disabled.

Tip: Improper scan hygiene or product misconfigurations can cause scan overages, which result in inflated asset counts. To learn more, see Scan Best Practices.

Expired Licenses

The Tenable Vulnerability Management 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, you can no longer sign in to the Tenable platform.

Excluded Plugin Output

The plugins listed in this section do not count towards your license limit.

Note: Plugin IDs are static, but Tenable products may sometimes update plugin names. For the latest information on plugins, see Tenable Plugins.

Tenable Nessus Plugins in Discovery Settings

Configure the following Tenable Nessus plugins in Discovery Settings. These plugins do not count towards your license.

Tenable Nessus Plugin ID	Plugin Name
10180	Ping the remote host
10335	Nessus TCP scanner
11219	Nessus SYN scanner
14274	Nessus SNMP Scanner
14272	Netstat Portscanner (SSH)

34220	Netstat Portscanner (WMI)
34277	Nessus UDP Scanner

Tenable Nessus Plugins on the Plugins Page

Configure the following Tenable Nessus plugins on the **Plugins** page. These plugins do not count towards your license.

Tenable Nessus Plugin ID	Plugin Name
45590	Common Platform Enumeration (CPE)
54615	Device Type
12053	Host Fully Qualified Domain Name (FQDN)
11936	OS Identification
10287	Traceroute Information
22964	Service Detection
11933	Do not scan printers
87413	Host Tagging
19506	Nessus Scan Information
33812	Port scanners settings
33813	Port scanner dependency
209654	OS Fingerprints Detected
204872	Integration Status

Tenable Network Monitor Plugins

The following Tenable Network Monitor plugins do not count towards your license.

Tenable Network Monitor Plugin ID	Plugin Name

0	Open Ports
12	Host TTL discovered
18	Generic Protocol Detection
19	VLAN ID Detection
20	Generic IPv6 Tunnel Traffic Detection
113	VXLAN ID Detection
132	Host Attribute Enumeration

System Requirements

Display Settings

Minimum screen resolution: 1440 x 1024

Supported Browsers

Tenable Vulnerability Management supports the latest versions of the following browsers.

> **Note:** Before reporting issues with Tenable Vulnerability Management, ensure your browser is up to date.

- Google Chrome
- Apple Safari
- Mozilla Firefox
- Microsoft Edge

> **Note**: Tenable Vulnerability Management is not supported on mobile browsers.

Sensor Connection Requirements

Tenable Vulnerability Management requires access to specific addresses and ports for inbound and outbound traffic with Tenable Nessus scanners, Tenable Agents, and Tenable Sensor Proxy:

- 162.159.129.83/32
- 162.159.130.83/32
- 162.159.140.26/32
- 172.66.0.26/32
- 2606:4700:7::1a
- 2a06:98c1:58::1a
- 2606:4700:7::a29f:8153
- 2606:4700:7::a29f:8253
- *.cloud.tenable.com with the wildcard character (*) to allow cloud.tenable.com and all subdomains, such as sensor.cloud.tenable.com

Tip: For information about the port requirements for Tenable Security Center, Tenable Nessus scanners, and Tenable Agents, see the following topics:

- Tenable Security Center Port Requirements
- Tenable Nessus Port Requirements
- Tenable Agent Port Requirements

Log in to Tenable Vulnerability Management

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Note: If you bookmark a Tenable Vulnerability Management page within your browser, you must still log in before accessing the bookmarked page.
In some cases, you may also need to navigate through the Workspace page and navigate to the Tenable Vulnerability Management application before accessing the bookmarked page.

Before you begin:

- Obtain credentials for your Tenable Vulnerability Management user account.

  > **Note**: If you are an administrator logging in to your Tenable Vulnerability Management instance for the first time, Tenable provides your first-time credentials during setup. After you log in for the first time, you can set your new password. If you are logging in to Tenable Vulnerability Management after initial setup, your username is the email address you used to register for your Tenable Vulnerability Management account.

- Review the System Requirements in the *General Requirements User Guide* and confirm that your computer and browser meet the requirements.

> **Note:** If your account is configured to use SAML, you can log in to Tenable Vulnerability Management directly through your SAML provider. For more information, see SAML.

To log in to Tenable Vulnerability Management:

1. In a supported browser, navigate to https://cloud.tenable.com.

   The Tenable Vulnerability Management login page appears.

2. In the username box, type your Tenable Vulnerability Management username.

3. In the password box, type the Tenable Vulnerability Management password you created during registration.

4. (Optional) To retain your username for later sessions, select the **Remember Me** check box.

5. Click **Sign In**.

   The Workspace page appears.

   > **Note:**Tenable Vulnerability Management logs you out after a period of inactivity (typically, 30 minutes).

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 by Plugin** page), the metrics represent the highest value assigned or calculated

for a vulnerability associated with the plugin.

For Tenable Lumin-specific information about VPR and the other Tenable Lumin metrics, see Tenable Lumin Metrics.

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. CVSS scores power a vulnerability's **Severity** and **Risk Factor** values.

Note: If a vulnerability's related plugin has CVSS vectors, the **Risk Factor** is calculated based on the CVSSv2 vector and equates to the CVSSv2 score **Severity**. If a plugin does not have CVSS vectors, Tenable independently calculates the **Risk Factor**.

Tenable Vulnerability Management imports a CVSS score every time a scan sees a vulnerability.

CVSS-Based Severity

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 Configure Your Severity Metric.

Tenable Vulnerability Management analysis pages provide summary information about vulnerabilities using the following CVSS categories. For more information about the icons used for each severity, see Vulnerability Severity Indicators.

Severity	CVSSv2 Range	CVSSv3 Range	CVSSv4 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.	The plugin's highest vulnerability CVSSv4 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.	The plugin's highest vulnerability CVSSv4 score is between 7.0 and 8.9.
Medium	The plugin's highest	The plugin's highest	The plugin's highest

	vulnerability CVSSv2 score is between 4.0 and 6.9.	vulnerability CVSSv3 score is between 4.0 and 6.9.	vulnerability CVSSv4 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.	The plugin's highest vulnerability CVSSv4 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.	The plugin's highest vulnerability CVSSv3 score is 0. - or - The plugin does not search for vulnerabilities.

CVSS-Based Risk Factor

For each plugin, Tenable interprets CVSS scores for the vulnerabilities associated with the plugin and assigns an overall risk factor (**Low**, **Medium**, **High**, or **Critical**) to the plugin. The **Vulnerability Details** page shows the highest risk factor value for all the plugins associated with a vulnerability.

Note: Detection (non-vulnerability) plugins and some automated vulnerability plugins do not receive CVSS scores. In these cases, Tenable determines the risk factor based on vendor advisories.

Tip: **Info** plugins receive a risk factor of **None**. Other plugins without associated CVSS scores receive a custom risk factor based on information provided in related security advisories.

Vulnerability Priority Rating

Video: Vulnerability Priority Rating in Tenable Vulnerability Management

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 Vulnerability Management provides a VPR value the first time you scan a vulnerability on your network. Then, Tenable Vulnerability Management automatically provides new and updated VPR values daily.

Tenable recommends resolving vulnerabilities with the highest VPRs first. You can view VPR scores and summary data in:

- The Tenable-provided Vulnerability Management Overview dashboard
- The Explore Findings page
- The Vulnerabilities by Plugin page

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
Age of Vuln	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 Vulnerability Management 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 Severity Indicators

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 Configure Your Severity Metric.

The Tenable Vulnerability Management interface uses different icons for each severity category and accepted or recasted status.

Icon	Category	And
	Critical	You have not accepted or recasted the risk.
		You accepted the risk.
		You recasted the severity to **Critical**.
	High	You have not accepted or recasted the risk.
		You accepted the risk.
		You recasted the severity to **High**.
	Medium	You have not accepted or recasted the risk.
		You accepted the risk.
		You recasted the severity to **Medium**.
	Low	You have not accepted or recasted the risk.
		You accepted the risk.
		You recasted the severity to **Low**.
	Info	You have not accepted or recasted the risk.
		You accepted the risk.
		You recasted the severity to **Info**.

Vulnerability Mitigation

Tenable Vulnerability Management vulnerabilities exist in one of two categories: **Active** or **Fixed**. When Tenable Vulnerability Management discovers a vulnerability on an asset, the vulnerability remains in the **Active** category until it is mitigated or fixed. Then, the vulnerability moves to the **Fixed** category.

Active Vulnerabilities

Active vulnerabilities are any vulnerabilities in the **New**, **Active**, or **Resurfaced** states. For more information, see Vulnerability States.

Fixed Vulnerabilities

The **Fixed** category contains vulnerabilities that Tenable Vulnerability Management determines are not vulnerable, based on the scan definition, the results of the scan, and authentication information. To be considered for mitigation, a vulnerability must be active and successfully authenticated.

A vulnerability is mitigated when:

- The vulnerability's IP address or another combination of identifying attributes (IAs) is on the scan's target list. For more information on IAs, see the Tenable Community.
- The vulnerability's plugin ID is listed in the scan policy.
- The vulnerability's port is on the list of scanned port ranges, and the remote port is found open.
- A vulnerability with that combination of IP address, port, protocol, and plugin ID is not listed in the scan results.

Mitigation Exceptions

Note the following exceptions for vulnerability mitigation:

- Vulnerabilities identified during a thorough scan by a plugin with the **thorough_tests** attribute can only be mitigated by another thorough scan.
- Vulnerabilities identified during a paranoid scan by a plugin with the **requires_paranoid_scanning** attribute can only be mitigated by another paranoid scan.

- Vulnerabilities discovered by a local or combined plugin reported on port 0 or 445 via a credential scan can only be mitigated by another credential scan.
- The list of scanned ports can be expanded to “all” ports when one of the following plugins triggered the host:14272 (SSH netstat), 34220 (WMI netstat), 14274 (SNMP).
- Agent scans cannot mitigate vulnerabilities discovered by a combined type plugin reported on a remote port (not 0/445).

Vulnerability States

Tenable assigns a *state* to vulnerabilities detected on your network. You can track and filter by vulnerability state to see the detection, resolution, and reappearance of vulnerabilities over time. To filter for vulnerabilities by their state, use the **Findings** workbench.

Vulnerability State	Description
New	Indicates that Tenable Vulnerability Management detected the vulnerability once.
Active	Indicates that Tenable Vulnerability Management detected the vulnerability more than once. **Note:** When you filter for **Active** vulnerabilities, Tenable Vulnerability Management also returns **New** vulnerabilities. For filtering purposes, **New** is a subcategory of **Active**.
Fixed	Indicates that Tenable Vulnerability Management detected the vulnerability on a host, but no longer detects it. **Note**: To view **Fixed** vulnerabilities by date range, use the **Last Fixed** filter.
Resurfaced	Indicates that Tenable Vulnerability Management previously marked the vulnerability as **Fixed**, but has detected it again. When a vulnerability is **Resurfaced**, it remains in this state until a scan identifies the vulnerability as remediated. Then, the vulnerability returns to **Fixed**.

Note: The API uses different terms for vulnerability states than the user interface. In the API, the new and active states are both labeled as open. The resurfaced state is labeled as reopened. The fixed state is the same.

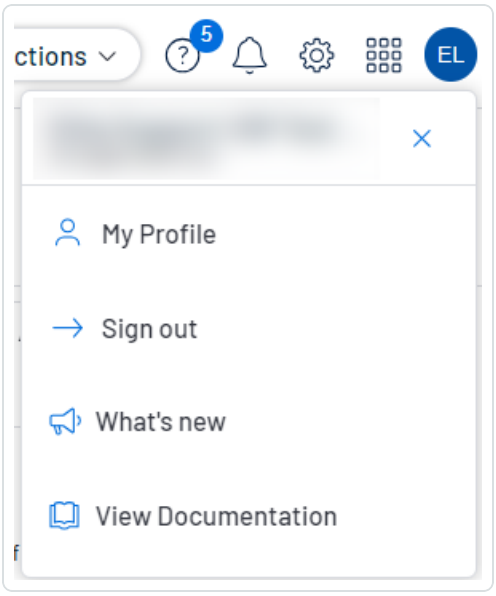
Log Out of Tenable Vulnerability Management

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

To log out of Tenable Vulnerability Management:

1. In the upper-right corner, click the blue user circle.

   The user account menu appears.



2. Click **Sign Out**.

Navigate Tenable Vulnerability Management

Tenable Vulnerability Management includes several helpful shortcuts and tools that highlight important information and help you to navigate the user interface more efficiently:

Quick Actions Menu

The quick actions menu displays a list of the most commonly performed actions.

To access the quick actions menu:

1. In the upper-right corner, click the ☆ **Quick Actions** button.

   The quick actions menu appears.

2. Click a link to begin one of the listed actions.

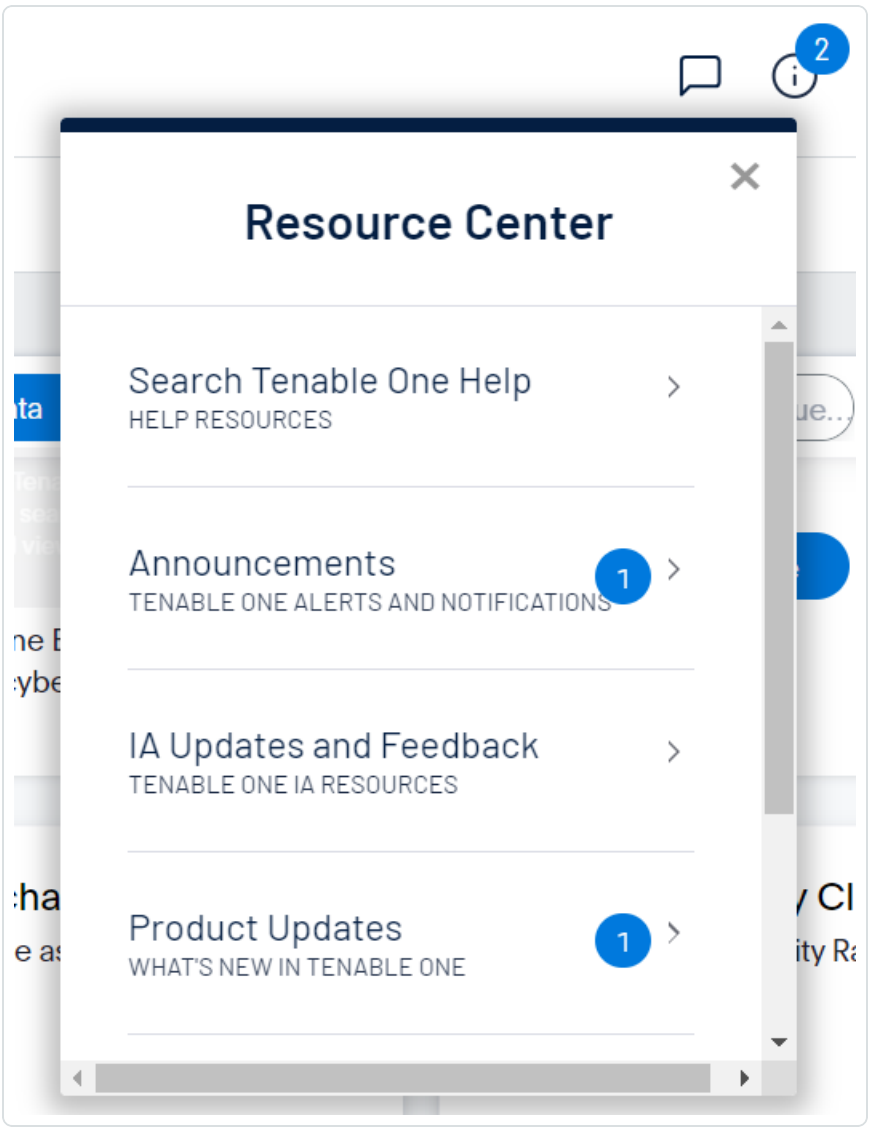
Resource Center

The **Resource Center** displays a list of informational resources including product announcements, Tenable blog posts, and user guide documentation.

To access the Resource Center:

1. In the upper-right corner, click the ⓘ button.

   The **Resource Center** menu appears.



2. Click a resource link to navigate to that resource.

Notifications

In Tenable Vulnerability Management, the **Notifications** panel displays a list of system notifications. The 🔔 button shows the current number of unseen notifications. When you open the **Notifications** panel, Tenable Vulnerability Management marks those notifications as seen. Once you have seen a notification, you can clear it to remove it from the **Notifications** panel.

> **Note:** Tenable Vulnerability Management groups similar notifications together.

To view notifications:

- In the upper-right corner, click the button.

  The **Notifications** panel appears and displays a list of system notifications.

  In the **Notifications** panel, you can do the following:

  - To clear one notification, next to the notification, click the button.
  - To expand a group of notifications, at the bottom of the grouped notification, click **More Notifications**.
  - To collapse an expanded group of notifications, at the top of the expanded notifications, click **Show Less**.
  - To clear an expanded group of notifications, at the top of the expanded notifications, click **Clear Group**.
  - To clear all notifications, at the bottom of the panel, click **Clear All**.

Settings

Click the button to navigate directly to the **Settings** page, where you can configure your system settings.

> **Note:** For more information, see Settings within the *Tenable Vulnerability Management User Guide*.

Workspace

When you log in to Tenable, the **Workspace** page appears by default. On the **Workspace** page, you can switch between your Tenable applications or set a default application to skip the **Workspace** page in the future. You can also switch between your applications from the **Workspace** menu, which appears in the top navigation bar.

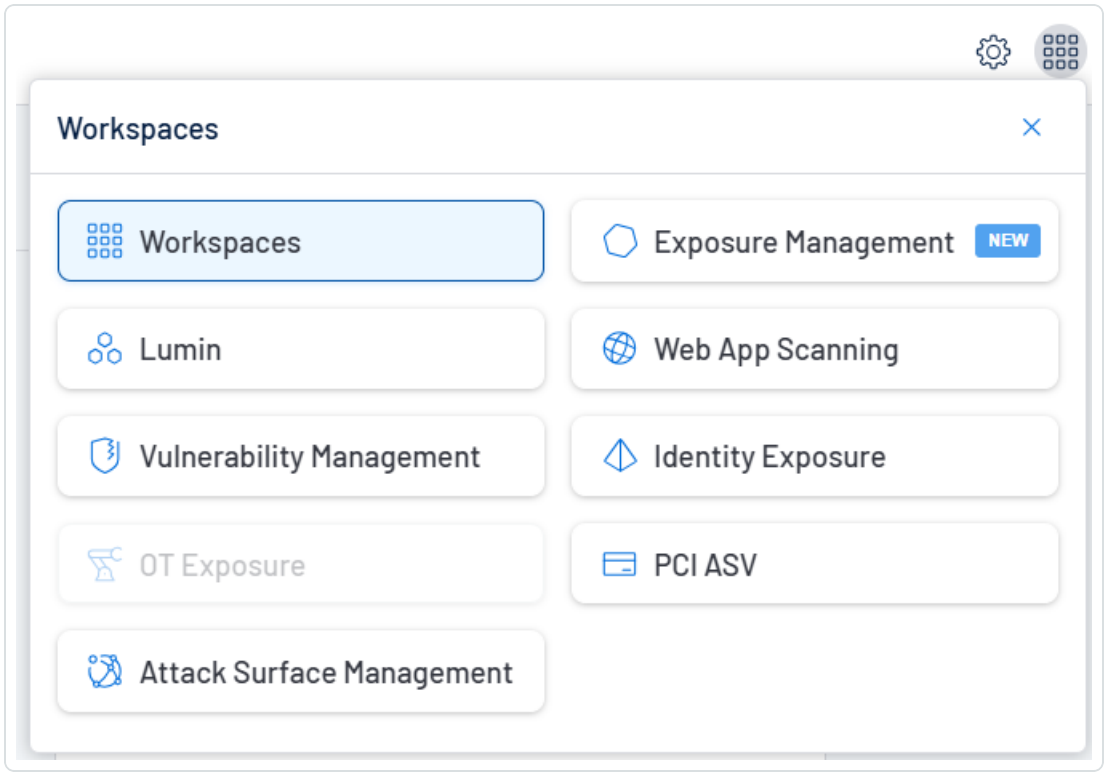
> **Important:** Tenable disables application tiles for expired applications. Tenable removes expired application tiles from the **Workspace** page and menu 30 days after expiration.

Open the Workspace Menu

To open the **Workspace** menu:

1. From any Tenable application, in the upper-right corner, click the button.

   The **Workspace** menu appears.



2. Click an application tile to open it.

View the Workspace Page

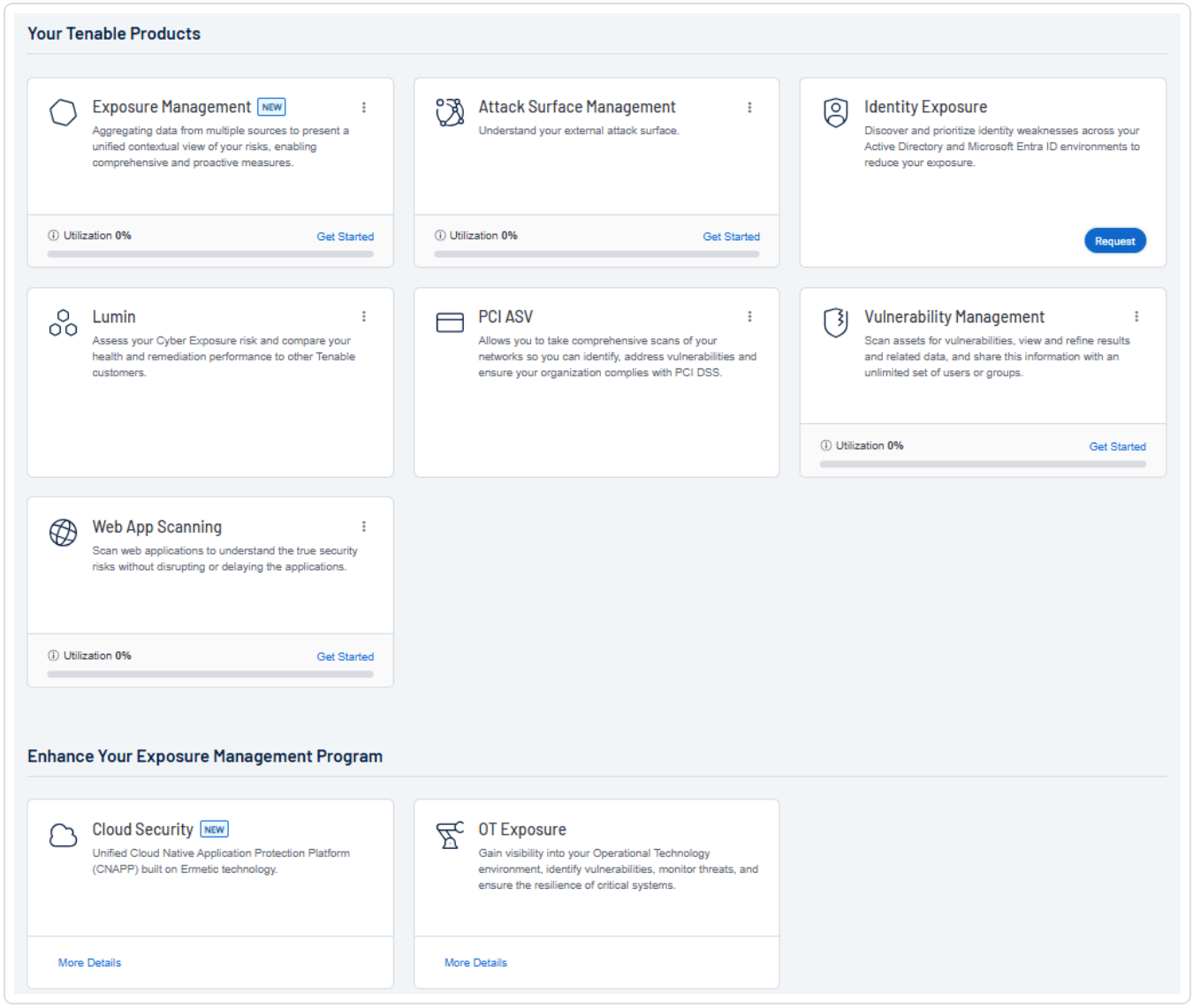
To view the Workspace page:

1. From any Tenable application, in the upper-right corner, click the button.

   The **Workspace** menu appears.

2. In the **Workspace** menu, click **Workspaces**.

The **Workspace** page appears.



On the **Workspace** page, you can do the following:

- Where applicable, at the bottom of a tile, view the percentage of your license utilization for the application. Click **See More** to navigate directly to the **License Information** page for the selected application.

  Tip: For more information on how Tenable licenses work and how assets or resources are licensed in each product, see Licensing Tenable Products.

- Set a default application:

When you log in to Tenable, the **Workspace** page appears by default. However, you can set a default application to skip the **Workspace** page in the future.

> By default, users with the **Administrator**, **Scan Manager**, **Scan Operator**, **Standard**, and **Basic** roles can set a default application. If you have another role, contact your administrator and request the **Manage** permission under **My Account**. For more information, see Custom Roles.

To set a default login application:

1. In the top-right corner of the application to choose, click the ⋮ button.

   A menu appears.

2. In the menu, click **Make Default Login Page**.

   This application now appears when you log in.

- Remove a Default Application:

To remove a default login application:

1. In the top-right corner of the application to remove, click the ⋮ button.

   A menu appears.

2. Click **Remove Default Login Page**.

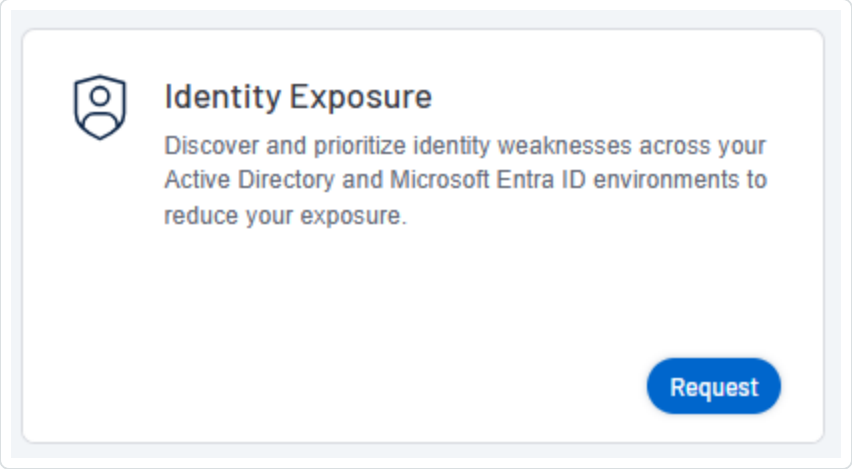
   The **Workspace** page now appears when you log in.

- Request Access to a Tenable application:

Some applications, like Tenable Identity Exposure, require you to request access to the application. You can do this directly via the **Workspace** page.

To request access to a Tenable application:

1. In the lower-right corner of the tile, click **Request**.



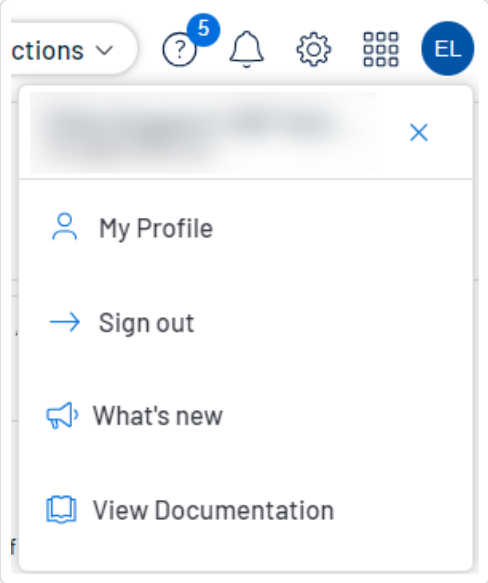
You navigate directly to the request page for the selected application.

User Account Menu

The user account menu provides several quick actions for your user account.

1. In the upper-right corner, click the blue user circle.

   The user account menu appears.



2. Do one of the following:

    - Click **My Profile** to configure your own user account. You navigate directly to the **My Account** settings page. See My Account for more information.
    - Click **Sign out** to sign out of Tenable Vulnerability Management.
    - Click **What's new** to navigate directly to the Tenable Vulnerability Management Release Notes.
    - Click **View Documentation** to navigate directly to the Tenable Vulnerability Management User Guide documentation.

For additional information about navigating the Tenable Vulnerability Management interface, see the following topics:

My Account

Breadcrumbs

Planes

Tables

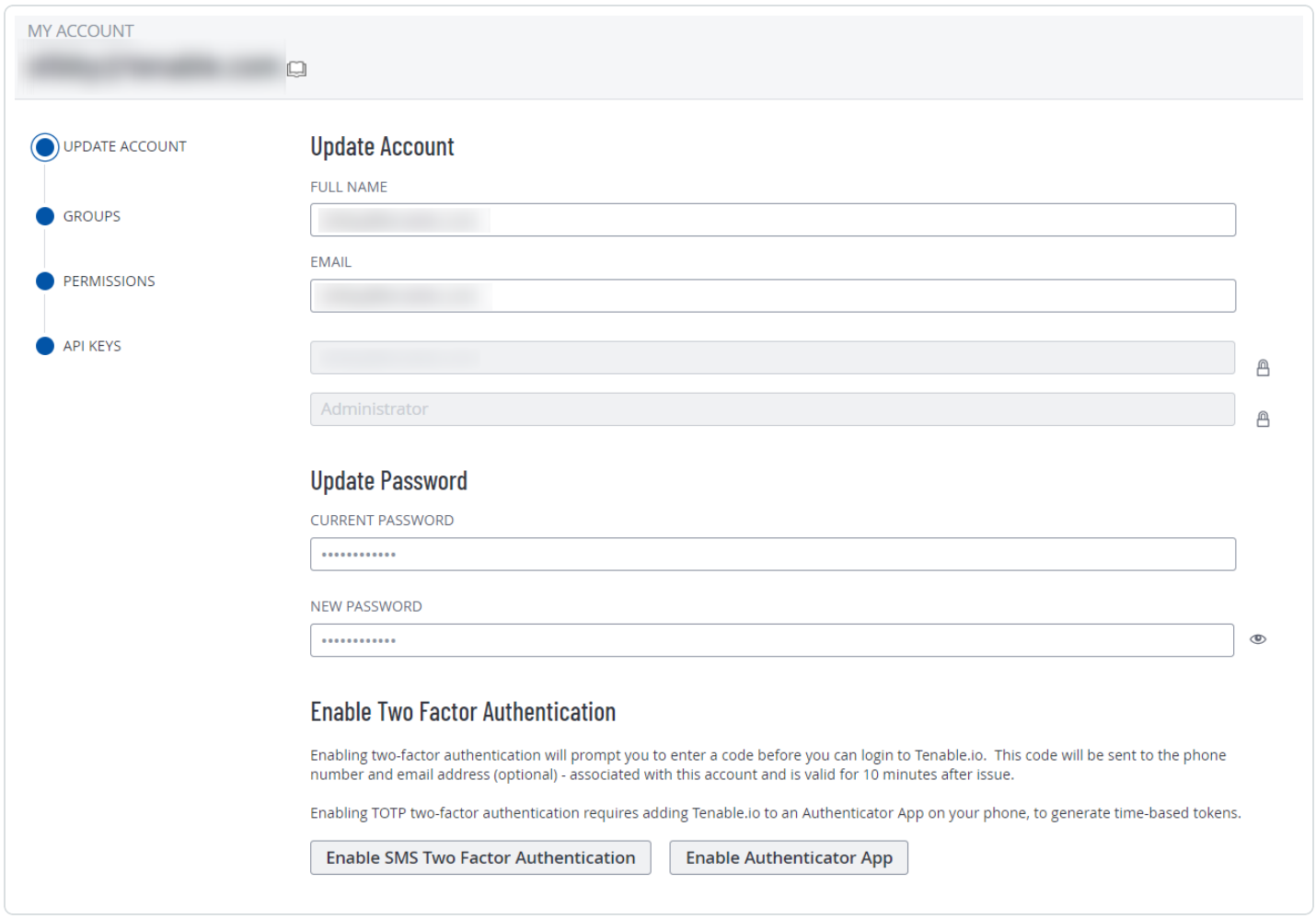
Query Builder

Saved Queries

Export Findings or Assets

My Account

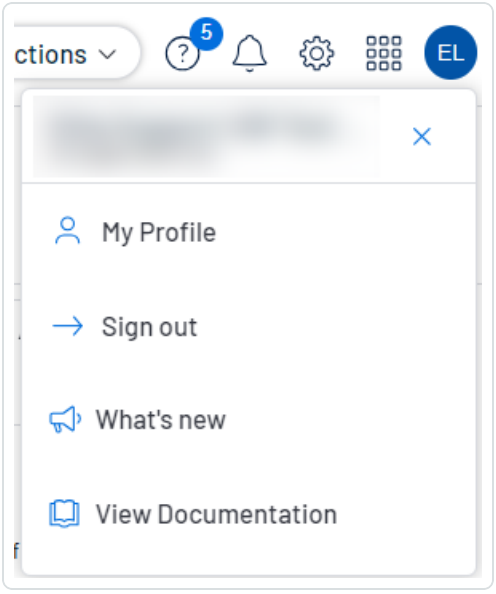
From the **My Account** page, you can make changes to your own user account.



To access the **My Account** page:

1. In the upper-right corner, click the blue user circle.

   The user account menu appears.



2. Click **My Profile**.

   The **My Account** page appears.

View Your Account Details

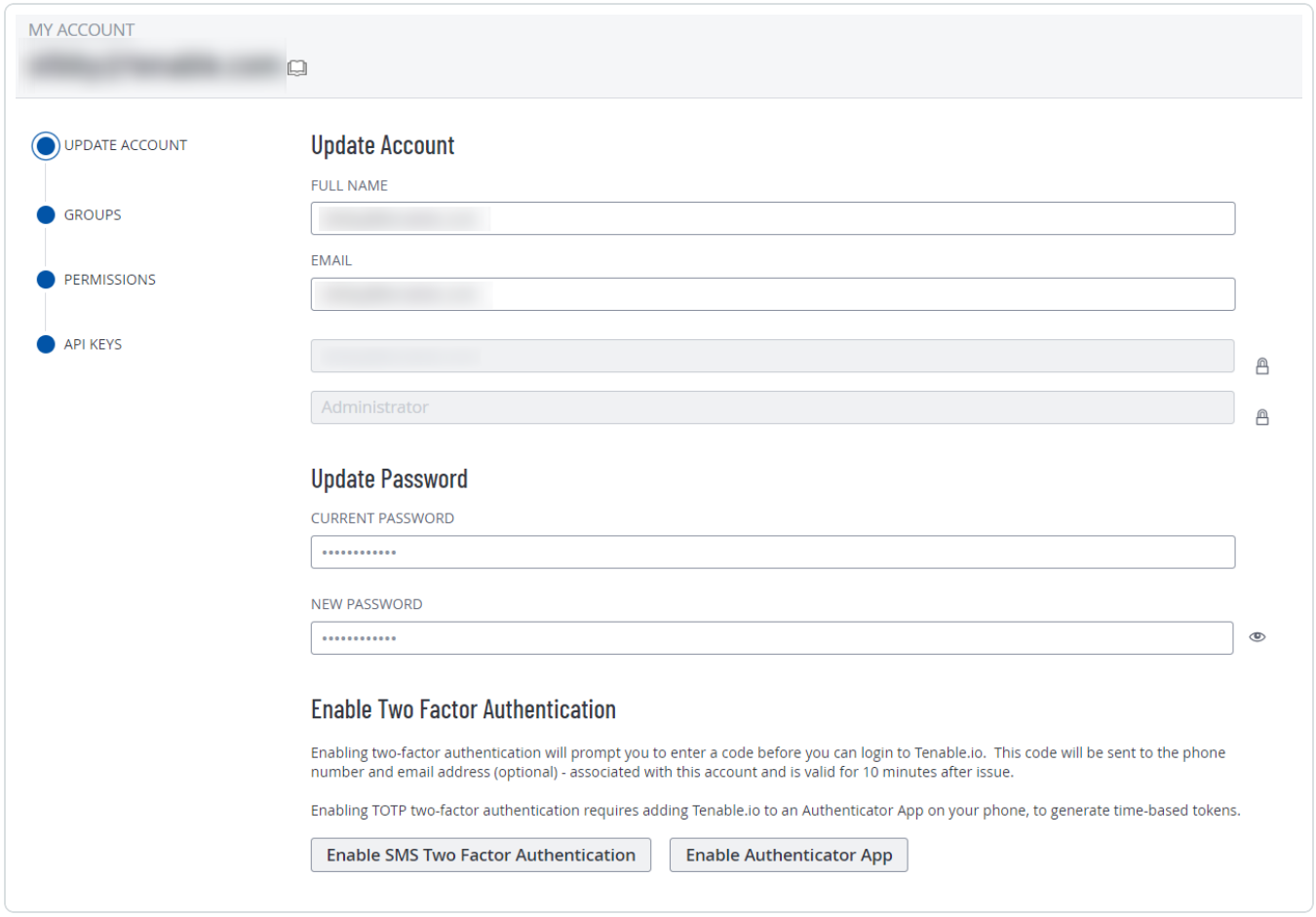
Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **My Account** page, you can view details about your account, including your log in details, user role, and the groups and permissions assigned to you.

To view your account details:

1. Access the My Account page.



2. On the left side of the page, you can select from the following:

Option	Action
Update Account	• Click **Update Account**. The **Update Account** section appears, showing the following details for your account: ◦ **Full Name** ◦ **Email** ◦ **Username** ◦ **Role**

	• (Optional) Update your basic account information, including name and email address. **Note**: You cannot change your username or role. • (Optional) Change your password. • (Optional) Configure or disable two-factor authentication on your account. • (Optional) Enable or disable Explore beta features on your account.

Groups	• Click **Groups**.
	
	Note: You cannot change your groups settings on the **My Accounts** page. For more information, see User Groups.
	
	• In the **Groups** table, view:
	  ◦ The user groups you are assigned to.
	  ◦ The number of members in each user group.

Permissions	• Click **Permissions**.
	
	Note: Permissions, when applied a user, allow that user to perform certain actions to specified asset tags (i.e., objects) and the assets to which those objects apply. Permissions can be applied to individual users or to all members of a user group. For more information, see Permissions.
	
	Note: You cannot change your permissions settings on the **My Accounts** page.
	
	• In the **Permissions** table, view:
	  ◦ The names of the permissions assigned to your account.
	  ◦ The actions those permissions allow you to perform.

	◦ The objects each permission applies to.
API Keys	• Click **API Keys**. • View a description of API keys. • Generate API Keys. **Caution:** Any existing API keys are replaced when you click the **Generate** button. You must update the applications where the previous API keys were used. **Caution**: Be sure to copy the access and secret keys before you close the **API Keys** tab. After you close this tab, you cannot retrieve the keys from Tenable Vulnerability Management.

Note: User accounts expire according to when the Tenable Vulnerability Management container they belong to was created. Tenable controls this setting directly. For more information, contact Tenable Support.

Update Your Account

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

To update your account:

1. Access the My Account page.
2. (Optional) Edit your **Name**.
3. (Optional) Edit your **Email**.

   A valid email address must be in the format:

   name@domain

where *domain* corresponds to a domain approved for your Tenable Vulnerability Management instance.

This email address overrides the email address set as your **Username**. If you leave this option empty, Tenable Vulnerability Management uses the **Username** value as your email address.

> **Note:** During initial setup, Tenable configures approved domains for your Tenable Vulnerability Management instance. To add domains to your instance, contact Tenable Support.

4. Click **Save**.

   Tenable Vulnerability Management saves the changes to the account.

5. (Optional) Change your password.
6. (Optional) Configure two-factor authentication.
7. (Optional) Generate an API key.

Change Your Password

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

> **Required Tenable Web App Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can change the password for your own account as any type of user. The method of changing your password varies slightly based on the role assigned to your user account.

To change another user's password, see Change Another User's Password.

To change your password:

1. Access the My Account page.
2. In the **Current Password** box, type your current password.
3. In the **New Password** box, type a new password. See Tenable Vulnerability Management Password Requirements for more information.
4. Click the **Save** button.

Tenable Vulnerability Management saves the new password and terminates any currently active sessions for your account. Tenable Vulnerability Management then prompts you to re-authenticate.

5. Log in to Tenable Vulnerability Management using your new password.

Configure Two-Factor Authentication

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **My Account** page, you can configure two-factor authentication for your account.

Tip: Administrators can also enforce two-factor authentication for other accounts when creating or editing a user account.

Note: Before configuring two-factor authentication, check the International Phone Availability list to ensure you are able to receive text messages from Tenable Vulnerability Management.

To add or modify two-factor authentication:

1. Access the My Account page.
2. In the **Enable Two Factor Authentication** section, do one of the following:
   - To enable SMS two factor authentication:
     a. Click **Enable SMS Two Factor Authentication**.

        The **Two-Factor Setup** plane appears.

     b. In the **Current Password** box, type your Tenable Vulnerability Management password.

     c. In the **Phone Number** box, type your mobile phone number.

> **Note:** By default, Tenable Vulnerability Management treats mobile numbers as U.S. numbers and prepends the +1 country code. If your mobile phone number is a non-U.S. number, be sure to prepend the appropriate country code.

d. Click **Next**.

   The **Verification Code** plane appears and Tenable Vulnerability Management sends a text message with a verification code to the phone number.

e. In the **Verification Code** box, type the verification code you received.

f. Click **Next**.

   A **Two-Factor Setup Successful** message appears and Tenable Vulnerability Management applies your settings to your Tenable Vulnerability Management account.

g. (Optional) To configure whether Tenable Vulnerability Management sends a verification code to the email associated with your user account:

   a. Select or clear the **Send backup email** check box.

   b. Click **Update**.

      Tenable Vulnerability Management updates your backup email settings.

> **Note:** Once you save the phone number for this configuration, you cannot edit or change the phone number. You must configure a new authentication setup for any additional phone numbers you want to use.

- To enable authenticator application based authentication:

  a. Click **Enable Authenticator App**.

     The **Two-Factor Setup** plane appears.

  b. In the **Current Password** box, type your Tenable Vulnerability Management password.

  c. Click **Next**.

     The **Time-based One-Time Password** plane appears.

d. In the authenticator application of your choice, scan the QR code.

   In the authenticator application, a Tenable Vulnerability Management verification code appears.

e. In the **Verification Code** box, type the code provided by your authenticator application.

   > **Note:** If you do not type the correct verification code, Tenable Vulnerability Management locks the QR code. Delete the setup from your authenticator application and scan a new QR code.

f. Click **Next**.

   A **Two-Factor Setup Successful** message appears and Tenable Vulnerability Management applies your settings to your Tenable Vulnerability Management account.

To disable two-factor authentication in the new interface:

1. Do one of the following:

   - In the upper-left corner, click the ☰ button.

     The left navigation plane appears.

     a. In the left navigation plane, click **Settings**.

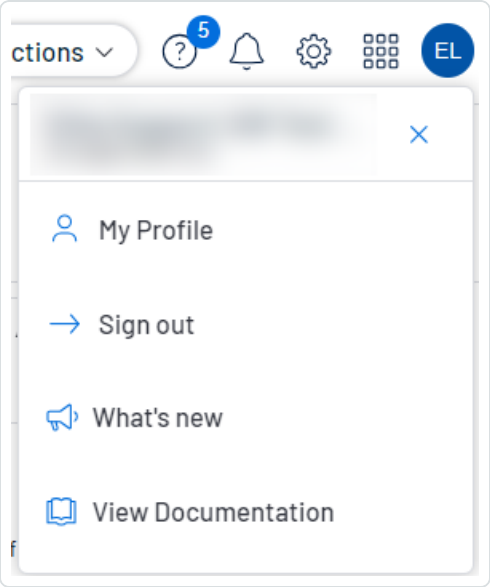
        The **Settings** page appears.

     b. Click the **My Account** tile.

        The **My Account** page appears, where you can view and update your account details.

   - In the upper-right corner, click the blue user circle.

     The user account menu appears.



a. Click **My Profile**.

   The **My Account** page appears.

2. In the **Change Password** section, in the **Current Password** box, type your current password.
3. In the **Enable Two Factor Authentication** section, click **Disable**.

   A **Disable Two-Factor** confirmation message appears.
4. Read the warning message, then click **Continue**.

   Tenable Vulnerability Management disables two-factor authentication for your account.

Generate API Keys

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

The API keys associated with your user account enable you to access the API for all Tenable Vulnerability Management products for which your organization is licensed.

Note: Tenable Vulnerability Management API access and secret keys are required to authenticate with the Tenable Vulnerability Management API.

Note: The API keys associated with your user account enable you to access the API for all Tenable Vulnerability Management products for which your organization is licensed. You cannot set separate keys for individual products. For example, if you generate API keys in Tenable Vulnerability Management, this action also changes the API keys for Tenable Web App Scanning and Tenable Container Security.

Note: Be sure to use one API key per application. Examples include, but are not limited to:

- Tenable Vulnerability Management integration
- Third-party integration
- Other custom applications, including those from Tenable Professional Services

The method to generate API keys varies depending on the role assigned to your user account. Administrators can generate API keys for any user account. For more information, see Generate Another User's API Keys. Other roles can generate API keys for their own account.

To generate API keys for your own account:

1. Access the My Account page.
2. Click the **API Keys** tab.

   The **API Keys** section appears.
3. Click **Generate**.

   The **Generate API Keys** window appears with a warning.

   Caution: Any existing API keys are replaced when you click the **Generate** button. You must update the applications where the previous API keys were used.
4. Review the warning and click **Generate**.

   Tenable Vulnerability Management generates new access and secret keys, and displays the new keys in the **Custom API Keys** section of the page.

   Tip: If the **Generate** button is inactive, contact your administrator to ensure they've enabled API access for your account. For more information, see Edit a User Account.
5. Copy the new access and secret keys to a safe location.

Caution: Be sure to copy the access and secret keys before you close the **API Keys** tab. After you close this tab, you cannot retrieve the keys from Tenable Vulnerability Management.

Unlock Your Account

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable Vulnerability Management locks you out if you attempt to log in and fail 5 consecutive times.

Note: If you no longer have access to the email address specified in your account, an administrator for your Tenable Vulnerability Management instance can reset your password instead. If you are unsure which email address to use, contact your Tenable representative.

Note: A user can be locked out of the user interface but still submit API requests if they are assigned the appropriate authorizations (api_permitted). For more information, see the Tenable Developer Portal.

To unlock your account:

1. On the Tenable Vulnerability Management login page, click the **Forgot your password?** link.

   The password reset page appears.

2. In the **Username** box, enter your Tenable Vulnerability Management username.

3. Where applicable, respond to the CAPTCHA security challenge.

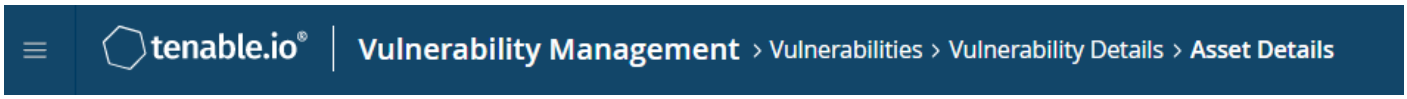
4. Click **Send**.

   Tenable Vulnerability Management sends password recovery instructions to the email address specified in your user account.

5. Reset your password using the instructions in the email message. See Password Requirements for more information.

Breadcrumbs

In the Tenable Vulnerability Management interface, certain pages display breadcrumbs in the top navigation bar. From left to right, the breadcrumbs show the path of pages you visited to reach your current page:



To navigate breadcrumbs:

- In the top navigation bar, click a link in the breadcrumb trail to return to a previous page.

Planes

Tenable Vulnerability Management combines fixed pages with overlapping planes.

To navigate planes in the new interface:

1. Access a plane using one of the following methods:
   - Click a widget on a dashboard.
   - Use the left navigation plane as follows:
     a. In the upper-left corner, click the ☰ button.

        The left navigation plane appears.

     b. In the left navigation plane, click a menu option.

   With the exception of the left navigation plane, planes open from the right side of the screen.
2. Manipulate a plane using the following buttons at the left edge of the plane:

Button	Short Name	Action
⛶	expand	Expand a plane. Some planes can expand to full screen.
⛶	retract	Retract an expanded plane to its default size.
✕	close	Close a plane.
←	expand preview	Expand a preview plane.

→	retract preview	Retract an expanded plane to the preview plane.

3. Return to a previous plane or page (and close a new plane or planes) by clicking the previous plane.

Tables

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable Vulnerability Management Workbench Tables

Tenable Vulnerability Management Workbench tables are any tables in the Tenable Vulnerability Management interface outside of the **Explore** section. These tables feature search and navigational capabilities. They also include the ability to drag and drop columns in any order, change column width, and sort the data in multiple columns at one time. For more information, see Tenable Vulnerability Management Workbench Tables.

Explore Tables

Explore tables are any tables within the **Explore** section in the Tenable Vulnerability Management user interface. They include many of the features of Tenable Vulnerability Management Workbench tables, but include additional customization and filtering capabilities. For more information, see Explore Tables.

Use Tables

In Tenable Vulnerability Management, you can use and interact with tables in the following ways:

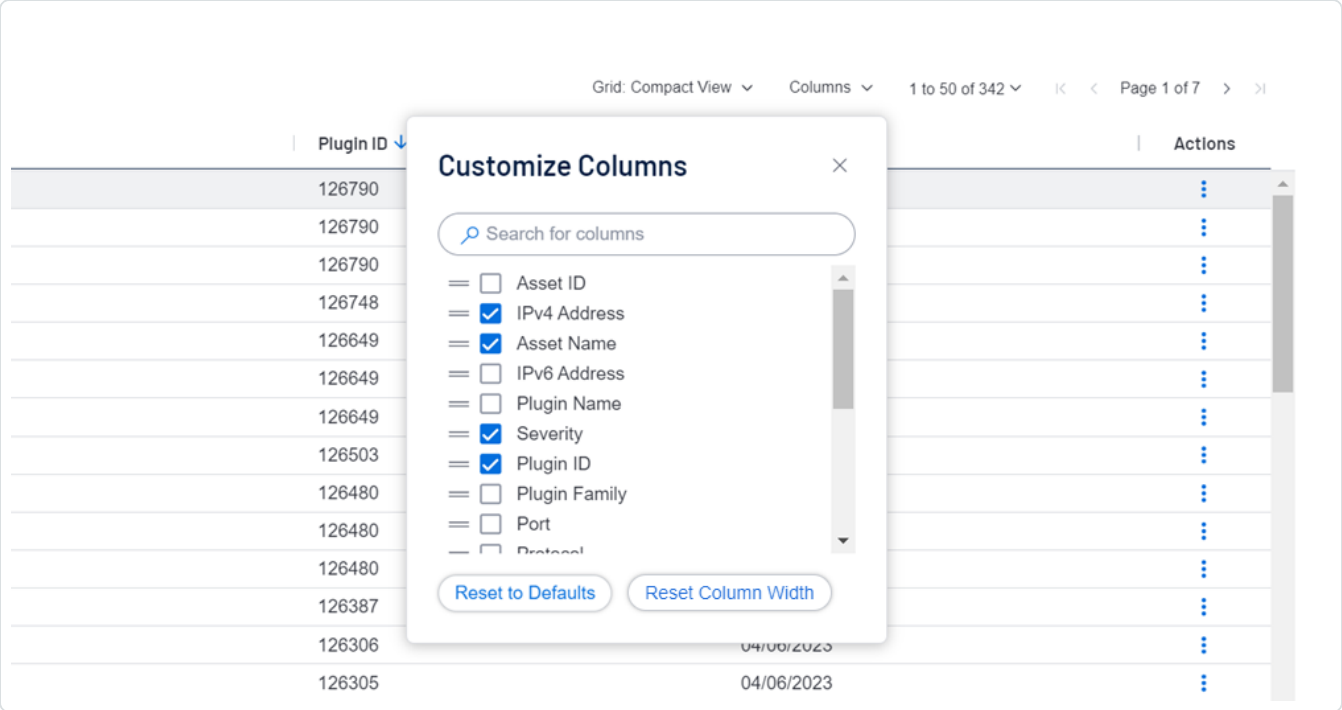
Customize Table Columns

You can customize the columns in any Tenable Vulnerability Management table.

To customize table columns:

1. Above a table, click **Columns**.

A dialog appears.



2. In the dialog:

Action	Description
Add or remove a column	Select or clear the check box next to the column.
Find a column to add	Search for a column and select its check box.
Reorder columns	Click and drag columns from top to bottom.
Change column width	Hover on the separator between column headings and drag left or right.
Reset column width to default	Click **Reset Column Width**.
Reset all column customizations to default	Click **Reset to Defaults**.

Right-Click Menu

Within any table, you can right-click to access a menu with additional options.

To access the right-click menu:

1. In the table, right-click the row for which you want to view menu items.

   The right-click menu appears.

   The options in the menu depend on the type of table you are viewing, however the following options are always available:

   - **Copy to Clipboard** – Click to copy the table value to your clipboard.
   - **Filter By Value** – Click to automatically filter the table by rows that include the selected value.

     > **Note:** By default, Tenable Vulnerability Management applies the AND operator to the filter. To use the OR operator, you must use the Query Builder.

   - **Filter Out Value** – Click to automatically filter the table by rows that do not include the selected value.

     > **Note:** By default, Tenable Vulnerability Management applies the AND operator to the filter. To use the OR operator, you must use the Query Builder.

Filter a Table

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In Tenable Vulnerability Management, a **Filters** box appears above individual tables in various pages and planes.

To filter a table:

1. Next to **Filters**, click the ⌄ button.

   The filter settings appear.

2. (Optional) In Tenable Vulnerability Management, to quick-select filters, click ☆ **Select Filters**.

   A drop-down list appears.

a. In the drop-down list, search for the filter you want to apply.

   The list updates based on your search criteria.

b. Select the check box next to the filter or filters you want to apply.

   The selected filters appear in the filter section.

3. In the **Select Category** drop-down box, select an attribute.

   For example, you might select **Severity** if filtering findings or **Asset ID** if filtering assets.

4. In the **Select Operator** drop-down box, select an operator.

   Note: When using the **contains** or **does not contain** operators, use the following best practices:

   - For the most accurate and complete search results, use full words in your search value.
   - Do not use periods in your search value.
   - Remember that when filtering assets, the search values are case sensitive.
   - Where applicable, Tenable recommends using the **contains** or **does not contain** instead of the **is equal to** or **is not equal to** operators.

5. In the **Select Value** box, do one of the following:

Value Type	Action
Text	Type the value on which you want to filter. An example of the expected input is present in the box until you start typing. If what you type is invalid for the attribute, a red outline appears around the text box.
Single valid value	If a default value is associated with the attribute, Tenable Vulnerability Management selects the default value automatically. To change the default value, or if there is not an associated default value present: a. Click the box to display the drop-down list.

	b. Search for and select one of the listed values.
Multiple valid values	To select one or more values: a. Click the box to display the drop-down list. b. Search for and select a value. The selected value appears in the box. c. Repeat until you have selected all appropriate values d. Click outside the drop-down list to close it. To deselect values: a. Roll over the value you want to remove. The ✕ button appears over the value. b. Click the ✕ button. The value disappears from the box.

6. (Optional) In the lower-left corner of the filter section:
   - To add another filter, click the **Add** button.
   - To clear all filters, click the **Reset Filters** button.
7. Click **Apply**.

   Tenable Vulnerability Management applies your filter or filters to the table.
8. (Optional) Save your filter or filters for later use.
9. (Optional) Clear the filters you applied:
   a. In the table header, click **Clear All Filters**.

   Tenable Vulnerability Management clears all filters from the table, including saved searches.

   > **Note:** Clearing filters does not change the date range selected in the upper-right corner of the page. For more information, see Tables.

Explore Tables

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

The **Findings** and **Assets** workbenches use *Explore tables* to present your organization's data. You can filter these tables to view specific assets or findings.

Use Filters

In Explore tables on the **Findings** and **Assets** workbenches, you can use filters to view specific findings or assets.

Note: To optimize performance, Tenable limits the number of Findings filters that you can apply to 18 and the number of Asset filters that you can apply to 35.

Tip: For a list of available filters, see Findings Filters or Asset Filters.

Note: When filtering findings to generate a Findings Report, you can apply a maximum of 5 filters to each report.

To use filters in Explore tables:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, under **Explore**, click **Findings** or **Assets**.

3. Do one of the following:

   Filter the table in Basic mode

   a. In the upper-left corner, click the ▽ button.

      The filters plane expands with a list of default filters selected.

   b. Click **Select Filters**.

      The **Select Filters** box appears with all available filters.

c. Select the filters you want to apply.

d. Click outside the **Select Filters** box.

   The **Select Filters** box closes.

e. For each filter, choose the appropriate *operator* and *option*. For example, to return vulnerabilities with Critical Severity, select an operator of **is equal to** and the **Critical** option, as shown in the following image:

Search operators are contextual, depending on the filter you select. For a complete reference, see the following table:

Operator	Description
exists	Filters for items for which the selected filter exists.
does not exist	Filters for items for which the selected filter does not exist.
is equal to	Filters for items that match the filter value.
is not equal to	Filters for items that do not include the filter value.

Operator	Description
is greater than **is greater than or equal to**	Filters for items with a value greater than the specified filter value. If you want to include the value you specify in the filter, then use the **is greater than or equal to** operator.
is less than **is less than or equal to**	Filters for items with a value less than the specified filter value. If you want to include the value you specify in the filter, then use the **is less than or equal to** operator.
within last	Filters for items with a date within a number of hours, days, months, or years before today. Type a number, then select a unit of time.
after	Filters for items with a date after the specified filter value.
before	Filters for items with a date before the specified filter value.
older than	Filters for items with a date more than a number of hours, days, months, or years before today. Type a number, then select a unit of time.
is on	Filters for items with a specified date.
between	Filters for items with a date between two specified dates.
contains	Filters for items that contain the specified filter value.
does not contain	Filters for items that do not contain the specified filter value.
wildcard	Filters for items with a wildcard (*) as follows: • **Begin or end with** – Filters for values that begin or end with text you specify. For example, to find all values that begin with "1", type *1**. To find all values that end in "1", type **1*.

Operator	Description
	• **Contains** –Filters for values that contain text you specify. For example, to find all values with a "1" between the first and last characters, type **1**. • **Turn off case sensitivity** – Filters for values without case sensitivity. For example, to search for findings with a **Plugin Name** of "TLS Version 1.2 Protocol Detection" *or* "tls version 1.2 protocol detection", type **tls version 1.2 protocol detection*.

f. (Optional) To remove or reset filters, do one of the following:

- To clear the values for a filter, hover on the right side of the filter and click **Clear**.
- To remove a filter, hover on the right side of the filter and click **Remove**.
- On the **Findings** workbench, to reset filters to the default set, at the top of the filters plane, click **Reset**.
- On the **Assets** workbench, to remove all filters, at the top of the filters plane, click **Clear All**.

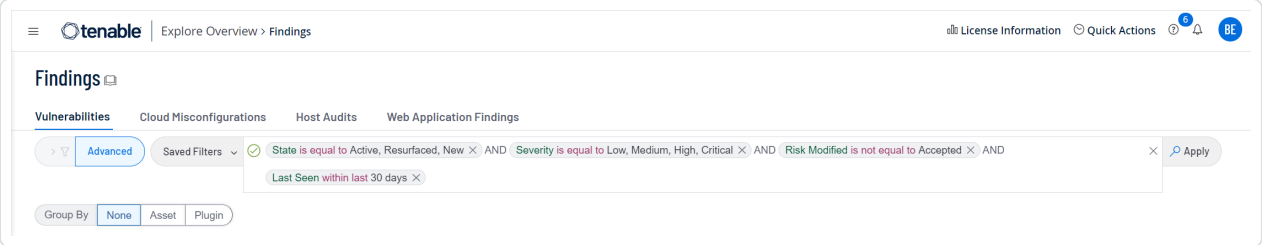
g. Click **Apply**.

Tenable Vulnerability Management filters your data.

Filter the table in Advanced mode

a. In the upper-left corner, click **Advanced**.

A box appears with the current filters displayed.



b. Click inside the box.

   A drop-down appears.

c. In the drop-down, select the **AND** or **OR** conditions or type them in the box.

d. In the drop-down, select a filter or type its name in the box.

e. In the drop-down, select one of the following operators or type it in the box.

> **Note**: If you want to filter on a value that starts with (') or ("), or includes (*) or (,), then you must wrap the value in quotation marks (").

> **Note**: Filters can have a maximum of two nesting levels.

Operator	Description
exists	Filters for items for which the selected filter exists.
does not exist	Filters for items for which the selected filter does not exist.
is equal to	Filters for items that match the filter value.
is not equal to	Filters for items that do not include the filter value.
is greater than **is greater than or equal to**	Filters for items with a value greater than the specified filter value. If you want to include the value you specify in the filter, then use the **is greater than or equal to** operator.
is less than **is less than or equal to**	Filters for items with a value less than the specified filter value. If you want to include the value you specify in the filter, then use the **is less than or equal to** operator.
within last	Filters for items with a date within a number of hours, days, months,

Operator	Description
	or years before today. Type a number, then select a unit of time.
after	Filters for items with a date after the specified filter value.
before	Filters for items with a date before the specified filter value.
older than	Filters for items with a date more than a number of hours, days, months, or years before today. Type a number, then select a unit of time.
is on	Filters for items with a specified date.
between	Filters for items with a date between two specified dates.
contains	Filters for items that contain the specified filter value.
does not contain	Filters for items that do not contain the specified filter value.
wildcard	Filters for items with a wildcard (*****) as follows: • **Begin or end with** – Filters for values that begin or end with text you specify. For example, to find all values that begin with "1", type *1**. To find all values that end in "1", type **1*. • **Contains** –Filters for values that contain text you specify. For example, to find all values with a "1" between the first and last characters, type **1**. • **Turn off case sensitivity** – Filters for values without case sensitivity. For example, to search for findings with a **Plugin Name** of "TLS Version 1.2 Protocol Detection" *or* "tls version 1.2 protocol detection", type **tls version 1.2 protocol detection*.

f. In the drop-down, select a filter value or type one in the box.

g. (Optional) To add or remove filters, do one of the following:

- To add multiple filters, press **Space** and then select another condition, operator, filter, and value.
- To remove one filter, click the ✕ button on the right side of the filter.
- To remove all filters, on the right side of the text box, click the ✕ button.

h. Click **Apply**.

Tenable Vulnerability Management filters your data.

4. (Optional) Save the filters to access later or share with other team members.

> **Tip**: Tenable Vulnerability Management runs Findings searches in the background so that you can navigate away from the **Findings** page and return when a complex search is complete. You can also **Cancel** a search. Finally, Tenable Vulnerability Management caches your most recent search for 30 minutes, notes the date and time in the top toolbar, and saves the state of the **Findings** page for your next visit.

Use the Context Menu

In Explore tables, on the **Findings** and **Assets** workbenches, right-click any row to show a menu with contextual options for both findings and assets. In the menu, the following options always appear.

Option	Description
View All Details	Open the details page for the finding or asset.
View All Details in New Tab	Open the details page for the finding or asset in a new browser tab.
Copy to Clipboard	Get any value from an Explore table. For example, when creating a tag, copy an operating system value from a field on the **Assets** workbench and paste it into your tag.
Filter by Value	Filter an Explore table by any value. For example, on the **Findings** workbench, right-click on an IPv4 address and click this option to view all findings with that IPv4 address.

Option	Description
Filter Out Value	Remove all entries with a certain value from an Explore table. For example, on the **Assets** workbench, right click an operating system type to filter out all assets with that operating system.

Customize Explore Tables

In the **Explore** section, on the **Findings** or **Assets** workbenches, you can customize the table columns.

To customize an Explore table:

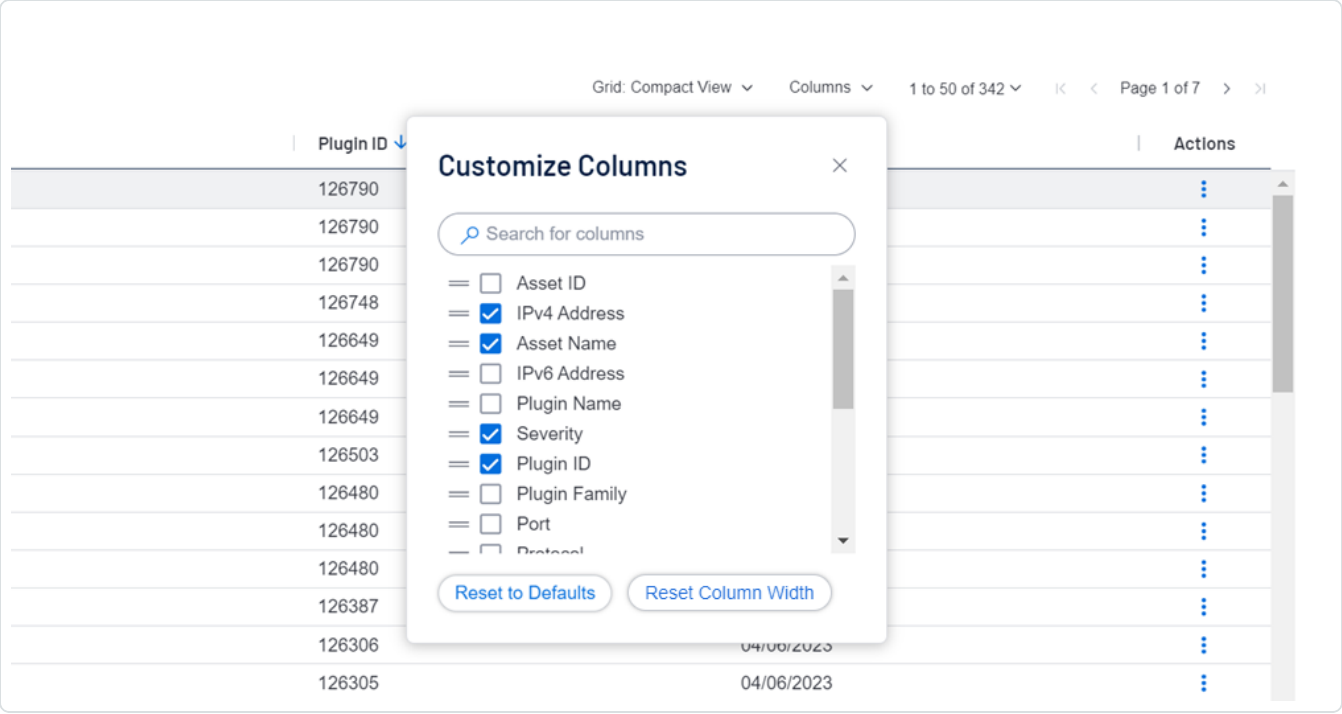
1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, under **Explore**, click **Findings** or **Assets**.

3. On the right side, above the table, click **Columns**.

   The **Customize Columns** dialog appears.



4. Do one of the following:

Action	Description
Add or remove a column	In the **Customize Columns** dialog, select or clear the check box next to the column.
Find a column to add	In the **Customize Columns** dialog, search for a column and select its check box.
Reorder columns	In the **Customize Columns** dialog, click and drag columns from top to bottom.
Change column width	In the **Assets** or **Findings** tables, hover on the separator between column headings and drag left or right.
Reset column width to default	In the **Customize Columns** dialog, click **Reset Column Width**.
Reset all column customizations to default	In the **Customize Columns** dialog, click **Reset to Defaults**.

Query Builder

In Tenable Vulnerability Management, you can use the *Query Builder* to view specific data via queries.

Important! When you run a query using the Query Builder, it applies to all data on the page, including the quick filters on the left side of your data table. These quick filters, on the other hand, only affect the data within the table itself. Any filters applied on the left side of the page do not affect the Query Builder.

How Queries Work

Queries are joined by *Conditions* (for example, AND). They have three components:

- **Filter** – The search criteria (for example, for a finding, *Severity*).
- **Operator** – The condition to filter on (for example, *is not equal to*).
- **Value** – The value to search (for example, a Severity of *High*).

Tip: You can nest queries with parentheses. For example, to search for high-severity findings where the VPR is greater than seven or the CVSSv3 Base Score is greater than six, use:

Severity is equal to High AND (VPR is greater than 7 OR CVSSv3 is greater than 6) .

Build a Query

To build a query with the Query Builder:

1. Click the query box.

   A pane appears with a list of filters, which vary in each section of Tenable Vulnerability Management.

2. Under **Filters**, choose a filter.

   A list of operators appears.

3. Under **Operators**, choose an operator.

   For filters where the value is text or a number, a hint appears. Otherwise, a list of options appears.

4. Under **Value**, type a value or select one from the list.

5. (Optional) Add another query (that is, type a Condition and then add a Filter, an Operator, and a Value).

   Tip: Under **Nesting Operators**, select an opening parentheses (or `NOT(` to start building a nested query.

6. Press **Enter** to run the query.

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 the **X**.

Keyboard Shortcuts

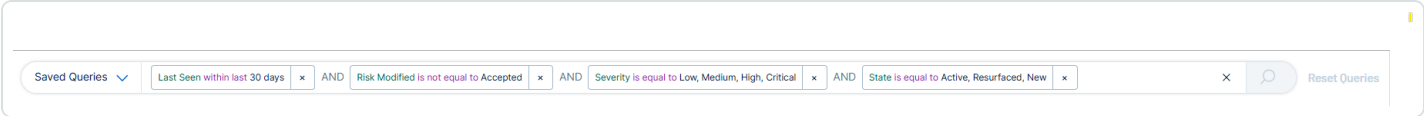
Use the following keyboard shortcuts in the Query Builder.

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 or **⌘ -C**	Copy the highlighted text.
Ctrl-V or **⌘ -V**	Paste your clipboard contents into the Query Builder.
Ctrl-Z or **⌘ -Z**	Undo the last action.
Ctrl-Y or **⌘ -Y**	Redo the last action.

Saved Queries

In Tenable Vulnerability Management, you can build custom queries with the Query Builder and save them to reuse or share. In the user interface, this feature is called **Saved Queries**.

You can access the **Saved Queries** menu to the left of the search/query bar within the Tenable Vulnerability Management user interface.



Additionally, when viewing your **Saved Queries**, you can view Tenable Queries which highlight common key performance indicators (KPIs).

Tenable Queries

Asset Tenable Queries	Findings Tenable Queries
External Assets (ASM) – Assets or domains discovered by Tenable Attack Surface Management, integrated with the steps described in Manage Integrations in the *Tenable Attack Surface Management User Guide*. This filter does not appear for Domain Inventory assets.	**AI Inventory** – AI-related Vulnerabilities and Web Application findings identified by Tenable's plugins.
Network Devices – Assets identified as a networking devices, including routers, switches, firewalls and SSL gateways. This filter does not appear for Domain Inventory, Cloud Resource, or Web Application assets.	**CISA Known Exploitable** – Vulnerabilities that appear in the CISA Known Exploited Vulnerabilities Catalog. **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.

	In the News – Vulnerabilities being widely reported in the press with notable coverage over the past 30 days.
	Persistently Exploited – Vulnerabilities being leveraged by threat actors over an extended period of time in targeted attacks, ransomware, or malware campaigns. These vulnerabilities are curated by the Tenable Research team.
	Ransomware – Vulnerabilities used in current or historical ransomware attacks, as determined from evidence gathered by the Tenable Research team.
	Recently Exploited – Vulnerabilities with notable coverage in the press over the past 30 days, and for which Tenable has evidence of active exploitation.
	Top 50 VPR – The top 50 vulnerabilities by Vulnerability Priority Rating (VPR).

Manage Queries

You can manage your queries in the following ways:

Save a Query

To save a query:

1. In a query box, use the Query Builder to refine results.
2. To the left of the query box, click **Saved Queries**.

   A drop-down appears.

3. Click **Save As New Query**.
4. In **New Query Name**, type a name and click the ✓ button.

Set a Default Query

You can set any query to be your default query when navigating to the Tenable Vulnerability Management page.

To set a default query:

1. To the left of a query box, click **Saved Queries**.

   A drop-down appears.

2. To the right of the query, click the ☆ button.

   Tenable Vulnerability Management saves the query as your default, and applies it to the page automatically.

Run a Saved Query

To run a saved query:

1. To the left of a query box, click **Saved Queries**.

   A drop-down appears.

2. In the drop-down, click a query to run it.

Share a Saved Query

To share a saved query:

1. To the left of a query box, click **Saved Queries**.

   A drop-down appears.

2. To the right of the query to share, click the button.
3. Paste the link to share the query.

Note: Any Tenable Vulnerability Management user can run a shared query, but the assets they can view are based on permissions. To learn more, see Access Control.

Edit a Saved Query

To edit a saved query:

1. To the left of a query box, click **Saved Queries**.

   A drop-down appears.

2. In the drop-down, click the query to edit.

3. Do one of the following:

   #### Rename the query:

   a. Click the ✎ button.

   b. Type a new name and click the ✓ button.

   #### Save the query as a new query:

   a. In the filter box, update the query.

   b. To the left of the query box, click **Saved Queries**.

   c. In the drop-down that appears, click **Save as New Query**.

   d. Type a new name in the box and click the ✓ button.

Delete a Saved Query

To delete a saved query:

1. To the left of a query box, click **Saved Queries**.

   A drop-down appears.

2. Next to the query to delete, click the 🗑 button.

Export Findings or Assets

You can export data from the **Findings** and **Assets** workbenches to CSV or JSON. While these workbenches contain different data, the basic export process is the same.

To export findings or assets:

1. Do one of the following:
   - In the left navigation, click **Findings**.

     The **Findings** workbench appears.
   - In the left navigation, click **Assets**.

     The **Assets** workbench appears.
2. In the left navigation plane, under **Explore**, do one of the following:
   - To export your organization's scanned vulnerability findings, click **Findings**.

     The **Findings** workbench appears.
   - To export your organization's scanned assets, click **Assets**.

     The **Assets** workbench appears.
3. Refine the displayed data, as described in Use Filters.

   Note: On the **Findings** workbench, when using the **Group By** filter, you can only export five findings at a time.

   Note: On the **Assets** workbench, the **Asset ID**, **Last Authenticated Scan**, **Last Licensed Scan**, and **Source** fields are required.
4. Select the check boxs next to the findings or assets to export.

   Note: You can manually select up to 200 findings or assets. Otherwise, you must select them all.
5. In the action bar, click **Export**.

   The **Export** plane appears.

Option	Description

Name	Type a name for the export.
Formats	Select an export format: • **CSV** – A CSV file that you can open in a spreadsheet application such as Microsoft Excel. **Note**: For findings exports, the system automatically trims cells longer than 32,000 characters so they appear correctly in Microsoft Excel. Select **Untruncated Data** to disable this. **Note:** If your export file contains a cell starting with any of the following characters (=, +, -, @), the system adds a single quote (') at the beginning of the cell. For more information, see the Knowledge Base. • **JSON** – A JSON file containing a nested list of findings, with no empty fields.
Configurations	Select the fields to include: • Under **Select Field Set**, search for or select the fields to add to your export. • To view only selected fields, click **View Selected**. • In the **Expiration** box, type the number of days before the export file ages out. **Note**: In asset exports, **Asset ID**, **Last Authenticated Scan**, **Last Licensed Scan**, and **Source** are required.
Schedule	Turn on the **Schedule** toggle to schedule your export: a. In the **Start Date and Time** section, choose the date and time for the export. b. In the **Time Zone** drop-down, choose a time zone. c. In the **Repeat** drop-down, choose the cadence on which you

	want the export to repeat (for example, daily). d. In the **Repeat Ends** drop-down, choose the date when exports end. If you select **Never**, the export repeats until you modify or delete it.
Email Notifications	Turn on the **Email Notification** toggle to send email notifications: a. In the **Add Recipients** box, type the emails to notify. b. In the **Password** box, type a password for the export file. Share this password with the recipients so they can download the export file.

6. Click **Export**.

   Depending on size, the export file may take several minutes to process. When processing completes, the file downloads to your computer.

   Tip: If you close the **Export** plane before the download completes, you can access the completed export file in **Settings** > **Exports**.

Error Messages

For Tenable Vulnerability Management API status codes, see the Tenable Developer Portal.

Scanning

The following table describes the scanning error messages that may appear in Tenable Vulnerability Management.

Some scanning errors occur when you exceed the following Tenable Vulnerability Management scanning limitations:

Scan Limitations

The following table describes scanning limitations in Tenable Vulnerability Management:

Limitation	Description

Targeted IP addresses or hostnames per assessment scan	Tenable Vulnerability Management limits the number of IP addresses or hostnames you target with a single assessment scan (for more information, see Discovery Scans vs. Assessment Scans). The host target limit is 10 times your organization's licensed asset count. For example, if your organization has a licensed asset count of 1,000, Tenable Vulnerability Management does not allow you to target more than 10,000 hostnames or IP addresses in a single assessment scan. If you exceed the limit, Tenable Vulnerability Management aborts the scan.
Targeted IP addresses or hostnames per discovery scan	Tenable Vulnerability Management limits the number of IP addresses or hostnames you target with a single discovery scan (for more information, see Discovery Scans vs. Assessment Scans). The host target limit is 1,000 times your organization's licensed asset count. For example, if your organization has a licensed asset count of 1,000, Tenable Vulnerability Management does not allow you to target more than 1,000,000 hostnames or IP addresses in a single discovery scan. If you exceed the limit, Tenable Vulnerability Management aborts the scan.
Host scan results per scan	Tenable Vulnerability Management limits the number of live hosts for which a single scan can generate scan results for. The live host scan results limit is 1.1 times your organization's licensed asset count. For example, if your organization has a licensed asset count of 1,000, Tenable Vulnerability Management does not allow you to generate scan results for more than 1,100 live hosts from a single scan. If you exceed the limit, Tenable Vulnerability Management aborts the scan. Tenable Vulnerability Management does not apply the live host scan result limit to discovery scans. Tenable Vulnerability Management also limits the number of dead hosts for which a single scan can generate scan results for. The dead host scan results limit is 100 times your organization's licensed asset count. For example, if your organization has a licensed asset count of 1,000, Tenable Vulnerability Management does not allow you to generate scan

	results for more than 100,000 dead hosts from a single scan. If you exceed the limit, Tenable Vulnerability Management aborts the scan.
Targeted IP addresses or ranges per scan	You cannot specify more than 300,000 comma-separated IP addresses or ranges when configuring a scan's targets.
Active scans	You cannot have more than 25 scans running in your container simultaneously.
Scan chunks	Tenable Vulnerability Management limits scan chunks to 10,000 hosts, 150,000 findings, or 7 GB in total size. If a scan chunk exceeds any of these values, Tenable Vulnerability Management does not process the scan and eventually aborts it. **Note:** This limits items like MDM assessments, importing Nessus files, and very large Auto Discovery scenarios (for example, VMware) to individual scans with less than 10,000 assessed targets.
Scan configurations	Tenable Vulnerability Management limits the number of scan configurations you can create to 10,000 scans. Tenable recommends re-using scheduled scans instead of creating new scans. This approach helps to avoid latency issues in the user interface.

For more information about creating, modifying, and launching scans, see Manage Scans. For more information about scan status values, see Scan Status.

Warning	Message	Recommended Action
Aborted Task Targets	The following targets were aborted: *[scan targets]*	If needed, perform a rollover scan on the aborted targets.
Aborted Task Targets Summary	There were *[number]* aborted targets, including *[number of targets not in notes]* above the limit for reporting notes.	If needed, perform a rollover scan on the aborted targets.
Account Target Limit	The target count exceeds the limit for this account. Please contact	You reached the maximum scan target limit. To increase your scan

Warning	Message	Recommended Action
	customer support to upgrade your license.	target limit by upgrading your license, contact Tenable Support.
Agent Group Error	Unexpected error retrieving the agent groups.	
Agent Group Permissions	The owner does not have access to all of the configured agent groups.	You do not have access to all the agent groups selected for this scan. Select the correct groups. For more information, see Agent Groups.
Agent Scan Indexing Error	Tenable Vulnerability Management aborted a scan task after an unexpected error occurred during indexing. You may need to re-scan the agent. (Agent: *[agent name]*, Agent UUID: *[agent uuid]*)	Re-scan the affected agent.
Agent Unscanned	Scan not *{completed | started}*. Agent with plugin set: *{pluginSet}* last connected: *{lastConnected}* and last scanned *{lastScanned}*. (Agent: *[agent name]*, Agent UUID: *[agent uuid]*)	Re-run the scan.
All Inactive Scanners	All targets were routed to scanner groups with no active scanners.	
All Scans Aborted	All active scans were aborted.	Tenable Vulnerability Management aborted the scan due to a system abort request. Re-run the scan.
Auto Routed Custom Targets	Custom scan targets are not currently supported for auto	Select a specific scanner to run scans on custom targets.

Warning	Message	Recommended Action
	routed scans.	
Auto Routing Disabled	The scan is configured for auto routing, but that feature is not enabled.	
Concurrent Scan Limit	Concurrent scan limit reached for this account. Please contact customer support to upgrade your license.	You reached the maximum concurrent scan limit. Re-run the scan later.
Concurrent Scan Limit Reached	Scan could not be completed: concurrent scan limit reached for this account. Please contact customer support to upgrade your license.	You reached the maximum concurrent scan limit. Re-run the scan later.
Conflict	Transition for indexing to pausing not supported.	The scan is completed and is now in the process of indexing. Wait for the indexing to complete.
Empty Scanner Group	The scan is configured to use a scanner group with no assigned scanners.	Confirm that the scanner group contains functioning scanners, then re-run the scan.
Empty Targets	No targets are configured for the scan.	Confirm the scan configuration contains one or more valid targets, then re-run the scan.
Import Failed	Failed to import scan results from the agent. Invalid results, multiple hosts detected in scan results. (Agent: *[agent name]*, Agent UUID: *[agent uuid]*)	Re-run the scan.
Inactive Scanners	The scan is configured to use a scanner group with no active	Confirm that the configured scanner is functioning, or that the

Warning	Message	Recommended Action
	scanners.	configured scanner group contains functioning scanners, then re-run the scan.
Indexing Error	Unexpected error during task processing. Targets may need to be rescanned : *[scan targets]*	Re-run the scan for unscanned targets or targets that need to be re-scanned.
Initialization Error	Unexpected error during initialization.	Tenable Vulnerability Management aborted the scan. Re-run the scan.
Invalid AWS Targets	No valid AWS targets are configured for the scan.	Confirm the scan contains valid AWS scan targets and re-run the scan. For more information, see Targets.
Invalid PCI Scanner	The PCI scan can only be launched using Tenable Cloud Scanners	Use a Tenable cloud sensor to run a Tenable PCI ASV scan. For more information, see Cloud Sensors.
Invalid Tag Target	Failed to resolve a target FQDN or IP from an asset in the configured tags.	One or more assets in a tag configured for the scan requires an associated scan target. Confirm the tag configuration, then re-run the scan. For more information, see Tags.
Invalid Tag Rule As Target	Tags with the "Match All" filter can only have one rule for scans with the "Targets defined by tags" option enabled. Tag category: *[tag category]*, Tag value: *[tag value]*.	Adjust your tag rules, then re-run the scan.
Invalid Target	Can't resolve target.	Confirm your scan includes valid scan targets, then re-run the scan. For more information, see Targets.

Warning	Message	Recommended Action
Invalid Target Range	An invalid target range is configured for the scan: *[scan targets]*	Correct or remove the invalid scan target range, then re-run the scan. For more information, see Targets.
Invalid Targets	No valid targets are configured for the scan.	Confirm the scan targets meet the following criteria: • IP addresses use a valid format • Use commas to separate lists of IP addresses • IP addresses in target groups use a valid format For more information, see Targets and Target Groups. For more troubleshooting assistance, see the knowledge base article.
Job Initialization Error	Unexpected error during initialization. Please check the scan targets and settings for irregularities and contact support if the problem persists.	Re-run the scan.
Log4j DNS Failed Request	Unable to resolve DNS *[scan target]* to check Log4j Vulnerability.	Re-run the scan for unscanned targets or targets that need to be re-scanned.
Max Findings Error	The maximum number of findings was reached.	Review the Tenable Vulnerability Management scan limitations and adjust the scan configuration to produce an allowed number of

Warning	Message	Recommended Action
		findings.
Max Hosts Reached Error	Scan has exceeded the maximum number of allowed hosts.	Review the Tenable Vulnerability Management scan limitations and adjust the scan configuration to scan an allowed number of hosts.
Network Congestion Detected	Some network congestion was detected during the scan. This may indicate that one or more of the remote hosts are connected through a connection that does not have enough bandwidth to handle the network traffic generated while scanning.	To reduce the risk of congestion: • Reduce **max hosts** to a lower value • Increase the **network read timeout** in your policy
No Available Scanner	Unable to find a scanner that is able to run the scan.	Confirm you selected the correct scanner, then re-run the scan.
No Configured Agent Groups	The scan has no configured Agent Groups.	Add at least one Agent Group to the scan.
No Scan Policy	The scan must be configured with a scan policy.	The scan requires a scan policy. Configure a scan policy, then re-run the scan.
No Tag Targets	No valid targets were found from the configured tags.	
Notification Error	Notifications for this scan may not have been sent.	The scan completed, but failed to send a notification.
Owner Disabled	The owner of the scan is disabled.	Enable the owner of the scan or transfer ownership to an enabled user. For more information, see Permissions.

Warning	Message	Recommended Action
Paused Scan Timeout	Paused scan exceeded timeout of *[maximum allowed pause]* days. Some tasks were aborted. Targets may need to be rescanned.	The paused scan exceeded the maximum pause duration. Re-run the scan for all incomplete scan targets.
Pending Scan Timeout	The scan was unable to transition to running within the expected timeout.	Confirm that the selected scanner or scanner group has sufficient capacity, then re-run the scan.
Policy Permissions	The owner of the scan does not have access to the configured policy.	You do not have access to the scan policy for this scan. Re-run the scan with correct permissions. For more information, see Permissions.
Portscanner Max Ports Exceeded	Portscanners have found more than *[number]* ports open for target *[target name]*, and the number of reported ports has been truncated to *[number]* (threshold controlled by scanner preference portscanner.max_ ports). Usually this is due to intervening network equipment intercepting and responding to connection requests as a countermeasure against portscanning or other potentially malicious activity.	Since this negatively impacts both scan accuracy and performance, you may want to adjust your network security configuration to disable this behavior for vulnerability scans.
Processing Error	Unexpected error in processing.	Tenable Vulnerability Management aborted the scan. Re-run the scan.
Routed To Inactive Scanners	The following targets were routed to a scanner group with no active	Confirm the scanner group contains functioning scanners,

Warning	Message	Recommended Action
	scanners: *[scan targets]*	then re-run the scan.
Running Scan Timeout	The scan exceeded the maximum allowed runtime.	The scan may be taking too long to scan some scan targets. Re-run the scan.
Scan Aborted	Scan aborted because it stalled in initializing.	Tenable Vulnerability Management aborted the scan. Re-run the scan.
Scan Aborted	An error occurred while initializing the scan.	Tenable Vulnerability Management failed to initialize the scan. Re-run the scan.
Scan Aborted	Failed to obtain plugin set information from Tenable Nessus.	Tenable Vulnerability Management failed to download the plugin set. Re-run the scan.
Scan Aborted	The assigned scanner was not found.	Tenable Vulnerability Management could not find the selected scanner. Select a different scanner and re-run the scan.
Scan Extraction Error	An error occurred during the scan extraction.	
Scan Extraction Timeout Error	The scan extraction timed out.	
Scan Forbidden	Rejected attempt to scan *[scan target]*, as it violates user-defined rules.	The scan target is excluded from scans. If you want to scan this target, remove it from the exclusion and re-run the scan. For more information, see Exclusions. Alternatively, you many not have the correct user permissions to run the scan. Check your user

Warning	Message	Recommended Action
		permissions and re-run the scan. For more information, see Permissions.
Scan Force Stopped	The scan was forcefully stopped, which cancels all incomplete tasks and updates scan status to **Aborted**.	
Scan Job Initialization Error	The scan could not be initialized. Please check the scan targets setting for irregularities and contact support if the problem persists.	Tenable Vulnerability Management failed to launch the scan. Re-run the scan with the correct scan target. For more information, see Targets.
Scanner Disabled	The assigned scanner is disabled.	A user disabled the selected scanner. Select a different scanner and re-run the scan.
Scanner Error	Unexpected error retrieving the assigned scanner.	
Scanner Group Error	Unable to load scanner group for scanner *[scanner ID]*.	Confirm the scan configuration contains one or more valid targets, then re-run the scan.
Scanner Interruptions	Due to detection of scanner interruptions during the scan, this scan might have run longer than expected. Scanner name: *[scanner name]*	This error occurs when a Tenable Nessus scanner is unable to complete a scan task, and Tenable Vulnerability Management reassigns the scan task to another scanner. This usually happens when the original scanner goes offline intentionally (for example, a user stops, powers off, or unlinks the scanner) or experiences an

Warning	Message	Recommended Action
		unexpected failure while completing the scan task (for example, power or network loss). Adjust the Tenable Nessus scanner as needed to prevent interruptions.
Scanner Not Found	The assigned scanner was not found.	Tenable Vulnerability Management could not find the selected scanner. Select a valid scanner and re-run the scan.
Scanner Permissions	The owner of the scan does not have access to the assigned scanner.	You do not have access to the selected scanner. Select a different scanner and re-run the scan. For more information, see Permissions.
Stalled Task	A task was automatically aborted after stalling on scanner. Targets may need to be rescanned: *[scan targets]*	Confirm the scanners are functioning properly and have enough capacity for your scans, then re-run the scan for unscanned targets or targets that need to be re-scanned.
Tag Not Found	Tenable Vulnerability Management could not process the tag. The tag either did not exist at the time of scanning or the user does not have access to the tag. Tag UUID: *[tag uuid]*.	Open the scan configuration in Tenable Vulnerability Management to automatically remove any tags that no longer existing. Save the scan configuration and re-run the scan.
Tag Targets Error	Failed to obtain tag targets	Tenable Vulnerability Management

Warning	Message	Recommended Action
	associated with scan.	could not obtain the scan targets. Verify the targets and re-run the scan. For more information, see Targets.
Target Access Error	The owner of the scan does not have access to any configured targets.	You do not have the correct user permissions to run the scan. Check your user permissions and re-run the scan. For more information, see Permissions.
Target Group Permissions	The owner of the scan does not have access to all of the configured target groups.	Confirm the scan owner's permissions, then re-run the scan. For more information, see Target Groups.
Target Limit	The target count exceeds the maximum allowed for Tenable Vulnerability Management.	The scan target range is too large. Confirm the scan configuration includes a valid target range, then re-run the scan. For more information, see Targets.
Target Range Limit	A target range exceeds the maximum allowed targets: *[scan targets]*	Confirm or reduce the configured scan target range and re-run the scan. For more information, see Targets.
Targets Unable To Complete	The following targets are not able to complete scanning in the allowed scan time and will need to be rescanned: *[scan targets]*	Re-run the scan for unscanned targets or targets that need to be scanned again.
Task Initialization Error	Unexpected error during initialization. Targets may need to be rescanned: *[scan targets]*	Re-run the scan for unscanned targets or targets that need to be re-scanned.

Warning	Message	Recommended Action
Task Processing Error	Unexpected error in processing. Targets may need to be rescanned: *[scan targets]*	Re-run the scan for unscanned targets or targets that need to be re-scanned.
Transition Timeout	Some tasks stalled when being *[resumed, paused, or stopped]* and were aborted. Targets may need to be rescanned.	Failed to complete scan on some scan targets. Re-run the scan for all unscanned scan targets.
Unable To Route Targets	Unable to find a matching scanner route for the following targets: *[scan targets]*	Tenable Vulnerability Management could not find one or more scan targets specified in the scan configuration. Do the following, then re-run the scan: • Confirm the scan configuration specifies the correct network. • Confirm the scan routing configuration of the scanner groups in that network.
	The total number of scan configurations cannot exceed 10,000.	Review and remove any scan configurations that your organization no longer uses.
	The following targets were not routable: *[scan targets]*	Ensure that you are using the correct scanner to scan the targets and that there are not any protective securities between the scanner and the targets.
Unenforceable Rules	Some dynamic rules are disabled because IP address resolution. Rules containing the following host names are affected: *[rules]*	Verify that the host names are correct and check your DNS configuration.

Dashboards

Dashboards are interactive, graphical interfaces that often provide at-a-glance views of key performance indicators (KPIs) relevant to a particular objective or business process.

The **Dashboards** page contains tiles that represent:

- Tenable-provided dashboards. For a complete index of Tenable-provided dashboard templates, see Tenable Vulnerability Management Dashboards.

  > **Note:** Depending on your license, more dashboards are included. For example, the Tenable Lumin dashboard.

- Dashboards you have created. To create a template-based or custom dashboard with Tenable-provided or custom widgets, see Create a Dashboard.
- Dashboards that other users have shared with you. Click the **Shared with Me** tab to view dashboards that others have shared with you.

Vulnerability Management Dashboard

This Tenable-provided dashboard visualizes actionable insights for your vulnerability management program. Tenable Vulnerability Management updates dashboard data every time you run a scan.

> **Note:** There may be a delay between when a scan completes and when the dashboard data updates while Tenable Vulnerability Management indexes the data.

To access the Vulnerability Management Overview dashboard:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Vulnerability Management**.

   The **Vulnerability Management Overview** dashboard appears.

You can roll over individual items to reveal additional information or click on items to drill down into details behind the data.

Tip: All charts on the **Vulnerability Management Overview** show **New**, **Active**, and **Resurfaced** vulnerability data. However, the counts or data displayed on each chart may differ for other reasons. For example, the **Vulnerability Priority Rating (VPR)** widget organizes vulnerabilities by VPR category, but the **Vulnerability Trending** widget graphs vulnerabilities by CVSS-based severity category. For more information about how severity and VPR metrics compare, see CVSS vs. VPR.

In the **Vulnerability Management Overview**, you can interact with the following widgets:

Widget	Action
Cyber Exposure News Feed	This widget highlights the most recent Tenable blog posts related to exposure incidents. • Click on a tile to navigate to the Tenable blog post. • Click the ⌄ or ⌃ button to collapse or expand the feed. • Click the ‹ or › button to scroll through the tiles.
Statistics	This widget summarizes the highest severity vulnerabilities on for your network during the last 30 days. • View a count of your total vulnerabilities and counts for the highest severity vulnerabilities (**Critical** and **High**) during the past 30 days. • To view a list of vulnerabilities, click one of the counts. The **Vulnerabilities** page appears, filtered by a severity if you selected the **Critical** or **High** count. • View a count of your total licensed assets, your assets discovered during the last 7 days, and your assets discovered during the last and 30 days. If necessary, onboard your newly discovered assets. • To view a list of assets, click one of the counts. The **Assets** page appears, filtered by a time range if you selected the **7 days** or **30 days** count. For more information, see View Asset Details.

	• View a count of your scans run during the last 90 days and the percentage that succeeded and failed. To investigate your failed scans, review your scans with the status **Aborted** or **Canceled**. For more information, see View Scans. • To export the data in the widget, click the ⋮ button and select a format.
CISA Alerts AA22-011A and AA22-047A	This widget provides a vulnerability count of risks associated with the CISA Alerts AA22-011A and AA22-047A vulnerabilities that have been identified or mitigated. • To view a list of related vulnerabilities by plugin, in the **Vulnerabilities** column, click one of the tiles. The **Vulnerabilities** page appears with results filtered by vulnerability state. • To view a list of related vulnerabilities by asset, in the **Assets** column, click one of the tiles. The **Vulnerabilities** page appears, filtered by vulnerability state. • To export the data in the widget, click the ⋮ button and select a format.
Vulnerability Priority Rating (VPR)	This widget summarizes the number of vulnerabilities on your network, organized by VPR. For more information, see CVSS vs. VPR. • To view a list of vulnerabilities filtered by a VPR range, click one of the tiles. The **Vulnerabilities** page appears, filtered by the range you selected. • To export the data in the widget, click the ⋮ button and

	select a format.
SLA Progress: Vulnerability Age	This widget visualizes vulnerability counts by severity and by compliance with your Service Level Agreements (SLAs). To modify how Tenable Vulnerability Management calculates SLA severity, see General Settings. • To view a list of vulnerabilities, click one of the tiles. The **Vulnerabilities** page appears, filtered by severity. • To export the data in the widget, click the ⋮ button and select a format.
Vulnerability Trending	This widget shows the cumulative number of **Critical**, **High**, **Medium**, and **Low** severity vulnerabilities on your network over time. For more information, see CVSS vs. VPR. • To show or hide data for a severity, click the boxes in the graph legend. The system updates the widget to show or hide the data you selected. • To view historical vulnerability count and severity data, roll over a point on the graph. • To view a list of current vulnerabilities, click a point on the graph. The **Vulnerabilities** page appears, filtered by the severity you selected and by **New**, **Active**, or **Resurfaced** state. • To export the data in the widget, click the ⋮ button and select a format.
Critical and High Exploitable Vulnerabilities	This widget summarizes the number of **Critical** and **High** severity vulnerabilities on your network, organized by exploitability characteristic category. A single vulnerability may have multiple exploitability characteristics and count towards

	multiple categories. • To view the counts of your vulnerabilities by decreasing priority, view the categories and counts from left to right. • To view a list of vulnerabilities, click one of the bars on the graph. The **Vulnerabilities** page appears, filtered by **Critical** and **High** severity and the exploitability characteristic you selected. • To export the data in the widget, click the ⋮ button and select a format.
Future Threats: Not Yet Exploitable Vulnerabilities	This widget summarizes the vulnerabilities that are not yet exploitable, determined by their **Exploit Code Maturity** and **Vulnerability Publication Date**. • To view the counts of your vulnerabilities by decreasing priority, view the categories and counts from upper left to lower right. Tenable recommends addressing vulnerabilities with proof-of-concept before those with no known exploit. • To export the data in the widget, click the ⋮ button and select a format.
Vulnerability Age	This widget summarizes the age of your vulnerabilities (by **Vulnerability First Seen** date), organized by severity, to help you manage your SLAs. For more information about severity, see CVSS vs. VPR. • To view a list of vulnerabilities, click one of the vulnerability counts. The **Vulnerabilities** page appears, filtered by the **Vulnerability First Seen** date and severity you selected.

	• To export the data in the widget, click the ⋮ button and select a format.

Vulnerability Management Overview (Explore)

The Vulnerability Management Overview (Explore) dashboard provides executive management with a summary of risk information at a glance, while enabling security analysts to drill down into technical details by clicking on the widgets. Tenable Vulnerability Management updates the dashboard data each time you run a scan.

> **Note:** There may be a delay between the time when a scan completes and when the dashboard data updates while Tenable Vulnerability Management indexes the data.

Hovering over individual items reveals a data summary that you can click to drill down for further details.

In the **Vulnerability Management Overview (Explore)**, you can interact with the following widgets:

Widget	Action
Cyber Exposure News Feed	This widget highlights the most recent Tenable blog posts related to exposure incidents. • Click on a tile to navigate to the Tenable blog post. • Click the ⌄ or ⌃ button to collapse or expand the feed. • Click the ‹ or › button to scroll through the tiles.
Severity Statistics by Source	The widget provides a count of vulnerabilities collected through multiple sources: Tenable Nessus scan and Tenable Agents. The numbers displayed in this widget use severity to determine the precedence of vulnerabilities to mitigate. • To view the list of assets for a specific category, click on the summary information in the relevant category. The **Findings** page appears with details about the assets detected for the category.

	• To export the data in the widget, click the ⋮ button and select a format.
Tenable Research Advisory	This widget provides two indicators for current major threats discovered by Tenable Research. The red indicator signifies the presence of the relevant vulnerabilities, while the green indicator is enabled when these vulnerabilities are patched. • Click on the tiles to display a **Findings** page with details about the assets detected for **Missing Patches** and **Applied Patches**. • To export the data in the widget, click the ⋮ button and select a format.
Vulnerability Priority Rating (VPR)	This widget displays vulnerabilities grouped by Vulnerability Priority Rating (VPR). VPR is the output of Tenable's predictive prioritization process which it is continually updates to accommodate the evolving threat landscape. Following the initial scan of an asset on the network, Tenable computes an initial VPR using a machine-learning algorithm that analyzes more than 150 different aspects of each vulnerability to determine the level of risk. Vulnerabilities listed on the left have the highest VPR, while those on the right have the lowest. For more information, see CVSS vs. VPR. • To view the asset details detected in a specific range, click on a VPR range. The **Findings** page appears with details about the assets detected in the selected range. • To export the data in the widget, click the ⋮ button and select a format.
SLA Progress: Vulnerability	This widget helps organizations manage Service Level Agreements (SLAs) by providing a vulnerability view organized

Age	by Vulnerability Priority Rating (VPR) Score and Vulnerability Age. Tenable calculates the vulnerabilities that do not meet SLAs using a date filter for within the last X days. The vulnerabilities that meet SLAs use a date filter for older than X days. When you apply default SLA settings: • **Critical**: row uses VPR greater than 9.0. • **High**: row uses VPR between 7.0-8.9. • **Medium**: row uses VPR between 4.0-6.9. • **Low**: row uses VPR between 0-3.9. To know how Tenable Vulnerability Management calculates SLA severity, see General Settings. • To view the list of assets detected for a specific category, click on the summary information under the SLA categories. The **Findings** page appears with details about the assets. • To export the data in the widget, click the ⋮ button and select a format.
Critical and High Exploitable Vulnerabilities	This widget focuses on the most severe current threats, critical, and high exploitable vulnerabilities to help prioritize remediation. Each bar represents vulnerabilities grouped by an exploitability characteristic. • **Exploited by Malware**: Vulnerabilities that can be exploited by malicious software, such as viruses, worms, spyware, adware, and ransomware. • **Remotely Exploitable (Low Complexity)**: Vulnerabilities that can easily be exploited remotely and require little skill or information gathering to exploit.

	• **Locally Exploitable (Low Complexity)**: Vulnerabilities that can easily be exploited with local access and require little skill or information gathering to exploit. • **Exploited by Framework (Metasploit)**: Vulnerabilities that have publicly available exploit code imported into various exploit frameworks, such as Metasploit, pose risks. These common exploit frameworks are easily accessible, which both security researchers and malicious attackers use. • **Remotely Exploitable (High Complexity)**: Vulnerabilities that can be exploited remotely, but require a high degree of skill and information gathering to exploit. **Note**: These groupings are not mutually exclusive, as a single vulnerability can fall into multiple exploitability categories. Tenable recommends prioritizing remediation starting with vulnerabilities in the left-most column, **Exploited by Malware**. • To view details about assets for a specific category, click one of the bars on the graph. The **Findings** page appears with details about assets detected for the category. • To export the data in the widget, click the ⋮ button and select a format.
Future Threats: Not Yet Exploitable Vulnerabilities	This widget provides a view of vulnerabilities based on exploit code maturity and vulnerability publication date. The columns display counts of published vulnerabilities within the specified time period present in the organization. The rows display the exploit code maturity, where **Proof of Concept** is more serious than **Unproven Exploit**. • To view the list of assets for a specific category, click on the counts under the **Published** categories. The **Findings** page appears with details about the assets

	detected for the category. **Tip**: Tenable recommends addressing vulnerabilities with proof-of-concept before those with no known exploit. • To export the data in the widget, click the ⋮ button and select a format.
Scan Health	This widget provides a summary of scan health in relation to authentication success and failures. The five columns display asset counts related to: • **Authentication Success** - Scans authenticate successfully with full administrator/root privileges. Scan results are the most comprehensive. • **Success but Insufficient Access** - Scans authenticate successfully, but do not have privileged access. Scan results are limited to the scope of a local non-privileged user. • **Success but Intermittent Failure** - Scan credentials intermittently fail, which result from session rate limits, session concurrency limits, or other issues preventing consistent authentication success. • **Authentication Failure (Credentials)** - Incorrect credentials provided. • To view the list of assets that falls in a specific category, click the required category. The **Findings** page appears with details about assets detected for the category. • To export the data in the widget, click the ⋮ button and select a format.
Vulnerability Age:	This widget provides a view of vulnerabilities based on severity

and age. The columns display counts of published vulnerabilities within the specified time period present in the organization. The rows display the severity level of the vulnerability.

- To view asset details for a specific category, click vulnerability count in the required category.

  The **Findings** page appears with details about assets detected for the category.

- To export the data in the widget, click the ⋮ button and select a format.

Tenable Web App Scanning Dashboard

The default **Web Applications Scanning** dashboard displays data Tenable Web App Scanning collects.

The tables below describes the sections and widgets displayed in the **Web Applications Scanning** dashboard. You can view details about the data in a widget by clicking the widget.

Tenable Web App Scanning Statistics

The table below describes the widgets displayed in the Statistics section of the **Web Applications Scanning** dashboard. You can view details about the data in a widget by clicking the widget.

Widget	Description
Findings	Number of findings Tenable Web App Scanning has discovered. The findings are categorized by severity (**Critical** and **High**). For information about vulnerability ratings and the severity metrics Tenable uses to analyze risk, see Severity vs. VPR in the *Tenable Vulnerability Management User Guide*.
Web Assets Scanned	Number of assets scanned over time.
Incomplete Scans	Number of incomplete scans in the past 90 days.

Widget	Description
Non Authenticated Scans	Number of non-authenticated scans in the past 90 days.

OWASP Top 10

This chart displays the vulnerabilities discovered by Tenable Web App Scanning that appear in the latest Open Web Application Security Project (OWASP) Top 10 Most Critical Web Application Security Risks document.

View the Dashboards Page

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable Vulnerability Management updates dashboard data based on date filters you add when you Create a Custom Widget for the dashboard.

To view the Dashboards page:

1. Access the **Dashboards** page in one of the following ways:
   - On any Tenable-provided dashboard page, click the **Dashboards** button.
   - On any other page, do the following:
     a. In the upper-left corner, click the button.

        The left navigation plane appears.

     b. In the left navigation plane, click **Dashboards**.

   The **Dashboards** page appears. The page contains tiles that represent:

- Tenable-provided dashboards
- Dashboards you have created
- Dashboards that other users have shared with you

2. Do any of the following:
    - In the upper-left corner, use the **Search** bar to search for specific dashboards.
    - In the upper-left corner, use the drop-down to change the order in which dashboards appear on the **Dashboards** page.
    - In the **Groups** section, do any of the following:
        - Use the **Search Groups** bar to search for specific dashboard groups.
        - Click the **Shared with Me** tab to view dashboards that have been shared with you.
        - Click the **Updates Available** tab to view dashboards that are eligible for auto-update.
    - Roll over individual dashboard tiles to reveal additional information.
    - Toggle between the grid and list view.
    - Set a default dashboard.
    - Edit a dashboard.
    - Share a dashboard.
    - Export a dashboard.
    - Duplicate a dashboard.
    - Delete a dashboard.
    - Click a dashboard tile to view the individual dashboard.

Tenable-Provided Dashboards

On the **Dashboards** page, Tenable Vulnerability Management shows dashboards in the following order:

1. Tenable-provided dashboards. For a complete index of Tenable-provided dashboard templates, see Tenable Vulnerability Management Dashboards.
2. Dashboards you create and dashboards that have been shared with you.

Note: You can change the order in which dashboards appear by using the drop-down in the upper-right corner of the **Dashboards** page.

The Tenable-provided dashboards you see depend on the licenses you have, but can include the following:

Dashboard	License
Vulnerability Management Overview	Tenable Vulnerability Management
Lumin	Tenable Lumin
Web Application Scanning	Tenable Web App Scanning

Note: You can export the **Vulnerability Management Overview** and **Asset View** dashboard landing pages, or export individual widgets on those dashboards. For more information, see Export a Full Dashboard and Export an Individual Dashboard Widget.

Note: If your dashboard fails to show data, you may be filtering the dashboard by a target group with too many targets. Tenable recommends limiting the number of targets in any individual target group.

Export a Full Dashboard Landing Page

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

In Tenable Vulnerability Management, you can export the following dashboard landing pages:

- Vulnerability Management Overview
- Tenable Lumin
- Tenable Web App Scanning

To export a full dashboard landing page:

1. View the dashboard page you want to export.
2. In the upper-right corner, click **Export**.

   A drop-down menu appears.
3. From the drop-down menu, select one of the following options:
   - Click **PDF** to export the dashboard in PDF format.
   - Click **PNG** to export the dashboard in PNG format.
   - Click **JPG** to export the dashboard in JPG format.

   An **In Progress** message appears.

   Once the export completes, a **Success** message appears and Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

Export an Individual Dashboard Widget

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

In Tenable Vulnerability Management, you can export individual widgets from the following dashboard landing pages:

- Vulnerability Management Overview
- Tenable Lumin
- Tenable Web App Scanning

To export an individual dashboard widget:

1. View the dashboard page that contains the widget you want to export.
2. In the header of the widget you want to export, click the ••• button.

   A drop-down menu appears.

3. From the drop-down menu, select one of the following options:

    - Click **PDF** to export the dashboard in PDF format.
    - Click **PNG** to export the dashboard in PNG format.
    - Click **JPG** to export the dashboard in JPG format.

    An **In Progress** message appears.

    Once the export completes, a **Success** message appears and Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

View an Individual Dashboard

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable Vulnerability Management updates dashboard data every time you run a scan.

To view an individual dashboard:

1. View the **Dashboards** page.
2. Do one of the following:

    - In grid view, roll over the tile for the dashboard you want to view.

      Dashboard information and options overlay the dashboard tile.
    - In list view, roll over the thumbnail dashboard image for the dashboard you want to view.

      Dashboard options overlay the thumbnail dashboard image.

3. Click **View**.

    The page for that dashboard appears.

4. Do one of the following:

    - Change the dashboard you are viewing:

        a. In the upper-right corner, click **Jump to Dashboard**.

        A drop-down box appears.

b. Select the dashboard you want to view.

> **Tip:** Use this option to view legacy versions of Explore dashboards. For more information, see Enable Explore Dashboards

- Roll over individual widgets to reveal additional information.
- Click on widget elements to drill down into details behind the data.
- Share the dashboard.
- Export the dashboard.
- Edit the dashboard.
- Set the dashboard as default.
- Duplicate the dashboard.
- Create a new dashboard.
- Delete the dashboard.

View the Dashboard Template Library

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

The **Template Library** provides a selection of Tenable-provided dashboards.

To view the dashboard template library:

1. View the **Dashboards** page.
2. Click ⊕ **New Dashboard**.

   A list of options appears.

3. Click **Template Library**.

   The **Template Library** page appears.

   On the **Template Library** page, you can:

- Sort the **Template Library** page:
  a. In the upper-right corner of the page, click the ⌄ button in the drop-down box.
  b. Select the criteria by which you want to sort the page.
- In the upper-left corner, use the **Search** bar to search for specific dashboards.
- Click the **New and Updated** tab to view dashboards that are eligible for auto-update.
- Toggle between the grid and list view.
- Preview a dashboard.
- Create a dashboard.

Create a Dashboard

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, Administrator, or Custom Role with appropriate privileges

You can create a custom dashboard or use the **Template Library** to create a copy from the available templates. Dashboards let you drill down to view the details of each widget.

Important: The **Template Library** in Tenable Vulnerability Management includes **Explore** dashboard templates. The **Explore** dashboard templates are marked with **Explore** at the end of the template name. For example: **Vulnerability Management (Explore)**. From the dashboards that you create using these templates, you can drill down to the **Findings** or **Assets** pages. To add an **Explore** dashboard, see Enable Explore Dashboards.

To create a dashboard:

1. View the **Dashboards** page.
2. Click ⊕ **New Dashboard**.

   A list of options appears.
3. Do one of the following:

   To create a dashboard from a template:

a. Click **Template Library**.

   The **Template Library** page appears.

b. In the **Groups** panel on the left, click the group name to view the templates for the category.

Category	Description
Center for Internet Security (CIS)	CIS Benchmarks are best practices for the secure configuration of a target system. Be sure to use the proper audit file for scans.
Defense Information Systems Agency (DISA)	The Defense Information Systems Agency (DISA) is a United States Department of Defense combat support agency composed of military, federal civilians, and contractors. Security Technical Implementation Guides (STIG) is a configuration standard that consists of cybersecurity requirements for a specific product. Be sure to use the proper audit file for scans.
Compliance Framework	Tenable allows you to audit configuration compliance with a variety of standards including GDPR, ISO 27000, HIPAA, NIST 800-53, PCI DSS, and so on. These reports provide summary and detailed information for all the supported frameworks. Be sure to use the proper audit file for scans.
Host Audit Plugin Type	Organizations such as CIS, DISA, and some vendors create golden configurations standards, known as benchmarks. Tenable creates audit files that perform a detailed configuration review. Scanning the assets with the Host Audit Compliance Check plugins allows you to do detailed configuration checks. These reports provide summary and detailed information for all the Host Audit Compliance Check plugins.
Tenable Best Practice Audits	Allows you to implement best practice audits for new technologies. Be sure to use the proper audit file for scans.

Vendor Based Audits	Allows you to implement vendor-specific guidance for new technologies. Vendors include: Vendor, IBM, Juniper, Microsoft, NetApp, VMware, and others. Be sure to use the proper audit file for scans.
Vulnerability Management	Tenable Vulnerability Management provides the most comprehensive vulnerability coverage with real-time continuous assessment of the organization. These built-in reports allow organizations to communicate risk based on prioritization, threat intelligence and real-time insights to prioritize remediation actions. These reports provide summary and detailed information on data collected using Tenable Vulnerability Management applications such as Tenable Nessus.
Web App Scanning	Web application security provides the ability to detect and mitigate threats and vulnerabilities that may compromise the confidentiality, integrity, and availability of web applications. These reports leverage data from Tenable Web App Scanning, a comprehensive and automated vulnerability scanning tool for modern web applications.

c. In the library, locate the template you want to use.

d. Hover over the template.

   An overlay of template information and options appears.

e. (Optional) To preview the dashboard template, click **Preview**. For more information, see Preview a Dashboard.

f. Click ⊕ **Add**.

   An **Added dashboard to Dashboards** confirmation message appears.

   The new dashboard appears on the **Dashboards** page with the name **Copy of *selected dashboard***.

To create a custom dashboard:

a. Click **Custom Dashboard**.

   The **Edit Dashboard** page appears.

b. Name the dashboard:

   a. Click the name of the dashboard.

      The name becomes an editable text box.

   b. Type a name for the dashboard.

   c. Click the ✓ button to confirm the name change.

      Tenable Vulnerability Management saves the updated name.

c. Add a dashboard description:

   a. Click the dashboard description.

      The description becomes an editable text box.

   b. Type a description for the dashboard.

d. Add widgets to the dashboard:

   a. In the upper-right corner of the page, click ⊕ **Add Widgets**.

      A menu appears.

   b. Do one of the following:

      - To add a widget from a template, click **Template Widget**.

        The **Widgets** page appears.

        ◦ Select the widget as described in Add a Widget to a Dashboard.

      - To add a custom widget, click **Custom Widget**.

        The **Create Widget** page appears.

        ◦ Configure the custom widget as described in Create a Custom Widget.

e. Add dashboard filters:

a. In the upper-right corner of the page, click **Edit Filter**.

   The **Filter** plane appears.

   > **Note:** The **Edit Filter** option does not appear if there are no widgets added to the dashboard.

b. Configure your dashboard filters as described in Filter a Dashboard.

f. (Optional) Reorder widgets on the dashboard:

   a. Hover over the widget you want to move.

   b. Press and hold the mouse button to highlight the widget.

      The edges of the widget become defined and exhibit a raised appearance.

   c. Using the mouse, drag the widget to the new location.

   d. Release the mouse button to drop the widget in the new location.

g. (Optional) Delete the dashboard:

   - In the lower-left corner of the page, click **Delete Dashboard**.

     Tenable Vulnerability Management discards the newly created dashboard.

What to do next:

- Manage Dashboards

Preview a Dashboard

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

When creating a new dashboard from a template, you can preview the dashboard before adding it to the **Dashboards** page.

To preview a dashboard:

1. Create a dashboard.
2. In the **Template Library**, roll over the template you want to preview.

   An overlay of template information and options appears.
3. Click **Preview**.

   A preview of the dashboard appears.
4. To exit the preview, in the top navigation bar, click a link in the breadcrumb trail to return to the **Template Library**, or the **Dashboards** page.
5. To add the template to the **Dashboards** page, click ⊕ **Add to Dashboards**.

   An **Added dashboard to Dashboards** confirmation message appears, and the new dashboard appears on the **Dashboards** page with the name **Copy of *selected dashboard***.

Enable Explore Dashboards

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

To use **Explore** dashboards within Tenable Vulnerability Management, you must first add them to your interface via the **Template Library**.

Note: The numerical data that appears on your Explore dashboards may not match the data on your legacy Tenable Web App Scanning or VM dashboards.

Note: The data on your Explore Tenable Web App Scanning and VM dashboards reflects your complete scanning history. This differs from the Tenable Web App Scanning and VM dashboards, which display data for only the last 30 calendar days.

To enable Explore dashboards:

1. View the **Dashboards** page.
2. Click ⊕ **New Dashboard**.

   A list of options appears.
3. Click **Template Library**.

The **Template Library** page appears.

4. In the upper-left corner, in the **Search** bar, type "(Explore)".

   All available **Explore** dashboards appear.

   > If **Explore** dashboards do not appear, your container may not have enabled them. Please contact your Customer Success Manager.

5. For each **Explore** dashboard you want to add to your interface, do the following:

   a. Roll over the Explore dashboard template.

      An overlay of template information and options appears.

   b. Click ⊕ **Add**.

      An **Added dashboard to Dashboards** confirmation message appears, and the **Explore** dashboard appears on the **Dashboards** page.

> **Note:** To reenable your Tenable Web App Scanning or VM dashboards, enable the corresponding workbench.

Manage Dashboards

This section contains the following topics to help you manage your Tenable Vulnerability Management dashboards:

Dashboard Groups

In Tenable Vulnerability Management, you can organize dashboards into groups via the dashboard **Groups** panel. This allows you to track different types of dashboards, and dashboards that others have shared with you. You can also share a dashboard group with one or more users or user groups.

The **Groups** panel automatically expands when you view the **Dashboards** page. The panel is separated by Tenable-provided dashboard groups and user-created dashboard groups.

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

Add a Dashboard Group

You can add a dashboard group via the **Groups** panel on the **Dashboards** page.

To add a dashboard group:

1. View the **Dashboards** page.

   By default, the **Groups** panel expands.

2. In the **Groups** panel, click ⊕**Add**.

   The **Edit Group** pane appears.

3. In the **Group Name** box, type a name for your dashboard group.

4. In the **Dashboards to Include** section, select the check box next to any dashboards you want to add to the dashboard group.

5. Click **Save**.

   Tenable Vulnerability Management adds the dashboard group to the user-created dashboard list in the **Groups** panel.

Share a Dashboard Group

In Tenable Vulnerability Management, you can share user-created dashboard group with other users or user groups via the **Groups** panel.

Note: Dashboard groups are not automatically re-shared with a user after they have been updated. For example:
User A shares a dashboard group with User B. User A then makes a change to the dashboard group. To see the update, User A must re-share the dashboard group, with User B.

Note: Shared content may appear differently to the users with which it is shared based on the access group to which they belong.

To share a dashboard group:

1. View the **Dashboards** page.

   By default, the **Groups** panel expands.

2. In the **Groups** panel, click the user-created dashboard group you want to share.

   The group and its included dashboards appears.

3. Click **Share Group**.

   The **Share Group** pane appears.

4. Do one of the following:

   - To share the dashboard group with all users, select the **All Users** check box.
   - To share the dashboard group with specific users or user groups, from the drop-down box, select the users or user groups with which you want to share the dashboard group.

     Tip: You can share with multiple users or user groups.

5. Click **Share**.

   A **Group shared successfully** message appears. Tenable Vulnerability Management shares the dashboard group with the designated users or user groups and sends an email indicating that you shared a dashboard with them.

Edit a Dashboard Group

In Tenable Vulnerability Management, you can edit user-created dashboard groups via the **Groups** panel.

To edit a dashboard group:

1. View the **Dashboards** page.

   By default, the **Groups** panel expands.

2. In the **Groups** panel, click the user-created dashboard group you want to edit.

   The group and its included dashboards appears.

3. Click **Edit Group**.

The **Edit Group** pane appears.

4. (Optional) In the **Group Name** box, edit the name of the dashboard group.
5. (Optional) In the **Dashboards to Include** section, select or deselect the dashboards that appear in the dashboard group.
6. Click **Save**.

   Tenable Vulnerability Management saves your changes to the dashboard group.

Delete a Dashboard Group

In Tenable Vulnerability Management, you can delete user-created dashboard groups via the **Groups** panel.

To delete a dashboard group:

1. View the **Dashboards** page.

   By default, the **Groups** panel expands.

2. In the **Groups** panel, click the user-created dashboard group you want to delete.

   The group and its included dashboards appear.

3. Click **Delete Group**.

   A confirmation message appears.

4. Click **Delete**.

   Tenable Vulnerability Management deletes the dashboard group.

   > **Note**: Deleting dashboard groups does not delete the dashboards within the group.

Automatically Update Widgets on a Dashboard

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To provide the most up-to-date vulnerability information, Tenable updates or adds new dashboard widgets when, for example, a new vulnerability is exposed or when Tenable Vulnerability

Management adds a new vulnerability filter. When Tenable updates these widgets, you can view and automatically update them in one of the following ways:

- **Dashboards** page – On the **Dashboards** page, you can update all updated widgets on a dashboard at one time.
- Dashboard **Template Library** – When creating a custom dashboard via the **Template Library**, you can view new or updated widgets and add them to the custom dashboard.

  Note: On predefined dashboard templates, Tenable Vulnerability Management always includes the most recent version of widgets.

- **Widget Library** – In the **Widget Library**, you can view new or updated widgets and add them to up to ten individual dashboards.

To update widgets automatically via the **Dashboards** page:

1. View the **Dashboards** page.
2. In the **Groups** section, click the **Updates Available** tab.

   A list of dashboards with updated widgets appears.

   Note: You can also see dashboards with new and updated widgets on the **All** tab. These dashboards appear with a pulsing blue dot next to the dashboard name.

3. Roll over the dashboard for which you want to update widgets.

   An overlay of options appears.

4. Click **Apply**.

   An **Update Available** message appears that describes the updates to the widgets on the dashboard.

5. Click **Update**.

   An **Update Applied Successfully** message appears and Tenable Vulnerability Management updates the widgets on the dashboard.

To update widgets automatically via the dashboard **Template Library**:

1. View the dashboard **Template Library**.
2. Click the **New and Updated** tab.

   A list of dashboard templates with new and updated widgets appears.
3. Roll over the dashboard template you want to add.

   An overlay of options appears.
4. Click **Add**.

   An **Added Dashboard Template to Dashboards** message appears, and the dashboard template with the new or updated widget appears on the **Dashboards** page.

To update widgets automatically via the **Widget Library**:

1. View the **Widget Library**.
2. Click the **New and Updated** tab.

   A list of new and updated widgets appears.
3. Roll over any widget you want to add to a dashboard.
4. Click **Add to Dashboards**.

   The **Add to Dashboards** plane appears.
5. In the **Dashboards** drop-down, select the dashboard or dashboards to which you want to add the new or updated widget.
6. Click **Save**.

   A **Successfully Added to Selected Dashboards** message appears and Tenable Vulnerability Management adds the new or updated widget to the selected dashboards.

Edit a Dashboard

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To edit a dashboard:

1. Do one of the following:

   - Access the **Edit Dashboard** page via the **Dashboards** page:

     a. View the **Dashboards** page.

     b. In the dashboard header, click the ⋮ button.

        A drop-down list appears.

     c. Click **Edit**.

   - Access the **Edit Dashboard** page via an individual dashboard:

     a. View the dashboard you want to edit.

     b. In the dashboard header, click the **More** ⌄ button.

        > **Note:** The **More** button is not available on Tenable-provided dashboards.

        A drop-down appears.

     c. Click ✎ **Edit dashboard**.

   The **Edit Dashboard** page appears.

2. On the **Edit Dashboard** page, do any of the following:

   - Rename the dashboard:

     a. Click the name of the dashboard.

        The name becomes an editable text box.

     b. Type a new name for the dashboard.

     c. Click the ✓ button to confirm the name change.

        Tenable Vulnerability Management saves the name.

   - Edit the dashboard description:

a. Click the dashboard description.

   The description becomes an editable text box.

b. Type a new description for the dashboard.

- Edit the dashboard filters:

a. In the upper-right corner of the page, click **Edit Filter**.

   The **Filter** plane appears.

b. Configure your dashboard filters as described in Filter a Dashboard.

- Add widgets to the dashboard:

a. In the upper-right corner of the page, click **Add Widgets**.

   A menu appears.

b. Do one of the following:

   - To add a widget from a template, click **Template Widget**.

     The **Widgets** page appears.

     - Select the widget as described in Add a Widget to a Dashboard.

   - To add a custom widget, click **Custom Widget**.

     The **Create Widget** page appears.

     - Configure the custom widget as described in Create a Custom Widget.

- Reorder widgets on the dashboard:

a. Roll over the top of the widget until the move cursor appears.

b. Click and drag the widget to the desired location.

- Resize the widgets on the dashboard:

a. Roll over the lower-right corner of the widget until the resize cursor appears.

b. Click and drag the widget to the desired size.

The widgets shift to accommodate the new widget size.

- Delete the dashboard:
  - In the lower-left corner of the page, click **Delete Dashboard**.

    Tenable Vulnerability Management removes the dashboard from the **Dashboards** page.

3. Click **Done Editing**.

   You return to the selected dashboard and Tenable Vulnerability Management applies your changes. If the dashboard is shared with other users, those users automatically receive the updated dashboard.

Set a Default Dashboard

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can set any dashboard as the default dashboard to make it your landing page. If you do not set a default dashboard, Tenable Vulnerability Management uses the Tenable-provided **Vulnerability Management Overview** dashboard as the default.

When you set a dashboard as default, on the **Dashboards** page, the **Default** label appears in the header of the dashboard tile.

Note: If you delete a dashboard set as default, the product Tenable-provided dashboard becomes the default.

To set a default dashboard:

1. Do one of the following:
   - Set a default dashboard via the **Dashboards** page:
     a. View the **Dashboards** page.
     b. In the dashboard tile header, click the ⋮ button.

- Set a default dashboard via an individual dashboard:

  a. View the dashboard you want to make the default.

  b. In the dashboard header, click the **More** button.

A drop-down list appears.

2. Select **Make Default**.

   A **Successfully set as default dashboard** confirmation message appears, and Tenable Vulnerability Management sets the dashboard as the default.

   Note: You may have to log out and log back in to see the updated default dashboard.

Rename a Dashboard

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

To rename a dashboard:

1. View the dashboard you want to rename.
2. On the dashboard page, roll over the dashboard name.

   The name becomes highlighted and shows a button.

3. Click the button or double-click the name.

   The name field becomes a text box.

4. Enter a new name for the dashboard.
5. Click the button to confirm the name change.

   A confirmation appears at the top of the page.

   The new name appears.

Duplicate a Dashboard

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Web App Scanning User Role: Scan Operator, Standard, Scan Manager, or Administrator

To duplicate a dashboard:

1. Do one of the following:

   - To duplicate a dashboard via the **Dashboards** page:

     a. View the **Dashboards** page.

     b. In the dashboard header, click the ⋮ button.

     A drop-down list appears.

   - To duplicate a dashboard via an individual dashboard:

     a. View the dashboard you want to duplicate.

     b. In the dashboard header, click the **More** ⌄ button.

     A drop-down list appears.

2. Click **Duplicate**.

   A **Successfully copied the dashboard** confirmation message appears, and Tenable Vulnerability Management copies the dashboard on the **Dashboards** page.

Filter a Dashboard

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can apply filters at the dashboard level to all widgets within that dashboard.

Note: You can apply configurations to individual widgets. The widget-level configuration takes precedence over dashboard-level configuration.

To filter a dashboard in the new interface:

1. View the dashboard you want to filter.
2. In the dashboard header, click the **More** button.

   Note: The **More** button is not available on Tenable-provided dashboards.

   A drop-down appears.
3. Click **Filter**.

   The **Filter** plane appears.
4. In the **Select Filter Type** drop-down, select the assets you want the dashboard to analyze. See the following table for options and requirements.

Option	Description	Requirement
All Assets	(Default) This option includes all the assets in the dashboard.	This is the default option and includes all assets in the dashboard. There is not a requirement for this option.
Target Group	This option only includes assets in a specific target group.	An extra field for **Select Target Groups** appears when you select this option. Select the desired target group from the drop-down list.
Custom	This option only includes assets with a specific hostname, IP address, FQDN, or CIDR.	A text box appears when you select this option. Enter one or more of the custom option formats (hostname, IP address, FQDN, or CIDR). Separate multiple items with commas. **Important**: Make sure that the number of IP addresses in your search filter is less than or equal to 25. **Important:** Make sure that the number of Hostnames in your search

		filter is less than or equal to 300.

5. Click **Apply**.

   The ▽ icon appears in the header of all the dashboard widgets.

6. In the widgets section, roll over the ▽ icon to view the added filter.

Note: The following are the filtering limitations for **Explore** widgets:

- **Explore** widgets do not support **Target Groups**.
- **Cloud Misconfigurations** widgets do not support filtering by IP or hostname.
- **Cloud Misconfigurations** and **Web Application Findings** widgets do not support tags.

Note: You can filter only with the tags you can access. You cannot apply tags that you do not have access to.

Filter a Dashboard by Time

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can filter a dashboard to show only vulnerabilities within a specific timeframe – in hours, days, months, or years. Filters are available only for custom dashboards or dashboards created using the template library.

Note: Filter by time option is available only for Explore dashboards and Explore widgets.

To filter a dashboard by a specific timeframe:

1. View the dashboard you want to filter.
2. To filter your dashboard data for a specific timeframe, do one of the following:
   - In the **All** drop-down box, select the required timeframe: **All**, **7 days ago**, **14 days ago**, **30 days ago**, **60 days ago**, **90 days ago**.

- For a custom timeframe, in the **Last Seen** box, type the value to view the data within the last number of days, hours, years, or months.

Tenable Vulnerability Management displays the vulnerabilities for the selected timeframe on the dashboard.

Share a Dashboard

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, Administrator, or Custom Role with appropriate privileges

Tenable Vulnerability Management users can share a dashboard with one or more users, or one or more user groups. Shared dashboards appear automatically for the users or groups with which they are shared. Additionally, when you update a shared dashboard, the users with which it is shared automatically receive the updated dashboard.

Note: You cannot edit dashboards that are shared with you. You can, however, duplicate or delete a dashboard that is shared with you.

Note: Shared content may appear differently to the users with which it is shared based on the access group to which they belong.

To share a dashboard:

1. Do one of the following:
   - To share a dashboard via the **Dashboards** page:
     a. View the **Dashboards** page.
     b. In the dashboard tile header, click the ⋮ button.

        A drop-down list appears.

     c. Click **Share**.
   - To share a dashboard via an individual dashboard:

a. View the dashboard you want to share.

b. In the upper-right corner, click **Share**.

The **Share** panel appears,

2. Do one of the following:

   - To share the dashboard with all users, select the **All Users** check box.
   - To share the dashboard with specific users or user groups, from the drop-down box, select the users or user groups with which you want to share the dashboard.

     Tip: You can share with multiple users or user groups.

3. Click **Share**.

   A **Dashboard shared successfully** message appears. Tenable Vulnerability Management shares the dashboard with the designated users or user groups and sends an email indicating that a dashboard has been shared with them.

Manage Dashboard Exports

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

With the export feature, you can export dashboard data in CSV, PDF, and detailed PDF formats. You can create dashboard exports on demand or schedule automated exports to specified recipients.

You can also manage your dashboard exports. You can download them, view your export history, delete your exports, or delete their configuration.

Note: While you cannot export the **Vulnerability Management Overview** and **Asset View** dashboards, you can export their associated landing pages, or export individual widgets on those dashboards. For more information, see Export a Full Dashboard Landing Page and Export an Individual Dashboard Widget.

Export a Dashboard

To export a dashboard in CSV format:

1. Do one of the following:

   - Export the dashboard via the **Dashboards** page:

     a. View the **Dashboards** page.

     b. In the dashboard header, click the ⋮ button.

        A drop-down list appears.

     c. Click **Export to CSV**.

   - Export the dashboard while viewing the individual dashboard:

     a. View the dashboard you want to export.

     b. In the upper-right corner, click **Export**.

        A drop-down list appears.

     c. Click **CSV**.

   An **Export in Progress** confirmation message appears.

   The export request and status appears in the **Downloads** section on the **Exports** plane.

   When the export completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

To export a dashboard in PDF format:

You can use the **Export PDF** feature to share customized dashboards externally. The exported PDF is a generated report of the selected dashboard.

To export a PDF:

1. Do one of the following:

   - Export the dashboard via the **Dashboards** page:

     a. View the **Dashboards** page.

     b. In the dashboard header, click the ⋮ button.

        A drop-down list appears.

     c. Click **Export to PDF** or, where available, **Export to PDF - Detailed**.

        Note: By default, the following dashboards support **PDF-Detailed** exports:

        - Executive Summary
        - Exploitable by Malware
        - Exploitable Framework Analysis
        - Measuring Vulnerability Management
        - Mitigation Summary
        - Outstanding Remediation Tracking
        - Prioritize Assets
        - Vulnerabilities by Common Ports
        - Vulnerability Management
        - Web Services

   - Export the dashboard via an individual dashboard:

     a. View the dashboard you want to export.

     b. In the upper-right corner, click [→ **Export**.

        A drop-down list appears.

     c. Click **PDF** or, where available, **PDF - Detailed**.

Note: The **PDF** report contains the displayed information for the selected dashboard. The information that you see on the screen is the information that is included in the report.

The **PDF - Detailed** report has in-depth information, including vulnerability details, that goes beyond the items displayed.

Note: If you select **PDF - Detailed** and there are user-created filters applied to one or more widgets on the dashboard, a **Confirm Export** message appears indicating that Tenable Vulnerability Management does not apply user-created filters to any additional chapters. Click **Confirm** to continue with the export.

An **Export in Progress** confirmation message appears.

The export request and status appears in the **Downloads** section on the **Exports** plane.

When the export completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

To schedule a dashboard export:

The **Schedule Export** option allows you to export a dashboard at specified times.

To schedule an export:

1. Do one of the following:
   - Access the **Schedule Export** plane via the **Dashboards** page:
     a. View the **Dashboards** page.
     b. In the dashboard header, click the ⋮ button.

        A drop-down list appears.
     c. Click **Schedule Export**.
   - Access the **Schedule Export** plane via an individual dashboard:
     a. View the dashboard you want to export.
     b. In the upper-right corner, click [→ **Export**.

        A drop-down list appears.
     c. From the drop-down list, click **Schedule**.

The **Schedule Export** plane appears.

2. Do one of the following:

   - If you have never exported and/or scheduled an export for the dashboard, the **Schedule** options automatically appear.
   - If you have already exported the dashboard, in the **Schedule** section, click ⊕ **Add New**.

     The **Schedule** options appear.
   - If you have already scheduled an export for the dashboard, you cannot create another one. You must first cancel the scheduled dashboard export.

3. Select **CSV**, **PDF** or, where available, **PDF - Detailed**.

   Note: The **PDF** report contains the displayed information for the selected dashboard. The information that you see on the screen is the information included in the report.

   The **PDF - Detailed** report has in-depth information, including vulnerability details, that goes beyond the items displayed.

   Note: If you select **PDF - Detailed** and there are user-created filters applied to one or more widgets on the dashboard, a **Confirm Export** message appears indicating that Tenable Vulnerability Management does not apply user-created filters to any additional chapters. Click **Confirm** to continue with the export.

4. In the **Schedule** section, set the following parameters:

Option	Description
Name	A name for the scheduled export.
Start Date and Time	The date and time that you want the export to begin.
Repeat	The frequency that you want Tenable Vulnerability Management to send the export: • **Daily** – The export occurs daily at the time specified. • **Weekly** – The export occurs every week on the same day

	at the time specified (for example, Weekly on Tuesday). • **Monthly** – The export occurs once a month on the day of the week and time specified (for example Monthly on Last Tuesday) • **Custom** – The export occurs at a custom interval. If you select **Custom**, more options appear: a. In the **Repeat Every** section, in the drop-down, select how often you want the export to repeat. For example, if you want the export to repeat every 2 days, then in the first drop-down box, select **2** and in the second drop-down box, select **Days**. • **Does not Repeat** – The export does not repeat.
Password Protection	Specifies the export as encrypted or unencrypted. If you toggle this option on, an **Encryption Password** box appears. Type the password you want to use to encrypt the export file. **Note:** Once you save the scheduled export, you cannot edit the **Encryption Password**. Instead, you must create a copy of the dashboard, create a scheduled export, and then select the desired password.
Add Recipients	(Optional) The email address for the person that receives the report. You can specify multiple email addresses as a comma-separated list.

5. Click **Schedule**.

   The scheduled export appears in the **Schedule Export** plane.

Download a Dashboard Export

To download a dashboard export:

1. Do one of the following:

   - Access the **Schedule Export** plane via the **Dashboards** page:

     a. View the **Dashboards** page.

     b. In the dashboard header, click the ⋮ button.

        A drop-down list appears.

     c. Click **Export**.

   - Access the **Schedule Export** plane via an individual dashboard:

     a. View the dashboard with the export you want to download.

     b. In the upper-right corner, click **Export**.

        A drop-down list appears.

     c. From the drop-down list, click **Schedule**.

   The **Schedule Export** plane appears.

2. In the **Downloads** section, next to the export download you want to download, click the ⬇ button.

   Tenable Vulnerability Management downloads the export file to your computer.

View Dashboard Export History

To view dashboard export history:

1. View the dashboard for which you want to view export history.
2. In the upper-right corner, click [→ **Export**.

   A drop-down list appears.

3. In the drop-down list, click **History**.

   The **Export History** plane appears.
   On the **Export History** plane, you can view:

- The schedule for the dashboard export.
- Available downloads of previous dashboard exports.

> You cannot access the **Export History** plane if the dashboard has not yet been exported.

Delete a Dashboard Export Download

To delete a dashboard export download:

1. Do one of the following:
   - Access the **Schedule Export** plane via the **Dashboards** page:
     a. View the **Dashboards** page.
     b. In the dashboard header, click the ⋮ button.

        A drop-down list appears.
     c. Click **Export**.
   - Access the **Schedule Export** plane via an individual dashboard:
     a. View the dashboard for which you want to delete an export.
     b. In the upper-right corner, click **Export**.

        A drop-down list appears.
     c. From the drop-down list, click **Schedule**.

   The **Schedule Export** plane appears.
2. In the **Downloads** section, roll over the export download you want to delete.
3. Click the 🗑 button.

   A **Confirm Deletion** message appears.
4. Click **Delete**.

   A **Download deleted successfully** message appears and Tenable Vulnerability Management removes the export download from the **Schedule Export** plane.

Delete a Dashboard Export Configuration

To delete a dashboard export configuration:

1. Do one of the following:

   - Access the **Schedule Export** plane via the **Dashboards** page:

     a. View the **Dashboards** page.

     b. In the dashboard header, click the ⋮ button.

     A drop-down list appears.

     c. Click **Export**.

   - Access the **Schedule Export** plane via an individual dashboard:

     a. View the dashboard for which you want to delete a scheduled export.

     b. In the upper-right corner, click **Export**.

     A drop-down list appears.

     c. From the drop-down list, click **Schedule**.

   The **Schedule Export** plane appears.

2. In the **Schedule** section, roll over the scheduled export configuration you want to delete.
3. Click the 🗑 button.

   A **Confirm Deletion** message appears.

4. Click **Confirm**.

   A **Successfully deleted export configuration** message appears and Tenable Vulnerability Management removes the export configuration from the **Schedule** section of the **Schedule Export** plane.

Delete a Dashboard

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Note: In Tenable Vulnerability Management, you can only delete custom dashboards. You cannot delete Tenable-Provided Dashboards.

To delete a dashboard:

1. Do one of the following:

   - Delete a dashboard from the **Dashboards** page:

     a. View the **Dashboards** page.

     b. In the dashboard tile header, click the ⋮ button.

   - Delete a dashboard from the individual dashboard:

     a. View the dashboard page you want to delete.

     b. In the dashboard header, click the **More** ⌄ button.

   A drop-down list appears.

2. Click **Delete**.

   A **Confirm Deletion** confirmation message appears.

3. Click **Delete**.

   A **Successfully deleted the dashboard** confirmation message appears and Tenable Vulnerability Management removes the dashboard from the **Dashboards** page.

Manage Widgets

You can use the widget library to create and edit widgets to use across your dashboards.

To manage widgets in the widget library:

- View the Widget Library
- Create a Custom Widget
- Edit a Custom Widget
- Add a Widget to a Dashboard

On your dashboards, you can further configure widgets to modify your dashboards.

To manage widgets on a dashboard:

- Configure a Widget
- Duplicate a Widget
- Rename a Widget
- Delete a Widget from a Dashboard

View the Widget Library

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

The widget library provides a selection of Tenable-provided widgets to add to your template-based or custom dashboard.

Note: The Tenable-provided **Vulnerability Trending** widget is not available in the widget library. All other Tenable-provided widgets appear in the widget library.

To view the widget library:

1. View the **Dashboards** page.
2. In the upper-right corner of the page, click the **Widget Library** button.

   The **Widgets** page appears.
3. (Optional) In the upper-left corner of the page, click the tab for the dashboard widgets you want to view. For example, if you want to only widgets associated with Tenable Vulnerability Management, click the **Vulnerability Management** tab.

   Note: The tabs that appear on the **Widgets** page depend on the licenses (for example, Tenable Lumin, Tenable Web App Scanning) you have enabled in Tenable Vulnerability Management.

   On the **Widgets** page you can:

   - Sort the **Widgets** page:
     a. In the upper-right corner of the page, click the button in the drop-down box.
     b. Select the criteria by which you want to sort the widgets page.
   - In the upper-left corner, use the **Search** bar to search for specific widgets.

- Click the **New and Updated** tab to view dashboard widgets that are eligible for auto-update.
- Add the widget to a dashboard.
- Delete a widget from the widget library.

Delete a Widget from the Widget Library

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Note: You can only delete custom widgets. You cannot delete pre-configured Tenable Vulnerability Management widgets.

To delete a custom widget:

1. View the widget library.
2. Click the **My Widgets** tab.

   All user-created widgets appear.
3. In the header of the widget you want to delete, click the ⋮ button.

   A drop-down menu appears.
4. Click **Delete**.

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

   Tenable Vulnerability Management removes the widget from the widget plane, and a message confirming the deletion appears at the top of the plane.

Create a Custom Widget

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

In Tenable Vulnerability Management, you can create custom widgets to add to dashboards you define, giving you custom views of your data.

To create a custom widget:

1. Do one of the following:

   - Create a custom widget via the widget library:

     a. View the widget library.

     b. In the upper-right corner of the page, click ⊕ **New Custom Widget**.

        The **Create Custom Widget** page appears.

   - Create a custom widget while editing a dashboard:

     a. Edit a dashboard.

     b. In the upper-right corner of the page, click ⊕ **Add Widgets**.

        A menu appears.

     c. Click ⊕ **New Custom Widget**.

   The **Create Custom Widget** page appears.

2. Under **Chart Type**, choose an option:

   - **Bar**
   - **Column**
   - **Doughnut**
   - **Matrix**
   - **Multi-series Bar**
   - **Multi-series Column**
   - **Stacked Bar**
   - **Stacked Column**
   - **Table**

3. In the **Data Set** drop-down, select the type of information Tenable Vulnerability Management uses to update the widget:

- **Vulnerabilities**
- **Assets**

> **Note:** If you selected ring chart or bar chart in the charts section, selecting the **Assets** dataset resets the chart selection to a table.

The chart type, **Data Grouping**, and **Display Fields** options update based on your selection.

4. In the **Group By** drop-down box, select how you want to group the data:
   - **By Plugin** (**Vulnerabilities** dataset only)
   - **By Asset** (**Vulnerabilities** dataset only)
   - **By CVE** (**Vulnerabilities** dataset only)
   - **Asset List** (**Assets** dataset only)
5. (Optional) To filter the widget data using filters:
   a. Click the ⌄ button to expand the filter options.
   b. In the drop-down box, select category, operator, and value types.
   c. (Optional) Click the ⊕ **Add** button to specify more filters.

> **Note:** Some filters are unsupported by certain **Group By** options in specific environments and you will not be able to select them. Please contact the Tenable support team in these cases.

> **Note:** If you previously created a tag, it appears in the custom widget's list of filters.

> **Note:** If you exceed the current asset query limitation of 5,000, a message appears in your interface. Refine the query to a smaller set of asset tags.

> **Note:** Tenable Vulnerability Management does not currently support tag filters in exports.

6. (Optional) To filter the widget data using an existing saved search, in the **Saved Searches** drop-down box, select the saved search you want to use to filter your widget data.

> **Note:** If you do not have any saved searches, this option does not appear. To create a new saved search, see Saved Search.

7. In the **Name** box, type a name for the custom widget.

   In the **Widget Preview**, the title updates automatically.

8. (Optional) In the **Description** box, type a description for the custom widget.

   In the **Widget Preview**, the ⓘ icon appears and the description hover text updates automatically.

9. Click **Update Preview** to update the widget preview.

   > **Note:** While **Name**, **Description**, and the chart type all update in the widget preview automatically, all other configuration options refresh after you click **Update Preview**.

10. Click **Save and Exit**.

    Tenable Vulnerability Management saves the custom widget to the widget library, and you can add the widget to any user-defined dashboards.

Create a Custom Widget for Explore Dashboards

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, Administrator, or Custom Role with appropriate privileges

> **Required Tenable Web App Scanning User Role:** Scan Operator, Standard, Scan Manager, or Administrator

You can use the custom widget option to create uniquely defined widgets, which you can then add to any user-defined Explore dashboards. You can create custom widgets with vulnerabilities and assets data. Vulnerabilities can include host vulnerabilities, Tenable Web App Scanning vulnerabilities, and vulnerabilities from Legacy Tenable Cloud Security. Adding a mix of these custom widgets to your dashboard provides you with a holistic view of the vulnerability environment.

You can drill down from the custom widgets to the Findings and Assets pages.

To create a custom widget:

1. Do one of the following:
    - Create a custom widget via the widget library:
        a. View the widget library.
        b. In the upper-right corner of the page, click the ⊕ **New Custom Widget** button.

        The **Create Custom Widget** page appears.
    - Create a custom widget while editing a dashboard:
        a. Edit a dashboard.
        b. In the upper-right corner of the page, click ⊕ **Add Widgets**.

        A menu appears.
        c. Click **Custom Widget**.

    The **Create Custom Widget** page appears.
2. In the **Chart Type** section, select the chart type for your custom widget:
    - Chart types for findings:
        - **Bar**
        - **Column**
        - **Doughnut**
        - **Matrix**
        - **Multi-series Bar**
        - **Multi-series Column**
        - **Stacked Bar**
        - **Stacked Column**
        - **Table**

- Chart types for assets:
    - **Bar**
    - **Column**
    - **Doughnut**
    - **Table**

3. In the **Name** box, type a name for the custom widget.

   In the **Widget Preview**, the title updates automatically.

4. (Optional) In the **Description** box, type a description for the custom widget.

   In the **Widget Preview**, the ⓘ icon appears and the contextual description updates automatically.

5. In the **Data Set** drop-down box, select the type of information Tenable Vulnerability Management uses to update the widget:
    - **Findings**
    - **Assets**

   The **Chart Type**, **Group By**, and **Sort Fields** options update based on your selection.

If you selected...	Options
Findings	Provide the following details: a. In the **Entity** drop-down box, select the type of vulnerability for which you want to create a widget. You can select from the following: • **Host Audits** – Includes host vulnerabilities. • **Vulnerabilities** – Includes the list of findings. • **Web Application Findings** – Includes vulnerabilities from Tenable Web App Scanning.

	• **Cloud Misconfigurations**– Includes vulnerabilities from Legacy Tenable Cloud Security. b. In the **Limit** box, enter the number of records you want to show on the widget. Type a number between 1 and 200. c. In the **Group By** drop-down box, select how you want to group the data. The values in the **Group By** drop-down changes based on the **Entity** you select. > **Note**: For **Bar**, **Column**, **Doughnut**, and **Table** chart types, you can select only one option to group vulnerabilities. For **Matrix**, **Multi-series Bar**, **Multi-series Column**, **Stacked Bar**, and **Stacked Column** chart types, you must select two options for grouping vulnerabilities. For more information about all filters, see Findings Filters. d. In the **Stats** drop-down box, select the statistics you want to show on the widget. For all chart types except **Table**, `count` is the default statistic option. For the **Table** chart type, you can select from multiple options. e. In the **Sort Fields** drop-down box, select how you want to sort the data on the widget. You can sort by one of these options: • **Count** • Value in **Group By** f. In the **Sort Order** drop-down box, select whether you want the sort in ascending or descending order.
Assets	Provide the following details: a. In the **Limit** box, enter the number of records you want to show on the widget. Type a number between 1 and 200.

b. In the **Group By** drop-down box, select how you want to group the data:

- **System Type**
- **Name**
- **Operating System**
- **SSH Fingerprint**
- **Fully Qualified Domain**
- **Mac Addresses**
- **Asset Types**

> **Note**: For **Bar**, **Column**, **Doughnut**, and **Table** chart types, you can select only one option to group assets. For **Matrix**, **Multi-series Bar**, **Multi-series Column**, **Stacked Bar**, and **Stacked Column** chart types, you must select two options for grouping assets.

c. In the **Stats** drop-down box, select the statistics you want to show on the widget.

For all chart types except **Table**, `count` is the default statistic option. For the **Table** chart type, you can select from multiple options.

6. For each filter you want to use, do the following:

> **Note**: Tenable recommends that you use simple instead of complex queries or one level of nested filters when creating your custom widgets. Widgets can only have a maximum of one level of nested filters, provided no additional context filters are applied when the widgets are added to the dashboards. An example of a query with one level of nesting:
> `(CVSSv3 Base Score is greater than 8.9 OR VPR is greater than 8.9) AND State is not equal to Fixed`

a. Click **Select Filters**.

The **Select Filters** drop-down box appears.

b. Click the filter you want to apply.

   The filter appears in the box.

c. In the filter, click the ∨ button.

   A list of filter value and operator options appears.

d. In the first drop-down box, select the operator you want to apply to the filter.

e. In the second drop-down box, select one or more values to apply to the filter.

f. Select **Match All** from the drop-down box. By default, Tenable Vulnerability Management sets the filter to **Match All**.

7. Click **Update Preview** to update the widget preview.

   Note: While **Name**, **Description**, and the chart type all update in the widget preview automatically, all other configuration options refresh after you click **Update Preview**.

8. Click **Save and Exit**.

   Tenable Vulnerability Management saves the custom widget to the widget library, and you can add the widget to any user-defined dashboards.

Edit a Custom Widget

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Note: You cannot edit Tenable-provided widgets.

To edit a custom widget:

1. View the widget library.
2. Click the **My Widgets** tab.

   All user-created widgets appear.

3. In the upper-right corner of the widget you want to edit, click the ⋮ button.

   A menu appears.

4. Click **Edit**.

   The widget options appear.

5. Edit the widget options.

6. Click **Save and Exit**.

   A confirmation appears.

Note: A custom widget that was previously included in dashboards before you edited the widget does not update to reflect your edits. To include the edited widget, you must add the widget again as described in Add a Widget to a Dashboard.

Add a Widget to a Dashboard

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Use the following steps to add a widget to your template-based and custom dashboards.

You can add custom widgets, widgets from Tenable-provided dashboards, and other general purpose Tenable-provided widgets.

To add a widget to a dashboard:

Note: These steps describe how to add a template widget to a dashboard. See custom widgets for information on how to create custom widgets and add them to your dashboard.

1. View the widget library.
2. For each widget you want to add:
   a. Do one of the following:
      - Scroll through the list of widgets.
      - Use the **Search** box to find a specific widget.

      Tip: You can hover over a widget tile for brief descriptions of each widget. For detailed descriptions about widgets originating from Tenable-provided dashboards, see Tenable-Provided Dashboards.

b. Roll over the widget you want to add.

   The ⊕ **Add to Dashboards** button appears.

c. Click ⊕ **Add to Dashboards**.

   The **Add to Dashboards** plane appears.

d. In the **Dashboards** drop-down box, select the dashboard or dashboards to which you want to add the widget.

e. Click **Save**.

   Tenable Vulnerability Management adds the widget to the bottom of the appropriate dashboard or dashboards.

f. Click ⊕ **Add**.

   Tenable Vulnerability Management adds the widget to the bottom of the appropriate dashboard.

3. Click **Done**.

   You return to the **Dashboards** page.

Configure a Widget

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

To configure a widget:

1. View the dashboard page that contains the widget you want to configure.
2. In the upper-right corner of the widget you want to change, click the ⋮ button.

   A menu appears.

3. Click **Configure**.

   The widget summary plane appears.

4. On the widget summary plane, do any of the following:

- Rename the widget:

  a. Do one of the following:

     - Click the name of the widget.
     - In the widget summary plane, roll over the widget name and click the ✎ button.

     The name field becomes an editable text box.

  b. Type a new name for the widget.

  c. Click the ✓ button to confirm the name change.

     A confirmation message appears at the top of the page, and the new name appears in the widget header.

- Edit the widget description:

  a. Do one of the following:

     - Click the widget description.
     - In the widget summary plane, roll over the widget description and click the ✎ button.

     The description field becomes an editable text box.

  b. Type a new description for the widget.

  c. Click the ✓ button to confirm the change.

     A confirmation message appears at the top of the page, and the new description appears in the widget header.

- Duplicate the widget:

  - In the **Actions** row, click the ⧉ button.

    A confirmation message appears and Tenable Vulnerability Management adds the duplicated widget to the dashboard.

- Delete the widget from the dashboard:

  a. In the **Actions** row, click the button.

     A **Confirm Deletion** message appears.

  b. Click **Delete**.

     A confirmation message appears and Tenable Vulnerability Management removes the dashboard from the **Dashboards** page.

- Apply filters to the widget:

Option	Description	Requirement
All Assets	(Default) This option includes all the assets in the dashboard.	This is the default option and includes all assets in the dashboard. There is not a requirement for this option.
Custom	This option only includes assets with a specific hostname, IP address, FQDN, or CIDR.	When you select this option, a text box appears. Enter one or more of the custom option formats (hostname, IP address, FQDN, or CIDR). You must separate multiple items with a comma.
Tags	This option uses tags to filter asset results or vulnerability results. **Note:** Because the ACR Widget uses Tenable Lumin data, this widget does not support filtering by tag.	When you select this option, a drop-down box appears. Select or type the tag name by which you want to filter results. Tenable Vulnerability Management filters the results by the selected tags. **Note:** Tenable Vulnerability Management supports a maximum of 100 filters.

> **Note:** Once you apply a filter to a widget, a ▽ icon appears in the widget header. Roll over the ▽ icon to view the applied filter.

5. Click **Apply**.

   A confirmation message appears and Tenable Vulnerability Management applies your changes to the widget.

Duplicate a Widget

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To duplicate a widget:

1. View the dashboard page that contains the widget you want to duplicate.
2. In the upper-right corner of the widget you want to duplicate, click the ⋮ button.

   A menu appears.
3. Click **Duplicate**.

   The duplicated widget appears at the bottom of the page.
4. (Optional) Change the name of the widget.
5. (Optional) Reorder the widget sections.

Rename a Widget

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

To rename a widget:

1. View the dashboard page that contains the widget you want to change.
2. In the upper-right corner of the widget you want to rename, click the ⋮ button.

   A menu appears.

3. Click **Configure**.

   The widget summary plane appears.

4. In the widget summary plane, roll over the widget name.

   The ✎ button appears next to the name.

5. Click the ✎ button or double-click the name.

   The name field becomes an editable text box.

6. Type a new name for the widget.
7. Click the ✓ button to confirm the name change.

   A confirmation message appears at the top of the page.

   The new name appears in the widget header.

Delete a Widget from a Dashboard

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

To remove a widget from a dashboard:

1. View the dashboard page that contains the widget you want to remove.
2. In the upper-right corner of the widget you want to remove, click the ⋮ button.

   A menu appears.

3. Click 🗑 **Delete**.

   Tenable Vulnerability Management prompts you to confirm the removal.

4. Click **Delete**.

   A confirmation message appears at the top of the page.

   Tenable Vulnerability Management removes the widget from the dashboard. Remaining widgets adjust to fill the new space.

Scans

You can create, configure, and manage scans in Tenable Vulnerability Management.

Section	Description
Manage Scans	Create, import, and launch scans. View and manage scans and scan results.
Scans (Unified Configuration) Overview	Create, launch, and manage Tenable Vulnerability Management and Tenable Web App Scanning scans in the Tenable Vulnerability Management unified user interface.
Scan Templates and Settings	Use a Tenable-provided scanner template, agent template or a user-defined template to configure scan settings.
Sensors	Link your sensors, such as Tenable Nessus scanners, Tenable Agents, and Tenable Network Monitors, to Tenable Vulnerability Management.

Note: For information about scanning in Tenable Web App Scanning, see the Tenable Web App Scanning Getting Started Guide.

Manage Scans

To manage your Tenable Vulnerability Management and Tenable Web App Scanning scans in the unified **Scans** user interface, see Scans Overview.

To manage your Tenable Web App Scanning scans in Tenable Web App Scanning, see the Tenable Web App Scanning Getting Started Guide.

Scans Overview

The **Scans** page allows you to create, launch, and configure Tenable Vulnerability Management scans and Tenable Web App Scanning scans.

Tip: Before you begin, check out the Tenable Vulnerability Management scan limitations.

Caution: Tenable occasionally performs maintenance on Tenable Vulnerability Management. To avoid performance issues, Tenable recommends not running or scheduling scans during maintenance windows. For current maintenance status and updates, see the Tenable Status page.

Create a Scan

In Tenable Vulnerability Management, you can create scans using scan templates. For general information about templates and settings, see Scan Templates and Settings.

When you create a scan, Tenable Vulnerability Management assigns you owner permissions for the scan.

Tip: To quickly target specific vulnerabilities that previous scans have identified on your assets, create a Tenable Vulnerability Management remediation scan.

Note: If you are scanning a Linux machine with Tenable Vulnerability Management, 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.

Caution: Tenable occasionally performs maintenance on Tenable Vulnerability Management. To avoid performance issues, Tenable recommends not running or scheduling scans during maintenance windows. For current maintenance status and updates, see the Tenable Status page.

Before you begin:

- Review the Tenable Vulnerability Management scan limitations.
- If you want to create a scan from a user-defined template, create a user-defined template as described in Create a User-Defined Template.
- Create an access group for any targets you want to use in the scan and assign **Can Scan** permissions to the appropriate users.

To create a scan:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.

   This also determines whether you are creating a Tenable Vulnerability Management or Tenable Web App Scanning scan.

3. In the upper-right corner of the page, click the [→ **Create a Scan** button.

   The **Select a Scan Template** page appears.

4. Do one of the following:

   - If you are creating a Tenable Vulnerability Management scan, use the following procedure:

     a. Click the **Nessus Scanner**, **Nessus Agent**, or **User Defined** tab to view available templates for your scan.

        The tab appears.

        > **Note:** Users with Scan Operator permissions can see and use only the user-defined templates shared with their account.

     b. Click the tile for the template you want to use for your scan.

        The **Create a Scan** page appears.

     c. Configure the scan:

Tab	Action
Settings	Configure the settings available in the scan template. • Basic Settings – Specifies the organizational and security-related aspects of a scan template. This includes specifying the name of the scan, its targets, whether you want to schedule the scan, and who has permissions for the scan.

	• Discovery Settings – Specifies how a scan performs discovery and port scanning. • Assessment Settings – Specifies how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications. • Report Settings – Specifies whether the scan generates a report. • Advanced Settings – Specifies advanced controls for scan efficiency.
Credentials	Specify credentials you want Tenable Vulnerability Management to use to perform a credentialed scan.
Compliance/SCAP	Specify the platforms you want to audit. Tenable, Inc. provides best practice audits for each platform. Additionally, you can upload a custom audit file.
Plugins	Select security checks by plugin family or individual plugin.

d. Do one of the following:

- If you want to save without launching the scan, click **Save**.

  Tenable Vulnerability Management saves the scan.

- If you want to save and launch the scan immediately, click **Save & Launch**.

  > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

> **Note:** If you are editing an imported scan, the **Save & Launch** option is not available.

Tenable Vulnerability Management saves and launches the scan.

- If you are creating a Tenable Web App Scanning scan, use the following procedure:

  a. Click the **Web Application** or **User Defined** tab to view available templates for your scan.

  The tab appears.

  > **Note:** Users with Scan Operator permissions can see and use only the user-defined templates shared with their account.

  b. Click the tile for the template you want to use for your scan.

  The **Create a Scan** page appears.

  c. Configure the scan:

Tab	Action
Settings	Configure the settings available in the scan template. For more information, see Basic Settings in Tenable Web App Scanning Scans.
Scope	Specify the URLs and file types that you want to include in or exclude from your scan. For more information, see Scope Settings in Tenable Web App Scanning Scans.
Assessment	Specify how a scan identifies vulnerabilities and what vulnerabilities the scan identifies. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications. For more information, see Assessment Settings in Tenable Web App Scanning Scans.
Advanced	Specify advanced controls for scan efficiency.

Credentials	Specify credentials you want Tenable Vulnerability Management to use to perform a credentialed scan.
Plugins	Select security checks by plugin family or individual plugin.

d. Do one of the following:

- If you want to save without launching the scan, click **Save**.

  Tenable Vulnerability Management saves the scan.

- If you want to save and launch the scan immediately, click **Save & Launch**.

  > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

  > **Note:** If you are editing an imported scan, the **Save & Launch** option is not available.

  Tenable Vulnerability Management saves and launches the scan.

View Scans

> **Required Scan Permissions**: Can View

You can view configured and imported scans. If you have appropriate permissions, you can also perform actions to manage the scans.

> **Note:** You can export the archived scan results, but you cannot view them in Tenable Vulnerability Management. This limitation applies to both imported scan results and scan results that Tenable Vulnerability Management collects directly from scanners. After 15 months, Tenable Vulnerability Management removes the scan data entirely.

Before you begin:

- Create or import one or more scans.

To view scans in the **Scans** section:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.

3. In the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

   For more information about scan folders, see Organize Scans by Folder.

4. Do any of the following:

Section	Action
Search box	Search the table by scan name or status. For more information, see Tables.
Filter	Filter the table with Tenable-provided scan filters.
Create Scan button	In the upper-right corner, click the **Create Scan** button to create a new scan.
Tools button	In the upper-right corner, click the **Tools** button. A menu appears with the following options: • Import Scan (Tenable Vulnerability Management scans only) • Manage Sensors • Manage Credentials • Manage Exclusions

Scans table	• View summary information about each scan:
	  • **Name** – The scan name.
	  If you have assigned permissions for the scan to other users, the label **Shared** appears next to the scan name.
	  • **Schedule** – The scan schedule.

	• **Last Modified** – (Tenable Web App Scanning scans only) The date and time the scan was last modified. • **Last Run** – The date and time the scan was last run. • **Status** – The status of the scan. • Sort, increase or decrease the number of rows per page, or navigate to another page of the table. For more information, see Tables. • View details for a scan. • Launch a scan. • Change the read status for a scan. • Export scan results. • Move a scan to the trash. • Delete a scan permanently. • Move a scan to a different folder.

View Scan Details

Required Scan Permissions: Can View

You can view scan results for scans you own and scans that were shared with you.

Consider the following when viewing scan results:

- You can view details for an individual scan based on the permissions configured for the scan. However, when you view aggregated scan results in dashboards and other analysis views (for example, the **Vulnerabilities** or **Assets** tables), your access is based on the access groups you belong to.
- You can export the archived scan results, but you cannot view them in Tenable Vulnerability Management. This limitation applies to both imported scan results and scan results that Tenable Vulnerability Management collects directly from scanners. After 15 months, Tenable Vulnerability Management removes the scan data entirely.

- When you view results from the latest run of the scan, Tenable Vulnerability Management categorizes the scan as **Read**. The **Read** status is specific to your user account only. You can also manually change the read status.
- Tenable Vulnerability Management retains scan data for 15 months. If you want to store scan data for longer than 15 months, you can export the scan data for storage outside of Tenable Vulnerability Management.
- You can view a maximum of 5,000 rows at a time in the **Vulns by Asset** table.

To view scan details for an individual scan:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.
3. In the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

4. In the scan table, click the scan where you want to view details.

   The scan details plane appears below the scan table. By default, this plane shows details for the latest run of the scan.

5. Do any of the following:

Section	Action
Scan Actions menu	• Launch a scan. • Edit a scan configuration. • Export scan results. • Move a scan to a different folder. • Change the read status for a scan. • Delete a scan permanently. • Copy a scan.

	• Move a scan to the trash.
See All Details button	Click the **See All Details** button to open the **Scan Details** page and view the scan's vulnerabilities and affected assets, target information, and scan history. You can also use the **Scan Details** page to export the scan, edit the scan configuration, move the scan to the trash folder, and submit the scan for PCI validation. The scan details page includes the following features and information: **Page header** • (Rollover scans only) Download a list of a rollover scan's remaining targets. • Export the currently visible scan results. • Edit the scan configuration. • Move a scan to the trash folder. **Severity summaries** The number of vulnerabilities with a **Critical**, **High**, **Medium**, and **Low** severity in the scan results. **Details section** View details about the scan run: • **Status** – The status of the scan. • **Start Time** – The start date and time for the scan. • **Template** – The Tenable-provided template on which the scan configuration is based. • **Scanner** – The scanner that performed the scan. • **Scanner Groups** – The scanner group or groups

to which Tenable Vulnerability Management assigned the scan. This detail appears only if scan routing is enabled for the scan.

- **Targets** – The targets that the scan evaluated.

Vulns by Plugin tab

View the vulnerabilities in the scan results, organized by plugin.

> **Note:** This tab does not appear for scan results older than 35 days.

> **Note:** When you view scan results of a plugin that has multiple CVEs, one scan result row appears for that plugin in the **Vulns by Plugin** table. However, if you export that plugin's scan results in a CSV file, Tenable Vulnerability Management generates one row of scan results per CVE.

- View information about each vulnerability:
  - Severity icon – The severity of the vulnerability.
  - **Name** – The name of the plugin that identified the vulnerability.
  - **Family** – The family of the plugin that identified the vulnerability.
  - **Instances** – The number of 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.

- To filter the data displayed in the table, see Filter a Table.
- To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see Tables.
- To view details for a vulnerability, click a row of the table.

  The **Vulnerability Details** page appears. For more information, see Vulnerability Details.

Vulns by Asset tab

View the vulnerabilities in the scan results, organized by asset. By default, assets in the table are sorted by decreasing number of vulnerabilities, then by decreasing severity.

> **Tip:** This tab does not appear for scan results older than 35 days.

- View information about each vulnerability:
  - **Assets** – The asset identifier. Tenable Vulnerability Management assigns this identifier based on the presence of certain asset attributes in the following order:
    - Agent Name (if agent-scanned)
    - NetBIOS Name
    - FQDN
    - IPv4 address

    For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the

	NetBIOS name appears as the Asset Name. • **Vulnerabilities** – A visual summary of the vulnerabilities on the asset, organized by severity. • **Vuln Count** – The total number of vulnerabilities on the asset. • **Critical** – The total number of vulnerabilities on the asset with a critical severity. • **High** – The total number of vulnerabilities on the asset with a high severity. • **Audits** – A visual summary of the audits on the vulnerability, organized by severity. • **Audit Count** – The total number of audits on the asset. • To filter the data displayed in the table, see Filter a Table. • To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see Tables. • To view details for an asset, click a row of the table. The **Asset Details** page appears. For more information, see View Legacy Workbench Asset Details. ### Audit tab View compliance audit check results. This tab only appears if the scan results include data from

compliance audit checks.

> **Tip:** This tab does not appear for scan results older than 35 days.

On this tab, you can view:

- View tiles representing the number of audit checks identified the last time the scan was completed organized by severity level.
- View a table of audits detected during the scan. Each row represents a specific audit, and includes the following information:
    - **Status** – The status of the audit, for example **Passed**, **Warning**, or **Failed**.
    - **Name** – The name of the compliance check.
    - **Family** – The compliance check family to which the audit belongs.
    - **Count** – The number of times the audit was identified.
- To view additional information about a specific audit check, click a row in the audits table.

  The **Audit Details** page appears.

    - **Overview** – Information about the audit check, including a description of the check and the audit file used for the check.
    - **Assets** – A list of assets where the scan performed the audit check.

Summary tab

(Rule-based scans only) Shows the scan's description, triggers, an explanation of rule-based scanning, and a link to the vulnerabilities workbench.

Warnings tab

View warnings about problems Tenable Vulnerability Management or the scanner encountered while running the scan. This tab only appears if Tenable Vulnerability Management or the scanner encountered an issue while running the scan. This tab does not appear for scan results older than 35 days.

Review the warnings to determine how to resolve the scan problem. For example, if an **Invalid Target** note is present, check the target parameters in the scan configuration.

> **Tip:** In the scan warnings table header, click ⬇
>
> **Download All Warnings** to download a JSON file of all the scan result's warnings. The button is not shown if the scan was archived.

Remediations tab

View remediation details.

> **Note:** The **Remediation** tab only appears if there are known remediations for the scan.

This tab contains a table listing each remediation action. On this tab, you can view:

- **Vulnerabilities** – The number of vulnerabilities resolved by the recommended remediation.
- **Assets** – The number of assets scanned.

History tab

View the scan history.

This tab contains a table listing each time the scan has run. For the scan run currently displaying in the **Scan Details** page, Tenable Vulnerability Management adds the label **Current** to the run. By default, the latest scan run is labeled **Current**.

> **Note:** Scan history is unavailable for imported scans, configured scans that have not yet run, and triggered scans.

> **Note:** Tenable Vulnerability Management retains scan data for 15 months. If you want to store scan data for longer than 15 months, you can export the scan data for storage outside of Tenable Vulnerability Management.
>
> An exception to this is that Tenable Vulnerability Management only retains up to 15 triggered scan histories at a time for each scan, showing a scan history entry for each 12-hour window of the past seven days.

On this tab, you can:

- View summary information about each time the scan was run:
  - **Start Time** – The start date and time for the scan.
  - **End Time** – The end date and time for the scan.
  - **Duration** – The duration of the scan .
  - **Status** – The status of the scan.

	• Filter the data displayed in the table. • Sort, increase or decrease the number of rows per page, or navigate to another page of the table. For more information, see Tables. • View details for a historical scan by clicking a row in the table. Tenable Vulnerability Management marks the run you selected as **Current** and updates the **Scan Details** section to show data for the selected run. If the historical scan results are younger than 35 days, Tenable Vulnerability Management also updates the tabs on the **Scan Details** page. If the historical scan results are older than 35 days, the additional tabs are absent from the **Scan Details** page. Use export instead to obtain the results.
Activity section	A history of the scan's activity. In this section, you can view the date and time when the scan **Started**, **Completed**, and when it was **Modified**, **Canceled**, or manually **Aborted**.
Vulnerabilities by Severity/VPR Breakdown section	The number of vulnerabilities with a **Critical**, **High**, **Medium**, and **Low** severity in the scan results.
Scan Duration section	The amount of time elapsed between the start and end of the scan.
Targets section	The number of targets scanned.
Type section	The scan type.

Template section	The scan template used.
Schedule section	The scan schedule.

View Scan Vulnerability Details

You can view a scan's vulnerability details by plugin or by asset (Tenable Vulnerability Management scans only) from the **Scans** section.

To view a scan's vulnerability details from the **Scans** section:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans**.

3. In the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

4. In the scans table, click the scan where you want to view details.

   The scan details plane appears below the scan table. By default, this plane shows details for the latest run of the scan.

5. In the scan details plane, click the **See All Details** button.

   The **Scan Details** page appears. The **Vulns by Plugin** tab shows by default.

6. If you would rather view vulnerabilities by the affected asset, click the **Vulns by Asset** tab.

   The vulnerabilities by asset table appears.

   > **Note:** You can view a maximum of 5,000 rows at a time in the **Vulns by Asset** table.

7. From either the **Vulns by Plugin** tab or the **Vulns by Asset** tab, do one of the following:

   - Filter the plugins table by vulnerability attributes.
   - Search the plugins table.
   - View the number of plugin results, next to the **Search** box.

- On the **Vulns by Plugin** tab, click a vulnerability to view its details. For more information, see View Finding Details.
- On the **Vulns by Asset** tab, click an asset row to view its vulnerability details. For more information, see View Asset Details.

Scan Filters

On the **Scans** page, you can filter scans using Tenable-provided filters. The Tenable Vulnerability Management scan view allows you to filter by scan status, and the Tenable Web App Scanning scan view allows you to filter by multiple values.

Filter	Description
Status	The status of the scan. For more information about scan statuses, see Scan Status.
Created Date (Tenable Web App Scanning scans only)	The date the scan configuration was created.
Description (Tenable Web App Scanning scans only)	The description of the scan configuration.
Finalized Date (Tenable Web App Scanning scans only)	The date on which the scan last completed.
Last Modified Date (Tenable Web App Scanning scans only)	The date on which the scan configuration was last modified.
Last Scanned Date (Tenable Web App Scanning scans only)	The date on which the scan was last ran.
Name (Tenable Web App Scanning scans only)	The name of the scan configuration.
Schedule (Tenable Web App Scanning scans only)	Whether a scan schedule is enabled or on demand.
Target (Tenable Web App Scanning scans only)	The target URL used to launch the scan.
Template (Tenable Web App	The Tenable-provided scan template the scan

Scanning scans only)	configuration was based on.
User Template (Tenable Web App Scanning scans only)	The user-defined scan template the scan configuration was based on.

Launch a Scan

In addition to configuring a scan's Schedule settings to launch the scan at scheduled times, you can launch a scan manually. You can only launch a new scan when the previous scan has the **Completed**, **Aborted**, or **Canceled** status (for more information, see Scan Status).

To launch a standard scan manually, see Launch a Scan.

Alternatively, you can launch a *rollover scan* to scan the remaining targets of a previous scan that ended prematurely (for more information, see Launch a Rollover Scan). You can also launch a *remediation scan* to run a follow-up scan against existing scan results (for more information, see Launch a Remediation Scan).

Note: If you are scanning a Linux machine with Tenable Vulnerability Management, 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.

Note: To learn more about scan limitations in Tenable Vulnerability Management, see Scan Limitations.

Launch a Scan

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Required Scan Permissions: Can Control

Use the following steps to launch a scan manually. You can launch the scan using the targets as configured in the scan, or you can launch the scan with custom targets that override the configured targets.

To launch a scan:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.

3. In the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

   For more information about scan folders, see Organize Scans by Folder.

4. In the scans table, roll over the scan you want to launch.

   The action buttons appear in the row.

5. Do one of the following:

   - To launch the scan using the targets as configured in the scan, click the ▷ button in the row.
   - If you have previously launched the scan and want to use custom targets that override the configured targets:

     a. In the row, click the button.

        The **Custom Launch Scan** plane opens.

     b. In the **Targets** box, type a comma-separated string of targets.

     c. Click **Launch**.

   Tenable Vulnerability Management launches the scan.

   You can follow the scan's progress by checking its Scan Status on the **Scans** page.

Launch a Rollover Scan

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Required Scan Permissions: Can Control

When you launch a rollover scan, the scan runs only against targets and hosts that Tenable Vulnerability Management did not scan previously. This happens when a scan ends before scanning all the assigned targets, which can occur when:

- A user manually stops the scan
- The scan times out due to the Scan Window setting
- The scanner aborts scan tasks or does not initialize properly

In some cases, you may see **Completed** scans that you can perform rollover scans for. This indicates that even though all the assigned targets were scanned, some individual scan tasks may have failed.

Rollover scans allow you to achieve complete scan coverage for all your assets, and you can use the rollover feature to split up large, network-impacting scans. You can launch a rollover scan from **Scans** page. Tenable Vulnerability Management marks scans that you can launch a rollover scan for in the scan table with the **Rollover** tag in the **Name** column.

To view the remaining targets that the rollover scan will run against, see Download Rollover Targets. If you want to restart the scan and rescan all the targets, see Launch a Scan.

> **Note:** You cannot launch rollover Web Application scans.

To launch a rollover scan:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.
3. In the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

   For more information about scan folders, see Organize Scans by Folder.

4. In the scans table, roll over the scan you want to launch.
5. In the row, click the ⋮ button.

A menu appears.

6. Click the **Launch Rollover** option.

   Tenable Vulnerability Management launches the rollover scan.

   You can follow the scan's progress by checking its Scan Status on the **Scans** page.

Launch a Remediation Scan

> **Required Tenable Vulnerability Management User Role:** Standard, Scan Manager, or Administrator

> **Required Access Group Permissions**: Can Scan

You can create a remediation scan to run a follow-up scan against existing scan results. A remediation scan evaluates a specific plugin against a specific scan target or targets where a vulnerability was present in your earlier active scan.

Remediation scans allow you to validate whether your vulnerability remediation actions on the scan targets have been successful. If a remediation scan cannot identify a vulnerability on targets where the vulnerability was previously identified, the system changes the status of the vulnerability to **Fixed**.

Tenable Vulnerability Management automatically creates remediation scans from the Tenable-provided **Advanced Network Scan** template and populates certain settings based on the assets and vulnerabilities you selected.

You can perform remediation scans for scan results from certain sensors only:

Sensor Type	Supported?
Tenable Vulnerability Management Cloud Sensor	yes
On-premises Tenable Nessus	yes
Tenable Nessus scanner for Amazon Web Services (AWS)	yes
Tenable Web App Scanning	no
Tenable Network Monitor	no
Tenable Agent	no

To learn more about scan limitations in Tenable Vulnerability Management, see Scan Limitations.

To launch a remediation scan:

1. Set the scope for the remediation scan:

Remediation Scan Scope	Action
All vulnerabilities on all affected assets	This scope is not supported.
All vulnerabilities on an individual asset	To set this scope: a. View asset details. b. On the asset details page, click the **Findings** tab. The **Findings** tab appears. c. In the ribbon of the **Findings** table (next to the **Vulnerability/Host Audit** drop-down menu), select the blank checkbox to select all vulnerabilities. d. In the ribbon of the **Findings** table, click **Launch Remediation Scan**.
All vulnerabilities on multiple assets	This scope is not supported.
An individual vulnerability on an individual asset	To set this scope: a. View asset details. b. On the asset details page, click the **Findings** tab. The **Findings** tab appears. c. In the **Findings** table, select the checkbox next to the vulnerability you want to select. d. In the ribbon of the **Findings** table, click **Launch Remediation Scan**.
Multiple	This scope is not supported.

vulnerabilities on all affected assets	
Multiple vulnerabilities on an individual asset	To set this scope: a. View asset details. b. On the asset details page, click the **Findings** tab. The **Findings** tab appears. c. In the **Findings** table, select the checkbox next to each vulnerability you want to select. d. In the ribbon of the **Findings** table, click **Launch Remediation Scan**.
Multiple vulnerabilities on multiple assets	This scope is not supported.
An individual finding	To set this scope: a. View findings details for a host vulnerability finding or web application vulnerability finding. b. On the findings details page, in the upper-right corner, click the **Actions** button. The actions menu appears. c. In the actions menu, click **Launch Remediation Scan**.

The **Create a Scan - Remediation Scan** appears.

Tenable Vulnerability Management automatically creates the remediation scan from the Tenable-provided Advanced Network Scan template and populates certain settings based on the assets and vulnerabilities you selected.

2. On the **Create a Scan** page:

a. Verify the settings that Tenable Vulnerability Management populated based on the vulnerabilities and assets you selected.

b. Configure additional settings for the scan.

   The number of manual changes you must make depends on the plugins involved in the remediation scan.

The following table defines the inherited and default values for settings in the remediation scan.

Setting Category	Setting	Remediation Scan Value
Basic	**Name**	Specifies an editable scan name in the format "Remediation scan of plugin # *number*" where *number* is the number of the plugin that identified the vulnerability.
	Folder	Cannot be configured. Remediation scans appear in the **Remediation Scans** folder only.
	Scanner	Specifies the scanner that performs the scan. The scanner you select depends on the location of the targets included in the remediation scan. For example: • By default, this value is the cloud scanner for your geographical region (for example, **US Cloud Scanner**). However, a cloud scanner cannot scan non-routable IP addresses. If the scan targets include non-routable IP addresses, select a linked scanner instead. • Select a scanner group if you want to: ◦ Improve scan speed by balancing the

		scan load among multiple scanners. ◦ Rebuild scanners and link new scanners in the future without having to update scanner designations in scan configurations.
	Network	(Required if the scanner is set to **Auto-Select**) Do one of the following: • If your scans involve separate environments with overlapping IP ranges, select the network that contains the scanner groups that you configured for scan routing. • If your scans do not involve separate environments with overlapping IP ranges, retain the **Default** network.
	Targets	Specifies the scan targets based on the assets you selected for the remediation scan.
	User Permissions	Specifies default settings for the Advanced Network Scan template. By default, only you have access to the individual scan results for the remediation scan. The **Default** user permissions are set to **No Access**. If you want to share the remediation scan with other users, configure the user permissions.
	Schedule	Cannot be configured. If you do *not* launch a remediation scan when you create it, you can launch the scan manually later.
	all other settings	Specifies default settings for the Advanced

		Network Scan template.
Discovery	all	Specifies default settings for the Advanced Network Scan template. **Note:** The default **Port Scan Range** scans common ports only. If the plugins used in the remediation scan require specific ports, configure this setting for a range that includes those ports.
Assessment	all	Specifies default settings for the Advanced Network Scan template.
Report	all	Specifies default settings for the Advanced Network Scan template.
Advanced	all	Specifies default settings for the Advanced Network Scan template.
Credentials	all	By default, there are no credentials configured. If the plugins in the remediation scan require credentials, configure them in the remediation scan. **Note:** Remediation scans work best for un-credentialed network scan results. Use caution when running a remediation scan for a plugin that requires scan credentials. If you neglect to add scan credentials when required for a specific plugin, or if you type the credentials incorrectly, the system may identify the related vulnerabilities as fixed. In fact, the vulnerabilities do not appear in the scan results because the system could not complete the credentialed scan.
Compliance	all	By default, no compliance audits are configured. If the plugins in the remediation scan require compliance audit settings, configure the

		appropriate settings.
Plugins	limited	Specifies plugins limited to the following: • the plugins you selected for remediation scanning • any plugins on which the selected plugins are dependent

3. Do one of the following:

   - If you want to save without launching the scan, click **Save**.

     Tenable Vulnerability Management saves the scan.

   - If you want to save and launch the scan immediately, click **Save & Launch**.

     > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

     Tenable Vulnerability Management saves and launches the scan.

What to do next:

- In the **Remediation Scans** folder on the **Scans** page:
  - View the scan status to determine when the scan completes.
  - Edit the scan configuration.
  - Change the read status of the scan results.
  - Launch the scan.
- Once the scan completes:
  a. On the **Findings** page, search for the plugin.
  b. Verify that the status for the selected vulnerabilities is now **Fixed** on the assets that the remediation scan targeted.

Stop a Running Scan

> **Required Scan Permissions**: Can Control

When you stop a scan, Tenable Vulnerability Management terminates all tasks for the scan and categorizes the scan as canceled. The scan results associated with the scan reflect only the completed tasks. You cannot stop individual tasks, only the scan as a whole.

To stop a running scan:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. In the scans table, roll over the scan you want to stop.
3. In the row, click the button.

   A menu appears.

4. Click **Stop**.

   A confirmation window appears.

5. In the confirmation window, click **Stop**.

   Tenable Vulnerability Management stops the scan. The **Status** column updates to reflect the status of the scan.

Pause or Resume a Scan

> **Required Scan Permissions**: Can Control

You can pause scans that you want to stop temporarily. When you pause a scan, Tenable Vulnerability Management pauses all active tasks for that scan and concludes the scanner's local scan task. Paused scans do not consume scanner resources, and other scans can run while there is a paused scan. Tenable Vulnerability Management does not dispatch new tasks from a paused scan job. If the scan remains in a paused state for more than 14 days, the scan times out. Tenable Vulnerability Management terminates the related tasks on the scanner and categorizes the scan as aborted.

You can resume scans that you previously paused. When you resume a scan, Tenable Vulnerability Management instructs the scanner to start the tasks from the point at which the scan was paused. If Tenable Vulnerability Management encounters problems when resuming the scan, the scan fails, and Tenable Vulnerability Management categorizes the scan as aborted. Tenable Vulnerability

Management does not dispatch new tasks from a paused scan job. If the scan remains in a paused state for more than 14 days, the scan times out. Tenable Vulnerability Management terminates the related tasks on the scanner and categorizes the scan as aborted.

Note: You can only pause and resume Tenable Vulnerability Management scans.

To pause or resume a scan:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. In the scans table, roll over the scan.

3. Do one of the following:

   - To pause the scan, click the ⏸ button in the row.
   - To resume the scan, click the ▷ button in the row.

   A confirmation window appears.

4. In the confirmation window, click **Pause** or **Resume** as appropriate.

   Tenable Vulnerability Management pauses or resumes the scan.

Change Scan Ownership

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Required Scan Permissions: Owner

Before you begin:

- If the scan is based on a user-defined template, assign the new owner at least **Can View** permissions for that template. Otherwise, the new owner cannot view the scan configuration.

Note: Only the scan owner can change scan ownership. Therefore, if an administrator needs to change the ownership of another user's scan, they must first assist the user with their account and then assign ownership to the appropriate user.

To change the ownership of a scan in the new interface:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.

3. In the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

4. (Optional) Search for the scan you want to edit. For more information, see Tables.

5. In the scans table, click the scan you want to edit.

   The scan details appear.

6. Click the button next to the scan name.

   The **Edit a Scan** page appears.

7. In the left navigation menu, in the **Settings** section, click **Basic**.

   The **Basic** settings appear.

8. In the **User Permissions** section, next to the permission drop-down for **Owner**, click the button.

   A list of available user accounts appears.

9. Select a user from the list.

   Tenable Vulnerability Management automatically adds you to the list of users and assigns **Can View** permissions to your user account.

10. (Optional) Remove all permissions for your user account:

    a. In the user list, roll over your user account.

       The button appears at the end of the listing.

    b. Click the button.

       Tenable Vulnerability Management removes your account from the list of users.

11. (Optional) Edit the Tenable Vulnerability Management permissions for your user account:
    a. Next to the permission drop-down for your user account, click the ⌄ button.
    b. Select a permission.
12. Click **Save**.

    Tenable Vulnerability Management assigns ownership to the selected user and assigns your user account the permissions you selected. If you removed all permissions for your user account from the scan, the scan no longer appears in any of your scan folders.

Change the Scan Read Status

> **Required Scan Permissions**: Can View

On the **Scans** page, a scan appears in bold in the scans table if you have *not* yet viewed (read) the results of the latest run of the scan.

If you view the scan results, Tenable Vulnerability Management categorizes the scan as "read" and removes the bold formatting from the scan in the scans table.

You can also manually change the scan read status.

To change the scan read status:

1. View your scans.
2. In the scans table, roll over the scan you want to change.
3. Click the ⋮ button.

   A menu appears.
4. Do one of the following:
   - If you have already read the scan, click ✉ **Mark Unread**.
   - If you have not read the scan, click ✉ **Mark Read**.

   Tenable Vulnerability Management changes the read status for the scan.

Edit a Scan Configuration

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Required Scan Permissions: Can Configure

To edit a scan configuration:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.

3. In the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

4. (Optional) Search for the scan you want to edit. For more information, see Tables.

5. In the scans table, click the scan you want to edit.

   The scan details appear.

6. Click the button next to the scan name.

   The **Edit a Scan** page appears.

7. Change the scan configuration. For more information about scan configuration settings, see Scan Settings.

8. Do one of the following:

   - If you want to save without launching the scan, click **Save**.

     Tenable Vulnerability Management saves the scan.

   - If you want to save and launch the scan immediately, click **Save & Launch**.

     Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

> **Note:** If you are editing an imported scan, the **Save & Launch** option is not available.

Tenable Vulnerability Management saves and launches the scan.

Configure vSphere Scanning

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

You can configure a scan 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.

Scenario 1: Scanning ESXi/vSphere Not Managed by vCenter

To configure an ESXi/vSphere scan that vCenter does not manage:

1. Create an advanced network Tenable Vulnerability Management scan.
2. In the left navigation menu, in the **Settings** section, click **Basic**.

   The **Basic** settings appear.
3. In the **Targets** section, type the IP address or addresses of the ESXi host or hosts.
4. In the left navigation menu, click **Credentials**.

   The **Credentials** page appears. This page contains a table of credentials configured for the scan.
5. Next to **Add Credentials**, click the ⊕ button.

   The **Select Credential Type** plane appears.
6. In the **Miscellaneous** section, select **VMware ESX 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. Otherwise, leave the toggle enabled.
10. Click **Save**.
11. Do one of the following:

    - If you want to save without launching the scan, click **Save**.

      Tenable Vulnerability Management saves the scan.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

      > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

      > **Note:** If you are editing an imported scan, the **Save & Launch** option is not available.

      Tenable Vulnerability Management saves and launches the scan.

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.

Scenario 2: Scanning vCenter-Managed ESXi/vSpheres

Note: 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. Create an advanced network Tenable Vulnerability Management scan.
2. In the left navigation menu, in the **Settings** section, click **Basic**.

   The **Basic** settings appear.
3. In the **Targets** section, type the IP addresses of:
   - the vCenter host
   - the ESXi host or hosts

   Note: Listing the vCenter as a target results in the scan collecting the vCenter version and its vulnerabilities, but not operating system-level details. Listing the vCenter server as a target is also required for vCenter compliance scanning.
4. In the left navigation menu, click **Credentials**.

   The **Credentials** page appears. This page contains a table of credentials configured for the scan.
5. Next to **Add Credentials**, click the ⊕ button.

   The **Select Credential Type** plane appears.
6. In the **Miscellaneous** section, select **VMware vCenter API**.
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. By default, this value is 443.

9. In the **Username** box, type the username associated with the vCenter account.
10. In the **Password** box, type the password associated with the vCenter account.
11. If the vCenter host is SSL enabled, enable the **HTTPS** toggle.
12. If your vCenter host includes an SSL certificate (not a self-signed certificate), enable the **Verify SSL Certificate** toggle. Otherwise, leave the toggle disabled.
13. Click **Save**.
14. Do one of the following:
    - If you want to save without launching the scan, click **Save**.

      Tenable Vulnerability Management saves the scan.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

      > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

      > **Note:** If you are editing an imported scan, the **Save & Launch** option is not available.

      Tenable Vulnerability Management saves and launches the scan.

Section 3: Scanning Virtual Machines

You can scan virtual machines just like any other host on the network. Be sure to include the IP address or addresses of your virtual machines in the **Targets** text box. For more information, see Create a 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

Copy a Scan Configuration

Required Scan Permissions: Owner

When you copy a scan configuration, Tenable Vulnerability Management assigns you owner permissions for the copy and assigns the copy scan permissions from the original scan.

Note: You cannot copy a scan from the **Remediation Scans** folder.

To copy a scan configuration:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.

3. In the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

4. In the scans table, roll over the scan you want to copy.

5. In the row, click the ⋮ button.

   A menu appears.

6. Click **Copy**.

   The **Copy to Folder** plane appears, which contains a list of your scan folders.

7. Click the folder where you want to save the copy.

8. Click **Copy**.

   Tenable Vulnerability Management creates a copy of the scan with *Copy of* prepended to the name and assigns you owner permissions for the copy. The copy appears in the scans table of the folder you selected.

Export Scan Results

Required Scan Permissions: Can View

You can export both imported scan results and results that Tenable Vulnerability Management collects directly from scanners.

Tenable Vulnerability Management retains individual scan results until the results are 15 months old.

Notes:

- Filters are not applicable for Tenable Web App Scanning exports, All results will are exported.
- For archived scan results (that is, results older than 35 days), Tenable Vulnerability Management limits export types to `.nessus` and `.csv` files.
- When a scan is actively running, the **Export** button does not appear in the Tenable Vulnerability Management interface. Wait until the scan completes, then export the scan results.

To export results for an individual scan:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.
3. In the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

4. Do one of the following:

Location	Scope of Export
Scans table	a. In the scans table, roll over the scan you want to export. b. Click the ⋮ button. A menu appears. c. Click ↦**Export**. The **Export** plane appears. **Note:** You cannot export scan results from the Scans table if the scan has multiple targets. For scans with multiple targets, you can export scan results for each target from the **Scan Details** page.
Scan Details	a. In the scans table, click the scan you want to export. The scan details plane appears below the scan table. b. Click the **Scan Actions** button. A menu appears. c. Click ↦**Export**. The **Export** plane appears.

5. Select an export format:

Format	Description	Supported for Archived Scan Results
Tenable Vulnerability Management Scans		
PDF - Custom	An Adobe `.pdf` file. **Note:**Tenable Vulnerability Management cannot export PDF files with more than 400,000 individual scan	No

	results.	
PDF - Executive Summary	An Adobe `.pdf` file. **Note:** Tenable Vulnerability Management cannot export PDF files with more than 400,000 individual scan results.	No
HTML - Custom	A web-based `.html` file.	No
HTML - Executive Summary	A web-based `.html` file.	No
Nessus	A `.nessus` file in XML format that contains the list of targets, scan settings defined by the user, and scan results. Tenable Vulnerability Management strips password credentials and does not export them as plain text in the XML. If you import a `.nessus` file as a user-defined scan template, you must re-apply your passwords to any credentials. Unlike other export formats, the `.nessus` file includes individual open port findings. This ensures that you can still view open port findings in Tenable Security Center if your organization integrates Tenable Vulnerability Management with Tenable Security Center.	Yes
CSV	A `.csv` text file with only scan results. **Note:** When exporting scan results as a `.csv` file, the severities always show CVSSv2 scores regardless of your configured severity metric. When exporting compliance scan results as a	Yes

	.csv file, the **Risk** column results are replaced with the following values: • PASSED results show as None • WARNING results show as Medium • FAILED results show as High	
Tenable Web App Scanning Scans		
HTML	A web-based .html file that contains the list of targets, scan results, and scan notes.	n/a
PDF	An Adobe .pdf file that contains the list of targets, scan results, and scan notes. **Note:** Tenable Vulnerability Management cannot export PDF files with more than 400,000 individual scan results.	n/a
Nessus	A .nessus file in XML format that contains the list of targets, scan settings defined by the user, and scan results. Tenable Vulnerability Management strips password credentials and does not export them as plain text in the XML.	n/a
CSV	A .csv text file with only scan results.	n/a
JSON	A .json file that contains the list of targets, scan settings defined by the user, scan results, and scan notes. Tenable Vulnerability Management strips password credentials and does not export them as plain text in the JSON file.	n/a

6. For Tenable Vulnerability Management scans, if you select the **PDF - Custom** or **HTML - Custom** formats:

- In the **Data** section, select the **Vulnerabilities**, **Audits**, and **Remediations** checkboxes to include vulnerability data, audit (compliance), and remediation patch information in the export, respectively. You can also leave them unselected to omit the relevant data from the export.

  The **Data** section options available for each scan result vary depending on the scan result's data. For example, if the scan result does not include remediation patch information, the **Remediations** checkbox does not show.

- In the **Group** by section, select **Asset** to group vulnerabilities, audits, and remediations by asset, or select **Plugin** to group them by plugin.

7. Click **Export**.

   Tenable Vulnerability Management generates the export file. Depending on your browser settings, your browser may automatically download the export file to your computer, or may prompt you to confirm the download before continuing.

Import a Scan

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can import scan results into Tenable Vulnerability Management.

Imported scans always belong to the default network. For more information, see Networks.

Note: You can only import Tenable Vulnerability Management scans.

Note: Tenable Vulnerability Management supports scan imports up to 4GB in size.

To import a scan in the new interface:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. In the upper-right corner of the page, click the **Tools** button.

   A menu appears.

3. Click **Import Scan**.

   Your file directory appears.

4. Browse to and select the scan file you want to import.

   If the scan file is a .nessus or .db file, the **Import** plane appears.

   > **Note:** To learn more about the `.nessus` file format, see Nessus File Format.

   If the scan file is any other file type, the **Scan Import** window appears.

5. Do one of the following:

   - If the scan file is a `.nessus` or `.db` file:

     a. In the **Password** box, type the password to allow Tenable Vulnerability Management to view the scan.

     b. (Optional) To show the scan results in dashboards, select the **Show in Dashboard?** check box.

     c. Click **Import**.

   - If the scan file is any other file type, specify if you want the scan results to appear in dashboards:

     - Click **Yes** to show the scan results in dashboards.
     - Click **No** to prevent the scan results from appearing in dashboards.

   > **Note:** Clicking **Cancel** cancels the import.

   The **Scans** page appears, and the imported scan appears in the scans table.

   Tenable Vulnerability Management begins processing the imported scan results. Once this process is complete, the imported data appears in the individual scan details and aggregated data views (such as dashboards). This process can take up to 30 minutes, depending on the size of the import file.

   > **Tip:** If the imported data does not appear in the individual scan results or aggregated data views after a reasonable processing time, verify that you are assigned adequate permissions for the imported targets in access groups.

Organize Scans by Folder

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

In Tenable Vulnerability Management, the **Scans** page contains a **Folders** section that automatically groups your configured and imported scans into default folders. To organize your scans further, you can create custom folders.

To organize your scans by folder:

1. View scans in default folders.

   Note: You cannot rename or delete the default folders.

   By default, Tenable Vulnerability Management provides the following folders:

Folder	Description
My Scans	Contains scans that you have created or imported. This folder appears by default when you access the **Scans** page.

All Scans	• (Administrators) Contains scans created by any users.
	• (All other users) Contains:
	  ◦ Scans that you have created
	  ◦ Any shared scans for which you have **Can View** permissions or higher
	  ◦ Scans that have been moved to the **Trash** folder

Remediation Scans	Contains any remediation scans you own or that another user has shared with you.
Trash	Contains scans that you have moved to the trash. If you have **Can Configure** permissions for a scan in this folder, you can permanently delete the scan for all users.

	If you delete a custom folder that contains scans, Tenable Vulnerability Management automatically moves any scans in the deleted folder to the **Trash** folder.

2. (Optional) Manage custom folders using the following procedures:

Manage scan folders

Use the following procedures to manage your custom scan folders:

Create a custom scan folder

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

The custom scan folders you create appear only to you and cannot be shared with other users. You are the only user who can view, rename, or delete the scan folders you create.

Note: The custom folders you create appear only to you and cannot be shared with other users.

To create a scan folder:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Next to **Folders**, click the ⊕ button.

   The **New Folder** box appears at the bottom of the folder list.

3. In the **New Folder** box, type a name for the folder.

4. Click the ✓ button.

   A **Folder added successfully** message appears and the new folder appears in the **Folders** section.

Move a scan to a scan folder

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Scan Permissions: Can View

You can move a scan from a default folder to either the **My Scans** default folder or a custom scan folder. You can also move a scan from a custom folder to the **My Scans** default folder or a different custom folder.

If you move a scan from the **All Scans** default folder, the scan appears in both the folder you select and the **All Scans** folder.

If you move a scan from the **My Scans** default folder, the scan appears in the custom folder only.

For information about moving a scan to the trash, see Move a Scan to the Trash Folder.

Note: You cannot move scans to or from the **Remediation Scans** folder.

To move a scan to a scan folder:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. In the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

3. In the scan table, roll over the scan you want to move.

   The action buttons appear in the row.

4. Do one of the following:

   - Tenable Vulnerability Management scans:

     a. In the row, click the ⋮ button.

        A menu appears.

b. In the menu, click **Move**.

The **Move to Folder** plane appears. This plane contains a list of your scan folders.

- Tenable Web App Scanning scans:

a. In the row, click the button.

The **Move to Folder** plane appears. This plane contains a list of your scan folders.

5. Search for a folder:

a. In the search box, type the folder name.

b. Click the button.

Tenable Vulnerability Management limits the list to folders that match your search.

6. In the folder list, click the folder where you want to move the scan.

7. Click **Move**.

Tenable Vulnerability Management moves the scan to the selected folder.

Rename a custom scan folder

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can rename custom scan folders only. You cannot rename the default scan folders.

Renaming a scan folder affects your user account only, because the custom folders you create appear only to you and cannot be shared with other users.

To rename a scan folder:

1. In the left navigation, click **Scans**.

The **Scans** page appears.

2. In the **Folders** section, roll over the folder you want to rename.

The action buttons appear in the row.

3. In the row, click the button.

An editable box replaces the folder name.

4. In the box, type a new name for the folder.
5. Click the ✓ button.

   Tenable Vulnerability Management updates the folder name and a **Folder updated successfully** message appears.

Delete a custom scan folder

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can delete custom scan folders only. You cannot delete the default scan folders that Tenable Vulnerability Management provides (**All Scans**, **My Scans**, and **Trash**).

Deleting a scan folder affects your user account only, because the custom folders you create appear only to you and cannot be shared with other users.

If you delete a scan folder that contains inactive scans, Tenable Vulnerability Management moves the folder's scans to the **Trash** folder. If you delete a scan folder that contains at least one active (Pending or Running) scan, Tenable Vulnerability Management moves the folder's scans to the **My Scans** folder.

To delete a scan folder:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. In the **Folders** section, roll over the folder you want to delete.

   The action buttons appear in the row.

3. In the row, click the ✕ button.

   A confirmation window appears.

4. Click **Delete** to confirm the action.

   A **Folder deleted successfully** message appears, and Tenable Vulnerability Management deletes the folder.

Move a Scan to the Trash Folder

Required Scan Permissions: Can View

When you move a shared scan to the **Trash** folder, Tenable Vulnerability Management moves the scan for your account only. The scan remains in the original folder for all other users who have **Can View** permissions or higher for the scan.

Scans moved to the **Trash** folder also appear in the **All Scans** folder, marked with the label, **Trash**.

Note: After you move a scan to the **Trash** folder, the scan remains in the **Trash** folder until the scan owner or an administrator permanently deletes the scan.

Note: Scheduled scans do not run if they are in the scan owner's **Trash** folder.

- For more information about Tenable Vulnerability Management scan schedules, see Schedule.
- For more information about Tenable Web App Scanning scan schedules, see Schedule.

Note: You cannot move scans from the **Remediation Scans** folder to the **Trash** folder. Instead, delete remediation scans directly in the folder.

To move a scan or scans to the **Trash** folder:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.
3. In the **Folders** section, click the folder that contains the scan you want to move.

   The scans table lists scans in the selected folder.

4. Do one of the following:

   - Select a single scan:

     a. In the scans table, roll over the scan you want to move.

     b. Click the ⋮ button.

A menu appears.

c. Click **Trash**.

- Select multiple scans:

  a. In the scans table, select the check box next to each scan you want to move.

  The action bar appears at the top of the table.

  b. In the action bar, click **Trash**.

Tenable Vulnerability Management moves the scan or scans you selected to the **Trash** folder.

Delete a Scan

> **Required Policy Permissions**: Administrator or scan owner

When you permanently delete a scan, you delete the scan configuration and scan results for all users the scan is shared with.

The workflow for deleting a remediation scan differs from the workflow described in this procedure. For more information, see the Delete a remediation scan steps at the end of this topic.

> **Caution**: After you delete a scan, you cannot recover the scan or any scan data associated with the scan. Delete only scans you are certain you no longer need to view or run.

Before you begin:

- Move the scan to the **Trash** folder.

To delete a scan:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.

3. In the **Folders** section, click the **Trash** folder.

   The scan table updates to show the scans in the trash folder.

4. Do one of the following:

   - Select a single scan:

     a. In the scans table, roll over the scan you want to delete.

     b. In the row, click the ⋮ button.

        A menu appears.

     c. Click **Delete**.

        A confirmation window appears.

   - Select multiple scans:

     a. In the scans table, select the check box next to the scans you want to delete.

        The action bar appears at the top of the table.

     b. In the action bar, click the **Delete** button.

        A confirmation window appears.

5. In the confirmation window, click **Delete**.

   Tenable Vulnerability Management deletes the scan or scans you selected.

Delete a remediation scan

> **Required Scan Permissions**: Can Configure

When you delete a remediation scan, you delete the scan configuration and scan results for all users the scan is shared with.

> **Note:** Tenable Vulnerability Management deletes scan results older than 90 days.

To delete a remediation scan:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Scans**.

The **Scans** page appears.

3. In the **Folders** section, click the **Remediation Scans** folder.

   Note: The **Remediation Scans** folder only shows for Tenable Vulnerability Management scans.

   The scan table updates to show remediation scans that you own or that other users have shared with you. By default, the rows are sorted by **Created Date**.

4. Do one of the following:

   - Select a single scan:

     a. In the scans table, roll over the scan you want to delete.

     b. In the row, click the ⋮ button.

     A menu appears.

     c. Click **Delete**.

     A confirmation window appears.

   - Select multiple scans:

     a. In the scans table, select the check box next to the scans you want to delete.

     The action bar appears at the top of the table.

     b. In the action bar, click the **Delete** button.

     A confirmation window appears.

5. In the confirmation window, click **Delete**.

   Tenable Vulnerability Management deletes the scan or scans you selected.

   Note: Tenable Vulnerability Management keeps up to 10,000 of the most recent remediation scan results. Once you have more than 10,000 remediation scan results, Tenable Vulnerability Management deletes the scan results, starting with the oldest result.

Discovery Scans vs. Assessment Scans

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.

For information about how discovered and assessed assets are counted towards your license, see Tenable Vulnerability Management Licenses.

Type	Description	Licensing
Discovery scans	Find assets on your network. For example: • a scan configured with the **Host Discovery** template. • a scan configured to use only discovery plugins. • a scan configured to use Tenable Network Monitor in discovery mode.	Assets identified by discovery scans do not count toward your license.
Assessment scans	Find vulnerabilities on your assets. For example, run an *authenticated* or *unauthenticated* scan using a Tenable Nessus scanner or Tenable Agent. **Authenticated 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	In general, assets assessed by assessment scans count toward your license.

	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 in Tenable Vulnerability Management Scans. **Unauthenticated 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.	

Identify Assets That Have Not Been Assessed

Tenable Vulnerability Management can discover, or *see*, assets without assessing the assets for vulnerabilities (for example, via a host discovery scan, Tenable Network Monitor running in discovery mode, or connectors). Assets that have been seen but not assessed do not count towards your asset license limit. For a list of conditions that cause an asset to be assessed, see How Assets are Counted. However, once assessed, the asset is always categorized as assessed, even if it ages out of the license count.

This licensing exception allows you to discover assets on your network without the large number of assets counting towards your license limit. After you discover your assets, you can then identify

which assets have not yet been assessed for vulnerabilities, and choose which of those assets you want to scan and manage going forward.

To identify assets that have not been assessed:

1. Discover assets using any of the following methods:

   - Create and launch a host discovery scan in Tenable Vulnerability Management.
   - Configure Tenable Network Monitor with discovery mode enabled, linked to Tenable Vulnerability Management.
   - Configure a connector.

   Assets discovered by these methods do not count towards your asset license limit until they have been assessed for vulnerabilities.

2. Filter for assets that have not been assessed.

   a. In the assets table, create a filter with the following settings:

      - In the **Category** box, select **Asset Assessed**.
      - In the **Operator** box, select **is equal to**.
      - In the **Value** box, select **false**.

   a. Click **Apply**.

      Tenable Vulnerability Management filters for assets that have not yet been assessed for vulnerabilities.

      > **Note:** Unassessed assets (where **Asset Assessed** is equal to **false**) can differ from unlicensed assets (where **Is Licensed (VM)** is equal to **false**). Once you scan an asset for vulnerabilities, Tenable Vulnerability Management categorizes the asset as assessed from that point on, but the licensing status of an asset can change over time as assets are deleted or age out of your organization's license count.

   b. (Optional) Save the search for later use.

3. (Optional) Tag assets to identify assets that have not been assessed.

a. Create tags to identify assets that have not been assessed.

   For example, Assets:NotYetAssessed.

b. Manually apply the tag to assets, or create tag rules that automatically filter for assets that have not been assessed.

   For example, to create a dynamic tag for assets that have not yet been assessed, set the tag rules to filter for **Asset Assessed is equal to false**.

4. (Optional) Create a scan to target assets using the tag you created.

Scan Failovers

If Tenable Vulnerability Management assigns a scan job to a scanner, and the scanner goes offline while scanning, the following happens:

1. The scan job times out if the assigned scanner does not respond to Tenable Vulnerability Management after two hours.
2. Tenable Vulnerability Management removes the scan job from the scanner and attempts the scan job on another scanner in the same scanner group, or on the same scanner if it comes back online.
3. Tenable Vulnerability Management attempts steps 1 and 2 three times. If the scan job is not completed after three attempts, Tenable Vulnerability Management aborts the scan job.

Scan Status

Tenable Vulnerability Management provides a scan status for each of your configured scans.

If the scan is in progress, Tenable Vulnerability Management shows the number of scan tasks completed as a percentage.

For example, if you scan less than 120 IP addresses in a single scan, Tenable Vulnerability Management creates a single scan task and the progress percentage changes from 0% to 100% when it completes.

However, if you target more than 120 IP addresses, Tenable Vulnerability Management creates multiple scan tasks. After each task completes, the percentage changes to reflect the number of completed tasks. For example, a scan that targets 300 IP addresses is split into three scan tasks,

and as each task completes, the progress bar updates the percentage to reflect the completed tasks.

Note: Pausing a scan causes Tenable Vulnerability Management to move any completed results to processing. When you resume the scan, Tenable Vulnerability Management creates a new scan task or tasks for incomplete results. Therefore, pausing a scan can cause the progress percentage to update.

Tip: For Tenable Vulnerability Management scans, you can hover over the scan status to view more status information in a pop-up window, such as the number of targets scanned and the elapsed or final scan time. The window shows different information based on the scan's current status.

Tenable Vulnerability Management scans can have the following status values:

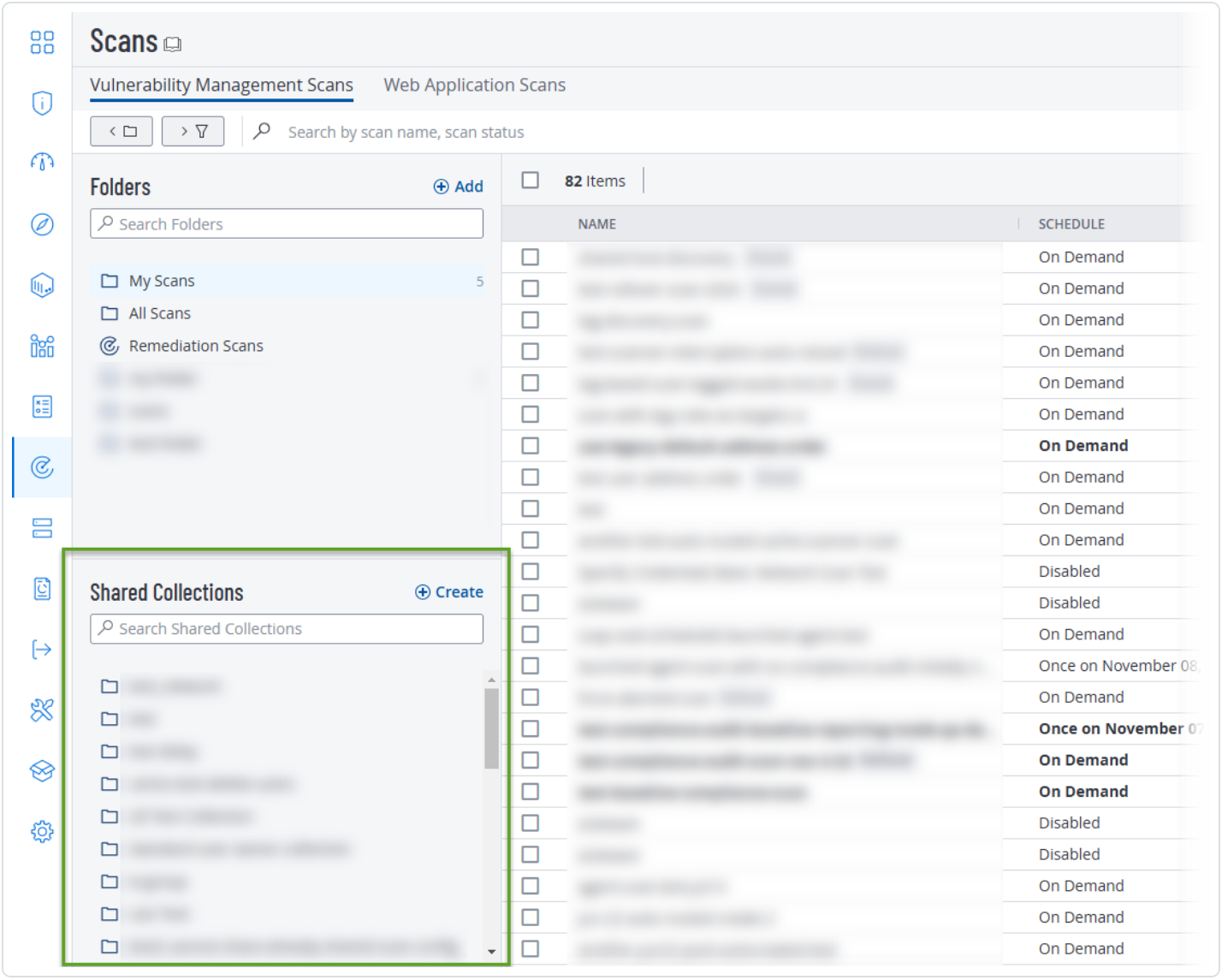
Status	Description
Tenable Vulnerability Management Scans **Tip:** The typical Tenable Vulnerability Management scan status flow is as follows: **Initializing**, **Running**, **Publishing Results**, **Completed**.	
Aborted	Either the latest run of the scan is incomplete because Tenable Vulnerability Management or the scanner encountered problems during the run, or the scan remained queued without running for four or more hours. For more information about the problems encountered during the run, view the scan warnings.
Canceled	At user request, Tenable Vulnerability Management successfully stopped the latest run of the scan.
Completed	The latest run of the scan is complete.
Disabled	(Triggered agent scans only) The scan configuration is disabled and does not launch scans based on the configured triggers. You can enable or disable triggered agent scan configurations in the scan table's **Actions** ⋮ menu.
Empty	The scan is either empty (the scan is new or has yet to run) or pending (Tenable Vulnerability Management is processing a request to run the scan).
Enabled	(Triggered agent scans only) The scan configuration is enabled and launches scans based on the configured triggers. You can enable or disable triggered

Status	Description
	agent scan configurations in the scan table's **Actions** ⋮ menu.
Imported	A user imported the scan. You cannot run imported scans. Scan history is unavailable for imported scans.
Pausing	A user paused the scan, and Tenable Vulnerability Management is processing the action.
Paused	At user request, Tenable Vulnerability Management successfully paused active tasks related to the scan. The paused tasks continue to fill the task capacity of the scanner that the tasks were assigned to. Tenable Vulnerability Management does not dispatch new tasks from a paused scan job. If the scan remains in a paused state for more than 14 days, the scan times out. Tenable Vulnerability Management then aborts the related tasks on the scanner and categorizes the scan as aborted.
Pending	Tenable Vulnerability Management has the scan queued to launch and is assigning scan tasks to the assigned sensors. **Note**: Tenable Vulnerability Management aborts scans that remain in **Pending** status for more than four hours. If Tenable Vulnerability Management aborts your scan, modify your scan schedule to reduce the number of overlapping scans. If you still have issues, contact Tenable Support.
Publishing Results	Tenable Vulnerability Management processes and stores the scan results data for you to view and use in the Tenable Vulnerability Management user interface. The **Publishing Results** status begins once the **Running** status reaches 100%.
Resuming	Tenable Vulnerability Management is in the process of restarting tasks after the user resumed the scan. Tenable Vulnerability Management instructs the scanner to start the tasks from the point at which the scan was paused. If Tenable Vulnerability Management or the scanner encounters problems when resuming the scan, the scan fails, and Tenable Vulnerability Management updates the scan status to aborted.

Status	Description
Running	The scan is currently running. While this status is shown, the scan's sensors complete their assigned scan tasks, and Tenable Vulnerability Management processes the scan results. The progress bar shows next to the status when a scan is running. The progress bar shows the percentage of the completed tasks.
Stopping	A user stopped the scan, the scan timed out or reached the end of the configured scan window, or Tenable Vulnerability Management is stopping the scan after all associated scan tasks are complete.

Shared Collections

On the **Scans** page in Tenable Vulnerability Management, you can create and manage *shared collections*. Shared collections allow you to quickly and conveniently share scan configurations with specific groups and other Tenable Vulnerability Management users.



Note: Shared collections are only available for vulnerability management scans.

Create a shared collection

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. In the **Shared Collections** section, click **Create**.

   The **Create Shared Collection** pane opens.

3. Enter the following information for the shared collection:

Setting	Description
Name	(Required) The name of the shared collection.
Description	The description of the shared collection.
Add Users or Groups	Determines what users and groups have access to the shared collection. To add a new user or group: a. Click the **Select Users or Groups** dropdown. A list of your organization's users and groups appear. Note that your user account is already listed as **Owner**. Each shared collection can only have one **Owner**, but ownership can be transferred by the current owner or by an administrator. b. Search for and select the user or group that you want to add permission for. **Tip:** You can scroll to the bottom of the dropdown and select **All Users** to set global permissions. The selected user or group appears below the dropdown. c. Select the **Can View** dropdown next to the selected user or group. • To give the user or group view access, select **Can View**. • To give the user or group editing access, select **Can Edit**. **Note:** Users with the **Administrator** role automatically have **Can Edit** access to all shared collections. **Note:** To give a group **Can Edit** access to a shared collection, every user in the group must have the **Scan Operator** privilege or higher for shared collections (or a custom role with the **Manage Shared Collections** privilege). After you give a group **Can Edit** access, you can add users with lower privileges to

	the group, but those users are not able to modify the shared collection. d. Repeat steps a-c to add your desired users and groups.

4. Click **Save**.

   Tenable Vulnerability Management creates the new shared collection. You can view the new collection under the **Shared Collections** header on the **Scans** page.

Add scans to a shared collection

Note: To add a scan configuration to a shared collection, you must have **Can View** permission or higher for the scan configuration you are adding and **Can Edit** or **Owner** permission for the shared collection you are adding to.

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Search for the scan or scans that you want to add to a shared collection.

3. Do one of the following:

   - To add a single scan to a shared collection:

     a. In the scan row of the scan table, right-click or click ⋮ in the **Actions** column.

        A list of actions appears.

     b. Click ⊕ **Add to Shared Collection**.

        The **Add to Shared Collection** pane appears.

   - To add multiple scans to a shared collection:

     a. In the scans table, select the checkboxes of each scan that you want to add.

     b. Right-click in the scans table or click ⋮ **More** in the table header.

        A list of actions appears.

c. Click ⊕ **Add to Shared Collection**.

   The **Add to Shared Collection** pane appears.

4. Select the shared collection to add the scan or scans to.
5. Click **Save**. Tenable Vulnerability Management adds the scan or scans to the shared collection.

Remove scans from a shared collection

Note: To remove a scan configuration from a shared collection, you must have **Can View** permission or higher for the scan configuration you are removing and **Can Edit** or **Owner** permission for the shared collection you are removing from.

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. In the **Shared Collections** section, open the shared collection you want to remove scans from .
3. Do one of the following:

   - To remove a single scan to a shared collection:

     a. In the scan row of the scan table, right-click or click ⋮ in the **Actions** column.

        A list of actions appears.

     b. Click ⊖ **Remove from Shared Collection**.

        The **Remove Scans from Shared Collection** window appears.

   - To remove multiple scans to a shared collection:

     a. In the scans table, select the checkboxes of each scan that you want to remove.

     b. Right-click in the scans table or click ⋮ **More** in the table header.

        A list of actions appears.

c. Click ⊖ **Remove from Shared Collection**.

The **Remove from Shared Collection** pane appears.

4. Click **Continue**. Tenable Vulnerability Management removes the scan or scans from the shared collection.

Edit a shared collection

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. In the **Shared Collections** section, hover over the shared collection you want to edit.
3. Click ✎ to edit the shared collection.

   The **Edit Shared Collection** pane opens.

4. Edit the following settings as needed:

Setting	Description
Name	(Required) The name of the shared collection.
Description	The description of the shared collection.
Add Users or Groups	Determines what users and groups have access to the shared collection. To add a new user or group: a. Click the **Select Users or Groups** dropdown. A list of your organization's users and groups appear. b. Search for and select the user or group that you want to add permission for. **Tip:** You can scroll to the bottom of the dropdown and select **All Users** to set global permissions. The selected user or group appears below the dropdown. c. Select the **Can View** dropdown next to the selected user or

	group. • To give the user or group view access, select **Can View**. • To give the user or group editing access, select **Can Edit**. **Note:** Users with the **Administrator** role automatically have **Can Edit** access to all shared collections. d. Repeat steps a-c to add your desired users and groups.

5. Click **Save**. Tenable Vulnerability Management updates the shared collection.

Delete a shared collection

Note: Only the shared collection's **Owner** can delete the shared collection.

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. In the **Shared Collections** section, hover over the shared collection you want to delete.
3. Click ✕ to delete the shared collection.

   A confirmation window appears in the upper-right corner.

4. Click **Delete** to confirm the deletion.

   The shared collection is deleted. The scan data in the deleted shared collection is still available in your standard folders.

Scan Templates

Scan templates contain granular configuration settings for your scans. You can use Tenable's scan templates to create custom scan configurations for your organization. Then, you can run scans based on Tenable's scan templates or your custom configurations' settings.

When you create a scan configuration, the **Select a Scan Template** page appears. Tenable Vulnerability Management provides separate templates for Tenable Vulnerability Management and

Tenable Web App Scanning. Within Tenable Vulnerability Management scanning, Tenable Vulnerability Management provides separate templates for scanners and agents, depending on which sensor you want to use for scanning:

If you have custom configurations, they appear in the **User Defined** tab. For more information about user-defined templates, see User-Defined Templates.

When you configure a Tenable-provided scan template, you can modify only the settings included for the scan template type. When you create a user-defined scan template, you can modify a custom set of settings for your scan.

For descriptions of all scan template settings, see Scan Settings.

> **Tip:** For information and tips on optimizing your Tenable Vulnerability Management scan configurations, see the Tenable Vulnerability Management Scan Tuning Guide.

Tenable-Provided Tenable Nessus Scanner Templates

There are three scanner template categories in Tenable Vulnerability Management:

- Vulnerability Scans (Common) – Tenable recommends using vulnerability scan templates for most of your organization's standard, day-to-day scanning needs.
- Configuration Scans – Tenable recommends using configuration scan templates to check whether host configurations are compliant with various industry standards. Configuration scans are sometimes referred to as *compliance* scans. For more information about the checks that compliance scans can perform, see Compliance in Tenable Vulnerability Management Scans and SCAP Settings in Tenable Vulnerability Management Scans.
- Tactical Scans – Tenable recommends using the tactical scan templates to scan your network for a specific vulnerability or group of vulnerabilities. Tactical scans are lightweight, timely scan templates that you can use to scan your assets for a particular vulnerability. Tenable frequently updates the Tenable Vulnerability Management Tactical Scans library with templates that detect the latest vulnerabilities of public interest, such as Log4Shell.

The following table describes the available Tenable Nessus Scanner templates:

Template	Description
Vulnerability Scans (Common)	

Advanced Network 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 Tenable Vulnerability Management experts 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 Vulnerability Management direct access to the host, scan the target hosts, and enumerate missing patch updates.
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 Tenable 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.
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).
Legacy Web App Scan	Uses a Tenable Nessus scanner to scan your web applications. **Note:** Unlike the Tenable Web App Scanning scanner, the Tenable Nessus scanner does not use a browser to scan your web applications. Therefore, a **Legacy Web App Scan** is not as comprehensive as Tenable Web App Scanning.
Mobile Device Scan	Assesses mobile devices via Microsoft Exchange or an MDM.
PCI Quarterly External Scan	Performs quarterly external scans as required by PCI. **Note:** Because the nature of a PCI ASV scan is more paranoid and may lead to false positives, the scan data is not included in the aggregate Tenable Vulnerability Management data. This is by design. **Note:**Tenable Vulnerability Management excludes **PCI Quarterly External** scan data from dashboards, reports, and workbenches intentionally. This is due to the scan's paranoid nature, which may lead to false positives that Tenable Vulnerability Management would otherwise not detect. For more information, see Tenable PCI ASV Scans.
Configuration Scans	
Audit Cloud Infrastructure	Audits the configuration of third-party cloud services. You can use this template to scan the configuration of Amazon Web Service (AWS), Google Cloud Platform, Microsoft Azure, Rackspace, Salesforce.com, and Zoom, given that you provide credentials for the service you want to audit.

MDM Config Audit	Audits the configuration of mobile device managers. The MDM Config Audit template reports on a variety of MDM vulnerabilities, such as password requirements, remote wipe settings, and the use of insecure features, such as tethering and Bluetooth.
Offline Config Audit	Audits the configuration of network devices. Offline configuration audits allow Tenable Vulnerability Management to scan hosts without the need to scan over the network or use credentials. Organizational policies may not allow you to scan devices or know credentials for devices on the network for security reasons. Offline configuration audits use host configuration files from hosts to scan instead. Through scanning these files, you can ensure that devices' settings comply with audits without the need to scan the host directly. Tenable recommends using offline configuration audits to scan devices that do not support secure remote access and devices that scanners cannot access.
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.
Tactical Scans	
Active Directory Identity	Use a Domain User account to query AD identity information. This policy enumerates Active Directory identity information via LDAPS. It requires Domain User credentials, LDAPS configuration, and an Active Directory Domain Controller as the scan target.
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 AI, LLM, and ML-related vulnerabilities.
Malware Scan	Scans for malware on Windows and Unix systems.
Nessus 10.8.0 /	Scan to find, reset, and update Tenable Agents on versions 10.8.0 and

10.8.1 Agent Reset	10.8.1. For more information, see the upgrade notes of the Tenable Agent 10.8.2 release notes.
Ping-Only Discovery	A simple scan to discover live hosts with minimal network traffic.

Tenable-Provided Tenable Agent Templates

There are two agent template categories in Tenable Vulnerability Management:

- Vulnerability Scans – Tenable recommends using vulnerability scan templates for most of your organization's standard, day-to-day scanning needs.
- Inventory Collection – Unlike standard Tenable Agent vulnerability scans, the Collect Inventory template provides faster scan results and reduce the scan's system footprint. Agent-based inventory scans gather basic information from a host and upload it to Tenable Vulnerability Management. Then, Tenable Vulnerability Management analyzes the information against missing patches and vulnerabilities as Tenable releases coverage. This reduces the performance impact on the target host while also reducing the time it takes for an analyst to see the impact of a recent patch.

Note: If a plugin requires authentication or settings to communicate with another system, the plugin is not available on agents. This includes, but is not limited to:

- Patch management
- Mobile device management
- Cloud infrastructure audit
- Database checks that require authentication

The following table describes the available Tenable Agent templates:

Template	Description
Vulnerability Scans	
Advanced Agent Scan	An agent scan without any recommendations, so that you can fully customize the scan settings. In Tenable Vulnerability Management, the Advanced Agent Scan template allows for two scanning methods:

Template	Description
	• Scan Window - Specify the timeframe during which the agent must report to be included and visible in vulnerability reports. • Triggered Scans - Provide the agent with specific criteria that indicates when to launch a scan. The agent launches the scan when one (or more) of the criteria are met. For more information, see Basic Settings in the *Tenable Vulnerability Management User Guide*. **Note:** When you create an agent scan using the Advanced Agent Scan template, you must also select the plugins you want to use for the scan.
Agent Log4Shell	Agent detection of Apache Log4j CVE-2021-44228.
Basic Agent Scan	Scans systems connected via Tenable Agents.
Malware Scan	Scans for malware on systems connected via Tenable Agents. Tenable Agent 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.
PCI Internal Nessus Agent	Perform an internal PCI DSS 4.0 credentialed vulnerability scan. This template creates scans that you can use to satisfy internal (PCI DSS 4.0) 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. PCI DSS 4.x provides the ability to use a customized approach objective. Using PCI DSS 4.x, this template provides the most comprehensive view of local vulnerabilities on your systems. For systems where agents cannot be installed, the defined approach in

Template	Description
	11.3.1.2 (by way of the **Internal PCI Network Scan** template) is still applicable. Internal, uncredentialed network scans are still required to cover vulnerabilities related to network services by port scans. **Note:** Tenable highly recommends configuring the **Open Agent Port** profile setting for any agents that run scans based on this template to avoid asset duplication. For more information, see Agent Profiles. **Note:** Tenable assessors do not review internal PCI scans for false positives or compensating controls. Therefore, Tenable highly recommends using your organization's internal security assessor (ISA) or qualified security assessor (QSA) to validate internal scan findings.
Policy Compliance Auditing	Audits system configurations against a known baseline for systems connected via Tenable Agents. 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 Agent Auditing	Audits systems using SCAP and OVAL definitions for systems connected via Tenable Agents. 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

Template	Description
	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.
Inventory Collection	
Collect Inventory	Scans with a compiled, limited selection of software inventory plugins. This template provides faster scan results and a reduced system footprint because the agent only performs checks that collect asset information (for example, installed software and IP addresses). This scanning method is sometimes referred to as *inventory scanning* in the Tenable Vulnerability Management user interface and documentation. Collect Inventory scans provide coverage for: • RedHat local security checks • Oracle Linux local security checks • CentOS local security checks • Amazon Linux local security checks • Debian local security checks • Fedora local security checks • SUSE local security checks • Ubuntu local security checks • Windows/Microsoft bulletin checks (All Windows roll-up checks since 2017) Collect Inventory scans do not currently provide coverage for: • Malware and compliance checks

Template	Description
	• Third-party Linux application detection (for example, Apache HTTP or Postgres) for instances not installed via dpkg or rpm • Third-party Windows applications (for example, Google Chrome or Mozilla Firefox) • Microsoft product Patch Tuesday updates (for example, Exchange or Sharepoint) **Note:** An asset that Tenable Vulnerability Management has performed inventory scanning on continues to report vulnerabilities until the asset ages out, even if the asset is offline.

Tenable-Provided Tenable Web App Scanning Templates

The following table describes the available Tenable Web App Scanning scan templates:

Template	Description
API	A scan that checks an API for vulnerabilities. This scan analyzes RESTful APIs described via an OpenAPI (Swagger) specification file. File attachment size is limited to 1 MB. **Tip:** If the API you want to scan requires keys or a token for authentication, you can add the expected custom headers in the Advanced settings in the **HTTP Settings** section. **Note:** The API scan template is available as a public beta. Its functionality is subject to change as ongoing improvements are made throughout the beta period. **Note:** API scans support only one target at a time.
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 the **Config Audit** scan template, Tenable Web App

	Scanning analyzes your web application only for plugins related to security industry standards compliance.
Log4Shell	Detects the Log4Shell vulnerability (CVE-2021-44228) in Apache Log4j via local checks.
Overview	A high-level preliminary scan that determines which URLs in a web application Tenable Web App Scanning scans by default. The **Overview** scan template does not analyze the web application for active vulnerabilities. Therefore, this scan template does not offer as many plugin family options as the **Scan** template.
PCI	A scan that assesses web applications for compliance with Payment Card Industry Data Security Standards (PCI DSS) for Tenable PCI ASV.
Quick Scan	A high-level scan similar to the **Config Audit** scan 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 template, Tenable Vulnerability Management 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** template provides plugin family options for all active web application plugins. If you create a scan using the **Scan** template, Tenable Web App Scanning analyzes your web application for all plugins that the scanner checks for when you create a scan using the **Config Audit**, **Overview**, or **SSL TLS** 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 Tenable Web App Scanning 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** template, Tenable Web App Scanning analyzes your web application only for plugins related to SSL/TLS implementation. The scanner does not crawl URLs or assess individual pages for vulnerabilities.

User-Defined Templates

Required Template Permissions: Owner

Tenable provides a variety of scan templates for specific scanning purposes. If you want to customize a Tenable-provided scan template and share it with other users, you can create a user-defined scan template.

For information about any scan settings, see Scan Settings.

You can create, edit, copy, export, or delete user-defined Tenable Vulnerability Management and Tenable Web App Scanning Scan templates from the **Scans** page. You can also import and export Tenable Vulnerability Management scan templates.

To manage your user-defined scan templates:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. In the upper-right corner of the page, click the **Tools** button.

   A menu appears.

3. Select **Manage Scan Templates**.

   The **Scan Templates** page appears.

4. Below **Scan Templates**, choose to view **Vulnerability Management Scan Templates** or **Web Application Scan Templates**.

   The scan template table updates based on your selection.

Click a template to view or edit its settings and parameters, or use the following procedures to further manage your user-defined templates:

Create a user-defined template

You can create user-defined scan templates to save and share custom scan settings with other Tenable Vulnerability Management users.

When you define a scan template, Tenable Vulnerability Management assigns you owner permissions for the scan template. You can share the scan template by assigning template permissions to other users, but only you can delete the scan template.

To create a user-defined scan template:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.
3. In the upper-right corner of the page, click the ⊕ **Create Template** button.

   The **Select a Template** page appears.

4. Click the tile for the template you want to use as the base for your user-defined scan template.

   The **Create a Template** page appears.

5. Do one of the following:

   - If you are creating a Tenable Vulnerability Management scan template, use the following procedure:

a. Configure the scan template:

Tab	Action
Settings	Configure the settings available in the scan template. • Basic Settings – Specifies the name of the scan template, its description, and who has permissions for the scan template. • Discovery Settings – Specifies how a scan performs discovery and port scanning. • Assessment Settings – Specifies how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications. • Report Settings – Specifies whether the scan generates a report. • Advanced Settings – Specifies advanced controls for scan efficiency.
Credentials	Specify credentials you want Tenable Vulnerability Management to use to perform a credentialed scan.
Compliance/SCAP	Specify the platforms you want to audit. Tenable, Inc. provides best practice audits for each platform. Additionally, you can upload a custom audit file.
Plugins	Select security checks by plugin family or individual plugin.

- If you are creating a Tenable Web App Scanning scan, use the following procedure:

a. Configure the scan:

Tab	Action
Settings	Configure the settings available in the scan template. For more information, see Basic Settings in Tenable Web App Scanning Scans.
Scope	Specify the URLs and file types that you want to include in or exclude from your scan. For more information, see Scope Settings in Tenable Web App Scanning Scans.
Assessment	Specify how a scan identifies vulnerabilities and what vulnerabilities the scan identifies. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications. For more information, see Assessment Settings in Tenable Web App Scanning Scans.
Advanced	Specify advanced controls for scan efficiency.
Credentials	Specify credentials you want Tenable Vulnerability Management to use to perform a credentialed scan.
Plugins	Select security checks by plugin family or individual plugin.

6. Click **Save**.

   Tenable Vulnerability Management saves the user-defined scan template and adds it to the list of scan templates on the **Scan Templates** page.

Edit a user-defined template

Required Template Permissions: Can Configure

To edit a user-defined scan template:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.
3. In the upper-right corner of the page, click the **Tools** button.

   A menu appears.

4. Select **Manage Scan Templates**.

   The **Scan Templates** page appears.

5. In the scan templates table, click the scan template you want to edit.

   The **Edit a Scan Template** page appears.

6. Do one of the following:

- If you are editing a Tenable Vulnerability Management scan template, use the following procedure:

a. Configure the scan template options:

Tab	Action
Settings	Configure the settings available in the scan template. • Basic Settings – Specifies the name of the scan template, its description, and who has permissions for the scan template. • Discovery Settings – Specifies how a scan performs discovery and port scanning. • Assessment Settings – Specifies how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications. • Report Settings – Specifies whether the scan generates a report. • Advanced Settings – Specifies advanced controls for scan efficiency.
Credentials	Specify credentials you want Tenable Vulnerability Management to use to perform a credentialed scan.
Compliance/SCAP	Specify the platforms you want to audit. Tenable, Inc. provides best practice audits for each platform. Additionally, you can upload a custom audit file.
Plugins	Select security checks by plugin family or individual plugin.

- If you are editing a Tenable Web App Scanning scan template, use the following procedure:

    a. Configure the scan template options:

Tab	Action
Settings	Configure the settings available in the scan template. For more information, see Basic Settings in Tenable Web App Scanning Scans.
Scope	Specify the URLs and file types that you want to include in or exclude from your scan. For more information, see Scope Settings in Tenable Web App Scanning Scans.
Assessment	Specify how a scan identifies vulnerabilities and what vulnerabilities the scan identifies. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications. For more information, see Assessment Settings in Tenable Web App Scanning Scans.
Advanced	Specify advanced controls for scan efficiency.
Credentials	Specify credentials you want Tenable Vulnerability Management to use to perform a credentialed scan.
Plugins	Select security checks by plugin family or individual plugin.

7. Click **Save**.

    Tenable Vulnerability Management saves the user-defined scan template and adds it to the list of templates on the **Scan Templates** page.

Copy a user-defined template

When you copy a user-defined scan template, Tenable Vulnerability Management assigns you owner permissions for the copy. You can share the copy by assigning template permissions to other users, but only you can delete the copied scan template.

To copy a user-defined scan template:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.

3. In the upper-right corner of the page, click the **Tools** button.

   A menu appears.

4. Select **Manage Scan Templates**.

   The **Scan Templates** page appears.

5. In the scans table, roll over the scan you want to launch.

6. In the row, click the ⋮ button.

   A menu appears.

7. In the menu, click the button.

   A **Template copied** message appears. Tenable Vulnerability Management creates a copy of the scan template with *Copy of* prepended to the name and assigns you owner permissions for the copy. The copy appears in the scan templates table.

Export a user-defined template (Tenable Vulnerability Management only)

You can export a user-defined scan template for later import.

> **Note:** Tenable Vulnerability Management does not export passwords, credentials, and file-based settings (for example, `.audit` files and the SSH **known_hosts file**) in user-defined scan templates.

To export a user-defined scan template:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans**

3. In the upper-right corner of the page, click the **Tools** button.

A menu appears.

4. Select **Manage Scan Templates**.

   The **Scan Templates** page appears.

5. In the scans table, roll over the scan template you want to export.
6. In the row, click the ⋮ button.

   A menu appears.

7. In the row, click the [→ button.

   Tenable Vulnerability Management exports the user-defined scan template as a `.nessus` file.

   > **Note:** To learn more about the `.nessus` file format, see Nessus File Format.

Import a user-defined template (Tenable Vulnerability Management only)

When you import a scan template, Tenable Vulnerability Management assigns you owner permissions for the scan template. You can share the scan template by assigning template permissions to other users, but only you can delete the scan template.

Tenable Vulnerability Management does not include passwords or compliance audit files in exported user-defined scan templates. You must add these settings in manually after importing the scan template.

To import a user-defined scan template:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans**.
3. In the upper-right corner of the page, click the **Tools** button.

   A menu appears.

4. Select **Manage Scan Templates**.

   The **Scan Templates** page appears.

5. In the upper-right corner of the page, click the **Import** button.

   Your file manager appears.

6. Select the scan template you want to import.
7. Click **Open**.

   A **Template uploaded** message appears, and the scan template appears on the **Scan Templates** page.

What to do next:

- As needed, add passwords and compliance audit files to the imported template.

Delete a user-defined template

If you delete a user-defined scan template, Tenable Vulnerability Management deletes it from all user accounts.

Before you begin:

- Delete any scans that use the template you want to delete. You cannot delete a scan template if a scan is using the template.

To delete a user-defined scan template or templates:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.
3. In the upper-right corner of the page, click the **Tools** button.

   A menu appears.

4. Select **Manage Scan Templates**.

   The **Scan Templates** page appears.

5. Select the scan template or templates you want to delete:

- Select a single scan template:

  a. In the scans table, roll over the scan you want to launch.

  b. In the row, click the ⋮ button.

     A menu appears.

  c. In the menu, click the 🗑 button.

     A confirmation window appears.

- Select multiple scan templates:

  a. In the scan templates table, select the check box for each scan template you want to delete.

     The action bar appears at the bottom of the page.

  b. In the action bar, click the 🗑 button.

     A confirmation window appears.

6. In the confirmation window, click **Delete**.

   Tenable Vulnerability Management deletes the user-defined scan template or templates you selected.

Change user-defined template ownership

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Required Template Permissions: Owner

To change the ownership of a user-defined scan template in the new interface:

1. Edit a user-defined template.
2. In the left navigation menu, in the **Settings** section, click **Basic**.

   The **Basic** settings appear.

3. In the **User Permissions** section, next to the permission drop-down for **Owner**, click the ⌄ button.

   A list of available user accounts appears.

4. Select a user from the list.

   Tenable Vulnerability Management automatically adds you to the list of users and assigns **Can View** permissions to your user account.

5. (Optional) Remove all permissions for your user account:

   a. In the user list, roll over your user account.

      The ✕ button appears at the end of the listing.

   b. Click the ✕ button.

      Tenable Vulnerability Management removes your account from the list of users.

6. (Optional) Edit permissions for your user account:

   a. Next to the permission drop-down for your user account, click the ⌄ button.

   b. Select a permission.

7. Click **Save**.

   Tenable assigns ownership to the selected user and assigns your user account the permissions you selected. If you removed all permissions for your user account from the template, the template no longer appears in the templates table.

Scan Settings

Scan settings enable you to refine parameters in scans to meet your specific network security needs. The scan settings you can configure vary depending on the Tenable-provided template on which a scan or user-defined template is based.

You can configure these settings in individual scans or in user-defined templates from which you create individual scans.

Scan settings are organized into the following categories:

Tenable Vulnerability Management Scans	Tenable Web App Scanning Scans
• Basic Settings in User-Defined Templates • Basic Settings in Tenable Vulnerability Management Scans • Discovery Settings in Tenable Vulnerability Management Scans • Assessment Settings in Tenable Vulnerability Management Scans • Report Settings in Tenable Vulnerability Management Scans • Advanced Settings in Tenable Vulnerability Management Scans • Credentials in Tenable Vulnerability Management Scans • Compliance in Tenable Vulnerability Management Scans • SCAP Settings in Tenable Vulnerability Management Scans • Configure Plugins in Tenable Vulnerability Management Scans	• Basic Settings in User-Defined Templates • Basic Settings in Tenable Web App Scanning Scans • Scope Settings in Tenable Web App Scanning Scans • Report Settings in Tenable Web App Scanning Scans • Assessment Settings in Tenable Web App Scanning Scans • Advanced Settings in Tenable Web App Scanning Scans • Credentials in Tenable Web App Scanning Scans • Plugin Settings in Tenable Web App Scanning Scans

Settings in User-Defined Templates

When configuring settings for user-defined templates, note the following:

- If you configure a setting in a user-defined template, that setting applies to any scans you create based on that user-defined template.
- You base a user-defined template on a Tenable-provided template. Most of the settings are identical to the settings you can configure in an individual scan that uses the same Tenable-provided template.

However, certain **Basic** settings are unique to creating a user-defined template, and do not appear when configuring an individual scan. For more information, see Basic Settings in User-Defined Templates.

- You can configure certain settings in a user-defined template, but cannot modify those settings in an individual scan based on a user-defined template. These settings include **Discovery**, **Assessment**, **Report**, **Advanced**, **Compliance**, **SCAP**, and **Plugins**. If you want to modify these settings for individual scans, create individual scans based on a Tenable-provided template instead.
- If you configure **Credentials** in a user-defined template, other users can override these settings by adding scan-specific or managed credentials to scans based on the template.

Tenable Vulnerability Management Scan Settings

Scan settings enable you to refine parameters in scans to meet your specific network security needs. The scan settings you can configure vary depending on the Tenable-provided template on which a scan or user-defined template is based.

You can configure these settings in individual scans or in user-defined templates from which you create individual scans.

Tenable Vulnerability Management scan settings are organized into the following categories:

- Basic Settings in User-Defined Templates
- Basic Settings in Tenable Vulnerability Management Scans
- Discovery Settings in Tenable Vulnerability Management Scans
- Assessment Settings in Tenable Vulnerability Management Scans
- Report Settings in Tenable Vulnerability Management Scans
- Advanced Settings in Tenable Vulnerability Management Scans
- Credentials in Tenable Vulnerability Management Scans
- Compliance in Tenable Vulnerability Management Scans
- SCAP Settings in Tenable Vulnerability Management Scans
- Configure Plugins in Tenable Vulnerability Management Scans

Settings in User-Defined Templates

When configuring settings for user-defined templates, note the following:

- If you configure a setting in a user-defined template, that setting applies to any scans you create based on that user-defined template.
- You base a user-defined template on a Tenable-provided template. Most of the settings are identical to the settings you can configure in an individual scan that uses the same Tenable-provided template.

  However, certain **Basic** settings are unique to creating a user-defined template, and do not appear when configuring an individual scan. For more information, see Basic Settings in User-Defined Templates.
- You can configure certain settings in a user-defined template, but cannot modify those settings in an individual scan based on a user-defined template. These settings include **Discovery**, **Assessment**, **Report**, **Advanced**, **Compliance**, **SCAP**, and **Plugins**. If you want to modify these settings for individual scans, create individual scans based on a Tenable-provided template instead.
- If you configure **Credentials** in a user-defined template, other users can override these settings by adding scan-specific or managed credentials to scans based on the template.

Basic Settings in Tenable Vulnerability Management Scans

> **Note:** This topic describes **Basic** settings you can set in individual scans. For **Basic** settings in user-defined templates, see Basic Settings in User-Defined Templates.

You can use **Basic** settings to specify organizational and security-related aspects of a scan configuration. This includes specifying the name of the scan, its targets, whether the scan is scheduled, and who has access to the scan.

> **Note:** To learn more about scan limitations in Tenable Vulnerability Management, see Scan Limitations.

The **Basic** settings include the following sections:

- General
- Schedule

- Notifications
- User Permissions

General

The general settings for a scan.

Setting	Default Value	Description
Name	None	Specifies the name of the scan.
Description	None	(Optional) Specifies a description of the scan.
Scan Results	Show in dashboard	Specifies whether the results of the scan should appear in workbenches, dashboards, and reports, or be kept private. When set to **Keep private**, the scan results **Last Seen** dates do not update and you must access the scan directly to view the results. Private scan results do not show new **Active** findings in the workbenches, dashboards, and reports, and they do not transition the vulnerability states of previously discovered findings to **Fixed** or **Resurfaced**. **Note: Show in dashboard** is always enabled for triggered scans.
Folder	My Scans	Specifies the folder where the scan appears after being saved. You cannot specify a folder when you launch a remediation scan. All remediation scans appear in the **Remediation Scans** folder only.
Agent Groups	None	(Tenable Agent templates only) Specifies the agent group or groups you want the scan to target. In the

		drop-down box, select an existing agent group, or create a new agent group.
Template	n/a	Specifies which scan template the scan configuration uses. This setting is visible only if you own the scan configuration.
Scanner Type	Internal Scanner	Specifies whether a local, internal scanner or a cloud-managed scanner performs the scan, and determines whether the **Scanner** field lists local or cloud-managed scanners to choose from.
Scanner	Auto-Select	Specifies the scanner that performs the scan. Select a scanner based on the location of the targets you want to scan. For example: • Select a linked scanner to scan non-routable IP addresses. **Note:** Auto-select is not available for cloud scanners. • Select a scanner group if you want to: ◦ Improve scan speed by balancing the scan load among multiple scanners. ◦ Rebuild scanners and link new scanners in the future without having to update scanner designations in scan configurations. • Select **Auto-Select** to enable scan routing for the targets.
Network	Default	Select the network of scanners and asset that you want to scan with. Unless your organization has created and uses

		custom networks for specific business needs (for example, scanning different sub-organizations, differentiating between external and internal asset scanning, or differentiating between ephemeral and static asset scanning), Tenable recommends using the **Default** network, which all scanners and scanner groups are assigned to by default. For more information about networks, see Networks.
Tags	None	Select one or more tags to scan all assets that have any of the specified tags applied. To see a list of assets identified by the specified tags, click **View Assets**.
IP Selection	Internal	(Required) Select whether to run a tag-based scan on **Internal** or **External** IP addresses. • **Internal** – RFC 1918 (private) IP addresses. • **External** – Non-RFC 1918 (public) IP addresses. **Note:** You can use your organization's non-cloud scanners to scan both **Internal** and **External** targets. Cloud scanners can only be used to scan **External** targets. **Tip:** If you need to scan both **External** and **Internal** targets with the same tag or tags, create two different scan configurations; one scan that targets **External** IPs, and one scan that targets **Internal** IPs. Tenable Vulnerability Management evaluates the identifiers to determine a single target in the following order: 1. Last scan target 2. Most recent IPv4

		3. Most recent IPv6 4. Most recent FQDN added **Note:** Scan routing is available for linked scanners only.
Use Tag Rules as Targets	Existing tagged assets only	(Required) Specifies whether Tenable Vulnerability Management scans tagged assets only, or any assets that which the selected tags' rules apply to. • **Existing tagged assets only** – Tenable Vulnerability Management scans all existing assets that have any of the specified tags applied. • **Targets defined by tags** – Tenable Vulnerability Management scans all assets whose IP address or DNS matches the rules of the specified tag. The **Targets defined by tags** option only works for the following tag rules: IPv4, IPv6, and DNS. **Note:** If you select the **Match All** filter, you can have only one tag rule. Otherwise, the tag resolves to empty targets. If you select the **Match Any** filter, you are allowed to have more than one tag rule. All tag rules resolve as targets as long as the rules are for IPv4, IPv6, and DNS. For example, you create a scan policy that scans for a tag with a tag rule that specifies a certain IPv4 range. The example tag name is *My IPv4s*. • If you choose **Existing tagged assets only**, Tenable Vulnerability Management only scans assets that are already tagged with the *My IPv4s* tag.

		• If you choose **Targets defined by tags**, Tenable Vulnerability Management scans any assets whose IPv4 addresses are within the range specified in the *My IPv4s* tag rule. For more information about tags and tag rules, see Tags and Tag Rules.
Scan Window	Disabled	(Tenable Nessus Scanner templates only) Specifies the timeframe after which the scan automatically stops. Use the drop-down box to select an interval of time, or click to type a custom scan window. **Note:** The scan window timeframe only applies to the scan job. After the scan job completes within the timeframe, or once the scan job stops due to the scan window ending, Tenable Vulnerability Management may still need to index the scan job. This can cause the scan not to show as **Completed** after the scan window is complete. Once Tenable Vulnerability Management indexes the scan, it shows as **Completed**.
Scan Type	Scan Window	(Tenable Agent templates only) (Required) Specifies whether the agent scans occur based on a scan window or triggers: • **Scan Window** – Specifies the timeframe during which agents must report in order to be included and visible in vulnerability reports. Use the drop-down box to select an interval of time, or click to type a custom scan window. Window scans must be explicitly launched or scheduled to launch at a particular time. • **Triggered Scan** – Specifies the triggers that cause agents to report in. Use the drop-down boxes to select from the following trigger types:

		• **Interval** – The time interval (hours) between each scan (for example, every **12** hours). • **File Name** – The file name that triggers the agent scan. The scan triggers when the file name is detected in the trigger directory. **Tip:** You can set multiple triggers for a single scan, and the scan searches for the triggers in their listed order (in other words, if the first trigger does not trigger the scan, it searches for the second trigger). To learn more about triggered agent scanning, see Triggered Agent Scans. **Note:** Tenable Vulnerability Management ignores triggered agent scan data that is older than 14 days. This ensures that Tenable Vulnerability Management is not processing stale data from agents that have been offline for extended periods of time.
Info-level Reporting	Triggered agent scans – After 10 scans Scan Window agent scans – After 10 days **Note:** Tenable highly recommends using the default values. Only lower the	(Tenable Agent vulnerability templates only) (Required) Specifies how often the agent scan should report unchanged Info-severity vulnerability findings. To learn more about this setting, see Info-level Reporting. You can configure the agent scan to report all severity findings by launching a new baseline scan after one of the following intervals: • **After number of scans** – The agent scan reports all findings every *x* number of scans. You choose from the following increments: 4, 7, 10,

	value if doing so is necessary for your organization.	15, or 20 scans. • **After number of days** – The agent scan reports all findings after a set number of days after the previous day on which the agent scan last reported all findings. You choose from the following increments: 7, 10, 20, 30, 60, or 90 days. You can only set triggered agent scans to **After number of scans**. You can set Scan Window scans to either **After number of scans** or **After number of days**.
Target Groups	None	You can select or add a new target group to which the scan applies. Assets in the target group are used as scan targets. **Note**: Tenable plans to deprecate target groups in the near future. Currently, you can still create and manage target groups. However, Tenable recommends that you instead use tags to group and scan assets on your Tenable Vulnerability Management instance.
Targets	None	Specifies one or more targets to be scanned. If you select a target group or upload a target file, you are not required to specify additional targets. Targets can be specified using a number of different formats. The targets you specify must be appropriate to the scanner you select for the scan. For example, cloud scanners cannot scan non-routable IP addresses. Select an internal scanner instead. **Tip:** You can force Tenable Vulnerability Management to use a given hostname for a server during a scan by

		using the `hostname[ip]` syntax (for example, `www.example.com[192.168.1.1]`). However, you cannot use this approach if you enable scan routing for the scan. **Note:** You cannot apply more than 300,000 IP address targets to a scan. To learn more about scan limitations in Tenable Vulnerability Management, see Scan Limitations. **Note:** See Permissions for more information on how permissions affect targets.
Upload Targets	None	Uploads a text file that specifies the targets. The targets file must be formatted in the following manner: • ASCII file format • Only one target per line • No extra spaces at the end of a line • No extra lines following the last target **Note:** Unicode/UTF-8 encoding is not supported.
Select Targets	n/a	(`--aws-scanner`Tenable Nessus scanners only) Opens a window that allows you to select from a list of visible network scans via AWS IMDSv2. Use this page to select the AWS targets to scan, then click **Confirm**.
Policy	None	This setting appears only when the scan owner edits an existing scan that is based on a user-defined scan template. **Note:** After scan creation, you cannot change the Tenable-provided scan template on which a scan is based.

		In the drop-down box, select a user-defined scan template on which to base the scan. You can select user-defined scan templates for which you have **Can View** or higher permissions. In most cases, you set the user-defined scan template at scan creation, then keep the same template each time you run the scan. However, you may want to change the user-defined scan template when troubleshooting or debugging a scan. For example, changing the template makes it easy to enable or disable different plugin families, change performance settings, or apply dedicated debugging templates with more verbose logging. When you change the user-defined scan template for a scan, the scan history retains the results of scans run under the previously assigned template.

Schedule

The scan schedule settings.

By default, scans are not scheduled. When you first access the **Schedule** section, the **Enable Schedule** setting appears, set to **Off**. To modify the settings listed on the following table, click the **Off** button. The rest of the settings appear.

Note: Scheduled scans do not run if they are in the scan owner's **Trash** folder.

Caution: Tenable occasionally performs maintenance on Tenable Vulnerability Management. To avoid performance issues, Tenable recommends not running or scheduling scans during maintenance windows. For current maintenance status and updates, see the Tenable Status page.

Setting	Default Value	Description
Frequency	Once	Specifies how often the scan is launched.

		• **Once**: Schedule the scan at a specific time.
		• **Daily**: Schedule the scan to occur every 1-20 days, at a specific time.
		• **Weekly**: Schedule the scan to occur every 1-20 weeks, by time and day or days of the week.
		• **Monthly**: Schedule the scan to occur every 1-20 months, by:
		  • **Day of Month**: The scan repeats monthly on a specific day of the month at the selected time. For example, if you select a start date of October 3, the scan repeats on the 3rd of each subsequent month at the selected time.
		  • **Week of Month**: The scan repeats monthly on a specific day of the week. For example, if you select a start date of the first Monday of the month, the scan runs on the first Monday of each subsequent month at the selected time.
		Note: If you schedule your scan to recur monthly and by time and day of the month, 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 (for example, the 29th), Tenable Vulnerability Management cannot run the scan on those days.
		• **Yearly**: Schedule the scan to occur every 1-20 years, by time and date.

Starts	Varies	Specifies the exact date and time when a scan

		launches. The starting date defaults to the date when you are creating the scan. The starting time is the nearest half-hour interval. For example, if you create your scan on 09/08/2023 at 9:16 AM, the default starting date and time is set to *09/08/2023* and *09:30*.
Timezone	Zulu	Specifies the timezone of the value set for **Starts**.
Repeat Every	Varies	Specifies the interval at which a scan is relaunched. The default value of this item varies based on the frequency you choose.
Repeat On	Varies	Specifies what day of the week a scan repeats. This item appears only if you specify *Weekly* for **Frequency**. The value for **Repeat On** defaults to the day of the week on which you create the scan.
Repeat By	Day of the Month	Specifies when a monthly scan is relaunched. This item appears only if you specify *Monthly* for **Frequency**.
Summary	N/A	Provides a summary of the schedule for your scan based on the values you have specified for the available settings.

Notifications

The notification settings for a scan.

Setting	Default Value	Description
Email Recipient(s)	None	Specifies zero or more email addresses (separated by commas) that are alerted when a scan completes and the results are available.

Result Filters	None	Defines the type of information to be emailed.

User Permissions

You can share the scan with other users by setting permissions for users or groups. When you assign a permission to a group, that permission applies to all users within the group.

Tip: Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

Permission	Description
No Access	(Default user only) Groups and users set to this permission cannot interact with the scan in any way.
Can View	Groups and users with this permission can view the results of the scan, export the scan results, and move the scan to the **Trash** folder. They cannot view the scan configuration or permanently delete the scan.
Can Execute	In addition to the tasks allowed by **Can View**, groups and users with this permission can launch, pause, and stop a scan. They cannot view the scan configuration or permanently delete the scan. **Note:** In addition to **Can Execute** permissions for the scan, users running a scan must have **Can Scan** permissions in an access group for the specified target, or the scanner does not scan the target.
Can Edit	In addition to the tasks allowed by **Can Execute**, groups and users with this permission can view the scan configuration and modify any setting. They cannot change the scan's ownership (only the scan owner can change scan ownership) or permanently delete the scan. **Note:** User roles override scan permissions in the following cases: • A basic user cannot run a scan or configure a scan, regardless of the permissions assigned to that user in the individual scan. • An administrator always has the equivalent of **Can Edit** permissions, regardless of the permissions set for the administrator

	account in the individual scan. This does not apply to user-defined scan templates.

Basic Settings in User-Defined Templates

Note: This topic describes **Basic** settings you can set in user-defined templates. For **Basic** settings in individual scans, see Basic Settings in Tenable Vulnerability Management Scans .

You can use **Basic** settings to specify basic aspects of a user-defined template, including who has access to the user-defined template.

The **Basic** settings include the following sections:

- General
- Permissions

General

The general settings for a user-defined template.

Setting	Default Value	Description
Name	None	Specifies the name of the user-defined template.
Description	None	(Optional) Specifies a description of the user-defined template.

Permissions

You can share the user-defined template with other users by setting permissions for users or groups. When you assign a permission to a group, that permission applies to all users within the group.

Tip: Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

Permission	Description
No Access	(Default user only) Groups and users set to this permission cannot interact with the scan in any way.
Can View	Groups and users with this permission can view the results of the scan, export the scan results, and move the scan to the **Trash** folder. They cannot view the scan configuration or permanently delete the scan.
Can Execute	In addition to the tasks allowed by **Can View**, groups and users with this permission can launch, pause, and stop a scan. They cannot view the scan configuration or permanently delete the scan. **Note:** In addition to **Can Execute** permissions for the scan, users running a scan must have **Can Scan** permissions in an access group for the specified target, or the scanner does not scan the target.
Can Edit	In addition to the tasks allowed by **Can Execute**, groups and users with this permission can view the scan configuration and modify any setting for the scan except scan ownership. They can also delete the scan. **Note:** Only the scan owner can change scan ownership. **Note:** User roles override scan permissions in the following cases: • A basic user cannot run a scan or configure a scan, regardless of the permissions assigned to that user in the individual scan. • An administrator always has the equivalent of **Can Edit** permissions, regardless of the permissions set for the administrator account in the individual scan. This does not apply to user-defined scan templates.

Authentication

In user-defined templates, you can use **Authentication** settings to configure the authentication Tenable Vulnerability Management performs for credentialed scanning.

Tip: The **Authentication** settings are equivalent to the **Scan-wide Credential Type Settings** in Tenable-provided scan templates.

Setting	Default Value	Description
SNMPv1/v2c		
equivalent to Scans > Credentials > Plaintext Authentication > SNMPv1/v2c		
UDP Port	161	Ports where Tenable Vulnerability Management attempts to authenticate on the host device.
Additional UDP port #1	161	
Additional UDP port #2	161	
Additional UDP port #3	161	
HTTP		
equivalent to Scans > Credentials > Plaintext Authentication > HTTP		
Login method	POST	Specify if the login action is performed via a GET or POST request.
Re-authenticate delay (seconds)	0	The time delay between authentication attempts. Setting a time delay is useful to avoid triggering brute force lockout mechanisms.
Follow 30x redirections (# of levels)	0	If a 30x redirect code is received from a web server, this setting directs Tenable Vulnerability Management to follow the link provided or not.
Invert authenticated regex	Disabled	A regex pattern to look for on the login page, that if found, tells Tenable Vulnerability Management that authentication was not successful (e.g., Authentication failed!).
Use authenticated regex on HTTP headers	Disabled	Rather than search the body of a response, Tenable Vulnerability Management can search the HTTP response headers for a given regex pattern to better determine authentication state.

Case insensitive authenticated regex	Disabled	he regex searches are case sensitive by default. This instructs Tenable Vulnerability Management to ignore case.
telnet/rsh/rexec		
equivalent to Scans > Credentials > Plaintext Authentication > telnet/ssh/rexec		
Perform patch audits over telnet	Disabled	Tenable Vulnerability Management uses telnet to connect to the host device for patch audits.
Perform patch audits over rsh	Disabled	Tenable Vulnerability Management uses rsh to connect to the host device for patch audits.
Perform patch audits over rexec	Disabled	Tenable Vulnerability Management uses rexec to connect to the host device for patch audits.
Windows		
equivalent to Scans > Credentials > Host > Windows		
Never send credentials in the clear	Enabled	By default, for security reasons, this option is enabled.
Do not use NTLMv1 authentication	Enabled	If the **Do not use NTLMv1 authentication** option is disabled, then it is theoretically possible to trick Tenable Vulnerability Management into attempting to log into a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a hash obtained from Tenable Vulnerability Management. This hash can be potentially cracked to reveal a username or password. It may also be used to directly log into other servers. Force Tenable Vulnerability Management to use NTLMv2 by enabling the **Only use NTLMv2** setting at scan time. This prevents a hostile Windows server from using NTLM and receiving a hash. Because NTLMv1 is an insecure protocol, this option is enabled

		by default.
Start the Remote Registry service during the scan	Disabled	This option tells Tenable Vulnerability Management to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Tenable Vulnerability Management to execute some Windows local check plugins. **Note:** This option is disabled by default to improve default scan performance. Additionally, enabling this option can have implications depending on your network security implementation. For example, certain access control configurations for your network firewall might blacklist your scanner for attempting to negotiate Server Message Block Protocol (SMB protocol) connections.
Enable administrative shares during the scan	Disabled	This option allows Tenable Vulnerability Management to access certain registry entries that can be read with administrator privileges. **Note:** This option is disabled by default to improve default scan performance. Additionally, enabling this option can have implications depending on your network security implementation. For example, certain access control configurations for your network firewall might blacklist your scanner for attempting to negotiate Server Message Block Protocol (SMB protocol) connections.
SSH		
equivalent to Scans > Credentials > Host > SSH		
known_hosts file	None	If you upload an SSH known_hosts file, Tenable Vulnerability Management only attempts to log in to hosts in this file. This can ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log into a system that may not be under your control.

Preferred port	22	The port on which SSH is running on the target system.
Client version	OpenSSH_5.0	The type of SSH client Tenable Vulnerability Management impersonates while scanning.
Attempt least privilege	Cleared	Enables or disables dynamic privilege escalation. When enabled, Tenable Vulnerability Management attempts to run the scan with an account with lesser privileges, even if the **Elevate privileges with** option is enabled. If a command fails, Tenable Vulnerability Management escalates privileges. Plugins 101975 and 101976 report which plugins ran with or without escalated privileges. **Note:** Enabling this option may increase scan run time by up to 30%.
Amazon AWS		
equivalent to Scans > Credentials > Cloud Services > Amazon AWS		

Regions to access	Rest of the World	In order for Tenable Vulnerability Management to audit an Amazon AWS account, you must define the regions you want to scan. Per Amazon policy, you need different credentials to audit account configuration for the China region than you do for the rest of the world.
		
		Possible regions include:
		
		• **GovCloud** – If you select this region, you automatically select the government cloud (e.g., us-gov-west-1).
		
		• **Rest of the World** – If you select this region, the following additional options appear:
		
		  • us-east-1
		
		  • us-east-2

		• us-west-1 • us-west-2 • ca-central-1 • eu-west-1 • eu-west-2 • eu-central-1 • ap-northeast-1 • ap-northeast-2 • ap-southeast-1 • ap-southeast-2 • sa-east-1 • **China** – If you select this region, the following additional options appear: • cn-north-1 • cn-northwest-1
HTTPS	Enabled	Whether Tenable Vulnerability Management authenticates over an encrypted (HTTPS) or an unencrypted (HTTP) connection.
Verify SSL Certificate	Enabled	Whether Tenable Vulnerability Management verifies the validity of the SSL digital certificate.
Rackspace		
equivalent to Scans > Credentials > Cloud Services > Rackspace		
Location	-	Location of the Rackspace Cloud instance. Possible locations include: • Dallas-Fort Worth (DFW)

		• Chicago (ORD) • Northern Virginia (IAD) • London (LON) • Syndney (SYD) • Hong Kong (HKG)
Microsoft Azure		
equivalent to Scans > Credentials > Cloud Services > Amazon AWS		
Subscription IDs	-	List subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.

Scan Targets

In Tenable Vulnerability Management, you can use a number of different formats when specifying targets for a scan. The following tables contain target formats, examples, and a short explanation of what occurs when Tenable Vulnerability Management scans that target type.

Note: Tenable limits the number of targets that you can scan in a single scan. For more information, see Scan Limitations.

Note: For previously scanned assets, you can configure scan targets based on host attributes like operating system or installed software, instead of host identifiers like IP address.

Tip: If a hostname target looks like either a link6 target (start with the text "link6") or one of the two IPv6 range forms, put single quotes around the target to ensure that Tenable Vulnerability Management processes it as a hostname.

Target Description	Example	Explanation
A single IPv4 address	192.168.0.1	Scans the single IPv4 address.
A single IPv6 address	2001:db8::2120:17ff:fe56:333b	Scans the single IPv6 address.

Target Description	Example	Explanation
A single link local IPv6 address with a scope identifier	fe80:0:0:0:216:cbff:fe92:88d0%eth0	Scans the single IPv6 address. Use interface indexes, not interface names, for the scope identifier on Windows platforms.
A list of IPv4 addresses	192.168.0.1, 192.168.0.32, 192.168.0.200, 192.168.0.255	Scans a list of different IPv4 addresses.
An IPv4 range with a start and end address	192.168.0.1-192.168.0.255	Scans all IPv4 addresses between the start address and end address, including both addresses. **Caution:** When entering a target range, do not enter a space before or after the hyphen (for example, 192.168.0.1 - 192.168.0.255). Tenable Vulnerability Management does not accept ranges in this format.
An IPv4 address with the last octet range replaced with numeric ranges	192.168.0-1.3-5	Scans all combinations of the values given in the octet ranges. In this example, scans: 192.168.0.3, 192.168.0.4, 192.168.0.5, 192.168.1.3, 192.168.1.4 and 192.168.1.5 **Caution:** When entering a target range, do not enter a space before or after the hyphen (for example, 192.168.0 - 1.3 - 5). Tenable

Target Description	Example	Explanation
		Vulnerability Management does not accept ranges in this format.
An IPv4 subnet with CIDR notation	192.168.0.0/24	Scans all addresses within the specified subnet. The address given is not the start address. Specifying any address within the subnet with the same CIDR scans the same set of hosts.
An IPv4 subnet with netmask notation	192.168.0.0/255.255.255.128	Scans all addresses within the specified subnet. The address is not a start address. Specifying any address within the subnet with the same netmask scans the same hosts.
A host resolvable to either an IPv4 or an IPv6 address	www.yourdomain.com	Scans the single host. If Tenable Vulnerability Management can resolve the hostname to multiple addresses, Tenable Vulnerability Management scans the first resolved IPv4 address or, if Tenable Vulnerability Management cannot resolve an IPv4 address, the first resolved IPv6 address.
A host	www.yourdomain.com/24	Resolves the hostname to an

Target Description	Example	Explanation
resolvable to an IPv4 address with CIDR notation		IPv4 address, then scans all addresses within the specified subnet. Tenable Vulnerability Management treats this format like any other IPv4 address with CIDR notation.
A host resolvable to an IPv4 address with netmask notation	www.yourdomain.com/255.255.252.0	Resolves the hostname to an IPv4 address, then scans all addresses within the specified subnet. Tenable Vulnerability Management treats this format like any other IPv4 address with netmask notation.
The text **link6** optionally followed by an IPv6 scope identifier	link6 or link6%16	Scans all hosts that respond to multicast ICMPv6 echo requests sent out on the interface specified by the scope identifier to the ff02::1 address. If no IPv6 scope identifier is given, the requests are sent out on all interfaces. Use interface indexes, not interface names, for the scope identifier on Windows platforms.
Some text with either a single	Test Host 1[10.0.1.1] or	Scans the IPv4 or IPv6 address within the brackets, like a

Target Description	Example	Explanation
IPv4 or IPv6 address within square brackets	Test Host 2[2001:db8::abcd]	normal single target.

Target Groups

You can still use target groups to manage your scan targets. However, Tenable recommends that you instead use tags to group and scan your assets when possible. In the future, when tagging features and options match those currently available in target groups, Tenable will convert your target groups into tags and retire your existing target groups. No action is required on your part, and Tenable will provide you with 60 calendar days notice before converting and retiring your target groups. For more information, contact your Tenable representative.

A target group allows you to construct a list of scan targets by FQDN, CIDR notation, or IP address range. You can then specify which users in your organization can use the target group in scan configurations or filtering dashboards (including workbenches).

Note: Tenable recommends limiting the number of targets in any single target group. When filtering a dashboard by a target group with too many targets, Tenable Vulnerability Management may fail to show data.

Note: Scan targets listed by CIDR notation must be in one of the following formats:

- xx.xx.0.0/16
- xx.xx.xx.0/24

If you grant a user permissions in a target group, the user can use the target group in the **Target Groups** option for scan configuration. However, you must also grant the user **Can Scan** permissions in an access group for the targets, or Tenable Vulnerability Management excludes the targets from the scan results. For more information, see Permissions.

To manage target groups, use the following procedures:

Create a target group

System target groups:

Required User Role: Administrator

User target groups:

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

To create a target group in the new interface:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Target Groups** tile.

   The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

3. If you want to edit a user target group, click **User**. Otherwise, stay on the **System** target groups tab.

4. In the upper-right corner of the page, click the **Create Target Group** button.

   The **Create a Target Group** page appears.

5. Configure the **General** settings:

Setting	Description
Name	A name for the target group.
Targets	A comma-separated list of FQDNs, CIDR notation, or IP address ranges that you want to scan. **Note:** Scan targets listed by CIDR notation must be in one of the following formats: • xx.xx.0.0/16 • xx.xx.xx.0/24 **Note**: For the IP address range format (example: 192.168.0.1-192.168.0.255),

Setting	Description
	Tenable Vulnerability Management supports a maximum count of "-" to 1023.
Upload Targets	A text file containing a comma-separated list of FQDNs or IP address ranges that you want to scan. The system adds the uploaded targets to the **Targets** box after you save the target group.

6. Configure the user permissions for the group.

   Note: If you grant a user permissions in a target group, the user can use the target group in the **Target Groups** option for scan configurations. However, you must also grant the user **Can Scan** permissions in an access group for the targets, or Tenable Vulnerability Management excludes the targets from the scan results. For more information, see Access Groups.

7. Click **Save**.

   One of the following occurs:

   - If you configured user permissions for the target group, Tenable Vulnerability Management creates the target group and adds it to the table on the **Target Groups** page.
   - If you retained the default **No Access** permissions for the target group, a confirmation window appears.

     In response, do one of the following:

     - If the default configuration is appropriate for the target group, click **Continue** to confirm your action.
     - If the default configuration is not appropriate for the target group, click **Cancel** to return to user permissions configuration for the target group.

Configure user permissions for a target group

System target groups:

Required User Role: Administrator

Required Target Group Permissions: Any

User target groups:

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Required Target Group Permissions: Can Change

Note: For auditing cloud infrastructure, Tenable Vulnerability Management requires a target group with **Can Scan** permissions to be present on 127.0.0.1.

Note: To enable the user to use a target group in the **Target Groups** option for scan configurations, you must also grant the user **Can Scan** permissions in an access group for the targets. If you do not, Tenable Vulnerability Management excludes the targets from the scan results. For more information, see Access Groups.

To configure permissions for a target group:

1. Create or edit a target group.
2. In the **User Permissions** section, do one of the following:
   - Change the permissions for the **Default** user

     Note: The **Default** user represents any users that have not been specifically added to the target group.

     a. Next to the permission drop-down for the **Default** user, click the ⌄ button.

     b. Select a permissions level.

     c. Click **Save**.
   - Add permissions

     a. Next to **User Permissions**, click the ⊕ button.

     The **Add User Permission** plane appears.

     b. In the **Add users or groups** box, type the name of a user or group.

As you type, a filtered list of users and groups appears.

c. Select a user or group from the search results.

The selected user or group appears in the list of users and groups.

By default, Tenable Vulnerability Management assigns **Can Use** permissions to the new user or group.

d. Next to the permission drop-down for the user or group, click the ⌄ button.

e. Select a permissions level.

f. Click **Save**.

- Edit permissions

a. Next to the permission drop-down for the user or group, click the ⌄ button.

b. Select a permissions level.

c. Click **Save**.

- Delete permissions

a. In the list of users, roll over the user or group you want to delete.

b. Click the ✕ button next to the user or user group.

The user or group disappears from the permissions list.

c. Click **Save**.

Edit a target group

System target groups:

Required User Role: Administrator

Required Target Group Permissions: Any

User target groups:

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Required Target Group Permissions: Can Change

Note: System target groups and related functionality asset isolation are deprecated. To control scan permissions, use access groups instead.

You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

To edit a target group in the new interface:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Target Groups** tile.

   The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

3. If you want to edit a user target group, click **User**. Otherwise, stay on the **System** target groups tab.

4. In the target groups table, click the target group you want to edit.

   The **Update a Target Group** page appears.

5. Edit the **General** settings for the target group:

Setting	Description
Name	A name for the target group.
Targets	A comma-separated list of FQDNs, CIDR notation, or IP address ranges that you want to scan.
Upload Targets	A text file containing a comma-separated list of FQDNs or IP address ranges that you want to scan.

Setting	Description
	The system adds the uploaded targets to the **Targets** box after you save the target group.

6. Configure user permissions for the target group.
7. Click **Save**.

   A confirmation window appears.
8. In the confirmation window, click **Continue**.

   Tenable Vulnerability Management saves the changes to the target group.

Import a target group

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

You can import a target group as a `.csv` file.

Tip: To create or modify the `.csv` file, Tenable recommends using a robust editor such as Microsoft Excel.

Before you begin:

- Create a `.csv` file in the specified format.

To import a target group:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.
2. Click the **Target Groups** tile.

   The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.
3. If you want to import a user target group, click **User**. Otherwise, stay on the **System** target groups page.

> **Note:** System target groups and related functionality asset isolation are deprecated. To control scan permissions, use access groups instead.
>
> You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

4. In the upper-right corner of the page, click the **Import** button.

   Your operating system's file manager appears.

5. Select a `.csv` file to import.

   Tenable Vulnerability Management imports the file and adds the target groups to the target groups box.

Target Group Import File Format

Each line of the target group import file must have the following fields:

Field Name	Description
`id`	Numeric field used to identify the target group.
`name`	Field used to identify the name of the target group. You can use any combination of alphanumeric characters or symbols in the **name** field.
`members`	Field used to identify the host address or addresses to include in the target group.
`creation_date`	Numeric field in UNIX timestamp format.
`last_modification_date`	Numeric field in UNIX timestamp format.

Export a target group

Required Tenable Vulnerability Management User Role: Standard, Scan Manager, or Administrator

Required Target Group Permissions: Can Use

You can export a target group as a `.csv` file. Depending on your browser, the target group may download automatically.

To export a target group or groups in the new interface:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Target Groups** tile.

   The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

3. If you want to export a user target group, click **User**. Otherwise, stay on the **System** target groups tab.

   > **Note:** System target groups and related functionality asset isolation are deprecated. To control scan permissions, use access groups instead.
   >
   > You can still create and edit system target groups, as well as use system target groups in scan configurations and dashboard filters. However, Tenable recommends using user target groups instead.

4. Select the target group or groups you want to export.

   - Select a single target group.

     a. In the target groups table, roll over the target group you want to export.

        The action buttons appear in the row.

     b. In the row, click the [→ button.

        Tenable Vulnerability Management automatically exports the target group or groups you selected as a single `.csv` file.

   - Select multiple target groups.

     a. In the target groups table, select the check boxes for each target group you want to export.

The action bar appears at the bottom of the page.

b. Next to **Target Groups**, click the [→ button.

Target Group Export File Header Fields

The following table describes the headers that appear in the exclusion export file.

Field Name	Description
id	Numeric identifier for the target group.
name	Alphanumeric name of the target group.
members	Host address(es) to be included in the target group.
creation_date	Date (in UNIX timestamp format) when the target group was created.
last_modification_date	Date (in UNIX timestamp format) when the target group was last modified.

Delete a target group

System target groups:

Required User Role: Administrator

Required Target Group Permissions: Any

User target groups:

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Required Target Group Permissions: Can Change

To delete a target group in the new interface:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Target Groups** tile.

   The **Target Groups** page appears. By default, the **System** tab is active. This tab contains a table of system target groups.

3. If you want to delete a user target group, click **User**. Otherwise, stay on the **System** target groups tab.

4. Select the target group or groups you want to delete:

   - Select a single target group.

     a. In the target groups table, roll over the target group you want to delete.

        The action buttons appear in the row.

     b. In the row, click the button.

        A confirmation window appears.

   - Select multiple target groups.

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

        The action bar appears at the bottom of the page.

     b. In the action bar, click the button.

        A confirmation window appears.

5. In the confirmation window, click **Delete**.

   Tenable Vulnerability Management deletes the target group or groups you selected.

Target group permissions

The following table describes user permissions for both system and user target groups.

Permission	Description
System Target Group	
No Access	(Default user only) Users assigned this permission cannot use the system target group to filter dashboards.
Can Use	**Note:** System target groups are deprecated; Tenable recommends using user target groups instead. Users assigned this permission can use hosts in the user target groups to filter dashboards and configure scans. **Note:** To enable the user to use a target group in the **Target Groups** option for scan configurations, you must also grant the user **Can Scan** permissions in an access group for the targets. If you do not, Tenable Vulnerability Management excludes the targets from the scan results. For more information, see Access Groups.
User Target Group	
No Access	(Default user only) Users assigned this permission cannot configure scans for hosts in the user target group or use hosts in the user target group to filter dashboards.
Can Use	Users assigned this permission can use hosts in the user target groups to filter dashboards and configure scans. **Note:** To enable the user to use a target group in the **Target Groups** option for scan configurations, you must also grant the user **Can Scan** permissions in an access group for the targets. If you do not, Tenable Vulnerability Management excludes the targets from the scan results. For more information, see Access Groups.
Can Change	In addition to using hosts in this user target group when configuring scans and filtering dashboards, users assigned this permission can modify any setting for the target group except permissions.

Info-level Reporting

Info-level Reporting is a scan setting available for agent vulnerability scan templates. The setting specifies how often the agent scan should report unchanged Info-severity vulnerability findings.

Description

Info-severity findings can account for up to 90% of agent scan findings. Most Info-level findings do not change from scan to scan and have minimal impact on your overall network exposure. Configuring **Info-level Reporting** can help minimize your scan processing times by decreasing the number of unchanged Info-severity findings that Tenable Vulnerability Management processes after every agent scan.

After you configure an agent scan, the first execution of that scan always reports all detected findings regardless of severity level. This is known as a *baseline* scan. Subsequent scans return all vulnerability findings with a severity of Low or higher, and any new or changed Info-level findings. Agents do not re-report existing, unchanged Info-level findings to Tenable Vulnerability Management until a new baseline scan is performed.

When you view agent vulnerability scan results in the Tenable Vulnerability Management user interface, baseline scans are indicated with the baseline icon ( ). For example:

Note: The baseline icon does not appear for triggered scans, regardless of whether or not the scan was a baseline scan.

The baseline icon always appears for scans whose scan configurations do not have the **Info-level Reporting** setting. This is because every execution of that scan includes all findings and is, therefore, a baseline scan.

The baseline icon does not appear for scans whose configurations *have* the **Info-level Reporting** setting, but were run before the **Info-level Reporting** feature was released.

Configuration

You can configure the agent scan to report all severity findings by launching a new baseline scan after one of the following intervals:

- **After number of scans** – The agent scan reports all findings every *x* number of scans. You choose from the following increments: 7, 10, 15, or 20 scans.

  For example, if you set the value to the default of 10, the agent scan reports all findings in its next scan and then reports all findings again during every 10th scan. All interim scans only return findings with a severity of Low or higher, as well as any new or changed Info-level findings.

- **After number of days** – The agent scan reports all findings after a set number of days after the previous day on which the agent scan last reported all findings. You choose from the following increments: 7, 10, 20, 30, 60, or 90 days.

  For example, if you set the value to the default of 10, the agent scan reports all findings in its next scan. For 10 days, all interim scans return all findings with a severity of Low or higher and any new or changed Info-level findings. After the 10-day period passes, the agent scan reports all findings again in its next scan.

  You can only set triggered agent scans to **After number of scans**. You can set Scan Window scans to either **After number of scans** or **After number of days**.

  The default value for triggered agent scans is **After 10 scans**, and the default value for Scan Window agent scans is **After 10 days**. Tenable recommends using the default values. Only lower the value if doing so is necessary for your organization.

In addition to **Info-level Reporting**, you can enable **Force refresh of all Info-severity vulnerabilities on next scan** to force the agent scan to report all findings in the next scan. After the next scan

completes and reports all findings, the **Info-level Reporting** setting determines how often the scan reports Info-severity findings.

> **Note:** All vulnerability findings with a severity of Low or higher and new or changed Info-severity vulnerabilities are always reported after every scan.

Limitations and Considerations

- Only agents version 10.5.0 and later can use the **Info-level Reporting** setting. Any agents on earlier versions always perform baseline scans.
- The **Info-level Reporting** setting is not supported when Tenable Vulnerability Management is connected to Tenable Security Center.
- Agent scans with configured Compliance settings do not support the **Info-level Reporting** setting. All agent scans with Compliance settings configured are baseline scans.
- If you recast an Info-level plugin to a higher severity level (for example, Low or Medium), the plugin is still affected by **Info-level Reporting** and excluded from non-baseline scans if the plugin output has not changed.
- Each individual agent calculates the **After number of scans** value separately. Therefore, triggered scans can return a combination of baseline and non-baseline results.
- Plugins 19506 (Nessus Scan Information) and 42980 (SSL Certificate Expiry) are always reported in full with every scan.

Discovery Settings in Tenable Vulnerability Management Scans

> **Note:** If a scan is based on a user-defined template, you cannot configure **Discovery** settings in the scan. You can only modify these settings in the related user-defined template.

The **Discovery** settings relate to discovery and port scanning, including port ranges and methods.

Certain Tenable-provided scanner templates include preconfigured discovery settings.

If you select the **Custom** preconfigured setting option, or if you are using a scanner template that does not include preconfigured discovery settings, you can manually configure **Discovery** settings in the following categories:

- Host Discovery
- Port Scanning
- Service Discovery
- Identity

Host Discovery

By default, some settings in the **Host Discovery** section are enabled. When you first access the **Host Discovery** section, the **Ping the remote host** option appears and is set to **On**.

Setting	Default Value	Description
Ping the Remote Host	On	If set to `On`, the scanner pings remote hosts on multiple ports to determine if they are alive. Additional options **General Settings** and **Ping Methods** appear. If set to `Off`, the scanner does not ping remote hosts on multiple ports during the scan. **Note:** To scan VMware guest systems, **Ping the remote host** must be set to **Off**.
Scan Unresponsive Hosts	Disabled	Specifies whether the Nessus scanner scans hosts that do not respond to any ping methods. This option is only available for scans using the PCI Quarterly External Scan template.
General Settings		
Use Fast Network Discovery	Disabled	When disabled, if a host responds to ping, Tenable Vulnerability Management attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. These checks can take some time, especially if the remote host is firewalled. When enabled, Tenable Vulnerability Management

		does not perform these checks.
Ping Methods		
ARP	Enabled	Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.
TCP	Enabled	Ping a host using TCP.
Destination Ports (TCP)	Built-In	Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that are checked via TCP ping. Type one of the following: `built-in`, a single port, or a comma-separated list of ports. For more information about which ports `built-in` specifies, see the knowledge base article.
ICMP	Enabled	Ping a host using the Internet Control Message Protocol (ICMP).
Assume ICMP Unreachable From the Gateway Means the Host is Down	Disabled	Assume ICMP unreachable from the gateway 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 this option is enabled, when the scanner receives an ICMP Unreachable message, it considers the targeted host dead. This approach helps speed up discovery on some networks. **Note:** Some firewalls and packet filters use this same behavior for hosts that are up, but connected 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.
UDP	Disabled	Ping a host using the User Datagram Protocol (UDP). 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.
Maximum Number of Retries	2	Specifies the number of attempts to retry pinging the remote host.
Fragile Devices		
Scan Network Printers	Disabled	When enabled, the scanner scans network printers.
Scan Novell Netware Hosts	Disabled	When enabled, the scanner scans Novell NetWare hosts.
Scan Operational Technology Devices	Disabled	When enabled, the scanner 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, the scanner uses ICS/SCADA Smart Scanning to cautiously identify OT devices and stops scanning them once they are discovered.
Wake-on-LAN		
List of MAC Addresses	None	The Wake-on-LAN (WOL) menu controls which hosts to send WOL magic packets to before performing a scan. Hosts that you want to start prior to scanning are provided by uploading a text file that lists one MAC address per line. For example:

		`33:24:4C:03:CC:C7` `FF:5C:2C:71:57:79`
Boot Time Wait (In Minutes)	5 minutes	The amount of time to wait for hosts to start before performing the scan.

Port Scanning

The **Port Scanning** section includes settings that define how the port scanner behaves and which ports to scan.

Setting	Default Value	Description
Ports		
Consider Unscanned Ports as Closed	Disabled	When enabled, if a port is not scanned with a selected port scanner (for example, the port falls outside of the specified range), the scanner considers it closed.
Port Scan Range	Default	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`

Setting	Default Value	Description
		• `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 – 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, including 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		

Setting	Default Value	Description
SSH (netstat)	Enabled	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)	Enabled	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 Credentials.
SNMP	Enabled	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	Enabled	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

Setting	Default Value	Description
Failed		port scans regardless of the local port enumeration status.
Verify Open TCP Ports Found By Local Port Enumerators	Disabled	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	Disabled	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.
SYN	Enabled	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 Detection** option.
Override Automatic Firewall Detection	Disabled	This setting can be enabled if you enable either the **TCP** or **SYN** option. When enabled, this setting overrides automatic firewall detection. This setting has three options: • **Use aggressive detection** attempts to run plugins even if the port appears to be closed. It is recommended that this option not be used on a production network. • **Use soft detection** disables the ability to monitor how

Setting	Default Value	Description
		often resets are set and to determine if there is a limitation configured by a downstream network device. • **Disable detection** disables the firewall detection feature.
UDP	Disabled	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

The **Service Discovery** section includes settings that attempt to map each open port with the service that is running on that port.

Setting	Default Value	Description
General Settings		
Probe All Ports to Find Services	Enabled	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 Based Services	On	Controls how the scanner tests SSL-based services. **Caution:** Testing for SSL capability on all ports may be

Setting	Default Value	Description
		disruptive for the tested host.
Search for SSL/TLS/DTLS Services (enabled)		
Search for SSL/TLS On	Known SSL/TLS ports	Specifies which ports on target hosts the scanner searches for SSL/TLS services. This setting has three options: • **None** **Note:** Setting this option to **None** enables the global_settings/disable_test_ssl_based_services KB item. • **Known SSL/TLS ports** • **All TCP ports**
Search for DTLS On	None	Specifies which ports on target hosts the scanner searches for DTLS services. This setting has the following options: • **None** • **Known DTLS ports** • **All UPD ports**
Identify Certificates Expiring Within x Days	60	When enabled, the scanner identifies SSL and TLS certificates that are within the specified number of days of expiring.
Enumerate All SSL/TLS Ciphers	True	When enabled, the scanner ignores the list of ciphers advertised by SSL/TLS services and enumerates them by attempting to establish connections using all possible ciphers.

Setting	Default Value	Description
Enable CRL Checking (Connects to the Internet)	False	When enabled, the scanner checks that none of the identified certificates have been revoked.

Identity

The **Identity** section allows you to enable or disable the collection of Active Directory data.

General Settings		
Collect Identity Data from Active Directory	Disabled	Enable this setting to allow Tenable Vulnerability Management to gather user, computer, and group objects from Active Directory (AD). This setting requires that you specify an AD user account for the scan. You also need to enable LDAPS on the domain controller that the scan is targeting. When enabled, upon launch, the scan configuration uses LDAP Active Directory plugins to query AD for identity vulnerability data on all targeted domain controllers. **Note:** This setting is only applicable in Tenable One Enterprise customers, and is only intended for use by Tenable One Enterprise customers who do not already have Tenable Identity Exposure deployed.

Preconfigured Discovery Settings

Certain Tenable-provided scanner templates include preconfigured discovery settings, described in the following table. The preconfigured discovery settings are determined by both the template and the **Scan Type** that you select.

Template	Scan Type	Preconfigured Settings

Vulnerability Scans (Common)		
Advanced Network Scan	-	All defaults
Basic Network Scan	**Port scan (common ports)** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan common ports ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Port scan (all ports)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan all ports (1-65535)

		◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Custom	All defaults
Credentialed Patch Audit	**Port scan (common ports)** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan common ports ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP

		◦ ICMP (2 retries)
	Port scan (all ports)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan all ports (1-65535) ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Custom	All defaults
Host Discovery	**Host enumeration** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Ping hosts using: ◦ TCP

		◦ ARP ◦ ICMP (2 retries)
	OS Identification	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP
	Port scan (common ports)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan common ports ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP

		◦ ICMP (2 retries)
	Port scan (all ports)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan all ports (1-65535) ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Custom	All defaults
Internal PCI Network Scan	**Port scan (common ports)** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan common ports

		◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Port scan (all ports)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan all ports (1-65535) ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)

	Custom	All defaults
Legacy Web App Scan	**Port scan (common ports)** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan common ports ◦ Use netstat if credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Port Scan (all ports)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Port Scanner Settings: ◦ Scan all ports (1-65535) ◦ Use netstat if

		credentials are provided ◦ Use SYN scanner if necessary • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Custom	All defaults
Mobile Device Scan	-	-
PCI Quarterly External Scan	-	**Scan unresponsive hosts** default
Configuration Scans		
Audit Cloud Infrastructure	-	-
MDM Config Audit	-	-
Offline Config Audit	-	-
Policy Compliance Auditing	**Default** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Tenable Nessus host • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts
	Custom	All defaults

SCAP and OVAL Auditing	**Host enumeration** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Custom	All defaults
Tactical Scans		
Badlock Detection	**Quick**	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan TCP ports 23, 25, 80, and 443 ◦ Detect SSL/TLS on ports where it is commonly used
	Normal (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings:

		◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports
	Custom	All defaults
Bash Shellshock Detection	**Quick**	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan TCP ports 23, 25, 80, and 443 ◦ Detect SSL/TLS on ports where it is commonly used • Scan all devices, including: ◦ Printers

		○ Novell Netware hosts

	Normal (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts
	Custom	All defaults
DROWN Detection	**Quick**	• General Settings:

		◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan TCP ports 23, 25, 80, and 443 ◦ Detect SSL/TLS on ports where it is commonly used
	Normal (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports

	Custom	All defaults
Intel AMT Security Bypass	**Quick**	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan TCP ports 16992, 16993, 623, 80, and 443 ◦ Detect SSL/TLS on ports where it is commonly used
	Normal (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings:

		◦ Scan all TCP ports ◦ Detect SSL on all open ports
	Custom	All defaults
Malware Scan	**Host enumeration** (default)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries)
	Host enumeration (include fragile hosts)	• General Settings: ◦ Always test the local Nessus host ◦ Use fast network discovery • Ping hosts using: ◦ TCP ◦ ARP ◦ ICMP (2 retries) • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts

	Custom	All defaults
Shadow Brokers Scan	**Normal** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports • Scan all devices, including: ◦ Printers ◦ Novell Netware hosts

	Custom	All defaults
Spectre and Meltdown Detection	**Normal** (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports
	Custom	All defaults
WannaCry Ransomware Detection	**Quick**	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan TCP ports 139

		and 445 ◦ Detect SSL/TLS on ports where it is commonly used
	Normal (default)	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan the default Nessus port range ◦ Detect SSL/TLS on ports where it is commonly used
	Thorough	• General Settings: ◦ Ping the remote host ◦ Always test the local Nessus host • Service Discovery Settings: ◦ Scan all TCP ports ◦ Detect SSL on all open ports
	Custom	All defaults

Assessment Settings in Tenable Vulnerability Management Scans

Note: If a scan is based on a user-defined template, you cannot configure **Assessment** settings in the scan. You can only modify these settings in the related user-defined template.

You can use **Assessment** settings to configure how a scan identifies vulnerabilities, as well as what vulnerabilities are identified. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications.

Certain Tenable-provided scanner templates include preconfigured assessment settings.

If you select the **Custom** preconfigured setting option, or if you are using a scanner template that does not include preconfigured assessment settings, you can manually configure **Assessment** settings in the following categories:

- General
- Brute Force
- SCADA
- Web Applications
- Windows
- Malware
- Databases

Note: The following tables include settings for the **Advanced Network Scan** template. Depending on the template you select, certain settings may not be available, and default values may vary.

General

The **General** section includes the following groups of settings:

- Accuracy
- Antivirus
- SMTP

Setting	Default Value	Description
Accuracy		
Override Normal	Disabled	In some cases, Tenable Vulnerability Management cannot remotely determine whether a flaw is present or not. If report

Accuracy		paranoia is set to **Show potential false alarms**, a flaw is reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of **Avoid potential false alarms** causes Tenable Vulnerability Management to not report any flaw whenever there is a hint of uncertainty about the remote host. As a middle ground between these two settings, disable this setting.
Perform thorough tests (may disrupt your network or impact scan speed)	Disabled	Causes various plugins to work harder. For example, when looking through SMB file shares, a plugin analyzes 3 directory levels deep instead of 1. This could cause much more network traffic and analysis in some cases. By being more thorough, the scan is more intrusive and is more likely to disrupt the network, while potentially providing better audit results.
Antivirus		
Antivirus definition grace period (in days)	0	Configure the delay of the Antivirus software check for a set number of days (0-7). The Antivirus Software Check menu allows you to direct Tenable Vulnerability Management to allow for a specific grace time in reporting when antivirus signatures are considered out of date. By default, Tenable Vulnerability Management considers signatures out of date regardless of how long ago an update became available (e.g., a few hours ago). You can configure this option to allow for up to 7 days before reporting them out of date.
SMTP		
Third party domain	Tenable Vulnerability Management attempts to send spam through each SMTP device to the address listed in this field. This third party domain address must be outside the range of the site being scanned or the site performing the scan. Otherwise, the test may be aborted by the SMTP server.	
From	The test messages sent to the SMTP server(s) appear as if the messages	

address	originated from the address specified in this field.
To address	Tenable Vulnerability Management attempts to send messages addressed to the mail recipient listed in this field. The postmaster address is the default value since it is a valid address on most mail servers.

Brute Force

The **Brute Force** section includes the following groups of settings:

- General Settings
- Oracle Database

Setting	Default Value	Description
General Settings		
Only use credentials provided by the user	Enabled	In some cases, Tenable Vulnerability Management 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 Vulnerability Management from performing these tests.
Oracle Database		
Test default accounts (slow)	Disabled	Test for known default accounts in Oracle software.

SCADA

Setting	Default Value	Description
ICCP/COTP TSAP		The ICCP/COTP TSAP Addressing menu determines a

Setting	Default Value	Description
Addressing Weakness		Connection Oriented Transport Protocol (COTP) Transport Service Access Points (TSAP) value on an ICCP server by trying possible values.

Web Applications

The **Web Applications** section includes the following groups of settings:

- General Settings
- Web Crawler
- Application Test Settings

Setting	Default Value	Description
Scan web applications	Disabled	By default, Tenable Vulnerability Management does not scan web applications. To edit the following settings, enable this setting.
Use a custom User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	Specifies which type of web browser Tenable Vulnerability Management impersonates while scanning.
Web Crawler		
Start crawling from	/	The URL of the first page that is tested. If multiple pages are required, use a colon delimiter to separate them (e.g., /:/php4:/base).
Excluded pages (regex)	/server_ privileges\.php|logout	Specifies portions of the web site to exclude from being crawled. For example, to exclude the /manual directory and all Perl CGI, set this field to: (^/manual) **<>** (\.pl (\?.*)?$).

Setting	Default Value	Description
		Tenable Vulnerability Management supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).
Maximum pages to crawl	1000	The maximum number of pages to crawl.
Maximum depth to crawl	6	Limit the number of links Tenable Vulnerability Management follows for each start page.
Follow dynamically generated pages	Disabled	If selected, Tenable Vulnerability Management follows dynamic links and may exceed the parameters set above.
Application Test Settings		
Enable generic web application tests	Disabled	Enables the following settings.
Abort web application tests if HTTP login fails	Disabled	If Tenable Vulnerability Management cannot log in to the target via HTTP, then do not run any web application tests.
Try all HTTP methods	Disabled	This option instructs Tenable Vulnerability Management to also use POST requests for enhanced web form testing. By default, the web application tests only use GET requests, unless you enable this option. Generally, more complex applications use the POST method when a user submits

Setting	Default Value	Description
		data to the application. When enabled, Tenable Vulnerability Management tests each script or variable with both GET and POST requests. This setting provides more thorough testing, but may considerably increase the time required.
Attempt HTTP Parameter Pollution	Disabled	When performing web application tests, attempt to bypass filtering mechanisms by injecting content into a variable while also supplying the same variable with valid content. For example, a normal SQL injecton 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	Disabled	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	Disabled	This setting 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 Vulnerability Management would attempt

Setting	Default Value	Description
		`/test.php?arg1=XSS&b=1&c=1`, where b and c allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. This setting has four options: • **Test random pairs of parameters**: This form of testing randomly checks a combination of random pairs of parameters. This is the fastest way to test multiple parameters. • **Test all pairs of parameters (slow)**: This form of testing is slightly slower but more efficient than the one value test. While testing multiple parameters, it tests an attack string, variations for a single variable and then use the first value for all other variables. For example, Tenable Vulnerability Management would attempt `/test.php?a=XSS&b=1&c=1&d=1` and then cycle through the variables so that one is given the attack string, one is cycled through all possible values (as discovered during the mirror process) and any other variables are given the first value. In this case, Tenable Vulnerability Management would never test for `/test.php?a=XSS&b=3&c=3&d=3`

Setting	Default Value	Description
		when the first value of each variable is 1. • **Test random combinations of three or more parameters (slower)**: This form of testing randomly checks a combination of three or more parameters. This is more thorough than testing only pairs of parameters. Increasing the amount of combinations by three or more increases the web application test time. • **Test all combinations of parameters (slowest)**: This method of testing checks 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 first flaw is found per web page	Stop after one flaw is found per web server (fastest)	This setting determines when a new flaw is targeted. This applies at the script level. Finding an XSS flaw does not disable searching for SQL injection or header injection, but unless otherwise specified, there is at most one report for each type on a given port. Note that several flaws of the same type (for example, XSS or SQLi) may

Setting	Default Value	Description
		be reported if they were caught by the same attack. If this option is disabled, as soon as a flaw is found on a web page, the scan moves on to the next web page. If you enable this option, select one of the following options: • **Stop after one flaw is found per web server (fastest)** – (Default) As soon as a flaw is found on a web server by a script, Tenable Vulnerability Management stops and switches to another web server on a different port. • **Stop after one flaw is found per parameter (slow)** – As soon as one type of flaw is found in a parameter of a CGI (for example, XSS), Tenable Vulnerability Management switches to the next parameter of the same CGI, the next known CGI, or to the next port or server. • **Look for all flaws (slowest)** – Perform extensive tests regardless of flaws found. This option can produce a very verbose report and is not recommend in most cases.
URL for Remote File Inclusion	http://rfi.nessus.org/rfi.txt	During Remote File Inclusion (RFI) testing, this setting specifies a file on a remote host to use for tests. By default, Tenable

Setting	Default Value	Description
		Vulnerability Management uses a safe file hosted by Tenable for RFI testing. If the scanner cannot reach the Internet, you can use an internally hosted file for more accurate RFI testing.
Maximum run time (min)	5	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 website. Scanning the local network for web sites with small applications typically completes in under an hour, however web sites with large applications may require a higher value.

Windows

The Windows section contains the following groups of settings:

- General Settings
- User Enumeration Methods

Setting	Default Value	Description
General Settings		
Request information about the SMB Domain	Disabled	If enabled, domain users are queried instead of local users.
User Enumeration Methods		
You can enable as many of the user enumeration methods as appropriate for user discovery.		
SAM Registry	Enabled	Tenable Vulnerability Management enumerates users via

		the Security Account Manager (SAM) registry.
ADSI Query	Enabled	Tenable Vulnerability Management enumerates users via Active Directory Service Interfaces (ADSI). To use ADSI, you must configure credentials under **Credentials** > **Miscellaneous** > **ADSI**.
WMI Query	Enabled	Tenable Vulnerability Management enumerates users via Windows Management Interface (WMI).
RID Brute Forcing	Disabled	Tenable Vulnerability Management enumerates users via relative identifier (RID) brute forcing. Enabling this setting enables the **Enumerate Domain Users** and **Enumerate Local User** settings.
Enumerate Domain Users (available with RID Brute Forcing enabled)		
Start UID	1000	The beginning of a range of IDs where Tenable Vulnerability Management attempts to enumerate domain users.
End UID	1200	The end of a range of IDs where Tenable Vulnerability Management attempts to enumerate domain users.
Enumerate Local User (available with RID Brute Forcing enabled)		
Start UID	1000	The beginning of a range of IDs where Tenable Vulnerability Management attempts to enumerate local users.
End UID	1200	The end of a range of IDs where Tenable Vulnerability Management attempts to enumerate local users.

Malware

The **Malware** section contains the following groups of settings:

- General Settings
- Hash and Whitelist Files

- Yara Rules
- File System Scanning

Setting	Default Value	Description
Hash and Allow List Files		
Custom Netstat IP Threat List	None	A text file that contains a list of known bad IP addresses that you want to detect. Each line in the file must begin with an IPv4 address. Optionally, you can add a description by adding a comma after the IP address, followed by the description. You can also use hash-delimited comments (e.g., #) in addition to comma-delimited comments. **Note:** Tenable does not detect private IP ranges in the text file.
Provide your own list of known bad MD5 hashes	None	A text file with one MD5 hash per line that specifies additional known bad MD5 hashes. Optionally, you can include a description for a hash by adding a comma after the hash, followed by the description. If any matches are found when scanning a target, the description appears in the scan results. You can also use hash-delimited comments (for example, fop) in addition to comma-delimited comments.
Provide your own list of known good MD5 hashes	None	A text file with one MD5 hash per line that specifies additional known good MD5 hashes. Optionally, you can include a description for each hash by adding a comma after the hash, followed by the description. If any matches are found when

		scanning a target, and a description was provided for the hash, the description appears in the scan results. You can also use hash-delimited comments (for example, #) in addition to comma-delimited comments.
Hosts file allow list	None	Tenable Vulnerability Management checks system hosts files for signs of a compromise (for example, Plugin ID 23910 titled Compromised Windows System (hosts File Check)). This option allows you to upload a file containing a list of IPs and hostnames you want Tenable Vulnerability Management to ignore during a scan. Include one IP and one hostname (formatted identically to your hosts file on the target) per line in a regular text file.
Yara Rules		
Yara Rules	None	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.
File System Scanning		
Scan file system	Disabled	If enabled, Tenable Vulnerability Management can scan system directories and files on host computers. **Caution:** Enabling this setting in scans targeting 10 or more hosts could result in performance degradation.
Windows Directories (available if Scan file system is enabled)		
Scan %Systemroot%	Disabled	Enables file system scanning to scan %Systemroot%.
Scan %ProgramFiles%	Disabled	Enables file system scanning to scan %ProgramFiles%.
Scan %ProgramFiles	Disabled	Enables file system scanning to scan %ProgramFiles

(x86)%		(x86)%.
Scan %ProgramData%	Disabled	Enables file system scanning to scan %ProgramData%.
Scan User Profiles	Disabled	Enables file system scanning to scan user profiles.
Custom Filescan Directories	None	A custom file that lists directories to be scanned by malware file scanning. List each directory on one line.
Linux Directories		
Scan $PATH	Disabled	Enables file system scanning to scan $PATH.
Scan /home	Disabled	Enables file system scanning to scan /home.
MacOS Directories		
Scan $PATH	Disabled	Enables file system scanning to scan $PATH.
Scan /Users	Disabled	Enables file system scanning to scan /Users.
Scan /Applications	Disabled	Enables file system scanning to scan /Applications.
Scan /Library	Disabled	Enables file system scanning to scan /Library.

Databases

Setting	Default Value	Description
Oracle Database		
Use detected SIDs	Disabled	When enabled, if at least one host credential and one Oracle database credential are configured, the scanner authenticates to scan targets using the host credentials, and then attempts to detect Oracle System IDs (SIDs) locally. The scanner then attempts to authenticate using the specified Oracle database credentials and the detected SIDs. If the scanner cannot authenticate to scan targets using

		host credentials or does not detect any SIDs locally, the scanner authenticates to the Oracle database using the manually specified SIDs in the Oracle database credentials.

Preconfigured Assessment Settings

Certain Tenable-provided Tenable Nessus templates include preconfigured assessment settings, described in the following table. The preconfigured assessment settings are determined by both the template and the **Mode** that you select.

Template	Mode	Preconfigured Settings
Vulnerability Scans (Common)		
Advanced Network Scan	-	All defaults
Basic Network Scan	**Default**	• General Settings: ◦ Avoid false alarms ◦ Disable CGI scanning • Web Applications: ◦ Disable web application scanning
	Scan for known web vulnerabilities	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories

		(max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Generic web application tests disabled
	Scan for all web vulnerabilities (quick)	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Perform each generic web app test for 5 minutes (max)
	Scan for all web vulnerabilities (complex)	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning ◦ Perform thorough tests • Web Applications:

		◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Perform each generic web app test for 10 minutes (max) ◦ Try all HTTP methods ◦ Attempt HTTP Parameter Pollution
	Custom	All defaults
Credentialed Patch Audit	-	All defaults
Host Discovery	-	-
Internal PCI Network Scan	**Default**	• General Settings: ◦ Avoid false alarms ◦ Disable CGI scanning • Web Applications: ◦ Disable web application scanning
	Scan for known web vulnerabilities	• General Settings: ◦ Avoid potential false alarms

		◦ Enable CGI scanning • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Generic web application tests disabled
	Scan for all web vulnerabilities (quick)	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Perform each generic web app test for 5 minutes (max)
	Scan for all web	• General Settings:

	vulnerabilities (complex)	◦ Avoid potential false alarms ◦ Enable CGI scanning ◦ Perform thorough tests • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Perform each generic web app test for 10 minutes (max) ◦ Try all HTTP methods ◦ Attempt HTTP Parameter Pollution
	Custom	All defaults
Legacy Web App Scan	**Scan for known web vulnerabilities**	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max)

		◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Generic web application tests disabled
	Scan for all web vulnerabilities (quick) (Default)	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning • Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Perform each generic web app test for 5 minutes (max)
	Scan for all web vulnerabilities (complex)	• General Settings: ◦ Avoid potential false alarms ◦ Enable CGI scanning ◦ Perform thorough tests

		• Web Applications: ◦ Start crawling from "/" ◦ Crawl 1000 pages (max) ◦ Traverse 6 directories (max) ◦ Test for known vulnerabilities in commonly used web applications ◦ Perform each generic web app test for 10 minutes (max) ◦ Try all HTTP methods ◦ Attempt HTTP Parameter Pollution
	Custom	All defaults
Mobile Device Scan	-	-
PCI Quarterly External Scan	-	-
Configuration Scans		
Audit Cloud Infrastructure	-	-
MDM Config Audit	-	-
Offline Config Audit	-	-
Policy Compliance Auditing	-	-
SCAP and OVAL	-	-

Auditing		
Tactical Scans		
Badlock Detection	-	**Web Crawler** defaults
Bash Shellshock Detection	-	**Web Crawler** defaults
DROWN Detection	-	-
Intel AMT Security Bypass	-	-
Malware Scan	-	**Malware** defaults
Shadow Brokers Scan	-	-
Spectre and Meltdown Detection	-	
	-	-
WannaCry Ransomware Detection	-	-

Report Settings in Tenable Vulnerability Management Scans

Note: If a scan is based on a user-defined template, you cannot configure **Report** settings in the scan. You can only modify these settings in the related user-defined template.

The **Report** settings include the following groups of settings:

- Processing
- Output

Setting	Default Value	Description
Processing		

Setting	Default Value	Description
Override normal verbosity	Disabled	When disabled, provides the standard level of plugin activity in the report. The output does not include the informational plugins 56310, 64582, and 58651. When enabled, this setting has two options: • **I have limited disk space. Report as little information as possible** – Provides less information about plugin activity in the report to minimize impact on disk space. • **Report as much information as possible** – 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	Enabled	When enabled, includes superseded patch information in the scan report.
Hide results from plugins initiated as a dependency	Enabled	When enabled, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, disable this setting.
Output		
Max Ports Reported	1,024	(Agent scans only) Determines the maximum number of ports that can be included in the agent scan report.
Designate hosts by their DNS name	Disabled	Uses the host name rather than IP address for report output.
Display hosts that respond to ping	Disabled	Reports hosts that successfully respond to a ping.
Display	Disabled	When enabled, hosts that did not reply to the ping

Setting	Default Value	Description
unreachable hosts		request are included in the security report as dead hosts. Do not enable this option for large IP blocks. **Caution:** Enabling this setting causes the scan to create a finding for every target in the scan, whether responsive or not. This may cause the scan to abort if the number of hosts returned exceeds your license limit. For more information, see Scan Limitations.
Display Unicode characters	Disabled	When enabled, Unicode characters appear in plugin output such as usernames, installed application names, and SSL certificate information. **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.

Advanced Settings in Tenable Vulnerability Management Scans

Note: If a scan is based on a user-defined template, you cannot configure **Advanced** settings in the scan. You can only modify these settings in the related user-defined template.

The **Advanced** settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enable plugin debugging.

Certain Tenable-provided scanner templates include preconfigured advanced settings.

If you select the **Custom** preconfigured setting option, or if you are using a Nessus Scanner template that does not include preconfigured advanced settings, you can manually configure **Advanced** settings in the following categories:

- General Settings
- Performance Options
- Unix Find Command Options

- Agent Performance (Agent scans only)
- Windows File Search Options
- Debug Settings
- Stagger Scan Start (Agent scans only)
- Compliance Output Settings
- Vulnerability Options

Note: The following tables include settings for the **Advanced Network Scan** template. Depending on the template you select, certain settings may not be available, and default values may vary.

Setting	Default Value	Description
General Settings		
Enable Safe Checks	Enabled	When enabled, disables all plugins that may have an adverse effect on the remote host.
Stop scanning hosts that become unresponsive during the scan	Disabled	When enabled, Tenable Vulnerability Management stops scanning if it detects that the host has become unresponsive. This may occur if users turn off their PCs during a scan, a host has stopped responding after a denial of service plugin, or a security mechanism (for example, an IDS) has started to block traffic to a server. Normally, continuing scans on these machines sends unnecessary traffic across the network and delay the scan.
Scan IP addresses in a random order	Disabled	By default, Tenable Vulnerability Management scans a list of IP addresses in sequential order. When this option is enabled, Tenable Vulnerability Management scans the list of hosts in a random order within an IP address range. This approach is typically useful in helping to distribute the network traffic during large scans.
Automatically	Disabled	When enabled, if a credentialed scan tries to connect via

Setting	Default Value	Description
accept detected SSH disclaimer prompts		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	Disabled	When disabled, to avoid overwhelming a host, Tenable Vulnerability Management prevents a single scanner from simultaneously scanning multiple targets that resolve to a single IP address. Instead, Tenable Vulnerability Management 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 Vulnerability Management 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 scanned using credentials	Enabled	When enabled, the scanner creates a unique identifier (Tenable UUID) . Tenable Vulnerability Management and Tenable Security Center use the 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.
Trusted CAs	None	Specifies CA certificates that the scan considers as

Setting	Default Value	Description
		trusted. This allows you to use self-signed certificates for SSL authentication without triggering plugin 51192 as a vulnerability in your Tenable Vulnerability Management environment. **Note:** In addition to this setting, you can configure trusted CAs at the individual scanner level (for more information, see Trust a Custom CA in the *Tenable Nessus User Guide*). There is no precedence or hierarchy between trusted CAs configured in the Tenable Vulnerability Management scan configuration and trusted CAs configured on the Tenable Nessus scanner. Tenable Vulnerability Management uses the correct certificate needed to complete the scan and ignores irrelevant certificates, regardless of which product you configure them in.
Performance Options		
Slow down the scan when network congestion is detected	Disabled	When enabled, Tenable detects when it is sending too many packets and the network pipe is approaching capacity. If network congestion is detected, throttles the scan to accommodate and alleviate the congestion. Once the congestion has subsided, Tenable automatically attempts to use the available space within the network pipe again.
Use Linux kernel congestion detection	Disabled	When enabled, Tenable Vulnerability Management uses the Linux kernel to detect when it sends too many packets and the network pipe approaches capacity. If detected, Tenable Vulnerability Management throttles the scan to accommodate and alleviate the congestion. Once the congestion subsides, Tenable Vulnerability Management automatically attempts to use the available space within the network pipe again.

Setting	Default Value	Description
Network timeout (in seconds)	5	Specifies the time that Tenable waits for a response from a host unless otherwise specified within a plugin. If you are scanning over a slow connection, you may want to set this to a higher number of seconds.
Max simultaneous checks per host	5	Specifies the maximum number of checks a Tenable scanner will perform against a single host at one time.
Max simultaneous hosts per scan	Depends on the Tenable-provided template used for the scan	Specifies the maximum number of hosts that Tenable Vulnerability Management submits for scanning at the same time in an individual scan task. To further refine scan performance using host limits, Tenable recommends adjusting **Advanced** settings for your individual scanners (for example, **max_hosts**, **global.max_hosts**, and **global.max_scans**). For more information, see Advanced Settings in the *Tenable Nessus User Guide*. If you set **Max simultaneous hosts per scan** to more than scanner's **max_hosts** setting, Tenable Vulnerability Management caps **Max simultaneous hosts per scan** at the **max_hosts** value. For example, if you set the **Max simultaneous hosts per scan** to 150 and scanner's **max_hosts** is set to 100, with more than 100 targets, Tenable Vulnerability Management scans 100 hosts simultaneously. **Note:** You can only adjust individual scanner settings for your organization's managed scanners. You cannot modify the settings of Tenable-hosted scanners.
Max number of concurrent TCP	None	Specifies the maximum number of established TCP

Setting	Default Value	Description
sessions per host		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.
Max number of concurrent TCP sessions per scan	None	Specifies the maximum number of established TCP sessions for each scan task, regardless of the number of hosts being scanned. **Note:** The `MAX NUMBER OF CONCURRENT TCP SESSIONS PER SCAN` setting is not enforceable in a Discovery scan. The `global.max_simult_tcp_sessions` Nessus Engine setting (that you set on each scanner) is an absolute cap that applies across all running scans on a scanner. (For example, if you have four scanners and do not want them to generate more than 10000 simultaneous TCP sessions in total at any point in time, you can set that global setting to 2500 for each individual scanner.) For scanners installed on any Windows host, you must set this value to 19 or less to get accurate results.
Unix Find Command Options		
Command Timeout	240	The maximum number of seconds the find command is allowed to run on Unix systems. Not all **Find** commands use this timeout. **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**,

Setting	Default Value	Description
Exclude Filepath	None	A plain text file containing a list of filepaths to exclude 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.
Exclude Filesystem	None	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	None	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.

Setting	Default Value	Description
Agent Performance Options		
Use Tenable supplied binaries for 'find' and 'unzip'	Disabled	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 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	None	A plain text file containing a list of filepaths to exclude from all plugins that search using Tenable's unmanaged software directory scans.

Setting	Default Value	Description
		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	None	A plain text file containing a list of filepaths to include 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 only include absolute directory names, examples such as `E:\`, `E:\Testdir\`, and `C:\`. **Note:** The **Windows Include Filepath** overrides the default included directory (for example, the `C:` drive on Windows). Therefore, if you want to include the default directory in addition to other directories, you must list the default directory in an additional filepath line. **Caution:** Avoid having the same filepaths in the **Windows Include Filepath** and **Windows Exclude Filepath** settings. This conflict results in the filepath being excluded from the search.
Debug Settings		
Enable plugin debugging	Disabled	Attaches available debug logs from plugins to the vulnerability output of this scan.

Setting	Default Value	Description
Audit Trail Verbosity	Default	Controls verbosity of the plugin audit trail. Options include: • **No audit trail** – (Default) Tenable Vulnerability Management does not generate a plugin audit trail. • **All audit trail data** – The audit trail includes the reason why plugins were not included in the scan. • **Only scan errors** – The audit trail includes only errors encountered during the scan.
Stagger Scan Start		
Maximum delay (minutes)	0	(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.
Compliance Output Settings		
Maximum Compliance Output Length in KB	128,000 KB	Controls the maximum output length for each individual compliance check value that the target returns. If a compliance check value that is greater than this setting's value, Tenable Vulnerability Management truncates the result. **Note:** If you notice that your compliance scan processing is slow, Tenable recommends reducing this setting to increase the processing speed.

Setting	Default Value	Description
Maximum Compliance Check Timeout in Seconds	300 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.
Generate gold image .audit	Disabled	Determines whether Tenable Vulnerability Management attaches a compliance gold image .audit file to the scan results. You can download the gold image audit from the vulnerabilities tab labeled **Compliance Export Gold Image Audit**. For more information, see Compliance Export Gold Image.
Generate XCCDF result file	Disabled	Determines whether Tenable Vulnerability Management attaches XCCDF results files to the scan results. You can download the generated XCCDF result files from the vulnerabilities tab labeled **Export compliance results to XCCDF**. For more information, see Compliance Export XCCDF Results.
Generate JSON result file	Disabled	Determines whether Tenable Vulnerability Management attaches a .audit JSON file to the scan results. You can download the JSON files from the vulnerabilities tab labeled **Export compliance results to JSON**. For more information, see Compliance Export JSON Results.
Vulnerability Options		

Setting	Default Value	Description
Scan for unpatched vulnerabilities (no patches or mitigations available)	Disabled	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. **Note:** If you configure a scan to produce findings for unpatched vulnerabilities and then the setting is unchecked, Tenable Vulnerability Management 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.
Custom Red Hat Repository Mapping	Disabled, requires you to upload a .json file	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.

Preconfigured Advanced Settings

Certain Tenable-provided Nessus Scanner templates include preconfigured advanced settings, described in the following table. The preconfigured advanced settings are determined by both the template and the **Mode** that you select.

Template	Scan Type	Preconfigured Settings
Vulnerability Scans (Common)		
Advanced Network Scan	-	All defaults
Basic Network Scan	**Default** (default)	• Performance options:

		◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials • Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected • Asset identification options:

		◦ Create unique identifier on hosts scanned using credentials
	Custom	All defaults
Credentialed Patch Audit	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Custom	All defaults

Host Discovery	-	-
Internal PCI Network Scan	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Custom	All defaults
Legacy Web App Scan	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host

		(max) ◦ 5 second network read timeout • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Custom	All defaults
Mobile Device Scan	-	**Debug Settings** defaults
PCI Quarterly External Scan	**Default** (default)	• Performance options: ◦ 20 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 15 second network read timeout

		◦ Slow down the scan when network congestion is detected
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Custom	• Performance Options (default options) • Unix Find Command Exclusions (default options)
Configuration Scans		
Audit Cloud Infrastructure	-	**Debug Settings** defaults
MDM Config Audit	-	-
Offline Config Audit	-	**Debug Settings** defaults
Policy Compliance Auditing	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max)

		◦ 5 second network read timeout • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Custom	All defaults
SCAP and OVAL Auditing	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials

	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Custom	All defaults
Tactical Scans		
Badlock Detection	-	All defaults
Bash Shellshock Detection	-	All defaults
DROWN Detection	-	All defaults
Intel AMT Security Bypass	-	All defaults
Malware Scan	**Default** (default)	• Performance options: ◦ 30 simultaneous hosts (max) ◦ 4 simultaneous checks per host (max) ◦ 5 second network read timeout • Asset identification options:

		◦ Create unique identifier on hosts scanned using credentials
	Scan low bandwidth links	• Performance options: ◦ 2 simultaneous hosts (max) ◦ 2 simultaneous checks per host (max) ◦ 15 second network read timeout ◦ Slow down the scan when network congestion is detected • Asset identification options: ◦ Create unique identifier on hosts scanned using credentials
	Custom	All defaults
Shadow Brokers Scan	-	All defaults
Spectre and Meltdown Detection	-	All defaults
WannaCry Ransomware Detection	-	All defaults

Credentials in Tenable Vulnerability Management Scans

You can use credentials to grant a Tenable Vulnerability Management scanner local access to scan a target system without requiring an agent. Credentialed scans can perform a wider variety of checks than non-credentialed scans, which can result in more accurate scan results. This approach 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 (for example, root or administrator access), the more thorough the scan results.

In Tenable Vulnerability Management, you can create credentials for use in scans in the following ways:

Category	Description	Permissions
Scan-specific	• You configure and store these credentials in an individual scan. • If you delete the scan, you also delete the credentials. • If you want to use the credentials in a different scan, you must either convert the scan-specific credential to a managed credential or recreate the scan-specific credential settings in the other scan.	**User Permissions** in **Basic** settings in the scan
Template-specific	• You configure and store these credentials in a user-defined template. You can then use the template to create individual scans. • If you add credentials to a user-defined template, other users can override those credentials by adding scan-specific or managed credentials to scans created from the template. Tenable recommends adding managed credentials to scans, instead of adding credentials to user-defined templates. • If you delete the template, you also delete the template-specific credentials. However, Tenable Vulnerability Management retains the credentials in any scans you used the template to create before deletion. • If you want to use the credentials in a different	**User Permissions** in **Basic** settings in the template

	template, you must recreate the template-specific credentials in the other template.	
Managed	• Tenable Vulnerability Management stores managed credentials centrally in the credential manager. You can configure managed credentials directly in the credential manager or during scan configuration. You can also convert a scan-specific credential to a managed credential during scan configuration. • You can use managed credentials in multiple scans. You can also grant other users permissions to use managed credentials in scans. • You cannot use managed credentials in templates.	Configure User Permissions for a Credential

The settings you configure for a credential vary based on the credential type. Credential types include:

- Cloud Services
- Database
- Host
- Miscellaneous
- Mobile Device Management
- Patch Management
- Plaintext authentication

For more information, see:

- Add a Credential to a Scan
- Edit a Credential in a Scan
- Convert a Scan-specific Credential to a Managed Credential

- Add a Credential to a User-defined Template
- Edit a Credential in a User-defined Template

Note: Tenable Vulnerability Management opens several concurrent authenticated connections. Ensure that the host being audited does not have a strict account lockout policy based on concurrent sessions.

Note: By default, when creating credentialed scans or user-defined templates, hosts are identified and marked with a **Tenable Asset Identifier (TAI)**. This globally unique identifier is written to the host's registry or file system, and subsequent scans can retrieve and use the **TAI**.

This option is enabled (by default) or disabled in the **Advanced -> General Settings** of a scan configuration or template: **Create unique identifier on hosts scanned using credentials**.

Note: If a Tenable Vulnerability Management scan contains multiple instances of one type of credential, Tenable Vulnerability Management attempts to log into a valid target using each credential in sequence, **in the same order in which they were added to the scan**. Tenable Vulnerability Management uses the first credential it is able to log in successfully with to perform credentialed checks on the target. Once Tenable Vulnerability Management 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.

Add a Credential to a Scan

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Scan Permissions: Can Control

In the event that a scan contains multiple instances of a single type of credential (SSH logins, SMB logins, etc.), Tenable Vulnerability Management attempts to use them on a valid target in the order that they were added to the scan configuration.

Note: The first credential that allows successful login is used to perform credentialed checks on the target. After a credential provides successful login, Tenable Vulnerability Management does not try any of the other credentials in the list, even if one of the latter credentials has a greater degree of access or privileges.

To add a credential to a scan:

1. Create or edit a scan.
2. In the left navigation menu, click **Credentials**.

   The **Credentials** page appears. This page contains a table of credentials configured for the scan.
3. Next to **Add Credentials**, click the ⊕ button.

   The **Select Credential Type** plane appears.
4. Do one of the following:

   ### Add an existing managed credential.

   The **Managed Credentials** section of the **Select Credential Type** plane contains any credentials where you have **Can Use** or **Can Edit** permissions.

   a. (Optional) Search for a managed credential in the list by typing your search criteria in the text box and clicking the 🔍 button.

   b. In the **Managed Credentials** section, click the ⌄ button to display all managed credentials.

   c. Click each managed credential you want to add.

      The **Select Credential Type** plane remains open.

   d. To close the **Select Credential Type** plane, click the ✕ button in the upper-right corner of the plane.

   ### Add a scan-specific credential.

   a. In the **Select Credential Type** plane, in any section except **Managed Credentials**, click the ⌄ button to display the credentials for that type.

   b. Click each credential you want to add.

      The settings plane for that credential type appears.

   c. Configure the settings for the individual credential configuration.

   ### Add a new managed credential.

a. In any section of the **Select Credential Type** plane except the **Managed Credentials** section, click the ⌄ button to display the credentials for that type.

b. Click each credential you want to add.

   The settings plane for that credential type appears.

c. Configure the settings for the new managed credential.

d. Click the **Save to Managed Credentials** toggle.

   The managed credential settings appear.

e. In the first text box, type a name for the managed credential.

f. (Optional) In the second text box, type a brief description of the managed credential.

g. Configure user permissions for the managed credential.

5. Click **Save** to save your credential changes.

   Tenable Vulnerability Management closes the settings plane and adds the credential to the credentials table for the scan.

   > **Note:** Upon saving, Tenable Vulnerability Management automatically orders the credentials by ascending ID and groups the credentials by type.

6. Do one of the following:

   - If you want to save without launching the scan, click **Save**.

     Tenable Vulnerability Management saves the scan.

   - If you want to save and launch the scan immediately, click **Save & Launch**.

     > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

     > **Note:** If you are editing an imported scan, the **Save & Launch** option is not available.

     Tenable Vulnerability Management saves and launches the scan.

Edit a Credential in a Scan

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Scan Permissions: Can Configure

To edit a credential in a scan:

1. Edit a scan.
2. In the left navigation menu, click **Credentials**.

   A table of credentials configured for the scan appears.
3. In the credentials table, click the credential you want to edit.

   The credential settings plane appears.
4. Do one of the following:
   - For scan-specific credentials, configure the settings for the credential.
   - For managed credentials:
     a. Edit the name or description.
     b. Configure the credential settings.
     c. Configure user permissions for the managed credential.
   - **Note:** You can only view or edit settings for managed credentials where you have **Can Edit** permissions.
5. Click **Save** to save your changes to the credential.

   If you edited a managed credential, Tenable Vulnerability Management determines whether any other scans use the managed credential and prompts you to confirm the changes.
6. (Managed credentials only) Click **Yes** to save the changes to the managed credential.
7. Click **Save** to save your scan changes.

Add a Credential to a User-defined Template

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Template Permissions: Can Configure

Before you add credentials to a user-defined template, consider the following:

- Other users can override template-specific credentials by adding scan-specific or managed credentials to scans created from the template. Tenable recommends adding managed credentials to scans, instead of adding credentials to user-defined templates.
- You cannot use managed credentials in user-defined templates. To use a single set of credentials for multiple scans, add managed credentials to scans, instead of adding credentials to user-defined templates.

Note: In scan configurations, the **Scan-wide Credential Type** settings are located in individual credentials. In user-defined templates, these settings are located in the **Authentication** section of the **Basic** settings for the template.

To add a template-specific credential:

1. Create or edit a template.
2. In the left navigation menu, click **Credentials**.

   The **Credentials** page appears. This page contains a table of credentials configured for the template.
3. Next to **Add Credentials**, click the ⊕ button.

   The **Select Credential Type** plane appears.
4. In the **Select Credential Type** plane, click a credential type.

   The settings plane for that credential type appears.
5. Configure the settings for the individual credential configuration.
6. Click **Save** to save your credential changes.

   Tenable Vulnerability Management closes the settings plane and adds the credential to the credentials table for the template.

7. Click **Save** to save your template changes.

   Tenable Vulnerability Management adds the credential to the credentials table for the template.

Edit a Credential in a User-defined Template

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Template Permissions: Can Configure

To edit a credential in a user-defined template:

1. Edit a user-defined template.
2. In the left navigation menu, click **Credentials**.

   A table of credentials configured for the template appears.
3. In the credentials table, click the credential you want to edit.

   The credential settings plane appears.
4. Configure the settings for the credential.
5. Click **Save** to save your changes to the credential.
6. Click **Save** to save your changes to the template.

Convert a Scan-specific Credential to a Managed Credential

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Scan Permissions: Owner

A scan-specific credential can only be used in a single scan. To reuse a scan-specific credential in multiple scans, convert it to a managed credential.

To convert a scan-specific credential:

1. In the left navigation, click **Scans**.

   The **Scans** page appears.

2. In the **Folders** section, click a folder to load the scans you want to view.

   The scans table updates to display the scans in the folder you selected.

3. In the scans table, click the scan you want to edit.

   The **Scan Details** page appears.

4. Next to the scan name, click the button.

   The **Update a Scan** page appears.

5. In the left navigation menu, click **Credentials**.

   A table of credentials configured for the scan appears.

6. In the credentials table, click the scan-specific credential you want to convert.

   The credential settings plane appears.

7. Click the **Save to Managed Credentials** toggle.

   The managed credential settings appear.

8. In the first text box, type a name for the managed credential.

9. (Optional) In the second text box, type a brief description of the managed credential.

10. Configure user permissions for the managed credential.

11. Click **Save** to save your credential changes.

    Tenable Vulnerability Management closes the settings plane and adds the credential to the credentials table for the scan.

12. Click **Save** to save your scan changes.

Cloud Services

Tenable Vulnerability Management can authenticate a scan using accounts in the cloud services listed below.

Note: Some credential types may not be available for configuration, depending on the scan template you selected.

AWS

Option	Default Value	Description	Required
AWS Access Key IDS	-	The AWS access key ID string.	yes
AWS Secret Key	-	AWS secret key that provides the authentication for AWS Access Key ID.	yes
Scan-wide Credential Type Settings			

Regions to access	Rest of the World	In order for Tenable Vulnerability Management to audit an Amazon AWS account, you must define the regions you want to scan. Per Amazon policy, you need different credentials to audit account configuration for the China region than you do for the rest of the world.
		
		Possible regions include:
		
		• **GovCloud** – If you select this region, you automatically select the government cloud (e.g., us-gov-west-1).
		
		• **Rest of the World** – If you select this region, the following additional options appear:
		
		  • us-east-1
		
		  • us-east-2
		
		  • us-west-1
			yes

		• us-west-2
		• ca-central-1
		• eu-west-1
		• eu-west-2
		• eu-central-1
		• ap-northeast-1
		• ap-northeast-2
		• ap-southeast-1
		• ap-southeast-2
		• sa-east-1
		• **China** – If you select this region, the following additional options appear:
		  • cn-north-1
		  • cn-northwest-1	

HTTPS	Enabled	Whether Tenable Vulnerability Management authenticates over an encrypted (HTTPS) or an unencrypted (HTTP) connection.	no
Verify SSL Certificate	Enabled	Whether Tenable Vulnerability Management verifies the validity of the SSL digital certificate.	no

Microsoft Azure

Option	Default Value	Description	Required
Username	-	Username required to log in to Microsoft Azure.	yes

Password	-	Password associated with the username.	yes
Client Id	-	The application ID (also known as client ID) for your registered application.	yes
Scan-wide Credential Type Settings			
Subscription IDs	-	List subscription IDs to scan, separated by a comma. If this field is blank, all subscriptions are audited.	no

Rackspace

Option	Default Value	Description	Required
Username	-	Username to log in.	yes
Password or API Key	-	Password or API key associated with the username.	yes
Authentication Method	API-Key	Select **Password** or **API-Key** from the drop-down box.	yes
Scan-wide Credential Type Settings	all locations selected	Location of the Rackspace Cloud instance. Possible locations include: • Dallas-Fort Worth (DFW) • Chicago (ORD) • Northern Virginia (IAD) • London (LON) • Syndney (SYD) • Hong Kong (HKG)	no

Salesforce.com

Option	Default	Description	Required

	Value		
Username	-	Username required to log in to Salesforce.com	yes
Password	-	Password associated with the Salesforce.com username	yes

Database Credentials

Note: Some credential types may not be available for configuration, depending on the scan template you selected.

The following topic describes the available **Database** credentials.

Cassandra

Option	Description
Auth Type	The authentication method for providing the required credentials. • **Password** • **CyberArk** • **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
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
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	Yes

Option	Description	Required
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
Use Private Key	Use key-based authentication for SSH connections instead of password authentication.	No

Option	Description	Required
Use SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Verify the Delinea Secret Server SSL certificate.	No

DB2

The following table describes the additional options to configure for **DB2** credentials.

Options	Description
Auth Type	The authentication method for providing the required credentials. • **Password** • **Import** • **CyberArk** • **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Database Port	The TCP port that the IBM DB2 database instance listens on for communications from Tenable Vulnerability Management. The default is port 50000.
Database Name	The name for your database (not the name of your instance).

MongoDB

Option	Description
Auth Type	The authentication method for providing the required credentials. **Note:** This option is only available for non-legacy versions of the MongoDB

Option	Description
	authentication method. • **Password** • **Client Certificate** • **CyberArk** • **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Username	(Required) The username for the database.
Password	(Required) 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 Vulnerability Management.

MySQL

The following table describes the additional options to configure for **MySQL** credentials.

Options	Description
Auth Type	The authentication method for providing the required credentials. • **Password** • **Import** • **CyberArk** • **Lieberman**

Options	Description
	• **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Username	The username for a user on the database.
Password	The password associated with the username you provided.
Database Port	The TCP port that the MySQL database instance listens on for communications from Tenable Vulnerability Management. The default is port 3306.

Oracle

The following table describes the additional options to configure for **Oracle** credentials.

Options	Description
Auth Type	The authentication method for providing the required credentials. • **Password** • **Import** • **CyberArk** • **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Database Port	The TCP port that the Oracle database instance listens on for communications from Tenable Vulnerability Management. The default is port 1521.
Auth Type	The type of account you want Tenable Vulnerability Management to use to access the database instance: • **SYSDBA**

Options	Description
	• **SYSOPER** • **NORMAL**
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
Auth Type	The authentication method for providing the required credentials. • **Password** • **Client Certificate** • **CyberArk** • **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Database Port	The TCP port that the PostgreSQL database instance listens on for communications from Tenable Vulnerability Management. 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
Auth Type	The authentication method for providing the required credentials. • **Password** • **Import** • **CyberArk** • **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Username	The username for a user on the database.
Password	The password associated with the username you provided.
Database Port	The TCP port that the SQL Server database instance listens on for communications from Tenable Vulnerability Management. The default is port 1433.
AuthType	The type of account you want Tenable Vulnerability Management 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
Auth Type	The authentication method for providing the required credentials. • **Password** • **CyberArk**

Options	Description
	• **Lieberman** • **Hashicorp Vault** For descriptions of the options for your selected authentication type, see Database Credentials Authentication Types.
Database Port	The TCP port that the Sybase ASE database instance listens on for communications from Tenable Vulnerability Management. The default is port 3638.
Auth Type	The type of authentication used by the Sybase ASE database: **RSA** or **Plain Text**.

Database Credentials Authentication Types

Depending on the authentication type you select for your database credentials, you must configure the options described in this topic.

Client Certificate

The **Client Certificate** authentication type is supported for **PostgreSQL** databases only.

Option	Description	Required
Username	The username for the database.	yes
Client Certificate	The file that contains the PEM certificate for the database.	yes
Client CA Certificate	The file that contains the PEM certificate for the database.	yes
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes
Client Certificate Private Key Passphrase	The passphrase for the private key, if required in your authentication implementation.	no

Option	Description	Required
Database Port	The port on which Tenable Vulnerability Management communicates with the database.	yes
Database Name	The name of the database.	no

Password

Option	Database Types	Description	Required
Username	All	The username for a user on the database.	yes
Password	All	The password for the supplied username.	no
Database Port	All	The port on which Tenable Vulnerability Management 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: • SYSDBA • SYSOPER • NORMAL Sybase ASE values include: • RSA	yes

Option	Database Types	Description	Required
		• Plain Text	
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

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 Vulnerability Management can retrieve the credentials.

Database Credential	CSV Format
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_`

Database Credential	CSV Format
	`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*.

BeyondTrust

Option	Description	Required
Username	The username to log in to the host you want to scan.	yes
Domain	The domain of the username, which is recommended if using domain-linked accounts (managed accounts of a domain that are linked to a managed system).	no
BeyondTrust host	The BeyondTrust IP address or DNS address.	yes
BeyondTrust port	The port on which BeyondTrust listens.	yes
BeyondTrust API user	The API user provided by BeyondTrust.	yes
BeyondTrust API key	The API key provided by BeyondTrust.	yes
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 scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in BeyondTrust so that password changes do not	yes

	disrupt your scans. If BeyondTrust changes a password during a scan, the scan fails.	
Use SSL	When enabled, the integration uses SSL through IIS for secure communications. Configure SSL through IIS in BeyondTrust before enabling this option. **Caution:** If you do not enable this option the traffic that is sent is http and will not be accepted by the Beyond Trust server.	no
Verify SSL certificate	When enabled, the intergation validates the SSL certificate. Configure SSL through IIS in BeyondTrust before enabling this option.	no

CyberArk

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can get credentials from CyberArk to use in a scan.

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	no

Option	Description	Required
	Tenable's Community post about CyberArk Client Certification Authentication Issue.	
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 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
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	no

Option	Description	Required
	through IIS and you want to validate the certificate.	

CyberArk (Legacy)

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can get credentials from CyberArk to use in a scan.

Option	Database Types	Description	Required
Username	All	The target system's username.	yes
Central Credential Provider Host	All	The CyberArk Central Credential Provider IP/DNS address.	yes
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	no

Option	Database Types	Description	Required
		information you would like to retrieve.	
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
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

Option	Database Types	Description	Required
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
Database Port	All	The port on which Tenable Vulnerability Management 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: • **SYSDBA** • **SYSOPER** • **NORMAL** Sybase ASE values include: • RSA • Plain Text	yes

Option	Database Types	Description	Required
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

Delinea

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 or DNS address.	yes
Delinea Port	The port on which Delinea Secret Server listens.	yes
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, credentials are 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 Delinea Login Name you provided.	yes

Delinea API key	The API key provided by Delinea Secret Server.	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

Delinea Auto Discovery

Option	Description	Required
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 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

Option	Description	Required
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
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

HashiCorp Vault

HashiCorp Vault is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can get credentials from HashiCorp Vault to use in a scan.

Option	Description	Required
Hashicorp Vault 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 Vault port	The port on which Hashicorp Vault listens.	yes
Authentication Type	Specifies the authentication type for connecting to	yes

	the instance: **App Role** or **Certificates**. If you select **Certificates**, additional options for **Hashicorp Client Certificate** and **Hashicorp Client Certificate Private Key** appear. Select the appropriate files for the client certificate and private key.	
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 environment.	no
Vault Type	The Tenable Vulnerability Management version: KV1, KV2, AD, or LDAP. For additional information about Tenable Vulnerability Management versions, see the Tenable Vulnerability Management documentation.	yes
KV1 Engine URL	(KV1) The URL Tenable Vulnerability Management uses to access the KV1 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL Tenable Vulnerability Management uses to access the KV2 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL Tenable Vulnerability Management uses to access the active directory	yes, if you select the AD

	engine. Example: `/v1/path_to_secret`. No trailing `/`	**Vault Type**
LDAP Engine URL	(LDAP) The URL Tenable Vulnerability Management uses to access the LDAP engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the LDAP **Vault Type**
Username Source	(KV1 and KV2) A drop-down box to specify whether the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(KV1 and KV2) The name in Hashicorp Vault that usernames are stored under.	yes
Password Key	(KV1 and KV2) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	(KV1, KV2, and AD) The key secret you want to retrieve values for.	yes
Use SSL	If enabled, Tenable Nessus Manager uses SSL for secure communications. Configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, validates the SSL certificate. You must configure SSL in Hashicorp Vault before enabling this option.	no
Database Port	The port on which communicates with the database.	yes
Auth Type	The authentication method for the database credentials. Oracle values include: • SYSDBA • SYSOPER	yes

	• NORMAL	
Service Type	(Oracle databases only) Valid values include: SID and SERVICE_NAME.	yes
Service	(Oracle database only) A specific field for the configuration for the database.	yes

Lieberman

Lieberman is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can get credentials from Lieberman to use in a scan.

Option	Database Type	Description	Required
Username	All	The target system's username.	yes
Lieberman host	All	The Lieberman IP/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*.	yes
Lieberman port	All	The port on which Lieberman listens.	yes
Lieberman API URL	All	The URL Tenable Vulnerability Management uses to access Lieberman.	no
Lieberman user	All	The Lieberman explicit user for authenticating to the Lieberman API.	yes
Lieberman password	All	The password for the Lieberman explicit user.	yes
Lieberman Authenticator	All	The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman.	no

Option	Database Type	Description	Required
		Note: If you use this option, append a domain to the **Lieberman user** option, i.e., *domain\user*.	
Lieberman Client Certificate	All	The file that contains the PEM certificate used to communicate with the Lieberman host. **Note:** If you use this option, you do not have to enter information in the **Lieberman user**, **Lieberman password**, and **Lieberman Authenticator** fields.	no
Lieberman Client Certificate Private Key	All	The file that contains the PEM private key for the client certificate.	no
Lieberman Client Certificate Private Key Passphrase	All	The passphrase for the private key, if required.	no
Use SSL	All	If Lieberman is configured to support SSL through IIS, check for secure communication.	no
Verify SSL Certificate	All	If Lieberman is configured to support SSL through IIS and you want to validate the certificate, check this option. Refer to Custom CA documentation for how to use self-signed certificates.	no
System Name	All	In the rare case your organization uses one default Lieberman entry for	no

Option	Database Type	Description	Required
		all managed systems, enter the default entry name.	
Database Port	All	The port on which Tenable Vulnerability Management communicates with the database.	yes
Database Name	DB2 PostgreSQL	(PostgreSQL and DB2 databases only) The name of the database.	no
Auth type	Oracle SQL Server Sybase ASE	(SQL Server, Oracle. and Sybase ASE databases only) SQL Server values include: • Windows • SQL Oracle values include: • SYSDBA • SYSOPER • NORMAL 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	no

Option	Database Type	Description	Required
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.	yes

QiAnXin

QiAnXin is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can get credentials from QiAnXin to use in a scan.

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 Secret ID	The Secret ID for the embedded account application created in QiAnXin PAM	yes
Username	The username to log in to the hosts you want to scan.	yes
Host IP	Specify the host IP of the asset containing the account to use. If not specified, the scan target IP is used.	no
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:	no

Option	Description	Required
	• **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	
Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions
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

Option	Description	Required
Senhasegura Host	The IP address or URL for the Senhasegura host.	yes
Senhasegura Port	The port on which the Senhasegura API	yes

Option	Description	Required
	communicates. By default, Tenable uses 443.	
Senhasegura API Client ID	The Client ID for the applicable Senhasegura A2A Application for Oauth 2.0 API authentication.	yes
Senhasegura API Secret ID	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 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.
HTTPS	This is enabled by default.	yes
Verify SSL Certificate	This is disabled by default.	no

Host

Tenable Vulnerability Management supports the following forms of host authentication:

- SNMPv3
- Secure Shell (SSH)
- Windows

Note: Some credential types may not be available for configuration, depending on the scan template you selected.

SNMPv3

Use SNMPv3 credentials to scan remote systems that use an encrypted network management protocol (including network devices). Tenable Vulnerability Management uses these credentials to scan for patch auditing or compliance checks.

Note: SNMPv3 options are only available in the Advanced Network Scan template.

Click **SNMPv3** in the **Credentials** list to configure the following settings:

Option	Description	Default	Required
Username	(Required) The username for the SNMPv3 account that Tenable Vulnerability Management uses to perform checks on the target system.	-	yes
Port	The TCP port that SNMPv3 listens on for communications from Tenable Vulnerability Management.	161	no
Security level	The security level for SNMP: • **Authentication without privacy** • **Authentication and privacy**	Authentication and privacy	yes
Authentication algorithm	The algorithm the remove service supports: **SHA1**, **SHA224**, **SHA-256**, **SHA-**	SHA1	yes (if you select authentication)

Option	Description	Default	Required
	384, **SHA-512** or **MD5**.		
Authentication password	(Required) The password associated with the **Username**.	-	yes (if you select authentication)
Privacy algorithm	The encryption algorithm to use for SNMP traffic: **AES**, **AES-192**, **AES-192C**, **AES-256**, **AES-256C**, or **DES**.	AES-192	yes (if you select authentication with privacy)
Privacy password	(Required) A password used to protect encrypted SNMP communication.	-	yes (if you select authentication with privacy)

SSH

Use SSH credentials for host-based checks on Unix systems and supported network devices. Tenable Vulnerability Management uses these credentials to obtain local information from remote Unix systems for patch auditing or compliance checks. Tenable Vulnerability Management uses Secure Shell (SSH) protocol version 2 based programs (e.g., OpenSSH, Solaris SSH, etc.) for host-based checks.

Tenable Vulnerability Management encrypts the data 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.

Select **SSH** in the **Credentials** list to configure the settings for the following SSH authentication methods:

SSH Authentication Method: Public Key

Public Key Encryption, also referred to as asymmetric key encryption, provides a more secure authentication mechanism by the use of a public and private key pair. In asymmetric cryptography, the public key is used to encrypt data and the private key is used to decrypt it. The use of public and private keys is a more secure and flexible method for SSH authentication. Tenable Vulnerability Management supports both DSA and RSA key formats.

Like Public Key Encryption, Tenable Vulnerability Management supports RSA and DSA OpenSSH certificates. Tenable Vulnerability Management also requires the user certificate, which is signed by a Certificate Authority (CA), and the user's private key.

> **Note:** Tenable Vulnerability Management supports the OpenSSH SSH public key format. Formats from other SSH applications, including PuTTY and SSH Communications Security, must be converted to OpenSSH public key format.

The most effective credentialed scans are when the supplied credentials have root privileges. Since many sites do not permit a remote login as root, Tenable Vulnerability Management can invoke su, sudo, su+sudo, dzdo, .k5login, or pbrun with a separate password for an account that has been set up to have su or sudo privileges. In addition, Tenable Vulnerability Management can escalate privileges on Cisco devices by selecting Cisco 'enable' or .k5login for Kerberos logins.

> **Note:** Tenable Vulnerability Management supports the blowfish-cbc, aes-cbc, and aes-ctr cipher algorithms. Some commercial variants of SSH do not have support for the blowfish algorithm, possibly for export reasons. It is also possible to configure an SSH server to accept certain types of encryption only. Check your SSH server to ensure the correct algorithm is supported.

Tenable Vulnerability Management encrypts all passwords stored in policies. However, the use of SSH keys for authentication rather than SSH passwords is recommended. This helps ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log into a system that may not be under your control.

> **Note:** For supported network devices, Tenable Vulnerability Management only supports the network device's username and password for SSH connections.

If an account other than root must be used for privilege escalation, it can be specified under the Escalation account with the Escalation password.

Option	Description	Required
Username	The username to authenticate to the host.	yes
Private Key	The RSA or DSA Open SSH key file of the user.	yes
Private key passphrase	The passphrase of the Private Key.	no
Elevate privileges with	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your selection determines the specific options you must configure. For more information, see Privilege Escalation.	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

SSH Authentication Method: Certificate

Option	Description	Required
Username	The username to authenticate to the host.	yes
User Certificate	The RSA or DSA Open SSH certificate file of the user.	yes
Private Key	The RSA or DSA Open SSH key file of the user.	yes

Option	Description	Required
Private key passphrase	The passphrase of the Private Key.	no
Elevate privileges with	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your selection determines the specific options you must configure. For more information, see Privilege Escalation.	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

SSH Authentication Method: CyberArk Vault

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can get credentials from CyberArk to use in a scan.

CyberArk

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the CyberArk AIM Web Service.	yes
Port	The port on which the CyberArk API communicates. By	yes

Option	Description	Required
	default, Tenable uses 443.	
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	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

Option	Description	Required
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 Vulnerability Management uses 443.	yes
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

Option	Description	Required
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

CyberArk Auto-Discovery

You can now take advantage of a significant improvement to Tenable's CyberArk Integration which gathers bulk account information for specific target groups without entering multiple targets. For more information, see CyberArk Dynamic Scanning in the *Tenable CyberArk Integrations Guide*.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the user's CyberArk Instance. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
Port	The port on which the CyberArk API communicates. By	yes

Option	Description	Required
	default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
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
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 for the username to log in to CyberArk web console. This is used to authenticate to the PVWA	yes

Option	Description	Required
Password	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 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
Elevate Privileges with	Users can only select Nothing or sudo at this time.	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.	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
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	no

Option	Description	Required
	use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	

CyberArk (Legacy)

Option	Description	Required
Username	The username of the target system.	yes
CyberArk AIM Service URL	The URL for the CyberArk AIM web service. By default, Tenable Vulnerability Management uses `/AIMWebservice/v1.1/AIM.asmx`.	no
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.	yes
Central Credential Provider Port	The port on which the CyberArk Central Credential Provider is listening.	yes
Central Credential Provider Username	The username of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.	no
Central Credential Provider Password	The password of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.	no
Safe	The safe on the CyberArk Central Credential Provider server that contained the authentication information that you want to retrieve.	yes

Option	Description	Required
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	no
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.	yes
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information that you want to retrieve.	yes
PolicyId	The PolicyID assigned to the credentials that you want to retrieve from the CyberArk Central Credential Provider.	no
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.	no
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.	no
Targets to	Specify IPs or CIDR blocks on which this credential is	no

Option	Description	Required
Prioritize Credentials	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.	
CyberArk Account Details Name	The unique name of the credential you want to retrieve from CyberArk.	no
CyberArk Address	The domain for the user account.	no
CyberArk elevate privileges with	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your selection determines the specific options you must configure.	no
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable Vulnerability Management receiving an unrecognized password prompt on the target host's interactive SSH shell.	no

DelineaSSH Authentication Method: Delinea

Option	Description	Required
Delinea	Indicates whether to use credentials or an API key for	yes

Authentication Method	authentication. By default, **Credentials** is selected.	
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
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
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
Use Private Key	If enabled, uses key-based authentication for SSH connections instead of password authentication.	no
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	no

	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.	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
Elevate privileges with	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 prompts. Leave this blank for most standard password prompts.	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	no

	the scan to use the successful credential first, which allows the scan to access the target faster.	

Delinea Auto DiscoverySSH Authentication Method: Delinea Auto Discovery

Option	Description	Required
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 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

Option	Description	Required
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
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
Delinea Elevate Privileges With	The privilege escalation method to use to increase users' privileges after initial authentication. Multiple options for privilege escalation are supported, including su, su+sudo and sudo. Selecting a privilege escalation method provides options to configure an escalation query, similar to “query mode” and its related options. These fields must only be completed if using a separate account for escalation than initial login (for example, “su”).	Yes

SSH Authentication Method: Hashicorp Vault

HashiCorp Vault is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can retrieve credentials from HashiCorp Vault to use in a scan.

Windows and SSH Credentials		
Option	Description	Required

Hashicorp Vault 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 Vault 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 environment.	no
Vault Type	The Tenable Vulnerability Management version: KV1, KV2, AD, or LDAP. For additional information about Tenable Vulnerability Management versions, see the Tenable Vulnerability Management documentation.	yes

KV1 Engine URL	(KV1) The URL Tenable Vulnerability Management uses to access the KV1 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL Tenable Vulnerability Management uses to access the KV2 engine. Example: `/v1/kv_mount_name`. No trailing `/` **Note:** You cannot use the path to the secret for the KV2 Engine URL because an additional string/segment, `data`, gets injected into the read request made to Vault for KV v2 stores. Only enter the name of the KV mount, not the path to the secret, in the **Engine URL** field. **Note:** You do not need to include the `data` segment yourself. If you include it in the secret name/path, the read call to Vault includes `/data/data`, which is invalid.	yes, if you select the KV2 **Vault Type**
AD Engine URL	(AD) The URL Tenable Vulnerability Management uses to access the Active Directory engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the AD **Vault Type**
LDAP Engine URL	(LDAP) The URL Tenable Vulnerability Management uses to access the LDAP engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the LDAP **Vault Type**
Username Source	(KV1 and KV2) A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(KV1 and KV2) The name in Hashicorp Vault that usernames are stored under.	yes

Domain Key	(KV1 and KV2) The name in Hashicorp Vault that domains are stored under.	no
Password Key	(KV1 and KV2) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	(KV1, KV2, and AD) 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	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 (Windows)	(Required if Kerberos Target Authentication is enabled.) The domain to which Kerberos Target Authentication belongs, if applicable.	yes
Realm (SSH)	(Required if Kerberos Target Authentication is enabled.) The Realm is the authentication domain, usually noted as the domain name of the target (e.g., example.com).	yes
Use SSL	If enabled, Tenable Vulnerability Management uses SSL for secure communications. Configure SSL in	no

	Hashicorp Vault before enabling this option.	
Verify SSL Certificate	If enabled, Tenable Vulnerability Management uses SSL for secure communications. Hashicorp Vault must be using SSL to enable this option.	no
Enable for Tenable Vulnerability Management	Enables/disables IBM DataPower Gateway use with Tenable Vulnerability Management.	yes
Escalate Privileges with (SSH)	Use a privilege escalation method such as su or sudo to use extra privileges when scanning. **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 and can be completed to support authentication and privilege escalation through Tenable Vulnerability Management. 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 the Nessus User Guide and the Tenable Vulnerability Management User Guide.	Required if you wish to escalate privileges.
Escalation account credential ID or identifier (SSH)	If the escalation account has a different username or password from the least privileged user, enter the credential ID or identifier for the escalation account credential here.	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.	

SSH Authentication Method: Kerberos

Kerberos, developed by MIT's Project Athena, is a client/server application that uses a symmetric key encryption protocol. In symmetric encryption, the key used to encrypt the data is the same as the key used to decrypt the data. Organizations deploy a KDC (Key Distribution Center) that contains all users and services that require Kerberos authentication. Users authenticate to Kerberos by requesting a TGT (Ticket Granting Ticket). Once a user is granted a TGT, it can be used to request service tickets from the KDC to be able to utilize other Kerberos based services. Kerberos uses the CBC (Cipher Block Chain) DES encryption protocol to encrypt all communications.

Note: You must already have a Kerberos environment established to use this method of authentication.

The Tenable Vulnerability Management implementation of Unix-based Kerberos authentication for SSH supports the aes-cbc and aes-ctr encryption algorithms. An overview of how Tenable Vulnerability Management interacts with Kerberos is as follows:

1. The end user gives the IP of the KDC.
2. The nessusd asks sshd if it supports Kerberos authentication.
3. The sshd says yes.
4. The nessusd requests a Kerberos TGT, along with login and password.
5. Kerberos sends a ticket back to nessusd.

6. The nessusd gives the ticket to sshd.
7. The nessusd is logged in.

In both Windows and SSH credentials settings, you can specify credentials using Kerberos keys from a remote system. There are differences in the configurations for Windows and SSH.

Option	Description	Required
Username	The username of the target system.	yes
Password	The password of the username specified.	yes
Key Distribution Center (KDC)	This host supplies the session tickets for the user.	yes
KDC Port	Directs Tenable Vulnerability Management to connect to the KDC if it is running on a port other than 88.	no
KDC Transport	The method by which you want to access the KDC server. **Note:** if you set **KDC Transport** to **UDP**, you may also need to change the port number, because depending on the implementation, the KDC UDP protocol uses either port 88 or 750 by default.	no
Realm	The authentication domain, usually noted as the domain name of the target (for example, example.com).	yes
Elevate privileges with	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your selection determines the specific options you must configure. For more information, see Privilege Escalation.	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.	no

Option	Description	Required
	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.	

If Kerberos is used, sshd must be configured with Kerberos support to verify the ticket with the KDC. Reverse DNS lookups must be properly configured for this to work. The Kerberos interaction method must be gssapi-with-mic.

SSH Authentication Method: Password

Option	Description	Required
Username	The username of the target system.	yes
Password	The password of the username specified.	yes
Elevate privileges with	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your selection determines the specific options you must configure. For more information, see Privilege Escalation.	no
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable Vulnerability Management receiving an unrecognized password prompt on the target host's interactive SSH shell.	no
Targets to Prioritize	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple	no

Option	Description	Required
Credentials	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.	

SSH Authentication Method: Lieberman RED

Lieberman is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can get credentials from Lieberman to use in a scan.

Option	Description	Required
Username	The target system's username.	yes
Lieberman host	The Lieberman IP/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*.	yes
Lieberman port	The port on which Lieberman listens.	yes
Lieberman API URL	The URL Tenable Vulnerability Management uses to access Lieberman.	no
Lieberman user	The Lieberman explicit user for authenticating to the Lieberman RED API.	yes
Lieberman	The password for the Lieberman explicit user.	yes

Option	Description	Required
password		
Lieberman Authenticator	The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman. **Note:** If you use this option, append a domain to the **Lieberman user** option, i.e., *domain\user*.	no
Lieberman Client Certificate	The file that contains the PEM certificate used to communicate with the Lieberman host. **Note:** If you use this option, you do not have to enter information in the **Lieberman user**, **Lieberman password**, and **Lieberman Authenticator** fields.	no
Lieberman Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
Lieberman Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	no
Use SSL	If Lieberman is configured to support SSL through IIS, check for secure communication.	no
Verify SSL Certificate	If Lieberman is configured to support SSL through IIS and you want to validate the certificate, check this option. Refer to Custom CA documentation for how to use self-signed certificates.	no
System Name	In the rare case your organization uses one default Lieberman entry for all managed systems, enter the	no

Option	Description	Required
	default entry name.	
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable Vulnerability Management receiving an unrecognized password prompt on the target host's interactive SSH shell.	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

SSH Authentication Method: QiAnXin

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

Option	Description	Required
QiAnXin API Secret ID	The Secret ID for the embedded account application created in QiAnXin PAM.	yes
Username	The username to log in to the hosts you want to scan.	yes
Host IP	Specify the host IP of the asset containing the account to use. If not specified, the scan target IP is used.	no
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 • **OPENLDAP** – OpenLDAP	no

Option	Description	Required
	• **POSTGRESQL** – PostgreSQL	
Region ID	Specify the region ID of the asset containing the account to use.	Only if using multiple regions
Escalate Privileges with	Use the drop-down menu to select the privilege elevation method, or select “Nothing” to skip privilege elevation. **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 and can be completed to support authentication and privilege escalation through QiAnXin. The Escalation Account Name field is only required if the escalation password differs from the normal login password. **Note:** For more information about supported privilege escalation types and their accompanying fields, see the Nessus User Guide or the Tenable Vulnerability Management User Guide.	Required if you wish to escalate privileges.
Escalation Account Username	If the escalation account has a different username or password from the least privileged user, enter the credential ID or identifier for the escalation account credential here.	no
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution	(Required if Kerberos Target Authentication is	yes

Option	Description	Required
Center (KDC)	enabled) This host supplies the session tickets for the user.	
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 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	no

Option	Description	Required
	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.	

SSH Authentication Method: Thycotic Secret Server

Option	Description	Required
Username	The username to authenticate via SSH to the system.	yes
Thycotic Secret Name	The value of the secret on the Thycotic server. The secret is labeled **Secret Name** on the Thycotic server.	yes
Thycotic Secret Server URL	The transfer method, target, and target directory for the scanner. You can find this value on the Thycotic server in **Admin** > **Configuration** > **Application Settings** > **Secret Server URL**. For example, consider the following address: **`https://pw.mydomain.com/SecretServer/`**. • Transfer method: **`https`** indicates an ssl connection. • Target: **`pw.mydomain.com`** is the target address. • Target Directory: **`/SecretServer/`** is the root directory.	yes
Thycotic Login Name	The username to authenticate to the Thycotic server.	yes
Thycotic Password	The password to authenticate to the Thycotic server.	yes
Thycotic	The organization you want to query. You can use this	no

Organization	value for cloud instances of Thycotic.	
Thycotic Domain	The domain of the Thycotic server.	no
Use Private Key	The key for the SSH connection, if you do not use a password.	no
Verify SSL Certificate	Whether you want to verify if the SSL Certificate on the server is signed by a trusted CA.	no
Thycotic elevate privileges with	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. For more information, see Privilege Escalation.	no
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable Vulnerability Management receiving an unrecognized password prompt on the target host's interactive SSH shell.	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	no

	access the target faster.	

SSH Authentication Method: BeyondTrust

Option	Description	Required
Username	The username to log in to the hosts you want to scan.	yes
BeyondTrust host	The BeyondTrust IP address or DNS address.	yes
BeyondTrust port	The port on which BeyondTrust listens.	yes
BeyondTrust API user	The API user provided by BeyondTrust.	yes
BeyondTrust API key	The API key provided by BeyondTrust.	yes
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 Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in BeyondTrust so that password changes do not disrupt your Tenable Vulnerability Management scans. If BeyondTrust changes a password during a scan, the scan fails.	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.	no

	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.	
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 Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option. **Caution:** If you do not enable this option the traffic that is sent is http and will not be accepted by the Beyond Trust server.	no
Verify SSL certificate	When enabled, Tenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.	no
Use private key	When enabled, Tenable Vulnerability Management uses private key-based authentication for SSH connections instead of password authentication. If it fails, the password is requested.	no
Use privilege escalation	When enabled, BeyondTrust uses the configured privilege escalation command. If it returns something, it will use it for the scan.	no
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable Vulnerability Management receiving an unrecognized password prompt on the target host's interactive SSH shell.	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

Scan-wide Credential Type Settings for SSH

These settings apply to all SSH-type credentials in the current scan. You can edit these settings in any instance of the credential type in the current scan; your changes automatically apply to the other credentials of that type in the scan.

Option	Default Value	Description
known_ hosts file	None	If you upload an SSH known_hosts file, Tenable Vulnerability Management only attempts to log in to hosts in this file. This can ensure that the same username and password you are using to audit your known SSH servers is not used to attempt a log into a system that may not be under your control.
Preferred port	22	The port on which SSH is running on the target system.
Client version	OpenSSH_5.0	The type of SSH client Tenable Vulnerability Management impersonates while scanning.
Attempt least	Cleared	Enables or disables dynamic privilege escalation. When

Option	Default Value	Description
privilege		enabled, Tenable Vulnerability Management attempts to run the scan with an account with lesser privileges, even if the **Elevate privileges with** option is enabled. If a command fails, Tenable Vulnerability Management escalates privileges. Plugins 101975 and 101976 report which plugins ran with or without escalated privileges. **Note:** Enabling this option may increase scan run time by up to 30%.

SSH Authentication Method: Centrify

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 Vulnerability Management 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 Vulnerability Management uses *centrify*.
Authentication URL	(Required) The URL Tenable Vulnerability Management uses to access Centrify. By default, Tenable Vulnerability Management uses */Security*.
Password Query URL	(Required) The URL Tenable Vulnerability Management uses to query the passwords in Centrify. By default, Tenable Security Center uses */RedRock*.
Password Engine	(Required) The URL Tenable Vulnerability Management uses to access

URL	the passwords in Centrify. By default, Tenable Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.

SSH Authentication Method: Arcon

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.

Note: Non-privileged users with local access on Unix 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.

Windows

Click **Windows** in the **Credentials** list to configure settings for the following Windows-based authentication methods:

Windows Authentication Method: CyberArk Vault

CyberArk is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can get credentials from CyberArk to use in a scan.

CyberArk

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.	no

Option	Description	Required
	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.	
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	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 domain to which Kerberos Target Authentication belongs, if applicable.	yes
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Address**, **Identifier**, **Parameters**, or **Username**.	yes

Option	Description	Required
	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.	
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

CyberArk Auto-Discovery

You can now take advantage of a significant improvement to Tenable's CyberArk Integration which gathers bulk account information for specific target groups without entering multiple targets. For more information, see CyberArk Dynamic Scanning in the *Tenable CyberArk Integrations Guide*.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the user's CyberArk Instance. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
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

Option	Description	Required
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 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 (Legacy)

Option	Description	Required
Username	The username of the target system.	yes
CyberArk AIM Service URL	The URL for the CyberArk AIM web service. By default, Tenable Vulnerability Management uses `/AIMWebservice/v1.1/AIM.asmx`.	no

Option	Description	Required
Domain	The domain to which the username belongs.	no
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.	yes
Central Credential Provider Port	The port on which the CyberArk Central Credential Provider is listening.	yes
Central Credential Provider Username	The username of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.	no
Central Credential Provider Password	The password of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.	no
Safe	The safe on the CyberArk Central Credential Provider server that contained the authentication information that you want to retrieve.	yes
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
CyberArk Client Certificate	The passphrase for the private key, if required.	no

Option	Description	Required
Private Key Passphrase		
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.	yes
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information that you want to retrieve.	yes
PolicyId	The PolicyID assigned to the credentials that you want to retrieve from the CyberArk Central Credential Provider.	no
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.	no
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.	no
CyberArk Account Details Name	The unique name of the credential you want to retrieve from CyberArk.	no

Windows Authentication Method: Delinea

Option	Description	Required
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	The password to authenticate to the Delinea server. This	yes

Password	is associated with the Delinea Login Name you provided.	
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
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
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, 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

Windows Authentication Method: Delinea Auto Discovery

Option	Description	Required
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 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	No

Option	Description	Required
	default, this is unselected. This option is only available if query mode is set to **Simple**.	
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
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

Windows Authentication Method: Hashicorp Vault

HashiCorp Vault is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can retrieve credentials from HashiCorp Vault to use in a scan.

Windows and SSH Credentials		
Option	Description	Required
Hashicorp Vault 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 Vault 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	yes

	Hashicorp Client Certificate(Required) and **Hashicorp Client Certificate Private Key** (Required) appear. Select the appropriate files for the client certificate and private key.	
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 environment.	no
Vault Type	The Tenable Vulnerability Management version: KV1, KV2, AD, or LDAP. For additional information about Tenable Vulnerability Management versions, see the Tenable Vulnerability Management documentation.	yes
KV1 Engine URL	(KV1) The URL Tenable Vulnerability Management uses to access the KV1 engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the KV1 **Vault Type**
KV2 Engine URL	(KV2) The URL Tenable Vulnerability Management uses to access the KV2 engine. Example: `/v1/kv_mount_name`. No trailing `/` **Note:** You cannot use the path to the secret for the KV2 Engine URL because an additional string/segment, `data`, gets injected into the read request made to Vault for KV v2 stores. Only enter the name of the KV mount, not the path to the secret, in	yes, if you select the KV2 **Vault Type**

	the **Engine URL** field. **Note:** You do not need to include the `data` segment yourself. If you include it in the secret name/path, the read call to Vault includes `/data/data`, which is invalid.	
AD Engine URL	(AD) The URL Tenable Vulnerability Management uses to access the Active Directory engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the AD **Vault Type**
LDAP Engine URL	(LDAP) The URL Tenable Vulnerability Management uses to access the LDAP engine. Example: `/v1/path_to_secret`. No trailing `/`	yes, if you select the LDAP **Vault Type**
Username Source	(KV1 and KV2) A drop-down box to specify if the username is input manually or pulled from Hashicorp Vault.	yes
Username Key	(KV1 and KV2) The name in Hashicorp Vault that usernames are stored under.	yes
Domain Key	(KV1 and KV2) The name in Hashicorp Vault that domains are stored under.	no
Password Key	(KV1 and KV2) The key in Hashicorp Vault that passwords are stored under.	yes
Secret Name	(KV1, KV2, and AD) 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	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 (Windows)	(Required if Kerberos Target Authentication is enabled.) The domain to which Kerberos Target Authentication belongs, if applicable.	yes
Realm (SSH)	(Required if Kerberos Target Authentication is enabled.) The Realm is the authentication domain, usually noted as the domain name of the target (e.g., example.com).	yes
Use SSL	If enabled, Tenable Vulnerability Management uses SSL for secure communications. Configure SSL in Hashicorp Vault before enabling this option.	no
Verify SSL Certificate	If enabled, Tenable Vulnerability Management uses SSL for secure communications. Hashicorp Vault must be using SSL to enable this option.	no
Enable for Tenable Vulnerability Management	Enables/disables IBM DataPower Gateway use with Tenable Vulnerability Management.	yes
Escalate Privileges with (SSH)	Use a privilege escalation method such as su or sudo to use extra privileges when scanning. **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	Required if you wish to escalate privileges.

	sudo (directory) are provided and can be completed to support authentication and privilege escalation through Tenable Vulnerability Management. 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 the Nessus User Guide and the Tenable Vulnerability Management User Guide.	
Escalation account credential ID or identifier (SSH)	If the escalation account has a different username or password from the least privileged user, enter the credential ID or identifier for the escalation account credential here.	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.	

Windows Authentication Method: Kerberos

Option	Default	Description	Required
Username	None	The username on the target system.	yes

Option	Default	Description	Required
Password	None	The user password on the target system.	yes
Key Distribution Center (KDC)	None	The host that supplies the session tickets for the user.	yes
KDC Port	88	Directs Tenable Vulnerability Management to connect to the KDC if it is running on a port other than 88.	no
KDC Transport	TCP	The method by which you want to access the KDC server. **Note:** if you set **KDC Transport** to **UDP**, you may also need to change the port number, because depending on the implementation, the KDC UDP protocol uses either port 88 or 750 by default.	no
Domain	None	The Windows domain that the KDC administers.	yes

Windows Authentication Method: Lieberman RED

Lieberman is a popular enterprise password vault that helps you manage privileged credentials. Tenable Vulnerability Management can get credentials from Lieberman to use in a scan.

Option	Description	Required
Username	The target system's username.	yes
Domain	The domain, if the username is part of a domain.	no
Lieberman host	The Lieberman IP/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*.	yes

Option	Description	Required
Lieberman port	The port on which Lieberman listens.	yes
Lieberman API URL	The URL Tenable Vulnerability Management uses to access Lieberman.	no
Lieberman user	The Lieberman explicit user for authenticating to the Lieberman RED API.	yes
Lieberman password	The password for the Lieberman explicit user.	yes
Lieberman Authenticator	The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman. **Note:** If you use this option, append a domain to the **Lieberman user** option, i.e., *domain\user*.	no
Lieberman Client Certificate	The file that contains the PEM certificate used to communicate with the Lieberman host. **Note:** If you use this option, you do not have to enter information in the **Lieberman user**, **Lieberman password**, and **Lieberman Authenticator** fields.	no
Lieberman Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
Lieberman Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	no
Use SSL	If Lieberman is configured to support SSL through IIS, check for secure communication.	no
Verify SSL	If Lieberman is configured to support SSL through IIS	no

Option	Description	Required
Certificate	and you want to validate the certificate, check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.	
System Name	In the rare case your organization uses one default Lieberman entry for all managed systems, enter the default entry name.	no

Windows Authentication Method: LM Hash

The Lanman authentication method was prevalent on Windows NT and early Windows 2000 server deployments. It is retained for backward compatibility.

Option	Description	Required
Username	The username on the target system.	yes
Hash	The hash you want to use.	yes
Domain	The Windows domain to which the username belongs.	no

Windows Authentication Method: NTLM Hash

The NTLM authentication method, introduced with Windows NT, provided improved security over Lanman authentication. The enhanced version, NTLMv2, is cryptographically more secure than NTLM and is the default authentication method chosen by Tenable Vulnerability Management when attempting to log into a Windows server. NTLMv2 can use SMB Signing.

Option	Description	Required
Username	The username on the target system.	yes
Hash	The hash you want to use.	yes
Domain	The Windows domain to which the username belongs.	no

Windows Authentication Method: Password

Option	Description	Required
Username	The username on the target system.	yes
Password	The user password on the target system.	yes
Domain	The Windows domain to which the username belongs.	no

Windows Authentication Method: QiAnXin

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 Secret ID	The Secret ID for the embedded account application created in QiAnXin PAM.	yes
Domain	The domain to which the username belongs.	no
Username	The username to log in to the hosts you want to scan.	yes
Host IP	Specify the host IP of the asset containing the account to use. If not specified, the scan target IP is used.	no
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	no

Option	Description	Required
	• **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	
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 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	no

Option	Description	Required
	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

Windows Authentication Method: Thycotic Secret Server

Option	Description	Required
Username	The username to authenticate via SSH to the system.	yes
Domain	The domain to which the username belongs.	no
Thycotic Secret Name	The value of the secret on the Thycotic server. The secret is labeled **Secret Name** on the Thycotic server.	yes
Thycotic Secret Server URL	The transfer method, target, and target directory for the scanner. You can find this value on the Thycotic server in **Admin** > **Configuration** > **Application Settings** > **Secret Server URL**. For example, consider the following address: **`https://pw.mydomain.com/SecretServer/`**. • **`https`** indicates an ssl connection. • **`pw.mydomain.com`** is the target address. • **`/SecretServer/`** is the root directory.	yes
Thycotic Login Name	The username to authenticate to the Thycotic server.	yes

Thycotic Password	The password to authenticate to the Thycotic server.	yes
Thycotic Organization	The organization you want to query. You can use this value for cloud instances of Thycotic.	no
Thycotic Domain	The domain of the Thycotic server.	no
Verify SSL Certificate	Whether you want to verify if the SSL Certificate on the server is signed by a trusted CA.	no

Windows Authentication Method: BeyondTrust

Option	Description	Required
Username	The username to log in to the hosts you want to scan.	yes
Domain	The domain of the username, which is recommended if using domain-linked accounts (managed accounts of a domain that are linked to a managed system).	no
BeyondTrust host	The BeyondTrust IP address or DNS address.	yes
BeyondTrust port	The port on which BeyondTrust listens.	yes
BeyondTrust API user	The API user provided by BeyondTrust.	yes
BeyondTrust API key	The API key provided by BeyondTrust.	yes
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 Vulnerability Management scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in	yes

	BeyondTrust so that password changes do not disrupt your Tenable Vulnerability Management scans. If BeyondTrust changes a password during a scan, the scan fails.	
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, usually noted as the domain name of the target.	yes
Use SSL	When enabled, Tenable Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in BeyondTrust before enabling this option. **Caution:** If you do not enable this option the traffic that is sent is http and will not be accepted by the Beyond Trust server.	no
Verify SSL certificate	When enabled, Tenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in BeyondTrust before enabling this option.	no

Scan-wide Credential Type Settings for Windows

These settings apply to all Windows-type credentials in the current scan. You can edit these settings in any instance of the credential type in the current scan; your changes automatically apply to the other credentials of that type in the scan.

Option	Default	Description
Never send credentials in the clear	Enabled	By default, for security reasons, this option is enabled.
Do not use NTLMv1 authentication	Enabled	If the **Do not use NTLMv1 authentication** option is disabled, then it is theoretically possible to trick Tenable Vulnerability Management into attempting to log into a Windows server with domain credentials via the NTLM version 1 protocol. This provides the remote attacker with the ability to use a hash obtained from Tenable Vulnerability Management. This hash can be potentially cracked to reveal a username or password. It may also be used to log into other servers directly. Force Tenable Vulnerability Management to use NTLMv2 by enabling the **Only use NTLMv2** setting at scan time. This prevents a hostile Windows server from using NTLM and receiving a hash. Because NTLMv1 is an insecure protocol, this option is enabled by default.
Start the Remote Registry service during the scan	Disabled	This option tells Tenable Vulnerability Management to start the Remote Registry service on computers being scanned if it is not running. This service must be running in order for Tenable Vulnerability Management to execute some Windows local check plugins.
Enable administrative shares during the scan	Disabled	This option allows Tenable Vulnerability Management to access certain registry entries that can be read with administrator privileges.
Start the Server	Disabled	When enabled, the scanner temporarily enables the

Option	Default	Description
service during the scan		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.

Windows Authentication Method: Centrify

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 Vulnerability Management 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 Vulnerability Management uses *centrify*.
Authentication URL	(Required) The URL Tenable Vulnerability Management uses to access Centrify. By default, Tenable Vulnerability Management uses */Security*.
Password Query URL	(Required) The URL Tenable Vulnerability Management uses to query the passwords in Centrify. By default, Tenable Security Center uses */RedRock*.

Password Engine URL	(Required) The URL Tenable Vulnerability Management uses to access the passwords in Centrify. By default, Tenable Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.

Windows Authentication Method: Arcon

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.
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	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a

Credentials	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.

Windows Authentication Considerations

Regarding the authentication methods:

- Tenable Vulnerability Management automatically uses SMB signing if the remote Windows server requires it. SMB signing is a cryptographic checksum applied to all SMB traffic to and from a Windows server. Many system administrators enable this feature on their servers to ensure that remote users are 100% authenticated and part of a domain. In addition, make sure you enforce a policy that mandates the use of strong passwords that cannot be easily broken via dictionary attacks from tools like John the Ripper and L0phtCrack. There have been many different types of attacks against Windows security to illicit hashes from computers for re-use in attacking servers. SMB Signing adds a layer of security to prevent these man-in-the-middle attacks.
- The SPNEGO (Simple and Protected Negotiate) protocol provides Single Sign On (SSO) capability from a Windows client to a variety of protected resources via the users' Windows login credentials. Tenable Vulnerability Management supports use of SPNEGO Scans and Policies: Scans 54 of 151 with either NTLMSSP with LMv2 authentication or Kerberos and RC4 encryption. SPNEGO authentication happens through NTLM or Kerberos authentication; nothing needs to be set in the Tenable Vulnerability Management scan configuration.
- If an extended security scheme (such as Kerberos or SPNEGO) is not supported or fails, Tenable Vulnerability Management attempts to log in via NTLMSSP/LMv2 authentication. If that fails, Tenable Vulnerability Management then attempts to log in using NTLM authentication.

- Tenable Vulnerability Management also supports the use of Kerberos authentication in a Windows domain. To configure this, the IP address of the Kerberos Domain Controller (actually, the IP address of the Windows Active Directory Server) must be provided.

Server Message Block (SMB) is a file-sharing protocol that allows computers to share information across the network. Providing this information to Tenable Vulnerability Management allows it to find local information from a remote Windows host. For example, using credentials enables Tenable Vulnerability Management to determine if important security patches have been applied. It is not necessary to modify other SMB parameters from default settings.

The SMB domain field is optional and Tenable Vulnerability Management is able to log on with domain credentials without this field. The username, password, and optional domain refer to an account that the target machine is aware of. For example, given a username of joesmith and a password of my4x4mpl3, a Windows server first looks for this username in the local system's list of users, and then determines if it is part of a domain.

Regardless of credentials used, Tenable Vulnerability Management always attempts to log into a Windows server with the following combinations:

- Administrator without a password
- A random username and password to test Guest accounts
- No username or password to test null sessions

The actual domain name is only required if an account name is different on the domain from that on the computer. It is entirely possible to have an Administrator account on a Windows server and within the domain. In this case, to log on to the local server, the username of Administrator is used with the password of that account. To log on to the domain, the Administrator username is also used, but with the domain password and the name of the domain.

When multiple SMB accounts are configured, Tenable Vulnerability Management attempts to log in with the supplied credentials sequentially. Once Tenable Vulnerability Management is able to authenticate with a set of credentials, it checks subsequent credentials supplied, but only uses them if administrative privileges are granted when previous accounts provided user access.

Some versions of Windows allow you to create a new account and designate it as an administrator. These accounts are not always suitable for performing credentialed scans. Tenable recommends that the original administrative account, named Administrator be used for credentialed scanning to ensure full access is permitted. On some versions of Windows, this account may be hidden. To

unhide the real administrator account, open a DOS prompt with administrative privileges and run the following command:

```
C:\> net user administrator /active:yes
```

If an SMB account is created with limited administrator privileges, Tenable Vulnerability Management can easily and securely scan multiple domains. Tenable recommends that network administrators create specific domain accounts to facilitate testing. Tenable Vulnerability Management includes a variety of security checks for Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 that are more accurate if a domain account is provided. Tenable Vulnerability Management does attempt to try several checks in most cases if no account is provided.

Note: The Windows Remote Registry service allows remote computers with credentials to access the registry of the computer being audited. If the service is not running, reading keys and values from the registry is not possible, even with full credentials. This service must be started for a Tenable Vulnerability Management credentialed scan to audit a system fully using credentials.

For more information, see the Tenable blog post Dynamic Remote Registry Auditing - Now you see it, now you don't!

Credentialed scans on Windows systems require using a full administrator level account. Several bulletins and software updates by Microsoft have made reading the registry to determine software patch level unreliable without administrator privileges, but not all of them. Tenable Vulnerability Management plugins check that the provided credentials have full administrative access to ensure the plugins execute properly. For example, full administrative access is required to perform direct reading of the file system. This allows Tenable Vulnerability Management to attach to a computer and perform direct file analysis to determine the true patch level of the systems being evaluated.

Privilege Escalation

You can add privilege escalation while creating a credentialed scan if the scan uses the following authentication methods found in the **Elevate Privileges With** portion of the **Settings** tab for your selected **Authentication Method**.

Authentication Methods that Support Escalation	Supported Escalation Methods

Arcon certificate CyberArk Kerberos password public key Thycotic Secret Server	.k5login Cisco 'enable' dzdo pbrun su su+sudo sudo

The tables below describe the additional credential options you must configure for 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/.

Privilege Escalation Options for Arcon

Option	Escalation Type	Description	Required
Escalation Account Name	.k5login dzdo pbrun su su+sudo sudo	The username for the account with elevated privileges.	yes
Escalation Username	.k5login Cisco 'enable' dzdo pbrun	The username for the account with elevated privileges.	yes

	su su+sudo sudo Checkpoint Gaia 'expert'		
Escalation password	dzdo su su+sudo	The password for the account with elevated privileges.	yes
Location of dzdo (directory)	dzdo	The directory path for the dzdo command.	no
Location of pbrun (directory)	pbrun	The directory path for the pbrun command.	no
Location of su (directory)	su	The directory path for the su command.	no
Location of su and sudo (directory)	su+sudo	The directory path for the su and sudo commands.	no
Location sudo (directory)	sudo	The directory path for the sudo command.	no
SSH user password	pbrun	The password for the account with elevated	yes

		privileges.	
su login	su	The username for the account with su privileges.	yes
su user	su+sudo	The username for the account with su privileges.	yes
sudo password	sudo	The password for the account with sudo privileges.	yes
sudo user	su+sudo sudo	The username for the account with sudo privileges.	yes

Privilege Escalation Options for Certificate, Kerberos, Password, and Public Key

Option	Escalation Type	Description	Required
Enable password	Cisco 'enable'	The password to run the 'enable' utility on a Cisco device.	yes
Escalation account	.k5login pbrun dzdo	The username for the account with elevated privileges.	yes
Escalation password	dzdo pbrun su	The password for the account with elevated privileges.	yes

	su+sudo		
Location of dzdo (directory)	dzdo	The directory path for the dzdo command.	no
Location of pbrun (directory)	pbrun	The directory path for the pbrun command.	no
Location of su (directory)	su	The directory path for the su command.	no
Location of su and sudo (directory)	su+sudo	The directory path for the su and sudo commands.	no
Location sudo (directory)	sudo	The directory path for the sudo command.	no
SSH user password	pbrun	The password for the account with elevated privileges.	yes
su login	su	The username for the account with su privileges.	yes
su user	su+sudo	The username for the account with su privileges.	yes
sudo password	sudo	The password for the account with sudo privileges.	yes
sudo user	su+sudo sudo	The username for the account with sudo privileges.	yes

Privilege Escalation Options for CyberArk

Option	Escalation Type	Description	Required
CyberArk Account Details Name	.k5login Cisco 'enable' dzdo	The method with which your CyberArk Escalation credentials are retrieved. Can be Username, Identifier, Address, or	yes

	pbrun su su+sudo sudo	Parameters.	
Escalation account	dzdo	The username for the account with elevated privileges.	yes
Location of dzdo (directory)	dzdo	The directory path for the dzdo command.	no
Location of pbrun (directory)	pbrun	The directory path for the pbrun command.	no
Location of su (directory)	su	The directory path for the su command.	no
Location of su and sudo (directory)	su+sudo	The directory path for the su and sudo commands.	no
Location sudo (directory)	sudo	The directory path for the sudo command.	no
su login	su	The username for the account with su privileges.	yes
su user	su+sudo	The username for the account with su privileges.	yes
sudo user	su+sudo sudo	The username for the account with sudo privileges.	yes

Privilege Escalation Options for Thycotic Secret Server

Option	Escalation Type	Description	Required

Thycotic Escalation Account	.k5login Cisco 'enable' dzdo pbrun su su+sudo sudo	The name parameter for the Thycotic account with elevated privileges.	yes
Location of dzdo (directory)	dzdo	The directory path for the dzdo command.	no
Location of pbrun (directory)	pbrun	The directory path for the pbrun command.	no
Location of su (directory)	su	The directory path for the su command.	no
Location of su and sudo (directory)	su+sudo	The directory path for the su and sudo commands.	no
Location sudo (directory)	sudo	The directory path for the sudo command.	no
su user	su+sudo	The username for the account with su privileges.	yes

Miscellaneous

Tenable Vulnerability Management supports the additional authentication methods described below.

Note: Some credential types may not be available for configuration, depending on the scan template you selected. Additionally, some credential types only allow you to specify one set of credentials for the given type.

ADSI

ADSI requires the domain controller information, domain, and domain admin and password.

ADSI allows Tenable Vulnerability Management to query an ActiveSync server to determine if any Android or iOS-based devices are connected. Using the credentials and server information, Tenable Vulnerability Management authenticates to the domain controller (not the Exchange server) to directly query it for device information. This feature does not require any ports be specified in the scan configuration. These settings are required for mobile device scanning.

Option	Description
Domain Controller	(Required) Name of the domain controller for ActiveSync
Domain	(Required) Name of the Windows domain for ActiveSync
Domain Admin	(Required) Domain admin's username
Domain Password	(Required) Domain admin's password

Tenable Vulnerability Management supports obtaining the mobile information from Exchange Server 2010 and 2013 only; Tenable Vulnerability Management cannot retrieve information from Exchange Server 2007.

Cisco Meraki

Option	Description	Required
Cisco Meraki API Host	Hostname or IP address to the Cisco Meraki Dashboard API host.	Yes
Cisco Meraki API Port	Port of the Cisco Meraki Dashboard API. (Default 443)	Yes
Cisco Meraki API Key	API Key for authentication to the Cisco Meraki API.	Yes
CIsco Meraki Organization Name	Enter a single organization per credential.	Yes
CIsco Meraki Network Name	Enter one or more comma-separated network names.	No
Cisco Meraki	Enter one or more comma-separated product types. Valid	No

Option	Description	Required
Product Type	product types: **appliance**, **camera**, **cellularGateway**, **secureConnect**, **sensor**, **switch**, **systemManager**, **wireless**, and **wirelessController**.	
Cisco Meraki Tag	Enter one or more comma-separated tags used to filter device searches within an organization.	No
Cisco Meraki Device Name	Enter a single Cisco Meraki device name. (e.g., "Meraki MS120-8")	No
Cisco Meraki Device Model	Enter one or more comma-separated Cisco Meraki device models. (e.g., "MS120-8")	No
Device Serial Number	Enter one or more comma-separated device serial numbers.	No
Device MAC Address	Enter one or more comma-separated device MAC Addresses.	No
Discover Devices	Adds any discovered Cisco Meraki devices to the targets to scan. (Default Off)	No
HTTPS	When set to On, the field expands with the option to enable **Verification of SSL Client Certificate if a Custom CA is configured**. (Default Off)	No

F5

Option	Description
Username	(Required) Username for a scanning account on the F5 target.
Password	(Required) Password associated with the scanning account.
Port	Port to use when connecting to the F5 target.
HTTPS	When enabled, connect using secure communication (HTTPS). When disabled, connect using standard HTTP.
Verify SSL	Verify that the SSL certificate is valid. If you are using a self-signed certificate,

Certificate	disable this setting.

IBM iSeries

Note: This credential type is only available in the Advanced Network Scan template.

Option	Description
Username	(Required) An iSeries username.
Password	(Required) An iSeries password.

Netapp API

Note: This credential type is only available in the Advanced Network Scan template.

Option	Description
Username	(Required) Username for an account on the Netapp system that has HTTPS access.
Password	(Required) Password associated with the account.
vFiler	If this setting is blank, the scan audits for all discovered Netapp virtual filers (vFilers) on target systems. To limit the audit to a single vFiler, type the name of the vFiler.
Port	Ports to scan on target systems. Type a comma-separated list of port numbers.

Nutanix Prism

Note: This credential type is only available in the Advanced Network Scan template.

Option	Description	Default
Nutanix Host	(Required) Hostname or IP address of the Nutanix Prism Central host.	-
Nutanix Port	(Required) The TCP port that the Nutanix Prism Central	9440

Option	Description	Default
	host listens on for communications from Tenable.	
Nutanix Prism Central Authentication Method	(Required) The user can choose from a list of authentication methods: • Username and Password (manual entry) • Privileged Access Management (PAM) Integration. Use a specific PAM to gather vCenter API Authentication Credentials from the available list.	Username and Password
Discover Hosts	When enabled, Tenable adds all discovered Nutanix hosts to the list of scan targets.	enabled
Discover Virtual Machines	When enabled. Tenable 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

OpenStack

Note: This credential type is only available in the Advanced Network Scan template.

Option	Description
Username	(Required) Username for an account on the OpenStack deployment.

Password	(Required) Password associated with the account.
Tenant Name for Authentication	(Required) Name of the specific tenant the scan uses to authenticate. A tenant (also known as a project) is a group of resources that can be controlled by users in the tenant.
Port	(Required) Port that the scanner uses to connect to OpenStack.
HTTPS	When enabled, connect using secure communication (HTTPS). When disabled, connect using standard HTTP.
Verify SSL Certificate	Verify that the SSL certificate is valid. If you are using a self-signed certificate, disable this setting.

Palo Alto Networks PAN-OS

Option	Description
Username	(Required) The PAN-OS username.
Password	(Required) The Pan-OS password.
Port	(Required) The management port number.
HTTPS	Whether Tenable Vulnerability Management authenticates over an encrypted (HTTPS) or an unencrypted (HTTP) connection.
Verify SSL Certificate	Verify that the SSL certificate is valid. If the target is using a self-signed certificate, disable this setting.

Red Hat Enterprise Virtualization (RHEV)

Note: This credential type is only available in the Advanced Network Scan template.

Option	Description
Username	(Required) Username to login to the RHEV server.
Password	(Required) Username to the password to login to the RHEV server.
Port	Port to connect to the RHEV server.

Option	Description
Verify SSL Certificate	Verify that the SSL certificate for the RHEV server is valid.

VMware ESX SOAP API

Access to VMware servers is available through its native SOAP API. VMware ESX SOAP API allows you to access the ESX and ESXi servers via username and password. Additionally, you have the option of not enabling SSL certificate verification.

Note: This credential type is only available in the Advanced Network Scan template.

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
Do not verify SSL Certificate	Do not validate the SSL certificate for the ESXi server.	disabled

VMware vCenter SOAP API

VMware vCenter SOAP API allows you to access vCenter. If available, the vCenter REST API is used to collect data in addition to the SOAP API.

For more information on configuring VMWare vCenter SOAP API, see Configure vSphere Scanning.

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
vCenter Host	(Required) Name of the vCenter host.
vCenter Port	Port to access the vCenter host.
Username	(Required) Username to login to the vCenter server.
Password	(Required) Username to the password to login to the vCenter server.
HTTPS	Connect to the vCenter via SSL.
Verify SSL Certificate	Verify that the SSL certificate for the ESXi server is valid.

VMware vCenter Auto Discovery

Note: This credential type is only available in the Advanced Network Scan template.

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.	-

Option	Description	Default
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
Auto Discover Managed VMware ESXi Hosts	This option adds any discovered VMware ESXi hypervisor hosts to the scan targets you include in your scan.	disabled
Auto Discover Managed VMware ESXi Virtual Machines	This option adds any discovered VMware ESXi hypervisor virtual machines to the scan targets you include in your scan.	disabled

X.509

Note: This credential type is only available in the Advanced Network Scan template.

Option	Description
Client certificate	(Required) The client certificate.
Client key	(Required) The client private key.
Password for key	(Required) The passphrase for the key.
CA certificate to trust	(Required) The trusted Certificate Authority's (CA) digital certificate.

Mobile

Note: Some credential types may not be available for configuration, depending on the scan template you selected.

ActiveSync

Option	Default	Description
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 Vulnerability Management uses to authenticate to ActiveSync.
Domain Password	--	The password for the domain administrator user.
Scanner	--	Specifies which scanner Tenable Vulnerability Management uses when scanning the server. Tenable Vulnerability Management can only use one scanner to add data to a mobile repository.
Update Schedule	Every day at 12:30 -04:00	Specifies when Tenable Vulnerability Management scans the server to update the mobile repository. On each scan, Tenable Vulnerability Management removes the current data in the repository and replaces it with data from the latest scan.

AirWatch

Setting	Default Value	Description	Required
AirWatch Environment API URL	-	The Workspace ONE API url endpoint. (For example, https://xxx.awmdm.com/api)	yes

Port	443	The TCP port that AirWatch listens on for communications from Tenable.	yes
Username	-	The username for the AirWatch user account Tenable uses to authenticate to Workspace One's API.	yes
Password	-	The password for the AirWatch user.	yes
API Key	-	The API key for the VMware Workspace ONE API.	yes
HTTPS	Enabled	Enable for Tenable Vulnerability Management to authenticate over an encrypted (HTTPS) or an unencrypted (HTTP) connection.	no
Verify SSL Certificate	Enabled	Enable for Tenable Vulnerability Management to verify if the SSL Certificate on the server is signed by a trusted CA.	no

Blackberry UEM

Option	Description
Hostname	The server URL to authenticate with Blackberry UEM.
Port	The port to use to authenticate with Blackberry UEM.
Tenant	The SRP ID in Blackberry UEM. **Note:** To locate the SRP ID in Blackberry UEM: 1. In the Blackberry UEM top navigation bar, click the **Help** drop-down. 2. Click **About Blackberry UEM.** An information window containing the SRP ID appears. 3. Copy the SRP ID.

Domain	The domain name for Blackberry UEM.
Username	The username for the account you want Tenable Vulnerability Management to use to authenticate to Blackberry UEM.
Password	The password for the account you want Tenable Vulnerability Management to use to authenticate to Blackberry UEM.
HTTPS	When enabled, Tenable Vulnerability Management uses an encrypted connection to authenticate with Blackberry UEM.
Verify SSL Certificate	When enabled, Tenable Vulnerability Management verifies that the SSL Certificate on the server is signed by a trusted CA.

> Intune

Option	Description
Tenant	The Microsoft Azure Directory (tenant) ID visible in your App registration.
Client	The Microsoft Azure Application (client) ID generated during your App registration.
Secret	The secret key generated when you created your client secret key in Microsoft Azure.
Username	The username for the account you want Tenable Vulnerability Management to use to authenticate to Intune.
Password	The password for the account you want Tenable Vulnerability Management to use to authenticate to Intune.

MaaS360

Setting	Default Value	Description	Required
Username	-	The username to authenticate.	yes
Password	-	The password to authenticate.	yes

Root URL	-	The server URL to authenticate with MaaS360.	yes
Platform ID	-	The Platform ID provided for MaaS360.	yes
Billing ID	-	The Billing ID provided for MaaS360.	yes
App ID	-	The App ID provided for MaaS360.	yes
App Version	-	The App Version of MaaS360.	yes
App access key	-	The App Access Key provided for MaaS360.	yes
Collect All Device Data	On	When enabled, the scan collects all data types. When disabled, the scan collects one or more types of data to decrease the scan time. When disabled, choose one or more of the following collection options: • **Collect Device Summary** • **Collect Device Applications** • **Collect Device Compliance** • **Collect Device Policies**	no

MobileIron

Setting	Default Value	Description	Required
VSP Admin Portal URL	-	The server URL Tenable Vulnerability Management uses to authenticate with the MobileIron Admin Portal.	yes
VSP Admin Portal Port	443	The port Tenable Vulnerability Management uses to authenticate with the	no

		MobileIron Admin Portal.	
Port	443	The port Tenable Vulnerability Management uses to authenticate with the MobileIron System Manager.	yes
Username	-	The username to authenticate.	yes
Password	-	The password to authenticate.	yes
HTTPS	Enabled	Whether Tenable Vulnerability Management authenticates over an encrypted (HTTPS) or an unencrypted (HTTP) connection.	no
Verify SSL Certificate	Enabled	Whether Tenable Vulnerability Management verifies if the SSL Certificate on the server is signed by a trusted CA.	no

Workspace ONE

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	yes

		Workspace ONE's API.	
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 Vulnerability Management to authenticate over an encrypted (HTTPS) or an unencrypted (HTTP) connection.	no
Verify SSL Certificate	Enabled	Enable for Tenable Vulnerability Management 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	(Enabled if Collect All Device Data is set to "No") Collects applications installed on mobile devices.	no

Patch Management

Note: Some credential types may not be available for configuration, depending on the scan template you selected.

Tenable Vulnerability Management can leverage credentials for patch management systems to perform patch auditing on systems for which credentials may not be available.

Note: Patch management integration is not available on Tenable Nessus Essentials, Tenable Nessus Professional, Tenable Nessus Expert, or managed Tenable Nessus scanners.

Tenable Vulnerability Management supports:

Tenable Nessus Manager 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 the **Credentials** section while creating a scan, as described in Create a Vulnerability Management Scan.

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 Vulnerability Management is able to connect to the target system, it performs checks on that system and ignores the patch management system output.

Note: The data returned to Tenable Vulnerability Management 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.

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 Vulnerability Management is able to connect to the target system, it performs checks on that system and ignores the patch management system output.

Note: The data returned to Tenable Vulnerability Management 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 Vulnerability Management for patch management tools, Tenable Vulnerability Management uses all of them.

If you provide credentials for a host and for one or more patch management systems, Tenable Vulnerability Management 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.

If you provide multiple sets of credentials to Tenable Vulnerability Management for patch management tools, Tenable Vulnerability Management uses all of them.

If you provide credentials for a host and for one or more patch management systems, Tenable Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management user interface.

Tenable Vulnerability Management 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 Vulnerability Management.	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 Vulnerability Management uses to perform checks on the target system.	R1
K1000 Database Password	(Required) The password for the KACE K1000 user.	-

HCL Tivoli Endpoint Manager (BigFix)

HCL Bigfix is available to manage the distribution of updates and hotfixes for desktop systems.Tenable Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management.	-
Web Reports Username	(Required) The username for the HCL Bigfix Web Reports administrator account that Tenable Vulnerability Management 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 (HTTPS). When disabled, Tenable connects using standard HTTP.	Enabled

Option	Description	Default
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 Vulnerability Management.

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 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 Vulnerability Management 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 Vulnerability Management 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, configured sensors Tenable Vulnerability Management must connect to the SCCM server via WMI and HTTPS.

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 Vulnerability Management 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.	-

Microsoft 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 Vulnerability Management can query WSUS to verify whether or not patches are installed on systems managed by WSUS and display the patch information through the Tenable Vulnerability Management 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.	-
Port	(Required) The TCP port that Microsoft WSUS listens on for communications from Tenable Vulnerability Management.	8530
Username	(Required) The username for the WSUS administrator	-

Option	Description	Default
	account that Tenable Vulnerability Management 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 Vulnerability Management 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 name.	-
Port	(Required) The TCP port that Red Hat Satellite 6 listens on for communications from Tenable Vulnerability	443

Option	Description	Default
	Management.	
Username	(Required) The username for the Red Hat Satellite 6 account that Tenable Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management user interface.

Tenable Vulnerability Management 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 Vulnerability Management 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.	-
Database Port	(Required) The TCP port that Altiris listens on for	5690

Credential	Description	Default
	communications from Tenable Vulnerability Management.	
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 Vulnerability Management 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.	Disabled

Plaintext Authentication

Caution: Using plaintext credentials is not recommended. Use encrypted authentication methods when possible.

If a secure method of performing credentialed checks is not available, you can configure Tenable Vulnerability Management to perform checks over unsecure protocols using the **Plaintext Authentication** settings.

Note: Some credential types may not be available for configuration, depending on the scan template you selected.

FTP

Setting	Default Value	Description	Required?

Username	-	Login user’s name.	yes
Password	-	Password of the user specified.	yes

HTTP

Setting	Default	Description	Required
Authentication method	HTTP Login Form	The authentication method. Supported values are: • Automatic authentication • Basic/Digest authentication • HTTP login form – Controls where authenticated testing of a custom web-based application begins. • HTTP cookies import – Facilitates web application testing by using cookies imported from another piece of software (e.g., web browser, web proxy, etc.). when attempting to access a web application.	yes
Method: Automatic Authentication			
Username	-	Login user's name.	yes
Password	-	Password of the user specified.	yes
Method: Basic/Digest authentication			
Username	-	Login user's name.	yes
Password	-	Password of the user specified.	yes
Method: HTTP login form			
Username	-	Login user’s name.	yes

Setting	Default	Description	Required
Password	-	Password of the user specified.	yes
Login page	-	The absolute path to the login page of the application, e.g., /login.html.	yes
Login submission page	-	The action parameter for the form method. For example, the login form for <form method="POST" name="auth_ form" action="/login.php"> would be /login.php.	yes
Login parameters	-	Specify the authentication parameters (e.g., login=%USER%&password=%PASS%). If the keywords %USER% and %PASS% are used, the keywords will be substituted with values supplied on the Login configurations drop-down menu. This field can be used to provide more than two parameters if required (e.g., a group name or some other piece of information is required for the authentication process).	yes
Check authentication on page	-	The absolute path of a protected web page that requires authentication, to better assist Tenable Vulnerability Management in determining authentication status, e.g., /admin.html.	yes
Regex to verify successful authentication	-	A regex pattern to look for on the login page. Simply receiving a 200 response code is not always sufficient to determine session state. Tenable Vulnerability Management can attempt to match a	yes

Setting	Default	Description	Required
		given string such as Authentication successful!	
Method: HTTP cookies import			
Cookies file	-	Upload a cookie file. The file must be in Netscape format.	yes
All methods: Scan-wide Credential Type Settings			
Login method	POST	Specify if the login action is performed via a GET or POST request.	yes
Re-authenticate delay (seconds)	0	The time delay between authentication attempts. Setting a time delay is useful to avoid triggering brute force lockout mechanisms.	yes
Follow 30x redirections (# of levels)	0	If a 30x redirect code is received from a web server, this setting directs Tenable Vulnerability Management to follow the link provided or not.	yes
Invert authenticated regex	Disabled	A regex pattern to look for on the login page, that if found, tells Tenable Vulnerability Management that authentication was not successful (e.g., Authentication failed!).	no
Use authenticated regex on HTTP headers	Disabled	Rather than search the body of a response, Tenable Vulnerability Management can search the HTTP response headers for a given regex pattern to better determine authentication state.	no
Case insensitive	Disabled	The regex searches are case sensitive	no

Setting	Default	Description	Required
authenticated regex		by default. This instructs Tenable Vulnerability Management to ignore case.	

IMAP

Setting	Default Value	Description	Required?
Username	-	Login user's name.	yes
Password	-	Password of the user specified.	yes

IPMI

Setting	Default Value	Description	Required?
Username	-	Login user's name.	yes
Password	-	Password of the user specified.	yes

NNTP

Setting	Default Value	Description	Required?
Username	-	Login user's name.	yes
Password	-	Password of the user specified.	yes

POP2

Setting	Default Value	Description	Required?
Username	-	Login user's name.	yes
Password	-	Password of the user specified.	yes

POP3

Setting	Default Value	Description	Required?
Username	-	Login user's name.	yes
Password	-	Password of the user specified.	yes

SNMPv1/v2c

SNMPv1/v2c configuration allows you to use community strings for authentication to network devices. You can configure up to four SNMP community strings.

Setting	Default Value	Description	Required
Community string	public	The community string Tenable Vulnerability Management uses to authenticate on the host device.	yes
Scan-wide Credential Type Settings			
UDP Port	161	Ports where Tenable Vulnerability Management attempts to authenticate on the host device.	no
Additional UDP port #1	161		no
Additional UDP port #2	161		no
Additional UDP port #3	161		no

telnet/rsh/rexec

Tenable Vulnerability Management performs patch auditing on non-Windows targets only.

Setting	Default Value	Description	Required
Username	-	Login user's name.	yes

Password	-	Password of the user specified.	yes
Scan-wide Credential Type Settings			
Perform patch audits over telnet	Disabled	Tenable Vulnerability Management uses telnet to connect to the host device for patch audits.	no
Perform patch audits over rsh	Disabled	Tenable Vulnerability Management uses rsh to connect to the host device for patch audits.	no
Perform patch audits over rexec	Disabled	Tenable Vulnerability Management uses rexec to connect to the host device for patch audits.	no

Compliance in Tenable Vulnerability Management Scans

Note: If a scan is based on a user-defined template, you cannot configure **Compliance** settings in the scan. You can only modify these settings in the related user-defined template.

Tenable Vulnerability Management can perform vulnerability scans of network services as well as log in to servers to discover any missing patches.

However, a lack of vulnerabilities does not mean the servers are configured correctly or are “compliant” with a particular standard.

You can use Tenable Vulnerability Management to perform vulnerability scans and compliance audits to obtain all of this data at one time. If you know how a server is configured, how it is patched, and what vulnerabilities are present, you can determine measures to mitigate risk.

At a higher level, if this information is aggregated for an entire network or asset class, security and risk can be analyzed globally. This allows auditors and network managers to spot trends in non-compliant systems and adjust controls to fix these on a larger scale.

When configuring a scan or policy, you can include one or more compliance checks, also known as audits. Each compliance check requires specific credentials.

Some compliance checks are preconfigured by Tenable, but you can also create and upload custom audits.

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.

Compliance Check	Required Credentials
Adtran AOS	SSH
Alcatel TiMOS	SSH
Amazon AWS	Amazon AWS
Arista EOS	SSH
ArubaOS	SSH
Blue Coat ProxySG	SSH
Brocade FabricOS	SSH
Check Point GAiA	SSH
Cisco ACI	SSH
Cisco Firepower	SSH
Cisco IOS	SSH
Cisco Viptela	SSH
Citrix Application Delivery	Citrix NITRO API
Database	Database
Extreme ExtremeXOS	SSH
F5	F5
FireEye	SSH
Fortigate FortiOS	SSH

Compliance Check	Required Credentials
Generic SSH	SSH
Google Cloud Platform	Google Cloud Platform
HP ProCurve	SSH
Huawei VRP	SSH
IBM DB2 DB	Database
IBM iSeries	IBM iSeries or SSH
Juniper Junos	SSH
Microsoft Azure	Microsoft Azure
Mobile Device Manager	AirWatch or Mobileiron
MongoDB	MongoDB
Microsoft SQL DB	Database
MySQL DB	Database
NetApp API	NetApp API
NetApp Data ONTAP	SSH
OpenShift Container Platform	OpenShift Container Platform
OpenStack	OpenStack
Oracle DB	Database
Palo Alto Networks PAN-OS	PAN-OS
PostgreSQL DB	Database
Rackspace	Rackspace
RHEV	RHEV
Salesforce.com	Salesforce SOAP API

Compliance Check	Required Credentials
Snowflake	Snowflake API
SonicWALL SonicOS	SSH
Splunk	Splunk API
Sybase DB	Database
Unix	SSH
Unix File Contents	SSH
VMware vCenter/vSphere	VMware vCenter API or VMware ESX SOAP API
WatchGuard	SSH
Windows	Windows
Windows File Contents	Windows
Zoom	Zoom
ZTE ROSNG	SSH

Note: Plugins sometimes produce errors that fall into one of the following scenarios:

- Something should be notified as a concern, but not at the risk of impacting the results of a large scan
- Something happened where the plugin was unable to report issues

In either one of these scenarios, a compliance result with the name `Compliance Plugin Errors: <plugin name>` is posted as a WARNING. The output of the compliance results identifies the issue that should be reviewed. These results are posted by the plugin 214001 Compliance Status.

SCAP Settings in Tenable Vulnerability Management Scans

Security Content Automation Protocol (SCAP) is an open standard that enables automated management of vulnerabilities and policy compliance for an organization. SCAP relies on multiple open standards and policies, including OVAL, CVE, CVSS, CPE, and FDCC policies.

Tenable Vulnerability Management allows you to add SCAP (and OVAL) compliance checks to your scans. You can only configure **SCAP** settings when you use the **SCAP and OVAL Auditing** scan template.

Caution: SCAP scans in Tenable Vulnerability Management are unverified.

You can select **Linux (SCAP)**, **Linux (OVAL)**, **Windows (SCAP)**, or **Windows (OVAL)**. The following table describes each option's settings:

Setting	Default Value	Description
Linux (SCAP) or **Windows (SCAP)**		
SCAP File	None	A valid zip file that contains full SCAP content. The file contains XCCDF, OVAL, and CPE for versions 1.0 and 1.1, DataStream for version 1.2.
SCAP Version	1.2	The SCAP version that is appropriate for the content in the uploaded SCAP file.
SCAP Data Stream ID	None	(SCAP Version 1.2 only) The `data-stream id` that you copied from the SCAP XML file. Example: `<data-stream id="scap_gov.nist_datastream_USGCB-Windows-10-1.2.3.1.zip">`
SCAP Benchmark ID	None	The `Benchmark id` that you copied from the SCAP XML file. Example: `<xccdf:Benchmark id="xccdf_gov.nist_benchmark_USGCB-Windows-7">`

SCAP Profile ID	None	The `Profile id` that you copied from the SCAP XML file. Example: `<xccdf:Profile id="xccdf_gov.nist_profile_united_states_government_configuration_baseline_version_1.2.3.1">`
OVAL Result Type	Full results w/ system characteristics	The information you want the results file to include. The results file can be one of the following types: **Full results with system characteristics**, **Full results without system characteristics**, or **Thin results**.
Linux (OVAL) or **Windows (OVAL)**		
OVAL definitions file	None	A valid zip file that contains OVAL standalone content.

Configure Plugins in Tenable Vulnerability Management Scans

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Scan Permissions: Can Configure

Required Template Permissions: Can Configure

Note: If a scan is based on a user-defined template, you cannot configure **Plugin** settings in the scan. You can only modify these settings in the related user-defined template.

Note: When Tenable adds new plugins to Tenable Vulnerability Management, the new plugins are automatically enabled if the entire plugin family they belong to is enabled in your scan policy template.

If you create a scan or user-defined template using the Tenable-provided **Advanced Scan** template, you can configure which security checks the scan performs by enabling or disabling plugins individually or by plugin family.

When you create and save a scan or user-defined template, it records all the plugins that are initially selected. When new plugins are received via a plugin update, the plugins are automatically enabled if the family with which the plugins are associated is enabled. If the family has been disabled or partially enabled, new plugins in that family are also automatically disabled.

Caution: The **Denial of Service** family contains some plugins that could cause outages on a network if the **Safe Checks** option is not enabled, in addition to some useful checks that do not cause any harm. The **Denial of Service** family can be used with **Safe Checks** to ensure that any potentially dangerous plugins are not run. However, Tenable recommends that you do not use **Denial of Service** family on a production network except during a maintenance window and when staff are ready to respond to any issues.

To configure plugins for a scan or user-defined template:

1. Do one of the following:
   a. Create or edit a scan.
   b. Create or edit a user-defined template.
2. In the left menu of the scan configuration page, click **Plugins**.

   The **Plugins** page appears. This page contains a table of plugin families.
3. Do one of the following:
   - Filter the plugin families table by various attributes.
   - Search the plugin families table by plugin family name. For more information on searching, see Tables.
4. To enable or disable all the plugins in a plugin family, click the **Status** toggle in row for the plugin family.
   - **On** – The scan includes the security checks associated with the plugin family.
   - **Off** – The scan excludes the security checks associated with the plugin family.

5. To enable or disable specific plugins for an individual plugin family:

    a. In the plugin families table, click the plugin family where you want to edit plugins. The plugin family plane appears.

    b. (Optional) Click an individual plugin to review plugin details (**Synopsis**, **Description**, and **Solution**).

    c. For each plugin you want to enable or disable, select or clear the **Status** checkbox.

    d. Click **Save**.

    The **Plugins** page appears. In the plugin families table, Tenable Vulnerability Management updates the plugin family status as follows:

    - **On** – If you enabled all plugins for the plugin family, the scan includes the security checks associated with the plugin family.
    - **Off** – If you disabled all plugins for the plugin family, the scan excludes the security checks associated with the plugin family.

      > **Tip:** Disabling a plugin family reduces the time and resources required to run the scan.

    - **Mixed** – If you enabled only some of the plugins for the plugin family, the scan includes only the enabled 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 are disabled automatically in the policy.
        - Unlocked – New plugins added to the plugin family via plugin feed updates are enabled automatically in the policy.

    e. Click **Save** to save your changes to the plugin family.

6. Click **Save** to save your changes to the scan or user-defined template.

Tenable Web App Scanning Scan Settings

Scan settings enable you to refine parameters in scans to meet your specific network security needs. The scan settings you can configure vary depending on the Tenable-provided template on which a scan or user-defined template is based.

You can configure these settings in individual scans or in user-defined templates from which you create individual scans.

Tenable Web App Scanning scan settings are organized into the following categories:

- Basic Settings in User-Defined Templates
- Basic Settings in Tenable Web App Scanning Scans
- Scope Settings in Tenable Web App Scanning Scans
- Report Settings in Tenable Web App Scanning Scans
- Assessment Settings in Tenable Web App Scanning Scans
- Advanced Settings in Tenable Web App Scanning Scans
- Credentials in Tenable Web App Scanning Scans
- Plugin Settings in Tenable Web App Scanning Scans

Settings in User-Defined Templates

When configuring settings for user-defined templates, note the following:

- If you configure a setting in a user-defined template, that setting applies to any scans you create based on that user-defined template.
- You base a user-defined template on a Tenable-provided template. Most of the settings are identical to the settings you can configure in an individual scan that uses the same Tenable-provided template.

  However, certain **Basic** settings are unique to creating a user-defined template, and do not appear when configuring an individual scan. For more information, see Basic Settings in User-Defined Templates.
- You can configure certain settings in a user-defined template, but cannot modify those settings in an individual scan based on a user-defined template. These settings include **Discovery**, **Assessment**, **Report**, **Advanced**, **Compliance**, **SCAP**, and **Plugins**. If you want to modify these settings for individual scans, create individual scans based on a Tenable-provided template instead.

- If you configure **Credentials** in a user-defined template, other users can override these settings by adding scan-specific or managed credentials to scans based on the template.

Basic Settings in Tenable Web App Scanning Scans

Configure **settings** to specify basic organizational and security-related aspects of your scan configuration. This includes specifying the name of the scan, one or more targets, whether the scan is scheduled, and who has access to the scan.

You can configure **settings** when you create a scan or user-defined scan template and select any scan type. For more information, see Scan Templates.

> **Tip**: If you want to save your settings configurations and apply them to other scans, you can create and configure a user-defined scan template.

The **Basic** settings include the following sections:

- General
- Pause Window
- Notifications
- User Permissions
- Data Sharing
- Schedule

General

The general settings for a scan.

Setting	Default Value	Description	Required
Name	none	Specifies the name of the scan or template.	Yes
Description	none	Specifies a description of the scan or template.	No
Folder	My Scans	Specifies the folder where the scan appears	Yes

Setting	Default Value	Description	Required
		after being saved.	
Scanner Type	Internal Scanner	Specifies whether a local, internal scanner or a cloud-managed scanner performs the scan, and determines whether the **Scanner** field lists local or cloud-managed scanners to choose from.	Yes
Target	none	Specifies the URL for the target you want to scan, as it appears on your Tenable Web App Scanning license. Regular expressions and wildcards are not allowed. **Caution**: When removing targets from a Tenable Web App Scanning scan (for example, going from two, or more, targets down to one target), the scan must be re-launched before any exports can be delivered. **Note**: If the URL you type in the **Target** box has a different FQDN host from the URL that appears on your license, and your scan runs successfully, the new URL you type counts as an additional asset on your license. **Note**: If you create a user-defined scan template, the target setting is not saved to the template. Type a target each time you create a new scan.	Yes
Scanner	varies	Specifies the scanner that performs the scan.	Yes
Tags	none	Select one or more tags to scan all assets that have any of the specified tags applied.	No

Setting	Default Value	Description	Required
Target	none	Specifies the URL for the target you want to scan, as it appears on your Tenable Web App Scanning license. Regular expressions and wildcards are not allowed. Targets must start with the http:// or https:// protocol identifier. The **Import from file** link opens a file manager window. You can import a target list in TXT format with one target per line. The file must be 1MB or smaller, and each line must be shorter than 4096 characters. After you add targets, you can search and delete targets from the list. You cannot modify targets inline. **Tip:** If you upload a new target list, it replaces any existing targets in the scan. If you have multiple target lists, consolidate them in one file before you upload them to Tenable Web App Scanning. You can add up to 1000 targets to a scan, with the exception of scans that include API targets. API scans support only one target at a time. **Note**: If the URL you type in the **Target** box has a different FQDN host from the URL that appears on your license, and your scan runs successfully, the new URL you type counts as an additional asset on your license. **Note**: If you create a user-defined scan template, the target setting is not saved to	Yes

Setting	Default Value	Description	Required
		the template. Type a target each time you create a new scan.	

Schedule

The schedule settings for the scan.

Note: If you create a user-defined scan template, your schedule settings are not saved to the scan template. Configure the schedule settings each time you create a new scan.

Setting	Default	Description
Schedule	off	A toggle that specifies whether the scan is scheduled. By default, scans are not scheduled. When the **Schedule** toggle is disabled, the other schedule settings remain hidden. Click the toggle to enable the schedule and view the remaining **Schedule** settings:
Frequency	Once	Specifies how often the scan is launched. **Note**: The frequency with which you scan your target(s) depends on several factors (e.g., how often you update your web application, the content your web application contains, etc.). For most web applications, Tenable recommends at least monthly scans. • **Once**: Schedule the scan at a specific time. • **Daily**: Schedule the scan to occur on a daily basis, at a specific time, up to 20 days. • **Weekly**: Schedule the scan to occur on a recurring basis, by time and day of week, up to 20 weeks.

Setting	Default	Description

		• **Monthly**: Schedule the scan to occur every 1-20 months, by:
		  • **Day of Month**: The scan repeats on a specific day of the month at the selected time.
		  • **Week of Month**: The scan repeats monthly on the week you begin the scan. For example, if you select a start date of October 3rd, and that falls on the first week of the month, then the scan repeats the first week of each subsequent month at the selected time.
		
		Note: If you schedule your scan to recur monthly and by time and day of the month, 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 Vulnerability Management cannot run the scan on those days.
		
		• **Yearly**: Schedule the scan to occur every year, by time and day, up to 20 years.

Starts	varies	Specifies the exact date and time at which a scan launches. **Note**: If you schedule an excessive number of scans to run concurrently, you may exhaust the scanning capacity on Tenable Web App Scanning. If necessary, Tenable Web App Scanning staggers concurrent scans to ensure consistent scanning performance. The starting date defaults to the date you create the scan. The starting time is the next hour interval, displayed in 24-hour clock format. For example, if you create your scan on October 31, 2019 at 9:12 PM, the default starting date and time is *10/31/2019* and *22:00*.
Timezone	varies	The time zone of the value set for **Starts**.

Setting	Default	Description
Repeat	Daily	The frequency of the value set for **Schedule**.

Pause Window

Note: Pause Window is not available in the **Quick Scan** template.

Setting	Default	Description
Pause Window	Disabled	The scheduled scan is paused/resumed during the configured time frames. You can manually select days and times, or use the following presets: • **Everyday**: Selects all days of the week to schedule the scan pause/resume. • **Today**: Selects today to schedule the scan pause/resume. • **Working Days**: Selects only working days (MO, TU, WE, TH, FR) to schedule the scan pause/resume. • **Weekend**: Selects only weekend days (SU, SA) to schedule the scan pause/resume. • **Apply to all**: Applies the daily schedule you input to all days of the week. **Note:** • You can only pause a scan that is currently in `Running` state, and only resume a scan that is currently in a `Paused` state. • With default performance settings, pausing may take up to 15 minutes, based upon your current scan window configuration and only if scan is `Running`. Reducing the default performance settings may further impact the time it takes to pause.

Setting	Default	Description
		• If the scan status is other than `Running`, the scan continues without being affected by any pause that you schedule in the scan window configuration, • If the scan status is `Paused`, the scan can only `Resume` with a time you set in the scan window configuration,

Notifications

The notification settings for a scan.

Setting	Default Value	Description
Email Recipient(s)	None	Specifies zero or more email addresses, separated by commas, whitespace, or new lines that are alerted when a scan completes and the results are available.

User Permissions

Share the scan or user-defined scan template with other users by setting permissions for users. For more information on adding or editing user permissions, see Set Scan Permissions.

Permission	Description
No Access	(Default) Users set to this permission cannot interact with the scan in any way.
Can View	Users set to this permission can view the results of the scan.
Can Control	In addition to the tasks allowed by **Can View**, users with this permission can launch and stop a scan. They cannot view or edit the scan configuration or delete the scan.
Can Configure	In addition to the tasks allowed by **Can Control**, users with this permission can view the scan configuration and modify any setting for the scan except scan ownership. They can also delete the scan.

Data Sharing

Setting	Default Value	Description
Scan Results	Show in dashboard	Specifies whether the results of the scan should be kept private or appear on your **Dashboard** and **Findings** pages. When set to **Keep private**, the scan results **Last Seen** dates do not update and you must access the scan directly to view the results.

Scope Settings in Tenable Web App Scanning Scans

Configure **Scope** settings to specify the URLs and file types that you want to include in or exclude from your scan.

You can configure **Scope** settings when you create a scan or user-defined scan template and select the **Overview** or **Scan** template type. For more information, see Scan Templates.

Tip: If you want to save your settings configurations and apply them to other scans, you can create and configure a user-defined scan template.

The **Scope** settings include the following sections:

- Crawl Scripts
- OpenAPI (Swagger) Specification
- Scan Inclusion
- Scan Exclusion

Crawl Scripts

Selenium scripts you want to add to your scan to enable the scanner to analyze pages with complex access logic.

Note: If you add more than one target to your scan, these settings are disabled.

Setting	Description
Add File	Hyperlink that allows you to add one or more recorded Selenium script files to your scan. Your script must be added as a `.side` file.

OpenAPI (Swagger) Specification

The specification (file upload or URL of the file location) for the RESTful API that you want to scan. The file should be OpenAPI Specification (v2 or v3) compliant and represented in either JSON or YAML format.

Setting	Description
File	Selecting this option in the drop-down list enables you to add one or more OpenAPI (v2 or v3) specification files as a file upload. The specification files should be represented in either JSON or YAML format.
URL	Selecting this option in the drop-down list enables you to add one or more OpenAPI (v2 or v3) specification files by entering the URL of the file location. The specification files should be represented in either JSON or YAML format.

Scan Inclusion

The URLs you want the scanner to include, along with how you want the scanner to crawl them.

Note: If you add more than one target to your scan, these settings are disabled.

Setting	Default	Description
List of URLs	none	A list of any URLs you want to ensure the scanner analyzes, in addition to the target URL you specified in the Basic settings. Type each URL as an absolute URL. Type each URL on a separate line.

Setting	Default	Description
		Note: All URLs should have the same domain and wildcards are not allowed.
Specify how the scanner handles URLs found during the application crawl	Crawl all URLs detected	Specifies the limits you want the scanner to adhere to as it crawls URLs. Select one of the following: • **Crawl all URLs detected** – The scanner crawls all URLs and child paths it detects on the target URL's domain host. • **Limit crawling to specified URLs, sibling paths, and child paths** – The scanner crawls the target URLs, sibling, and child paths only. • **Limit crawling to specified URLs and child paths** – The scanner crawls only the target URL and child paths. • **Limit crawling to specified URLs** – The scanner crawls the target URL only. It does not crawl child paths for the target URL.

Scan Exclusion

The attributes of URLs you want the scanner to exclude from your scan.

Setting	Default Value	Description
Regex for Excluded URLs	logout	Text box option in which you can specify a regex pattern that the scanner can look for in URLs to exclude from the scan. You can specify multiple regex patterns separated by new lines.

Setting	Default Value	Description
		Note: The regex values should be values contained within the URL to be excluded. For example, in the URL `http://www.example.com/blog/today.htm`, valid regex values would be `blog` or `today` (not the full URL). Additionally, regex values are case-sensitive.
File Extensions to Exclude	js, css, png, jpeg, gif, pdf, csv, svn-base, svg, jpg, ico, woff, woff2, exe, msi, zip	Text box option in which you can specify the file types you want the scanner to exclude from the scan. Separate each file type with a comma. **Note**: Excluding certain file extensions may be useful as the scanner may not realize something is not a web page and attempt to scan it, as if it actually is a web page. This wastes time and slows down the scan. You can add additional file extensions if you know you use them, and are certain they do not need to be scanned. For example, Tenable includes different image extensions by default: .png, .jpeg, etc.
Decompose Paths	not selected	Check box option that allows you to specify whether you want the scanner to break down each URL identified during the scan into additional URLs, based on directory path level. For example, if you specify *www.example.com/dir1/dir2/dir3* as your target and select **Decompose Paths**, the scanner analyzes each of the following as separate URLs of the target: • www.example.com/dir1/dir2/dir3 • www.example.com/dir1/dir2 • www.example.com/dir1 Select this option to increase the surface coverage of your web application scan.

Setting	Default Value	Description
		Note: Scans that include path decomposition can take longer to complete than scans that do not.
Exclude Binaries	selected	Check box option that allows you to specify whether you want the scanner to audit URLs with responses in binary format. Select this option to increase the surface coverage of your web application scan. **Note**: Scans that include binaries can take longer to complete, because the scanner cannot read the binary responses.

Miscellaneous

Setting	Description
Deduplicate Similar Pages	Checkbox option that allows you to specify whether you want the scanner to ignore pages in situations when similar pages have already been audited.

Assessment Settings in Tenable Web App Scanning Scans

Assessment settings specify which web application elements you want the scanner to audit as it crawls your URLs. You can configure **Assessment** settings when you create a scan or user-defined scan template. For more information, see Scan Templates.

The **Assessment** settings include the following sections:

- Scan Type
- Common and Backup Pages
- Credentials Bruteforcing
- Elements to Audit

- Optional
- DOM Element Exclusion

Scan Type

These settings specify the intensity of the assessment you want the scanner to perform.

Setting	Default Value	Description	Required
Assessment	Recommended	Drop-down box that allows you to choose from the following options to specify the scan type you want the scanner to perform. • **Recommended** – The scanner audits elements based on Tenable's recommendations. • **None** – The scanner does not audit any elements. • **Quick** – The scanner audits the most common elements listed. • **Extensive** – The scanner audits all the elements listed. • **Custom** – The scanner audits only the elements you select. **Note:** If you select **Recommended**, **Quick**, or **Extensive** and then make changes to the settings in this section, the **Scan Type** setting automatically changes to **Custom**.	Yes

Common and Backup Pages

Setting	Default Value	Description
Detection Level	Most Detected Pages	Drop-down box that allows you to choose from the following options to specify which pages you want the scanner to crawl. • **Most Detected Pages** - The scanner crawls only the most detected pages. • **Extended Dictionary** - The scanner tests more path variations for detecting hidden pages, increasing the overall scan duration. **Note:** The **Detection Level** drop-down box is available only when you select **Custom** in the **Scan Type** settings.

Credentials Bruteforcing

The **Credentials Bruteforcing** setting is available only for the **Scan** template.

Setting	Default	Description
Credentials Bruteforcing	Disabled	When enabled, any plugins that perform bruteforcing included in the **Plugins** settings run. When disabled, bruteforcing plugins do not run, even if they are included in the **Plugins** settings. **Note:** The **Credentials Bruteforcing** setting is available only when you select **Custom** in the **Scan Type** settings.

File Upload Assessment

Setting	Default	Description
File Upload Assessment	Disabled	When enabled, the scanner attempts to detect file upload vulnerabilities based on generic attacks against relevant inputs, or specific attacks against known software

Setting	Default	Description
		vulnerabilities. A file upload vulnerability detection can remotely create files on the scanned web application which the scanner cannot delete.

Elements to Audit

These settings specify the elements in your web application that you want the scanner to analyze for vulnerabilities.

Setting	Scanner Action
Cookies	Checks for cookie-based vulnerabilities.
Headers	Checks for header vulnerabilities and insecure configurations (for example, missing X-Frame-Options).
Forms	Checks for form-based vulnerabilities.
Links and Query String Parameters	Checks for vulnerabilities in links and their parameters.
Parameter Names	Performs extensive fuzzing of parameter names.
Parameter Values	Performs extensive fuzzing of parameter values.
Path Parameters	Assesses path parameters. Path parameters are used in URL rewrite to identify the object of the action within the URL. For example, **`scanId`** is a path parameter for the following URL, used to identify the scan to display results: `http://example.com/scan/`**`scanId`**`/results`
JSON Elements / Request Body (JSON)	Audits JSON request data.
XML Elements / Request Body (XML)	Audits XML request data.

Setting	Scanner Action
UI Forms	Checks input and button groups associated with JavaScript code. **Note**: With UI Forms, Tenable Web App Scanning takes the inputs on the page, and any buttons, and creates form-like elements from them (UI Forms). For each button, Tenable Web App Scanning creates a `UIForm` element with inputs that are all the inputs on the page.
UI Inputs	Checks orphan input elements against associated document object model (DOM) events. **Note**: UI Inputs are when there is an input that responds to an event. For example, after typing in the input in a search bar, the search bar responds to an "onEnter" event which loads the next page. So, Tenable Web App Scanningcreates a `UIInput` element to audit this vector as well.

Optional

Setting	Default	Description
URL for Remote Inclusion	None	Specifies a file on a remote host that Tenable Web App Scanning can use to test for a Remote File Inclusion (RFI) vulnerability. If the scanner cannot reach the internet, the scanner uses this internally-hosted file for more accurate RFI testing. **Note**: If you do not specify a file, Tenable Web App Scanning uses a safe, Tenable-hosted file for RFI testing.

DOM Element Exclusion

DOM element exclusions prevent scans from interacting with specific page elements and their children. This setting is available for Scan, Overview, and PCI scan templates.

Note: When the scanner is deciding whether to exclude an element based on an attribute value, it performs an equality check. So, if you want to exclude any element with css `class foo`, the scanner excludes an element that has `class="foo"`, but not an element that has `class="foo bar"`.

You can add exclusions by clicking the ⊕ button and selecting **Text Contents** or **CSS Attribute**.

Setting	Default	Description
Text Contents	None	Excludes elements based on text contents. For example, if you want to prevent the scanner from clicking a logout button named Log Out, you could match the text `Log Out`.
CSS Attribute	None	Excludes elements based on a CSS attribute key-value pair. For example, if you want to prevent the scanner from interacting with a form that contains the CSS attribute key-value pair `id="logout"`, type `id` for the key and `logout` for the value.

Report Settings in Tenable Web App Scanning Scans

Report settings specify extra items to include in the scan report. For example, scan reports for Tenable PCI ASV scans require load balancer usage details if applicable.

You can configure **Report** settings when you create a scan or user-defined scan template using the Tenable-provided scan template, **PCI**. For more information, see Scan Templates.

The **Report** settings include the following sections:

(Tenable PCI ASV 6.1) Load Balancers Usage

This setting specifies load balancer usage to include in the scan report.

Setting	Default Value	Description	Required
(Tenable PCI ASV 6.1) Load Balancers Usage	None	Text box that allows you to enter a list of load balancers and their configuration as required for Tenable PCI ASV. Include any information that may be pertinent to the scan in relation to load balancers, specifically if the environments behind the load balancers are	No

Setting	Default Value	Description	Required
		synchronized.	

Advanced Settings in Tenable Web App Scanning Scans

Advanced settings specify additional controls you want to implement in a web application scan.

You can configure **Advanced** settings when you create a scan or user-defined scan template using any Tenable-provided scan template. However, the **Overview** and **Scan** template types have more configurable **Advanced** settings than the **Config Audit** and **SSL TLS** template types. For more information, see Scan Templates.

The **Advanced Settings** options allow you to control the efficiency and performance of the scan.

- General
- HTTP Settings
- Screen Settings
- Limits
- Selenium Settings
- Performance Settings
- Session Settings

General

You can configure **General** options in scans and user-defined scan templates based on the **Overview** and **Scan** templates only.

Setting	Default	Description
Target Scan Max Time (HH:MM:SS)	08:00:00	Specifies the maximum duration the scanner runs a scan job runs before stopping, displayed in hours, minutes, and seconds. **Note**: The maximum duration you can set is 99:59:59 (hours:

		minutes: seconds).
Maximum Queue Time (HH:MM:SS)	08:00:00	Specifies the maximum duration the scan remains in the Queued state, displayed in hours, minutes, and seconds. **Note**: The maximum duration you can set is 48:00:00 (hours: minutes: seconds).
Enable Debug logging for this scan	disabled	Specifies whether the scanner attaches available debug logs from plugins to the vulnerability output of this scan.
Debug Flags	disabled	(Only visible when you enable the **Enable Debug logging for this scan** feature). Allows you to specify key and value pairs, provided by support, for debugging.

HTTP Settings

These settings specify the user-agent you want the scanner to identify and the HTTP response headers you want the scanner to include in requests to the web application.

You can configure **Crawl Settings** options in scans and user-defined scan templates based on any Tenable-provided scan template.

Setting	Default	Description
Use a different User Agent to identify scanner	disabled	Specifies whether you want the scanner to use a user-agent header other than Chrome when sending an HTTP request.
User Agent	Chrome's user-agent	Specifies the name of the user-agent header you want the scanner to use when sending an HTTP request. You can configure this option only after you select the **Use a different User Agent to identify scanner** checkbox. By default, Tenable Web App Scanning uses the user-agent

		that Chrome uses for the operating system and platform that corresponds to your machine's operating system and platform. For more information about Chrome's user-agents, see the *Google Chrome Documentation*. **Note:** Specific version numbers are subject to change as components are updated. The current Tenable Web App Scanning user-agent header looks similar to: `Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.4.5678.900 Safari/537.36` **Note:** Not all requests from a scanner are guaranteed to have the User Agent sent.
Add Scan ID HTTP Header	disabled	Specifies whether the scanner adds an additional `X-Tenable-Was-Scan-Id` header (set with the scan ID) to all HTTP requests sent to the target, which allows you to identify scan jobs in web server logs and modify your scan configurations to secure your sites.
Custom Headers	none	Specifies the custom headers you want to inject into each HTTP request, in request and response format. You can add additional custom headers by clicking the ⊕ button and typing the values for each additional header. **Note:** If you enter a custom `User-Agent` header, that value overrides the value entered in the **User Agent** setting box.

Screen Settings

You can configure **Screen Settings** options in scans and user-defined scan templates based on the **Overview** and **Scan** templates only.

Setting	Default	Description
Screen	1600	Specifies the screen width, in pixels, of the browser embedded in

Width		the scanner.
Screen Height	1200	Specifies the screen height, in pixels, of the browser embedded in the scanner.
Ignore Images	disabled	Specifies if the browser embedded in the scanner crawls or ignores images on your target web pages.

Limits

You can configure **Limits** options in scans and user-defined scan templates based on the **Overview** and **Scan** templates only.

Setting	Default	Description
Number of URLS to Crawl and Browse	10000	Specifies the maximum number of URLs the scanner attempts to crawl.
Path Directory Depth	10	Specifies the maximum number of sub-directories the scanner crawls. For example, if your target is `www.example.com`, and you want the scanner to crawl `www.example.com/users/myname`, type *2* in the text box.
Page DOM Element Depth	5	Specifies the maximum number of HTML nested element levels the scanner crawls.
Max Response Size	500000	Specifies the maximum load size of a page, in bytes, which the scanner analyzes. If the scanner crawls a URL and the response exceeds the limit, the scanner does not analyze the page for vulnerabilities.
Request Redirect Limit	3	Specifies the number of redirects the scanner follows before it stops trying to crawl the page.

Selenium Settings

These settings specify how the scanner behaves when it attempts to authenticate to a web application using your recorded Selenium credentials.

Configure these options if you configured your scan to authenticate to the web application with Selenium credentials. For more information see Credentials in Tenable Web App Scanning Scans.

You can configure **Selenium Settings** options in scans and user-defined scan templates based on the **Overview** and **Scan** templates only.

Setting	Default	Description
Page Rendering Delay	30000	Specifies the time (in milliseconds) the scanner waits for the page to render.
Command Execution Delay	500	Specifies the time (in milliseconds) the scanner waits after processing a command before proceeding to the next command.
Script Completion Delay	5000	Specifies the time (in milliseconds) the scanner waits for all commands to render new content to finish processing.

Performance Settings

Setting	Default	Description
Max Number of Concurrent HTTP Connections	10	Specifies the maximum number of established HTTP sessions allowed for a single host.
Max Number of HTTP Requests Per Second	25	Specifies the maximum number of HTTP requests allowed for a single host for the duration of the scan. **Note:** The scanner utilizes a set of web browsers in addition to the main HTTP client, and these web browsers are not rate-limited.

Slow down the scan when network congestion is detected	disabled	Specifies whether the scanner throttles the scan in the event of network congestion.
Network Timeout (In Seconds)	30	Specifies the time, in seconds, the scanner waits for a response from a host before aborting the scan, unless otherwise specified in a plugin. If your internet connection is slow, Tenable recommends that you specify a longer wait time.
Browser Timeout (In Seconds)	60	Specifies the time, in seconds, the scanner waits for a response from a browser before aborting the scan, unless otherwise specified in a plugin. If your internet connection is slow, Tenable recommends that you specify a longer wait time.
Timeout Threshold	100	Specifies the number of consecutive timeouts allowed before the scanner aborts the scan.

Session Settings

Specifying these tokens speeds up the scan by allowing the scanner to skip token verification. Session Settings are only available when you are editing an existing scan.

Token Type	Default	Description
Cookie	None	Name of your application's authentication cookie for the scanner to use.
Header	None	Name of your application's authentication header for the scanner to use.

Credentials in Tenable Web App Scanning Scans

Note: You can set Credentials settings for single-target scans only. If you create a scan with more than one target, these settings are not available.

In Tenable Web App Scanning scans, you can configure credentials settings that allow Tenable Web App Scanning to perform an authenticated scan on a web application. Credentialed scans can perform a wider variety of checks than non-credentialed scans, which can result in more accurate scan results.

Scans in Tenable Web App Scanning use managed credentials. Managed credentials allow you to store credential settings centrally in a credential manager. You can then add those credential settings to multiple scan configurations instead of configuring credential settings for each individual scan.

Tenable Web App Scanning scans support credentials in the following authentication types:

- HTTP Server Authentication
- Web Application Authentication
- Client Certificate Authentication

Tip: If want to scan an API with the API scan template, and your API requires keys or a token for authentication, you can add the expected custom headers in the Advanced settings in the **HTTP Settings** section.

You can configure credentials settings in Tenable Web App Scanning scans using the following methods.

Credentials Category	Authentication Type	Configuration Method
HTTP Server Authentication	-	Use the Tenable Web App Scanning user interface to manually configure credentials settings in scans.
Web Application Authentication	Login Form	
	Cookie Authentication	
	API Key	Use the Tenable Web App Scanning user interface to manually configure credentials settings in scans.
	Bearer Authentication	
Client Certificate	-	Use the Tenable Web App Scanning user interface

Authentication		to manually configure credentials settings in scans.

Tenable Web App Scanning Selenium Commands

Selenium commands in Tenable Web App Scanning are used to record authentication and crawling scripts so that users can tell the scanner exactly what to do in certain scenarios.

Note: The Tenable-provided Selenium extension is no longer supported. The Edge and Firefox extensions provided by Selenium directly are supported. Selenium-provided packages running outside of browsers are also supported.

Support for Selenium commands in Tenable Web App Scanning is detailed below:

Commands Supported	Commands Not Supported
• addSelection • answerOnNextPrompt • assert • assertAlert • assertChecked • assertConfirmation • assertEditable • assertElementNotPresent • assertElementPresent • assertNotChecked • assertNotEditable • assertNotSelectedValue • assertNotText • assertPrompt • assertSelectedLabel	• close • debugger • do • else • else if • end • execute async script • execute script • for each • if • repeat if • run • select window • store • store attribute

- assertSelectedValue
- assertText
- assertTitle
- assertValue
- check
- chooseCancelOnNextConfirmation
- chooseCancelOnNextPrompt
- chooseOkOnNextConfirmation
- click
- clickAt
- doubleClick
- doubleClickAt
- echo
- editContent
- mouseDown
- mouseDownAt
- mouseMoveAt
- mouseOut
- mouseOver
- mouseUp
- mouseUpAt
- open
- pause
- removeSelection

- store json
- store text
- store title
- store value
- store window handle
- store xpath count
- times
- while

- runScript
- select
- selectFrame
- sendKeys

  > **Note:** In addition to arbitrary text, the `sendKeys` command only supports the following escape sequences:
  >
  > - `${KEY_ENTER}`
  > - `${KEY_DELETE}`
  > - `${KEY_BACKSPACE}`

- setSpeed
- setWindowSize
- submit
- type
- uncheck
- verify
- verifyChecked
- verifyEditable
- verifyElementNotPresent
- verifyElementPresent
- verifyNotChecked
- verifyNotEditable
- verifyNotSelectedValue
- verifyNotText
- verifySelectedLabel

• verifySelectedValue • verifyText • verifyTitle • verifyValue • waitForElementEditable • waitForElementNotEditable • waitForElementNotPresent • waitForElementNotVisible • waitForElementPresent • waitForElementVisible • webdriverAnswerOnNextPrompt • webdriverAnswerOnVisiblePrompt • webdriverChooseCancelOnNextConfirmation • webdriverChooseCancelOnNextPrompt • webdriverChooseCancelOnVisibleConfirmation • webdriverChooseCancelOnVisiblePrompt • webdriverChooseOkOnNextConfirmation • webdriverChooseOkOnVisibleConfirmation	

HTTP Server Authentication Settings in Tenable Web App Scanning Scans

In a Tenable Web App Scanning scan, you can configure the following settings for HTTP server-based authentication credentials.

Option	Action
Username	Type the username Tenable Web App Scanning uses to authenticate to the HTTP-based server.

Password	Type the password Tenable Web App Scanning uses to authenticate to the HTTP-based server.
Authentication Type	In the drop-down list, select one of the following authentication types: • **Basic/Digest** • **NTLM** • **Kerberos**
Kerberos Domain	(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) This host supplies the session tickets for the user.

Note: Tenable Web App Scanning does not support multiple HTTP authentication types for a single target.

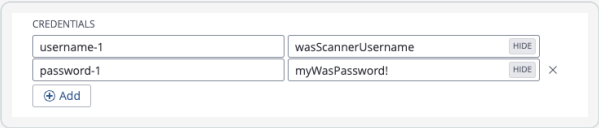
Web Application Authentication

In a Tenable Web App Scanning scan, you can configure one of the following types of **Web Application Authentication** credentials:

- Login Form Authentication
- Cookie Authentication
- Selenium Authentication
- API Key Authentication
- Bearer Authentication

Tip: If the log in process causes any headers or cookies to be set, the scanner should notice this and include those in subsequent requests. If this is not happening as you expect, use selenium authentication and record the log in process into a `.side` file, then use that in the scan. If you are still experiencing issues, contact your Tenable representative for support.

Login Form Authentication

Option	Action
Authentication Method	In the drop-down box, select **Login Form**.
Login Page	Type the URL of the login page for the web application you want to scan.
Credentials	For each field in the target's login form (that is, username, password, and domain, etc.) complete a credential entry as follows: a. In the left-hand text box, type the value of the login field's `name` or `id` HTML DOM attribute. b. In the right-hand text box in the row, type the literal value to insert in that text field at login. A typical configuration example:  **Tip:** To see a text field's `name` or `id` HTML DOM attribute, right-click on the text field and select "Inspect" in either your Firefox or Chrome browser. **Tip:** If you perform an uncredentialed **Overview** scan, plugin 98033 (**Login Form Detected**) may automatically detect and display the required login boxes in the plugin output.
Pattern to Verify Successful Authentication	Type 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 will be escaped and `.*` is not required at the beginning or end of the pattern.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type 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 will be escaped and `.*` is not required at the beginning or end of the pattern.

Cookie Authentication

Option	Action
Authentication Method	In the drop-down box, select **Cookie Authentication**.
Session Cookies	Do the following: a. In the first text box, type the name of the cookie authentication credentials. b. In the second text box, type the value of the cookie authentication credentials.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type 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 will be escaped and `.*` is not required at the beginning or end of the pattern.

Selenium Authentication

Option	Action
Authentication Method	Select **Selenium Authentication**.
Selenium Script (.side)	Do the following: a. In the Selenium IDE extension, record your authentication credentials in the Selenium IDE extension.

	Note: The Tenable-provided Selenium extension is no longer supported. The Edge and Firefox extensions provided by Selenium directly are supported. Selenium-provided packages running outside of browsers are also supported. b. Click **Add File**. The file manager for your operating system appears. c. Navigate to and select your Selenium credentials `.side` file. Tenable Web App Scanning imports the credentials file.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type 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 will be escaped and `.*` is not required at the beginning or end of the pattern.

API Key Authentication

Option	Action
Authentication Method	Select **API Key**.
Headers	Do the following: a. In the first text box, type the name of the HTTP header. b. In the second text box, type the value of the HTTP header. c. (Optional) Add additional headers by clicking the ⊕ button.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type 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 will be escaped and `.*` is not required at the beginning or end of the pattern.

Bearer Authentication

Option	Action
Authentication Method	Select **Bearer Authentication**.
Bearer Token	Type the value of the bearer token. **Note**: Bearer Token is a part of OAuth. Tenable Web App Scanning supports OAuth in cases where it is a part of OpenIDConnect and recordable via a selenium script. Implementations of OAuth that are not a part of OpenIDConnect are supported only where the token is dynamic, or you craft a special static (non-dynamic) token for authentication purposes.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type 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 will be escaped and `.*` is not required at the beginning or end of the pattern.

Client Certificate Authentication

In a Tenable Web App Scanning scan, you can configure **Client Certificate Authentication** credentials.

Option	Action
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	The passphrase for the private key, if required.

Private Key Passphrase	
Page to Verify Successful Authentication	Type the URL that Tenable Web App Scanning can access to validate the authenticated session.
Pattern to Verify Successful Authentication	Type a word, phrase, or regular expression that appears on the website only if the authentication is successful (for example, Welcome, your username!). Leading slashes will be escaped and .* is not required at the beginning or end of the pattern.

Plugin Settings in Tenable Web App Scanning Scans

Required Tenable Web App Scanning User Role: Scan Manager or Administrator

Configure **Plugin** settings to specify the plugins and plugin families you want the scanner to use as it scans your web application.

When you create and launch a scan, Tenable Web App Scanning uses plugins in various plugin families, each designed to identify certain types of finding or vulnerabilities, to analyze your web application. Tenable Web App Scanning uses the 98000-98999 and 112290-117290 plugin ID ranges for scanning. For more information about Tenable Web App Scanning plugin families, see the Tenable Web App ScanningTenable Web App Scanning Plugin Families site.

Note: Tenable Web App Scanning displays only the first detected 25 instances of an individual plugin per scan in your scan results. If you see 25 instances of a single plugin in your scan results, Tenable recommends taking remediation steps to address the corresponding vulnerability and then rescanning your target.

You can configure **Plugin** settings when you create a scan or user-defined scan template and select the **API**, **Overview**, **(Basic) Scan**, **Standard Scan**, or **Custom** template or scan type. For more information, see View Your Scan Plugins.

Tip: If you want to save your settings configurations and apply them to other scans, you can create and configure a user-defined scan template.

The plugins settings contain the following sections:

- All enabled
- Plugins table

All Enabled

A toggle you can click to enable or disable all plugins simultaneously.

Plugins Table

Column	Description	Actions
Name	Specifies the plugin family to which the grouped plugins belong.	• View the name of each plugin family. • Select the column to sort the table alphabetically or by family name.
Total	Specifies the number of plugins in the plugin family.	• View the number of plugins in the family. • Select the column to sort the table by number of plugins in each family.
Status	Toggle that allows you to specify if you want the scanner to use the plugins in the plugin family to analyze your target.	• Click the **Status** toggle to disable the plugins in the plugin family. • (Optional) To enable a disabled plugin family, click the **Status** toggle.

In the plugins table, you can view details about or disable individual plugins.

To view details about individual plugins:

1. In the table, click the row for the family that contains a plugin you want to view.

   A plugin family details plane appears, displaying the name, ID, and status for each plugin in the family in a paginated list.

2. (Optional) To locate a specific plugin, in the **Search** box, type the name or ID.
3. Click the plugin for which you want to view details.

To disable individual plugins:

1. In the table, click the row for the family that contains the plugin you want to disable.

   A plugin family details plane appears, displaying the name, ID, and status for each plugin in the family in a paginated list.

2. (Optional) To locate a specific plugin, in the **Search** box, type the name or ID.
3. In the **Status** column, select the check box next to the plugin you want to disable.
4. (Optional) To enable a disabled plugin, select the check box.
5. Click **Save**.

   The details plane disappears.

   Tenable Web App Scanning updates your plugin selections.

Scan Distribution

Overview

Tenable Vulnerability Management's scan distribution method improves scan efficiency for your organization’s scanners and the cloud scanners that Tenable provides. Tenable Vulnerability Management distributes scans as tasks across multiple scanners in the scanner group assigned to the scan, rather than assigning complete scan jobs to individual scanners. When you assign a scan to a single scanner, Tenable Vulnerability Management assigns the scanner tasks that can run in parallel, enabling the scanner to complete the job more efficiently.

Scan distribution allows multiple scan tasks to run simultaneously, reducing bottlenecks that would occur if scans ran sequentially on individual scanners. As your organization’s scanning needs grow, this distribution method makes it less likely for your overall scan performance to degrade.

How Tenable Vulnerability Management Distributes Scans

Scan Job Creation and Queuing

When you launch a scan, Tenable Vulnerability Management creates a scan *job* and sends it to the job queue of the scanner group or individual scanner defined in the scan configuration. Jobs are always sent from Tenable Vulnerability Management and queued in scanner groups or individual scanners in the order they are created.

Tenable Vulnerability Management determines where and what to send scan jobs based on three aspects of the target scanner or scanner group's *capacity*:

- Target capacity — The number of assets a scanner can actively scan simultaneously. This value is by default based on the hardware resources of the scanner, including the number of processors and the amount of memory available.
- Task capacity — The number of tasks (parts of a scan) that a scanner can perform simultaneously. A scanner's task capacity is determined based on the target capacity.
- Job capacity — The number of different jobs a scanner can include tasks from at once. In this way, scans can be performed asynchronously, and a scanner that has available capacity can complete multiple tasks even if those tasks are not derived from the same scan. Job capacity is always determined to be less than equal to the task capacity so that when a scanner is at its job capacity, it will be able to complete tasks from every job.

For scanner groups, jobs are queued centrally, and the earliest job is held until the group has available capacity. For individual scanners, the job queue may include jobs assigned directly as well as jobs distributed from groups the scanner belongs to.

Scan Task Assignment

When a scanner or scanner group has available capacity, Tenable Vulnerability Management breaks the earliest job in its queue into scan *tasks* and dispatches them.

- For scanner groups, Tenable Vulnerability Management distributes tasks across scanners in the group using a "round robin" method.
- For individual scanners, tasks are pulled from the job queue and assigned in round robin order until the scanner's task capacity is full.

Each scan task accounts for up to 120 IP addresses. The last task in a job may contain fewer addresses. For example, Tenable Vulnerability Management splits a scan job of 300 IP addresses into two 120-address tasks and one 60-address task.

The way Tenable Vulnerability Management dispatches tasks depends on the scanning scenario. See the following examples for more information:

Example Scenario: One Scanner with One Job

A single standalone scanner processes jobs one at a time in the order they are queued. If the scanner has a task capacity of six, Tenable Vulnerability Management assigns six tasks from the job to run simultaneously. As each task completes, new tasks fill the available capacity until the job is finished.

Example Scenario: One Scanner with Multiple Jobs

If a scanner belongs to two scanner groups and also has a job assigned directly, its job queue may contain three jobs. Because the scanner's job capacity is three, it can process tasks from all three jobs at the same time.

If the scanner's task capacity is five, tasks are assigned in succession across the jobs: Job 1, Job 2, Job 3, Job 1, Job 2. In this case, the scanner works on two tasks from Job 1, two tasks from Job 2, and one task from Job 3. When one task completes, the next task from Job 3 is dispatched.

Example Scenario: Multiple Scanners with Multiple Jobs

If Scanner 1 and Scanner 2 are assigned to the same scanner group (SG1), and two jobs are created—Job 1 assigned directly to Scanner 1 and Job 2 assigned to SG1—Tenable Vulnerability Management breaks down both jobs into tasks.

- Only Scanner 1 works on Job 1.
- Both Scanner 1 and Scanner 2 work on Job 2.

If both scanners have a job capacity of three and a task capacity of six, Scanner 1 processes three tasks from Job 1 and three tasks from Job 2, while Scanner 2 processes six tasks from Job 2. Tasks from Job 2 continue to be dispatched to both scanners until the job is complete.

View Live Results

As scanners complete tasks, you can view live scan results in Tenable Vulnerability Management. Each time a task completes, the platform updates the scan results with new data. If a scan fails or is interrupted, Tenable Vulnerability Management retains all completed results, though the scan reflects an incomplete status. If a job is assigned to multiple scanners and one of those scanners fails, the remaining scanners continue processing tasks until completion.

Scan Routing

With *scan routing*, you can automatically dispatch scans across multiple scanner groups based on the network areas that each group can access. Scan routing reduces configuration and management overhead because you do not need to assign specific scanners to each scan. This feature is especially useful in large deployments. Users with higher-level permissions can manage scanner groups, and users with lower-level permissions can select those groups during scan configuration.

> **Note:** Scan routing is available only for linked scanners.

When you configure scan routing for a scan, Tenable Vulnerability Management automatically:

- Assigns scan targets to the scanner group with the narrowest matching target range.
- Within that scanner group, assigns targets to scanners as they connect, based on their available capacity and the targets remaining.

Configuration Guidelines

Tenable recommends that you plan your scan routing strategy in advance to ensure efficient coverage of your network. If you configure scan routing incorrectly, scanners may not be able to reach their targets.

- Use IP ranges and CIDR ranges where possible, rather than individual IP addresses. This approach differs from configuring scan targets, where narrower values are recommended.
- Tenable Vulnerability Management does not support numeric range format for IPv6 addresses. Use CIDR format instead.
- Typically, add each scanner to only one scanner group. However, you can configure overlapping groups for redundancy or coverage. If a host is included in multiple overlapping groups, Tenable Vulnerability Management assigns the host to any one of the groups. No

group receives preference. For information about scanner availability in a group, see Scanner Groups.

To configure scan routing:

1. **Configure a scanner group for scan routing.**

   a. Create or edit a scanner group.

   b. In the **Targets for Scan Routing** box, type a comma-separated list of scan routing targets.

   Tenable Vulnerability Management supports the following formats for scan routing targets:

Target Format	Example
A single IPv4 address	192.168.0.1
A single IPv6 address	2001:db8::2120:17ff:fe56:333b
An IPv4 range with a start and end address	192.168.0.1-192.168.0.255
An IPv4 subnet with CIDR notation	192.168.0.0/24
An IPv6 subnet with CIDR notation	2001:db8::/32
A host resolvable to either an IPv4 or an IPv6 address	www.yourdomain.com
A host resolvable to either an IPv4 address or an IPv 6 address with a wildcard as the subdomain	*.yourdomain.com

Note: You can specify up to 10,000 individual scan routing targets for an individual scanner group. For example, `192.168.0.1, example.com, *.example.net, 192.168.0.0/24` specifies four scan routing targets. To condense a scan routing target list, Tenable recommends using wildcard and range formats, instead of individual IP addresses.

c. Click **Save**.

Tenable Vulnerability Management saves your changes to the scanner group.

2. **Configure a scan for scan routing.**

a. Create or edit a scan configuration.

b. In the **Basic** settings section, configure the following options:

Option	Action
Scanner	Select the **Auto-Select** option. When you select this option, the **Network** box appears.
Network	Do one of the following: • If your scans involve separate environments with overlapping IP ranges, select the network that contains the scanner groups that you configured for scan routing. • If your scans do not involve separate environments with overlapping IP ranges, retain the **Default** network.
Targets / **Upload Targets** / **Tags**	Specify targets for the scan, using one of the following options: • In the **Targets** box, type the list of targets. • In the **Upload Targets** box, upload a file of targets. • In the **Tags** box, specify targets by tag. When specifying scan targets, note the following: • Be sure to match scan targets to the scan routing targets you specify in your scanner groups. If you specify scan targets outside the range of scanner group targets, Tenable Vulnerability Management scans only those hosts inside the scanner group range and returns the partial results with a warning that lists the hosts that were not

	scanned. • When matching scan routing targets to scan targets, Tenable Vulnerability Management does *not* resolve FQDNs to IP addresses. For example, if you specify `*.example.com` as a scan routing target, Tenable Vulnerability Management can assign a scan to that scanner group if the scan is configured with the scan target `www.example.com`. However, Tenable Vulnerability Management does not assign a scan to that scanner group if a scan is configured with the target `192.168.0.1`, even if `www.example.com` could potentially resolve to `192.168.0.1`.

c. Click **Save**.

Tenable Vulnerability Management saves your changes to the scan configuration.

Scan Best Practices

Introduction

Every organization has unique needs for their vulnerability management program. These requirements can vary from the scanner used (cloud or on-premises), the places where a sensor is deployed, technology in your environment, and other conditions of your vulnerability management program. The following information contains deployment best practices that should apply to everyone and assist in situations where continued overages occur.

General Best Practices

Role-Based Access Control (RBAC)

Familiarize yourself with Access Control and RBAC for controlling scan and view permissions for assets. Misconfigured access controls or User Groups can cause scan failures and asset or vulnerability deficiencies in dashboards and reports.

Credentialed Scanning

Tenable recommends running credentialed scans whenever possible. Credentialed scans provide your organization with a more accurate snapshot of your current environment, allowing you to quickly and safely collect information about your network and systems. You can use this information to fill in the gaps in your security architecture and make better decisions on how to improve your information security program.

Credentialed scans can also perform a wider variety of checks than non-credentialed scans, which provide you with more accurate scan results. This ensures extensive scanning of your network to determine local exposures or compliance violations. See Credentialed Network Scans in the *Tenable Agent User Guide* for more information about the benefits of credentialed scanning.

Proper Inventory of Assets

An accurate inventory of the existing assets in your network is the first step towards effective vulnerability management. To learn more, review asset inventory best practices and asset inventory analysis and review.

Deleting Assets

You can delete assets via the user interface, but they remain on the license for 90 days or until the Asset Age Out time has aged out. If the asset is found again before the 90 period or the Asset Age Out expiration, it counts as an additional licensed asset. With this in mind, if you expect to detect the asset again in the future, it is best to add this asset to the global exclusion list to avoid any licensing issues or enable Asset Age Out to purge deleted assets as early as seven days after they were deleted. For more information, see Delete Assets.

You can tag all assets that need to be deleted and use the API to bulk delete those assets. For instance, you could tag assets and use an automated script to delete assets with the “delete” tag on a custom time interval. If you know these assets may be found again (for example, honeypot networks), it is best practice to add these affected assets to the global exclusion list to avoid licensing issues or reduce your target scope to omit them.

- Bulk delete API documentation
- Exclusion API documentation
- Asset age out API documentation

Agent Scanning

Agents are a great way to capture vulnerability data on assets that are mobile or highly sensitive. It is essential to understand that an agent scan cannot interrogate the potential external exposure such as TLS vulnerabilities. If these types of vulnerabilities on these types of assets are important to your program, you should pair this with a network-based scan. If a credentialed vulnerability scan is not possible, you can use a non-credentialed scan. However, it is important to understand that non-credentialed scans on agents may produce an additional licensed asset. See the following section for more information.

Scan Hygiene

Before scanning, Tenable recommends reviewing the *Tenable Vulnerability Management Scan Tuning Guide*. Tenable Vulnerability Management limits the total number of scan schedules to 10,000. A scan schedule includes a scan template (including discovery and assessment settings), a list of scan targets, and (optionally) credentials and compliance audits. You can reuse can schedules, and doing so groups the scan results under the History tab of the given scan schedule.

It is best practice to reuse “on-demand” scan schedules, reduce clutter or confusion when looking for scan schedules, and adhere to good scan hygiene. There is little to no benefit to creating new “on-demand” scan schedules each time a new set of assets needs to be scanned. Instead, simply change the targets of the scan and use the history to see older data. Keep in mind, unless you avoid sending the data to the workbench, all of the changes found during the scan are reflected in the workbenches, reducing the need to review old scan results.

It is common to ask, “What changed since the previous scan?” This question can drive attention to the previous scan. However, you should note that each scan updates the assets with the newest information. You can use the asset Activity tab to identify when a Tenable sensor detected the asset. Furthermore, each vulnerability indicates when the vulnerability or plugin was first seen and last seen. The difference between those two dates typically helps in identifying what has changed since a previous scan.

Lastly, it is best practice to use remediation scans for re-scanning the asset outside of its predefined scan cycle. You can initiate remediation scans from the action button on the vulnerability details page. This is the most convenient way to manage remediation scans and helps keep scan hygiene clean.

API Scan Creation Best Practices

If you use the API to automate scan creation, it is still equally important to maintain scan hygiene. If you cannot reuse the same scan schedule for your workloads, Tenable recommends that you make scan deletion a part of your automated scan procedure. Instead of creating a new scan policy for every new scan, consider using the `alt_targets` parameter when launching a new scan as outlined in the API documentation.

Maintaining scan hygiene helps reduce the number of scans sent back on each request to the `/scans` endpoint and may speed up the endpoint.

Server with Multiple NICs

Non-credentialed scans may not collect enough data to merge the two network interfaces found during a scan.

Resolution:

- Scan the asset with credentials to uniquely identify the asset and de-duplicate the multiple NICs.
- Exclude any extra IP addresses for the asset if they do not provide any reporting value. You may use network scanning to “pen test” an asset, and visibility into different vulnerabilities or open ports on a different network interface may provide insight and value. To correct any reporting accuracy issues, delete the asset using the user interface or API.
- To remove duplicates that were deleted, enable Asset Age Out to mirror your scan schedule.

Firewall and Layer 3 Switches

Non-credentialed scans cannot collect enough data to uniquely identify a firewall or Layer 3 switch in the event that multiple interfaces are scanned. In order to do so, Tenable Vulnerability Management would have to crawl the device’s system configuration to see the interface IPs. However, even with credentialed scans, Tenable Vulnerability Management does not crawl the configuration file and gather this data.

Resolution:

- When multiple interfaces are found in a scan, identify which ones are duplicates in value and add them to the exclusion list.

- Example: In the case of a firewall with three interfaces, and therefore three IP addresses, exclude two of the IP addresses and delete them using the user interface or API.

- To remove duplicates that were deleted, enable Asset Age Out to mirror your scan schedule.

Agents and Non-Credentialed Scans

Non-credentialed scans may not collect enough data to merge the two findings (agent scan and non-credentialed scan). A well-hardened server does not provide enough data to identify the asset uniquely. However, Tenable's algorithm de-duplicates the asset reducing the license count where there is more data.

Resolution:

- For assets that are well hardened or do not provide enough data for Tenable's algorithms to merge assets confidently, you should add credentials so that Tenable can collect the data necessary to merge the assets confidently.

Ephemeral Assets

Ephemeral assets or assets that are terminated and rebuilt before the 90-day period has aged out creates a new asset each time they are rebuilt or deployed. Many asset attributes may change after the asset has been terminated, making it difficult to merge the asset with its previous version.

Resolution:

- Use the cloud connectors. The cloud connectors not only help identify ephemeral assets in the cloud, but they also detect their termination and remove the corresponding license.

- For situations where you cannot use a cloud connector, you need to leverage the Asset Age Out feature. The Asset Age Out feature purges assets automatically if they are not found within the configured time period.

Scanning during Maintenance Windows

Tenable occasionally performs maintenance on Tenable Vulnerability Management. To avoid performance issues, Tenable recommends not running or scheduling scans during maintenance windows. For current maintenance status and updates, see the Tenable Status page.

Scan Limitations

The following table describes scanning limitations in Tenable Vulnerability Management:

Limitation	Description
Targeted IP addresses or hostnames per assessment scan	Tenable Vulnerability Management limits the number of IP addresses or hostnames you target with a single assessment scan (for more information, see Discovery Scans vs. Assessment Scans). The host target limit is 10 times your organization's licensed asset count. For example, if your organization has a licensed asset count of 1,000, Tenable Vulnerability Management does not allow you to target more than 10,000 hostnames or IP addresses in a single assessment scan. If you exceed the limit, Tenable Vulnerability Management aborts the scan.
Targeted IP addresses or hostnames per discovery scan	Tenable Vulnerability Management limits the number of IP addresses or hostnames you target with a single discovery scan (for more information, see Discovery Scans vs. Assessment Scans). The host target limit is 1,000 times your organization's licensed asset count. For example, if your organization has a licensed asset count of 1,000, Tenable Vulnerability Management does not allow you to target more than 1,000,000 hostnames or IP addresses in a single discovery scan. If you exceed the limit, Tenable Vulnerability Management aborts the scan.
Host scan results per scan	Tenable Vulnerability Management limits the number of live hosts for which a single scan can generate scan results for. The live host scan results limit is 1.1 times your organization's licensed asset count. For example, if your organization has a licensed asset count of 1,000, Tenable Vulnerability Management does not allow you to generate scan results for more than 1,100 live hosts from a single scan. If you exceed the limit, Tenable Vulnerability Management aborts the scan. Tenable Vulnerability Management does not apply the live host scan result limit to discovery scans. Tenable Vulnerability Management also limits the number of dead hosts for which a single scan can generate scan results for. The dead host scan results limit is 100 times your organization's licensed asset count. For example, if your organization has a licensed asset count of 1,000,

	Tenable Vulnerability Management does not allow you to generate scan results for more than 100,000 dead hosts from a single scan. If you exceed the limit, Tenable Vulnerability Management aborts the scan.
Targeted IP addresses or ranges per scan	You cannot specify more than 300,000 comma-separated IP addresses or ranges when configuring a scan's targets.
Active scans	You cannot have more than 25 scans running in your container simultaneously.
Scan chunks	Tenable Vulnerability Management limits scan chunks to 10,000 hosts, 150,000 findings, or 7 GB in total size. If a scan chunk exceeds any of these values, Tenable Vulnerability Management does not process the scan and eventually aborts it. **Note:** This limits items like MDM assessments, importing Nessus files, and very large Auto Discovery scenarios (for example, VMware) to individual scans with less than 10,000 assessed targets.
Scan configurations	Tenable Vulnerability Management limits the number of scan configurations you can create to 10,000 scans. Tenable recommends re-using scheduled scans instead of creating new scans. This approach helps to avoid latency issues in the user interface.

Triggered Agent Scans

When you configure a Tenable Agent scan in Tenable Vulnerability Management, Tenable Vulnerability Management offers two agent scan types: **Scan Window** and **Triggered Scan**.

For window scans, Tenable Vulnerability Management creates a timeframe (for example, the default is three hours) in which an agent group must report in order to be included in the scan results. You must schedule Tenable Vulnerability Management to launch window scan at a scheduled time, or you must manually launch the scan from the Tenable Vulnerability Management user interface (for example, if you schedule a three-hour agent window scan for every Monday, Tenable Vulnerability Management pulls data updates from the agent group for three hours every Monday).

Triggered scans differ from window agent scans in that the agent or agent group launches the scan without any Tenable Vulnerability Management or user intervention. Agents can launch triggered scans using three different methods:

- Interval trigger – Configure agents to scan at a certain time interval (for example, every 12 hours or every 24 hours).
- File Name trigger – Configure agents to scan whenever 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:

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`

- Nessuscli trigger – Launch an existing triggered scan manually by running the following command in the Tenable Agent `nessuscli` utility:

  ```
  # nessuscli scan-triggers --start --UUID=<scan-uuid>
  ```

You can also set multiple triggers for a single scan, and the scan searches for the triggers in their listed order (in other words, if the first trigger does not trigger the scan, it searches for the second trigger).

Note: Tenable Vulnerability Management ignores triggered agent scan data that is older than 14 days. This ensures that Tenable Vulnerability Management is not processing stale data from agents that have been offline for extended periods of time.

Triggered vs. Window Scans

Tenable recommends using triggered agent scans over window agent scans in many cases. Due to the scanning independence from Tenable Vulnerability Management or user intervention and the multiple trigger options, triggered scanning offers more flexibility to meet the needs of your workflow, especially if you have a mobile workforce in multiple time zones.

Triggered scans can provide more consistent coverage than window scans and help overcome connectivity issues between Tenable Vulnerability Management and linked agents. While window scans can create gaps in data coverage due to unresponsive or offline agents, triggered scans allow agents to scan and send data to Tenable Vulnerability Management whenever the triggers occur; Tenable Vulnerability Management accepts and processes data from triggered scans at any time.

Tenable recommends using scan windows if you need to export individual scan results, as you can only export triggered scan data by using the bulk vulnerability export API.

Disable and Re-enable Triggered Scans

Tenable Vulnerability Management allows you to easily disable and re-enable triggered scans from the scans table. Triggered scans are enabled by default when you first create them, but you may want to disable them in troubleshooting or testing situations.

To disable or re-enable a triggered scan configuration, navigate to the **Scans** > **Vulnerability Management Scans**. Then, in the **Actions** menu of the triggered scan configuration's row, select **Disable** or **Enable**.

Find Triggered Scan Details

To view triggered scan results, see View Tenable Vulnerability Management Scan Details.

> **Note:** For triggered scan histories, Tenable Vulnerability Management shows a scan history entry for each 12-hour window of the past 7 days. Tenable Vulnerability Management only retains up to 15 triggered scan histories at a time for each scan.

In addition to managing triggered scans from Tenable Vulnerability Management, you can view triggered scan details by running the following command in the Tenable Agent `nessuscli` utility:

```
# nessuscli scan-triggers --list
```

The `--list` command returns the agent's triggered scan details. These details include:

- Scan name
- Status (for example, **uploaded**)
- Time of last activity (shown next to the status)

- Scan description
- Time of last policy modification
- Time of last run
- Scan trigger description
- Scan configuration template

  For more information about the Tenable Agent `nessuscli` utility, see Nessuscli Agent in the *Tenable Nessus User Guide*.

You can also view your agent trigger information in the agent trigger directory:

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`

Continuous Assessment Scanning

Continuous assessment scanning is a scanning method that Tenable Vulnerability Management can perform through linked Tenable Agents. It provides continuous monitoring and reporting of software inventory changes on your hosts.

Continuous assessment scanning is currently only available for Tenable Agents installed on Linux hosts.

Note: Continuous assessment scanning does not support the **Show missing patches that have been superseded** scan report setting.

Caution: Agents that have NIAP mode enforced cannot perform continuous assessment scanning. For more information on NIAP mode, see Configure Tenable Agent for NIAP Compliance and Tenable Agent CLI Commands in the *Tenable Agent User Guide*.

Explanation

Enabling continuous assessment scanning on an agent provides a continuous monitoring solution for software inventory changes on the host the agent is installed on. Agents run an initial baseline scan to capture the full software inventory on the host and re-run these baseline scans every *x* amount of days, depending how you configure your agent profile. In between baseline scans, the agent monitors the software inventory on the host and reports any vulnerabilities associated with inventory changes as they occur (for example, when new software is installed or existing software is uninstalled).

Although continuous assessment scanning offers the convenience of continuous vulnerability monitoring, the vulnerability coverage differs from standard agent scanning. Continuous assessment scanning detects vulnerabilities found in the software versions installed on the host the agent resides on; it does not provide coverage for malware, remote system checks, or database enumerations.

In addition to continuous assessment scanning, Tenable recommends running a standard agent scan at your desired cadence to cover any checks that are not supported in continuous assessment scanning. Configuring a combination of continuous assessment scanning and standard agent scanning allows you to reduce your organization's scan impact while continuously monitoring your assets for software inventory vulnerabilities.

Agents configured with continuous assessment scanning can still perform standard scan window or triggered scans. Scan configuration settings do not affect continuous assessment scanning.

> **Note:** Continuous assessment scanning requires a system user to run under. When continuous assessment is first started on an agent, the agent automatically creates a system user called **tenable_tua_comm**. The tenable_tua_comm user is a locked system user and cannot be used for logging in.

System Requirements

Hardware	Minimum Requirement
CPU	• Single core – ~20% of available CPU when processing a baseline scan, ~1.5% of available CPU when processing continuous scans • Dual core – ~23% of available CPU when processing a baseline scan, ~2% of available CPU when processing continuous scans
RAM	~50 MB

Network Bandwidth	• Baseline scans – ~220 KB • Continuous scans – ~85 KB per every 500 inventory change events
Disk Space	Same as the standard agent disk space requirement.

Plugins

To view the plugins that are used in continuous assessment scanning, use the following plugin search filter (**Supported Sensors -Continuous Assessment**) on the Tenable Plugins site: https://www.tenable.com/plugins/search?q=supported_sensors%3A%28continuous_assessment%29&sort=&sort=&page=1

Using those search filters, enter an additional **CPE** filter and specify one of the following CPEs to view individual plugins that continuous assessment scanning supports:

- cpe:/a:amazon:cloudwatch_agent
- cpe:/a:cloudbees:jenkins
- cpe:/a:gitlab:gitlab
- cpe:/a:google:kubernetes
- cpe:/a:haxx:curl
- cpe:/a:haxx:libcurl
- cpe:/a:jenkins:jenkins
- cpe:/a:kubernetes:kubernetes
- cpe:/a:openssl:openssl
- cpe:/a:splunk:splunk
- cpe:/a:tenable:nessus
- cpe:/a:tenable:nessus_agent
- cpe:/a:vmware:workstation
- cpe:/a:zoom:zoom
- cpe:/a:zoom:zoom_cloud_meetings

The following Linux security check plugins on the Tenable Plugins site are supported by continuous assessment scanning. These local security checks are package-based checks that correspond to each distribution's security advisories. For example, the Alma Linux Local Security Checks check for any Alma Linux security advisories.

- Alma Linux Local Security Checks
- Amazon Linux Local Security Checks
- CentOS Local Security Checks
- Debian Local Security Checks
- Fedora Linux Local Security Checks
- Oracle Linux Local Security Checks
- Red Hat Local Security Checks
- Rocky Linux Local Security Checks
- SUSE Local Security Checks
- Ubuntu Local Security Checks

Configuration

You can configure continuous assessment scanning at the agent profile level. To enable continuous assessment scanning, select the **Enable Continuous Assessment module** option in the **Agent Profile** menu and configure the agent's **Baseline scan frequency**. Once you enable the setting, configure the baseline scan frequency, and save the agent profile changes, the agents assigned to that profile begin to perform continuous assessment scanning.

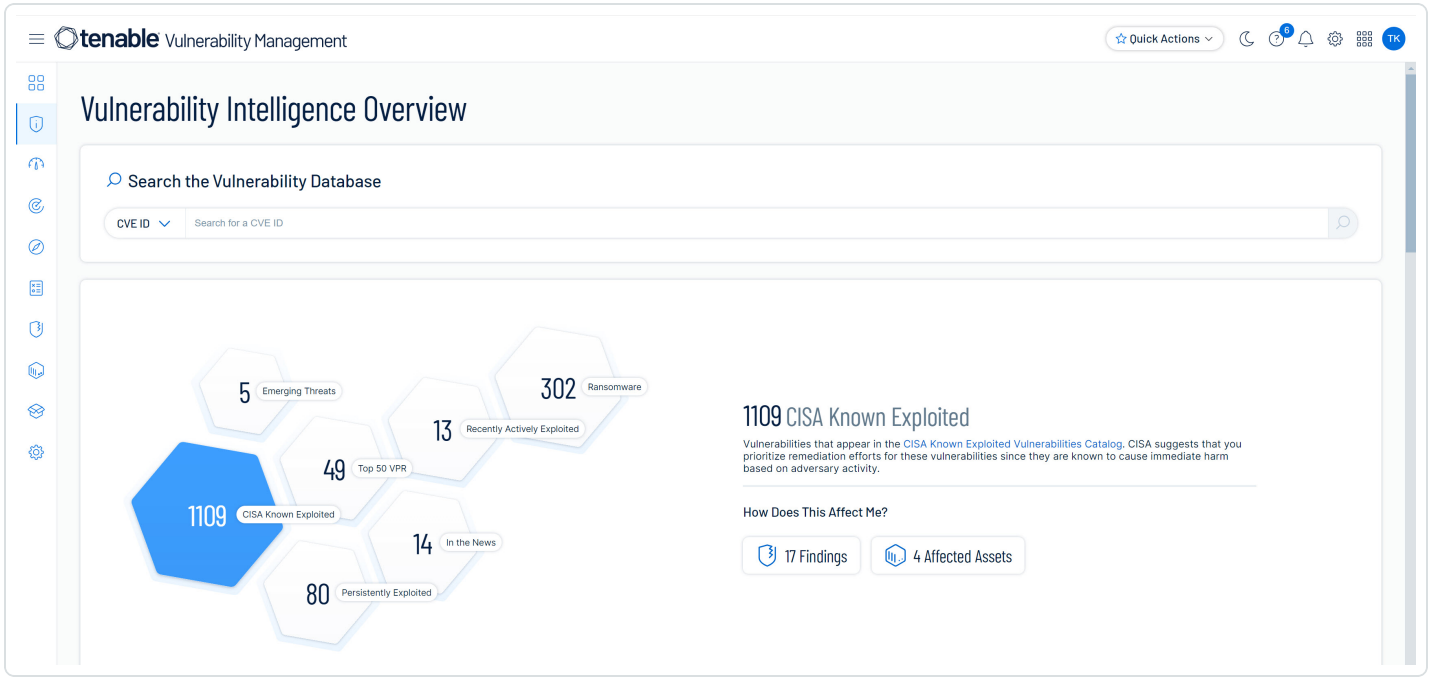
For more information, see Agent Profiles.

Vulnerability Intelligence

In the **Vulnerability Intelligence** section, you can review all vulnerabilities known to Tenable without leaving Tenable Vulnerability Management.

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.

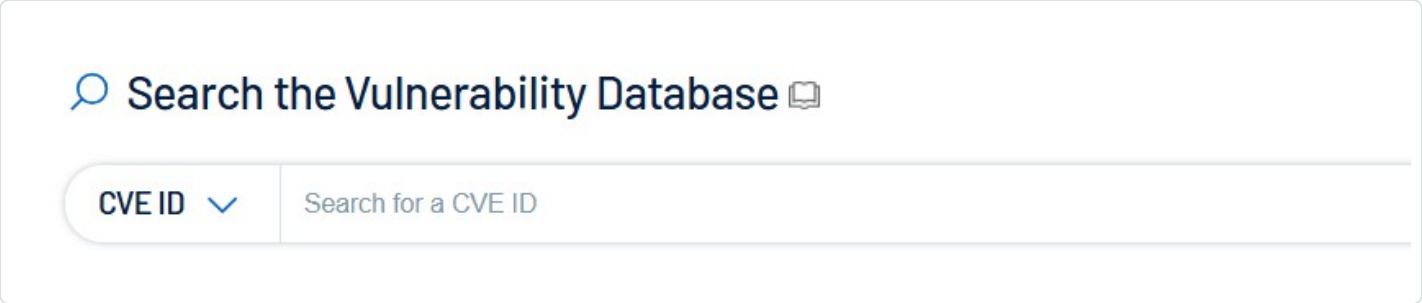
The following topics explain how to use the tools in the **Vulnerability Intelligence** section to: 1) search Tenable's vulnerability database, 2) view vulnerability profiles, and 3) identify your exposure when compared to known vulnerabilities.

- Search Known Vulnerabilities
- View Vulnerability Profiles

- Identify Your Exposure
- Vulnerability Intelligence Filters
- Vulnerability Categories

Search Known Vulnerabilities

On the **Vulnerability Intelligence Overview** page, you can search all vulnerabilities known to Tenable by *Common Vulnerabilities and Exposures* (CVE) ID or common name.



To search for a vulnerability:

1. In the left navigation, click **Vulnerability Intelligence**.

   The **Vulnerability Intelligence Overview** page appears.

2. In the drop-down, select **CVE ID** or **Common Name**.
3. In the search box, type a complete or partial search (for example, *CVE-2014-0160*, *2014*, or *Heartbleed*).
4. Press the **Enter** key.
5. In the list of results, click a vulnerability.

   The **Vulnerability Profile** page appears.

Export CVE Details

On the **Vulnerability Profile** page, you can export CVE details to PDF to share with your organization. You can schedule exports, email them, and protect them with a password.

To export CVE details:

1. Search for a vulnerability.
2. On the **Vulnerability Profile** page, click **Export**.
3. In the **Export PDF** dialog that appears, set the following options.

Option	Description
File Name	Type a name for the export file.
Affected Assets	(Optional) Turn on **Include list of Affected Assets**. You can include assets affected by the vulnerability as long as there are less than 5,000 assets.
PDF Password	(Optional) Enter a password for the export file.
Schedule	Turn on the **Schedule** toggle and set the following options: a. Choose an export **Start Date** and **Start Time**. b. Choose a **Time Zone**. c. Under **Frequency**, choose how often want the export to repeat. Then, choose **Repeat Every** and **Repeat By** (for example, the fourth Monday of the month). d. Under **Repeat Ends**, choose the when exports end. If you choose **Never**, the export repeats until you modify or delete it.
Email Notifications	Turn on the **Email Notification** toggle and set the following options: a. Under **Add Recipients**, type the emails to notify. b. Under **Password**, type a password for the export file which the recipient will need to enter.

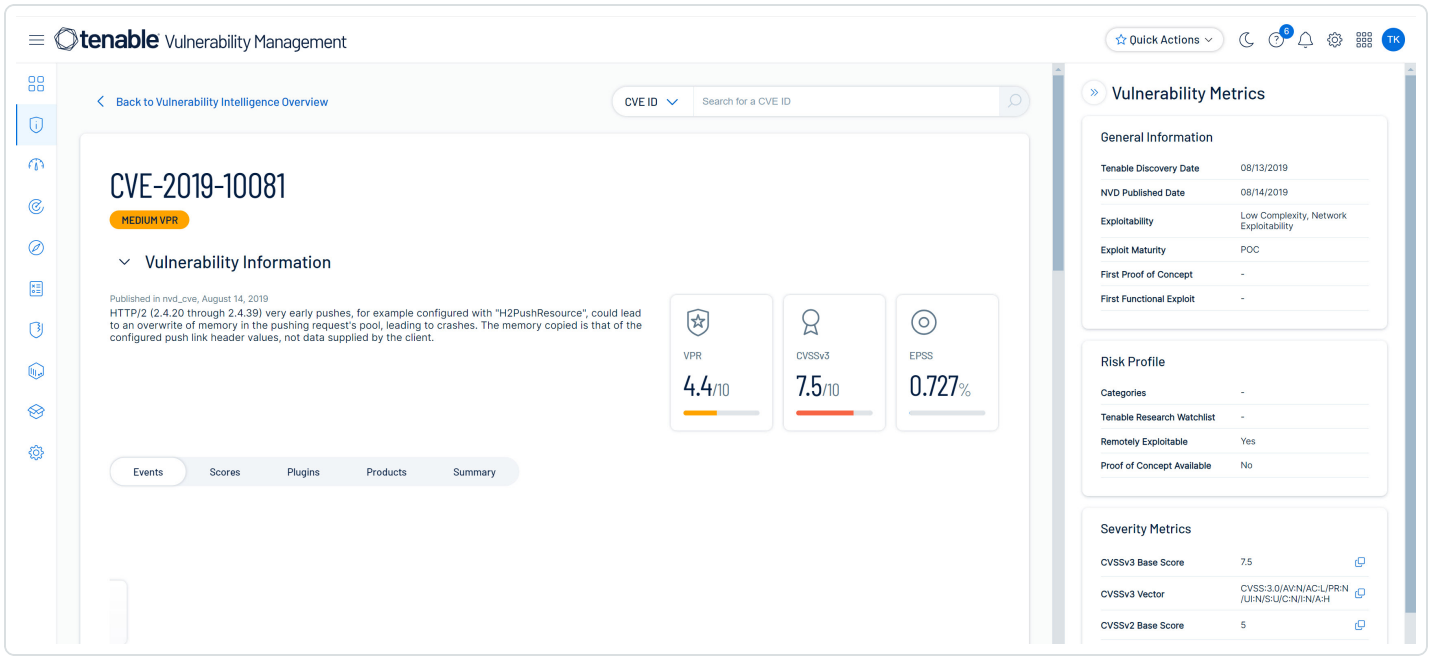
4. Click **Export**.

The system processes the export and the file downloads to your computer. If you close the page before the download completes, access the export file in **Settings** > **Exports**, in the **Activity** tab.

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 (CvSSv3), 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 (CVSSv3), and Exploit Prediction Scoring System (EPSS) scores.

It also contains tabs which allow you to delve further into your vulnerability data by viewing an event timeline, VPR and EPSS widgets, plugin details, known affected products, and more.

At the top of the section, you can:

- View a brief description of the vulnerability.
- View a tile that indicates the VPR of the vulnerability.
    - Click the ⌄ button to switch between viewing VPR and VPR (Beta) scores. For more information, see CVSS vs. VPR.

      Note: This toggle affects all data on the **Vulnerability Information** page.

      Tip: For more information, see the *Scoring Explained Quick Reference Guide*.
- View a tile that indicates the CVSS of the vulnerability.
    - Click the ⌄ button to switch between viewing CVSSv2 and CVSSv3 scores. For more information, see CVSS vs. VPR.

      Note: This toggle affects all data on the **Vulnerability Information** page.
- View a tile that indicates the EPSS (Exploit Prediction Scoring System) score of the vulnerability.

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.

Tip: Use the toggle in the upper-left corner of the timeline to switch between viewing VPR and VPR (Beta) data within the events timeline.

The timeline can contain the following events:

Event	Description
Discovery Date	When Tenable first observed the vulnerability.
NVD Published	When the National Vulnerability Database (NVD) disclosed the vulnerability.
First Tenable Coverage	The first time Tenable provided coverage for the vulnerability.
First Proof of Concept	When Tenable first observed a proof of concept for the vulnerability.
First Functional Exploit	When the first functional exploit for the vulnerability was released.
Consec Plugin Published	Indicates that a new Container Security Scanner plugin for the vulnerability is available.
LCE Plugin Published	Indicates that a new Log Correlation Engine plugin for the vulnerability is available.
Nessus Plugin Published	Indicates that a new Tenable Nessus plugin for the vulnerability is released.
NNM Plugin Published	Indicates that a new Tenable Network Monitor plugin for the vulnerability is available.
WAS Plugin Published	Indicates that a new Tenable Web App Scanning plugin for the vulnerability is available.

Ransomware	When Tenable first observed ransomware events for the vulnerability.
Malware	When Tenable first 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 when Tenable observes that the vulnerability is being persistently exploited.
CISA Known Exploits	When the Cybersecurity and Infrastructure Security Agency (CISA) added the vulnerability to their Known Exploited Vulnerabilities catalog.
CISA Due-Date	When federal agencies must fix vulnerabilities on the CISA Known Exploited Vulnerabilities (KEV) list.
Cyber Exposure Alert	Appears when Tenable publishes a Cyber Exposure Alert for the vulnerability.
EPSS Increased	Appears when the Exploit Prediction Scoring System (EPSS) increases.
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.
VPR Decreased	Appears when the VPR decreases.
VPR Assigned	Appears when a VPR score is assigned.
VPR (Beta) Increased	Appears when the Vulnerability Priority Rating (VPR) Beta increases.
VPR (Beta) Decreased	Appears when the VPR (Beta) decreases.
VPR (Beta) Assigned	Appears when a VPR (Beta) score is assigned.

Scores

The **Scores** tab contains ring charts for VPR, VPR (Beta) and EPSS along with trend charts to track how these scores have changed over time. Additionally, you can compare your score data across two points in the **Key Drivers** sections to the left of the charts.

On the **Scores** tab, you can:

- Hover over a point on the graph to see the score on that date.
- Click a point on the graph to update the data comparison in the **Key Drivers** sections.
- View the following **VPR Key Drivers**:

VPR Driver	Description
Age of Vulnerability	The number of days since the vulnerability was discovered.
CVSSv3 Impact Score	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	The relative number of unique products affected. Values are **Low**, **Medium**, **High**, or **Very High**.
Threat Intensity	The number and frequency of recent threat events. Values are **Very Low**, **Low**, **Medium**, **High**, or **Very High**.
Threat Sources	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	The number of days since a threat event occurred, from 0-180.

- View the following **VPR (Beta) Key Drivers**:

VPR Driver	Description

Exploit Chain	Indicates whether the vulnerability is present as part of an exploit chain.
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.
In the News, Intensity Last 30 days	Indicates whether the vulnerability has a high volume or frequency of media mentions in the last 30 days.
In the News Recency	Indicates whether recent media attention is a significant factor in the VPR (Beta) score.
In the News Sources Last 30 days	Indicates whether the is affected by the number or variety of news sources reporting on it within the last 30 days.
Malware Observations Intensity Last 30 days	Indicates whether the vulnerability has a significant volume of associated malware observations in the last 30 days.
Malware Observations Recency	Indicates whether the vulnerability is influenced by very recent observations of associated malware.
Score	The numerical Vulnerability Priority Rating (Beta) score value.
On CISA KEV	Indicates whether the vulnerability is listed on the CISA Known Exploited Vulnerabilities list.
Targeted Industries	Indicates whether the vulnerability is driven by evidence of targeting specific industries.
Targeted Regions	Indicates whether the vulnerability is part of active exploitation observed in particular geographic regions.
VPR Percentile	The vulnerability's VPR (Beta) score percentile ranking, indicating

	its position relative to other vulnerabilities.
VPR Severity	where the overall severity categorization of the VPR (Beta) for the vulnerability, for example, **Critical**, **High**, **Medium**, **Low**, or **Info**.

Plugins

The **Plugins** tab lists plugins that detected findings for the vulnerability. From the **Source** drop-down, choose between **Tenable Web App Scanning** and **Tenable Nessus**.

Column	Description
Plugin ID	The ID of the Tenable plugin that detected the finding.
Name	The name of the Tenable plugin that detected the finding.
Family	The type of plugin. 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	The severity of the vulnerability as **Low**, **Medium**, or **High**.

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. To view only your affected products, go to How Does This Affect Me.

Summary

In the **Summary** tab, view a summary and **Copy** it to your clipboard.

Threat Summary (Beta)

In the **Threat Summary** tab, view a summary of the threats associated with the vulnerability and **Copy** it to your clipboard.

Remedation Summary (Beta)

In the **Remediation Summary** tab, view a summary of the remediation steps you can take to mitigate the vulnerability 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 Customize Tables.

Column	Description
Asset ID	The asset's Universally Unique Identifier (UUID).
Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.
IPv4 Address	The IPv4 address for the affected asset.
IPv6 Address	The IPv6 address for the affected asset.
Vulnerabilities	A heatmap of the asset's vulnerabilities, color coded by severity. This column also lists the number of vulnerabilities.
ACR	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10.
ACR (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset-Criticality Rating* using a new algorithm based on asset profile, which assigns assets to classes by business and device function. This metric rates the importance of an asset to your organization from 1 to 10,

	with higher numbers for more critical assets. For more information, see Scoring and Asset Criticality Rating.
AES	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Exposure Score as an integer from 0 to 1000.
AES (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset Exposure Score* using a new algorithm. This metric weighs an asset's Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) and then assigns a number from 1 to 1000, with higher numbers for more exposed assets. For more information, see Scoring (Beta).
Tags	Any asset tags applied to the affected asset.

Affected Products

The table of results in the **Affected Products** tab has the following columns.

Column	Description
Product	The name of the affected product, using Common Platform Enumeration (CPE). For example, *cpe:/a:apache:httpd*. If multiple products are affected, click the link to view a complete list.
Plugin Name	The name of the Tenable plugin that detected a finding.
Findings	The number of findings affected by the vulnerability relating to that product. Click the number to view more information on the **Findings** workbench grouped by **None**.
Assets Affected	The number of assets with active findings relating to that product. Click the number to open that result on the **Findings** workbench grouped by **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	The date Tenable first discovered the vulnerability.
NVD Published Date	The date that the National Vulnerability Database (NVD) added the vulnerability.
Exploitability	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	The date the first proof of concept for the vulnerability was released.
First Functional Exploit	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	The categories a 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	If the vulnerability can be exploited from a remote network.
Proof of Concept Available	If Tenable has identified a proof of concept for this vulnerability.
Zero Day	**Yes** - This vulnerability was originally identified as a zero-day vulnerability. This value displays **Yes** even if a fix was made available after the vulnerability was publicized. **No** - This vulnerability has a publicly available fix that existed before the vulnerability was publicly disclosed or known to be exploited.

Severity Metrics

In the **Severity Metrics** section, view Common Vulnerability Scoring System (CVSS) v3 or CVSSv2 scores, depending on which are available, along with their vector strings.

Field	Description
CVSSv4 Base Score	The CVSSv4 score. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
CVSSv4 Vector	A vector string with the values used to calculate the CVSSv4 score, for example: *CVSS:4.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H*. To learn more, see this CVSSv4 calculator on the FIRST website.

CVSSv3 Base Score	The CVSSv3 score. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
CVSSv3 Vector	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 this CVSSv3 calculator on the FIRST website.
CVSSv2 Base Score	The CVSSv2 score. When not available from NVD, Tenable determines this score.
CVSSv2 Vector	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	The release date of the newest Tenable Nessus plugin to identify the vulnerability.
Web App Scanning	The release date of the newest Tenable Web App Scanning 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. Or, to search all vulnerabilities, click the default category to deselect it.

   In the **CVEs** tab on the lower area of the page, a table of results appears.

3. (Optional) Use the Query Builder to refine the results.

4. (Optional) Click a vulnerability row.

   The **Vulnerability Intelligence Profile** page 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 **Findings workbench** 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 **Findings workbench** 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.

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.

> **Tip**: Select the checkbox to only show CVEs affecting your assets.

The table in the **CVEs** tab has the following columns, which you can show or hide as described in Customize Tables.

Column	Description
CVE ID	The Common Vulnerability and Exposure (CVE) identifier for the vulnerability, as assigned by the CISA-sponsored CVE Program.
Common Name	The informal name of the vulnerability (for example, *Log4Shell*). Not all vulnerabilities have a common name.
VPR	The VPR score for the vulnerability. This Vulnerability Priority Rating (VPR) score is calculated by Tenable and ranges from 0.1 to 10.
VPR (Beta)	The VPR (Beta) score for the vulnerability. This updated version of your Vulnerability Priority Rating (VPR) score is calculated by Tenable and ranges from 0.1 to 10.
CVSSv2	The CVSSv2 score for the vulnerability. When not available from NVD, Tenable determines this score. To learn more, see CVSS vs. VPR.
CVSSv3	The CVSSv3 score for the vulnerability. When not available from NVD, Tenable determines this score.
CVSSv4	The CVSSv4 score for the vulnerability. When not available from NVD, Tenable determines this score.
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.
EPSS	The likelihood that the vulnerability will be actively exploited, based on the third-party Exploit Prediction Scoring System (EPSS).

First Discovered	When the vulnerability was first identified.
First Exploited	The date of the vulnerability's first-known exploitation.
First PoC	When the vulnerability's first proof of concept was discovered.
Zero Day	**Yes** - This vulnerability was originally identified as a zero-day vulnerability. This value displays **Yes** even if a fix was made available after the vulnerability was publicized. **No** - This vulnerability has a publicly available fix that existed before the vulnerability was publicly disclosed or known to be exploited.
Plugins	The IDs for the Tenable plugins that detected the vulnerability.

Affected Assets

In any row, click the drop-down **>** to reveal a table of assets on which that CVE appears, with the following columns.

Column	Description
Asset Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.
Operating System	The operating system running on the asset, for example *Linux Kernel 3.13*.
IPv4 Address	The IPv4 address for the asset.
IPv6 Address	The IPv6 address for the asset.
Plugin Count	The number of plugins that identified the CVE on the asset.
ACR	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10.
AES	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Exposure Score as an integer from 0 to 1000.

Last Seen	The date when the asset last appeared on a scan.
Source	The scanner or sensor that identified the finding, for example *Nessus network-based assessment*.
Tags	Any asset tags you applied in Tenable Vulnerability Management.

My Findings

On the **Vulnerability Intelligence Overview** page, the **My Findings** tab shows all active, new, or resurfaced findings 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.

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	The name of the Tenable plugin that detected the finding.
Plugin ID	The ID of the Tenable plugin that detected the finding.
Affected Assets	The number of affected assets. Click the number to open the Asset Details page.
CVSSv3	The Common Vulnerability Scoring System (CVSS) v3 score for the finding.
CVSSv4	The Common Vulnerability Scoring System (CVSS) v4 score for the finding. When not available from NVD, Tenable determines this score.

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 the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.
IPv4 Address	The IPv4 address for the asset.
IPv6 Address	The IPv6 address for the asset.
ACR	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10.
AES	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Exposure Score as an integer from 0 to 1000.
Last Seen	The date when the asset last appeared on a scan.
Tags	Any asset tags applied in Tenable Vulnerability Management.

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, or add tags to provide business context.

The **My Affected Assets** tab has the following columns.

Column	Description
Name	The name of the asset.
IPv4 Address	The IPv4 address for the asset.
IPv6 Address	The IPv6 address for the asset.
Plugin Count	The number of Tenable plugins that identified findings on the asset. Click the number to review details on the **Findings** workbench.

ACR	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10.
AES	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Exposure Score as an integer from 0 to 1000.
Tags	Any asset tags for 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	The vulnerability's severity based on the Common Vulnerability Scoring System (CVSS).
Plugin Name	The name of the Tenable plugin that detected the finding.
Plugin ID	The ID of the Tenable plugin that detected the finding.
Findings	The number of findings detected on the asset.
CVSSv3	The CVSSv3 score for the finding.

Tag Affected Assets

On the **Vulnerability Intelligence** page in the **My Affected Assets** tab, the **Tags** column shows all asset tags for your assets. You can add or remove these tags using the steps below.

Add Tags to an Asset

To add tags to an asset:

1. In the left navigation, click **Vulnerability Intelligence**.

   The **Vulnerability Intelligence Overview** page appears.

2. On the lower part of the page, click **My Affected Assets**.
3. In **My Affected Assets**, select the assets to tag.
4. In the blue bar, click **Add Tags**.

   The **Add Tags** dialog appears.

5. In the **Add Tags** dialog, do one of the following:

   Add new tags...

   a. In the two text boxes, type a tag *category* and *value* (for example, *Location: Headquarters*).

   b. After you type the value, in the drop-down that appears, click **Create**.

      The tag appears in the **Tags to be Added** section.

   c. (Optional) Add more tags as needed.

   Add recently used tags...

   a. In the **Recently Used Tags section**, click a tag.

      The tag appears in the **Tags to be Added** section.

   b. (Optional) Add more tags as needed.

6. Click **Add Tags**.

   The system adds the tag or tags to the assets.

Remove Tags from an Asset

To remove tags from an asset:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Vulnerability Intelligence**.

   The **Vulnerability Intelligence Overview** page appears.

3. On the lower part of the page, click **My Affected Assets**.

4. In **My Affected Assets**, select the assets to remove tags from.

5. In the blue bar, click **Remove Tags**.

   The **Remove Tags** dialog appears.

6. In the **Remove Tags** dialog and the **Current Tags** section, click the tag or tags to remove.

7. Click **Remove Tags**.

   The system removes the tag or tags from the assets.

Export Findings or Assets

On the **Vulnerability Intelligence** page, you can export results from the **My Findings** and **My Affected Assets** tabs in JSON or CSV format.

To export a finding or asset:

1. In the left navigation, click **Vulnerability Intelligence**.

   The **Vulnerability Intelligence Overview** page appears.

2. Refine the results that appear in the table on the lower area of the page, as described in Identify Your Exposure.

3. In **My Findings** or **My Affected Assets**, select the items to export.

   > **Note**: You export different items from the **Findings** and **Affected Assets** tabs:

- **My Findings** – In the main table, export findings. In the drop-downs **>**, export the assets that those findings appear on.
- **My Affected Assets** – In the main table, export assets. In the drop-downs **>**, export plugin results for those assets.

4. In the blue bar, depending on the items to export, click **Export Findings**, **Export Affected Assets**, or **Export Plugins**.

   The **Export** dialog appears.

5. In the **Export** dialog, select **JSON** or **CSV** and click **Export**.

   The system logs your request to the **Exports** page and the file downloads to your computer.

Note: If you request a large export and then leave the **Vulnerability Intelligence** page before it is processed, you must manually download the file from the **Exports** page.

Vulnerability Intelligence Filters

On the **Vulnerability Intelligence** page and the **Vulnerability Profile** page, use the Query Builder to refine your results and show only the CVEs, findings, or affected assets you want to take action on.

The following table lists the filters you can use.

Filter	Description
ACR	The Tenable-defined Asset Criticality Rating (ACR) as a number from 1 to 10.
AES (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset Exposure Score* using a new algorithm. This metric weighs an asset's Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) and then assigns a number from 1 to 1000, with higher numbers for more exposed assets. For more information, see Scoring (Beta).
AES	The Tenable-defined Asset Exposure Score (AES) as a number from 0 to 1000.
ACR (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset-Criticality Rating* using a new algorithm based on asset profile,

	which assigns assets to classes by business and device function. This metric rates the importance of an asset to your organization from 1 to 10, with higher numbers for more critical assets. For more information, see Scoring and Asset Criticality Rating.
Asset Name	The asset name, for example the IPv4 address *206.206.136.40*.
Category	The category of the vulnerability, as described in Vulnerability Categories.
Common Name	A vulnerability's common name, for example *Log4Shell*. Not all vulnerabilities have a common name.
CVE ID	The Common Vulnerabilities and Exposures (CVE) ID, for example *CVE-2002-2024*.
CVSSv2 Base Score	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.
CVSSv3 Attack Complexity	The attack complexity, which defines how difficult it is to use a vulnerability in an attack. Options are **High** or **Low**.
CVSSv3 Attack Vector	The attack vector, which defines an attack's location. Options are **Adjacent**, **Network**, **Local**, or **Physical**.
CVSSv3 Availability	Quantifies the impact on the availability of the affected asset. Options are **High** (the asset is completely unavailable), **Low** (some reduced performance or interruption in availability), or **None** (no impact on the availability of the asset).
CVSSv3 Base Score	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.
CVSSv3 Confidentiality	The expected impact of the affected asset's information confidentiality loss. Options are **High**, **Low**, or **None**. For example, an affected asset with **High** confidentiality may have a catastrophic adverse effect on your organization or customers.

CVSSv3 Integrity	The expected impact of the affected asset's data integrity loss. Options are **High**, **Low**, or **None**.
CVSSv3 Privileges Required	The permission level attackers require to exploit the vulnerability. Options are **High**, **Low**, or **None**. For example, **None** means attackers need no permissions in your environment and can exploit the vulnerability while unauthorized.
CVSSv3 Scope	If a vulnerability allows attackers to compromise resources beyond an affected asset's normal authorization privileges. Options are **Unchanged** or **Changed**. For example, **Changed** means the vulnerability increases the affected asset's privileges.
CVSSv3 User Interaction	If a vulnerability requires other users (such as end users) for attackers to be able to use it. Options are **Required** or **None**. **None** is more severe since it means no additional user interaction is required.
EPSS Score	The percentage likelihood that a vulnerability will be exploited, based on the third-party Exploit Prediction Scoring System (EPSS). Type a number from 0 to 100 with up to three decimal places, for example, *75.599*.
Exploit Maturity	The exploit maturity based on sophistication and availability. This information is drawn from Tenable's own research as well as key external sources. Options are **High**, **Functional**, **PoC**, or **Unproven**.
First Discovered	The date the vulnerability corresponding to a finding was first identified.
First Functional Exploit	The date a vulnerability was first known to be exploited.
First Proof of Concept	The date a vulnerability's first proof of concept was found.
Plugin ID	The ID of the Tenable plugin that detected the vulnerability, for example *157288*. To look up plugin IDs, go to the Tenable website.
Plugin Name	The name of the Tenable plugin that detected the vulnerability, for example *TLS Version 1.1 Protocol Deprecated*.

Plugins Available	If a vulnerability currently has a Tenable plugin that detects it. Options are **Yes** or **No**.
Tags	Tags on your affected assets. To learn more, see Tags.
VPR	The Tenable-calculated Vulnerability Priority Rating (VPR) score, as a number from 1 to 10. This score is based on the VPR of the plugin that identified the vulnerability. When plugins are associated with multiple vulnerabilities, the highest VPR appears.
VPR Threat Intensity	A vulnerability's Tenable-calculated threat intensity based on the number and frequency of threat events. Options are **Very Low**, **Low**, **Medium**, **High**, or **Very High**.
Weaponization	If a vulnerability is judged to be ready for use in a cyberattack. Options are **Advanced Persistent Threat**, **Botnet**, **Malware**, **Ransomware**, or **Rootkit**.
Zero Day	**Yes** - This vulnerability was originally identified as a zero-day vulnerability. This value displays **Yes** even if a fix was made available after the vulnerability was publicized. **No** - This vulnerability has a publicly available fix that existed before the vulnerability was publicly disclosed or known to be exploited.

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.
Top 50 VPR	The top 50 vulnerabilities by Vulnerability Priority Rating (VPR).
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.
Ransomware	Vulnerabilities used in current or historical ransomware attacks, as determined from evidence gathered by the Tenable Research team.
Recently Exploited	Vulnerabilities with notable coverage in the press over the past 30 days, and for which Tenable has evidence of active exploitation.
In the News	Vulnerabilities being widely reported in the press with notable coverage over the past 30 days.

Exposure Response

In the **Exposure Response** section, you create *initiatives*, which are projects to address vulnerabilities in your environment.

In initiatives, you track specific findings using combinations and apply asset tags to choose the assets in scope. Then, you assign initiatives to your team, set SLAs, and measure progress through remediation scan results.

As a Tenable administrator, you use the **Exposure Response** section to create, assign, and report on all initiatives. As a initiative owner, you only see and work with your initiatives.

The following topics explain how to use these tools to create, manage, review, and report on initiatives.

- Create Initiatives
- Edit or Delete Initiatives
- Review Initiatives
- View the Combination Timeline
- Manage Combinations
- Use Report Cards

Create Initiatives

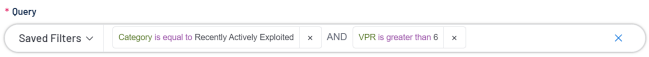
In the **Exposure Response** section, your first step is creating an initiative. To do this, add the initiative, define the scope with asset tags, assign an owner, and choose an SLA. Then, add combinations to define the vulnerabilities to track.

> **Note**: As a Tenable administrator, you can assign initiatives to other users. As a non-administrator, you can only create initiatives for yourself. As either type of user, you can create up to ten initiatives.

Example Initiative

To address recently exploited vulnerabilities on your Headquarters network, you might create an initiative as follows:

- **Name** – Recently exploited vulnerabilities at HQ
- **Asset Scope** – Network: HQ
- **Owner** – user@myorganization.com
- **Remediate Within** – 7 days
- **Combinations** – Category is equal to Recently Actively Exploited AND VPR is greater than 6



Before You Begin

Before you create an initiative:

- **Create asset tags** – Initiatives use asset tags to define the assets in scope.
- (Optional) **Create custom combinations** – If you plan to use custom combinations, create them.

Create a New Initiative

To create a new initiative:

1. In the left navigation, click **Exposure Response**.

   The **Exposure Response** page appears.

2. In **My Initiatives**, click **New**.

   The **Create New Initiative** pane appears.

3. Set the following options.

Option	Description
Name	Type a name for the initiative.
Description	Type a description for the initiative, for example *Reduce my external attack surface*.

Owner	Select the initiative owner from a list of Tenable Vulnerability Management users. You cannot reassign initiatives once created. **Note**: Only administrators and initiative owners can view initiatives.
Asset Scope	Choose up to ten tags to define which assets in your environment are in scope. Search for and select tags to assign, for example *Priority: High* or *Software: Oracle*.
Remediate Within	Choose an SLA by which all findings must be remediated. For example, to set an SLA of one week, enter *7*.

4. Under **Assign Combinations**, add up to ten combinations from the following tabs.

Tab	Description
My Combinations	Your personal combinations, which only you can view. You cannot assign personal combinations to initiatives you do not own.
Shared	Organization-wide combinations, which anyone can view or use and which your administrators and the combination owners can update. Updates may change the resources in your initiative. Track updates in the Combination Timeline.
Tenable	Predefined combinations from the Tenable Research Team. These may be updated infrequently, which can change the resources in your initiatives. Track updates in the Combination Timeline.

Note: Initiatives can contain no more than *17* queries across all combinations. For example, if you add four combinations to an initiative—and the combinations have five queries each for a total of 20, a warning appears and you cannot save the initiative.

Note: Initiatives with multiple combinations use a logical OR filter. The data displayed will include all results from each of the individual combinations.

5. Click **Save**.

   The initiative appears in the **My Initiatives** panel.

Edit or Delete Initiatives

You can edit initiatives that you own or have assigned. If you are a Tenable administrator, you can delete initiatives. This topic contains steps to complete both tasks.

Edit an Initiative

To edit an initiative:

1. In the left navigation, click **Exposure Response**.

   The **Exposure Response** page appears.

2. In **My Initiatives**, click ⋮ in the upper-right corner of the initiative.
3. In the menu that opens, click **Edit**.
4. The **Edit Initiative** panel appears.

   Edit the initiative settings, as described in Create Initiatives.

   > **Note**: You cannot edit an initiative's owner, since the system calculates initiative metrics based on the owner's Tenable permissions.

5. Click **Save**.
6. The system saves the initiative.

Delete an Initiative

To delete an initiative:

1. In the left navigation, click **Exposure Response**.

   The **Exposure Response** page appears.

2. In **My Initiatives**, click ⋮ in the upper-right corner of the initiative.
3. In the menu that opens, click **Delete**.
4. In the box that appears, click **Delete** again.

   The system permanently deletes the initiative.

Review Initiatives

On the **Exposure Response** page, review initiatives that you own or have assigned in two sections:

- **My Initiatives** – On the left, view all your initiatives.

  > **Tip**: If you have assigned initiatives to others, Click **Append from Other Users** on the lower area to follow those initiatives in the **My Initiatives** panel.

- **Initiative Details** – Under My Initiatives, click an initiative to view details.

Initiative Details

The initiative details section contains four panels.

In this section	You can...
Findings on Assets	View a sunburst chart of all findings. In the chart, each segment shows the percentage of assets with a relevant finding, by asset tag or combination.
How Am I Doing?	View a dashboard with at-a-glance metrics and a line chart that tracks finding and remediation trends.
What's New?	View recently identified findings and affected assets.
My Findings and Affected Assets	View all findings and affected assets in two tabs. Refine the displayed items with a query builder and save or share the results.

Findings on Assets

In the **Findings on Assets** panel, view a sunburst chart containing findings and assets.

Reading the chart

You can view the the chart in two tabs as follows:

- **By Tag** – View the chart broken down by the ten asset tags in the initiative with the most findings.
- **By Combination** – View the chart broken down by the combinations used in the initiative.

> **Note**: Findings whose risk is accepted by an Accept rule are still included in Exposure Response initiatives.

In the chart, each segment shows the percentage of assets containing a tag or a combination. The segment is colored green, yellow, or red to indicate low, medium, or high. Click a segment to open a popup with more details.

In the following example, 100% of the initiative's assets match a combination that checks for ransomware, as shown in the top left area. Since all assets have ransomware, the segment is red.

How Am I Doing?

In the **How Am I Doing?** panel, view key metrics and an area chart which tracks initiative trends over time.

Key Metrics

At the top of the panel, the following metrics appear.

Metric	Description
Average Age of Vulnerabilities	View the average age of findings in the initiative. This metric is based on the dates that findings were first seen or when they resurfaced.
Average Time to Remediate	View the average time to fix findings since they were discovere on a scan. A finding is marked **Fixed** after being **Active**, **New**, or **Resurfaced**.
Percentage of Findings Remediated	View the percentage of fixed findings in the initiative, including all historic findings.

New Findings vs. Remediations

In the **New Findings vs. Remediations** graph, view the initiative's finding and remediation trends, which change over time as scans run and new assets are found or added.

Do one of the following:

- To change the date range, select **30 Days**, **60 Days**, **90 Days**, or **Custom**.
- To see more details for a date, in the graph, hover on that date.
- To see details about major events, below the graph, click an *event marker* to open an event card.

Event Cards

Below the chart, the following events can appear.

Metric	Description
Asset Count	Appears when the number of affected assets changes by more than 20%.
Combination Changes	Appears when Tenable modifies or removes combinations in the initiative
Finding Count	Appears when the total findings count changes by more than 20%.
Resurfaced Findings	Appears when the resurfaced findings count changes by more than 20%.

What's New?

In the **What's New** panel, view how an initiative has recently changed. This includes new findings, new affected assets, and new Common Vulnerabilities and Exposures (CVEs) that are now in scope based on the combinations used (for example, a CVE whose VPR increased).

Top New Plugins

In the **Top New Findings** table, view recent findings in the following columns.

Column	Description
VPR	Indicates the Vulnerability Priority Rating (VPR) for the finding.
Plugin	Indicates the plugin that identified the finding. Click a plugin name to view all findings related to that plugin in **My Findings**.
Last Seen	Indicates the date when the finding last appeared on a scan.

Top New Assets

In the **Top New Assets** table, view recent findings in the following columns.

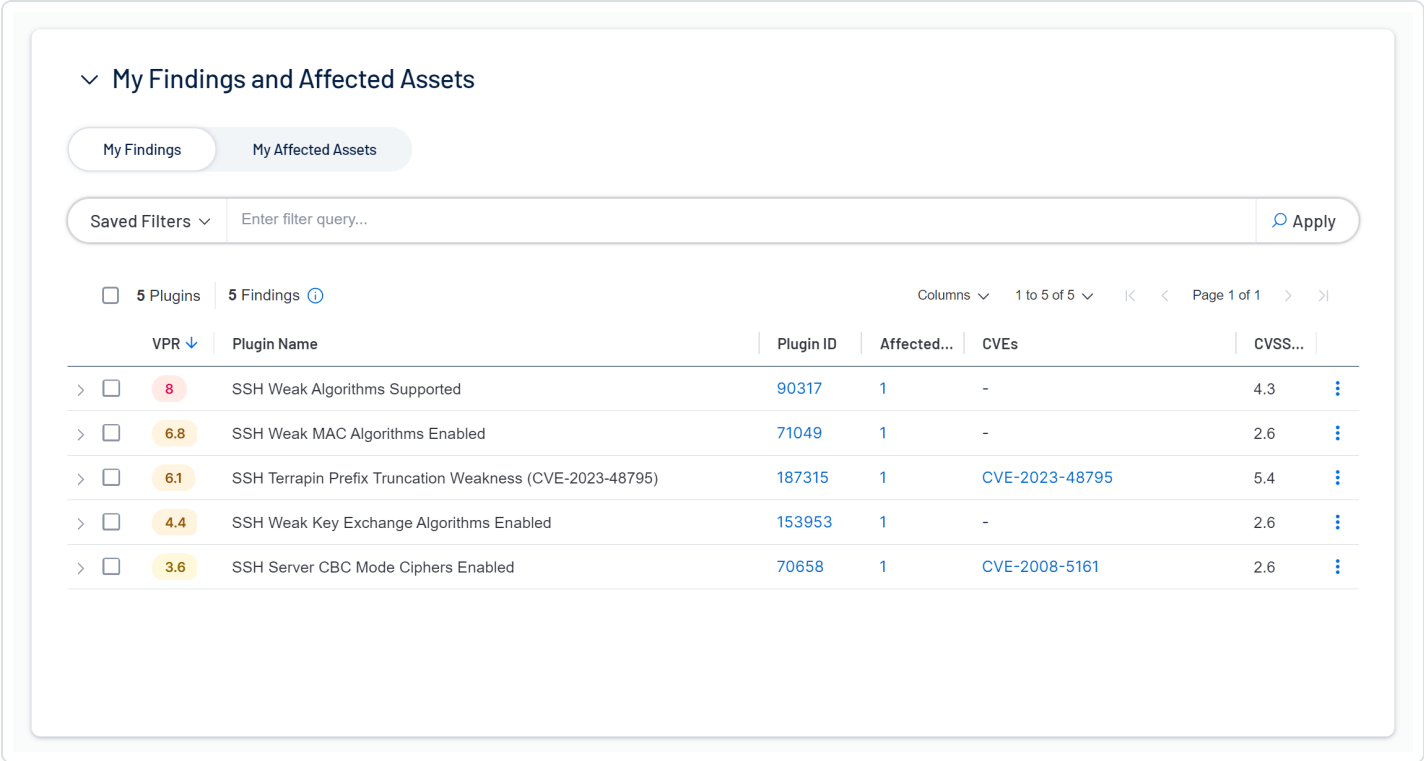
Column	Description
Asset Name	Indicates the name of the affected asset. Click an asset name to view all results for that Asset ID in **My Affected Assets**.
Findings	Indicates the number of findings on the asset.
Last Seen	Indicates the date when the asset last appeared on a scan.

Latest Combination Changes

In the **Latest Combination Changes** section, view CVEs recently found by the combinations in the initiative. Click a CVE to view it on the **Vulnerability Profile** page.

My Findings and Affected Assets

In the **Findings and Affected Assets** panel, view findings and affected assets in two tabs. Filter the items in each tab with the Query Builder, save queries, and export lists of resources.



Note: Findings whose risk is accepted by an Accept rule are still included in Exposure Response initiatives.

To learn more, see the following topics.

Topic	Description
Export from Exposure Response	Export lists of findings or affected assets to CSV or JSON.
Tag Affected Assets	Tag assets so they appear in initiatives.
My Findings	View all active, new, and resurfaced findings in an initiative.
My Affected Assets	View all affected assets in an initiative.

Export from Exposure Response

On the **Exposure Response** page, you can export results from both the **My Findings** and **My Affected Assets** tabs in CSV or JSON format.

To export a finding or affected asset:

1. In the left navigation, click **Exposure Response**.

   The **Exposure Response** page appears.

2. On the lower part of the page, click **My Findings** or **My Affected Assets**.

3. Select the items to export.

   > **Note**: You export different items from the **My Findings** and the **My Affected Assets** tabs:
   >
   > - **My Findings** – In the main table, export findings. In the drop-downs **>**, export the assets that those findings appear on.
   > - **My Affected Assets** – In the main table, export assets. In the drop-downs **>**, export plugin results for those assets.

   > **Tip**: To select *all* items, in the blue bar above the items to export, click the checkbox. Then, if your results span multiple pages, click **Select all**.

4. In the blue bar, depending on the items to export, click **Export Findings** or **Export Affected Assets**.

   The **Export** dialog appears.

5. In the **Export** dialog, select **JSON** or **CSV** and click **Export**.

   The system processes your request. Once processed, a confirmation message appears and your browser saves the file to your computer. Tenable Vulnerability Management also logs your request to the **Exports** page.

   > **Note**: If you request a large export and then leave the page before it is processed, you must manually download the file from the **Exports** page.

Tag Affected Assets

On the **Exposure Initiatives** page in the **My Affected Assets** tab, the **Tags** column shows all asset tags for your assets. You can add or remove these tags using the following steps.

Add Tags to an Asset

To add tags to an asset:

1. In the left navigation, click **Exposure Response**.

   The **Exposure Response** page appears.

2. On the lower part of the page, click **My Affected Assets**.
3. In **My Affected Assets**, select the assets to tag.
4. In the blue bar, click **Add Tags**.

   The **Add Tags** dialog appears.

5. In the **Add Tags** dialog, do one of the following:

   Add new tags...

   a. In the two text boxes, type a tag *category* and *value* (for example, *Location: Headquarters*).

   b. After you type the value, in the drop-down that appears, click **Create**.

      The tag appears in the **Tags to be Added** section.

   c. (Optional) Add more tags as needed.

   Add recently used tags...

   a. In the **Recently Used Tags section**, click a tag.

      The tag appears in the **Tags to be Added** section.

   b. (Optional) Add more tags as needed.

6. Click **Add Tags**.

   The system adds the tags to the assets.

Remove Tags from an Asset

To remove tags from an asset:

1. In the left navigation, click **Exposure Response**.

   The **Exposure Response** page appears.

2. On the lower part of the page, click **My Affected Assets**.

3. In **My Affected Assets**, select the assets to remove tags from.

4. In the blue bar, click **Remove Tags**.

   The **Remove Tags** dialog appears.

5. In the **Remove Tags** dialog and the **Current Tags** section, click the tag or tags to remove.

6. Click **Remove Tags**.

   The system removes the tag or tags from the assets.

My Findings

In the **My Findings and Affected Assets** section, the **My Findings** tab shows all active, new, or resurfaced findings for that initiative. Refine the results with the Query Builder.

The **My Findings** tab has the following columns, which you can show or hide as described in Customize Tables.

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	Indicates the Common Vulnerability and Exposure (CVE) identifier for the finding, as assigned by the CISA-sponsored CVE Program.
CVSSv2	Indicates the Common Vulnerability Scoring System (CVSS) v2 score for the finding.
CVSSv3	Indicates the Common Vulnerability Scoring System (CVSS) v3 score for the finding.
CVSSv4	Indicates the Common Vulnerability Scoring System (CVSS) v4 score for the finding.

Affected Assets

In any findings row, click the drop-down **>** 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 the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.
Operating System	Indicates the operating system run on the asset, for example *Linux Kernel 3.13*.
IPv4 Address	Indicates the IPv4 address for the asset.
IPv6 Address	Indicates the IPv6 address for the asset.
Findings Count	Indicates the number of findings on the asset. Click the number to view details on the **Findings** workbench.
ACR	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10.
AES	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Exposure Score as an integer from 0 to 1000.
Last Seen	Indicates the date when the asset last appeared on a scan.

Source	Indicates the scanner or sensor that identified the finding, for example *Nessus network-based assessment*.
Tags	Lists any asset tags you applied in Tenable Vulnerability Management.

My Affected Assets

In the **My Findings and Affected Assets** section, the **My Affected Assets** tab shows all assets in the initiative with a finding that has not yet been fixed. Refine the results with the Query Builder or add tags to provide business context.

The **My Affected Assets** tab has the following columns, which you can show or hide as described in Customize Tables.

Column	Description
Name	Indicates the name of the asset.
Operating System	Indicates the operating system run on the asset, for example *Linux Kernel 3.13*.
IPv4 Address	Indicates the IPv4 address for the asset.
IPv6 Address	Indicates the IPv6 address for the asset.
Plugin Count	Indicates the number of Tenable plugins that identified findings on the asset. Click the number to review details on the **Findings** workbench.
ACR	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10.
ACR (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset-Criticality Rating* using a new algorithm based on asset profile, which assigns assets to classes by business and device function. This metric rates the importance of an asset to your organization from 1 to 10, with higher numbers for more critical assets. For more information, see Scoring and Asset Criticality Rating.
AES	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Exposure Score as an integer from 0 to 1000.

AES (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset Exposure Score* using a new algorithm. This metric weighs an asset's Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) and then assigns a number from 1 to 1000, with higher numbers for more exposed assets. For more information, see Scoring (Beta).
CVEs	Indicates the Common Vulnerability and Exposure (CVE) identifier for the finding on the asset, as assigned by the CISA-sponsored CVE Program.
Source	Indicates the scanner or sensor that identified a finding on the asset, for example *Nessus network-based assessment*.
Tags	Lists any asset tags for the asset.

Plugins

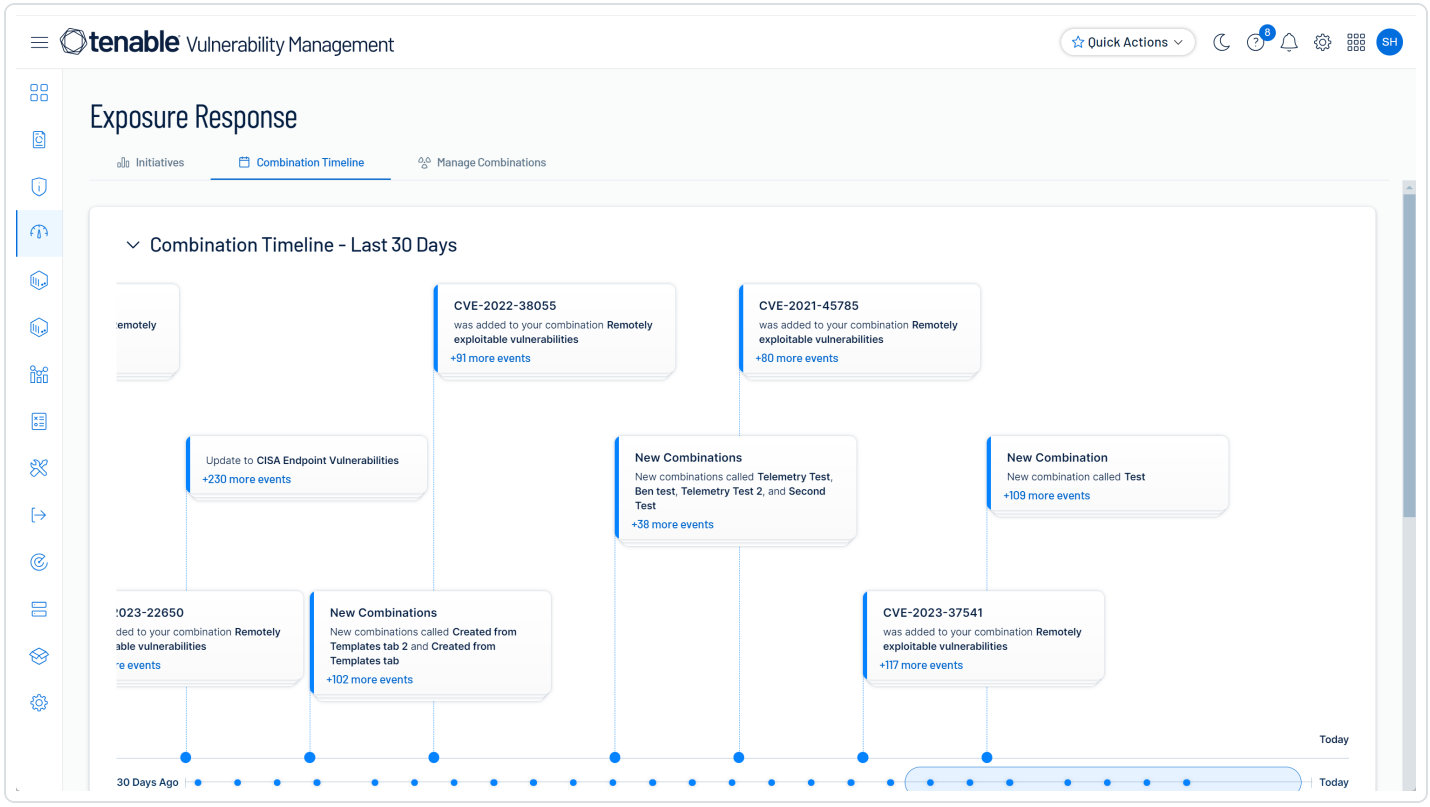
In any asset row, click the drop-down **>** to reveal a table of plugin results for the findings on that asset, with the following columns.

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.

View the Combination Timeline

In the **Combination Timeline** tab, you can view a 30-day timeline of combinations added to or removed from the initiatives you have access to. You can also view new combinations added by the Tenable research team.

- To view the **Combination Timeline**, in the left navigation, click **Exposure Response** > **Combination Timeline**.



On the lower area, in **Combinations with Updates**, view combinations edited in the past 30 days. You may want to do this when the data in one of your initiatives changes significantly, since editing combinations changes initiative data.

In the top-right corner of any combination, click ⋮ to open a menu where you can edit or delete the combination.

Note: Unless you are an administrator, you cannot delete a combination when it is the only one in an initiative. As an administrator, if you delete the only combination, its initiativestops updating.

Manage Combinations

When you create initiatives, you assign combinations to define what resources they track in your environment. Combinations use *queries* to search for specific findings. They work together with asset tags, which define the assets in scope.

You can use the query builder to create your own combinations, apply Tenable combinations, or combine the two. When you create combinations, you can save them as templates to share with your organization.

> **Note**: **Exposure Management** limits the number of combinations created:
>
> - 50 total combinations per user and
> - 100 total combinations per organization.

The following topics explain how to use combinations.

Topic	Description
Create Combinations	Create new combinations to add to initiatives.
Edit or Delete Combinations	Manage your current combinations.
Copy Shared Combinations	Copy combinations created by other users and then customize them.

Create Combinations

When you create initiatives, unless you want to use existing combinations, you must first create new ones in the **Manage Combinations** tab.

> **Note**: **Exposure Management** limits the number of combinations created:
>
> - 50 total combinations per user and
> - 100 total public combinations per organization.

To create new combinations:

1. In the left navigation, click **Exposure Response** > **Manage Combinations**.

   The **Exposure Response** page appears with the **Manage Combinations** tab open.

2. In the left panel, click ⊕ **New**.

   The **Create Combination** pane appears. It contains the following options.

Option	Description
Name	Type a combination name.
Description	Type a description, for example *High CvSS score*.
Query	In the query box, use the Query Builder to define what resources the combination searches for. For example, *CVSSv3 Base Score is greater than 6*. **Note**: For any combination, the system supports a maximum of *six* queries separated by operators.
Add to Initiatives	(Optional) Choose a current initiative in which to add the combination. **Note**: Initiatives with multiple combinations use a logical OR filter. The data displayed will include all results from each of the individual combinations.
Shared	(Optional) Enable this toggle to share the combination with your organization in the **Shared** tab.

3. Click **Save**.

   The combination appears in the left panel under **Personal** or **Shared**.

Edit or Delete Combinations

In the **Exposure Response** section, you can edit or delete combinations based on your Tenable user role and the combination status.

Edit a Combination

As an administrator, you can edit non-Tenable combinations. As a non-administrator, you can edit your combinations.

To edit a combination:

1. In the left navigation, click **Exposure Response** > **Manage Combinations**.

   The **Exposure Response** page appears with the **Manage Combinations** tab open.

2. In the left pane, in the combination to edit, click ⋮ and select **Edit**.

3. In the **Edit Combination** panel that appears, change the options.

   > **Note**: To remove a combination from a current initiative, edit the initiative instead.

4. Click **Save**.

   The system saves the combination.

Delete a Combination

As an administrator, you can delete non-Tenable combinations. As a non-administrator, you can delete your combinations in most cases.

Administrator	Non-administrator
You can delete any non-Tenable combination. **Note**: When a combination is the only data source for an initiative, deleting it pauses the initiative.	You can delete unshared combinations from **My Combinations**. You can delete **Shared** combinations that you created if they are not in use.

To delete a combination:

1. In the left navigation, click **Exposure Response**.

   The **Exposure Response** page appears.

2. Click **Manage Combinations**.

   The **Manage Combinations** tab appears.

3. In the left pane, in the combination to edit, click ⋮ and select **Delete**.

4. In the confirmation dialog that appears, click **Delete** again.

   The system deletes the combination.

Copy Shared Combinations

In the **Exposure Response** section, the **Shared** tab contains combinations shared by your organization. When you want to customize a combination that you did not create, you can copy it to **My Combinations** and then edit the copy.

To copy and edit a shared combination:

1. In the left navigation, click **Exposure Response** > **Manage Combinations**.

   The **Exposure Response** page appears with the **Manage Combinations** tab open.

2. In the left panel, click **Shared**.

3. In the left panel, click the template to copy and then, in the right panel, click **Copy to my combinations**.

   The system copies the shared combination.

Exposure Response Filters

In the **Exposure Response** section, use the Query Builder to view specific findings or affected assets or choose which vulnerabilities appear in a combination.

The following table lists the filters you can use. Not all filters appear in all sections.

Filter	Description
ACR	The Tenable-defined Asset Criticality Rating (ACR) as a number from 1 to 10.
AES	The Tenable-defined Asset Exposure Score (AES) as a number from 0 to 1000.
Asset ID	The UUID of the asset. This value is unique to Tenable Vulnerability Management.
Asset Name	The asset name, for example the IPv4 address *206.206.136.40*.

Filter	Description
Category	The vulnerability category, which the **Vulnerability Intelligence** features also use. To learn more, see Vulnerability Categories.
Common Name	The vulnerability's common name, for example *Log4Shell*. Not all vulnerabilies have a common name.
CVE ID	The Common Vulnerabilities and Exposures (CVE) ID, for example *CVE-2002-2024*.
CVSSv2 Base Score	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.
CVSSv3 Attack Complexity	The attack complexity, which defines how difficult it is to use a vulnerability in an attack. Choose from **High** or **Low**.
CVSSv3 Attack Vector	The attack vector, which defines an attack's location. Choose from **Adjacent**, **Network**, **Local**, or **Physical**.
CVSSv3 Availability	The affected asset's availability. Choose from **High**, **Low**, or **None**. For example, an affected asset with *High* is completely unavailable.
CVSSv3 Base Score	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.

Filter	Description
	VPR.
CVSSv3 Confidentiality	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.
CVSSv3 Integrity	The expected impact of the affected asset's data integrity loss. Choose from **High**, **Low**, or **None**.
CVSSv3 Privileges Required	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.
CVSSv3 Scope	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.
CVSSv3 User Interaction	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.
CVSSv4 Attack	The conditions beyond the attacker's

Filter	Description
Complexity (AC)	control that must exist to exploit the vulnerability.
CVSSv4 Attack Requirements (AT)	The resources, access, or specialized conditions required for an attacker to exploit the vulnerability.
CVSSv4 Attack Vector (AV)	The context where vulnerability exploitation is possible, such as **Network** or **Local**.
CVSSv4 Base Score	A numeric value between 0.0 and 10.0 that represents the intrinsic characteristics of a vulnerability independent of any specific environment.
CVSSv4 Privileges Required (PR)	The level of privileges an attacker must possess to exploit the vulnerability.
CVSSv4 Subsequent System Availability Impact (VA)	The impact on the availability of systems that can be impacted after the vulnerable system is exploited.
CVSSv4 Subsequent System Confidentiality Impact (SC)	The impact on the confidentiality of systems that can be impacted after the vulnerable system is exploited.
CVSSv4 Subsequent System Integrity Impact (SI)	The impact on the integrity of systems that can be impacted after the vulnerable system is exploited.
CVSSv4 User Interaction	The level of user involvement required for an attacker to exploit the vulnerability.
CVSSv4 Vulnerable	The impact on the availability of the

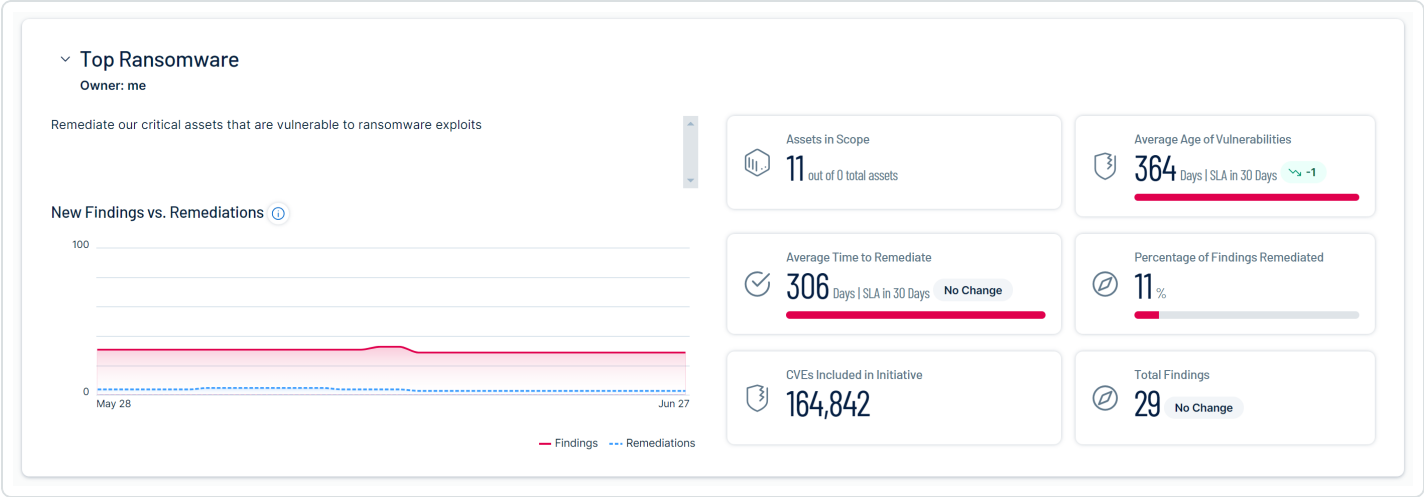
Filter	Description
System Availability Impact	vulnerable system when successfully exploited.
CVSSv4 Vulnerable System Confidentiality Impact (VC)	The impact on the confidentiality of the vulnerable system when successfully exploited.
CVSSv4 Vulnerable System Integrity Impact (VI)	The impact on the integrity of the vulnerable system when successfully exploited.
EPSS Score	The percentage likelihood that a vulnerability will be exploited, based on the third-party Exploit Prediction Scoring System (EPSS). Type a number from 0 to 100 with up to three decimal places, for example, *75.599*.
Exploit Maturity	The exploit maturity based on sophistication and availability. This information is drawn from Tenable's own research as well as key external sources. Options are **High**, **Functional**, **PoC**, or **Unproven**.
First Seen	The date when a scan first found the vulnerability on an asset.
First Functional Exploit	The date a vulnerability was first known to be exploited.
First Proof of Concept	The date a vulnerability's first proof of concept was found.
IPv4 Address	Affected asset IPv4 addresses as a

Filter	Description
	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*.
IPv6 Address	Affected asset IPv6 addresses as a single IP, an IP range, or an IP Classless Inter-Domain Routing (CIDR) block. For example, type *::ffff:c0a8:102*.
Last Seen	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.
Plugins Available	If a vulnerability currently has a Tenable plugin that detects it. Options are **Yes** or **No**.
Plugin ID	The ID of the Tenable plugin that detected the vulnerability, for example *157288*. To look up plugin IDs, go to the Tenable website.
Plugin Name	The name of the Tenable plugin that detected the vulnerability, for example *TLS Version 1.1 Protocol Deprecated*.
Resurfaced Date	The most recent date that a scan detected a Resurfaced vulnerability which was previously Fixed. If a vulnerability is Resurfaced multiple times, only the most recent date appears.

Filter	Description
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.
Tags	Filter by tags on affected assets by choosing them from a list. To learn more, see Tags.
VPR	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.
VPR Threat Intensity	A vulnerability's Tenable-calculated threat intensity based on the number and frequency of threat events. Choose from **Very Low**, **Low**, **Medium**, **High**, or **Very High**.
Vuln SLA Date	The date that the finding was last activated. It equals either the **First Seen** date when the finding is new or active or the **Resurfaced Date** if the finding is resurfaced.
Weaponization	Whether a vulnerability is judged to be ready for use in a cyberattack. Choose from **Advanced Persistent Threat**, **Botnet**, **Malware**, **Ransomware**, or **Rootkit**.

Use Report Cards

In the **Exposure Response** section of Tenable Vulnerability Management, you can view dashboard-style reports about the initiatives you have access to and export them to PDF.



View Report Cards

To view report cards:

1. In the left navigation, click **Exposure Response**.

   The **Exposure Response** page appears.

2. In the left panel, click **Create Report Card**.

3. The **Initiatives Report Card** page appears with cards for all the initiatives you can access.

4. (Optional) In the top-right corner, choose a date range.

Read Report Cards

Report cards contain the following sections.

Section	Description
Owner	Indicates the owner, chosen during initiative creation. You cannot reassign initiatives to other owners.
New Findings vs. Remediations	Indicates the findings and remediations as they have trended during the selected date range.

Assets in Scope	Indicates the assets tracked by the initiative when compared to all assets in your environment.
Average Time to Remediate	Indicates the average time in days to fix findings since they were identified on a scan and a countdown to the SLA.
CVEs Included in Initiative	Indicates the total number of vulnerabilities being tracked.
Average Age of Vulnerabilities	Indicates the average age of unfixed vulnerabilities and a countdown to the SLA.
Percentage of Findings Remediated	Indicates the percentage of remediated findings, as indicated by your scans.
Total Findings	Indicates the total number of active, new, or resurfaced findings in the initiative.

Export Report Cards

To export all your report cards:

1. In the left navigation, click **Exposure Response**.

   The **Exposure Response** page appears.

2. In the left pane, click **Create Report Card**.

   The **Initiatives Report Card** page appears.

3. In the top-right corner, click **Export**.

   The system downloads the report cards to your computer in a single PDF.

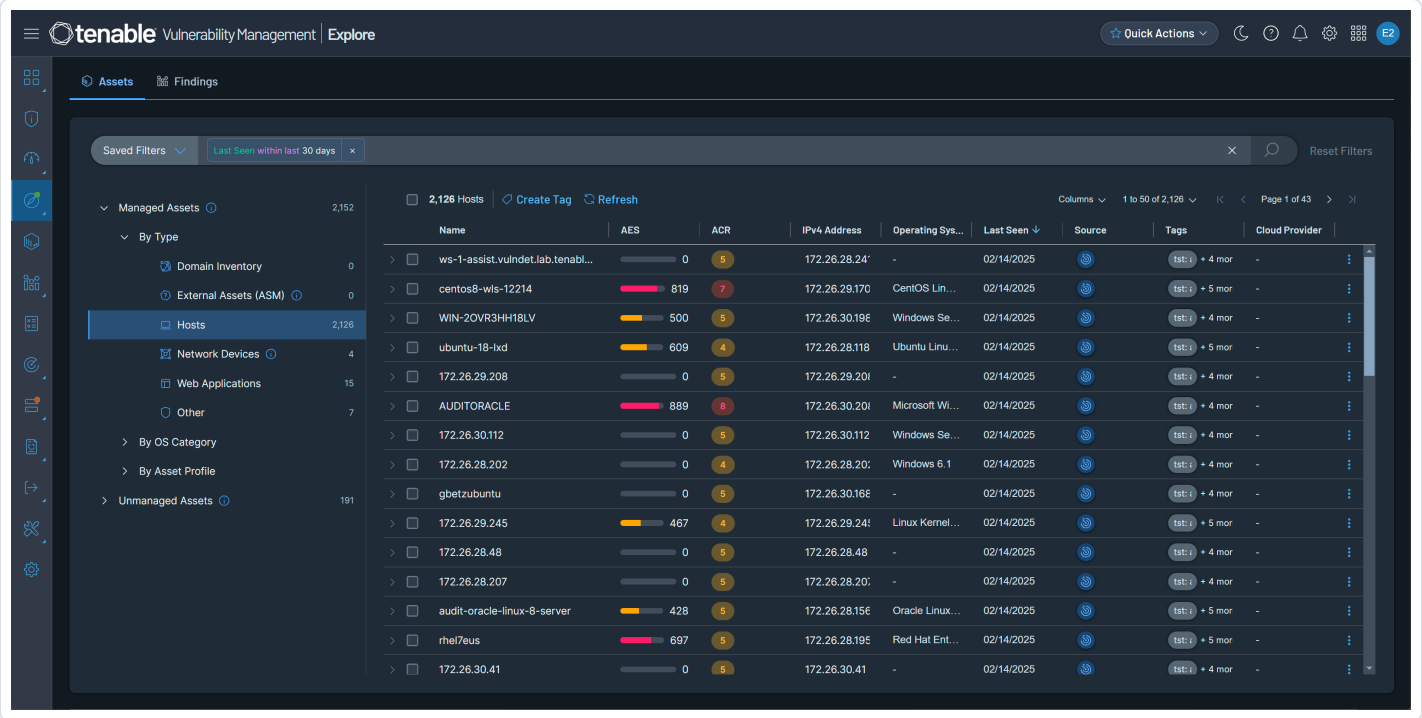
Explore

Explore is Tenable's replacement for Assets and Findings with a new design and an enhanced workflow. To learn more about the new features, see the release notes.

The **Explore** section in Tenable Vulnerability Management is the central location for all your scan data. In **Explore**, you view and manage:

- *Assets*, resources of value on your network that require protection from threats, and
- *Findings*, single instances of vulnerabilities identified on those assets.

As Tenable sensors scan your environment or you import resources from other Tenable products, the system matches incoming data to existing resources or creates new resources. This data is presented on the **Assets** and **Findings** pages. There, using an intuitive query builder, you build lists of assets or findings to take action on. For example, you might recast the severity of some findings to hide them from reports. Or, you might export lists of assets to a file.



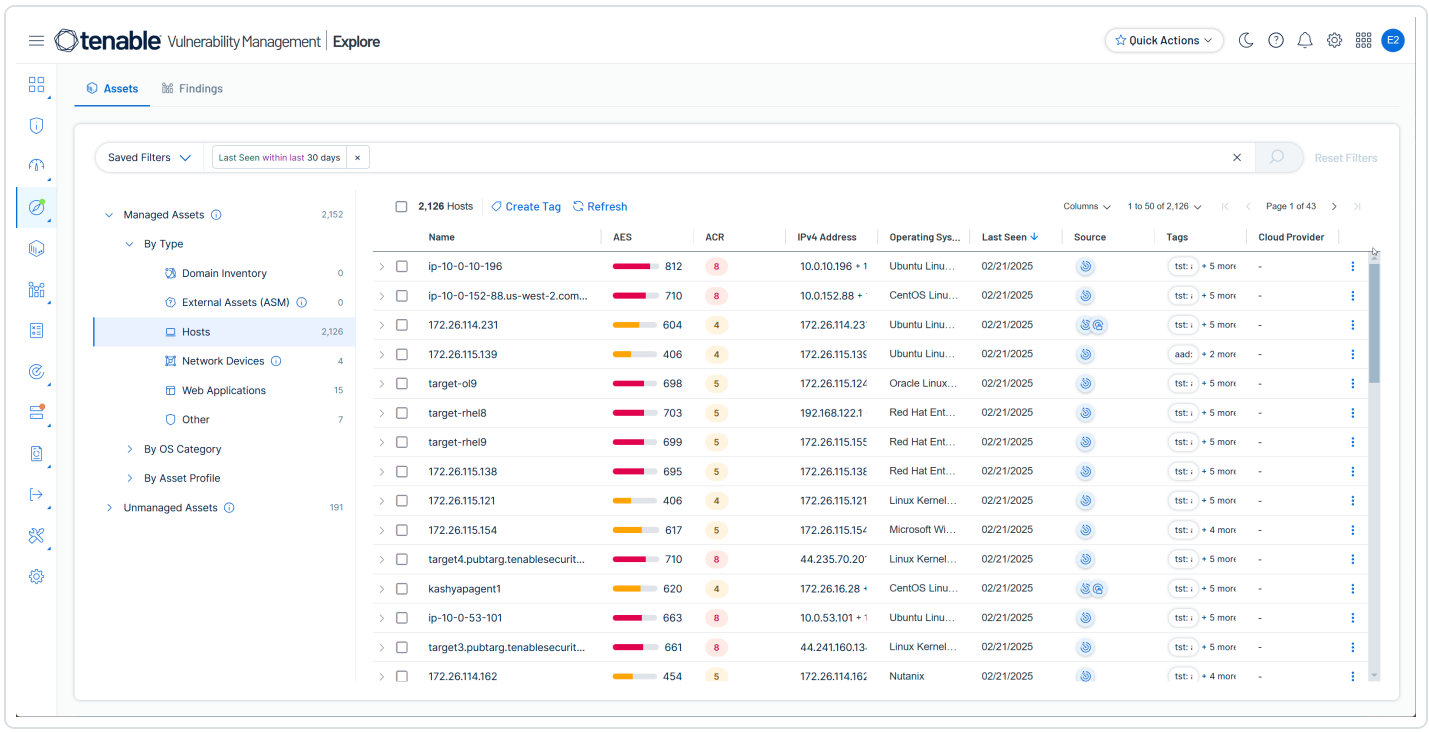
This guide explains how to use **Explore** and is arranged by the work you will do. Start with the following topics.

In This Topic	Learn How To...

Use the Assets Page	Perform common asset actions such as exporting lists, adding assets to scans, or viewing key details.
Use the Findings Page	Perform common findings actions such as creating Recast and Change Result rules or generating reports.
Asset Types	Understand asset types, including both licensed assets and assets which have not yet been scanned for vulnerabilities.
Findings Types	Understand finding types, which include Vulnerabilities, Host Audits and Web Applications.
Asset Filters	Build lists of assets with filters ranging from when assets were first scanned to which operating system they run.
Findings Filters	Build lists of findings with filters including vulnerability severity and Common Platform Enumeration (CPE) ID.

Assets

Assets are entities of value on your network that can be exploited. They include laptops, desktops, servers, routers, mobile phones, virtual machines, software containers, and cloud instances. Use the Assets page to view all the assets in your environment that Tenable Vulnerability Management has a record for. These are broken down into categories such as hosts, web applications, and network devices.



The following topics explain how to view and export lists of assets, build custom queries with filters, add assets to scans, and more.

Use the Assets Page

On the **Assets** page, you can view all the assets in your environment known to Tenable Vulnerability Management. These are broken down by asset type.

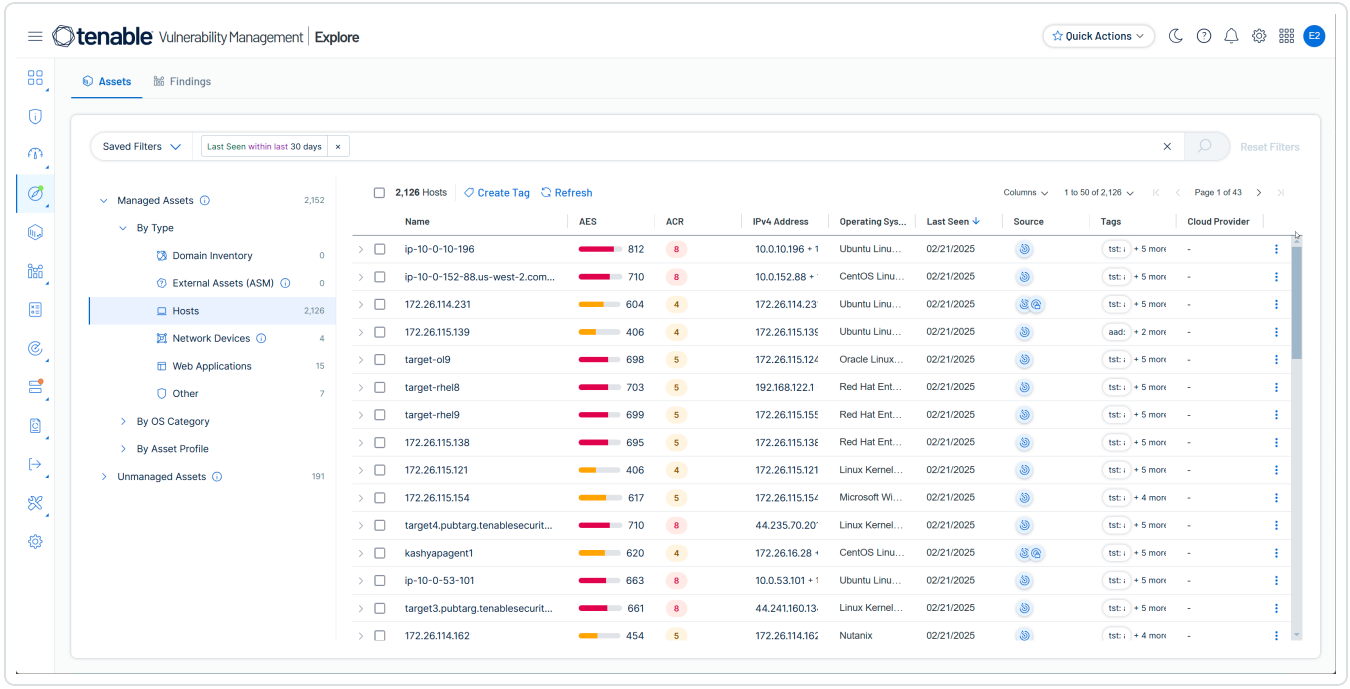
> **Note**: Tenable Vulnerability Management ages out assets which have not been updated for more than 15 months.

> **Important:** Due to differences in the asset source, asset counts within the **Tags** section may not match the asset counts within the **Assets** section of Tenable Vulnerability Management.

To view assets:

- In the left navigation, click **Explore (Preview)** > **Assets**.

  The **Assets** page appears, showing licensed Host assets from the past 30 days.



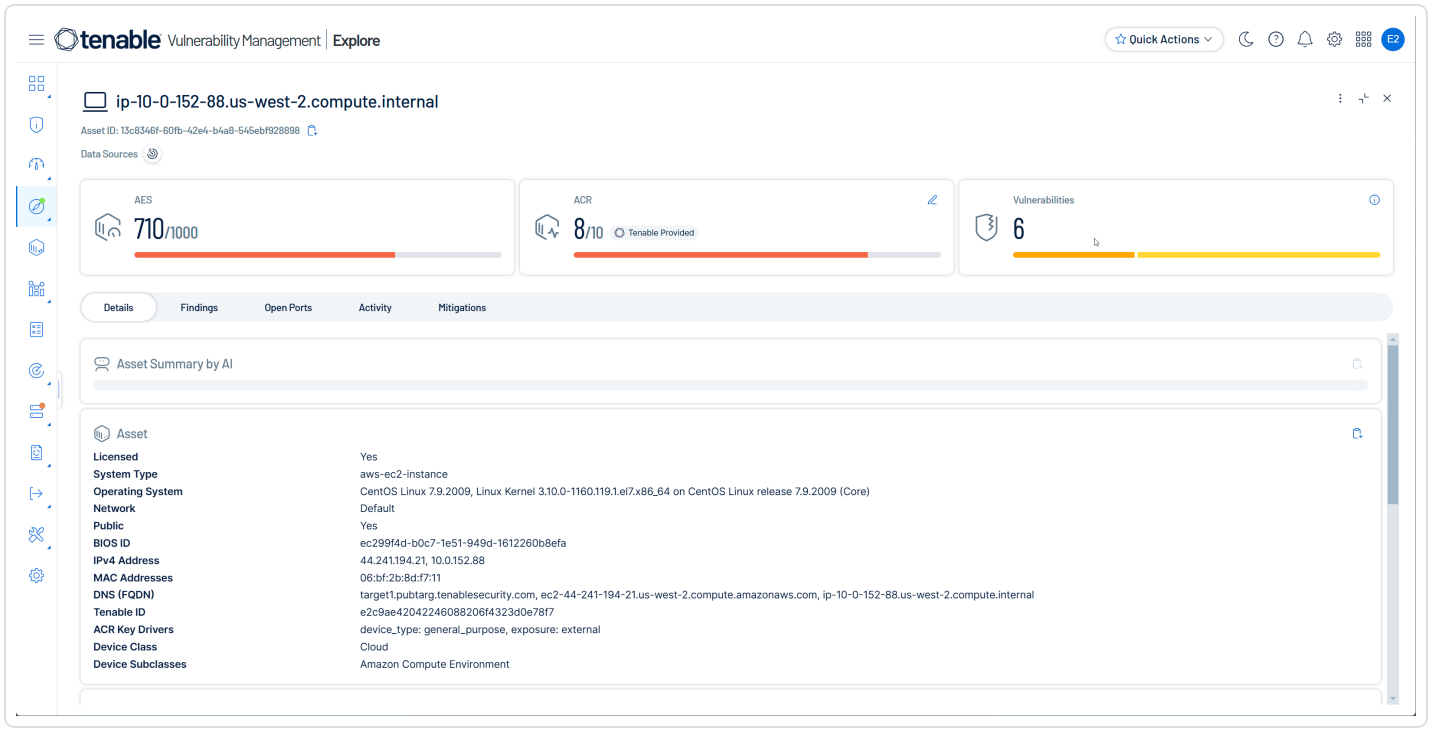
On the **Assets** page, you can:

- View individual assets in a table with columns of information.
- On the left, to refine the list of assets, choose an asset type.
- Click an individual asset to reveal a details pane.
- With the Query Builder, using asset filters, build custom queries
- With the Query Builder, save queries to reuse or share.
- Select assets and add or remove tags.
- Export asset lists to CSV or JSON.
- Select assets and add them to existing scans or create new scans.
- Edit the Asset Criticality Rating (ACR).
- Move assets between networks.
- Delete assets to remove them from your license count.

- Select an asset and view solutions for its vulnerabilities.
- In any asset row, click the drop-down **>** to reveal a list of related findings.
- In any asset row, use the menu ⋮ to access quick actions.

View Asset Details

On the **Assets** page, click an asset to open a pane of details. Then, click ⛶ to expand the pane.



The upper part of the **Asset Details** page contains the following information.

Attribute	Description
Asset Name	The name of the asset; based on the presence of certain attributes in the following logical order: 1. Agent name 2. Local hostname 3. NetBIOS name 4. Fully Qualified Domain Name (FQDN)

	5. IPv4 address 6. IPv6 address
Asset ID	The unique identifier for the asset.
Data Sources	The sources of the scan that identified the asset. Possible values include **AWS**, **AWS FA**, **Azure**, **AZURE FA**, **Cloud Connector**, **Cloud IAC**, **Cloud Runtime**, **GCP**, **Nessus Agent**, **Nessus Scan**, **NNM**, **ServiceNow**, and **WAS**.
AES	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Exposure Score as an integer from 0 to 1000.
ACR	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10.
Vulnerabilities	The number of vulnerabilities identified on the asset.

The lower part of the **Asset Details** page is divided into tabs. Not all information appears for all asset types.

Details

The **Details** tab breaks down information about an asset such as its license status and when it last appeared on a scan.

Panel	Description
Asset	Information about the asset, including the following attributes: • **Licensed** – Indicates if the asset counts towards your Tenable license count, as described in Tenable Vulnerability Management Licenses. • **System Type** – The device type, as reported by Plugin 54615. • **Operating Systems** – The operating system installed on the asset. • **Network** – The name of the network object associated with scanners that identified the asset. The default network name is

	Default. To learn more, see Networks. • **Public** – Specifies if the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public` attribute in the `query` namespace. • **BIOS ID** – The asset's unique BIOS ID. • **IPv4 Address** – The IPv4 address for the asset. • **IPv6 Address** – The IPv6 address for the asset. • **DNS (FQDN)** – The fully qualified domain name for the asset. • **MAC Addresses** – The MAC addresses for the asset. • **Tenable ID** – A UUID created for new assets during credentialed scans or agent scans. If an asset is found not to be unique, this UUID is not created and an existing one is reused. • **ACR Key Drivers** – Main drivers of the Asset Criticality Rating, as described in Tenable Lumin Metrics. • **Device Class** – The main class of the asset, for example *Compute and Application Server*. • **Device Subclass** – The subclass of the asset, for example *Web Application Server*.
Remote Authenticated Scan Information	Information about the scan, including: • **Last Authentication Attempt Time** – The last time that Tenable Nessus attempted to sign in, either with SSH on Unix-based systems or SMB on Windows. • **Last Authenticated Status** – Indicates if the last authentication attempt by Tenable Nessus was successful. • **Last Authenticated Successful** –The last time that Tenable Nessus authenticated successfully.
Last Seen	Information about the asset's scan history, including:

	• **Scan Name** – The name given to the last scan that detected the asset. • **Last Scan ID** – The identifier of the last scan that detected the asset. • **Last Seen** – The date and time of the scan that most recently identified the asset. • **Last Licensed Scan** – The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses. • **First Seen** – The time and date when a scan first identified the asset. • **Last Scan Target** – The IP address or fully qualified domain name (FQDN) of the asset targeted in the last scan.
Tags	A panel containing tags assigned to the asset. Click ⊕ to add a new tag or click × on a single tag to remove it.
CPE	A log of the Common Platform Enumeration (CPE) strings for the asset, identifying its software, hardware, or firmware using a standardized naming convention. This information is drawn from the National Vulnerability Database and Tenable's own plugins.

Findings

In the **Findings** tab, you can view all findings associated with the asset, with Fixed, Accepted, and Info vulnerabilities hidden by default. In the dropdown, switch between **Vulnerability** and **Host Audit** findings.

The **Findings** tab has the same layout as the **Findings** workbench and contains the following columns:

Column	Description
AI/LLM Tools	Indicates an informational finding about artificial intelligence services running on an asset. Hover on the **AI/LLM Tools** column to view details.
Region	The cloud region where the asset runs.
Product Type	The type of product, for example, *Application*.
Vendor	The vendor who makes the product on which the vulnerability was identified, for example, *Apache*.
Account ID	The unique identifier assigned to the asset resource in the cloud service that hosts the asset.
Live Result	Indicates whether the scan result is based on live results. In Agentless Assessment, you can use live results to view scan results for new plugins based on the most recently collected snapshot data, without running a new scan. The possible values are **Yes** or **No**.
Path	The installation path of the software with the vulnerability.
End of Life	If applicable, the end of life date for the affected product.
Fix Type	The type of fix, for example, *version*.
Fix	The version of the fix for the vulnerability.
CVSSv2 Base Score	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
CVSSv3 Base Score	The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
CVSSv4 Base Score	The CVSSv4 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
Last Seen	The date when a scan last found the vulnerability on an asset.
Plugin Family	The family of the plugin that identified the vulnerability.
Plugin ID	The ID of the plugin that identified the vulnerability.

Plugin Name	The name of the plugin that identified the vulnerability. Hover on the icon to view a detailed summary.
Port	The port that the scanner used to connect to the asset where the scan detected the vulnerability.
Product	The name of the product on which the vulnerability was found.
Protocol	The protocol the scanner used to communicate with the asset where the scan detected the vulnerability.
Scan Origin	The scanner that detected the finding. Also identifies if the scan is a workload scan. Possible values for this column are: Tenable Vulnerability Management, Tenable Security Center, and Agentless Assessment.
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.
Source	The sources of the scans that identified the finding. For example, *Seen by Nessus network-based assessment*.
State	The state of the vulnerability. For more information, see Vulnerability States.
Version	The version of the product on which the vulnerability was found.
VPR	A descriptive icon indicating the VPR of the vulnerability. For more information, see CVSS vs. VPR.

Open Ports

In the **Open Ports** tab, review open ports on the asset broken down as follows.

Column	Description
First Seen	The date when a scan first found the vulnerability on an asset.
Port	The open port or ports on the asset.
Protocol	The protocol with which information is transported to the open port, for example, TCP or UDP.

Service	The service running on the open port, such as HTTPS, SSH, or FTP. To learn more about possible services, see Service Name and Transport Protocol on the *Internet Assigned Numbers Authority* website.
First Detected Open	The date and time the port was first detected as open.
Port Last Detected Open	The date and time the port was last detected as open.

Activity

In the **Activity** tab, view an event log for the asset including the following columns. In a single row, click the dropdown **>** to see details.

Column	Description
Event	The title of the event, for example *Asset Discovered*.
Date	The event date.
Source	The event source, for example, *Seen by Nessus network-based assessment*.

Mitigations

In the **Mitigations** tab, view information about any mitigation software identified on the asset in the following columns.

Column	Description
Product Name	The name of the software.
Vendor Name	The vendor for the software.
Version	The version of the software.
Last Detected	The date and time the mitigation software was last detected.

Asset Types

The **Assets** page presents assets identified by scanners in Tenable Vulnerability Management or imported from other Tenable products. In the left navigation, these are broken down into two types: Managed Assets, which have been assessed for vulnerabilities in the past 90 days–and Unmanaged Assets, which have not. Choosing an asset type does not remove your current asset filters.

Refine Managed Assets with filters in drop-downs **>** such as **By Type**. Or, use **Tenable Queries** to apply additional filters.

Tenable Queries

To the right of the search bar, apply Tenable Queries as follows:

- **External Assets (ASM)** – Assets or domains discovered by Tenable Attack Surface Management, integrated with the steps described in Manage Integrations in the *Tenable Attack Surface Management User Guide*. This filter does not appear for Domain Inventory assets.
- **Network Devices** – Assets identified as a networking devices, including routers, switches, firewalls and SSL gateways. This filter does not appear for Domain Inventory, Cloud Resource, or Web Application assets.

For more information, see Tenable Queries.

Managed Assets

Managed assets are actively managed by Tenable Vulnerability Management and have been *assessed* for vulnerabilities in the past 90 days. For more information, see Discovery Scans vs. Assessment Scans.

The following table shows managed assets along with the filters **>** you can apply to them.

Asset Type	Description
By Type	Assets broken down by type, such as web applications or host assets.
Domain Inventory	Fully Qualified Domain Names (FQDNs) or IP addresses discovered by Tenable Attack Surface

	Management.
Hosts	Assets such as workstations, servers, virtual machines, or printers. Network-related assets are not included.
Web Applications	Assets identified as running web applications and assessed via Tenable Web App Scanning.
Other	Assets that do not fit into other categories.
By OS Category	Assets broken down by operating system.
Linux/Unix	Assets running Linux or Unix.
MacOS	Assets running Apple MacOS.
Windows	Assets running Microsoft Windows.
Other	Assets running another type of operating system.
None	Assets with no detected operating system.
By Asset Profile	Assets broken down by class and subclass according to business and device function. Assets can only be in one class.
Cloud	Assets such as virtual machines, containers, or compute instances hosted in cloud environments like AWS, Azure, or Google Cloud Platform.
Compute and	Assets including physical and virtual

Application Server	machines which run enterprise applications, databases, and web services. These support functions such as data processing, content management, identity access, and cloud application orchestration.
Healthcare	Assets used for healthcare services, such as blood pressure monitors.
Internet of Things	Assets including connected devices, sensors, gateways, and smart systems used for surveillance, media, retail, and automation. These support functions such as real-time data collection, remote monitoring, and transaction processing.
Legacy Devices	Assets with operating systems that have reached end of life or end of support.
Network Infrastructure	Assets including physical and virtual network infrastructure devices that manage connectivity or security. These support functions such as routing, firewall protection, load balancing, identity services, network storage, and virtualization platforms.
Operational Technology	Assets including industrial control systems, real-time embedded devices, and operational technology (OT) management infrastructure. These support functions such as automation, process control, and secure communication between OT and IT

	networks.
Peripheral	Assets which support document processing and output, including printers, faxes, and plotters.
Personal Computing	Assets including virtual machines, laptops, desktops, mobile devices, and thin clients.
Telecomm	Assets including telecommunications equipment, VoIP devices, and video conferencing hardware. These support functions such as voice and data transmission and real-time communication services.
Unknown Device	Assets without a class that the system cannot classify.
Unclassified Asset	Assets without a class that the system has not yet attempted to classify.
VM or Workload	Assets including virtual machines and containerized workloads running on platforms like OpenShift. These support functions such as application deployment and orchestration in virtualized environments.

Unmanaged Assets

Unmanaged assets have been *discovered* by Tenable Vulnerability Management or Tenable Nessus, but not scanned for vulnerabilities in the past 90 days.

Asset Type	Description
Domain Inventory	Fully Qualified Domain Names (FQDNs) or IP addresses discovered

	by Tenable Attack Surface Management.
Hosts	Assets such as workstations, servers, virtual machines, or printers. Network-related assets are not included.
Web Applications	Assets identified as running web applications and assessed via Tenable Web App Scanning.
Other	Assets that do not fit into other categories.

Export Assets

You can export data to CSV or JSON formats from the **Assets** page.

1. In the left navigation, click **Explore (Preview)** > **Assets**.

   The **Assets** page appears.

2. Do one of the following:

   - To export a single asset:
     - Above the selected asset, the action bar appears. In the action bar, click **Export**.
     - In the row for the asset that you want to export, click the button.

       A menu appears.

       a. Click **Export**.
   - Click on an asset to open that asset's Asset Details pane.

a. In the upper-right corner of the page, click the ⋮ button.

   A menu appears.

b. Click [→ **Export**.

- To export multiple assets:

  a. In the asset list, select the checkbox next to each asset that you want to export.

     An action bar appears at the top of the list.

  b. In the action bar, click [→ **Export**.

The **Export** dialog appears.

3. Configure the following export options:

Option	Description
File Name	Type a name for the export.
Formats	Select an export format: • **CSV** - A CSV file that you can open in a spreadsheet application such as Microsoft Excel. **Note:** If your export file contains a field starting with any of the following characters (=, +, -, @), the system adds a single quote (') at the beginning of the field. For more information, see the Knowledge Base. • **JSON** - A JSON file containing a nested list of findings.
Configuration	Search for and select the fields to include.
Expiration	Number of days the generated export file will be retained and displayed in the Export Activity list. Default is 3 days.

Schedule	Turn on the **Schedule** toggle and set the following options: a. Choose an export **Start Date** and **Start Time**. b. Choose a **Time Zone**. c. Under **Frequency**, choose how often you want the export to repeat. Choose either Once or one of the following: • Daily, also set **Repeat Every**. • Weekly, also set **Repeat Every** and **Repeat On** (for example, Mo, Tu, We, etc). • Monthly, also set **Repeat Every** and **Repeat By** (for example, Day of Month (Day 1)). d. Under **Repeat Ends**, choose when the exports end. If you choose **Never**, the export repeats until you modify or delete it.
Email Notifications	Turn on the **Email Notification** toggle and set the following options: a. Under **Add Recipients**, type the emails to notify. b. Under **Password**, type a password for the export file which the recipient will need to enter.

4. Click **Export**.

   The system processes the export and the file downloads to your computer. Processing may take several minutes.

> **Tip**: If you close the **Export** dialog before the download completes, you can access the export file in ⚙ **Settings** > [→ **Exports**.

Move Assets Between Networks

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Tenable Vulnerability Management automatically assigns scanned assets to networks based on the scanner's network ID, but you can move assets to different networks to keep them organized. For example, you might have multiple assets with the same IP address which belong on different subnets so they can be identified as separate entities.

Tips for Moving Assets

- Move assets before running scans on a new network. If you move assets to a network where scans have already run, the system may create duplicate records that count against your Tenable licenses.
- You cannot move Domain Inventory assets.
- When you move assets, also move the scanner. Otherwise, the scanner recreates the same asset. To learn more, see Add a Scanner to a Network.
- You can also move assets from the Settings section.

Move Assets from the Assets Workbench

To move assets:

1. In the left navigation, click **Explore (Preview)** > **Assets**
2. The **Assets** page appears.
3. Select the assets to move.

   Above the selected assets, the action bar appears.
4. In the action bar, click **More** > **Move**.

   The **Move Assets** dialog appears.
5. In the **Move Assets** dialog, choose a new network for the asset or assets.
6. Click **Move**.

The system moves the assets to the destination network. Large moves may take a few hours to complete.

Add Assets to Current Scans

On the **Assets** page, you can select assets and add them to a current scan. Then, you can run the scan right away or at its next scheduled time. If you want to add assets to a new scan instead, see Create a Scan.

To add assets to a scan:

1. In the left navigation, click **Explore (Preview)** > **Assets**.

   The **Assets** page appears.

2. Select the assets to scan.

   Above the selected assets, the action bar appears.

3. In the action bar, click **Add To Scan**.

   A dialog appears.

4. In the dialog, search for a scan or choose one from the list.

5. Do one of the following:

   - Click **Save** to add the assets to the scan.
   - Click **Save and Launch** to run the scan.

     A confirmation message appears.

Tip: To view details about your scans, in the left navigation, click **Scans**.

Edit Asset ACR

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

On the **Assets** page, you can manually override the Asset Criticality Rating (ACR) of Host assets to better reflect the needs of your organization.

To edit a Host asset's ACR:

1. In the left navigation, click **Explore (Preview)** > **Assets**.

   The **Assets** page appears.

2. Select the assets to edit.

   Above the selected assets, the action bar apears

3. In the action bar, click **More** > **Edit ACR**.

A dialog appears.

4. Using the slider, change the ACR.
5. (Optional) Under **Overwrite Reasoning**, select a reason.
6. (Optional) Under **Notes**, add notes.
7. Click **Save**.

   The system saves the new ACR, which can take up to 24 hours to appear.

Delete Assets

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Caution: Deleting assets quickly removes decommissioned hosts or other irrelevant assets from your license count and reports, but it is permanent! Be careful with this feature. Consider enabling **Asset Age Out** instead, as described in View or Edit a Network.

On the **Assets** page, you can delete Host, Web Application, or Domain Inventory assets. When you delete assets, Tenable Vulnerability Management removes them from the assets view, deletes all associated findings, and stops matching scan results. Within 24 hours, the assets are removed from your license count. For information on deleting duplicate assets, see Remove and Prevent Duplicate Assets.

Note: You cannot delete more than 200 assets at once.

To delete assets from Tenable Vulnerability Management:

1. In the left navigation, click **Explore (Preview)** > **Assets**.

   The **Assets** page appears.

2. On the **Assets** page, do one of the following:

   Delete a single asset with the ⋮ button

   a. In the row for the asset to delete, click the ⋮ button.

      A menu appears.

   b. In the menu, click **Delete**.

   c. The **Delete Assets** dialog appears.

   Delete a single asset with the Asset Details pane

a. Click on the row for the asset to delete.

   The Asset Details pane appears.

b. In the upper right corner, click the ⋮ button.

   A menu appears.

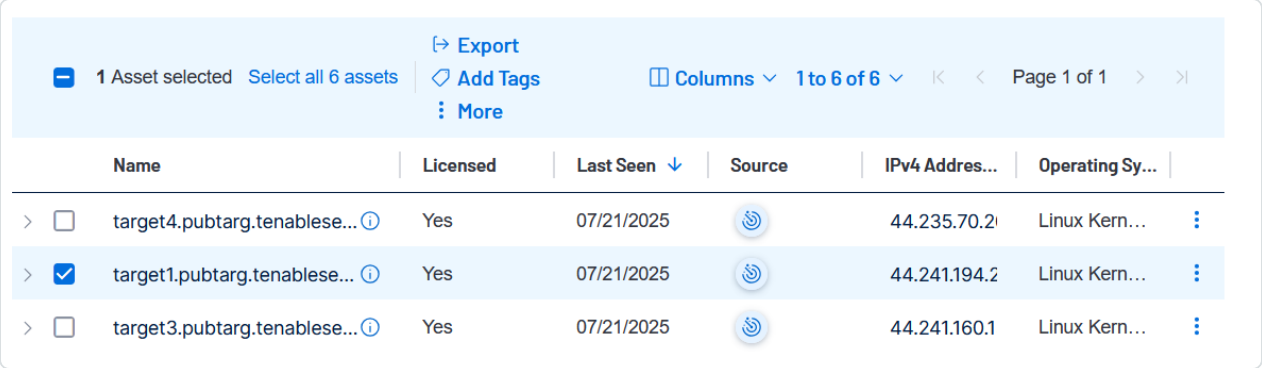
c. In the menu, click 🗑 **Delete**.

d. The **Delete Assets** dialog appears.

Delete multiple assets from the action bar

a. Select the checkbox for each asset to delete.

   Above the selected assets, the action bar appears.



> **Tip**: To select all assets, click the checkbox on the action bar. Then click select all assets. You can only delete 200 assets at a time.

> **Tip**: To select 50 assets at a time, click the checkbox on the action bar.

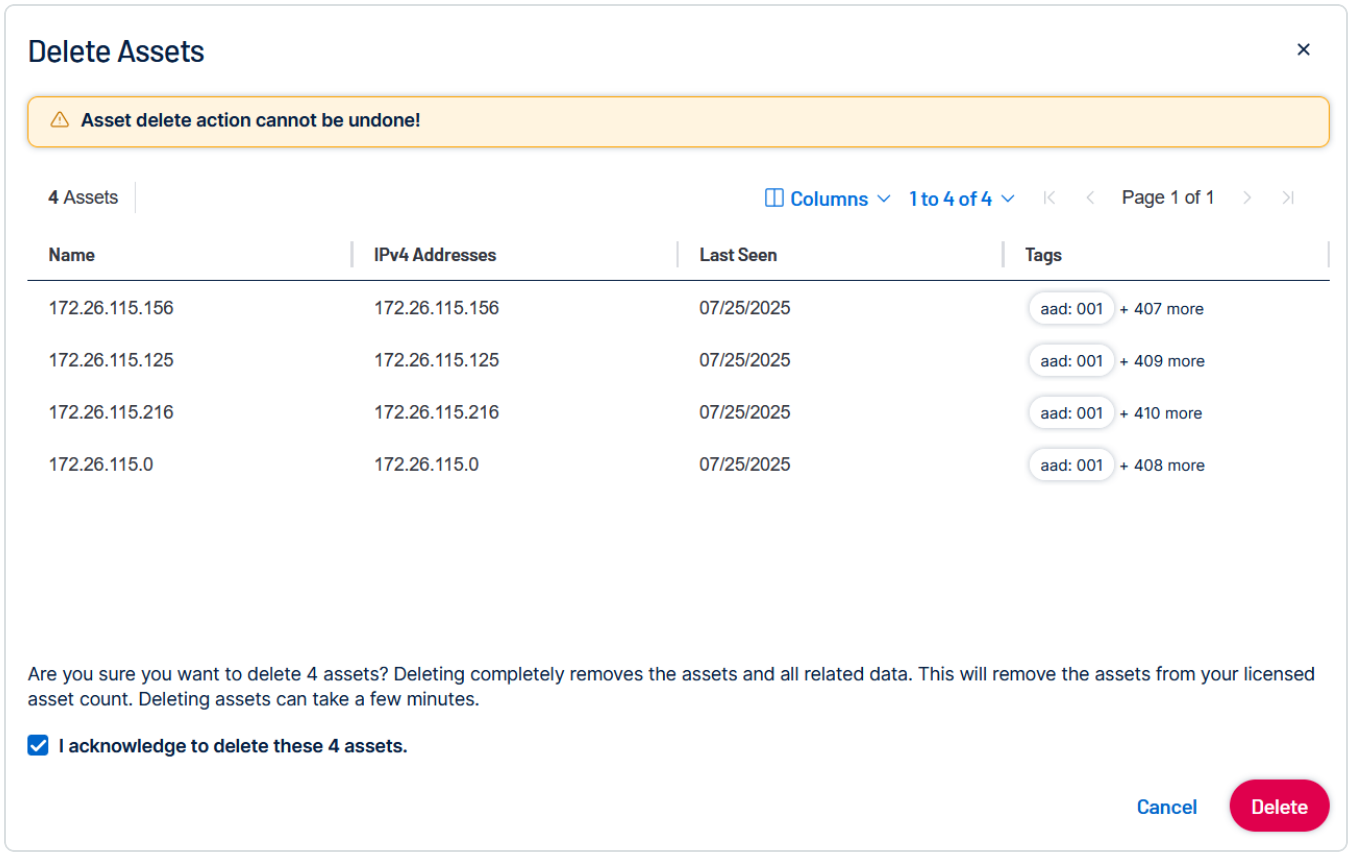
b. In the action bar, click ⋮ **More**.

   A menu appears.

c. Click 🗑 **Delete**.

d. The **Delete Assets** dialog appears.

3. In the **Delete Assets** dialog, select the checkbox to confirm your intent to delete the listed assets.



4. Click the **Delete** button.

   The system queues the assets for deletion. Any deleted assets seen with the **Asset ID** filter are temporary and do not count against your license.

Asset Filters

On the **Assets** tab in **Explore** use the query builder to build custom queries that display the assets you need to see. You can use up to 35 filters in a custom query.

The following table defines the filters you can use. Not all filters are relevant for all asset types.

Filter	Description
Account ID	The unique identifier assigned to the account.

Filter	Description
ACR	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10.
ACR V3 (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset-Criticality Rating* using a new algorithm based on asset profile, which assigns assets to classes by business and device function. This metric rates the importance of an asset to your organization from 1 to 10, with higher numbers for more critical assets. For more information, see Scoring and Asset Criticality Rating.
ACR Severity	(Requires Tenable One or Tenable Lumin license) The ACR category of the ACR calculated for the asset.
AES	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Exposure Score as an integer from 0 to 1000.
AES V3 (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset Exposure Score* using a new algorithm. This metric weighs an asset's Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) and then assigns a number from 1 to 1000, with higher numbers for more exposed assets. For more information, see Scoring (Beta).
AES Severity	(Requires Tenable One or Tenable Lumin license) The ACR category of the ACR calculated for the asset.
Agent Name	The name of the Tenable Nessus agent that scanned and identified the asset.
ASN	The Autonomous System Number (ASN) for the asset.
Assessed vs. Discovered	Specifies if the system scanned the asset for vulnerabilities or only identified it on a discovery scan. Possible values are **Assessed** or **Discovered Only**.
Asset ID	The asset's unique identifier.
AWS Availability Zone	The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see Regions and Zones in the AWS

Filter	Description
	documentation.
AWS EC2 AMI ID	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Instance ID	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Name	The name of the virtual machine instance in Amazon EC2.
AWS EC2 Product Code	The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2.
AWS Instance State	The state of the virtual machine instance in AWS at the time of the scan. For possible values, see InstanceState in the Amazon Elastic Compute Cloud Documentation.
AWS Instance Type	The type of virtual machine instance in Amazon EC2. Amazon EC2 instance types dictate the specifications of the instance (for example, how much RAM it has). For a list of possible values, see Amazon EC2 Instance Types in the AWS documentation.
AWS Owner ID	A UUID for the Amazon AWS account that created the virtual machine instance. This attribute only appears for Amazon EC2 instances. For more information, see View AWS Account Identifiers in the AWS documentation
AWS Region	The region where AWS hosts the virtual machine instance, for example, `us-east-1`.
AWS Security Group	The AWS security group (SG) associated with the Amazon EC2 instance.
AWS Subnet ID	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.
AWS VPC ID	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private

Filter	Description
	Cloud Documentation.
Azure Location	The location of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager documentation.
Azure Resource Group	The name of the resource group in the Azure Resource Manager. For more information, see the Azure Resource Manager documentation.
Azure Resource ID	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager documentation.
Azure Resource Type	The resource type of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager documentation.
Azure Subscription ID	The unique subscription identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager documentation.
Azure VM ID	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see the Azure Resource Manager documentation.
BIOS ID	The NetBIOS name for the asset.
Cloud Provider	The name of the cloud provider that hosts the asset.
Created Date	The date and time when Tenable Vulnerability Management created the asset record.
Custom Attribute	A filter that searches for custom attributes via a category-value pair. For more information about custom attributes, see the Tenable Developer Portal.
Device Class	The purpose of the asset. For example, "Is it a server?" Every asset belongs to exactly one Device Class creating a clear and organized hierarchy. Device Classes have Device Subclasses.
Device Subclasses	Specifies the primary function or role of the asset. For example, within the Compute and Application Server class, the device subclass would distinguish a web application server from a database server. Assets may

Filter	Description
	have multiple device subclass values.
DNS (FQDN)	The fully-qualified domain name of the host that the vulnerability was detected on.
Domain	The domain to which the asset belongs.
First Seen	The date and time when a scan first identified the asset.
Google Cloud Instance ID	The unique identifier of the virtual machine instance in Google Cloud Platform (GCP).
Google Cloud Project ID	The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see Creating and Managing Projects in the GCP documentation.
Google Cloud Zone	The zone where the virtual machine instance runs in GCP. For more information, see Regions and Zones in the GCP documentation.
Has Plugin Results	Specifies whether the asset has plugin results associated with it.
Host Name (Domain Inventory)	The host name for assets found during attack surface management scans; only for use with Domain Inventory assets.
Hosting Provider	The hosting provider for the asset.
Installed Software	A list of Common Platform Enumeration (CPE) values that represent applications identified on an asset from a scan. This field supports the CPE 2.2 format. For more information, see the Component Syntax section of the CPE Specification documentation. For assets identified in Tenable scans, this field only contains data when a scan using Tenable Nessus Plugin 45590 has evaluated the asset.
IPV4 Address	The IPv4 address associated with the asset record.

Filter	Description
IPV6 Address	The IPv6 address associated with the asset record.
Is Attribute	Specifies whether the asset is an attribute.
Is Auto Scale	Specifies whether the asset scales automatically.
Is Unsupported	Specifies whether the asset is unsupported in Tenable Vulnerability Management.
Last Authenticated Scan	The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field.
Last Licensed Scan	The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses.
Last Seen	The date and time at which the asset was last observed as part of a scan.
Licensed	Specifies whether the asset is included in the asset count for the Tenable Vulnerability Management instance.
MAC Address	A MAC address that a scan has associated with the asset record.
Mitigated	Specifies whether a scan has identified mitigation software on the asset.
Mitigation Last Detection	The date and time of the scan that last identified mitigation software on the asset.
Mitigation Product Name	The name of the mitigation software identified on the asset. Tenable Lumin defines mitigations as security agent software running on endpoint assets, which include antivirus software, Endpoint Protection Platforms (EPPs), or Endpoint Detection and Response (EDR) solutions.
Mitigation	The name of the vendor for the mitigation that a scan identified on the

Filter	Description
Vendor Name	asset.
Mitigation Version	The version of the mitigation that a scan identified on the asset.
Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.
NetBIOS Name	The NetBIOS name for the asset.
Network	The name of the network object associated with scanners that identified the asset. The default name is **Default**. For more information, see Networks.
Operating System	One of the operating system(s) that a scan identified on the asset.
Operating System (WAS)	The operating system that a Tenable Web App Scanning scan identified as installed on the asset.
OS Category	The operating system category that a scan detected as installed on the asset, for example *MacOS*.
Port	Search your hosts or domain inventory by port values or ranges for assets with a relationship to that port. For example, assets with port 80. If you import data from Tenable Attack Surface Management, those ports also appear.
Port Last Detected Open	Filter for all assets that had detected open ports as of a date or a date range you specify. For the best results, combine with the **Ports** filter.
Public	Specifies whether the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable Vulnerability Management `query` namespace.
Record Type	The asset type.

Filter	Description
Scan Frequency	The number of times the asset was scanned within the past 90 days.
ServiceNow Sys ID	Where applicable, the unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.
Source	The source of the scan that identified the asset. Possible values include **AWS**, **AWS FA**, **Azure**, **AZURE FA**, **Cloud Connector**, **Cloud IAC**, **Cloud Runtime**, **GCP**, **Nessus Agent**, **Nessus Scan**, **NNM**, **ServiceNow**, and **WAS**.
SSL/TLS	Specifies whether the application on which the asset is hosted uses SSL/TLS public-key encryption.
System Type	The system types as reported by Plugin ID 54615. For more information, see Tenable Plugins.
Tags	Asset tags, entered in pairs of `category` and `value` (for example Network: Headquarters). This includes the space after the colon (:). If there is a comma in the tag name, insert a backslash (\) before the comma. If your tag name includes double quotation marks (" "), use the UUID instead. You can add a maximum of 100 tags. For more information, see Tags.
Target Groups	The target group to which the asset belongs. This attribute is empty if the asset does not belong to a target group. For more information, see Target Groups.
Tenable ID	The UUID of the asset in Tenable Vulnerability Management.
Tenable.sc Host ID	The unique ID of an asset which was imported from Tenable Security Center.
Type	The system type on which the asset is managed. Possible options are **Cloud Resource**, **Container**, **Host**, and **Cloud**.
Updated Date	The last date when new information about an asset was added to the system.

Asset Columns

On the **Assets** tab in **Explore**, you can view the assets in your environment broken down into categories including hosts, web applications, domain inventory, and other devices.

The **Assets** tab has the following columns, which you can show or hide as described in Use Tables. Not all columns appear for all asset types.

Column	Description
ACR	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10.
ACR V3 (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset-Criticality Rating* using a new algorithm based on asset profile, which assigns assets to classes by business and device function. This metric rates the importance of an asset to your organization from 1 to 10, with higher numbers for more critical assets. For more information, see Scoring and Asset Criticality Rating.
AES	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Exposure Score as an integer from 0 to 1000.
AES V3 (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset Exposure Score* using a new algorithm. This metric weighs an asset's Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) and then assigns a number from 1 to 1000, with higher numbers for more exposed assets. For more information, see Scoring (Beta).
Agent Name	The name of the Tenable Nessus agent that scanned and identified the asset.
Asset ID	The UUID of the asset. This value is unique to Tenable Vulnerability Management.
AWS Availability Zone	The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see Regions and Zones in the AWS documentation.
AWS EC2 AMI ID	The unique identifier of the Linux AMI image in Amazon Elastic Compute

Column	Description
	Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Instance ID	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Name	The name of the virtual machine instance in Amazon EC2.
AWS EC2 Product Code	The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2.
AWS Instance State	The state of the virtual machine instance in AWS at the time of the scan. For possible values, see InstanceState in the Amazon Elastic Compute Cloud Documentation.
AWS Instance Type	The type of virtual machine instance in Amazon EC2. Amazon EC2 instance types dictate the specifications of the instance (for example, how much RAM it has). For a list of possible values, see Amazon EC2 Instance Types in the AWS documentation.
AWS Owner ID	A UUID for the Amazon AWS account that created the virtual machine instance. This attribute only appears for Amazon EC2 instances. For more information, see View AWS Account Identifiers in the AWS documentation
AWS Region	The region where AWS hosts the virtual machine instance, for example, `us-east-1`.
AWS Security Group	The AWS security group (SG) associated with the Amazon EC2 instance.
AWS Subnet ID	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.
AWS VPC ID	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud Documentation.
Azure Resource	Where applicable, the Azure resource ID of the asset, as described in the

Column	Description
ID	Tenable Vulnerability ManagementMicrosoft Azure documentation.
Azure VM ID	Where applicable, the Azure VM ID of the asset, as described in the Tenable Vulnerability Management Microsoft Azure documentation.
Cloud Provider	Indicates whether the asset is from AWS, Azure, or GCP.
Created Date	The date and time when Tenable Vulnerability Management created the asset record.
Device Class	The purpose of the asset. For example, "Is it a server?" Every asset belongs to exactly one Device Class creating a clear and organized hierarchy. Device Classes have Device Subclasses.
Device Subclasses	Specifies the primary function or role of the asset. For example, within the Compute and Application Server class, the device subclass would distinguish a web application server from a database server. Assets may have multiple device subclass values.
DNS (FQDN)	The fully qualified domain name of the asset host. When processing fully qualified domain names (FQDNs) for host assets, Tenable Vulnerability Management normalizes all FQDNs to lowercase and then merges any duplicates.
First Seen	The date and time when a scan first identified the asset.
Google Cloud Instance ID	Where applicable, the Google cloud instance ID of the asset, as described in the Tenable Vulnerability Management Google Cloud Platform documentation.
Google Cloud Project ID	Where applicable, the Google cloud project ID of the asset, as described in the Tenable Vulnerability Management Google Cloud Platform documentation.
Google Cloud Zone	Where applicable, the Google cloud zone of the asset, as described in the Tenable Vulnerability Management Google Cloud Platform documentation.

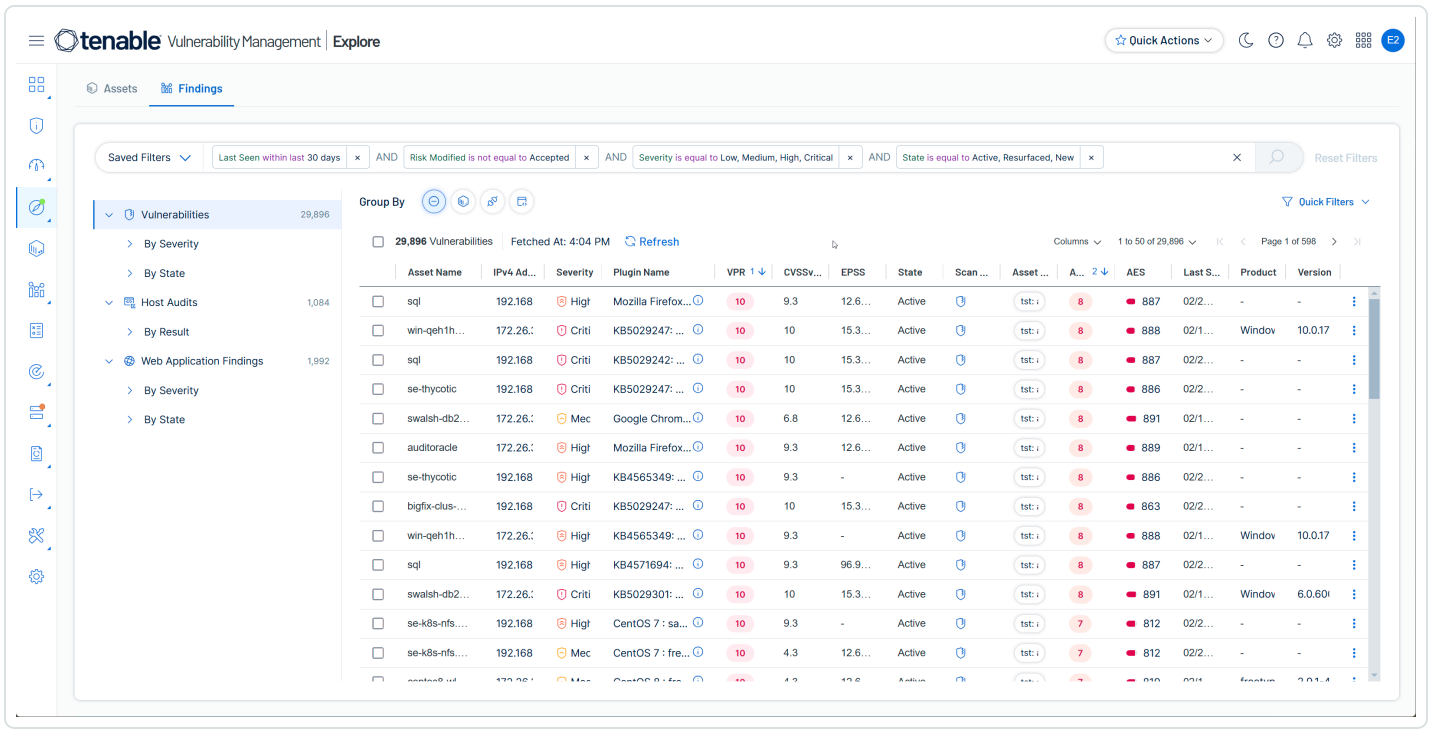
Column	Description
Has Plugin Results	Specifies whether the asset has plugin results associated with it.
IPV4 Address	The IPv4 address for the affected asset.
IPV6 Address	The IPv6 address for the affected asset.
Last Authenticated Scan	The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field.
Last Licensed Scan	The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses.
Last Seen	The date when a scan last found the vulnerability on an asset.
Licensed	Indicates if the asset is licensed within Tenable Vulnerability Management. For more information, see Tenable Vulnerability Management Licenses.
MAC Address	A MAC address that a scan has associated with the asset record.
Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.
NetBIOS Name	The asset's NetBIOS name.
Operating System	One of the operating system(s) that a scan identified on the asset.
Public	Specifies whether the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public`

Column	Description
	attribute in the Tenable Vulnerability Managementquery namespace.
Resource Tags	For assets with a source of **Cloud Discovery Connector**, specifies imported tags or labels. The limit is 50 tags per resource for AWS and Azure and 64 labels per resource for GCP. In addition, Azure tags do not support JSON strings.
ServiceNow Sys ID	Where applicable, the unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.
Source	The source of the scan that identified the asset.
System Type	The operating system installed on the asset.
Tags	Tags applied to the asset.
Updated Date	The date and time when Tenable Vulnerability Management last updated the asset record.

Findings

Findings are single instances of vulnerabilities on your assets, uniquely identified by plugin ID, port, and protocol. They are broken down into categories including vulnerabilities, host audit findings, and web application findings. Findings appear on the Findings page, where you can use them to identify security risks, get visibility into under-utilized resources, or support your compliance efforts.

Tenable Vulnerability Management automatically creates or updates findings when scans complete or you import scan results and retains this data for 15 months.



The following topics explain how to view and export lists of findings, build custom queries with filters, work with findings details, and more.

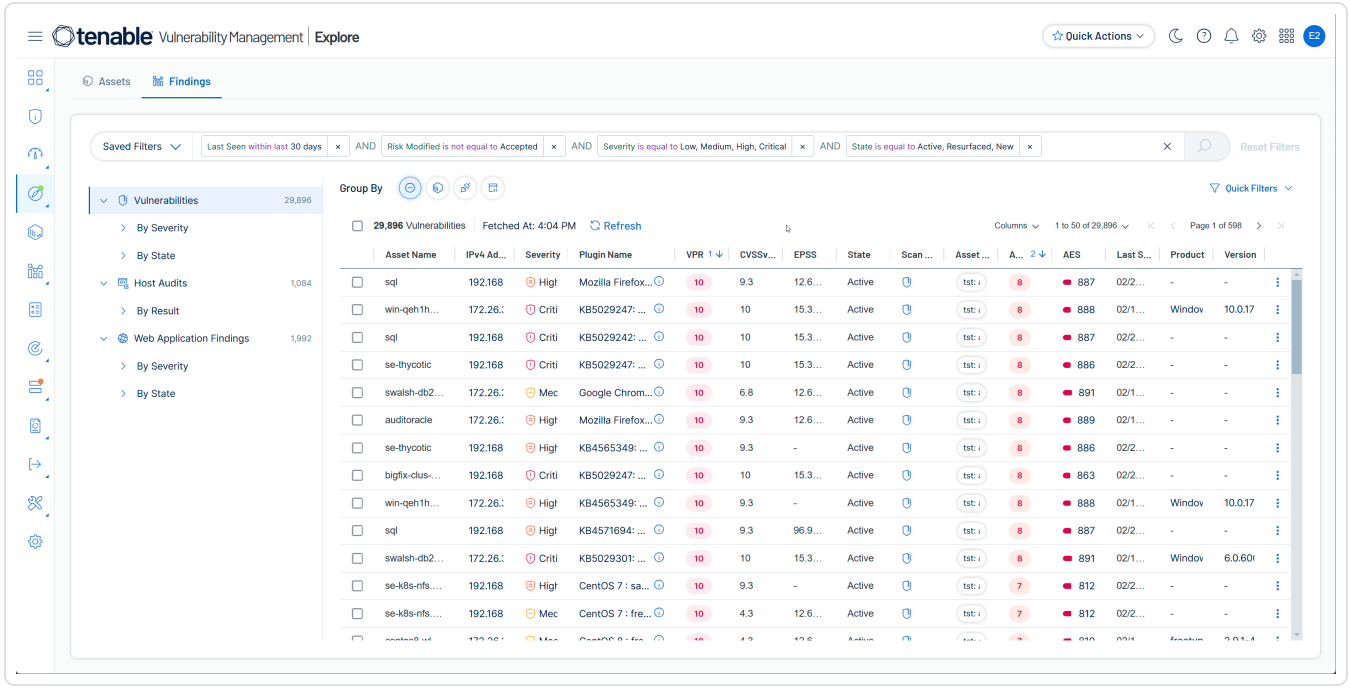
Use the Findings Page

On the **Findings** page, you can view all the findings in your environment known to Tenable Vulnerability Management. These are broken down by type.

To view findings:

- In the left navigation, click **Explore (Preview)** > **Findings**.

  The **Findings** page appears, showing Vulnerabilities from the past 30 days.

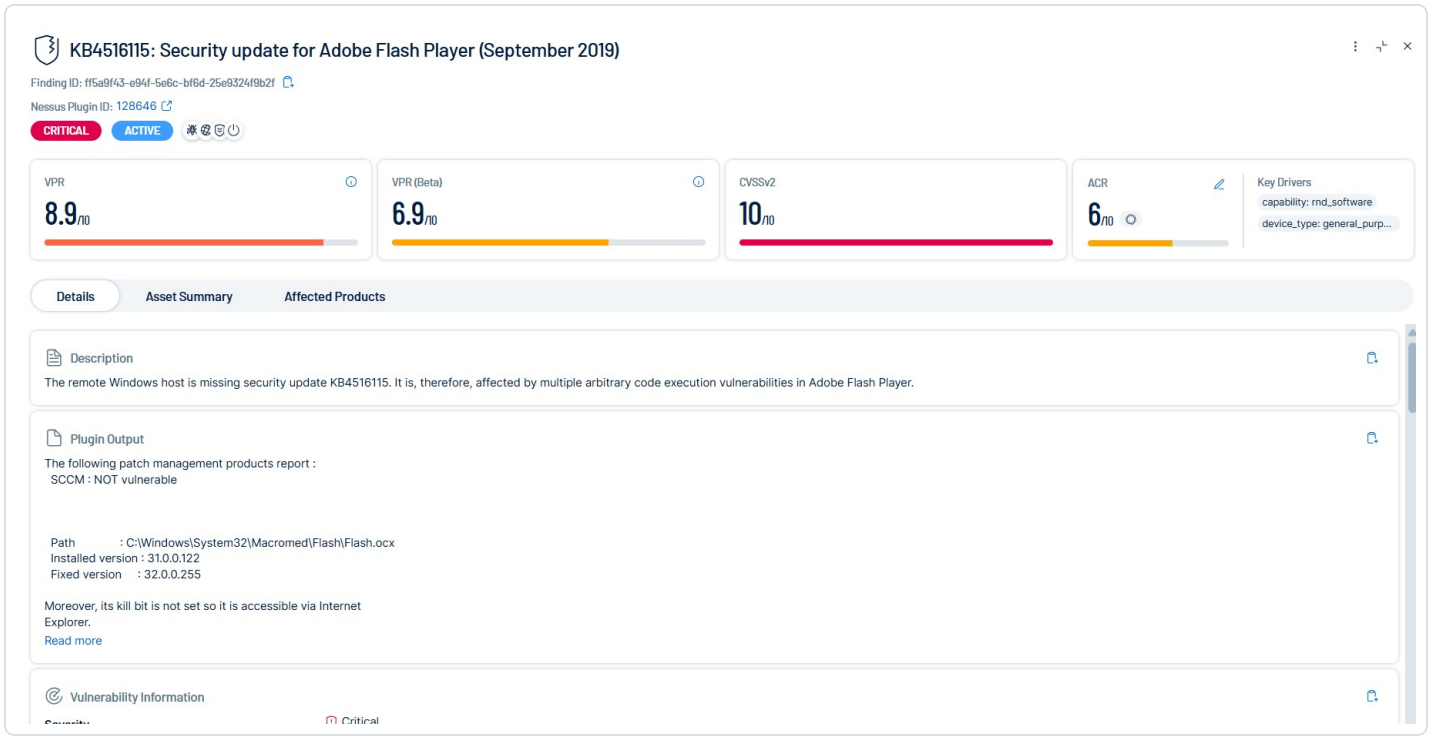


On the **Findings** page, you can:

- View individual findings in a table with columns of information.
- On the left, to refine the list of findings, choose a finding type.
- Click an individual finding to reveal a details pane.
- In the Query Builder, using findings filters, build custom queries
- In the Query Builder, save queries to reuse or share.
- Export findings lists to CSV or JSON.
- Generate findings reports.
- Apply recast rules to hide findings or change their severity.
- Group findings by their asset, plugin, or product; click **>** to view the groups in drop-downs.
- In any finding row, use the ⋮ menu to access quick actions such as remediation scans.

View Findings Details

On the **Findings** page, click a finding to open a pane of details. Then, click ⛶ to expand the pane.



The upper part of the **Findings Details** page contains the following information.

Attribute	Description
Finding Name	The name of the finding, for example *Microsoft Netlogon Elevation of Privilege (Zerologon) (Remote)*.
Nessus Plugin ID	If relevant, the unique identifier for the Tenable Nessus plugin that found the vulnerability.
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.
State	The state of the vulnerability, for example *Active*.
Exploitability	Icons indicating characteristics of the vulnerability that determine its potential exploitability; for example, *Exploited By Malware* or *Remotely Exploitable*.
VPR	The vulnerability's vulnerability priority rating.
VPR(Beta)	The vulnerability's vulnerability priority rating using VPR (Beta) scoring.

	Tip: For more information, see the *Scoring Explained Quick Reference Guide*.
CVSSv2	The corresponding vulnerability's CVSSv2 base score.
ACR	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR).

The lower part of the **Findings Details** page is divided into tabs. Not all information appears for all findings types.

Details

The **Details** tab breaks down information about a finding including its description and details for the corresponding vulnerability.

Section	Description
Description	A description of the corresponding vulnerability.
Plugin Output	Output from the plugin that identified the vulnerability.
Vulnerability Information	Important information about the vulnerability, including the following attributes: • **Severity** – The vulnerability's CVSS-based severity. • **Vulnerability Published** – The oldest date on which the vulnerability was either documented in an advisory or published in the National Vulnerability Database (NVD). • **Exploitability** – Characteristics of the vulnerability that determine its potential exploitability. • **Patch Published** – When a patch for the vulnerability was published. • **Remediation Type** – The type of fix recommended. Possible values are **Patch**, **Workaround**, **Patch and Workaround**, and **No Fix**. • **Exploitability Ease** – A description of how easy it is to exploit the vulnerability.

	• **Exploited By Malware** – Whether the vulnerability is known to be exploited by malware. • **Port** – The port the scanner used to connect to the asset where the vulnerability was found. • **Protocol** – The protocol the scanner used to communicate with the asset where the vulnerability was found. • **Live Result** – A **Yes** or **No** value that indicates if the scan result is based on live results, which you can use in Agentless Assessment to view scan results for new plugins based on recently collected snapshot data, without running a new scan.
Fixes	If available, details about fixes for the vulnerability, including: • **Solution** – A summary of how to officially remediate the vulnerability. • **Workaround** – The type of recommended workaround; possible values are **Configuration Change** or **Disable Service**. • **See Also** – Links to websites with helpful information about the vulnerability.
Vulnerability Detection Timeline	Information about when the vulnerability was detected, including: • **First Seen** – The date when a scan first found the vulnerability on an asset. • **Last Seen** – The date when a scan last found the vulnerability on an asset. • **Vulnerability Age** – The age of a vulnerability based on its **State**. For *Active* vulnerabilities, based on the time elapsed between **First Seen** and today's date. For *Fixed* vulnerabilities, based on the time elapsed between **First Seen** and **Last Fixed** or the time elapsed between **Resurfaced** and **Last Fixed**. For *Resurfaced* vulnerabilities, based on the time elapsed between **Resurfaced** and and today's date.
VPR Key Drivers	Information about the key drivers Tenable uses to calculate a VPR for the vulnerability, including, but not limited to:

	• **Age of Vuln** – The number of days since the National Vulnerability Database (NVD) published the vulnerability. • **CVSS3 Impact Score** – The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable Vulnerability Management shows 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 (for example, 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 (for example, 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 shows **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**.
VPR (Beta) Key Drivers	Information about the key drivers Tenable uses to calculate a VPR (Beta) score for the vulnerability, including, but not limited to: • **CVE ID** – The Common Vulnerabilities and Exposures (CVE) ID, for example *CVE-2002-2024*. • **VPR** – The vulnerability's vulnerability priority rating. • **VPR Percentile** – The finding's VPR (Beta) score percentile ranking, indicating its position relative to other vulnerabilities. • **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 (for example, Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (**High**, **Functional**, **PoC**, or **Unproven**) parallel the CVSS Exploit Code Maturity categories. • **On CISA Kev** – Indicates whether the CVE is listed on the CISA Known Exploited Vulnerabilities list. • **In the News, Intensity, Last 30 days** – Findings whose VPR (Beta) is elevated due to a high volume or frequency of media mentions in the last 30 days. • **Malware Observations Intensity, Last 30 days** – Findings with a higher VPR (Beta) due to a significant volume of associated malware observations in the last 30 days. • **Exploit Probability** – Findings where the VPR (Beta) score is primarily influenced by the estimated probability of the vulnerability being exploited.
Plugin Details	Information about the plugin that detected the vulnerability, including: • **Plugin Published** – The date on which the plugin that identified the vulnerability was published. • **Plugin Updated** – The date on which the plugin was last modified. • **Plugin Family** – The family of the plugin that identified the vulnerability. • **Plugin Type** – The general type of plugin check (for example, `local` or `remote`). • **Plugin Version** – The version of the plugin that identified the vulnerability.
CVEs	Links to the CVEs corresponding to the finding. Click a link to open the the Vulnerability Profile page in the **Vulnerability Intelligence** section.
Risk Information	Information about the vulnerability's risk profile, including:

	• **Risk Factor** – The CVSS-based risk factor associated with the plugin. • **CVSSv3 Base Score** – The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). • **CVSSv3 Vector** – A CVSSv3-based text string containing metric:value pairs to describe vulnerability characteristics, for example *AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H*. • **CVSSv3 Temporal Score** – A CVSSv3-based score from 0 to 10 indicating current severity. Higher scores are more severe. • **CVSSv3 Temporal Vector** – A CVSSv3-based text string containing metric:value pairs that indicate vulnerability maturity and remediation status, for example *E:H/RL:O/RC:C*. • **CVSSv2 Base Score** – The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). • **CVSSv2 Vector** – A CVSSv2-based text string containing metric:value pairs to describe vulnerability characteristics. • **CVSSv2 Temporal Score** – A CVSSv2-based score from 0 to 10 indicating current severity. • **CVSSv3 Temporal Vector** – A CVSSv2-based text string containing metric:value pairs that indicate vulnerability maturity and remediation status. • **STIG Severity** – A vulnerability's severity rating based on the Department of Defense's Security Technical Implementation Guide (STIG). • **Risk Modified** – The risk modification applied to the vulnerability's severity.
References	Industry resources that provide additional information about the vulnerability.

Asset Summary

The **Asset Summary** tab contains details about the asset corresponding to the finding, along with when the asset was last seen by a scanner.

Section	Description
Asset Summary	Information about the affected asset, including: • **Asset Name** – The name of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management. • **Asset ID** – The UUID of the asset where a scan detected the vulnerability. • **System Type** – The type of operating system that the scan identified on the affected asset. • **Operating System** – The operating system that the scan identified on the affected asset. • **Public** – Indicates if the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable Vulnerability Management query namespace. • **IPV4 Address** – The IPv4 address for the affected asset. • **IPV6 Address** – The IPv6 address for the affected asset. • **Network** – The name of the network object associated with scanners that identified the asset. The default name is **Default**. For more information, see Networks. • **MAC Addresses** – The MAC addresses for the affected asset. • **Tenable ID** – A UUID created for new assets during credentialed scans or agent scans. If an asset is found not to be unique, this UUID is not created and an existing one is reused. • **DNS (FQDN)** – The fully qualified domain name of the asset host.
Tags	A panel containing tags assigned to the affected asset. Click ⊕ to add a new

	tag or click × on a single tag to remove it.
CPE	The Common Platform Enumeration (CPE) numbers for vulnerabilities that the plugin identifies, using a standardized naming convention. To learn more, see the National Vulnerability Database website.
Last Seen	Information about when the affected asset was last identified on a scan, including: • **Last Seen** – The date when a scan last found the vulnerability on an asset. • **First Seen** – The date when a scan first found the vulnerability on an asset. • **Last Authenticated Scan** – The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates **Last Authenticated Scan**, but not **Last Licensed Scan**. • **Last Licensed Scan** – The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. • **Source** – The source of the scan that detected the vulnerability on the affected asset, for example Tenable Nessus. • **Scan Origin** – The scanner that detected the finding, for example Tenable Vulnerability Management or Tenable Security Center. You can use this attribute to identify if the scan is a work-load scan. • **Last Authentication Status** – The status of the last authentication attempt, for example, *Success*. • **Last Successful Authentication** – The date and time of the last successful authentication.

	• **Last Authentication Attempt Time** – The date and time of the last authentication attempt.

Affected Products

A table of information about the products on the affected assets. This section only appears for Vulnerabilities and has the following columns.

Column	Description
End of Life	If applicable, the end of life date for the affected product.
Path	The installation path of the product.
Product	The product name.
Product Type	The type of product, for example *Operating System*.
Vendor	The vendor who makes the product affected by the vulnerability, for example *Microsoft*.
Version	If relevant, the version number of the product.

Findings Types

The **Findings** page presents findings identified by scanners in Tenable Vulnerability Management as well as those imported from other Tenable products. In the left navigation, choose a findings type. Then, refine results with filters in drop-downs **>**. Choosing a findings type does not remove your current findings filters.

Findings Types

The following table defines the findings types in the left navigation.

Findings Type	Description
Vulnerabilities	Findings such as system misconfigurations, unpatched software, poor data encryption,

	and weak authorization credentials. Refine **By VPR**, **By Severity**, or **By State**.
Host Audits	Host audits assess workstations, services, or network devices to evaluate the configuration, hardening, and security controls applied to a target. Refine these **By Result** of an audit.
Web Application Findings	Findings such as SQL injections, cross-site scripting, local file inclusions, security misconfigurations, and XML external entity processing. Filter **By VPR**, **By Severity** or **By State**.

Findings Type Filters

Under each findings type, use drop-downs **>** to apply filters that vary by type:

- **By VPR** – Filter by the Vulnerability Priority Rating, which rates the risk and urgency of a vulnerability from 1 to 10.
- **By Severity** – Filter by a vulnerability's severity–for example, Critical. For more information, see Vulnerability Severity Indicators.
- **By State** – Filter by a vulnerability's state, which provides its detection status. For more information, see Vulnerability States.
- **By Result** – Filter by audit results–for example, Passed or Failed.

Create Recast Rules from the Findings Page

On the **Findings** page, you can create rules which change the status of Vulnerabilities or Host Audits or hide them. You can also create rules from **Settings** > **Recast**, as described in Create Recast Rules from Settings.

Tip: To learn more about when to create rules and how to manage them, see Recast Rules.

Here, you can create the following rule types:

Rule	Description
Recast	In the **Vulnerabilities** tab, modify the severity of vulnerability findings based on their Plugin ID.
Accept (for host vulnerabilities)	In the **Vulnerabilities** tab, accept the risk of vulnerability findings and hide them from the **Findings** workbench.
Change Result	In the **Host Audits** tab, modify the Result of host audit findings, for example by changing Failed results to Passed.
Accept (for host audits)	In the **Host Audits** tab, accept the Result of host audit findings and hide them from the the **Findings** workbench.

Add a Recast or Accept Rule

To add a Recast or Accept rule from the Findings page:

1. In the left navigation, click **Explore (Preview)** > **Findings**

   The **Findings** page appears.

2. In the table, in the row for the finding for which you want to create a rule, click the ⋮ button.

   A menu appears.

3. Click **Recast**.

   The **Add Recast Rule** window appears.

4. Configure the following options:

Option	Description
Action	Click **Accept** or **Recast**. To learn about these rule types, see About Recast and Accept Rules.
Description	Optionally, type a brief description of the rule.
Vulnerability Plugin ID	Type the Tenable Plugin ID for the vulnerability, for example *70658*.
New Severity	(Recast rules only) Select the severity you want to change the corresponding vulnerability to, for example *Low*. For more information, see Vulnerability Severity Indicators.
Targets	Select **All** or **Custom**. If the rule will override other rules, a warning appears. The most recently created rule trumps other rules.
Target Hosts	For **Custom** targets, enter up to 1000 comma-separated IPv4 addresses or ranges, hostnames, Classless Inter-Domain Routing (CIDR) notations, or fully qualified domain names (FQDNs). **Caution**: If you target findings by IP address and have multiple networks, the rule matches findings on all your networks. For more information, see Networks.
Expires	Select **After** or **Exact Date**. Then, type a number of days or a date when the rule will expire.
Comments	Type comments to provide rule details.
Report as False Positive to Tenable	(Optional) (Accept rules only) Turn on this toggle when a plugin generates inaccurate findings and you want Tenable to review the results.

5. Click **Save**.

The system processes the rule, which may take time. When complete, the **Findings** page updates and the rule appears in **Settings** > **Recast**.

Tip: For more information about **Recast** in **Settings**, see Recast Rules

Add a Change Result or Accept Rule

Note: For best performance, the system supports a maximum of *5000* Change Result and Accept rules in each container, total.

To add a Change Result or Accept rule:

1. In the left navigation, click **Explore (Preview)** > **Findings**.

   The **Findings** page appears.

2. In the left navigation, click **Host Audits**.
3. In the table, in the row for the finding for which you want to create a rule, click the ⋮ button.

   A menu appears.

4. Click **Add Recast Rule**.

   The Add Change Result Rule window appears.

5. Configure the following options:

Option	Description
Action	Click **Accept** or **Change Result**. To learn about these rule types, see About Change Result and Accept Rules.
Category	Select a category for the new rule, for example, *Windows*.
Audit File	Select an audit file to run against your assets, for example, *CIS_MS_Windows_11_Enterprise_Level_1_v1.0.0.audit*.
Audit Name	Type an audit name, for example, *9.3.1 Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'*.
Original Result	Select the original result of the host audit, for example, *Failed*.
New Result	(Change Result rules only) Select the result to change the targeted findings to.

Targets	(Optional) Select **Custom**. If the rule will override other rules, a warning appears. The most recently created rule trumps other rules.
Target Hosts	For **Custom** targets, type a comma-separated list of IPv4 addresses or ranges, hostnames, Classless Inter-Domain Routing (CIDR) notation, or fully qualified domain names (FQDNs). The system supports up to 100 items.
Expires	(Optional) Select **After** or **Exact Date**. Then, type a number of days or a date when the rule will expire.
Comments	Type comments to provide rule details.

6. Click **Save**.

   The system processes the rule, which may take time. When complete, the the **Findings** page updates and the rule appears in **Settings** > **Recast**.

Generate Findings Reports

On the **Findings** page, you can build a report about the vulnerabilities in your environment. You can also schedule this report and email it.

> **Note**: You can only generate reports for vulnerabilities findings. These reports must contain less than 10,000 findings. Additionally, you cannot run more than 50 reports at once.

To generate a report:

1. In the left navigation, click **Explore (Preview)** > **Findings**

   The **Findings** page appears.

2. (Optional) Using filters, refine the list of findings.
3. Select the findings to report on.

   Above the list of findings, the action bar appears.

4. In the action bar, click **Generate Report**.

   In the **Generate Report** dialog that appears, set the following options.

Option	Description
Name	(Optional) Type a name for the report.
Templates	Select a template for the report. Choose from the following templates: • **Host Findings Executive Summary Report** – Summarizes severity levels for the vulnerabilities you are reporting on, as well as the criticality, last scan time, and port count of the associated assets. • **Host Findings Vulnerability Details by Plugin** – Details the vulnerabilities you are reporting on by plugin. • **Host Findings Vulnerability Details by Asset** – Details associated assets for the vulnerabilities you are reporting on.
Schedule	Turn on the **Schedule** toggle to schedule the report: a. In the **Start Date and Time** section, choose the date and time when the report will run. b. In the **Time Zone** drop-down, choose a time zone. c. In the **Repeat** drop-down, choose the cadence on which you want the report to repeat (for example, daily). d. In the **Repeat Ends** drop-down, choose the date when the report will stop running.
Add Recipients	(Optional) Type the emails where you want Tenable Vulnerability Management to send the finished report.
Password Protection	(Optional) Enable this toggle to password-protect your report with AES 128-bit encryption. In the **Encryption Password** field, type a password to provide to the recipients.

5. Click **Generate Report**.

   A confirmation message appears and the system starts to build the report. Click the link in the message to view the report. Or, go to the **Reports** > **Report Results** page.

Export Findings

You can export data to CSV or JSON formats from the **Findings** page.

1. In the left navigation, click **Explore (Preview)** > **Findings**.

   The **Findings** page appears.

2. Do one of the following:

   - To export a single finding:
     - Above the selected finding, the action bar appears. In the action bar, click **Export**.
     - In the row for the finding that you want to export, click the ⋮ button.

       A menu appears.

       a. Click **Export**.
     - Click on a finding to open that finding's Finding Details pane.

       a. In the upper-right corner of the page, click the ⋮ button.

       A menu appears.

       b. Click **Export**.
   - To export multiple findings:

     a. In the findings list, select the checkbox next to each finding that you want to export.

     An action bar appears at the top of the list.

     b. In the action bar, click **Export**.

   The **Export** dialog appears.

3. Configure the following export options:

Option	Description
File Name	Type a name for the export.
Formats	Select an export format:

	• **CSV** – A CSV file that you can open in a spreadsheet application such as Microsoft Excel. **Note**: For findings exports, the system automatically trims fields longer than 32,000 characters so they appear correctly in Microsoft Excel. Select **Untruncated Data** to disable this. **Note:** If your export file contains a field starting with any of the following characters (=, +, -, @), the system adds a single quote (') at the beginning of the field. For more information, see the Knowledge Base. • **JSON** – A JSON file containing a nested list of findings.
Configuration	Search for and select the fields to include.
Expiration	Number of days the generated export file will be retained and displayed in the Export Activity list. Default is 3 days.
Schedule	Turn on the **Schedule** toggle and set the following options: a. Choose an export **Start Date** and **Start Time**. b. Choose a **Time Zone**. c. Under **Frequency**, choose how often you want the export to repeat. Choose either Once or one of the following: • Daily, also set **Repeat Every**. • Weekly, also set **Repeat Every** and **Repeat On** (for example, Mo, Tu, We, etc).

	• Monthly, also set **Repeat Every** and **Repeat By** (for example, Day of Month (Day 1)). d. Under **Repeat Ends**, choose when the exports end. If you choose **Never**, the export repeats until you modify or delete it.
Email Notifications	Turn on the **Email Notification** toggle and set the following options: a. Under **Add Recipients**, type the emails to notify. b. Under **Password**, type a password for the export file which the recipient will need to enter.

4. Click **Export**.

   The system processes the export and the file downloads to your computer. Processing may take several minutes.

   Tip: If you close the **Export** dialog before the download completes, you can access the export file in ⚙ **Settings** > [→ **Exports**.

Findings Filters

On the **Findings** tab in **Explore**, use the query builder to build custom queries that return the findings you need to see.

Tip: For the fastest results, Tenable recommends using the **Last Seen** filter in all queries to return findings from the last 30 days.

Important Usage Notes

Note: Custom query results for findings counts are cached for 60 minutes. The count updates every hour. This value can change if new scan data causes the findings counts to change during that 60-minute period.

Example Consider the following two queries:

Query 1:

```
state is equal to Resurfaced, Active, New
```

Query 2:

```
state is not equal to Fixed
```

Running additional scans within 60 minutes of the first query can result in different findings counts for the second query. The reason is that cached findings counts for the first query are not immediately updated with the new scan data.

Note: The counts for both queries will match if no new scan data changes the findings within 60 minutes.

The following table defines the filters you can use. This table explains the applicability of each filter, detailing which finding types may utilize each specific filter within queries.

Filter	Finding Type(s)	Description
ACR	**Vulnerabilities**	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10.
AES	**Vulnerabilities**	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Exposure Score as an integer from 0 to 1000.
Asset ID	**All**	The UUID of the asset where a scan detected the finding. This value is unique

Filter	Finding Type(s)	Description
		to Tenable Vulnerability Management.
Asset Name	**All**	The name of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management. This filter is case-sensitive, but you can use the wildcard character to turn this off.
Audit File	**Host Audits**	The name of Audit file the scanner used to perform the audit. Audit files are XML-based text files that contain the specific configuration, file permission, and access control tests to be performed.
Audit Name	**Host Audits**	The name Tenable assigned to the audit. In some cases, the compliance control may be listed as the prefix within the

Filter	Finding Type(s)	Description
		name.
Benchmark	**Host Audits**	Benchmarks are published best practices released from source authorities, such as Center for Internet Security (CIS), United States Defense Information Systems Agency (DISA), and Microsoft. This filter provides a list of the supported benchmarks and the version of the benchmark.
Benchmark Specification Name	**Host Audits**	The benchmark name.
Benchmark Version	**Host Audits**	The benchmark version. Use this filter with the **Benchmark** filter.
Bugtraq ID	**Web Application Findings, Vulnerabilities**	The Bugtraq ID for the plugin that identified the vulnerability.
Canvas Exploit	**Vulnerabilities**	The name of the CANVAS exploit

Filter	Finding Type(s)	Description
		pack that includes the vulnerability.
Categories	**Vulnerabilities**	The categories of software vulnerabilities. Possible values are displayed in the Query builder.
CERT Advisory ID	**Vulnerabilities**	The ID of the CERT advisory related to the vulnerability.
CERT Vulnerability ID	**Vulnerabilities**	The ID of the vulnerability in the CERT Vulnerability Notes Database.
CISA KEV Due Date	**Vulnerabilities**	The date on which Cybersecurity and Infrastructure Security Agency (CISA) Known Exploitable Vulnerability (KEV) remediation is due, as per Binding Operational Directive 22-01. Searches by the earliest due date for KEVs associated with the plugin. For more information,

Filter	Finding Type(s)	Description
		see the Known Exploited Vulnerabilities Catalog.
Common Name	**Vulnerabilities**	A vulnerability's common name, for example *Log4Shell*. Not all vulnerabilities have a common name.
Compliance Control	**Host Audits**	There are a series of designations within the compliance frameworks that Tenable calls controls. For example: CSF:DE.CM-3, 800-53:AU-12c, STIG-ID:WN10-AU-000045, and so on. This is a text-based field to filter on the specific control(s). Use this filter with the **Compliance Framework** filter.
Compliance Family Name	**Host Audits**	There are a series of designations within compliance frameworks that

Filter	Finding Type(s)	Description
		Tenable calls control. For example: ISO/IEC-27001:A.12.4.1, or CSF:DE.CM-1. This filter groups the controls into families for easier and more efficient queries. For example: A12 - Operations security or CSF:Detect. Use this filter with the **Compliance Framework** filter.
Compliance Framework	**Host Audits**	Tenable audits configuration compliance with a variety of standards including GDPR, ISO 27000, HIPAA, NIST 800-53, PCI DSS, and so on. This allows filtering based on the respective framework.
Control ID	**Host Audits**	An ID that can correlate results with other results that meet a certain benchmark recommendation.

Filter	Finding Type(s)	Description
		You can use this filter to identify checks in the audit portal.
CORE Exploit Framework	**Vulnerabilities**	Indicates whether an exploit for the vulnerability exists in the CORE Impact framework.
CPE	**Web Application Findings, Vulnerabilities**	The Common Platform Enumeration (CPE) numbers for vulnerabilities that the plugin identifies. (200 value limit)
CVE	**Web Application Findings, Vulnerabilities**	The Common Vulnerability and Exposure (CVE) IDs for the vulnerabilities identified by the plugin and corresponding to a specific finding. (200 value limit)
CVE (Product)	**Vulnerabilities**	The Common Vulnerability and Exposure (CVE) IDs for the vulnerabilities on the product where the finding was

Filter	Finding Type(s)	Description
		identified.
CVE Category	**Vulnerabilities**	The category of a vulnerability, as described in Vulnerability Categories.
CVSSv2 Base Score	**Web Application Findings, Vulnerabilities**	A numeric value between 0.0 and 10.0 that represents the intrinsic characteristics of a vulnerability independent of any specific environment.
CVSSv2 Temporal Score	**Vulnerabilities**	The CVSSv2 Temporal Score reflects the current real-world severity of a vulnerability, adjusting the Base Score based on factors that change over time.
CVSSv2 Temporal Vector	**Web Application Findings, Vulnerabilities**	CVSSv2 temporal metrics for the vulnerability.
CVSSv2 Vector	**Vulnerabilities**	The raw CVSSv2 metrics for the vulnerability. For more information,

Filter	Finding Type(s)	Description
		see the CVSSv2 documentation on the FIRST website.
CVSSv3 Attack Complexity	**Vulnerabilities**	The attack complexity, which defines how difficult it is to use a vulnerability in an attack. Options are **High** or **Low**.
CVSSv3 Attack Vector	**Vulnerabilities**	The attack vector, which defines an attack's location. Options are **Adjacent**, **Network**, **Local**, or **Physical**.
CVSSv3 Availability	**Vulnerabilities**	Quantifies the impact on the availability of the affected asset. Options are **High** (the asset is completely unavailable), **Low** (some reduced performance or interruption in availability), or **None** (no impact on the availability of the asset).

Filter	Finding Type(s)	Description
CVSSv3 Base Score	Web Application Findings, Vulnerabilities	A numeric value between 0.0 and 10.0 that represents the intrinsic characteristics of a vulnerability independent of any specific environment.
CVSSv3 Confidentiality	Vulnerabilities	The expected impact of the affected asset's information confidentiality loss. Options are **High**, **Low**, or **None**. For example, an affected asset with **High** confidentiality may have a catastrophic adverse effect on your organization or customers.
CVSSv3 Integrity	Vulnerabilities	The expected impact of the affected asset's data integrity loss. Options are **High**, **Low**, or **None**.
CVSSv3 Privileges Required	Vulnerabilities	The permission level attackers require to exploit the vulnerability. Options are **High**, **Low**, or

Filter	Finding Type(s)	Description
		None. For example, **None** means attackers need no permissions in your environment and can exploit the vulnerability while unauthorized.
CVSSv3 Scope	**Vulnerabilities**	If a vulnerability allows attackers to compromise resources beyond an affected asset's normal authorization privileges. Options are **Unchanged** or **Changed**. For example, **Changed** means the vulnerability increases the affected asset's privileges.
CVSSv3 Temporal Score	**Vulnerabilities**	The CVSSv3 temporal score (characteristics of a vulnerability that change over time but not among user environments).
CVSSv3 Temporal	**Vulnerabilities**	CVSSv3 temporal

Filter	Finding Type(s)	Description
Vector		metrics for the vulnerability.
CVSSv3 User Interaction	**Vulnerabilities**	If a vulnerability requires other users (such as end users) for attackers to be able to use it. Options are **Required** or **None**. **None** is more severe since it means no additional user interaction is required.
CVSSv3 Vector	**Web Application Findings, Vulnerabilities**	More CVSSv3 metrics for the vulnerability.
CVSSv4 Attack Complexity (AC)	**Web Application Findings, Vulnerabilities**	The conditions beyond the attacker's control that must exist to exploit the vulnerability.
CVSSv4 Attack Requirements (AT)	**Web Application Findings, Vulnerabilities**	The resources, access, or specialized conditions required for an attacker to exploit the vulnerability.
CVSSv4 Attack Vector	**Web Application**	The context where

Filter	Finding Type(s)	Description
(AV)	**Findings, Vulnerabilities**	vulnerability exploitation is possible, such as **Network** or **Local**.
CVSSv4 Base Score	**Web Application Findings, Vulnerabilities**	A numeric value between 0.0 and 10.0 that represents the intrinsic characteristics of a vulnerability independent of any specific environment.
CVSSv4 Privileges Required (PR)	**Web Application Findings, Vulnerabilities**	The level of privileges an attacker must possess to exploit the vulnerability.
CVSSv4 Subsequent System Availability Impact (SA)	**Web Application Findings, Vulnerabilities**	The impact on the availability of systems that can be impacted after the vulnerable system is exploited.
CVSSv4 Subsequent System Confidentiality Impact (SC)	**Web Application Findings, Vulnerabilities**	The impact on the confidentiality of systems that can be impacted after the vulnerable system is exploited.
CVSSv4 Subsequent	**Web Application**	The impact on the

Filter	Finding Type(s)	Description
System Integrity Impact (SI)	Findings, Vulnerabilities	integrity of systems that can be impacted after the vulnerable system is exploited.
CVSSv4 User Interaction (UI)	Web Application Findings, Vulnerabilities	The level of user involvement required for an attacker to exploit the vulnerability.
CVSSv4 Vulnerable System Availability Impact (VA)	Web Application Findings, Vulnerabilities	The impact on the availability of the vulnerable system when successfully exploited.
CVSSv4 Vulnerable System Confidentiality Impact (VC)	Web Application Findings, Vulnerabilities	The impact on the confidentiality of the vulnerable system when successfully exploited.
CVSSv4 Vulnerable System Integrity Impact (VI)	Web Application Findings, Vulnerabilities	The impact on the integrity of the vulnerable system when successfully exploited.
CWE	Web Application Findings, Vulnerabilities	The Common Weakness Enumeration (CWE) for the vulnerability.
Default/Known Account	Vulnerabilities	Indicates whether the plugin that

Filter	Finding Type(s)	Description
		identified the vulnerability checks for default accounts.
Elliot Exploit	**Vulnerabilities**	The name of the exploit for the vulnerability in the D2 Elliot Web Exploitation framework.
EPSS Score	**Vulnerabilities**	The percentage likelihood that a vulnerability will be exploited, based on the third-party Exploit Prediction Scoring System (EPSS). Type a number from 0 to 100 with up to three decimal places, for example, *75.599*.
Exploit Database ID	**Vulnerabilities**	The ID of the vulnerability in the Exploit Database.
Exploit Maturity	**Vulnerabilities**	The exploit maturity based on sophistication and availability. This information is drawn from Tenable's own research as well as

Filter	Finding Type(s)	Description
		key external sources. Options are **High**, **Functional**, **PoC**, or **Unproven**.
Exploitability Ease	**Vulnerabilities**	A description of how easy it is to exploit the vulnerability.
Exploited By Malware	**Vulnerabilities**	Indicates whether the vulnerability is known to be exploited by malware.
Exploited By Nessus	**Vulnerabilities**	Indicates whether Tenable Nessus exploited the vulnerability during the process of identification.
ExploitHub	**Vulnerabilities**	Indicates whether an exploit for the vulnerability exists in the ExploitHub framework.
Finding ID	**Vulnerabilities**	The unique Tenable ID for the finding. To view the ID for a finding, click its details and check the page URL in your browser's address

Filter	Finding Type(s)	Description
		bar for an alphanumeric string between *details* and *asset*.
First Audited	**Host Audits**	Identifies the first date the audit check was performed on the asset.
First Discovered	**Vulnerabilities**	The date the vulnerability corresponding to a finding was first identified.
First Functional Exploit	**Vulnerabilities**	The date a vulnerability was first known to be exploited.
First Proof of Concept	**Vulnerabilities**	The date a vulnerability's first proof of concept was found.
First Seen	**Web Application Findings, Vulnerabilities**	The date when a scan first found the vulnerability on an asset.
Fix Available	**Vulnerabilities**	If a fix is available for the corresponding vulnerability. Options are **Yes** or **No**.

Filter	Finding Type(s)	Description
FQDNs	Host Audits	The fully qualified domain names (FQDNs) for the asset.
IAVA ID	Vulnerabilities	The ID of the information assurance vulnerability alert (IAVA) for the vulnerability.
IAVB ID	Vulnerabilities	The ID of the information assurance vulnerability bulletin (IAVB) for the vulnerability.
IAVM Severity	Vulnerabilities	The severity of the vulnerability in Information Assurance Vulnerability Management (IAVM).
IAVT ID	Vulnerabilities	The ID of the information assurance vulnerability technical bulletin (IAVT) for the vulnerability.

Filter	Finding Type(s)	Description
In The News	**Vulnerabilities**	Indicates whether this plugin has received media attention (for example, ShellShock, Meltdown).
Input Name	**Web Application Findings**	The name of the specific web application component that the vulnerability exploits.
Input Type	**Web Application Findings**	The web application component type (for example, form, cookie, header) that the vulnerability exploits.
IPv4 Address	**All**	The IPv4 address for the affected asset. You can add up to 100 IP addresses to this filter.
IPv6 Address	**Host Audits, Vulnerabilities**	The IPv6 address for the affected asset.
Last Audited	**Host Audits**	Identifies the date of the most recent audit check performed on the asset.
Last Fixed	**All**	The last time a

Filter	Finding Type(s)	Description
		previously detected vulnerability was scanned and noted as no longer present on an asset.
Last Seen	**All**	The date when a scan last found the vulnerability on an asset.
Live Result	**Vulnerabilities**	TBD
Malware	**Vulnerabilities**	Indicates whether the plugin that identified the vulnerability checks for malware.
Metasploit Exploit	**Vulnerabilities**	The name of the related exploit in the Metasploit framework.
Microsoft Bulletin	**Vulnerabilities**	The Microsoft security bulletin that the plugin, which identified the vulnerability, covers.
Network	**Vulnerabilities**	The name of the network object associated with scanners that identified the asset. The default name is

Filter	Finding Type(s)	Description
		Default. For more information, see Networks.
Original Result	**Host Audits**	The result from the initial audit.
Original Severity	**Web Application Findings, Vulnerabilities**	The vulnerability's CVSS-based severity when a scan first detected the finding. For more information, see CVSS vs. VPR.
OSVDB ID	**Vulnerabilities**	The ID of the vulnerability in the Open Sourced Vulnerability Database (OSVDB).
OWASP 2010	**Web Application Findings**	The Open Web Application Security Project (OWASP) 2010 category for the vulnerability targeted by the plugin.
OWASP 2013	**Web Application Findings**	The Open Web Application Security Project (OWASP) 2013 category for the vulnerability targeted by the plugin.
OWASP 2017	**Web Application**	The Open Web

Filter	Finding Type(s)	Description
	Findings	Application Security Project (OWASP) 2017 category for the vulnerability targeted by the plugin.
OWASP 2021	**Web Application Findings**	The Open Web Application Security Project (OWASP) 2021 category for the vulnerability targeted by the plugin.
OWASP API 2019	**Web Application Findings**	The Open Web Application Security Project (OWASP) 2019 category for the API vulnerability targeted by the plugin.
Patch	**Vulnerabilities**	If a patch is available for the vulnerability.
Patch Published	**Vulnerabilities**	The date on which the vendor published a patch for the vulnerability.
Path	**Vulnerabilities**	The complete installation path of the software where a vulnerability was detected.
Plugin Description	**Web Application**	The description of

Filter	Finding Type(s)	Description
	Findings, Vulnerabilities	the Tenable plugin that identified the vulnerability.
Plugin Family	**Web Application Findings, Vulnerabilities**	The family of the plugin that identified the vulnerability. (200 value limit)
Plugin ID	**All**	The ID of the plugin that identified the vulnerability. (200 value limit)
Plugin Modification Date	**Web Application Findings, Vulnerabilities**	The date at which the plugin that identified the vulnerability was last modified.
Plugin Name	**All**	The name of the plugin that identified the vulnerability.
Plugin Output	**Vulnerabilities**	Use this filter to return findings with plugin output that you specify. Search for a value in the plugin output using the **contains** or **does not contain** operator, as described in Use Filters.

Filter	Finding Type(s)	Description
		Caution: Due to technical constraints in how the underlying system processes large data in JSON format, only the first 20,000,000 characters of raw plugin data are available when searching plugin output. If your search is too broad, the system suggests adding **Plugin ID** and **Last Seen** to refine the results and then displays the top ten plugins from that search. For example, to search for output that contains “Kernel,” in Advanced mode, type: `Plugin Output contains Kernel` **Note**: Manually enable this filter in **Settings** > **General** **Search** > **Enable**

Filter	Finding Type(s)	Description
		Plugin Output Search. If you do not use this filter for 35 days, it is disabled again. **Plugin Output search best practices...** Since plugin outputs can be large, broad searches may cause system timeouts! For the best results, combine the **Plugin Output** filter with the **Plugin ID** and **Last Seen** filters. Limit the number of plugin IDs you search at once. Specify plugin ID(s) to search for plugins or exclude them. These approaches apply to different use cases. For example, include plugins when searching for software listings by operating system. Exclude plugins from exploratory searches where the top plugins

Filter	Finding Type(s)	Description

		appear too frequently.
		• **Search for output from one plugin:**
		`Plugin Output contains Kernel AND Plugin ID is equal to 110483`
		• **Search for output from multiple plugins:**
		`Plugin Output contains Chrome AND Plugin ID is equal to 45590, 10456`
		• **Search for output from any plugin but the ones listed:**
		`Plugin Output`

Filter	Finding Type(s)	Description
		`contains Chrome AND Plugin ID is not equal to 45590, 10456`
Plugin Published	**Web Application Findings, Vulnerabilities**	The date on which the plugin that identified the vulnerability was published.
Plugin Type	**Vulnerabilities**	The general type of plugin check. Options are **Local**, **Remote**, **Local & Remote**, **Summary**, **Settings**, **Reputation**, and/or **Third Party**.
Plugins Available	**Vulnerabilities**	If a vulnerability currently has a Tenable plugin that detects it. Options are **Yes** or **No**.
Port	**Vulnerabilities**	Information about the port the scanner used to connect to the asset where the scan detected the vulnerability. (200 value limit)

Filter	Finding Type(s)	Description
Product	**Vulnerabilities**	The name of the product on which the vulnerability was detected.
Product Type	**Vulnerabilities**	The type of product. Options are **Application**, **Hardware**, **Operating System**, **Package**.
Protocol	**Vulnerabilities**	The protocol the scanner used to communicate with the asset where the scan detected the vulnerability.
Result	**Host Audits**	The current or modified result from the audit check.
Result Modified	**Host Audits**	Rules can be created to accept or modify the results of an audit check. This filter allows you to report modified results.
Resurfaced Date	**Vulnerabilities**	The most recent date that a scan detected a Resurfaced vulnerability which was previously

Filter	Finding Type(s)	Description
		Fixed. If a vulnerability is Resurfaced multiple times, only the most recent date appears.
Risk Modified	**Web Application Findings, Vulnerabilities**	The risk modification applied to the vulnerability's severity. Options are **Recast**, **Accepted**, and **None**. To learn more, see Recast Rules.
Scan Origin	**Vulnerabilities**	The scanner that detected the finding.
Secunia ID	**Vulnerabilities**	The ID of the Secunia research advisory related to the vulnerability.
See Also	**Web Application Findings, Vulnerabilities**	Links to external websites that contain helpful information about the vulnerability.
Severity	**Web Application Findings, Vulnerabilities**	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.
Solution	**Web Application**	A brief summary of

Filter	Finding Type(s)	Description
	Findings, Vulnerabilities	how you can remediate the vulnerability.
Source	**Vulnerabilities**	The source of the scan that identified the asset. Possible values include **Agent** for Tenable Agent, **Nessus** for Tenable Nessus, **PVS/NNM** for Tenable Network Monitor, and **WAS** for Tenable Web App Scanning.
State	**Web Application Findings, Vulnerabilities**	The state of the vulnerability detected in the finding. Options are Fixed, Resurfaced, Active, New. Appears in the vulnerability findings query builder by default, with **Active**, **Resurfaced** and **New** selected. For more information, see Vulnerability States.
Stig Severity	**Vulnerabilities**	The STIG severity associated with the finding.

Filter	Finding Type(s)	Description
Synopsis	**Vulnerabilities**	A brief description of the plugin or vulnerability.
Tags	**Vulnerabilities**	Asset tags, entered in pairs of `category` and `value` (for example Network: Headquarters). This includes the space after the colon (:). If there is a comma in the tag name, insert a backslash (\) before the comma. If your tag name includes double quotation marks (" "), use the UUID instead. You can add a maximum of 100 tags. For more information, see Tags.
Time Taken to Fix	**Vulnerabilities**	How long it took your organization to fix a vulnerability identified on a scan in days. Only appears for Fixed vulnerabilities. Use

Filter	Finding Type(s)	Description
		this filter along with the **State** filter set to **Fixed** for more accurate results. When exported, this field is shown in milliseconds.
Unsupported by Vendor	**Vulnerabilities**	Software found by this plugin is unsupported by the software's vendor (for example, Windows 95 or Firefox 3).
URL	**Web Application Findings**	The complete URL on which the scanner detected the vulnerability.
Vendor	**Vulnerabilities**	The vendor who makes the product on which the vulnerability was identified, for example, *Apache*.
Vendor Severity	**Vulnerabilities**	The severity of a vulnerability as assigned by a CVE Numbering Authority (CNA). Unlike a National Vulnerability

Filter	Finding Type(s)	Description
		Database (NVD) score, which reflects the worst-case scenario, this rating accounts for mitigations.
Version	**Vulnerabilities**	The version of the product on which the vulnerability was identified.
VPR	**Web Application Findings, Vulnerabilities**	The Vulnerability Priority Rating that Tenable calculated for the vulnerability.
VPR (Beta) Key Driver CVE ID	**Web Application Findings, Vulnerabilities**	Filter on a specific CVE ID for the CVE that is a primary contributor to the calculated VPR (Beta) score for a vulnerability.
VPR (Beta) Key Driver Exploit Chain	**Web Application Findings, Vulnerabilities**	Allows filtering on CVEs that are part of an exploit chain.
VPR (Beta) Key Driver Code Maturity	**Web Application Findings, Vulnerabilities**	Filter on current availability and maturity of exploit code. Options are **High**, **Functional**, **POC**, and

Filter	Finding Type(s)	Description
		Unproven.
VPR (Beta) Key Driver Probability	**Web Application Findings, Vulnerabilities**	Filter on the probability of exploitation produced by the VPR (Beta) threat model for the CVE.
VPR (Beta) Key Driver In the News Intensity, last 30 days	**Web Application Findings, Vulnerabilities**	Allows filtering on the volume of news reporting on the CVE within the last 30 days. Options are **Very Low**, **Low**, **Medium**, **High**, **Very High**.
VPR (Beta) Key Driver In the News Recency	**Web Application Findings, Vulnerabilities**	Allows filtering on the recency of news sources reporting on the CVE. Options are **No Recorded Events**, **60 to 180 days**, **30 to 60 days**, **14 to 30 days**, **7 to 14 days**, **0 to 7 days**.
VPR (Beta) Key Driver In the News Sources, last 30 days	**Web Application Findings, Vulnerabilities**	Filter on categories of news sources that have referenced the CVE within the last 30 days. Select from one or more of

Filter	Finding Type(s)	Description
		Academic and Research Institutions, **Blogs and Individual Researchers**, **Code Repositories**, **Cybersecurity News Media**, **Cybersecurity Vendors**, **Forums and Community Platforms**, **Government and Regulatory**, **Mainstream News and Media**, **Security Research**, **Technology Companies**, **Tools and Resources**, **Other**.
VPR (Beta) Key Driver Malware Observations Intensity, last 30 days	**Web Application Findings**, **Vulnerabilities**	Filter on the volume of observed malware exploiting the CVE within the last 30 days. Options are **Very Low**, **Low**, **Medium**, **High**, **Very High**.
VPR (Beta) Key Driver Malware Observations Recency	**Web Application Findings**, **Vulnerabilities**	Filter on the recency of observed malware

Filter	Finding Type(s)	Description
		exploiting the CVE. Options are **No Recorded Events**, **60 to 180 days**, **30 to 60 days**, **14 to 30 days**, **7 to 14 days**, **0 to 7 days**.
VPR (Beta) Key Driver On CISA KEV	**Web Application Findings, Vulnerabilities**	Filter on whether the CVE is listed on the CISA Known Exploited Vulnerabilities list. Options are **Yes**, **No**.
VPR (Beta) Key Driver Targeted Industries	**Web Application Findings, Vulnerabilities**	Allows filtering on specific industries where attacks leveraging the CVE have been observed. Sample options include **Banking**, **Technology**, **Government**.
VPR (Beta) Key Driver Targeted Regions	**Web Application Findings, Vulnerabilities**	Allows filtering on specific geographic regions where attacks leveraging the CVE have been observed.
VPR (Beta) Key Driver VPR Percentile	**Web Application Findings, Vulnerabilities**	Filter on the VPR (Beta) score percentile ranking of

Filter	Finding Type(s)	Description
		the CVE, indicating its position relative to other vulnerabilities.
VPR (Beta) Key Driver VPR Severity	**Web Application Findings, Vulnerabilities**	Filter on the VPR (Beta) severity categorization of the CVE. Options are **Critical**, **High**, **Medium**, **Low**, **Info**.
VPR (Beta) Score	**Web Application Findings, Vulnerabilities**	The numerical VPR (Beta) score itself. Allows filtering by specific ranges or values of the updated vulnerability priority rating.
VPR Threat Intensity	**Vulnerabilities**	A vulnerability's Tenable-calculated threat intensity based on the number and frequency of threat events. Options are **Very Low**, **Low**, **Medium**, **High**, or **Very High**.
Vuln SLA Date	Vulnerabilities, Web Application Findings	The date that the finding was last activated. It equals either the **First Seen** date when the finding is new or active or

Filter	Finding Type(s)	Description
		the **Resurfaced Date** if the finding is resurfaced.
Vulnerability Published	**Vulnerabilities**	The date when the vulnerability definition was first published (for example, the date that the CVE was published).
WASC	**Web Application Findings**	The Web Application Security Consortium (WASC) category associated with the vulnerability targeted by the plugin.
Weaponization	**Vulnerabilities**	If a vulnerability is judged to be ready for use in a cyberattack. Options are **Advanced Persistent Threat**, **Botnet**, **Malware**, **Ransomware**, or **Rootkit**.
Workaround	**Vulnerabilities**	If a workaround is available for the vulnerability.
Workaround Type	**Vulnerabilities**	The type of workaround

Filter	Finding Type(s)	Description
		available, if relevant. Possible values are **Configuration Change** and **Disable Service**.

Findings Columns

On the **Findings** tab in **Explore**, you can view the findings in your environment broken down into categories including vulnerabilities, the results of host audits, and web application findings.

The **Findings** tab has the following columns, which you can show or hide as described in Use Tables. When displaying columns or exporting values for a finding, the available column names vary by finding type. This table clarifies the columns you can display or export for each respective finding type.

Column	Finding Type(s)	Description
Account ID	**Vulnerabilities**	The unique identifier assigned to the asset resource in the cloud service that hosts the asset.
ACR	**Vulnerabilities**	(Requires Tenable One or Tenable Lumin license) The Tenable-defined Asset Criticality Rating (ACR) as an integer from 1 to 10.
AES	**Vulnerabilities**	(Requires Tenable

Column	Finding Type(s)	Description
		One or Tenable Lumin license) The Tenable-defined Asset Exposure Score as an integer from 0 to 1000.
AI/LLM Tools	Vulnerabilities, Web Application Findings	Indicates an informational finding about artificial intelligence services running on an asset. Hover on the **AI/LLM Tools** column to view details.
Asset ID	All	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Vulnerability Management.
Asset Name	All	The name of the asset. This value is unique to Tenable Vulnerability Management.

Column	Finding Type(s)	Description
Audit File	**Host Audits**	The name of the audit file the scanner used to perform the compliance check.
Audit Name	**Host Audits**	The name of the compliance check the scanner performed on the affected asset.
CVSSv2 Base Score	**Vulnerabilities, Web Application Findings**	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). Tenable Vulnerability Management shows the **CVSSv2** or **CVSSv3** column depending on the **Vulnerability Severity Metric** setting.
CVSSv3 Base Score	**Vulnerabilities, Web Application Findings**	The CVSSv3 base score (intrinsic and fundamental

Column	Finding Type(s)	Description
		characteristics of a vulnerability that are constant over time and user environments). Tenable Vulnerability Management shows the **CVSSv2** or **CVSSv3** column depending on the **Vulnerability Severity Metric** setting.
CVSSv4 Base Score	**Vulnerabilities, Web Application Findings**	The CVSSv4 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). To learn more, see the CVSSv4 specification.
Description	**All**	If present, a description of the vulnerability corresponding to the finding.

Column	Finding Type(s)	Description
EPSS	**Vulnerabilities**	EPSS Score. The percentage likelihood that a vulnerability will be exploited in the wild.
Fix Type	**Vulnerabilities**	The type of fix, for example, *version*.
Fix Version	**Vulnerabilities**	If present, the version number of the fix for the vulnerability corresponding to the finding.
First Seen	**Vulnerabilities, Web Application Findings**	The date when a scan first found the vulnerability on an asset.
IPv4 Address	**Vulnerabilities**	The IPv4 address for the affected asset.
IPv6 Address	**Vulnerabilities**	The IPv6 address for the affected asset.
Last Audited	**Host Audits**	Date of the most recent compliance check that was performed on the asset.

Column	Finding Type(s)	Description
Last Fixed	**Vulnerabilities**	The last time a previously detected vulnerability was scanned and noted as no longer present on an asset.
Last Scan Target	**Vulnerabilities**	The IP address or fully qualified domain name (FQDN) of the asset targeted in the last scan.
Last Seen	**Vulnerabilities, Web Application Findings**	The date when a scan last found the vulnerability on an asset.
Live Result	**Vulnerabilities**	Indicates whether the scan result is based on live results. In Agentless Assessment, you can use live results to view scan results for new plugins based on the most recently collected snapshot data,

Column	Finding Type(s)	Description
		without running a new scan. The possible values are **Yes** or **No**.
Original Result	**Host Audits**	The result from the initial audit.
Path	**Vulnerabilities**	The complete installation path of the software where a vulnerability was detected.
Plugin Family	**Vulnerabilities, Web Application Findings**	The family of the plugin that identified the vulnerability.
Plugin ID	**Vulnerabilities, Web Application Findings**	The ID of the plugin that identified the vulnerability.
Plugin Name	**All**	The name of the plugin that identified the vulnerability. Hover on the ⓘ icon to view a detailed summary that includes metrics and plugin output.

Column	Finding Type(s)	Description
Port	**Vulnerabilities**	The port that the scanner used to connect to the asset where the scan detected the vulnerability.
Product	**Vulnerabilities**	The name of the product on which the vulnerability was detected.
Product Type	**Vulnerabilities**	The type of product, for example, *Application*.
Protocol	**Vulnerabilities**	The protocol the scanner used to communicate with the asset where the scan detected the vulnerability.
Region	**Vulnerabilities**	The cloud region where the asset runs.
Result	**Host Audits**	The current or modified result from the audit check.
Result Modified Reason	**Host Audits**	Explanation for why the result of a compliance check

Column	Finding Type(s)	Description
		was modified.
Result Modified Expires	**Host Audits**	Date the modified compliance check result will expire.
Resurfaced Date	**Vulnerabilities**	The most recent date that a scan detected a Resurfaced vulnerability which was previously Fixed. If a vulnerability is Resurfaced multiple times, only the most recent date appears.
Scan Origin	**Vulnerabilities**	The scanner that detected the finding. Also identifies if the scan is a work-load scan. Possible values for this column are: Tenable Vulnerability Management, Tenable Security Center, and Agentless

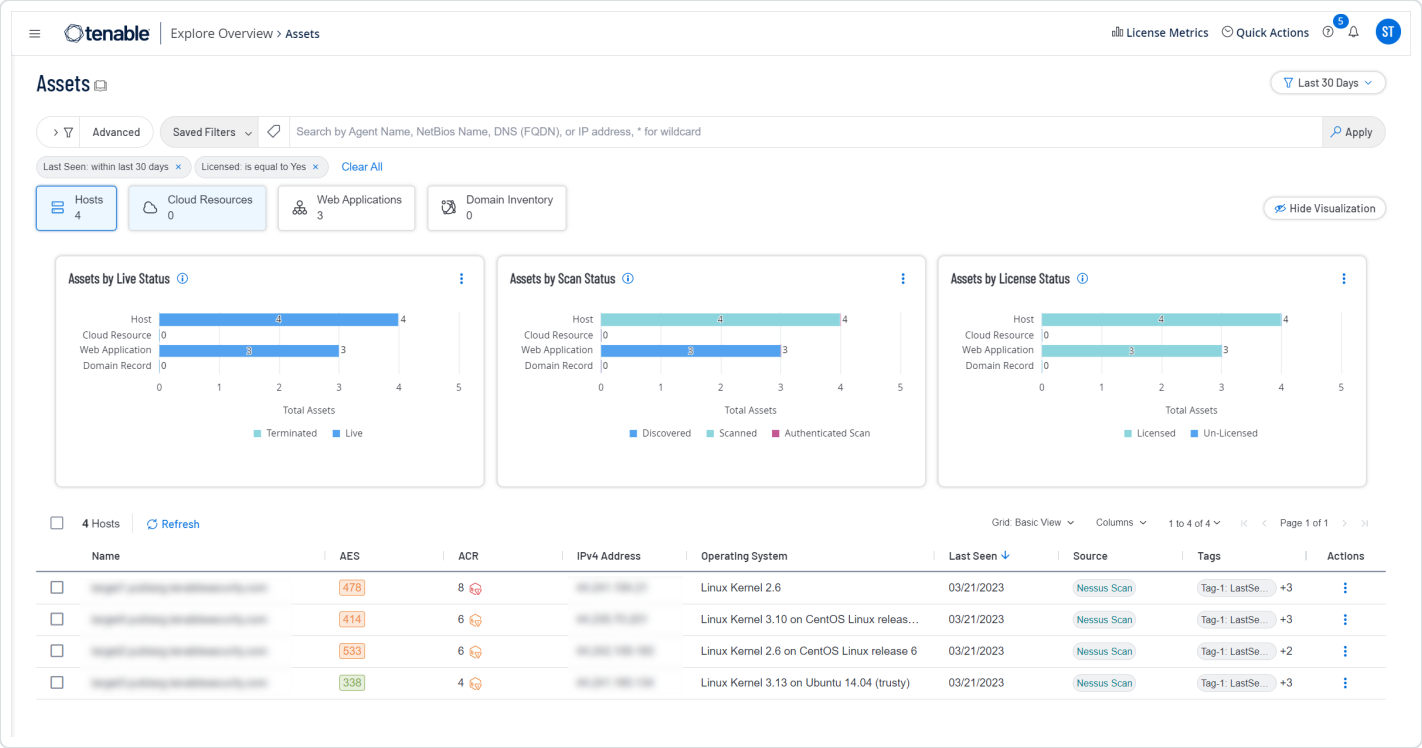
Column	Finding Type(s)	Description
		Assessment.
Severity	**Vulnerabilities, Web Application Findings**	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.
State	**Vulnerabilities, Web Application Findings**	The state of the vulnerability. For more information, see Vulnerability States.
Tags	**All**	Asset tags, entered in pairs of `category` and `value` (for example Network: Headquarters). This includes the space after the colon (:). If there is a comma in the tag name, insert a backslash (\) before the comma. If your tag name includes double quotation marks (" "), use the UUID instead. You can add a maximum of 100 tags.

Column	Finding Type(s)	Description
		For more information, see Tags.
Time Taken to Fix	**Vulnerabilities**	How long it took your organization to fix a vulnerability identified on a scan in days. Only appears for Fixed vulnerabilities. Use this filter along with the **State** filter set to **Fixed** for more accurate results. When exported, this field is shown in milliseconds.
Vendor	**Vulnerabilities**	The vendor who makes the product on which the vulnerability was identified, for example, *Apache*.
Version	**Vulnerabilities**	The version of the product on which the vulnerability was identified.
VPR	**Vulnerabilities, Web Application**	A descriptive icon indicating the VPR

Column	Finding Type(s)	Description
	Findings	of the vulnerability. For more information, see CVSS vs. VPR.
VPR (Beta)	**Vulnerabilities, Web Application Findings**	A descriptive icon indicating the VPR (Beta) of the vulnerability. For more information, see CVSS vs. VPR.
Vuln SLA Date	Vulnerabilities, Web Application Findings	The date that the finding was last activated. It equals either the **First Seen** date when the finding is new or active or the **Resurfaced Date** if the finding is resurfaced.

Assets

Assets are entities of value on your network that can be exploited. They include laptops, desktops, servers, routers, mobile phones, virtual machines, software containers, and cloud instances. Use the Assets workbench to get insight into assets broken down into four categories: host assets, cloud resources, web applications, and domain inventory.



When scans complete or you import scan results, Tenable Vulnerability Management uses an algorithm to look at the hosts from the scan or the import. It employs heuristics to match hosts with existing assets and update any changed properties—or, when no match is found, to create new assets. When available, Tenable Vulnerability Management also collects information about asset interfaces (IP and MAC address), DNS name, NetBIOS name, operating system, installed software, UUIDS (Tenable, ePO, BIOS), and if an Agent is installed.

> **Note**: Tenable Vulnerability Management ages out assets which have not been updated for more than 15 months.

The topics in this section explain how to use the **Assets** workbench, view asset details, export assets, use filters, and more.

- Use the Assets Workbench

View Asset Details

Asset Filters

Open Ports and the Assets workbench

Asset Widgets

Edit the ACR for Host Assets

Move Assets to Another Network

Remove and Prevent Duplicate Assets

Download Inventory Data

Delete Assets

Use the Assets Workbench

You can view all your assets on the **Assets** workbench.

Important: Due to differences in the asset source, asset counts within the **Tags** section may not match the asset counts within the **Assets** section of Tenable Vulnerability Management.

To view your assets:

1. In the left navigation, click **Assets**.

   The **Assets** workbench appears.

2. (Optional) To show or hide asset types, click the following tiles:

   - Host Assets
   - Cloud Resources
   - Web Applications
   - Domain Inventory

On the **Assets** workbench, you can do the following:

- In the Search box, search by Agent Name, NetBios Name, DNS (FQDN), or IP Address. Use (*) as a wildcard.
- Filter the displayed assets and customize your view, as described in Explore Tables.

  Tip: To view definitions for all Asset filters, see Asset Filters.
- Save filters as a custom search, as described in Saved Filters.
- Export assets to CSV or JSON format, as described in Export Findings or Assets.
- Filter the displayed assets by time period with a drop-down in the upper-right corner.
- View details about an asset, as described in View Asset Details.
- View visualizations for the displayed assets, as described in Asset Widgets.
- In any asset tile, select **Only Show Unmanaged Assets** to view assets which have been discovered, but not assessed for vulnerabilities.

Host Assets

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Assets** workbench, to view only your host assets, select the **Hosts** tile and deselect other tiles. Common host assets include workstations, servers, virtual machines, printers, network switches, routers, and wireless access points.

The **Hosts** tile contains a table with the following columns. To show or hide columns, see Customize Explore Tables.

Column	Description
Asset ID	The UUID of the asset. This value is unique to Tenable Vulnerability Management.
Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.
AES	The Asset Exposure Score of the asset.

AES (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset Exposure Score* using a new algorithm. This metric weighs an asset's Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) and then assigns a number from 1 to 1000, with higher numbers for more exposed assets. For more information, see Scoring (Beta).
ACR	The Asset Criticality Rating of the asset.
ACR (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset-Criticality Rating* using a new algorithm based on asset profile, which assigns assets to classes by business and device function. This metric rates the importance of an asset to your organization from 1 to 10, with higher numbers for more critical assets. For more information, see Scoring and Asset Criticality Rating.
IPV4 Address	The IPv4 address for the affected asset.
IPV6 Address	The IPv6 address for the affected asset.
Operating System	One of the operating system(s) that a scan identified on the asset.
Operating System List	All of the operating systems that a scan identified on the asset.
Licensed	Indicates if the asset is licensed within Tenable Vulnerability Management. For more information, see Tenable Vulnerability Management Licenses.
First Seen	The date and time when a scan first identified the asset.
Last Seen	The date when a scan last found the vulnerability on an asset.
Last Licensed Scan	The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management

	Licenses.
Last Authenticated Scan	The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field.
Last Scan Target	The IP address or fully qualified domain name (FQDN) of the asset targeted in the last scan.
Source	The source of the scan that identified the asset.
Tags	Tags applied to the asset.
System Type	The operating system installed on the asset.
NetBIOS Name	The asset's NetBIOS name.
DNS (FQDN)	The fully qualified domain name of the asset host. **Note:** When processing fully qualified domain names (FQDNs) for host assets, Tenable Vulnerability Management normalizes all FQDNs to lowercase and then merges any duplicates.
MAC Address	A MAC address that a scan has associated with the asset record.
ServiceNow Sys ID	Where applicable, the unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.
Agent Name	The name of the Tenable Nessus agent that scanned and identified the asset.
Created Date	The date and time when Tenable Vulnerability Management created the asset record.
Updated Date	The date and time when Tenable Vulnerability Management last updated the asset record.
Has Plugin Results	Specifies whether the asset has plugin results associated with it.
Public	Specifies whether the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public`

	attribute in the Tenable Vulnerability Management`query` namespace.
AWS Availability Zone	Where applicable, the AWS availability zone of the asset, as described in the Tenable Vulnerability Management AWS documentation.
AWS EC2 AMI ID	Where applicable, the AWS EC2 AMI ID of the asset, as described in the Tenable Vulnerability Management AWS documentation.
AWS EC2 Instance ID	Where applicable, the AWS EC2 instance ID of the asset, as described in the Tenable Vulnerability Management AWS documentation.
AWS Security Group	Where applicable, the AWS security group of the asset, as described in the Tenable Vulnerability Management AWS documentation.
AWS Instance State	Where applicable, the AWS instance state of the asset, as described in the Tenable Vulnerability Management AWS documentation.
AWS Instance Type	Where applicable, the AWS instance type of the asset, as described in the Tenable Vulnerability Management AWS documentation.
AWS EC2 Name	Where applicable, the AWS EC2 name of the asset, as described in the Tenable Vulnerability Management AWS documentation.
AWS EC2 Product Code	Where applicable, the AWS EC2 product code of the asset, as described in the Tenable Vulnerability Management AWS documentation.
AWS Owner ID	Where applicable, the AWS owner ID of the asset, as described in the Tenable Vulnerability Management AWS documentation.
AWS Region	Where applicable, the AWS region of the asset, as described in the Tenable Vulnerability Management AWS documentation.
AWS Subnet ID	Where applicable, the AWS subnet ID of the asset, as described in the Tenable Vulnerability Management AWS documentation.
AWS VPC ID	Where applicable, the AWS VPC ID of the asset, as described in the Tenable Vulnerability Management AWS documentation.
Azure Resource ID	Where applicable, the Azure resource ID of the asset, as described in the Tenable Vulnerability ManagementMicrosoft Azure documentation.

Azure VM ID	Where applicable, the Azure VM ID of the asset, as described in the Tenable Vulnerability Management Microsoft Azure documentation.
Google Cloud Instance ID	Where applicable, the Google cloud instance ID of the asset, as described in the Tenable Vulnerability Management Google Cloud Platform documentation.
Google Cloud Project ID	Where applicable, the Google cloud project ID of the asset, as described in the Tenable Vulnerability Management Google Cloud Platform documentation.
Google Cloud Zone	Where applicable, the Google cloud zone of the asset, as described in the Tenable Vulnerability Management Google Cloud Platform documentation.
Resource Tags	Specifies the tags or labels that have been imported from the cloud provider. This field appears for assets with source as **Cloud Discovery Connector**. **Note:** Tenable Vulnerability Management imports tags and labels with the following considerations: • For AWS and Azure, the limit is 50 tags per resource. • For GCP, the limit is 64 labels per resource. • Tenable Vulnerability Management does not support importing JSON strings for Azure tags.
Cloud Provider	Indicates whether the asset is from AWS, Azure, or GCP.
Actions	In this column, click the ⋮ button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **Add Tags** – Add new tags. In the dialog that appears, choose a *Category* and *Value*, as described in Tags. • **Remove Tags** – Remove existing tags. In the dialog that appears, click a tag and click **Remove**.

	• **Edit ACR** - (Tenable One or Tenable Lumin only). Edit the Asset Criticality Rating, as described in Edit the ACR for Host Assets. • **Move** – Move an asset to another network, as described in Move Assets to Another Network. • **View All Details** – View complete details for an asset, as described in View Asset Details. • **View All Details in New Tab** – View complete details for an asset in a new browser tab. • **View All Solutions** – View available solutions for asset vulnerabilities, as described in Solutions. • **Delete** – Permanently delete an asset, as described in Delete Assets.

Cloud Resources

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Assets** workbench, to view only your cloud resources, select the **Cloud Resources** tile and deselect other tiles. A cloud resource can be any compute instance, storage object, networking device, or object you can create or configure within a cloud platform. Examples of cloud resources include assets such as virtual servers, buckets, databases, disks, and containers. Other examples of cloud resources are configurable items such as resource groups, policies, users, and roles.

The **Cloud Resources** tile contains a table with the following columns. To show or hide columns, see Customize Explore Tables.

Column	Description
Asset ID	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Vulnerability Management.
Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.

Resource Type	The name of the cloud resource type (for example, a resource group or virtual machine).
Resource Category	The name of the category to which your cloud resource type belongs (for example, object storage or virtual network).
Resource Tags	Tags synced from a cloud source such as Amazon Web Services (AWS). Only the first tag is shown. Hover on the displayed tag to view a complete list.
Cloud Provider	The name of the cloud provider that hosts the asset.
Region	The cloud region where the asset runs.
Licensed	Indicates if the asset is licensed within Tenable Vulnerability Management. For more information, see Tenable Vulnerability Management Licenses.
First Seen	The date and time when a scan first identified the asset.
Last Seen	The date when a scan last found the vulnerability on an asset.
Source	The source of the scan that identified the asset.
Tags	Any Tenable Vulnerability Management tags applied to the asset.
Created Date	The date and time when Tenable Vulnerability Management created the asset record.
Updated Date	The date and time when Tenable Vulnerability Management last updated the asset record.
Actions	In this column, click the ⋮ button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **Add Tags** – Add new tags. In the dialog that appears, choose a *Category* and *Value*, as described in Tags. • **Remove Tags** – Remove existing tags. In the dialog that appears, click a tag and click **Remove**.

Web Applications

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Assets** workbench, to view only your web application assets, select the **Web Applications** tile and deselect other tiles. A web application is software that runs in a browser. Examples of web applications are: workplace collaboration apps, ecommerce apps, email apps, and banking apps.

The **Web Applications** tile contains a table with the following columns. To show or hide columns, see Customize Explore Tables.

Column	Description
Asset ID	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Vulnerability Management.
Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.
AES	The Asset Exposure Score of the asset.
ACR	The Asset Criticality Rating of the asset.
Licensed	Indicates if the asset is licensed within Tenable Vulnerability Management. For more information, see Tenable Vulnerability Management Licenses.
SSL/TLS	Specifies whether the application on which the asset is hosted uses SSL/TLS public-key encryption.
IPV4 Address	The IPv4 address for the affected asset.
Operating System	The operating system installed on the asset.
First Seen	The date and time when a scan first identified the asset.
Last Seen	The date when a scan last found the vulnerability on an asset.
Last Licensed Scan	The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan

	uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses.
Last Authenticated Scan	The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field.
Public	Specifies whether the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable Vulnerability Managementquery namespace.
Source	The source of the scan that identified the asset.
Tags	Tags applied to the asset.
Created Date	The date and time when Tenable Vulnerability Management created the asset record.
Updated Date	The date and time when Tenable Vulnerability Management last updated the asset record.
Actions	In this column, click the ⋮ button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **Add Tags** – Add new tags. In the dialog that appears, choose a *Category* and *Value*, as described in Tags. • **Remove Tags** – Remove existing tags. In the dialog that appears, click a tag and click **Remove**. • **View All Details** – View complete details for a finding, as described in View Finding Details. • **Delete** – Permanently delete an asset, as described in Delete Assets.

Domain Inventory

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Assets** workbench, to view only your domain inventory assets, select the **Domain Inventory** tile and deselect other tiles. A domain inventory is a complete account of every domain owned by your organization. Domains are associated with a wide range of assets: databases, applications, directory services, and identity or access management platforms.

The **Domain Inventory** tile contains a table with the following columns. To show or hide columns, see Customize Explore Tables.

Column	Description
Asset ID	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Vulnerability Management.
Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.
Host Name	The name of the host of the asset.
Record Type	The type of asset.
Record Value	The record value of the asset.
Domain	The domain to which the asset belongs.
DNS (FQDN) (ASM)	The fully qualified domain name of the asset host.
IPv4 Address (ASM)	The IPv4 address for the asset.
IPv6	The IPv6 address for the asset.

Address (ASM)	
Hosting Provider	The provider hosting the asset.
ASN	The Autonomous System Number (ASN) of the asset.
Licensed	Indicates if the asset is licensed within Tenable Vulnerability Management. For more information, see Tenable Vulnerability Management Licenses.
First Seen	The date and time when a scan first identified the asset.
Last Seen	The date when a scan last found the vulnerability on an asset.
Source	The source of the scan that identified the asset.
Tags	Tags applied to the asset.
Created Date	The date and time when Tenable Vulnerability Management created the asset record.
Updated Date	The date and time when Tenable Vulnerability Management last updated the asset record.
Port	The port associated with the asset.
Actions	In this column, click the ⋮ button to view a drop-down where you can: • **Add Tags** – Add new tags. In the dialog that appears, choose a *Category* and *Value*, as described in Tags. • **Remove Tags** – Remove existing tags. In the dialog that appears, click a tag and click **Remove**. • **Create Advanced Network Scan** – Create an advanced network scan, as described in Create a Scan • **Create Web Application Scan** – Create a web application scan, as described in Create a Scan • **Delete** – Permanently delete an asset, as described in Delete Assets.

View Asset Details

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Vulnerability Management Permission: Can View permission for applicable assets.

From the **Assets** workbench, you can drill down into a single asset to view it on the **Asset Details** page. Tenable Vulnerability Management customizes this page by asset type.

Note: Domain Inventory assets do not have an **Asset Details** page, but you can view them in a preview, as described in Domain Inventory Preview.

To view asset details:

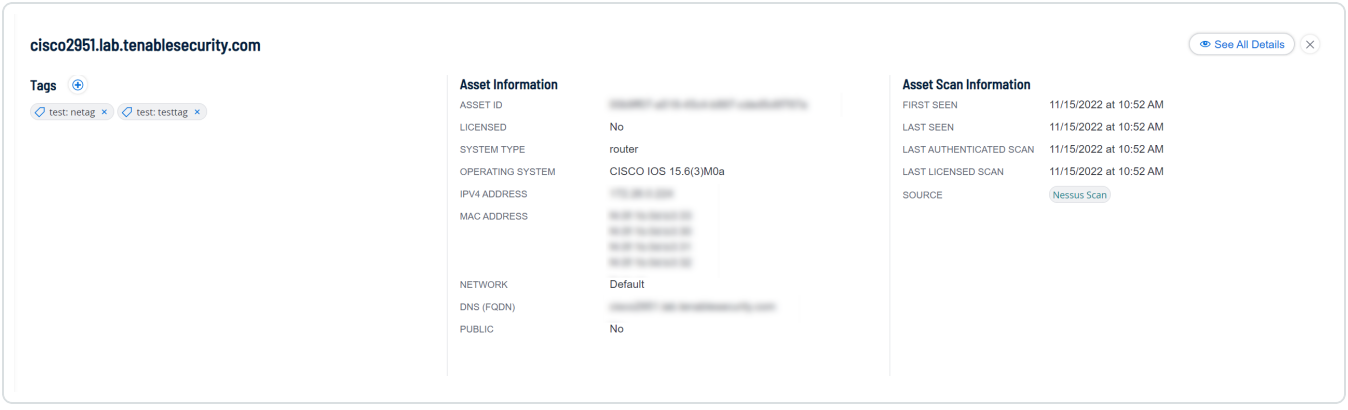
1. In the left navigation, click **Assets**.

   The **Assets** workbench appears.

2. (Optional) Click another asset tile to show or hide asset types or or use filters to refine your results.

3. Click the row for the asset to view.

   At the bottom of the page, a preview appears.



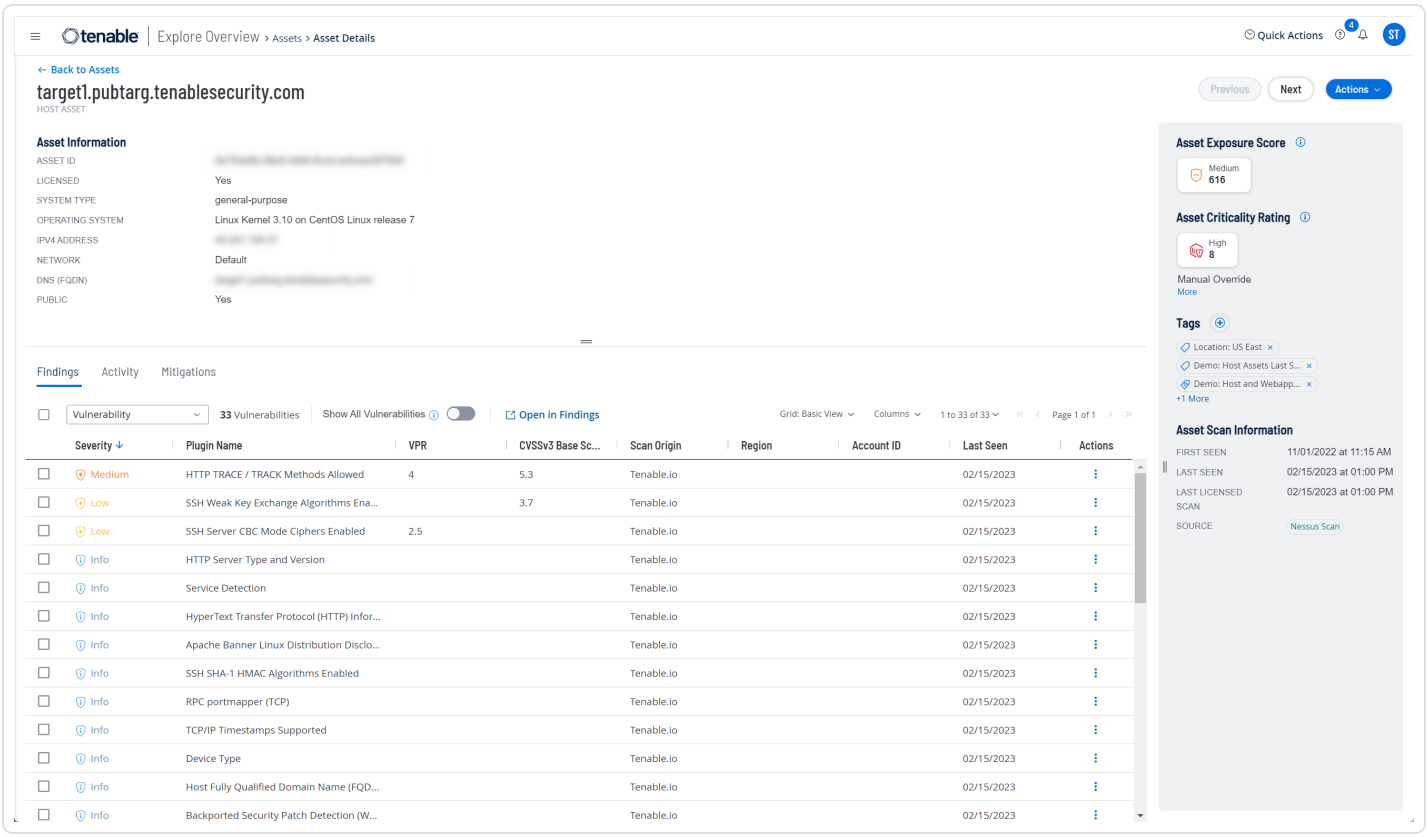
4. In the preview, click **See All Details**.

   The **Asset Details** page appears. Its layout varies by asset type as follows:

- Host Asset Details
- Cloud Resource Details
- Web Application Details

Host Asset Details

When you View Asset Details, the **Asset Details** page varies by asset type. For host assets, it includes asset information, a list of associated findings, the AES, and the ACR.



The **Asset Details** page for host assets contains the following sections.

Note: Tenable Vulnerability Management hides empty sections, so these may not appear in some cases.

Section	Description
Header	The asset header; based on the presence of certain attributes in the following logical order: 1. Agent name

	2. Local hostname 3. NetBIOS name 4. Fully Qualified Domain Name (FQDN) 5. IPv4 address 6. IPv6 address
Asset Information	Information about the host asset, including: • **Asset ID** – The UUID of the asset. • **Licensed** – Specifies whether the asset is licensed. • **System Type** – The system types as reported by Plugin ID 54615. For more information, see Tenable Plugins. • **Operating System** – The operating system that a scan identified as installed on the asset. • **IPv4 Address** – An IPv4 address for the asset. • **IPv6 Address** – An IPv6 address for the asset. • **MAC Address** – The MAC address for the asset. • **Network** – The name of the network object associated with scanners that identified the asset. The default network name is **Default**. For more information about networks, see Networks. • **Agent Name** – The name of the Tenable Agent that scanned and identified the asset. • **DNS (FQDN)** – The fully qualified domain name of the asset host. • **SSH Fingerprint** – The SSH key fingerprints that scans have associated with the asset record. • **Tenable ID** – A UUID created for new assets during credentialed scans or agent scans. If an asset is found not to be unique, this UUID is not created and an existing one is reused.

	• **Installed Software** – A log of the Common Platform Enumeration (CPE) strings for the asset, identifying its software, hardware, or firmware using a standardized naming convention. This information is drawn from the National Vulnerability Database and Tenable's own plugins. • **Public** – Specifies whether the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable Vulnerability Managementquery namespace. • **BIOS ID** – The asset's BIOS UUID. • **ServiceNow Sys ID** – Where applicable, the unique record identifier of the asset in ServiceNow. • **Network Device Serial ID** – The unique identifier of the asset as assigned by the manufacturer. This property is only available for network devices. • **Custom Attributes** – Custom attributes added to the asset. For more information, see the Tenable Developer Portal.
Findings	Click the **Findings** tab to view all findings associated with the asset: • In the drop-down, switch between **Vulnerability** and **Host Audit** findings. • Click the **Show All Vulnerabilities** toggle to hide Fixed and Accepted vulnerabilities or host audits. • Click **Open in Findings** to view all findings on the **Findings** workbench. • In a finding row, click ⋮ to show a menu where you can view findings details, export a finding, or launch a remediation scan. • Show or hide columns, as described in Customize Explore Tables.
Open Ports	Click the **Open Ports** tab to view open ports on the asset:

	• **Open Ports** – Specifies open ports on the asset. • **Protocol** – Specifies the protocol with which information is transported to the open port, for example, TCP or UDP. • **First Detected Open** – The date and time the port was first detected as open. • **Last Detected Open** – The date and time the port was last detected as open. • **Service** – The service running on the open port, such as HTTPS, SSH, or FTP. To learn more about possible services, see Service Name and Transport Protocol on the *Internet Assigned Numbers Authority* website.
Activity	Click the **Activity** tab to view activity for the asset: • **Event** – Specifies all asset events logged by Tenable Vulnerability Management, for example, Asset Discovered. • **Date** – Specifies the event date. • **Source** – Specifies the event source, for example, Nessus Scan.
Mitigations	Click the **Mitigations** tab to view information about any mitigation software that a scan identified on the asset.
Asset Exposure Score	(Requires Tenable Lumin license) An icon indicating the Asset Exposure Score (AES) calculated for the asset.
Asset Criticality Rating	(Requires Tenable Lumin license) An icon indicating the asset's Asset Criticality Rating.
Cloud Resource Information	Cloud resource information including: • **AWS Availability Zone** – The AWS EC2 AMI ID of the asset. For more information, see the Tenable Vulnerability Management AWS documentation. • **AWS EC2 AMI ID** – The AWS EC2 instance ID of the asset.

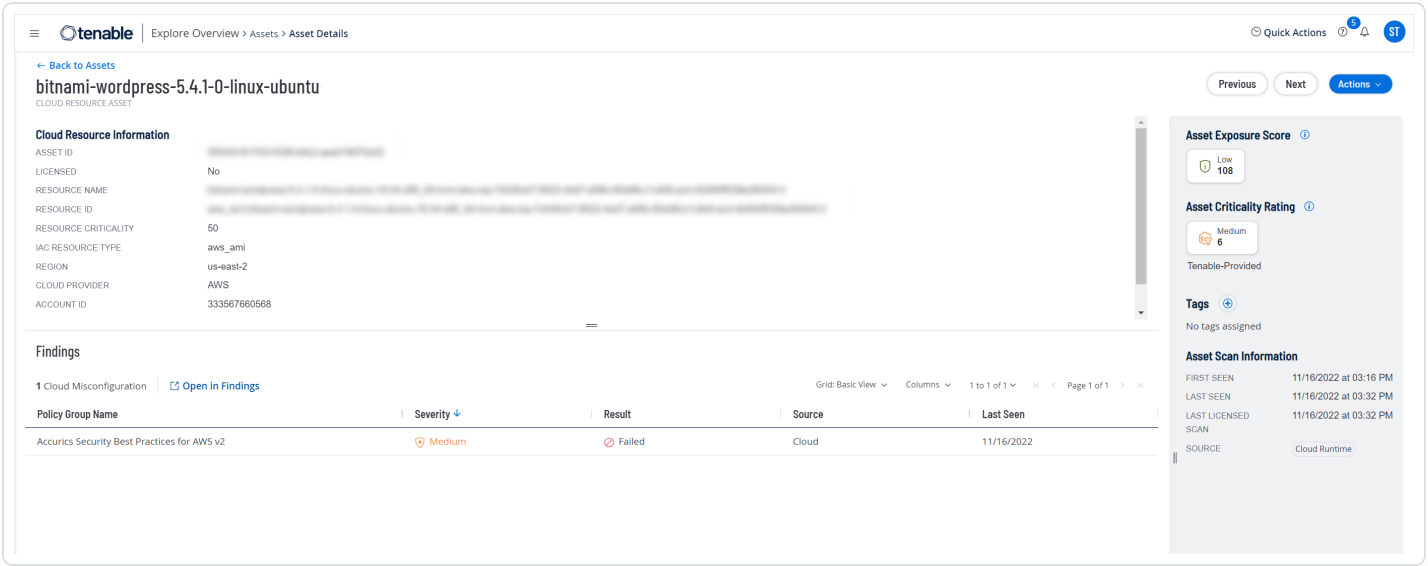
	• **AWS EC2 Instance ID** – The AWS EC2 instance ID of the asset. • **AWS Security Group** – The AWS security group of the asset. • **AWS Instance State** – The AWS instance state of the asset. • **AWS instance Type** – The AWS instance type of the asset. • **AWS EC2 Name** –The AWS EC2 name of the asset. • **AWS EC2 Product Code** – The AWS EC2 product code of the asset. • **AWS Owner ID** – The AWS owner ID of the asset. • **AWS Region** – The AWS region of the asset. • **AWS Subnet ID** – The AWS subnet ID of the asset. • **AWS VPC ID** – The AWS VPC ID of the asset. • **Google Cloud Instance ID** – The Google cloud instance ID of the asset. For more information, see the Tenable Vulnerability ManagementGoogle Cloud Platform documentation. • **Google Cloud Project ID** –The Google cloud project ID of the asset. • **Google Cloud Zone** – The Google cloud zone of the asset.
Tags	Tags applied to the asset. To add a tag, click the ⊕ button. To remove a tag, click the ✕ button on the tag label. For more information, see Tags.
Asset Scan Information	Information about the asset's scan history, including: • **First Seen** – The time and date when a scan first identified the asset. • **Last Seen** – The date and time of the scan that most recently identified the asset. • **Last Authenticated Scan** – The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated**

	Scan field, but not the **Last Licensed Scan** field. • **Last Authentication Attempt** – The last time that Tenable Nessus attempted to sign in, either with SSH on Unix-based systems or SMB on Windows. • **Last Authentication Status** – The last authentication attempt by Tenable Nessus was successful. • **Last Successful Authentication** – The last time that Tenable Nessus authenticated successfully. • **Last Licensed Scan** – The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses. • **Source** – The source of the scan that identified the asset. • **Last Scan Target** – The IP address or fully qualified domain name (FQDN) of the asset targeted in the last scan. • **Days Since Last Active** – For assets observed on a Tenable Agent scan, the time in days since the agent observed the asset.
Remote Authenticated Scan Information	Information about remote authenticated scans performed on the asset: • **Last Authentication Attempt** – The last time and date that a Tenable Nessus scanner attempted to log into the asset • **Last Authentication Status** – The authentication status of the Tenable Nessus scanner's last attempted login. • **Last Successful Authentication** – The last time and date that a Tenable Nessus scanner successfully logged into the asset.
Actions	In the upper-right corner, click the **Actions** button to view a drop-down where you can:

- **Export** – Export to CSV or JSON, as described in Export from Explore Tables.
- **Add Tags** – Add new tags. In the dialog that appears, choose a *Category* and *Value*, as described in Tags.
- **Remove Tags** – Remove existing tags. In the dialog that appears, click a tag and click **Remove**.
- **Edit ACR** - (Tenable One or Tenable Lumin only). Edit the Asset Criticality Rating, as described in Edit the ACR for Host Assets.
- **Move** – Move an asset to another network, as described in Move Assets to Another Network.
- **View All Solutions** – View available solutions for asset vulnerabilities, as described in Solutions.
- **Delete** – Permanently delete an asset, as described in Delete Assets.

Cloud Resource Details

When you View Asset Details, the **Asset Details** page varies by asset type. For cloud resource assets, it includes a summary, a list of associated findings, the AES, and the ACR.



The **Asset Details** page for cloud resources contains the following sections.

Note: Tenable Vulnerability Management hides empty sections, so these may not appear in some cases.

Section	Description
Header	The asset header; based on the presence of certain attributes in the following logical order: 1. Agent name 2. NetBIOS name 3. Local hostname 4. Fully Qualified Domain Name (FQDN) 5. IPv4 address 6. IPv6 address
Cloud Resource Information	Information about the cloud resource, including: • **Asset ID** – The resource's UUID. • **Licensed** – Whether the resource is licensed. • **Resource Name** – The name of the resource. • **Resource ID** – The unique identifier assigned to the resource in the cloud service that hosts it. • **Resource Criticality** – The criticality rating for the resource according to Tenable Container Security, based on the most recent scan. • **Region** – The cloud region where the resource runs. • **Cloud Provider** – The name of the cloud provider that hosts the asset. • **Account ID** – The account ID for the Legacy Tenable Cloud Security account associated with the resource. **Note**: This field is no longer used as it is from an old version of Tenable Cloud Security. • **VPC** – Virtual Private Cloud; the unique identifier of the public cloud

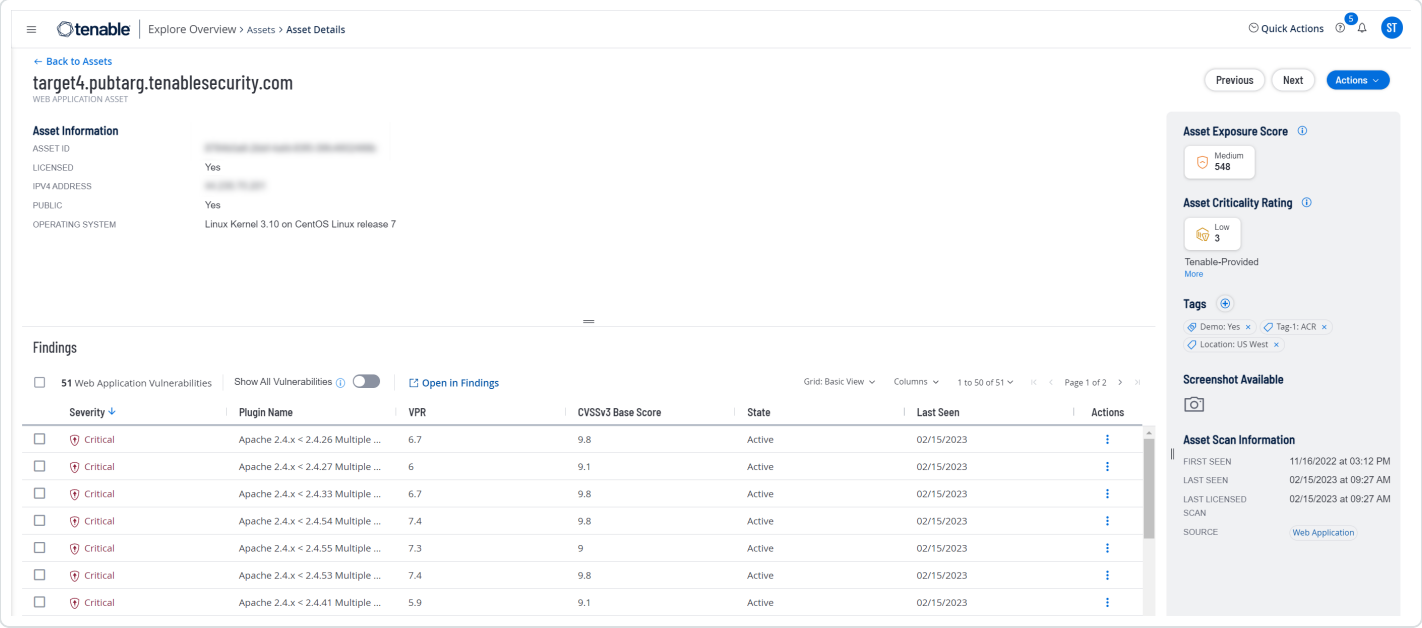
	that hosts the AWS virtual machine instance. • **Resource Type** – The asset's cloud resource type (for example, network, virtual machine). • **Resource Category** – The name of the category to which your cloud resource type belongs (for example, object storage or virtual network). • **Resource Tag** - The labels associated with the resource by the cloud provider. • **IaC Resource Type** – The Terraform resource type associated with the Infrastructure as Code (IaC) cloud resource asset. • **Repositories** – The path to the asset's source directory. • **Has Drift** – Indicates whether the asset has any drifts. • **Is Mapped** – Indicates whether the asset is mapped. • **Project** – The cloud project associated with the asset. • **Network** – The name of the network to which the scanner that scans the asset belongs. For more information, see Networks. • **Availability Zone** – The name of the availability zone where the virtual machine instance is hosted.
Findings	A table that lists all the findings associated with the resource. Click **Open in Findings** to view the Vulnerabilities page.
Asset Exposure Score	(Requires Tenable Lumin license) An icon indicating the Asset Exposure Score calculated for the asset.
Asset Criticality Rating	(Requires Tenable Lumin license) An icon indicating the asset's Asset Criticality Rating.
Tags	Tags applied to the asset. To add a tag, click the ⊕ button. To remove a tag, click the ✕ button on the tag label. For more information, see Tags.

Asset Scan Information	• **First Seen** – The time and date when a scan first identified the asset. • **Last Seen** – The date and time of the scan that most recently identified the asset. • **Last Licensed Scan** – The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses. • **Last Authenticated Scan** – The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field. • **Source** – The source of the scan that identified the asset.
Actions	In the upper-right corner, click the **Actions** button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **Add Tags** – Add new tags. In the dialog that appears, choose a *Category* and *Value*, as described in Tags. • **Remove Tags** – Remove existing tags. In the dialog that appears, click a tag and click **Remove**. • **View All Details** – View complete details for an asset, as described in View Asset Details. • **View All Details in New Tab** – View complete details for an asset in a new browser tab.

Web Application Details

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

When you View Asset Details, the **Asset Details** page varies by asset type. For web application assets, it includes asset information, a list of associated findings, the AES, and the ACR.



The **Asset Details** page for web application assets contains the following sections.

Note: Tenable Vulnerability Management hides empty sections, so these may not appear in some cases.

Section	Description
Header	The asset header; based on the presence of certain attributes in the following logical order: 1. Agent name 2. NetBIOS name 3. Local hostname 4. Fully Qualified Domain Name (FQDN) 5. IPv4 address 6. IPv6 address

Asset Information	Information about the asset, including: • **Asset ID** – The UUID of the asset. • **Licensed** – Specifies whether the asset is licensed. • **System Type** – The system types as reported by Plugin ID 54615. For more information, see Tenable Plugins. • **IPv4 Address** – The first IPv4 address for the asset. If there is no IPv4 address, then the first IPv6 for the asset. • **Public** – Specifies whether the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable Vulnerability Managementquery namespace. • **DNS** – The fully qualified domain name of the asset host. • **Operating System** – The operating system that a scan identified as installed on the asset. • **Network** – The name of the network object associated with scanners that identified the asset. The default network name is **Default**. For more information, see Networks. • **MAC Address** – The static Media Access Control (MAC) address for the asset. • **SSH Fingerprint** – The SSH key fingerprints that scans have associated with the asset record. • **Tenable UUID** – The unique identifier for the Tenable account associated with the asset. • **Custom Attributes** – Custom attributes added to the asset. For more information, see the Tenable Developer Portal.
Findings	A table that lists all the findings associated with the asset. In this section, you can perform the following actions: • Export selected findings.

	• Click **Open in Findings** to view the Vulnerabilities page for the asset.
Asset Exposure Score	(Requires Tenable Lumin license) An icon indicating the Asset Exposure Score for the asset.
Asset Criticality Rating	(Requires Tenable Lumin license) An icon indicating the asset's Asset Criticality Rating.
Screenshot Available	An interactive button that indicates whether a screenshot is available. To view a screenshot, click the button.
Tags	Tags applied to the asset. To add a tag, click the button. To remove a tag, click the button on the tag label. For more information, see Tags.
Scan Information	Information about the asset's scan history, including: • **First Seen** – The date and time when a scan first identified the asset. • **Last Seen** – The date and time at which the asset was last observed as part of a scan. • **Source** – The source of the scan that identified the asset.
Actions	In the upper-right corner, click the **Actions** button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **Add Tags** – Add new tags. In the dialog that appears, choose a *Category* and *Value*, as described in Tags. • **Remove Tags** – Remove existing tags. In the dialog that appears, click a tag and click **Remove**. • **View All Details** – View complete details for an asset, as described in View Asset Details. • **View All Details in New Tab** – View complete details for an asset in a

	new browser tab. • **Delete** – Permanently delete an asset, as described in Delete Assets.

Domain Inventory Preview

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Assets** workbench, click a domain inventory asset to preview its details.

The preview contains the following sections.

Section	Description
Header	The asset header; based on the presence of certain attributes in the following logical order: 1. Agent name 2. NetBIOS name 3. Local hostname 4. Fully Qualified Domain Name (FQDN) 5. IPv4 address 6. IPv6 address
Tags	Tags applied to the asset. To add a tag, click the ⊕ button. To remove a tag, click the × button on the tag label. For more information, see Tags.
Asset Information	Information about the asset, including: • **Asset ID** – The UUID of the asset. • **Licensed** – Specifies whether the asset is licensed. • **IPV4 Address** – The first IPv4 address for the asset. • **IPV6 Address** –The first IPv6 address for the asset.
Asset Scan	Information about the asset's scan history, including:

Information	• **First Seen** – The date and time when a scan first identified the asset. • **Last Seen** – The date and time at which the asset was last observed as part of a scan. • **Updated Date** – The date and time when the asset record was last updated. • **Source** – The source of the scan that identified the asset.
Related Assets	Links to filtered lists of assets, showing the other times Tenable Vulnerability Management scans identified the asset.

Asset Filters

On the **Assets** page, you can filter your assets via standard filters that apply to all assets or by asset-specific filters.

You can save a set of commonly used filters as a saved filter to access later or share with other members of your team.

Note: To optimize performance, Tenable limits the number of filters that you can apply to any **Explore** > **Assets** views (including **Group By** tables) to 35.

Note: You can right-click on values within a table cell to use the **Filter By** option. For more information, see Right-Click Filtering.

You can select from the following filter types:

All

The following table describes the filters that apply to all assets:

Filter	Description
Account ID	The unique identifier assigned to the asset resource in the cloud service that hosts the asset. **Note**: This filter is no longer used, as it is from a legacy version of Tenable Cloud Security.

ACR	(Requires Tenable Lumin license) The asset's ACR.
ACR (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset-Criticality Rating* using a new algorithm based on asset profile, which assigns assets to classes by business and device function. This metric rates the importance of an asset to your organization from 1 to 10, with higher numbers for more critical assets. For more information, see Scoring and Asset Criticality Rating.
ACR Severity	(Requires Tenable Lumin license) (Requires Tenable One or Tenable Lumin license) The ACR category of the ACR calculated for the asset.
AES	(Requires Tenable Lumin license)The Asset Exposure Score (AES) calculated for the asset.
AES (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset Exposure Score* using a new algorithm. This metric weighs an asset's Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) and then assigns a number from 1 to 1000, with higher numbers for more exposed assets. For more information, see Scoring (Beta).
AES Severity	(Requires Tenable Lumin license) (Requires Tenable Lumin license) The AES category of the AES calculated for the asset.
Agent Name	The name of the Tenable Nessus agent that scanned and identified the asset.
ARN	The Amazon Resource Name (ARN) for the asset.
ASN	The Autonomous System Number (ASN) for the asset.
Assessed vs. Discovered	Specifies whether Tenable Vulnerability Management scanned the asset for vulnerabilities or if Tenable Vulnerability Management only discovered the asset via a discovery scan. Possible values are: • **Assessed** • **Discovered Only**

	Note: This filter is selected by default.
Asset ID	The asset's unique identifier.
AWS Availability Zone	The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see Regions and Zones in the AWS documentation.
AWS EC2 AMI ID	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Instance ID	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Name	The name of the virtual machine instance in Amazon EC2.
AWS EC2 Product Code	The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2.
AWS Instance State	The state of the virtual machine instance in AWS at the time of the scan. For possible values, see InstanceState in the Amazon Elastic Compute Cloud Documentation.
AWS Instance Type	The type of virtual machine instance in Amazon EC2. Amazon EC2 instance types dictate the specifications of the instance (for example, how much RAM it has). For a list of possible values, see Amazon EC2 Instance Types in the AWS documentation.
AWS Owner ID	A UUID for the Amazon AWS account that created the virtual machine instance. This attribute only appears for Amazon EC2 instances. For more information, see View AWS Account Identifiers in the AWS documentation
AWS Region	The region where AWS hosts the virtual machine instance, for example, `us-east-1`.
AWS Security Group	The AWS security group (SG) associated with the Amazon EC2 instance.

AWS Subnet ID	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.
AWS VPC ID	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud Documentation.
Azure Location	The location of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure Resource Group	The name of the resource group in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure Resource ID	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager documentation.
Azure Resource Type	The resource type of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure Subscription ID	The unique subscription identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure VM ID	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see the Azure Resource Manager documentation.
BIOS ID	The NetBIOS name for the asset.
Cloud Provider	The name of the cloud provider that hosts the asset.
Created Date	The date and time when Tenable Vulnerability Management created the asset record.
Custom Attribute	A filter that searches for custom attributes via a category-value pair. For more information about custom attributes, see the Tenable Developer Portal.
DNS	The fully-qualified domain name of the host that the vulnerability was detected on.

Domain	The domain to which the asset belongs.
First Seen	The date and time when a scan first identified the asset.
Google Cloud Instance	The unique identifier of the virtual machine instance in Google Cloud Platform (GCP).
Google Cloud Project ID	The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see Creating and Managing Projects in the GCP documentation.
Google Cloud Zone	The zone where the virtual machine instance runs in GCP. For more information, see Regions and Zones in the GCP documentation.
Has Plugin Results	Specifies whether the asset has plugin results associated with it.
Host Name (Domain Inventory)	The host name for assets found during attack surface management scans; only for use with Domain Inventory assets.
Hosting Provider	The hosting provider for the asset.
IaC Resource Type	The Infrastructure as Code (IAC) resource type of the asset.
Installed Software	A list of Common Platform Enumeration (CPE) values that represent applications identified on an asset from a scan. This field supports the CPE 2.2 format. For more information, see the Component Syntax section of the CPE Specification documentation. For assets identified in Tenable scans, this field only contains data when a scan using Tenable Nessus Plugin 45590 has evaluated the asset.
IPV4 Address	The IPv4 address associated with the asset record.
IPV6 Address	The IPv6 address associated with the asset record.
Is Attribute	Specifies whether the asset is an attribute.

Is Auto Scale	Specifies whether the asset scales automatically.
Is Unsupported	Specifies whether the asset is unsupported in Tenable Vulnerability Management.
Last Audited	The time and date at which the asset was last audited.
Last Authenticated Scan	The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field.
Port Last Detected Open	Filter for all assets that had detected open ports as of a date or a date range you specify. For the best results, combine with the **Ports** filter.
Last Licensed Scan	The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses.
Last Scan Time	The date when a scan was last run against the asset.
Last Seen	The date and time at which the asset was last observed as part of a scan.
Licensed	Specifies whether the asset is included in the asset count for the Tenable Vulnerability Management instance.
MAC Address	A MAC address that a scan has associated with the asset record.
Mitigated	Specifies whether a scan has identified mitigation software on the asset.
Mitigation Last Detection	The date and time of the scan that last identified mitigation software on the asset.
Mitigation Product Name	The name of the mitigation software identified on the asset. Tenable Lumin defines mitigations as security agent software running on endpoint assets, which include antivirus software, Endpoint Protection Platforms (EPPs), or Endpoint Detection and Response (EDR) solutions.

Mitigation Vendor Name	The name of the vendor for the mitigation that a scan identified on the asset.
Mitigation Version	The version of the mitigation that a scan identified on the asset.
Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address. **Note**: This filter is selected by default.
NetBIOS Name	The NetBIOS name for the asset.
Network	The name of the network object associated with scanners that identified the asset. The default name is **Default**. For more information, see Networks.
Operating System	One of the operating system(s) that a scan identified on the asset. **Note**: This filter is selected by default.
Operating System (WAS)	The Tenable Web App Scanning (Tenable Web App Scanning) operating system that a scan identified as installed on the asset.
Port	Search your hosts or domain inventory by port values or ranges for assets with a relationship to that port. For example, assets with port 80. If you import data from Tenable Attack Surface Management, those ports also appear.
Public	Specifies whether the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable Vulnerability Management `query` namespace.
Record Type	The asset type.
Region	The cloud region where the asset runs.
Repositories	Any code repositories associated with the asset.

Resource Type	The asset's cloud resource type (for example, network, virtual machine). **Note**: This filter is selected by default.
Scan Frequency	The number of times the asset was scanned within the past 90 days.
ServiceNow Sys ID	Where applicable, the unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.
Source	The source of the scan that identified the asset. Possible values are: • AWS • AWS FA • Azure • AZURE FA • Cloud Connector • Cloud IAC • Cloud Runtime • GCP • Nessus Agent • Nessus Scan • NNM • ServiceNow • WAS **Note**: This filter is selected by default.
SSL/TLS	Specifies whether the application on which the asset is hosted uses SSL/TLS public-key encryption.
System Type	The system types as reported by Plugin ID 54615. For more information,

	see Tenable Plugins.
Tags	Asset tags, entered in pairs of `category` and `value` (for example Network: Headquarters). This includes the space after the colon (:). If there is a comma in the tag name, insert a backslash (\) before the comma. If your tag name includes double quotation marks (" "), use the UUID instead. You can add a maximum of 100 tags. For more information, see Tags. **Note**: This filter is selected by default.
Target Groups	The target group to which the asset belongs. This attribute is empty if the asset does not belong to a target group. For more information, see Target Groups.
Tenable ID	The UUID of the asset in Tenable Vulnerability Management.
Terminated	Specifies whether or not the asset is terminated.
Type	The system type on which the asset is managed. Possible options are: • **Cloud Resource** • **Container** • **Host** • **Cloud** **Note**: This filter is selected by default.

Host Assets

The following table describes the Host asset filters:

Filter	Description
ACR	(Requires Tenable Lumin license) The asset's ACR.
ACR Severity	(Requires Tenable Lumin license) (Requires Tenable One or Tenable

	Lumin license) The ACR category of the ACR calculated for the asset.
AES	(Requires Tenable Lumin license)The Asset Exposure Score (AES) calculated for the asset.
AES Severity	(Requires Tenable Lumin license) (Requires Tenable Lumin license) The AES category of the AES calculated for the asset.
Agent Name	The name of the Tenable Nessus agent that scanned and identified the asset.
Asset ID	The asset's unique identifier.
AWS Availability Zone	The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see Regions and Zones in the AWS documentation.
AWS EC2 AMI ID	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Instance ID	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Name	The name of the virtual machine instance in Amazon EC2.
AWS EC2 Product Code	The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2.
AWS Instance State	The state of the virtual machine instance in AWS at the time of the scan. For possible values, see InstanceState in the Amazon Elastic Compute Cloud Documentation.
AWS Instance Type	The type of virtual machine instance in Amazon EC2. Amazon EC2 instance types dictate the specifications of the instance (for example, how much RAM it has). For a list of possible values, see Amazon EC2 Instance Types in the AWS documentation.
AWS Owner ID	A UUID for the Amazon AWS account that created the virtual machine instance. This attribute only appears for Amazon EC2 instances. For

	more information, see View AWS Account Identifiers in the AWS documentation
AWS Region	The region where AWS hosts the virtual machine instance, for example, `us-east-1`.
AWS Security Group	The AWS security group (SG) associated with the Amazon EC2 instance.
AWS Subnet ID	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.
AWS VPC ID	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud Documentation.
Azure Location	The location of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure Resource Group	The name of the resource group in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure Resource ID	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager documentation.
Azure Resource Type	The resource type of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure Subscription ID	The unique subscription identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure VM ID	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see the Azure Resource Manager documentation.
BIOS ID	The NetBIOS name for the asset.
Cloud Provider	The cloud provider for the asset – AWS, Azure, or GCP.

	Note: Filter with the **Cloud Provider** instead of **Source** to search for resources with imported tags.
Created Date	The date and time when Tenable Vulnerability Management created the asset record.
Custom Attribute	A filter that searches for custom attributes via a category-value pair. For more information about custom attributes, see the Tenable Developer Portal.
DNS	The fully-qualified domain name of the host that the vulnerability was detected on.
Domain	The domain to which the asset belongs.
First Seen	The date and time when a scan first identified the asset.
Google Cloud Instance	The unique identifier of the virtual machine instance in Google Cloud Platform (GCP).
Google Cloud Project ID	The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see Creating and Managing Projects in the GCP documentation.
Google Cloud Zone	The zone where the virtual machine instance runs in GCP. For more information, see Regions and Zones in the GCP documentation.
Has Plugin Results	Specifies whether the asset has plugin results associated with it.
Installed Software	A list of Common Platform Enumeration (CPE) values that represent applications identified on an asset from a scan. This field supports the CPE 2.2 format. For more information, see the Component Syntax section of the CPE Specification documentation. For assets identified in Tenable scans, this field only contains data when a scan using Tenable Nessus Plugin 45590 has evaluated the asset.
IPv4 Address	The IPv4 address associated with the asset record.

	This filter supports multiple asset identifiers as a comma-separated list (for example, hostname_example, example.com, 192.168.0.0). For IP addresses, you can specify individual addresses, CIDR notation (for example, 192.168.0.0/24), or a range (for example, 192.168.0.1-192.168.0.255). **Note:** Tenable Vulnerability Management does not support a CIDR mask of /0 for this parameter, because that value would match all IP addresses. If you submit a /0 value for this parameter, Tenable Vulnerability Management returns a 400 Bad Request error message. **Note:** Ensure the filter value does not end in a period.
IPv6 Address	An IPv6 address that a scan has associated with the asset record. This filter supports multiple asset identifiers as a comma-separated list. The IPV6 address must be an exact match. (for example, 0:0:0:0:0:ffff:c0a8:0). **Note:** Ensure the filter value does not end in a period.
Last Authenticated Scan	The date and time of the last credentialed scan run on the asset.
Last Licensed Scan	The date and time of the last scan that identified the asset as licensed. For more information about licensed assets, see Tenable Vulnerability Management Licenses.
Last Seen	The date and time at which the asset was last observed as part of a scan. **Note**: This filter is selected by default.
Licensed	Specifies whether the asset is included in the asset count for the Tenable Vulnerability Management instance. **Note**: This filter is selected by default.

MAC Address	A MAC address that a scan has associated with the asset record.
Mitigated	Specifies whether a scan has identified mitigation software on the asset.
Mitigation Last Detection	The date and time of the scan that last identified mitigation software on the asset.
Mitigation Product Name	The name of the mitigation software identified on the asset. Tenable Lumin defines mitigations as security agent software running on endpoint assets, which include antivirus software, Endpoint Protection Platforms (EPPs), or Endpoint Detection and Response (EDR) solutions.
Mitigation Vendor Name	The name of the vendor for the mitigation that a scan identified on the asset.
Mitigation Version	The version of the mitigation that a scan identified on the asset.
Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address. **Note**: This filter is selected by default.
NetBIOS Name	The NetBIOS name for the asset.
Network	The name of the network object associated with scanners that identified the asset. The default name is **Default**. For more information, see Networks.
Operating System	One of the operating system(s) that a scan identified on the asset.
Public	Specifies whether the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable Vulnerability Management `query` namespace.
Resource Tags (By Key	The key in the key-value pair of the tags or labels imported from the cloud provider.

Resource Tags (By Value	The value in the key-value pair of the tags or labels imported from the cloud provider.
Scan Frequency	The number of times the asset was scanned within the past 90 days.
ServiceNow Sys ID	Where applicable, the unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.
Source	The source of the scan that identified the asset. Possible values are: • AWS • AWS FA • Azure • Azure FA • Cloud Discovery Connector **Note:** Tenable Vulnerability Management shows this source for compute assets with imported resource tags. • For existing assets, the **Source** column shows **Cloud Discovery Connector** along with the existing source (AWS, Azure, or GCP). • For new assets, the **Source** column shows **Cloud Discovery Connector**. See the **Cloud Provider** column to view from where the asset is imported from. **Caution**: If you currently have queries utilizing AWS, GCP, or Azure as sources, you must update these queries. The **Cloud Discovery Connector** source now replaces AWS, GCP, and Azure sources. Additionally, for the source of assets, use the **Cloud Provider** parameter to indicate AWS, Azure, or GCP. • Cloud IaC • Cloud Runtime

	• GCP • Nessus Agent • Nessus Scan • NNM • ServiceNow • WAS **Note**: This filter is selected by default.
System Type	The system types as reported by Plugin ID 54615. For more information, see Tenable Plugins.
Tags	Asset tags, entered in pairs of `category` and `value` (for example Network: Headquarters). This includes the space after the colon (:). If there is a comma in the tag name, insert a backslash (\) before the comma. If your tag name includes double quotation marks (" "), use the UUID instead. You can add a maximum of 100 tags. For more information, see Tags. **Note**: This filter is selected by default.
Target Groups	The target group to which the asset belongs. This attribute is empty if the asset does not belong to a target group. For more information, see Target Groups.
Tenable ID	The UUID of the agent present on the asset.
Terminated	Specifies whether or not the asset is terminated.
Updated Date	The time and date when the asset record was last updated.

Cloud Resources Assets

The following table describes the cloud resources asset filters:

Option	Description
Account ID	The account ID associated with the asset.
ARN	The Amazon Resource Name (ARN) for the asset.
Asset ID	The asset's unique identifier.
Cloud Provider	The name of the cloud provider that hosts the asset.
Created Date	The time and date when Tenable Vulnerability Management created the asset record.
First Seen	The date and time when a scan first identified the asset.
IaC Resource Type	The Infrastructure as Code (IAC) resource type of the asset.
Is Attribute	Specifies whether the asset is an attribute.
Is Auto Scale	Specifies whether the asset scales automatically.
Is Unsupported	Specifies whether the asset is unsupported in Tenable Vulnerability Management.
Last Audited	The time and date when Tenable Vulnerability Management last audited the asset.
Last Licensed Scan	The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses.
Last Seen	The date and time at which the asset was last observed as part of a scan.
Licensed	Specifies whether the asset is included in the asset count for the Tenable Vulnerability Management instance.

Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address. **Note**: This filter is selected by default.
Region	The cloud region where the asset runs.
Repositories	Any code repositories associated with the asset.
Resource Category	The category of the asset resource in the cloud service that hosts the asset.
Resource Tags (By Key)	Tags synced from a cloud source such as Amazon Web Services (AWS), matched by the tag key (for example, Name). Separate individual search items with commas and use wildcards (*) to locate keys that equal, begin with, end with, or contain part of a string. Alternately, search for Assets with or without tags.
Resource Tags (By Value)	Tags synced from a cloud source such as Amazon Web Services (AWS), matched by the tag value. Separate individual search items with commas and use wildcards (*) to locate values that equal, begin with, end with, or contain part of a string. Alternately, search for Assets with or without tags.
Resource Type	The asset's cloud resource type (for example, network, virtual machine). **Note**: This filter is selected by default.
Source	The source of the scan that identified the asset. Possible values are: • **Cloud IaC** • **Cloud Runtime** **Note**: This filter is selected by default.
Tags	Asset tags, entered in pairs of `category` and `value` (for example Network: Headquarters). This includes the space after the colon (*:*). If there is a comma in the tag name, insert a backslash (\) before the comma. If your

	tag name includes double quotation marks (" "), use the UUID instead. You can add a maximum of 100 tags. For more information, see Tags. **Note**: This filter is selected by default.

Web Applications Assets

The following table describes the web application asset filters:

Filter	Description
ACR	(Requires Tenable Lumin license) The asset's ACR.
ACR (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset-Criticality Rating* using a new algorithm based on asset profile, which assigns assets to classes by business and device function. This metric rates the importance of an asset to your organization from 1 to 10, with higher numbers for more critical assets. For more information, see Scoring and Asset Criticality Rating.
ACR Severity	(Requires Tenable Lumin license) (Requires Tenable One or Tenable Lumin license) The ACR category of the ACR calculated for the asset.
AES	(Requires Tenable Lumin license) (Requires Tenable Lumin license) The AES category of the AES calculated for the asset.
AES (Beta)	(Requires Tenable One or Tenable Lumin license) The Tenable-defined *Asset Exposure Score* using a new algorithm. This metric weighs an asset's Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) and then assigns a number from 1 to 1000, with higher numbers for more exposed assets. For more information, see Scoring (Beta).
AES Severity	(Requires Tenable Lumin license) (Requires Tenable Lumin license) The AES category of the AES calculated for the asset.
Asset ID	The asset's unique identifier.
Created Date	The date and time when Tenable Vulnerability Management created the

	asset record.
Custom Attribute	A filter that searches for custom attributes via a category-value pair. For more information about custom attributes, see the Tenable Developer Portal.
First Seen	The date and time when a scan first identified the asset.
Last Authenticated Scan	The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field.
Last Licensed Scan	The time and date of the last scan that identified the asset as licensed. For more information about licensed assets, see License Information.
Last Seen	The date and time at which the asset was last observed as part of a scan. **Note**: This filter is selected by default.
Licensed	Specifies whether the asset is included in the asset count for the Tenable Web App Scanning instance. An asset is licensed if it meets the following criteria: • The scan results for the asset do not include discovery plugin results. • The scan results for the asset do not include Tenable Web App Scanning sources (e.g., results from Tenable Nessus scanners, Agents, Tenable Network Monitor). • The asset has not been terminated.
Mitigated	Specifies whether a scan has identified mitigation software on the asset.
Mitigation Last Detected	The date and time of the scan that last identified mitigation software on the asset.
Mitigation Product Name	The name of the mitigation software identified on the asset. Tenable Lumin defines mitigations as security agent software running on endpoint

	assets, which include antivirus software, Endpoint Protection Platforms (EPPs), or Endpoint Detection and Response (EDR) solutions.
Mitigation Version	The version of the mitigation software that a scan identified on the asset.
Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address. **Note**: This filter is selected by default.
Operating System (WAS)	One of the operating system(s) that a scan identified on the asset.
Public	Specifies whether the asset is available on a public network. **Note**: A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable Vulnerability Management `query` namespace.
Source	The source of the scan that identified the asset. Possible values are: • **ASM** • **AWS** • **AWS FA** • **Azure** • **Azure FA** • **Cloud IAC** **Note**: This filter is selected by default.
SSL/TLS	Specifies whether the application on which the asset is hosted uses SSL/TLS public-key encryption.
Tags	Asset tags, entered in pairs of `category` and `value` (for example

	Network: Headquarters). This includes the space after the colon (:). If there is a comma in the tag name, insert a backslash (\) before the comma. If your tag name includes double quotation marks (" "), use the UUID instead. You can add a maximum of 100 tags. For more information, see Tags. **Note**: This filter is selected by default.
Updated Date	The time and date when the asset record was last updated.

Domain Inventory Assets

The following table describes the domain inventory asset filters:

Filter	Description
ASN	The Autonomous System Number (ASN) for the asset.
Asset ID	The asset's unique identifier.
Created Date	The date and time when Tenable Vulnerability Management created the asset record.
DNS (FQDN)	The fully-qualified domain name of the host that the vulnerability was detected on.
Domain	The domain name for the asset.
Host Name	The hostname of the asset. This string is determined by information reported by target plugins, and is dependent on the user's environment and configuration.
Hosting Provider	The hosting provider for the asset.
IPv4 Address	The IPv4 address associated with the asset record. This filter supports multiple asset identifiers as a comma-separated list (for example, hostname_example, example.com, 192.168.0.0). For IP addresses, you can specify individual addresses, CIDR notation (for example,

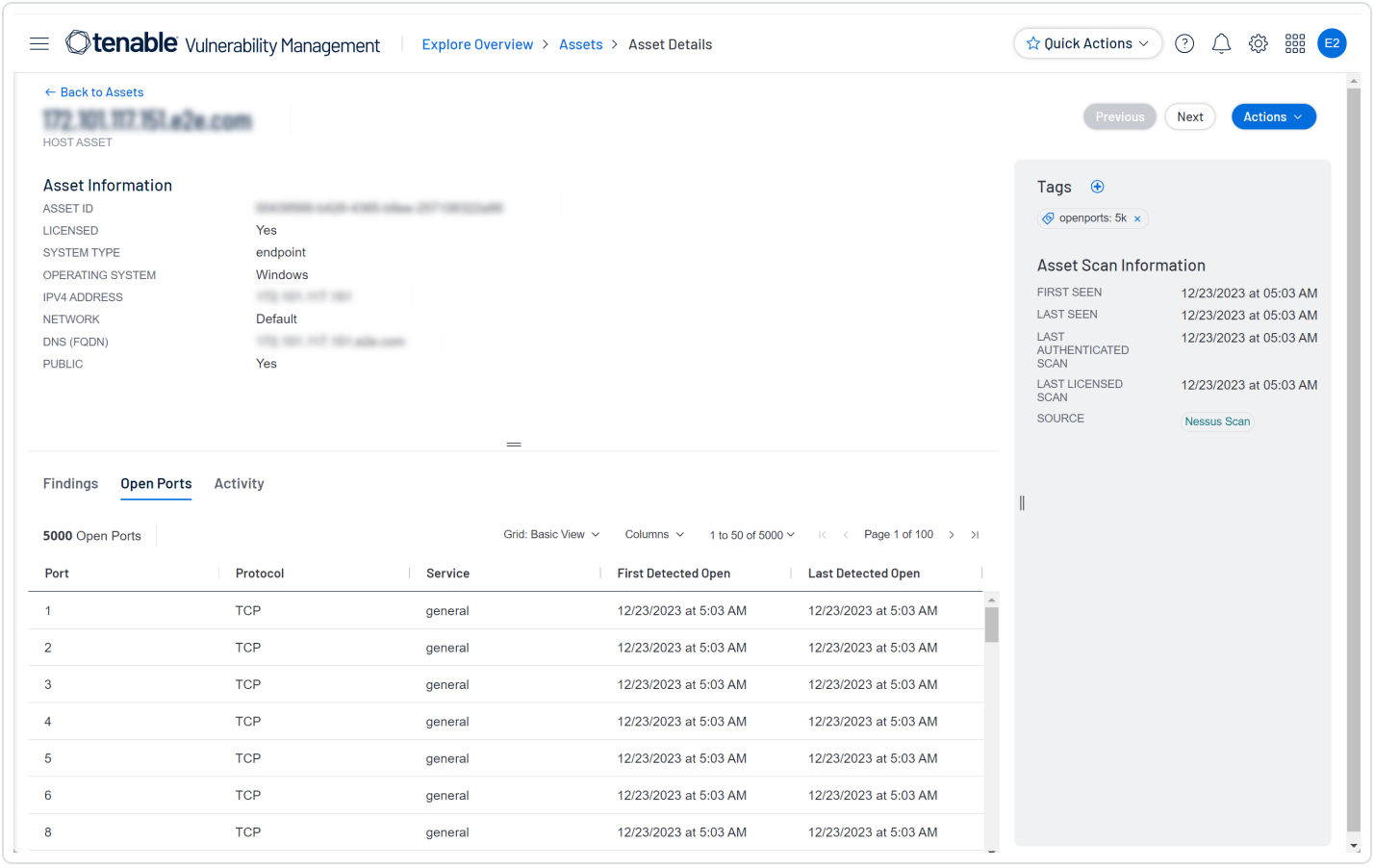
	192.168.0.0/24), or a range (for example, 192.168.0.1-192.168.0.255). **Note:** Tenable Vulnerability Management does not support a CIDR mask of /0 for this parameter, because that value would match all IP addresses. If you submit a /0 value for this parameter, Tenable Vulnerability Management returns a 400 Bad Request error message. **Note:** Ensure the filter value does not end in a period.
IPv6 Address	An IPv6 address that a scan has associated with the asset record. This filter supports multiple asset identifiers as a comma-separated list. The IPV6 address must be an exact match. (for example, 0:0:0:0:0:ffff:c0a8:0). **Note:** Ensure the filter value does not end in a period.
Last Seen	The date and time at which the asset was last observed as part of a scan.
Licensed	Specifies whether the asset is included in the asset count for the Tenable Vulnerability Management instance.
Name	The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address. **Note**: This filter is selected by default.
Port	A port associated with the asset, open or closed. Only applies to Domain Inventory assets.
Record Type	The type of asset.
Source	The source of the scan that identified the asset. Possible values are: • **ASM** • **AWS** • **AWS FA**

	• Azure • Azure FA • Cloud IAC **Note**: This filter is selected by default.
Tags	Asset tags, entered in pairs of `category` and `value` (for example Network: Headquarters). This includes the space after the colon (:). If there is a comma in the tag name, insert a backslash (\) before the comma. If your tag name includes double quotation marks (" "), use the UUID instead. You can add a maximum of 100 tags. For more information, see Tags.
Updated Date	The time and date when the asset record was last updated.

Open Ports and the Assets workbench

Tip: For more information about open ports and the Tenable Vulnerability Management API, see the API changelog in the *Tenable Developer Portal*. For more information, contact Tenable Customer Support.

Tenable Vulnerability Management displays open port findings on the **Asset Details** page, which appears when you click a host asset on the **Assets** workbench and then click **See All Details**. On the **Asset Details** page, the **Open Ports** tab shows open ports on an asset and includes the port protocol, when the port was first and last detected open, and the service running on the port.



Working with Ports

Use the following features to search for, manage, and export your port data:

- **Ports** – On the **Assets** workbench, search for ports on your host assets (or your domain inventory if you have imported data from Tenable Attack Surface Management).
- **Port tag rule** – On the **Assets** workbench, add tags to your ports.
- **Port export field** – With a custom field, export port data from the **Assets** workbench.

Supported Plugins

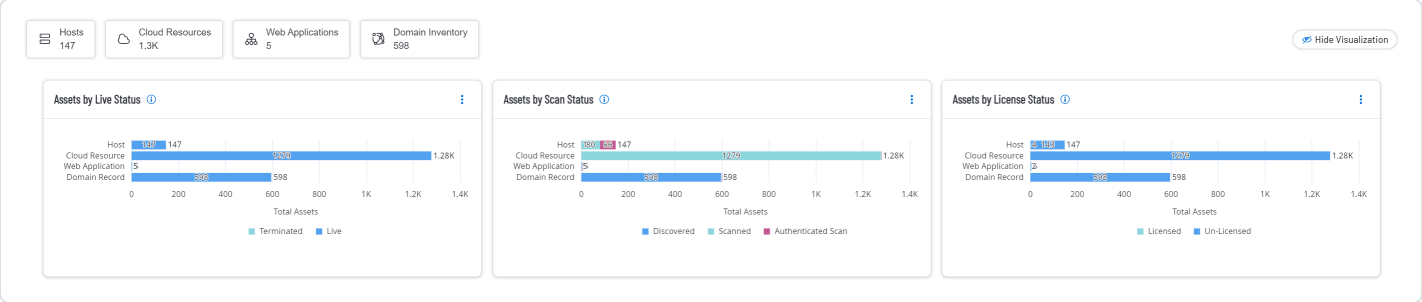
The **Open Ports** tab shows output from the following high-traffic plugins:

- 34220 - Netstat Portscanner (WMI)
- 34252 - Microsoft Windows Remote Listeners Enumeration (WMI)
- 11219 - Nessus SYN Scanner

- 14272 - Netstat Portscanner (SSH)
- 25221 - Remote listeners enumeration (Linux / AIX)
- 99265 - macOS Remote Listeners Enumeration
- 10335 - Nessus TCP scanner
- 14274 - Nessus SNMP Scanner
- 34277 - Nessus UDP Scanner

Asset Widgets

On the **Assets** workbench, interactive widgets break down the assets in your environment and update based on the filters you apply. To toggle these widgets, click **Show Visualization** or **Hide Visualization**.



Widget Types

The **Assets** workbench shows three widgets.

Widget	Description
Assets by Live Status	Groups assets by type and shows if they are or **Live** or **Terminated**. This metric is particularly relevant for cloud assets.
Assets by Scan Status	Groups assets by type and shows if they are **Discovered** but not scanned, **Scanned** without authentication, or have received an **Authenticated Scan**.
Assets by License Status	Groups assets by type and shows if they are **Licensed** or **Un-Licensed**. For more information on licensed assets, see Tenable Vulnerability Management Licenses.

Edit the ACR for Host Assets

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

In the **Explore** section of Tenable Vulnerability Management, you can manually override the Asset Criticality Rating (ACR) of Host assets to better reflect the unique infrastructure or needs of your organization.

To edit an Explore asset's ACR:

1. In the left navigation, click **Assets**.

   The **Assets** workbench appears.

2. Select the check boxes next to the host assets whose ACR you want to edit.

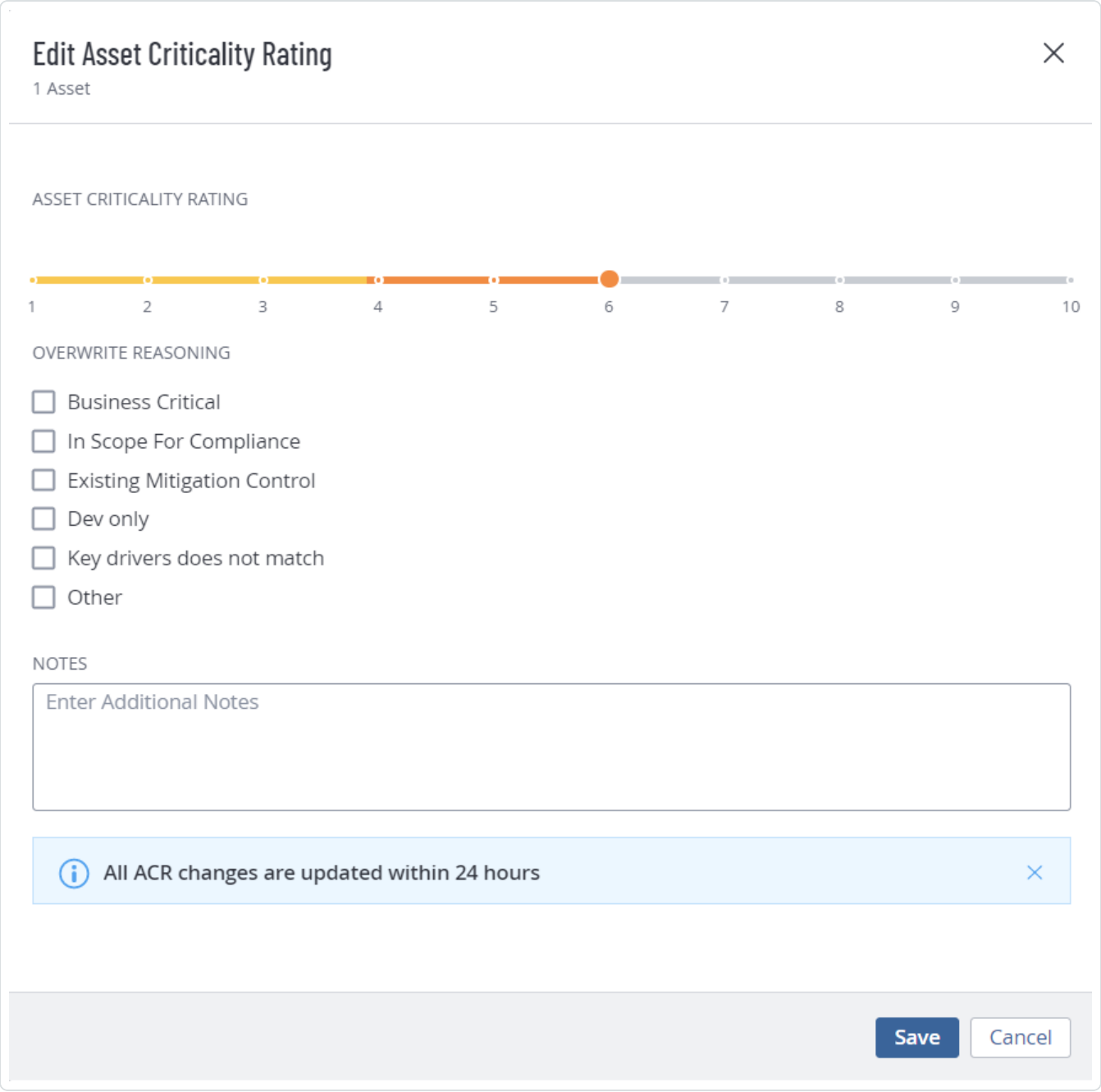
   The action bar appears.

3. In the action bar, click ⋮.

   A menu appears.

4. Click **Edit ACR**.

   The **Edit Asset Criticality Rating** window appears.



5. On the **Asset Criticality Rating** slider, click the number of the score to which you want to change the ACR.
6. In the **Overwrite Reasoning** section, select the check box next to the reason that best matches why you want to edit the ACR.
7. (Optional) In the **Notes** section, type any additional notes you want to add.
8. Click **Save**.

The system can take up to 24 hours to apply the new ACR. When this happens, **Processing** appears on the **Assets** workbench.

Move Assets to Another Network

> **Required Tenable Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

Tenable Vulnerability Management automatically assigns scanned assets to a network based on the scanner's network ID. However, you may need to manually move assets to another network. For example, you might have multiple assets with the same IP address which belong on different subnets so they can be identified as separate entities.

You can move assets to another network from the **Assets** workbench. If you first need to create the network to move assets to, see Create a Network.

> **Tip:** You can also move assets to a network via the **Settings** section.

When you move assets, be sure to move the scanner as well as the asset. Otherwise, the scanner will create the same asset again. For more information, see Add a Scanner to a Network.

> **Note:** Move assets before you run scans on a new network. If you move assets to a network where scans have already run, Tenable Vulnerability Management may create duplicate records that count against your license.

> **Tip**: On the **Assets** workbench, you can move host assets, cloud resources, or web applications to another network. You cannot move domain inventory assets.

To move assets to another network:

1. In the left navigation, click **Assets**.

   The **Assets** workbench appears.

2. Select the check boxes for the assets you want to move.

   The action bar appears.

3. In the action bar, click **Move**.

A dialog appears.

4. In the dialog, under **Choose a New Destination Network**, select the network to move the assets to.
5. Click **Move**.

   The system moves the assets to the destination network. If you moved a large number of assets, the move may take a few hours to complete.

Remove and Prevent Duplicate Assets

In Tenable Vulnerability Management, assets get assigned a unique ID when scanned with credentialed or agent scans. Tenable Vulnerability Management checks this unique ID each time a scan runs, so that it can update the existing asset record with new findings, resolved findings, or resurfaced findings. When you then run an uncredentialed scan against the same asset, there could be scenarios wherein the scanner cannot log in to the asset and retrieve the unique ID. This causes Tenable Vulnerability Management to view the asset as new, and therefore create a new record (in this case a duplicate of an asset).

Remove Duplicate Assets

To remove duplicate assets in Tenable Vulnerability Management:

1. Within the **Explore** section, view your asset list.
2. Delete any duplicate assets.

   Once an asset is deleted, Tenable Vulnerability Management immediately returns the license to your available license count.

Prevent Duplicate Assets

As a best practice, Tenable recommends scanning assets with a combination of uncredentialed, credentialed, and agent scans to ensure full vulnerability coverage. To resolve duplicate assets when running an agent scan and a non-credentialed Nessus scan, Tenable recommends using the **Open Agent Port** feature included in Tenable Agent versions 10.6.0 and later. To view more configuration information for this feature, see Configure Agent Profiles to Avoid Asset Duplication in Tenable Vulnerability Management in the Tenable Agent User Guide.

Note: The **Open Agent Port** feature does not merge existing duplicates. It only resolves asset duplication issues between agent scans and non-credentialed Nessus scans once you configure the setting.

While there are different use cases for each scan type, generally, Tenable recommends prioritizing the types of scans you run in the following order:

1. Credentialed Scans from a Tenable Nessus Scanner
2. Tenable Agent Scans
3. Uncredentialed Scans
4. Tenable Network Monitor

For more information, see Create a Tenable Vulnerability Management Scan.

Download Inventory Data

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Vulnerability Management Permission: Can Edit, Can Use permission for applicable asset tags

Required Access Group Permissions: Can View

When you open a support ticket related to a Tenable Vulnerability Management asset, you can download the asset's *inventory data* in ZIP format and attach it to the ticket. This data is only intended for support cases.

Note: You can only download inventory data for assets scanned in the past 90 days which either have **SSM** or **AZURE_FA** source types, or are **NESSUS_AGENT** scans with enabled inventory collection plugins.

To download asset inventory data:

1. In the left navigation, click **Assets**.

   The **Assets** workbench appears.

2. In the **Actions** column for the asset to download, click ⋮.

A menu appears.

3. In the menu, click **Download Inventory Debug Data**.

   The debug data downloads in ZIP format.

Delete Assets

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

On the **Assets** workbench, you can delete host assets, web application assets, or domain inventory assets. When you delete an asset, the system removes it from the **Assets** workbench, deletes all associated findings, and stops matching scan results to the asset. Within 24 hours, the asset is no longer included in your license count.

Caution: Deleting assets quickly removes decommissioned hosts or other irrelevant assets from your license count and reports, but it is permanent! Be careful with this feature.

Note: On a network with **Asset Age Out** enabled, assets expire on a schedule and do not need to be deleted. For more information, see View or Edit a Network and Create a Network.

Note: If you see deleted assets when using the **Asset ID** filter, these are temporary. Deleted assets do not count against your license and have no associated findings. Deleted assets are labeled as **Deleted**.

To delete assets from Tenable Vulnerability Management:

1. In the left navigation, click **Assets**.

   The **Assets** workbench appears.

2. On the **Assets** workbench, do one of the following:

   - **Delete a single asset with the ⋮ button**

     a. In the row for the asset to delete, click the ⋮ button.

        A menu appears.

     b. In the menu, click **Delete**.

c. In the confirmation window that appears, click **Delete** again.

> **Tip**: You can also delete single assets from the Asset Details page.

- **Delete multiple assets from the action bar**

a. Select the check boxes next to the assets to delete.

   The action bar appears.

> **Tip**: To delete all assets, click **Select all**. You can only delete 1,000 assets at a time.

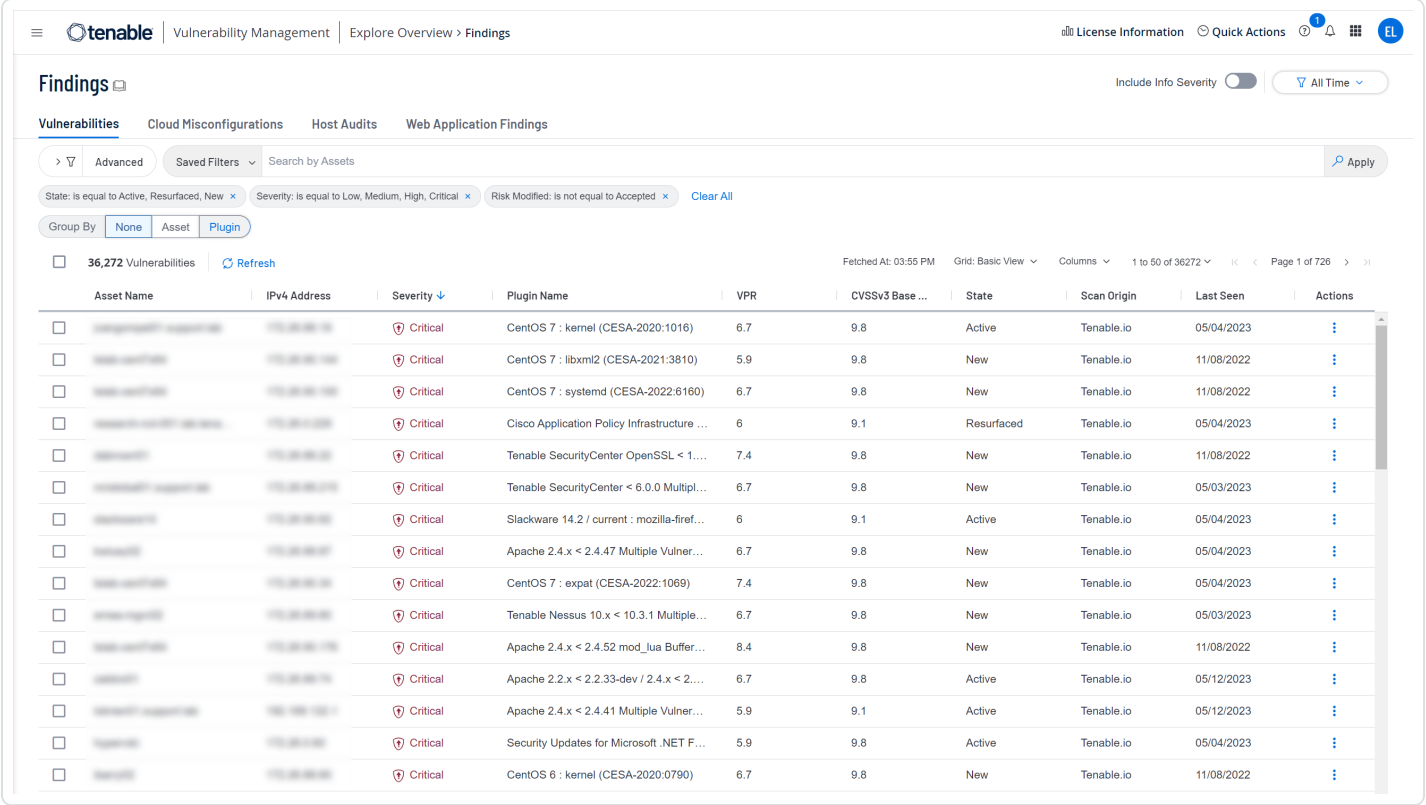
b. In the action bar, click **More**.

c. In the menu that appears, click **Delete**.

d. In the confirmation window that appears, click **Delete** again.

Findings

On the **Findings** workbench, you can get insight into your organization's findings. These include vulnerabilities, cloud misconfigurations, host audits, and web application findings.



Note: Tenable Vulnerability Management retains findings data for 15 months.

A finding is a single instance of a vulnerability appearing on an asset, uniquely identified by plugin ID, port, and protocol. By providing comprehensive information about your findings, Tenable Vulnerability Management helps to identify potential security risks, visibility on under-utilized resources, and support compliance efforts.

Tenable Vulnerability Management automatically creates or updates findings when a scan completes or scan results are imported.

See the following topics for more information.

- Use the Findings Workbench
- View Finding Details
- Findings Filters

Group Your Findings

Create Recast Rules from Findings

Generate a Findings Report

Use the Findings Workbench

You can view all your findings on the **Findings** workbench.

To view your findings:

1. In the left navigation, click **Findings**.

   The **Findings** workbench appears.

2. (Optional) To view a different finding type, click a tab:

   - Vulnerabilities
   - Cloud Misconfigurations
   - Host Audits
   - Web Application Findings

On the **Findings** workbench, you can do the following:

- In the search box, search for findings by asset name, IPv4 address or range, or Classless Inter-Domain Routing (CIDR) block. Or, use a wildcard (*)
- Filter the displayed findings and customize your view, as described in Explore Tables.

  Note: Tenable recommends that you use simple instead of complex queries or one level of nested filters when creating your findings filters. Nested filters can cause issues within your custom widgets, because custom widgets can only have a maximum of one level of nested filters. An example of a query with one level of nesting:
  `(CVSSv3 Base Score is greater than 8.9 OR VPR is greater than 8.9) AND State is not equal to Fixed`

- Save filters as a custom search, as described in Saved Filters.
- Group findings by asset, plugin, and more, as described in Group Your Findings.

- In the upper-right corner of the **Vulnerabilities** or **Web Application Findings** tabs, toggle **Include Info Severity**, as described in Vulnerability Severity Indicators.
- In the **Vulnerabilities** or **Web Application Findings** tabs, to view informational findings about artificial intelligence services on your assets, click **AI Inventory**. These findings cannot be grouped. To view their details, hover on the **AI/LLM Tools** column.
- Filter displayed findings by time period with a drop-down in the upper-right corner.
- Export findings to CSV or JSON format, as described in Export Findings or Assets.
- View details about a finding, as described in View Finding Details.

Vulnerabilities

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Findings** workbench, click the **Vulnerabilities** tab to view your asset vulnerabilities. Common vulnerabilities include system misconfigurations, unpatched software, poor data encryption, and weak authorization credentials.

The **Vulnerabilities** tab contains a table with the following columns. To show or hide columns, see Customize Explore Tables.

Column	Description
AI/LLM Tools	Indicates an informational finding about artificial intelligence services running on an asset. Hover on the **AI/LLM Tools** column to view details.
Asset ID	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Vulnerability Management.
Asset Name	The name of the asset. This value is unique to Tenable Vulnerability Management.
Asset Tags	Tags applied to the asset.
IPv4 Address	The IPv4 address for the affected asset.
IPv6 Address	The IPv6 address for the affected asset.

Last Fixed	The last time a previously detected vulnerability was scanned and noted as no longer present on an asset.
Last Scan Target	The IP address or fully qualified domain name (FQDN) of the asset targeted in the last scan.
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.
Plugin Name	The name of the plugin that identified the vulnerability detected in the finding.
Plugin ID	The ID of the plugin that identified the vulnerability.
Plugin Family	The family of the plugin that identified the vulnerability.
Port	The port that the scanner used to connect to the asset where the scan detected the vulnerability.
Protocol	The protocol the scanner used to communicate with the asset where the scan detected the vulnerability.
Resurfaced Date	The most recent date that a scan detected a Resurfaced vulnerability which was previously Fixed. If a vulnerability is Resurfaced multiple times, only the most recent date appears.
All IPv4 Addresses	All IPV4 addresses for the asset, separated by commas.
Time Taken to Fix	How long it took your organization to fix a vulnerability identified on a scan in days. Only appears for Fixed vulnerabilities. Use this filter along with the **State** filter set to **Fixed** for more accurate results. When exported, this field is shown in milliseconds.
VPR	A descriptive icon indicating the VPR of the vulnerability. For more information, see CVSS vs. VPR.
CVSSv2 Base Score	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). Tenable Vulnerability Management shows the **CVSSv2** or **CVSSv3** column depending on the **Vulnerability**

	Severity Metric setting.
State	The state of the vulnerability. For more information, see Vulnerability States.
CVSSv3 Base Score	The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). Tenable Vulnerability Management shows the **CVSSv2** or **CVSSv3** column depending on the **Vulnerability Severity Metric** setting.
Scan Origin	The scanner that detected the finding. Also identifies if the scan is a work-load scan. Possible values for this column are: Tenable Vulnerability Management, Tenable Security Center, and Agentless Assessment.
Region	The cloud region where the asset runs.
Account ID	The unique identifier assigned to the asset resource in the cloud service that hosts the asset.
Live Result	Indicates whether the scan result is based on live results. In Agentless Assessment, you can use live results to view scan results for new plugins based on the most recently collected snapshot data, without running a new scan. The possible values are **Yes** or **No**.
First Seen	The date when a scan first found the vulnerability on an asset.
Last Seen	The date when a scan last found the vulnerability on an asset.
Actions	In this column, click the ⋮ button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **Generate Report** – Generate a report from a template, as described in Reports.

	• **Recast** – Recast or accept finding severity, as described in Create Recast Rules from Findings. • **View All Findings** – View all findings for an asset, as described in View Asset Details. • **View All Details** – View complete details for a finding, as described in View Finding Details. • **Create Remediation Project** – Start a new remediation project for an asset, as described in Remediation Projects. • **Launch Remediation Scan** – Start a remediation scan to follow up on existing scan results, as described in Launch a Remediation Scan.

Cloud Misconfigurations

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Findings** workbench, click the **Cloud Misconfigurations** tab to view your cloud misconfigurations. Common cloud misconfigurations include unrestricted inbound and outbound ports, credential management and encryption, disabled monitoring and logging, insecure automated backups, and storage access.

The **Cloud Misconfigurations** tab contains a table with the following columns. To show or hide columns, see Customize Explore Tables.

Column	Description
Resource ID	A unique identifier made up of the resource type and the asset name.
Policy Name	The security policy that governs the affected asset.
Policy Group Name	The group associated with the security policy that governs the affected asset.
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.

Result	The outcome of the vulnerability scan.
Source	The environment where the affected asset runs.
First Seen	The date when a scan first found the vulnerability on an asset.
Last Seen	The date when a scan last found the vulnerability on an asset.
Asset ID	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Vulnerability Management.
Cloud Provider	The name of the cloud provider that hosts the asset.
IaC Resource Type	The Infrastructure as Code (IAC) resource type of the asset.
Resource Name	The name of the asset where the scanner detected the vulnerability. Tenable Vulnerability Management assigns this identifier based on the presence of certain asset attributes in the following order: 1. Agent Name (if agent-scanned) 2. NetBIOS Name 3. FQDN 4. IPv6 address 5. IPv4 address For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Resource Name.
Region	The cloud region where the asset runs.
VPC	The virtual private cloud on which the asset is hosted in AWS.
ARN	The unique Amazon Resource Name for the asset in AWS.
Resource Type	The types of assets affected, determined by plugin data.
Benchmark	The benchmark associated with the finding.
Account ID	The unique identifier assigned to the asset resource in the cloud service

	that hosts the asset.
Repositories	Any code repositories associated with the asset.
Resource Type	The types of assets affected, determined by plugin data.
Policy Category	The category associated with the security policy that governs the affected asset.
Last Scan Time	The date and time when Tenable Vulnerability Managementlast scanned the asset.
Updated Time	The date and time when a user last updated the asset.
Actions	In this column, click the ⋮ button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **Generate Report** – Generate a report from a template, as described in Reports. • **View All Findings** – View all findings for an asset, as described in View Asset Details.

Host Audits

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Findings** workbench, click the **Host Audits** tab to view your host audit findings. Host audits assess workstations, services, or network devices in order to evaluate the configuration, hardening, and security controls applied to a target. View specific host audit findings to identify issues to remediate.

The **Host Audits** tab contains a table with the following columns. To show or hide columns, see Customize Explore Tables.

Note: Because of inefficient host-specific details, the **Host Audits** tab does not include data from Cloud Infrastructure audits such as those found in the Audit Cloud Infrastructure scan template. To view this data, view the scan results for the audit.

Column	Description
Audit Name	The name of the compliance check the scanner performed on the affected asset.
Audit File	The name of the audit file the scanner used to perform the compliance check.
Description	A detailed description of the compliance check.
Result	The outcome of the compliance check.
Plugin Name	The name of the plugin that identified the compliance check finding.
Original Result	The outcome from the original compliance check.
Result Modified Version	Explanation for why the original compliance result was changed.
Result Modified Expires	When the change result rule expires.
Asset ID	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Vulnerability Management.
Asset Name	The name of the asset. This value is unique to Tenable Vulnerability Management.
Asset Tags	Tags applied to the asset.
Last Audited	The date and time when a scan last performed the compliance check on the asset.
Actions	In this column, click the ⋮ button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **View All Findings** – View all findings for an asset, as described in View Asset Details. • **View All Details** – View complete details for a finding, as described in View Finding Details.

Web Application Findings

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Findings** workbench, click the **Web Application Findings** tab to view your web application findings. Common web application findings include SQL injections, cross-site scripting, local file inclusions, security misconfigurations, and XML external entity processing.

The **Web Application Findings** tab contains a table with the following columns. To show or hide columns, see Customize Explore Tables.

Column	Description
Asset ID	The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management.
Asset Name	The name of the asset where the scanner detected the vulnerability. This value is unique to Tenable Vulnerability Management.
IPv4 Address	The IPv4 address associated with the asset record. This filter supports multiple asset identifiers as a comma-separated list (for example, hostname_example, example.com, 192.168.0.0). For IP addresses, you can specify individual addresses, CIDR notation (for example, 192.168.0.0/24), or a range (for example, 192.168.0.1-192.168.0.255). **Note:** Tenable Vulnerability Management does not support a CIDR mask of /0 for this parameter, because that value would match all IP addresses. If you submit a /0 value for this parameter, Tenable Vulnerability Management returns a 400 Bad Request error message.
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.
Plugin Name	The name of the plugin that identified the vulnerability.
Plugin ID	The ID of the plugin that identified the vulnerability.
Plugin	The family of the plugin that identified the vulnerability.

Family	
CVSSv2 Base Score	A numeric value between 0.0 and 10.0 that represents the intrinsic characteristics of a vulnerability independent of any specific environment. Tenable Vulnerability Management shows the **CVSSv2** or **CVSSv3** column depending on the **Vulnerability Severity Metric** setting.
CVSSv3 Base Score	The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). Tenable Vulnerability Management shows the **CVSSv2** or **CVSSv3** column depending on the **Vulnerability Severity Metric** setting.
State	The state of the vulnerability.
First Seen	The date when a scan first found the vulnerability on an asset.
Last Seen	The date when a scan last found the vulnerability on an asset.
Actions	In this column, click the ⋮ button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **Recast** – Recast or accept finding severity, as described in Create Recast Rules from Findings. • **View All Findings** – View all findings for an asset, as described in View Asset Details. • **View All Details** – View complete details for a finding, as described in View Finding Details.

View Finding Details

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Web App Scanning User Role: Scan Operator, Standard, Scan Manager, or Administrator

From the **Findings** workbench, you can drill down into a single asset to view it on the **Finding Details** page. Tenable Vulnerability Management customizes this page by finding type.

To view finding details:

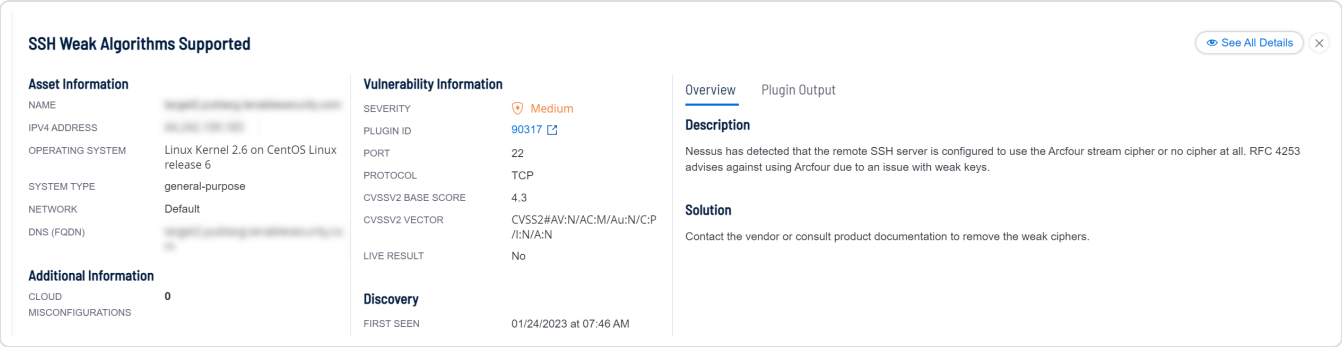
1. In the left navigation, click **Findings**.

   The **Findings** workbench appears.

2. (Optional) Click another tab to view a different finding type or use filters to refine your results.

3. Click the row for the finding to view.

   At the bottom of the page, a preview appears.



4. In the preview, click **See All Details**.

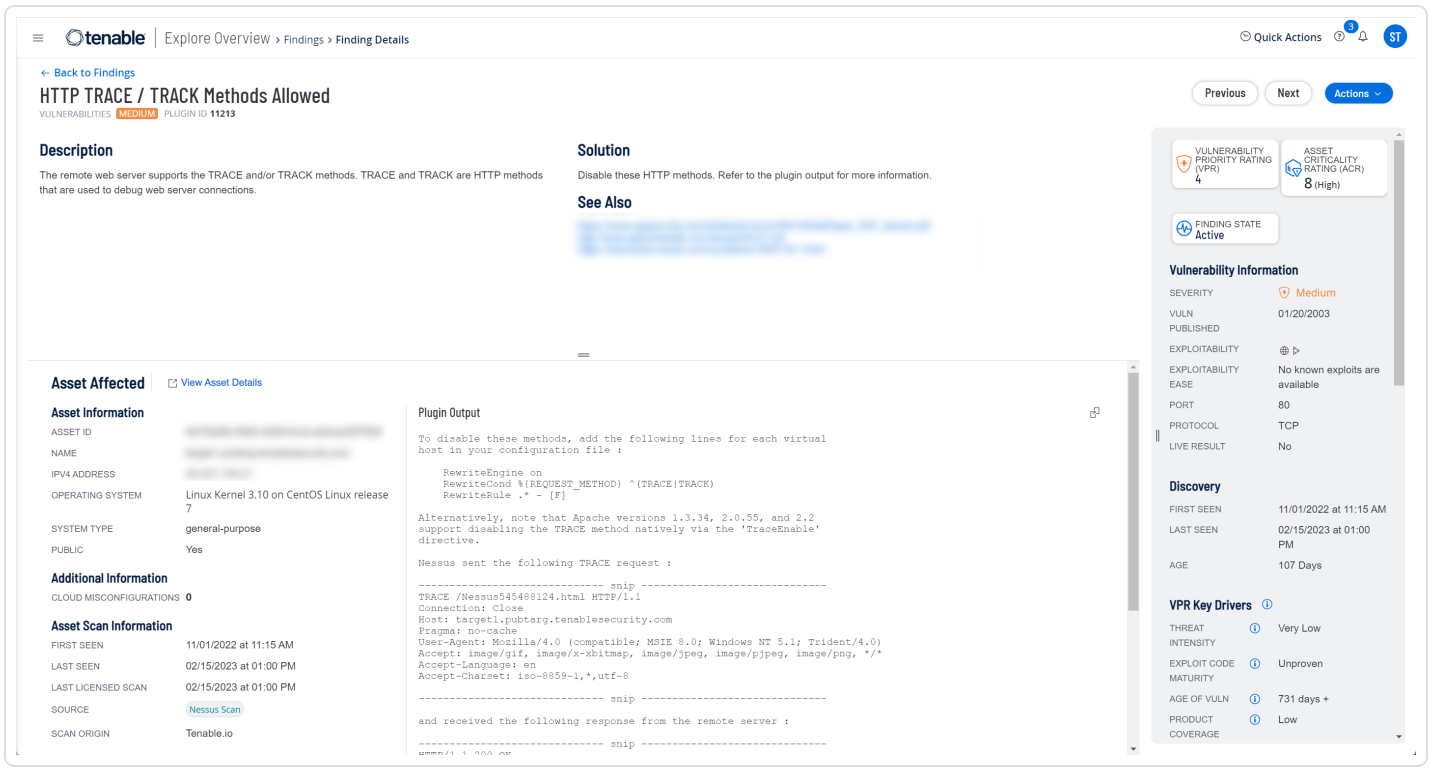
   The **Finding Details** page appears. Its layout varies by finding type:

   - Vulnerability Details
   - Cloud Misconfiguration Details
   - Host Audit Details
   - Web Application Findings Details

Vulnerability Details

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

When you View Finding Details, the **Finding Details** page varies by finding type. For vulnerability findings, it includes a description, the recommended solution, and the plugin output.



The **Finding Details** page for vulnerabilities contains the following sections.

> **Note**: Tenable Vulnerability Management hides empty sections, so these may not appear in some cases.

Section	Description
Description	A description of the Tenable plugin that identified the vulnerability detected in the finding.
Solution	A brief summary of how you can remediate the vulnerability detected in the finding. Only appears if an official solution is available.
Workaround	The type of workaround recommended for the vulnerability, if any. Possible values are **Configuration Change** or **Disable Service**. If there is a workaround, **Workaround Published** also appears.
AI Inventory	If a finding is AI-related, this section lists the AI/LLM-related tools found by Tenable's plugins.
See Also	Links to websites that contain helpful information about the vulnerability detected in the finding.

Asset Information	Information about the affected asset, including: • **Asset ID** – The UUID of the asset where a scan detected the vulnerability. • **Name** – The name of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management. • **All IPv4 Addresses** – All IPv4 addresses for the affected asset. • **IPV4 Address** – The IPv4 address for the affected asset. • **IPV6 Address** – The IPv6 address for the affected asset. • **Operating System** – The operating system that the scan identified as installed on the affected asset. • **System Type** – The type of operating system that the scan identified as installed on the affected asset. • **Network** – The name of the network object associated with scanners that identified the asset. The default name is **Default**. For more information, see Networks. • **Public** – Specifies whether the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable Vulnerability Management query namespace. • **Network Device Serial ID** – The unique identifier of the asset as assigned by the manufacturer. This property is only available for network devices.
Cloud Misconfigurations	The number of resources that failed to comply with the configured policies. Click this number to go to the **Cloud Misconfigurations** tile and view the affected resources.
Asset Scan Information	Information about the scan that detected the vulnerability, including: • **First Seen** – The date when a scan first found the vulnerability

	on an asset. • **Last Seen** – The date when a scan last found the vulnerability on an asset. • **Last Licensed Scan** – The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses. • **Last Authenticated Scan** – The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field. • **Source** – The source of the scan that detected the vulnerability on the affected asset. • **Scan Origin** – The scanner that detected the finding. It also helps identify whether the scan is a work-load scan. Possible values are: Tenable Vulnerability Management, Tenable Security Center, and Agentless Assessment. • **Last Scan Target** – The IP address or fully qualified domain name (FQDN) of the asset targeted in the last scan.
Additional Information	Additional information about the vulnerability findings, including: • **Network** –The name of the network object associated with scanners that identified the finding. The default network name is **Default**. For more information, see Networks. • **DNS (FQDN)** – The fully qualified domain name of the host on which the vulnerability identified in the finding was detected. • **MAC Address** – The static Media Access Control (MAC)

	address for the affected asset. • **Tenable ID** – The unique identifier for the Tenable account associated with the affected asset. • **Installed Software** – Software that a scan identified on the affected asset. • **SSH Fingerprint** – The SSH key fingerprints that scans have associated with the asset record.
Vulnerability Priority Rating (VPR)	(Requires Tenable Lumin license) A descriptive icon indicating the VPR of the vulnerability. For more information, see CVSS vs. VPR.
Asset Criticality Rating (ACR)	(Requires Tenable Lumin license) Rates the criticality of an asset to the organization from 1 to 10. A higher value means the asset is more crucial to the business. For more information, see Tenable Lumin Metrics.
Finding State	A descriptive icon indicating the state of the vulnerability. For more information, see Vulnerability States.
Vulnerability Information	Information about the vulnerability that the plugin identified, including: • **Severity** – The severity of the vulnerability on the finding. • **Original Severity** – The vulnerability's CVSS-based severity from when a scan first detected the finding. • **Vuln Published** – The oldest date on which the vulnerability was either documented in an advisory or published in the National Vulnerability Database (NVD). • **Exploitability** – Characteristics of the vulnerability that factor into its potential exploitability. • **Exploitability Ease** – A description of how easy it is to exploit the vulnerability. • **Exploited With** – The most common ways that the vulnerability may be exploited.

	• **Exploited by Malware** – Indicates whether the vulnerability is known to be exploited by malware. • **Exploited by Nessus** – Indicates whether Tenable Nessus exploited the vulnerability during the identification process. • **In the News** – Indicates whether this plugin has received media attention (for example, ShellShock, Meltdown). • **Last Fixed** – The last time a previously detected vulnerability was scanned and noted as no longer present on an asset. • **Malware** – Indicates whether the plugin that identified the vulnerability checks for malware. • **Resurfaced Date** – The most recent date that a scan detected a Resurfaced vulnerability which was previously Fixed. If a vulnerability is Resurfaced multiple times, only the most recent date appears. • **Time Taken to Fix** – How long it took your organization to fix a vulnerability identified on a scan in days. Only appears for Fixed vulnerabilities. Use this filter along with the **State** filter set to **Fixed** for more accurate results. When exported, this field is shown in milliseconds. • **Unsupported by Vendor** – Software found by this plugin is unsupported by the software's vendor (for example, Windows 95 or Firefox 3). • **Vulnerability Age** – The age of a vulnerability based on its State. For *Active* vulnerabilities, based on the time elapsed between First Seen and today's date. For *Fixed* vulnerabilities, based on the time elapsed between First Seen and Last Fixed or the time elapsed between Resurfaced and Last Fixed. For *Resurfaced* vulnerabilities, based on the time elapsed between Resurfaced and today's date. • **Patch Published** – Displays when a patch has been published

	for a vulnerability. • **Remediation Type** – The type of fix recommended. Possible values are **Patch**, **Workaround**, **Patch and Workaround**, and **No Fix**. • **Workaround Type** – Appears if the **Remediation Type** is **Workaround**. Possible values are **Configuration Change** or **Disable Service**. • **Port** – The port that the scanner used to connect to the asset where the scan detected the vulnerability. • **Protocol** – The protocol the scanner used to communicate with the asset where the scan detected the vulnerability. • **Live Result** – Indicates whether the scan result is based on live results. In Agentless Assessment, you can use live results to view scan results for new plugins based on the most recently collected snapshot data, without running a new scan. The possible values are **Yes** or **No**. • **CPE** – The Common Platform Enumeration (CPE) numbers for vulnerabilities that the plugin identifies. • **Asset Inventory** – This plugin is an Tenable Inventorynventory plugin. • **Default Account** – Any default credentials or accounts.
Discovery	Information about when Tenable Vulnerability Management first discovered the vulnerability, including: • **First Seen** – The date when a scan first found the vulnerability on an asset. • **Last Seen** – The date when a scan last found the vulnerability on an asset. • **Age** – The number of days since a scan first found the vulnerability on an asset in your network.

	• **Resurfaced Date** – The most recent date that a scan detected a Resurfaced vulnerability which was previously Fixed. If a vulnerability is Resurfaced multiple times, only the most recent date appears.
	• **Vulnerability Age** – The age of a vulnerability based on its current State:
	  • **New or Active** – The time elapsed between First Seen and today's date.
	  • **Fixed** – The time elapsed between First Seen and Last Fixed or between Resurfaced and Last Fixed.
	  • **Resurfaced** – The time elapsed between Resurfaced and today's date.

VPR Key Drivers	Information about the key drivers Tenable uses to calculate a VPR for the vulnerability, including: • **Threat Recency** – The number of days (0-730) since a threat event occurred for the vulnerability. • **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**. • **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 (for example, Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (**High**, **Functional**, **PoC**, or **Unproven**) parallel the CVSS Exploit Code Maturity categories. • **Age of Vuln** – The number of days since the National Vulnerability Database (NVD) published the vulnerability. • **Product Coverage** – The relative number of unique products affected by the vulnerability: **Low**, **Medium**, **High**, or **Very High**.

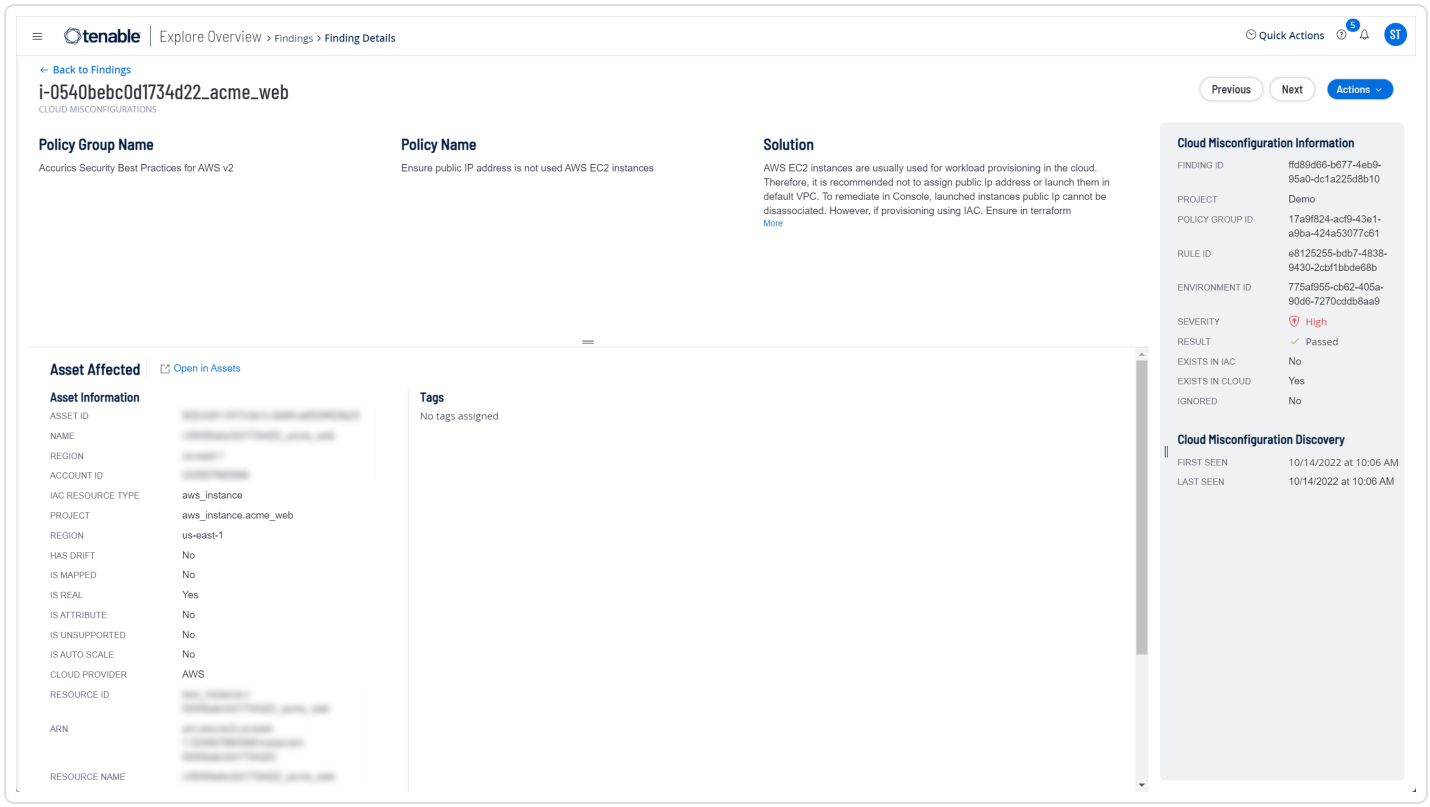
	• **CVSS3 Impact Score** – The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable Vulnerability Management shows a Tenable-predicted score. • **Threat Sources** – A list of all sources (for example, social media channels, the dark web, etc.) where threat events related to this vulnerability occurred. If the system did not observe a related threat event in the past 28 days, the system shows **No recorded events**.
Plugin Details	Information about the plugin that detected the vulnerability, including: • **Publication Date** – The date on which the plugin that identified the vulnerability was published. • **Modification Date** – The date on which the plugin was last modified. • **Family** – The family of the plugin that identified the vulnerability. • **Type** – The general type of plugin check (for example, `local` or `remote`). • **Version** – The version of the plugin that identified the vulnerability. • **Plugin ID** – The ID of the plugin that identified the vulnerability.
Risk Information	Information about the relative risk that the vulnerability presents to the affected asset, including: • **Risk Factor** – The CVSS-based risk factor associated with the plugin. • **CVSSV3 Base Score** – Intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments. • **CVSSV3 Temporal Score** – Characteristics of a vulnerability that change over time.

	• **CVSSV3 Vector** – More CVSSv3 metrics for the vulnerability. • **CVSSV2 Base Score** – Intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments. • **CVSSV2 Temporal Score** – A score that denotes characteristics of a vulnerability that change over time, but not among user environments. • **CVSSV2 Vector** – More CVSSv2 metrics for the vulnerability. • **STIG Severity** – A vulnerability's severity rating based on the Department of Defense's Security Technical Implementation Guide (STIG).
Reference Information	Industry resources that provide additional information about the vulnerability.
Actions	In the upper-right corner, click the **Actions** button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **Generate Report** – Generate a report from a template, as described in Reports. • **Recast** – Recast or accept finding severity, as described in Create Recast Rules from Findings. • **View All Findings** – View all findings for an asset, as described in View Asset Details. • **View All Details** – View complete details for a finding, as described in View Finding Details. • **View All Details in New Tab** – View complete details for an asset in a new browser tab. • **Create Remediation Project** – Start a new remediation project

	for an asset, as described in Remediation Projects. • **Launch Remediation Scan** – Start a remediation scan to follow up on existing scan results, as described in Launch a Remediation Scan.

Cloud Misconfiguration Details

When you View Finding Details, the **Finding Details** page varies by finding type. For cloud misconfiguration findings, it includes policy information, a recommended solution, and details on the affected asset.



The **Finding Details** page for cloud misconfigurations contains the following sections.

Note: Tenable Vulnerability Management hides empty sections, so these may not appear in some cases.

Section	Description
Policy Group Name	The name of the cloud policy group associated with the affected finding.

Policy Name	The name of the cloud policy associated with the affected finding.
Solution	A brief summary of how you can remediate the vulnerability. This section appears only if an official solution is available.
Asset Information	Information about the affected asset, including: • **Asset ID** – The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management. • **Name** – The name of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management. • **Project** – The cloud project associated with the findings and affected asset. • **Region** – The cloud region on which the asset resides. • **VPC** The unique identifier of the public cloud that hosts the AWS virtual machine instance. Stands for "virtual private cloud." • **Account ID** – The unique identifier assigned to the asset on which a scan detected the finding. • **Resource Name** – The asset identifier. • **Types** – The types of assets affected, determined by plugin data. • **IaC Resource Type** – The Infrastructure as Code (IAC) resource type of the asset. • **Resource Type** – The types of resources affected, determined by plugin data. • **Has Drift** – Indicates whether the asset has any drifts. • **Is Mapped** – Indicates whether the asset is mapped.

	• **Is Real** – Indicates whether the affected asset exists in a cloud environment.
	• **Cloud Provider** – The name of the cloud provider that hosts the resource.
	• **Resource ID** – The resource ID of the resource.
	• **Resource Name** – The name of the asset where the scanner detected the vulnerability. Tenable Vulnerability Management assigns this identifier based on the presence of certain asset attributes in the following order:
	  • Agent Name (if agent-scanned)
	  • NetBIOS Name
	  • FQDN
	  • IPv6 address
	  • IPv4 address
	  for example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Resource Name.
	• **ARN** – The unique Amazon resource name for the asset in AWS.
	• **Resource Criticality** – The criticality rating for the asset according to Container Security, based on the most recent scan.

Additional Information	The number of vulnerabilities the policy detected during the scan.
Asset Scan Information	Information about the scan that detected the vulnerability, including: • **First Seen** – The date when a scan first found the vulnerability on an asset. • **Last Seen** – The date when a scan last found the vulnerability on an asset.

	• **Last Licensed Scan** – The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses. • **Last Authenticated Scan** – The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field. • **Source** – The source of the scan that detected the vulnerability on the affected asset.
Tags	Tags assigned to the affected asset.
Cloud Misconfiguration Information	Information about the vulnerability finding, including: • **Finding ID** – The unique ID for the individual finding. You can view the ID for a finding by accessing the **Findings Details** page for the finding and checking the page URL. The finding ID is the alphanumeric text that appears in the path between *details* and *asset*. • **Project** – The cloud project associated with the findings and affected asset. • **Policy Group ID** – The type of policy group ID associated with the finding. • **Policy ID** – The unique ID for the cloud policy associated with the affected asset. • **Rule ID** – The rule ID associated with the finding.

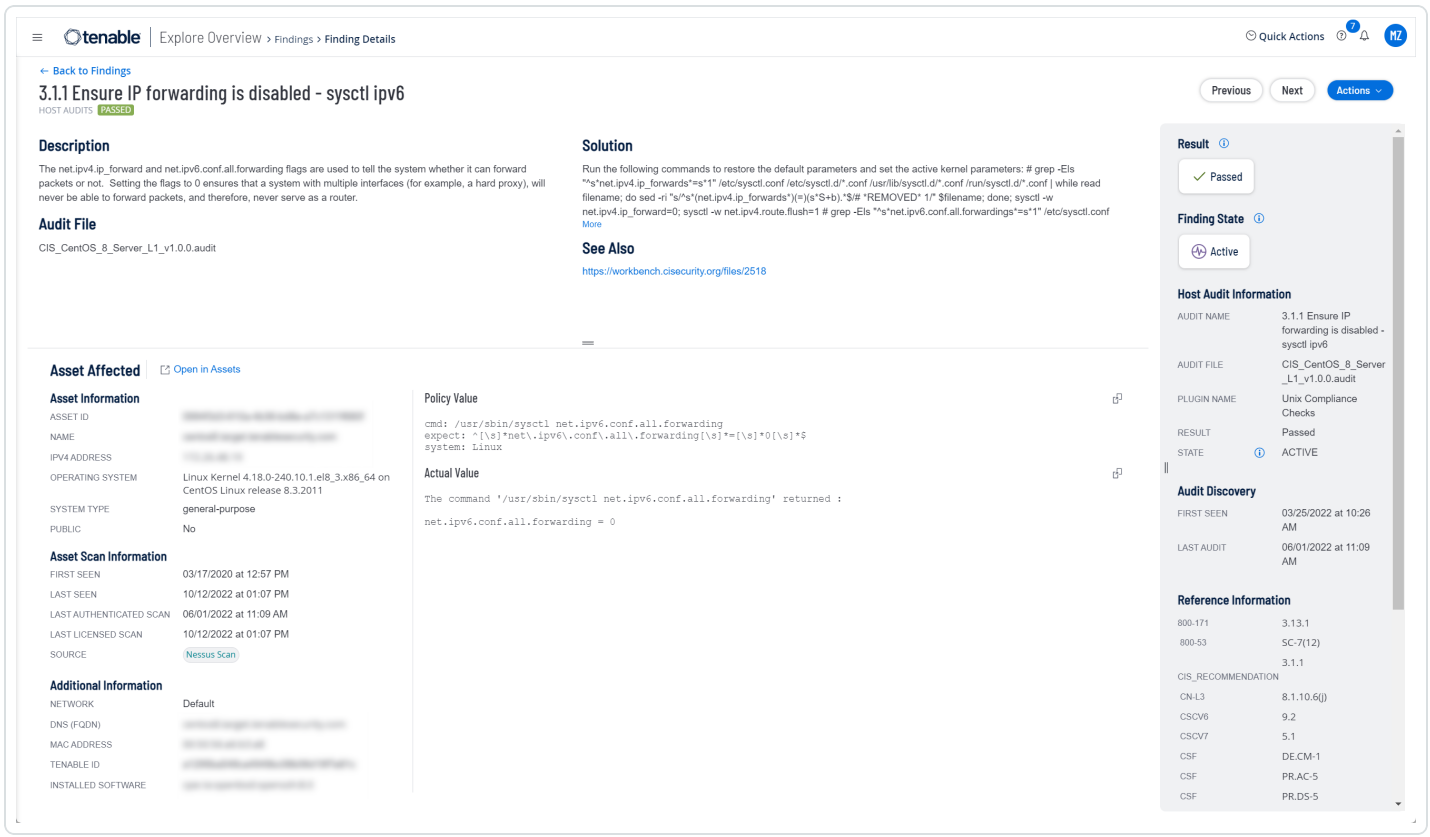
	• **Environment ID** – The environment ID associated with the finding. • **Severity** – A descriptive icon that indicates the CVSS-based severity of the vulnerability. For more information, see CVSS vs. VPR. • **Result** – The result of the finding. • **Benchmark** – The benchmark associated with the finding. • **Policy Category** – The policy category associated with the finding. • **IaC Type** – The Infrastructure as Code (IAC) resource type of the asset. • **Managed By** – The name of the person, group, or company that manages the affected asset. • **Policy Type** – The type of cloud policy associated with the finding. • **Rule Reference ID** – The reference ID for the security rule for which the scanner found a violation. • **Version** – The version associated with the finding. • **Exists in IAC** – Indicates whether the affected asset was created via Infrastructure as Code (IaC). • **Exists in Cloud** – Indicates whether the affected asset exists in a cloud environment. • **Ignored** – Indicates whether Legacy Tenable Cloud Security ignored the policy violation when determining the finding severity.
Cloud Misconfiguration Discovery	Information about when Tenable Vulnerability Management first discovered the vulnerability, including: • **First Seen** – The date when Tenable Vulnerability

	Management first scanned the affected asset. • **Last Seen** – The date when Tenable Vulnerability Management last scanned the affected asset.
Actions	In the upper-right corner, click the **Actions** button to view a drop-down where you can: • **Generate Report** – Generate a report from a template, as described in Reports. • **View All Findings** – View all findings for an asset, as described in View Asset Details.

Host Audit Details

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

When you View Finding Details, the **Finding Details** page varies by finding type. For host audit findings, it includes a description of the host audit finding, its recommended solution, and a summary of the corresponding asset.



The **Finding Details** page for host assets contains the following sections.

Note: Tenable Vulnerability Management hides empty sections, so these may not appear in some cases.

Section	Description
Description	A brief description of the plugin that identified the finding during a compliance check.
Solution	A brief summary of how you can address the compliance check findings.
Audit File	The name of the audit file the scanner used to perform the compliance check.
See Also	Links to external websites that contain helpful information about the compliance check.
Asset Information	Information about the affected asset, including: • **Asset ID** – The UUID of the asset where a scan detected the vulnerability.

	• **Name** – The name of the asset on which the scanner performed a compliance check. • **Operating System** – The operating system that the scan identified as installed on the affected asset. • **IPV4 Address** – The IPv4 address for the affected asset. • **System Type** – The type of system on which the affected asset runs. • **Public** – Specifies whether the asset is available on a public network. A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable Vulnerability Management query namespace.
Asset Scan Information	Information about the scan that detected the vulnerability, including: • **First Seen** – The date when a scan first found the vulnerability on an asset. • **Last Seen** – The date when a scan last found the vulnerability on an asset. • **Last Authenticated Scan** – The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field. • **Last Licensed Scan** – The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses. • **Source** – The source of the scan that detected the vulnerability on the affected asset.
Additional	Additional information about the affected asset, including:

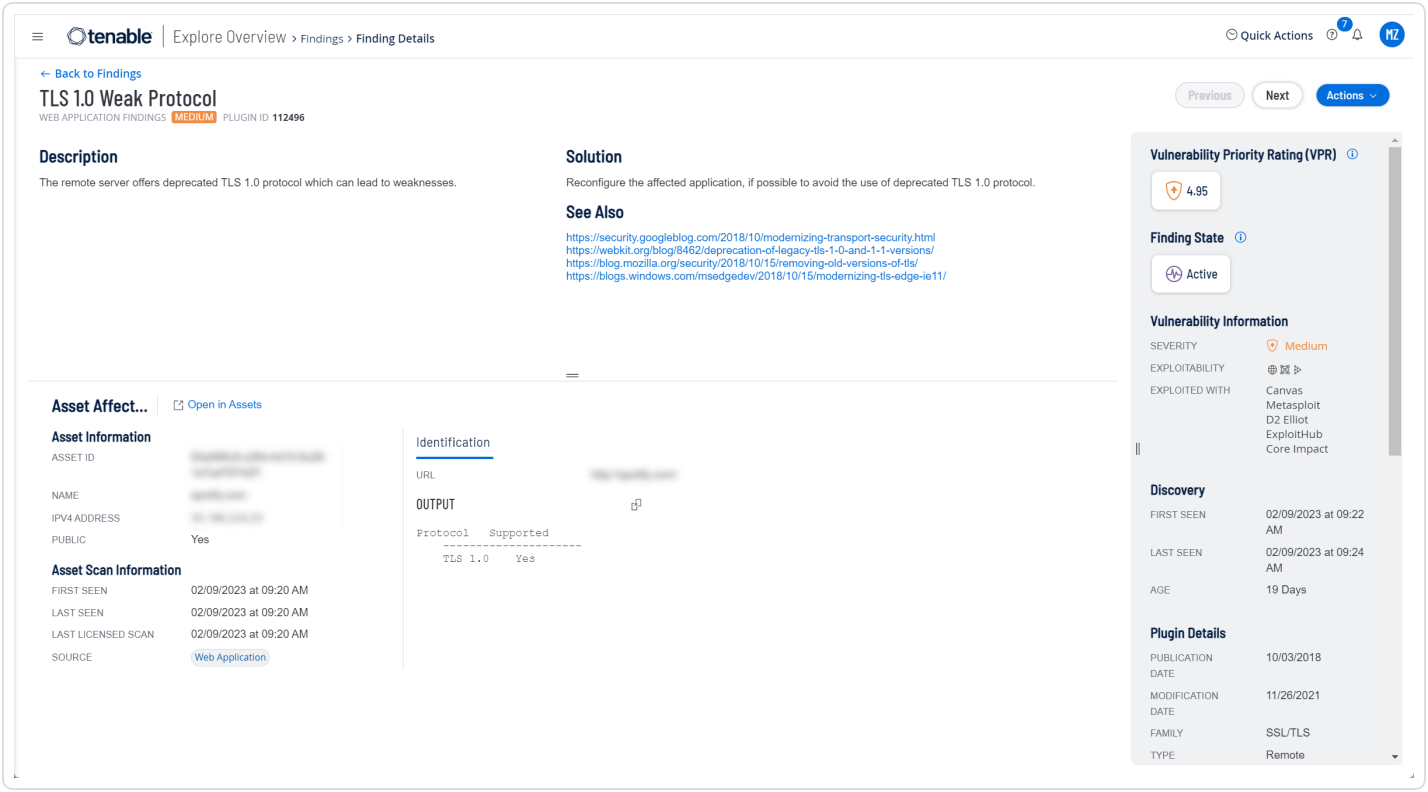
Information	• **Network** – The name of the network object associated with scanners that detected the finding. The default network name is **Default**. For more information, see Networks. • **Network (FQDN)** – The fully qualified domain name of the host on which the vulnerability identified in the finding was detected. • **MAC Address** – The static Media Access Control (MAC) address for the affected asset. • **Tenable ID** –The unique identifier for the Tenable account associated with the affected asset. • **Installed Software** – Software that a scan identified on the affected asset.
Policy Value	The plugin output that appears in the finding if the affected asset is compliant with the audit policy.
Actual Value	The plugin output that actually appears in the finding.
Host Audit Information	Information about the compliance check, including: • **Audit Name** – The name of the compliance check the scanner performed on the affected asset. • **Audit File** – The name of the audit file the scanner used to perform the compliance check. • **Benchmark** – Specific technical configurations recommended by an authoritative organization or vendor to securely harden an operating system, application, or network device. • **Benchmark Specification Name** – The unique, official title of the specific guideline or framework outlining the security configuration requirements. • **Benchmark Version** – The specific iteration or release number of the Benchmark Specification Name, indicating the precise set of requirements used for the compliance check.

	• **Plugin Name** – The name of the plugin that identified the compliance check. • **Source** – The name of the compliance check the scanner performed on the affected asset.
Audit Discovery	• **First Audit** – The date and time when a scan first performed the compliance check on the asset. • **Last Audit** – The date and time when a scan last performed the compliance check on the asset.
Reference Information	A list of industry resources that provide additional information about the compliance check.
Actions	In the upper-right corner, click the **Actions** button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **Generate Report** – Generate a report from a template, as described in Reports. • **View All Findings** – View all findings for an asset, as described in View Asset Details. • **View All Details** – View complete details for a finding, as described in View Finding Details. • **View All Details in New Tab** – View complete details for an asset in a new browser tab.

Web Application Findings Details

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

When you View Finding Details, the **Finding Details** page varies by finding type. For web application findings, it includes a description, the recommended solution, and details about the affected asset.



The **Finding Details** page for web application findings contains the following sections.

Note: Tenable Vulnerability Management hides empty sections, so these may not appear in some cases.

Section	Description
Description	A description of the Tenable plugin that identified the vulnerability detected in the finding.
Solution	A brief summary of how you can remediate the vulnerability detected in the finding. This section appears only if an official solution is available.
AI Inventory	If a finding is AI-related, this section lists the AI/LLM-related tools found by Tenable's plugins.
See Also	Links to external websites that contain helpful information about the vulnerability detected in the finding.
Asset Information	Information about the affected asset, including: • **Asset ID** – The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability

	Management. • **Name** – The name of the affected asset. You can click the link in the name to view details about the affected asset on the Web Application Details page. • **IPV4 Address** – The IPv4 address for your asset. • **Public** – Indicates whether or not the asset is public.
Asset Scan Information	Information about the scan that detected the vulnerability, including: • **First Seen** – The date and time when a scan first identified the asset. • **Last Seen** – The date and time at which the asset was last observed as part of a scan. • **Last Licensed Scan** – The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses. • **Last Authenticated Scan** – The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field. • **Source** – The source of the scan that detected the vulnerability on the affected asset.
Identification	Information about how the plugin identified the vulnerability detected in the finding, including: • **URL** – The target URL where the scanner detected the vulnerability. • **Proof** – Output from the scanner's attempt to verify the vulnerability that proves the vulnerability is exploitable on the affected asset.

	• **Input Type** – The component of the asset where an attacker could inject malicious code (for example, a form or session cookie). This section appears only if the asset is vulnerable to injection attacks. • **Input Name** – The name of the asset component where an attacker could inject malicious code. This section appears only if the asset is vulnerable to injection attacks. • **Output** – More detailed information from the plugin about the vulnerability detected during the scan.
Http Info	Information about the HTTP messages between the scanner and the web application, including: • **HTTP Request** – The HTTP request of the scanner that identified the vulnerability made to the web application. • **HTTP Response** – The HTTP response that the web application sent to the scanner that identified the vulnerability.
Attachments	Plugin attachments that include more details about the vulnerability detected in the finding. This section appears only if attachments are available.
Vulnerability Priority Rating (VPR)	The Vulnerability Priority Rating Tenable calculated for the vulnerability.
Finding State	The state of the vulnerability detected in the finding. For more information, see Vulnerability States.
Vulnerability Information	Information about the vulnerability that the plugin identified, including: • **Severity** – An icon that indicates the severity of the vulnerability. • **Exploitability** – Characteristics of the vulnerability that factor into its potential exploitability. • **Exploited With** – The most common ways that the vulnerability may be exploited.

Discovery	Information about when Tenable Vulnerability Management first discovered the vulnerability detected in the finding, including: • **First Seen** – The date when a scan first found the vulnerability on an asset. • **Last Seen** – The date when a scan last found the vulnerability on an asset. • **Age** – The number of days since a scan first found the vulnerability on an asset in your network.
Plugin Details	Information about the plugin that detected the vulnerability detected in the finding, including: • **Publication Date** – The date on which the plugin that identified the vulnerability was published. • **Modification Date** – The date on which the plugin was last modified. • **Family** – The family of the plugin that identified the vulnerability. • **Risk Factor** –The CVSS-based risk factor associated with the plugin. • **Plugin ID** – The ID of the plugin that identified the vulnerability.
Risk Information	Information about the relative risk that the vulnerability presents to the affected asset, including: • **Risk Factor** – The CVSS-based risk factor associated with the plugin. • **CVSSV3 Base Score** – The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). • **CVSSV3 Vector** – More CVSSv3 metrics for the vulnerability. • **CVSSV2 Base Score** – The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).

	• **CVSS2 Vector** – More CVSSv2 metrics for the vulnerability.
Reference Information	Industry resources that provide additional information about the vulnerability that Tenable Vulnerability Management detected in the finding, including but not limited to: • **OWASP** – A link or links to each Open Web Application Security Project (OWASP) Top 10 list on which the vulnerability appears. • **OWASP API** – A link or links to each OWASP API Top 10 list on which the vulnerability appears. • **WASC** – A link to the Web Application Security Consortium (WASC) description for the vulnerability's threat classification. • **CWE** – A link to the Common Weakness Enumeration (CWE) description for the vulnerability's CWE score.
Actions	In the upper-right corner, click the **Actions** button to view a drop-down where you can: • **Export** – Export to CSV or JSON, as described in Export from Explore Tables. • **Generate Report** – Generate a report from a template, as described in Reports. • **Recast** – Recast or accept finding severity, as described in Create Recast Rules from Findings. • **Recast** – Recast or accept finding severity, as described in Create Recast Rules from Findings. • **View All Findings** – View all findings for an asset, as described in View Asset Details. • **View All Details** – View complete details for a finding, as described in View Finding Details. • **View All Details in New Tab** – View complete details for an asset in a new browser tab.

Findings Filters

On the **Findings** page, you can filter and view analytics for the following findings types:

- Vulnerabilities
- Cloud Findings
- Host Audits Findings
- Web Application Vulnerabilities

You can save a set of commonly used filters as a saved filter to access later or share with other members of your team.

Note: To optimize performance, Tenable limits the number of filters that you can apply to any **Explore** > **Findings** or **Assets** views (including **Group By** tables) to 18.

Note: When Tenable Vulnerability Management identifies the same finding on multiple scans, it only stores the most recent result. For example, if an Agent scan identifies a finding and then a later Tenable Nessus scan identifies the same finding, that finding is associated with the Tenable Nessus scan. If you can't locate a known finding with a filter such as **Source**, search for the finding directly.

Vulnerabilities Filters

Option	Description
Asset ID	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Vulnerability Management.
Asset Name	The name of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management. This filter is case-sensitive, but you can use the wildcard character to turn this off.
Asset Tags	Asset tags, entered in pairs of `category` and `value` (for example Network: Headquarters). This includes the space after the colon (:). If there is a comma in the tag name, insert a backslash (\) before the comma. If your tag name includes double quotation marks (" "), use the UUID instead. You can add a maximum of 100

	tags. For more information, see Tags.
Bugtraq ID	The Bugtraq ID for the plugin that identified the vulnerability.
Canvas Exploit	The name of the CANVAS exploit pack that includes the vulnerability.
CERT Advisory ID	The ID of the CERT advisory related to the vulnerability.
CERT Vulnerability ID	The ID of the vulnerability in the CERT Vulnerability Notes Database.
CISA KEV Due Date	The date on which Cybersecurity and Infrastructure Security Agency (CISA) Known Exploitable Vulnerability (KEV) remediation is due, as per Binding Operational Directive 22-01. Searches by the earliest due date for KEVs associated with the plugin. For more information, see the Known Exploited Vulnerabilities Catalog.
Common Name	A vulnerability's common name, for example *Log4Shell*. Not all vulnerabilities have a common name.
CORE Exploit Framework	Indicates whether an exploit for the vulnerability exists in the CORE Impact framework.
CPE	The Common Platform Enumeration (CPE) numbers for vulnerabilities that the plugin identifies. (200 value limit)
CVE	The Common Vulnerability and Exposure (CVE) IDs for the vulnerabilities identified by the plugin and corresponding to a specific finding. (200 value limit)
CVE Category	The category of a vulnerability, as described in Vulnerability Categories.
CVE ID	The Common Vulnerabilities and Exposures (CVE) ID, for

	example *CVE-2002-2024*.
CVSSv2 Base Score	A numeric value between 0.0 and 10.0 that represents the intrinsic characteristics of a vulnerability independent of any specific environment.
CVSSv2 Temporal Score	The CVSSv2 temporal score (characteristics of a vulnerability that change over time but not among user environments).
CVSSv2 Temporal Vector	CVSSv2 temporal metrics for the vulnerability.
CVSSv2 Vector	The raw CVSSv2 metrics for the vulnerability. For more information, see the CVSSv2 documentation on the FIRST website.
CVSSv3 Attack Complexity	The attack complexity, which defines how difficult it is to use a vulnerability in an attack. Options are **High** or **Low**.
CVSSv3 Attack Vector	The attack vector, which defines an attack's location. Options are **Adjacent**, **Network**, **Local**, or **Physical**.
CVSSv3 Availability	Quantifies the impact on the availability of the affected asset. Options are **High** (the asset is completely unavailable), **Low** (some reduced performance or interruption in availability), or **None** (no impact on the availability of the asset).
CVSSv3 Base Score	The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
CVSSv3 Confidentiality	The expected impact of the affected asset's information confidentiality loss. Options are **High**, **Low**, or **None**. For example, an affected asset with **High** confidentiality may have a catastrophic adverse effect on your organization or customers.
CVSSv3 Integrity	The expected impact of the affected asset's data integrity loss. Options are **High**, **Low**, or **None**.

CVSSv3 Privileges Required	The permission level attackers require to exploit the vulnerability. Options are **High**, **Low**, or **None**. For example, **None** means attackers need no permissions in your environment and can exploit the vulnerability while unauthorized.
CVSSv3 Scope	If a vulnerability allows attackers to compromise resources beyond an affected asset's normal authorization privileges. Options are **Unchanged** or **Changed**. For example, **Changed** means the vulnerability increases the affected asset's privileges.
CVSSv3 Temporal Score	The CVSSv3 temporal score (characteristics of a vulnerability that change over time but not among user environments).
CVSSv3 Temporal Vector	CVSSv3 temporal metrics for the vulnerability.
CVSSv3 User Interaction	If a vulnerability requires other users (such as end users) for attackers to be able to use it. Options are **Required** or **None**. **None** is more severe since it means no additional user interaction is required.
CVSSv3 Vector	More CVSSv3 metrics for the vulnerability.
CVSSv4 Attack Complexity (AC)	The conditions beyond the attacker's control that must exist to exploit the vulnerability.
CVSSv4 Attack Requirements (AT)	The resources, access, or specialized conditions required for an attacker to exploit the vulnerability.
CVSSv4 Attack Vector (AV)	The context where vulnerability exploitation is possible, such as **Network** or **Local**.
CVSSv4 Base Score	A numeric value between 0.0 and 10.0 that represents the intrinsic characteristics of a vulnerability independent of any specific environment.
CVSSv4 Privileges Required (PR)	The level of privileges an attacker must possess to exploit the vulnerability.

CVSSv4 Subsequent System Availability Impact (VA)	The impact on the availability of systems that can be impacted after the vulnerable system is exploited.
CVSSv4 Subsequent System Confidentiality Impact (SC)	The impact on the confidentiality of systems that can be impacted after the vulnerable system is exploited.
CVSSv4 Subsequent System Integrity Impact (SI)	The impact on the integrity of systems that can be impacted after the vulnerable system is exploited.
CVSSv4 User Interaction	The level of user involvement required for an attacker to exploit the vulnerability.
CVSSv4 Vulnerable System Availability Impact	The impact on the availability of the vulnerable system when successfully exploited.
CVSSv4 Vulnerable System Confidentiality Impact (VC)	The impact on the confidentiality of the vulnerable system when successfully exploited.
CVSSv4 Vulnerable System Integrity Impact (VI)	The impact on the integrity of the vulnerable system when successfully exploited.
First Discovered	The date the vulnerability corresponding to a finding was first identified.
First Functional Exploit	The date a vulnerability was first known to be exploited.
First Proof of Concept	The date a vulnerability's first proof of concept was found.
First Seen	The date when a scan first found the vulnerability on an asset.
IAVA ID	The ID of the information assurance vulnerability alert (IAVA) for the vulnerability.
IAVB ID	The ID of the information assurance vulnerability bulletin (IAVB)

	for the vulnerability.
IAVM Severity	The severity of the vulnerability in Information Assurance Vulnerability Management (IAVM).
IAVT ID	The ID of the information assurance vulnerability technical bulletin (IAVT) for the vulnerability.
In The News	Indicates whether this plugin has received media attention (for example, ShellShock, Meltdown).
IPv4 Address	The IPv4 address for the affected asset. You can add up to 256 IP addresses to this filter.
IPv6 Address	The IPv6 address for the affected asset.
Last Fixed	The last time a previously detected vulnerability was scanned and noted as no longer present on an asset.
Last Seen	The date when a scan last found the vulnerability on an asset.
Malware	Indicates whether the plugin that identified the vulnerability checks for malware.
Metasploit Exploit	The name of the related exploit in the Metasploit framework.
Microsoft Bulletin	The Microsoft security bulletin that the plugin, which identified the vulnerability, covers.
Original Severity	The vulnerability's CVSS-based severity when a scan first detected the finding. For more information, see CVSS vs. VPR.
OSVDB ID	The ID of the vulnerability in the Open Sourced Vulnerability Database (OSVDB).
Patch Published	The date on which the vendor published a patch for the vulnerability.
Plugin Description	The description of the Tenable plugin that identified the vulnerability.

Plugin Family	The family of the plugin that identified the vulnerability. (200 value limit)
Plugin ID	The ID of the plugin that identified the vulnerability. (200 value limit)
Plugin Modification Date	The date at which the plugin that identified the vulnerability was last modified.
Plugin Name	The name of the plugin that identified the vulnerability.
Plugin Output	Use this filter to return findings with plugin output that you specify. Search for a value in the plugin output using the **contains** or **does not contain** operator, as described in Use Filters. **Caution**: Due to technical constraints in how the underlying system processes large data in JSON format, only the first 20,000,000 characters of raw plugin data are available when searching plugin output. If your search is too broad, the system suggests adding **Plugin ID** and **Last Seen** to refine the results and then displays the top ten plugins from that search. For example, to search for output that contains “Kernel,” in Advanced mode, type: `Plugin Output contains Kernel` **Note**: Manually enable this filter in **Settings** > **General Search** > **Enable Plugin Output Search**. If you do not use this filter for 35 days, it is disabled again. ### Plugin Output search best practices... Since plugin outputs can be large, broad searches may cause system timeouts! For the best results, combine the **Plugin Output** filter with the **Plugin ID** and **Last Seen** filters. Limit the number of

	plugin IDs you search at once.
	
	Specify plugin ID(s) to search for plugins or exclude them. These approaches apply to different use cases. For example, include plugins when searching for software listings by operating system. Exclude plugins from exploratory searches where the top plugins appear too frequently.
	
	• **Search for output from one plugin:**
	
	`Plugin Output contains Kernel AND Plugin ID is equal to 110483`
	
	• **Search for output from multiple plugins:**
	
	`Plugin Output contains Chrome AND Plugin ID is equal to 45590, 10456`
	
	• **Search for output from any plugin but the ones listed:**
	
	`Plugin Output contains Chrome AND Plugin ID is not equal to 45590, 10456`

Plugin Published	The date on which the plugin that identified the vulnerability was published.
Plugin Type	The general type of plugin check. Possible options are: • **Local** • **Remote** • **Local & Remote**
Plugins Available	If a vulnerability currently has a Tenable plugin that detects it. Options are **Yes** or **No**.
Port	Information about the port the scanner used to connect to the asset where the scan detected the vulnerability. (200 value limit)

Protocol	The protocol the scanner used to communicate with the asset where the scan detected the vulnerability.
Resurfaced Date	The most recent date that a scan detected a Resurfaced vulnerability which was previously Fixed. If a vulnerability is Resurfaced multiple times, only the most recent date appears.
Risk Modified	The risk modification applied to the vulnerability's severity. Possible options are: • **Recasted** • **Accepted** • **None** For more information, see Recast/Accept Rules.
Scan Origin	The scanner that detected the finding.
Secunia ID	The ID of the Secunia research advisory related to the vulnerability.
See Also	Links to external websites that contain helpful information about the vulnerability.
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR. This filter appears in the filters plane by default, with **Critical**, **High**, **Medium**, and **Low** selected.
Solution	A brief summary of how you can remediate the vulnerability.
Source	The source of the scan that identified the asset. Possible values include **Agent** for Tenable Agent, **Nessus** for Tenable Nessus, **PVS/NNM** for Tenable Network Monitor, and **WAS** for Tenable Web App Scanning.
State	The state of the vulnerability detected in the finding. Options are Fixed, Resurfaced, Active, New. Appears in the vulnerability

	findings query builder by default, with **Active**, **Resurfaced** and **New** selected. For more information, see Vulnerability States.
Stig Severity	The STIG severity associated with the finding.
Synopsis	A brief description of the plugin or vulnerability.
Target Groups	A target group or groups associated with the scan that identified the vulnerability. For more information, see Target Groups.
Time Taken to Fix	How long it took your organization to fix a vulnerability identified on a scan in days. Only appears for Fixed vulnerabilities. Use this filter along with the **State** filter set to **Fixed** for more accurate results. When exported, this field is shown in milliseconds.
Unsupported by Vendor	Software found by this plugin is unsupported by the software's vendor (for example, Windows 95 or Firefox 3).
VPR	The Vulnerability Priority Rating Tenable calculated for the vulnerability.
VPR Threat Intensity	A vulnerability's Tenable-calculated threat intensity based on the number and frequency of threat events. Options are **Very Low**, **Low**, **Medium**, **High**, or **Very High**.
Vulnerability Published	The date when the vulnerability definition was first published (for example, the date that the CVE was published).
Weaponization	If a vulnerability is judged to be ready for use in a cyberattack. Options are **Advanced Persistent Threat**, **Botnet**, **Malware**, **Ransomware**, or **Rootkit**.

Cloud

Cloud Misconfiguration Filters

Option	Description	
Filters		

Account ID	The unique identifier assigned to the asset resource in the cloud service that hosts the asset on which a scan detected the finding.	
ARN	The Amazon Resource Name (ARN) for the asset on which a scan detected the finding.	
Asset ID	The UUID of the asset on which a scan detected the finding. This value is unique to Tenable Vulnerability Management.	
Benchmark	The benchmark associated with the finding.	
Cluster	The cluster associated with the finding.	
Created Time	The time and date when Tenable Vulnerability Management created the asset record on which a scan detected the finding.	
Criticality	The criticality of the vulnerability finding.	
Exists in Cloud	Indicates whether the affected cloud resource exists in a cloud environment.	
Exists in IAC	Indicates whether the affected asset was created via Infrastructure as Code (IaC).	
Finding ID	The unique Tenable ID for the finding. To view the ID for a finding, click its details and check the page URL in your browser's address bar for an alphanumeric string between *details* and *asset*.	
First Seen	The date when Tenable Vulnerability Management first scanned the affected asset.	
Found in TF State	Indicates whether or not the finding was discovered in a TF state.	
IaC Resource Type	The Infrastructure as Code (IAC) resource type of the asset.	
IaC Type	The Infrastructure as Code (IAC) type of the asset.	
Ignored	Indicates whether Tenable Vulnerability Management ignored the policy violation when calculating the finding's severity.	

Immutable Drift	Indicates whether the asset has immutable drifts.	
Is Attribute	Specifies whether the asset is an attribute.	
Last Fixed	The date when the finding was last fixed.	
Last Scan Time	The date when a scan was last run against the finding.	
Last Seen	The date when Tenable Vulnerability Management last scanned the affected asset.	
Managed By	The name of the person, group, or company that manages the affected asset.	
Policy Category	The policy category associated with the finding.	
Policy ID	The unique ID for the cloud policy associated with the affected asset.	
Policy Name	The unique ID for the cloud policy associated with the affected asset.	
Policy Type	The unique ID for the cloud policy associated with the affected asset.	
Project	The project associated with the finding.	
Provider	The third-party provider associated with the finding.	
Region	The cloud region where the affected asset runs.	
Repositories	Any code repositories associated with the affected asset.	
Resource Category	The category of the asset resource in the cloud service that hosts the affected asset.	
Resource ID	The ID of the asset resource in the cloud service that hosts the affected asset.	
Resource Name	The name of the asset resource in the cloud service that hosts the affected asset.	

Resource Type	The type of the asset resource in the cloud service that hosts the affected asset.	
Result	The outcome of the scan. Possible options are: • **Failed** • **Passed** • **Unknown**	
Rule ID	The unique ID for the security rule for which the scanner found a violation.	
Rule Reference ID	The reference ID for the security rule for which the scanner found a violation.	
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR. This filter appears in the filters plane by default, with **Critical**, **High**, **Medium**, and **Low** selected.	
Source Line	The source line associated with the finding.	
Updated Time	The time and date when the asset record was last updated.	
Version	The version associated with the finding.	
VPC	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud Documentation.	

Host Audit Filters

Option	Description
Filters	
Asset ID	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Vulnerability Management.

Asset Name	The name of the asset on which the scanner performed an audit check. This value is unique to Tenable Vulnerability Management.
Asset Tags	Asset tags, entered in pairs of `category` and `value` (for example Network: Headquarters). This includes the space after the colon (:). If there is a comma in the tag name, insert a backslash (\) before the comma. If your tag name includes double quotation marks (" "), use the UUID instead. You can add a maximum of 100 tags. For more information, see Tags.
Audit File	The name of Audit file the scanner used to perform the audit. Audit files are XML-based text files that contain the specific configuration, file permission, and access control tests to be performed.
Audit Check Name	The name Tenable assigned to the audit. In some cases, the compliance control may be listed as the prefix within the name.
Benchmark	Benchmarks are published best practices released from source authorities, such as Center for Internet Security (CIS), United States Defense Information Systems Agency (DISA), and Microsoft. This filter provides a list of the supported benchmarks and the version of the benchmark.
Benchmark Specification Name	The benchmark name.
Benchmark Version	The benchmark version. **Note**: Use this filter with the **Benchmark** filter.
Compliance Control	There are a series of designations within the compliance frameworks that Tenable calls controls. For example: CSF:DE.CM-3, 800-53:AU-12c, STIG-ID:WN10-AU-000045, and so on. This is a text-based field to filter on the specific control(s). **Note**: Use this filter in conjunction with the **Compliance Framework** filter.

Compliance Family Name	There are a series of designations within compliance frameworks that Tenable calls control. For example: ISO/IEC-27001:A.12.4.1, or CSF:DE.CM-1. This filter groups the controls into families for easier and more efficient queries. For example: A12 - Operations security or CSF:Detect. **Note**: Use this filter in conjunction with the **Compliance Framework** filter.
Compliance Framework	Tenable audits configuration compliance with a variety of standards including GDPR, ISO 27000, HIPAA, NIST 800-53, PCI DSS, and so on. This filter allows searching based on the respective framework.
Control ID	An ID that can correlate results with other results that meet a certain benchmark recommendation. You can use this filter to identify checks in the audit portal.
First Audited	Identifies the first date the audit check was performed on the asset.
FQDNs	The fully qualified domain names (FQDNs) for the asset.
IPv4 Address	The IPv4 address for the affected asset. You can add up to 256 IP addresses to this filter.
IPv6 Address	The IPv6 address for the affected asset.
Last Audited	Identifies the date of the most recent audit check performed on the asset.
Last Fixed	The date when the finding was last fixed.
Last Seen	The date when a scan last observed the finding.
Original Result	The result from the initial audit.
Plugin ID	The Nessus Plugin ID used to perform the audit check.
Plugin Name	The name of the plugin that identified the audit finding.
Result	The current or modified result from the audit check.
Result Modified	Rules can be created to accept or modify the results of an audit check. This filter allows you to report modified results.

Web Application Vulnerabilities Filters

Option	Description
Asset ID	The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management.
Asset Name	The name of the asset where the scanner detected the vulnerability. This value is unique to Tenable Vulnerability Management. This filter appears on the filter plane by default.
Bugtraq ID	The Bugtraq ID for the plugin that identified the vulnerability.
CPE	The Common Platform Enumeration (CPE) numbers for vulnerabilities that the plugin identifies. (200 value limit)
CVE	The Common Vulnerability and Exposure (CVE) IDs for the vulnerabilities identified by the plugin and corresponding to a specific finding. (200 value limit)
CVSSv2 Base Score	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
CVSSv2 Vector	The raw CVSSv2 metrics for the vulnerability. For more information, see the CVSSv2 documentation on the FIRST website.
CVSSv3 Base Score	The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
CVSSv3 Vector	More CVSSv3 metrics for the vulnerability.
CWE	The Common Weakness Enumeration (CWE) for the vulnerability.
First Seen	The date when a scan first found the vulnerability on an asset.
Input Name	The name of the specific web application component that the vulnerability exploits.

Input Type	The web application component type (for example, form, cookie, header) that the vulnerability exploits.
IPv4 Address	The IPv4 address for the affected asset. You can add up to 256 IP addresses to this filter.
Last Fixed	The date when the finding was last fixed.
Last Seen	The date when a scan last observed the finding.
Original Severity	The vulnerability's CVSS-based severity when a scan first detected the finding. For more information, see CVSS vs. VPR.
OWASP 2010	The Open Web Application Security Project (OWASP) 2010 category for the vulnerability targeted by the plugin.
OWASP 2013	The Open Web Application Security Project (OWASP) 2013 category for the vulnerability targeted by the plugin.
OWASP 2017	The Open Web Application Security Project (OWASP) 2017 category for the vulnerability targeted by the plugin.
OWASP 2021	The Open Web Application Security Project (OWASP) 2021 category for the vulnerability targeted by the plugin.
OWASP API 2019	The Open Web Application Security Project (OWASP) 2019 category for the API vulnerability targeted by the plugin. Possible options are: • **API1:2019 Broken Object Level Authorization** • **API2:2019 Broken User Authentication** • **API3:2019 Excessive Data Exposure** • **API4:2019 Lack of Resources & Rate Limiting** • **API5:2019 Broken Function Level Authorization** • **API6:2019 Mass Assignment** • **API7:2019 Security Misconfiguration** • **API8:2019 Injection**

	• **API9:2019 Improper Assets Management** • **API10:2019 Insufficient Logging & Monitoring**
Plugin Description	The description of the Tenable plugin that identified the vulnerability.
Plugin Family	The family of the plugin that identified the vulnerability. (200 value limit)
Plugin ID	The ID of the plugin that identified the vulnerability. (200 value limit)
Plugin Modification Date	The date on which the plugin was last modified.
Plugin Name	The name of the plugin that identified the audit finding.
Plugin Published	The date on which the plugin that identified the vulnerability was published.
Risk Modified	The risk modification applied to the vulnerability's severity. Possible options are: • **Recast** • **Accepted** • **None** For more information, see Recast/Accept Rules.
See Also	Links to external websites that contain helpful information about the vulnerability.
Severity	The CVSS score-based severity. For more information, see CVSS Scores vs. VPR in the Tenable Vulnerability Management User Guide. This filter appears in the filters plane by default, with **Critical**, **High**, **Medium**, and **Low** selected.

Solution	A brief summary of how you can remediate the vulnerability.
State	The state of the vulnerability detected in the finding. Options are Fixed, Resurfaced, Active, New. Appears in the vulnerability findings query builder by default, with **Active**, **Resurfaced** and **New** selected. For more information, see Vulnerability States.
Url	The complete URL on which the scanner detected the vulnerability. This filter appears in the filters plane by default.
WASC	The Web Application Security Consortium (WASC) category associated with the vulnerability targeted by the plugin.

Group Your Findings

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Findings** workbench, you can group your findings by specific attributes. You can group host vulnerabilities, cloud misconfigurations, and web application findings, but you cannot group host audit findings.

To group your vulnerability findings:

1. In the left navigation, click **Findings**.

   The **Findings** workbench appears.

2. Do one of the following:

   To group your host vulnerability findings...

   a. Next to **Group By**, click one of the following:

   - **Asset** – The name of the asset where a scan identified a vulnerability.
   - **Plugin** – The name of the plugin that identified a vulnerability.

   The system groups your findings by the selected attribute.

b. View the following details about your grouped findings. These vary depending on the attribute you select:

Column	Description
Asset	
Asset Name	The name of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management.
Asset Tags	Asset tags for the affected asset. Hover over the first tag to view any additional tags.
Last Seen	The date and time when a scan last found the vulnerability on the asset.
Asset IP	The IPv4 or IPv6 address associated with the asset record.
Vulnerabilities	A descriptive image that indicates vulnerability percentages by CVSS-based severity for each set of grouped findings. For more information, see CVSS vs. VPR.
Vuln Count	The number of vulnerabilities that Tenable Vulnerability Management identified on each set of grouped findings.
Critical	The number of vulnerabilities with a critical CVSS-based severity rating on each set of grouped findings. For more information, see CVSS vs. VPR.
High	The number of vulnerabilities with a high CVSS-based severity rating on each set of grouped findings. For more information, see CVSS vs. VPR.
Plugin	
Severity	The CVSS-based severity score identified on each set of

	grouped findings. For more information, see CVSS vs. VPR.
Name	The name of the plugin that identified the vulnerability.
Family	The family of the plugin that identified the vulnerability.
Plugin ID	The ID of the plugin that identified the vulnerability.
Vuln Count	The number of vulnerabilities that Tenable Vulnerability Management identified on each set of grouped findings.

To group your cloud misconfiguration findings...

a. Next to **Group By**, click one of the following:

- **Policy** – The cloud policy associated with the affected asset.

  Policy Group – The unique ID for the cloud policy associated with the affected asset.

- **Resource Type** – The name of the cloud resource type (for example, a resource group or virtual machine).

The Findings table displays your findings grouped by the selected attribute.

b. View the following details about your grouped findings. These vary depending on the attribute you select:

Column	Description
Policy	
Policy Name	The name of the policy associated with the affected asset.
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.
Source	The source of the policy. Possible values are: • Cloud

	• IaC (Infrastructure as Code)
Last Seen	The last date the vulnerability was identified in a scan.
Count of Impacted Resources	The number of cloud resources the vulnerability impacts.
Policy Group	
Policy ID	The unique ID for the cloud policy associated with the affected asset.
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.
Policy Group	The group associated with the security policy that governs the affected asset.
Exists in Cloud	Indicates whether the affected cloud resource exists in a cloud environment.
Exists in IAC	Indicates whether the affected asset was created via Infrastructure as Code (IaC).
Count of Impacted Resources	The number of cloud resources the vulnerability impacts.
Misconfiguration Count	The number of misconfigurations that Tenable Vulnerability Management identified on each set of grouped findings.
Resource Type	
Resource Type	The CVSS-based severity score identified on each set of grouped findings. For more information, see CVSS vs. VPR.
Count of Affected Resources	The number of cloud resources the vulnerability affects.

Count of Immutable Drift	The number of discrepancies between the running cloud environment on which the affected resource runs and the Infrastructure as Code (IaC) that was used to deploy it.
Misconfiguration Count	The number of misconfigurations that Tenable Vulnerability Management identified on each set of grouped findings.

To group your web application findings...

a. Next to **Group By**, click one of the following:

- **Asset** – The unique name for the web application associated with the affected asset.
- **Plugin** – The ID of the web application resource type (for example, a resource group or virtual machine).

The web application findings table appears with your findings grouped by the selected attribute.

b. View the following details about your grouped findings. These vary depending on the attribute you select:

Column	Description
Asset	
Asset Name	The name of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management.
Vulnerabilities	A descriptive image that indicates vulnerability percentages by CVSS-based severity for each set of grouped findings. For more information, see CVSS vs. VPR.
Critical	The number of vulnerabilities with a critical CVSS-based severity rating on each set of grouped findings. For more

	information, see CVSS vs. VPR.
High	The number of vulnerabilities with a high CVSS-based severity rating on each set of grouped findings. For more information, see CVSS vs. VPR.
Vuln Count	The number of vulnerabilities that Tenable Vulnerability Management identified on each set of grouped findings.
Last Seen	The date and time when a scan last found the vulnerability on the asset.
Actions	The actions you can perform with each set of grouped findings.
Plugin	
Severity	The CVSS-based severity score identified on each set of grouped findings. For more information, see CVSS vs. VPR.
Name	The name of the plugin that identified the vulnerability.
Family	The family of the plugin that identified the vulnerability.
CVSSv2 Base Score	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). **Note:** Based on your severity metric settings, this parameter may display CVSSv3 base scores. For more information, see General Settings.
Plugin ID	The ID of the plugin that identified the vulnerability.
Asset Count	The number of assets that Tenable Vulnerability Management identified on each set of grouped findings.
Vuln Count	The number of vulnerabilities that Tenable Vulnerability

	Management identified on each set of grouped findings.
Actions	The actions you can perform with each set of grouped findings.

Create Recast Rules from Findings

On the **Findings** workbench in **Vulnerabilities** or **Host Audits**, you can create rules to change the status of findings or hide them. You can also create rules from **Settings** > **Recast**, as described in Create Recast Rules from Settings.

Tip: To learn more about when to create rules and how to manage them, see Recast Rules.

Create a Recast or Accept Rule

To create a Recast or Accept rule:

1. In the left navigation, click **Findings**.

   The **Findings** workbench appears.

2. Click the **Vulnerabilities** tab.

   A table of results containing your host vulnerabilities appears.

3. In the **Actions** column for the finding to target, click .

   A drop-down appears.

4. In the drop-down, click **Recast**.

   A plane of options appears. Set these options as follows:

Option	Description
Action	Click **Accept** or **Recast**. To learn about these rule types, see About Recast and Accept Rules.
Vulnerability	Type the Tenable Plugin ID for the vulnerability, for example *70658*.

Plugin ID	
New Severity	(Recast rules only) Select the severity you want to change the corresponding vulnerability to, for example *Low*.
Targets	Select **All** or **Custom**. If the rule will override other rules, a warning appears. The most recently created rule trumps other rules.
Target Hosts	For **Custom** targets, enter up to 1000 comma-separated IPv4 addresses or ranges, hostnames, Classless Inter-Domain Routing (CIDR) notations, or fully qualified domain names (FQDNs). **Caution**: If you target findings by IP address and have multiple networks, the rule matches findings on all your networks. For more information, see Networks.
Expires	Select **After** or **Exact Date**. Then, type a number of days or a date when the rule will expire.
Comments	Type comments to provide rule details.
Report as False Positive to Tenable	(Optional) (Accept rules only) Turn on this toggle when a plugin generates inaccurate findings and you want Tenable to review the results.

5. Click **Save**.

   The system processes the rule, which may take time if many findings are targeted. When complete, the the **Findings** workbench is updated and the rule appears in **Settings** > **Recast**.

Create a Change Result or Accept Rule

Caution: For best performance, the system supports a maximum of *5000* Change Result and Accept rules in each container, total.

To create a Change Result or Accept rule:

1. In the left navigation, click **Findings**.

   The **Findings** workbench appears.

2. Click the **Host Audits** tab.

   A table of results containing your host audit findings appears.

3. In the **Actions** column for the finding to target, click ⋮.

   A drop-down appears.

4. Click **Add Recast Rule**.

   A plane of options appears. Set these options as follows:

Option	Description
Action	Click **Accept** or **Change Result**. To learn about these rule types, see About Change Result and Accept Rules.
Category	Select a category for the new rule, for example, *Windows*.
Audit File	Select an audit file to run against your assets, for example, *CIS_MS_Windows_11_Enterprise_Level_1_v1.0.0.audit*.
Audit Name	Type an audit name, for example, *9.3.1 Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'*.
Original Result	Select the original result of the host audit, for example, *Failed*.
New Result	(Change Result rules only) Select the result to change the targeted findings to.
Targets	(Optional) Select **Custom**. If the rule will override other rules, a warning appears. The most recently created rule trumps other rules.
Target Hosts	For **Custom** targets, type a comma-separated list of IPv4 addresses or ranges, hostnames, Classless Inter-Domain Routing (CIDR) notation, or fully qualified domain names (FQDNs). The system supports up to

	100 items.
Expires	(Optional) Select **After** or **Exact Date**. Then, type a number of days or a date when the rule will expire.
Comments	Type comments to provide rule details.

5. Click **Save**.

   The system processes the rule, which may take time if many findings are targeted. When complete, the the **Findings** workbench is updated and the rule appears in **Settings** > **Recast**.

Generate a Findings Report

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

On the **Findings** workbench, you can build a report about the vulnerabilities in your environment. You can also schedule this report and email it.

Note: You can only generate reports for vulnerabilities and host audit findings. These reports must contain less than 10,000 findings.

Note: You cannot run more than 50 reports at a time.

To generate a report:

1. In the left navigation, click **Findings**.

   The **Findings** workbench appears.

2. Click the **Vulnerabilities** or the **Host Audits** tab.
3. (Optional) Using a maximum of *five* filters, refine the list of findings, as described in Use Filters.
4. Select the check boxes next to the findings to report on.

   The action bar appears.

5. In the action bar, click **Generate Report**.

The **Generate Report** plane appears.

Option	Description
Name	(Optional) Type a name for the report.
Templates	Select a template for the report. Vulnerabilities Findings Templates: • **Host Findings Executive Summary Report** – Summarizes severity levels for the vulnerabilities you are reporting on, as well as the criticality, last scan time, and port count of the associated assets. • **Host Findings Vulnerability Details by Plugin** – Details the vulnerabilities you are reporting on by plugin. • **Host Findings Vulnerability Details by Asset** – Lists associated assets for the vulnerabilities you are reporting on. Host Audit Findings Templates: • **Host Audits Executive Summary Report** – Summarizes severity levels for the vulnerabilities you are reporting on, as well as the criticality, last scan time, and port count of the associated assets. • **Host Audit Details by Audit Check** – Lists the vulnerabilities you are reporting on by audit check. • **Host Audit Details by Asset** – Lists the associated assets for the vulnerabilities you are reporting on.
Schedule	Turn on the **Schedule** toggle to schedule the report: a. In the **Start Date and Time** section, choose the date and time when the report will run. b. In the **Time Zone** drop-down, choose a time zone. c. In the **Repeat** drop-down, choose the cadence on which you want

	the report to repeat (for example, daily). d. In the **Repeat Ends** drop-down, choose the date when the report will stop running.
Add Recipients	(Optional) Type the emails where you want Tenable Vulnerability Management to send the finished report.
Password Protection	(Optional) Enable this toggle to password-protect your report with AES 128-bit encryption. In the **Encryption Password** field, type a password to provide to the recipients.

6. Click **Generate Report**.

   A confirmation message appears and the system starts to build the report. Click the link in the message to view the report. Or, go to the **Reports** > **Report Results** page.

Solutions

Tenable provides recommended solutions for all vulnerabilities on your network. You can sort recommended solutions by VPR to identify your highest priority solutions, then drill into the solution details to understand the steps to address the vulnerability on your network.

Note: You cannot view solution details without a Tenable Lumin license. For more information, see Welcome to Tenable Lumin.

View Solutions

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable provides recommended solutions for all vulnerabilities on your network. You can sort recommended solutions by Vulnerability Priority Rating (VPR) to identify your highest priority solutions, then drill into the solution details to understand the steps to address the vulnerability on your network.

Addressing a vulnerability instance lowers your CES and AES metrics.

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 solutions in the new interface:

1. In the left navigation, click **Solutions**.

   The **Solutions** page appears.

2. **Note:** All Tenable Lumin data reflects all assets within the organization's Tenable Vulnerability Management instance.

   On this page, you can:

Section	Action

Filters	Filter the data displayed in the table.
Saved Searches drop-down box	• Load or edit an existing saved search. • Save a new saved search.
Export	Export a solution as a `.csv` file.

Solutions table	• View information about each solution.
	  • **Solution** – A description for the solution.
	  • **Assets Affected** – The total number of assets affected by the vulnerabilities addressed by the solution.
	  • **CVE Count** – The CVEs included in the solution.
	  • **VPR** – The highest VPR for the vulnerabilities addressed by the solution.
	  • **CVSS** – The highest CVSSv2 score (or CVSSv3 score, when available) for the vulnerabilities addressed by the solution.
	• To view details for a solution, click a solution row.
	  The **Solution Details** page appears. For more information, see Solution Details.
	• To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see Tables.

Solutions Filters

> **Required Additional License:** Tenable Lumin

On the **Solutions** page, you can filter vulnerabilities using Tenable-provided filters and filters based on asset tags.

Tenable-provided Filters

Tenable Vulnerability Management provides the following solutions filters:

Filter	Description
ACR Score	The ACR of assets associated with the solution.
ACR Severity	The ACR severity of assets associated with the solution.
AES Severity	The AES severity of assets associated with the solution.
Asset Count	The number of assets impacted by the solution.
Asset ID	The UUID of assets associated with the solution. This value is unique to Tenable Vulnerability Management.
CVE Count	The Common Vulnerability and Exposure (CVE) count associated with the solution.
CVSS	The Common Vulnerability Scoring System (CVSS) score of vulnerabilities associated with the solution.
CVSS Severity	The Common Vulnerability Scoring System (CVSS) severity of vulnerabilities associated with the solution.
Family	The plugin family associated with the solution.
Hostname	The hostname of the asset associated with the solution. **Note:** Ensure the search query does not end in a period.
License Status	The licensing status of assets associated with the solution.
Solution	A brief summary of how you can remediate the vulnerability.
VPR	The Vulnerability Priority Rating (VPR) of vulnerabilities associated with the solution.
VPR Severity	TheVulnerability Priority Rating (VPR) severity of vulnerabilities associated with the solution.

Tag Filters

In Tenable Vulnerability Management, tags allow you to add descriptive metadata to assets that helps you group assets by business context. For more information, see Tags.

In the **Category** drop-down box for a filter, your organization's tags appear at the bottom of the list, after the Tenable-provided filters.

Export Solutions

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

In the new interface, the export feature allows you to export solution data `.csv` file format.

To export solutions as a `.csv` file:

1. In the left navigation, click **Solutions**.

   The **Solutions** page appears.

2. In the upper-right hand corner, click **Export**.

   The **Export** plane appears.

3. View the selected format for the export: CSV.

4. Click the check box next to the **Data** option you want included in the export file.

Data	Description
Solutions	Includes solutions data.
Details	Includes solutions data and data for assets affected where Tenable recommends the solutions.

5. Click **Export**.

   Tenable Vulnerability Management begins processing the report. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the report.

   When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the

download is complete.

6. Access the export file via your browser's downloads directory.

View Solution Details

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can use this page to view details for a solution, including asset and vulnerability information.

To view solution details in the new interface:

1. In the left navigation, click **Solutions**.

   The **Solutions** page appears.

2. Click a solution row.

   The **Solution Details** page appears.

   On this page, you can:

Section	Action
Summary panel	
Metrics summary	View summary statistics for the recommended solution. • **Assets Affected** – The total number of assets affected by the vulnerabilities addressed by the solution. • **CVE Count** – The total number of CVEs included in the solution. • **CVE Instances** – The total number of vulnerabilities addressed by the solution. • **VPR** – The highest VPR for a vulnerability included in the solution.

	• **CVSS V2/V3 Base Score** – The highest CVSSv2 score (or CVSSv3 score, when available) for the vulnerabilities addressed by the solution.

Vulnerabilities Included (#) table	• View all vulnerabilities addressed by the solution.
	  • **Identifier** – The vulnerability identifier: the CVE (if available), the TVI, or the plugin ID.
	  • **VPR** – The VPR for the vulnerability.
	  • **CVSS** – The CVSSv2 score (or CVSSv3 score, when available) for the vulnerability.
	  • **Assets Affected** – The total number of assets affected by the vulnerability.
	• To view details about a vulnerability, click a vulnerability row.
	The vulnerability details plane appears. On this plane, you can:
	  • View a summary of the vulnerability.
	  • View information about the key drivers Tenable used to calculate the VPR for this vulnerability.
	  • View a graph that shows the VPR adjustments over the past 30 days, compared to the static CVSSv2 score (or CVSSv3 score, when available).
	  • View additional information about the vulnerability, including the TVI.
	• To navigate to another page of the table, see Tables.

Assets Affected tab	
ACR tiles	View the ACR severity tiles, which summarize the number of affected assets in the **Low**, **Medium**, **High**, or **Critical**, or **Unclassified** ACR category.

Assets Affected table	• View asset information.
	  • **Asset** –
	  The asset identifier, assigned based on the availability of the following attributes in order: Agent name, NetBIOS name, Local hostname, Fully Qualified Domain Name (FQDN), IPv4 address, and IPv6 address.
	  • **IP** – The asset's IP address.
	  • **ACR** – The asset's ACR.
	  • **CVE Count** – The total number of CVEs on the asset.
	  • **OS** – The asset's operating system.
	  • **Detection Source** – The scanner type that first scanned the asset.
	• To view details for an asset, click an asset row.
	  The **Asset Details** page appears. For more information, see View Asset Details.
	• To filter the assets displayed in the table, see Filter a Table.
	  Tenable Vulnerability Management refreshes the table.
	• To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see Tables.

Reports

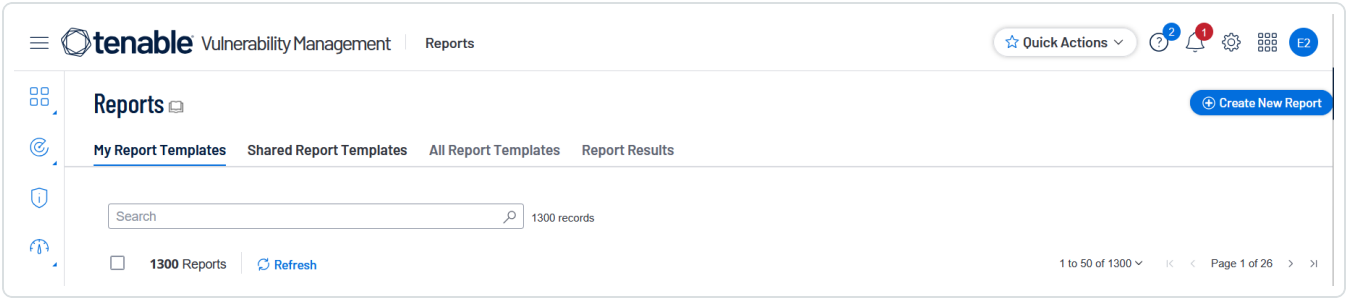
Reports consist of two parts: the report, and the report results. On the **Reports** page, you can create a report from a template, run existing reports, and view the results of those reports.

> **Note:** Reports show data from the last 30 days. Tenable recommends scanning at least monthly to maintain security hygiene and to keep report data up-to-date.

To view the **Reports** page:

1. In the left navigation, click **Reports**.

   The **Reports** page appears.



The **Reports** page includes the following folders:

- The **My Report Templates** folder is the default folder that appears when you access the **Reports** page. Reports that you create appear in this folder.
- The **All Report Templates** folder shows all reports that you have permission to interact with. All reports are user-specific.
- The **Report Results** folder shows all the results from reports that you have permissions to view. Results are displayed in chronological order based on when the reports were run. All results from reports under **Report Results** are user-specific.

  > **Note:** You can only view your own report results. You cannot view other Tenable Vulnerability Management users' report results.

Using Tenable Vulnerability Management, you can generate thematic, informative reports to help you find information that you might otherwise overlook. For example, the Credentialed Scan Failures report delivers a straightforward, organized list of failed credentialed scans that analysts can use to

address scanning issues quickly, making it simpler to troubleshoot problems with credentialed scans. For a complete list of report templates included with Tenable Vulnerability Management, see Tenable Vulnerability Management Report Templates.

Note: PCI Quarterly External scan data is excluded from dashboards, reports, and workbenches intentionally. This is due to the scan's paranoid nature, which may lead to false positives that would otherwise not be detected. For more information, see Tenable PCI ASV Scans.

Report Templates

Tenable Vulnerability Management 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 a complete index of Tenable-provided report templates, see Tenable Vulnerability Management Report Templates.

Tip: For more information on the specific data included in each individual report, see View Report Details.

Note: The **Cyber Insurance Report** includes the following caveats:

- The report cannot be edited in any way. This ensures underwriters can be confident their metrics are 100% accurate.
- This report only includes Explore data from the previous 180 days.
- This report is only available for customers with Explore reports enabled on their container.
- The report name does not change upon subsequent generations of the report. For example, the date/time stamp in the report name does not update the next time you run the report, however the report data itself includes the date on which the report was most recently run.
- Severities are reported using CVSSv3 base scores only.

For more information, see the **Cyber Insurance Report** blog post.

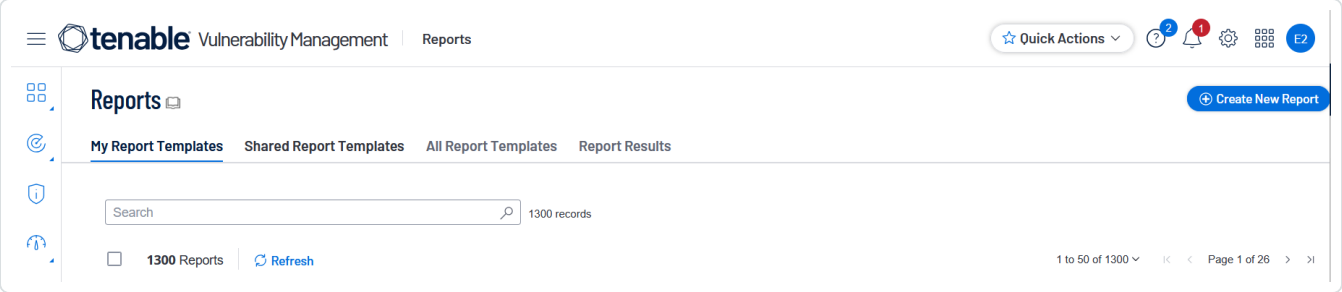
Create a Report

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

To create a new report:

1. In the left navigation, click **Reports**.

   The **Reports** page appears.



2. In the upper-right corner, click **Create New Report**.

   The **Report Templates** page appears, with reports organized by category.

3. Do one of the following:

- To create a report based on a template:

a. In the **Report Templates** list, select a template:

Category	Description
Center for Internet Security (CIS)	CIS Benchmarks are best practices for the secure configuration of a target system. Be sure to use the proper audit file for scans. For example: CIS PostgreSQL 12 v1.1.0 Audit Details, CIS Debian 8 v2.0.2 Audit Details, CIS Amazon Web Services Three-tier Web Architecture v1.0.0 Audit Details, and so on.
Defense Information Systems Agency (DISA)	The Defense Information Systems Agency (DISA) is a United States Department of Defense combat support agency composed of military, federal civilians, and contractors. Security Technical Implementation Guides (STIG) is a configuration standard that consists of cybersecurity requirements for a specific product. Be sure to use the proper audit file for scans.
Compliance Framework	Tenable allows you to audit configuration compliance with a variety of standards including GDPR, ISO 27000, HIPAA, NIST 800-53, PCI DSS, and so on. These reports provide summary and detailed information for all the supported frameworks. Be sure to use the proper audit file for scans.
Host Audit Plugin Type	Organizations such as CIS, DISA, and some vendors create golden configurations standards, known as benchmarks. Tenable creates audit files that perform a detailed configuration review. Scanning the assets with the Host Audit Compliance Check plugins allows you to do detailed configuration checks. These reports provide summary and detailed information for all the Host Audit Compliance Check plugins.

Tenable Best Practice Audits	Allows you to implement best practice audits for new technologies. Make sure that the proper audit file is used for scans.
Vendor Based Audits	Allows you to implement vendor-specific guidance for new technologies. Vendors include: Vendor, IBM, Juniper, Microsoft, NetApp, VMware and others. Be sure to use the proper audit file for scans.
Vulnerability Management	Tenable Vulnerability Management provides the most comprehensive vulnerability coverage with real-time continuous assessment of the organization. These built-in reports allow organizations to communicate risk based on prioritization, threat intelligence and real-time insights to proactively prioritize remediation actions. These reports provide summary and detailed information data collected using Tenable Vulnerability Management applications such as Tenable Nessus.
Web App Scanning	Web application security provides the ability to detect and mitigate threats and vulnerabilities that may compromise the confidentiality, integrity, and availability of web applications. These reports leverage data from Tenable Web App Scanning, a comprehensive and automated vulnerability scanning tool for modern web applications.

The **Report Details** page appears.

a. On the **Report Details** page, do the following:

- (Optional) Click **Update Logo** to add a new logo to your report or select from a list of recently uploaded logos. Select the **Set as default for all reports** checkbox to set a logo as the default.
- In the **Name** box, type a name for the report.

- (Optional) In the **Description** box, type a description.
- In the **Executive Summary** section, select from the available widgets or click **Add New Widget** to add a custom widget or a widget from the widget library to the report.
- In the **Additional Chapters** section, select from the available chapters or click **Add New Chapter** to add report chapters from the **Chapter Library**.
- (Optional) Add a filter to the reports. For more information, see Filter Reports.

- **To create a custom report:**

  a. In the upper-right corner of the Report Templates page, click **Create Custom Report**.

  The **Report Details** page appears.

  b. On the **Report Details** page, do the following:

  - (Optional) Click **Update Logo** to add a new logo to your report or select from a list of recently uploaded logos. Select the **Set as default for all reports** check box to set a logo as the default.
  - In the **Name** box, type a name for the report.
  - (Optional) In the **Description** box, type a description.
  - In the **Executive Summary** section, click **Add New Widget** to add a custom widget or a widget from the widget library to the report.
  - In the **Additional Chapters** section, click **Add New Chapter** to add report chapters from the **Chapter Library**.
  - (Optional) Add a filter to the reports. For more information, see Filter Reports.

4. Click **Save**.

   Tenable Vulnerability Management creates a new report and it appears on the **My Report Templates** page.

Tip: Once created, you can generate an initial report and download a copy. For more information, see Generate Reports.

Generate a Report

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

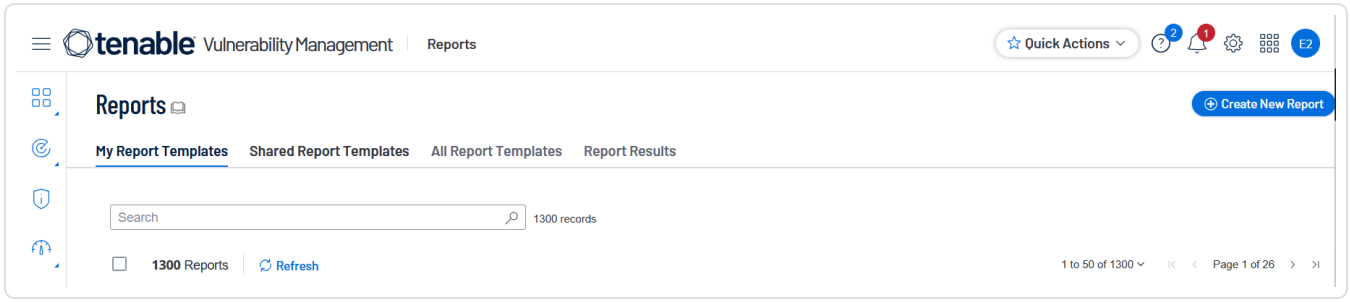
Note: When you disable a user account, that user's scheduled reports are not disabled. If the disabled user shared reports, users with access can still run them. For more information, see Disable a User Account.

Note You cannot run more than 50 reports at a time.

To generate a report:

1. In the left navigation, click **Reports**.

   The **Reports** page appears.

2. On the **Report Results** tab, select the check box next to the report you want to generate.

   The action bar appears at the top of the list.

3. In the action bar, click **Generate Report**.

   Tenable Vulnerability Management starts to generate the report. You can track the report status on the **Report Results** tab.

View Report Details

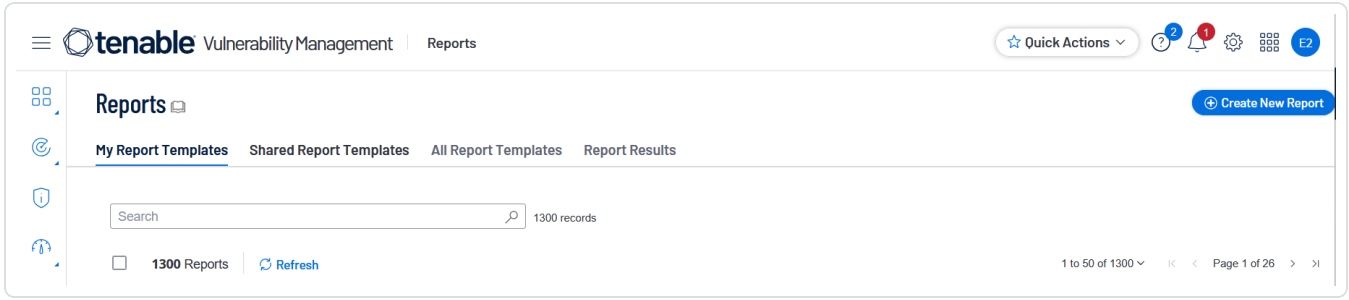
Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

Note: Non-administrator users can only view report details for reports that they created or that have been shared with them by another user.

To view the **Report Details** page, do the following:

1. In the left navigation, click **Reports**.

   The **Reports** page appears.



2. In the **My Report Templates** tab, click the row for the report for which you want to view the details.

   The **Report Details** page appears.

The **Report Details** page shows the following details about your report:

Section	Description
Description	This is a brief description of the report.
Targets	This section shows that all assets are included in the report.
Report Logo	The logo on the report.
History	This section shows the time when the report was generated, the time of report completion, and the current status of the report. a. In the reports table, to download or delete the report, do one of the following: • Select the check box next to the report you want to download or delete. Tenable Vulnerability Management enables **Download** and **Delete** options in the action bar. • In the **Actions** column, click the ⋮ button. From the action options, select one of the following: • **Download** – Click this option to download the report. The report

	downloads in the PDF format. • **Delete** – Click this option to delete the report.
Report Details	The report details include a brief summary of the report: • **Status** – The status of the report. • **Type** – The type of report. For example: PDF. • **Created On** – The date when the report was created. • **Start Time** – The time when the report generation was started. • **End Time** – The time when the report generation was complete. • **Created By** – The user who created the report.

Share Report Templates

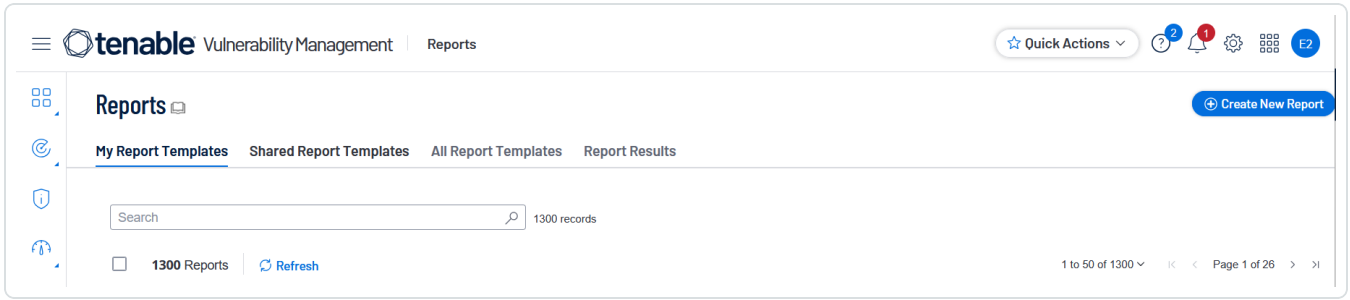
Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

You can share report templates with other users within the organization.

To share report templates:

1. In the left navigation, click **Reports**.

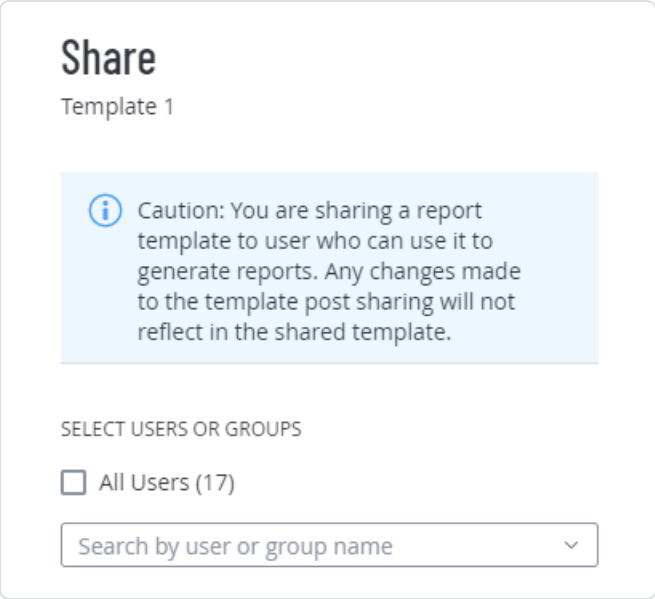
   The **Reports** page appears.



2. Select the report templates that you want to share:

Scope	Action
Share a single report	To share report templates from the **Reports** page: a. On the **My Report Templates** tab, right-click the row for the report template you want to share. -or- On the **My Report Templates** tab, in the **Actions** column, click the ⋮ button in the row for the report template you want to share. The action buttons appear in the row. -or- On the **My Report Templates** tab, select the check box next to the report template you want to share. In the action bar, Tenable Vulnerability Management enables **More** > **Share**. b. Click **Share**.

The **Share** plane appears.



3. In the **Select Users or Groups** section, select **All Users** or search for specific user or groups.

4. Click **Share**.

   Tenable Vulnerability Management shares the report template with the users who can view them in the **Shared Report Templates** tab. Each user receives an email notification with details of the shared report, the email address of the sender, and a link to the shared report.

Edit an Existing Report

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

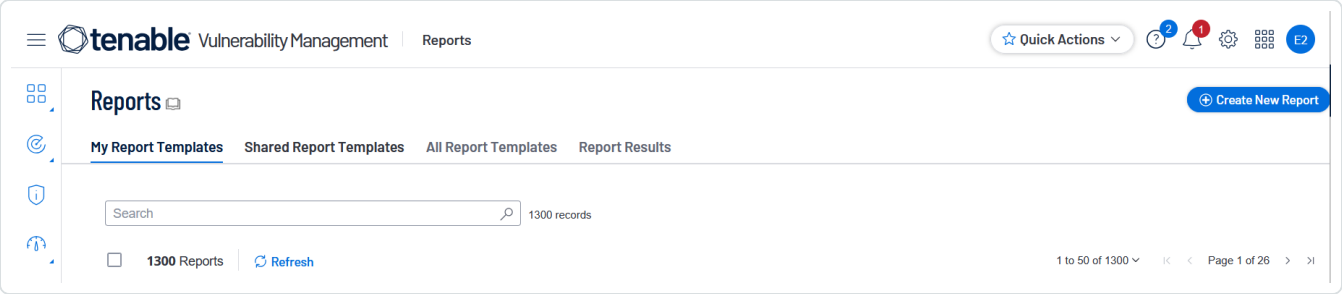
Before You Begin

You can only modify a report if you are the owner, a user with an administrator account, or you have been given the **Can configure** permission for that report.

To edit a report:

1. In the left navigation, click **Reports**.

   The **Reports** page appears.



2. Select the report that you want to edit:

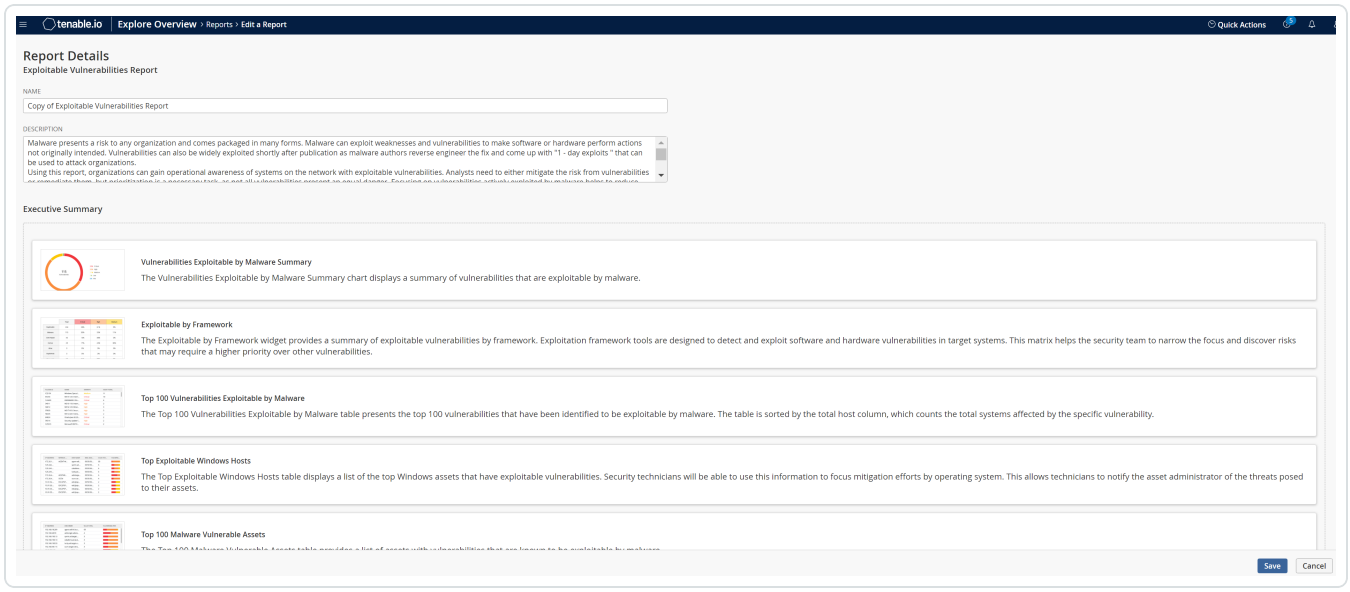
Scope	Action
Edit a single report	To edit a report from the **Reports** page: a. On the **My Report Templates** or **All Report Templates** tab, right-click the row for the report you want to edit. -or-

On the **My Report Templates** or **All Report Templates** tab, in the **Actions** column, click the ⋮ button in the row for the report you want to edit.

The action buttons appear in the row.

b. Click **Edit**.

The **Report Details** page appears.



3. Modify the report settings.
4. Apply filters as needed.
5. Click **Save**.

   Tenable Vulnerability Management saves the report and the **Reports** page appears.

Filter Reports

> **Required Tenable Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

You can add filters to widgets when you create or edit a report. Filters allow you to display details specific to filtered assets in the reports. You can filter by all assets, assets by tags, and custom assets.

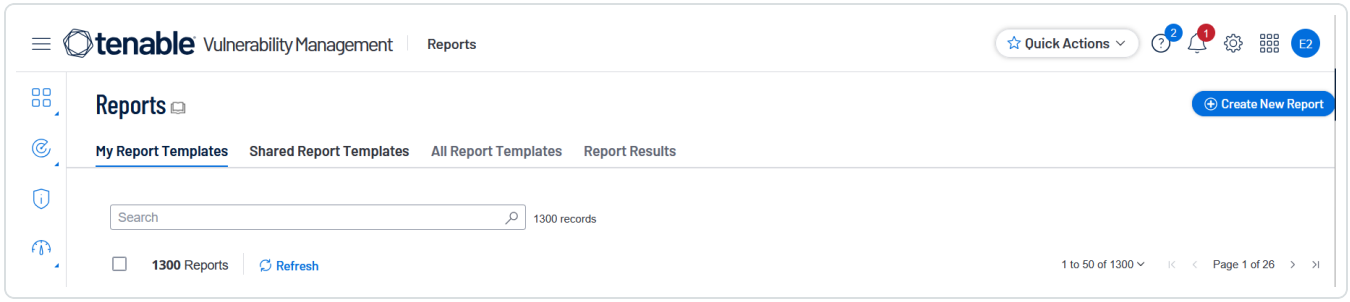
Note: Filtering for reports is currently available only for VM and Explore VM widgets.

Note: Tenable Web App Scanning does not support filtering vulnerabilities by tags.

To create a filter for a new report or an existing report:

1. In the left navigation, click **Reports**.

   The **Reports** page appears.

2. Create a new report or edit an existing report.
3. In the **Report Details** page, click **Edit Filters**.

   The **Filters** plane appears.

4. From the **Select Filter Type** drop-down box, select one of the filters:

   - **All Assets** – Select this to include the data for all assets in the reports. The **All Assets** filter is selected by default.
   - **Tags** – Select multiple tags to filter your reports.
   - **Custom Assets** – Type the IP addresses to filter the data by custom assets.

     Note: When using the **Custom Assets** filter, you can filter by no more than 100 individual IP addresses.

5. Click **Confirm**.

   Tenable Vulnerability Management applies the filters to all widgets. You can hover over the filter icon to view the applied filters.

> **Note**: Tenable Vulnerability Management disables the filter icon when there are no associated filters.

6. (Optional) To edit a filter for a widget, click the icon in the widget, then click **Configure** to open the **Filters** plane.
7. (Optional) To remove a filter for a widget:
   a. In the widget for which you want to remove the filter, click the icon, then click **Delete**.
   b. In the confirmation window, click **Delete** to delete the filter.
8. Click **Save**.

   Tenable Vulnerability Management applies the filters to the report templates.

Schedule a Report

> **Required Tenable Vulnerability Management User Role:** Scan Operator, Standard, Scan Manager, or Administrator

Before You Begin

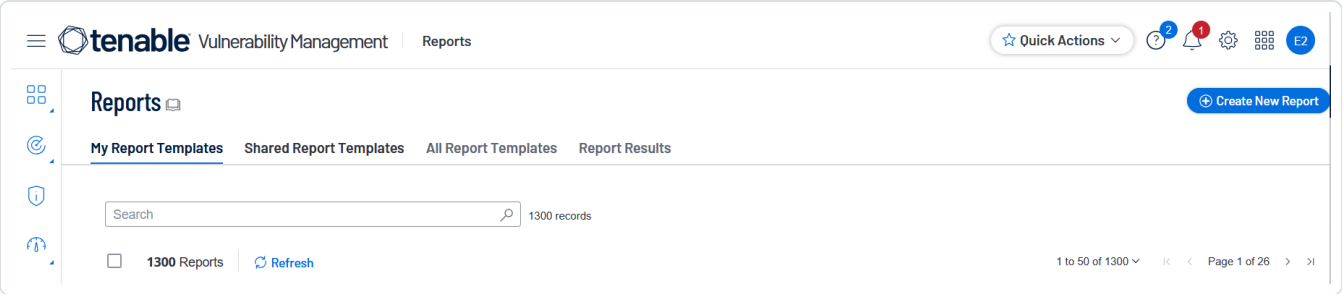
You can only schedule a report if you are the owner, a user with an administrator account, or you have been given the **Can configure** permission for that report.

> **Important:** Disabling a user account does not disable scheduled reports for that user. Additionally, if the disabled user shared a report with other users, these other users can still generate that report. For more information, see Disable a User Account.

To schedule a report:

1. In the left navigation, click **Reports**.

   The **Reports** page appears.



2. On the **My Report Templates** or **All Report Templates** tab, select the check box next to the report that you want to schedule.

   The action bar appears at the top of the table.

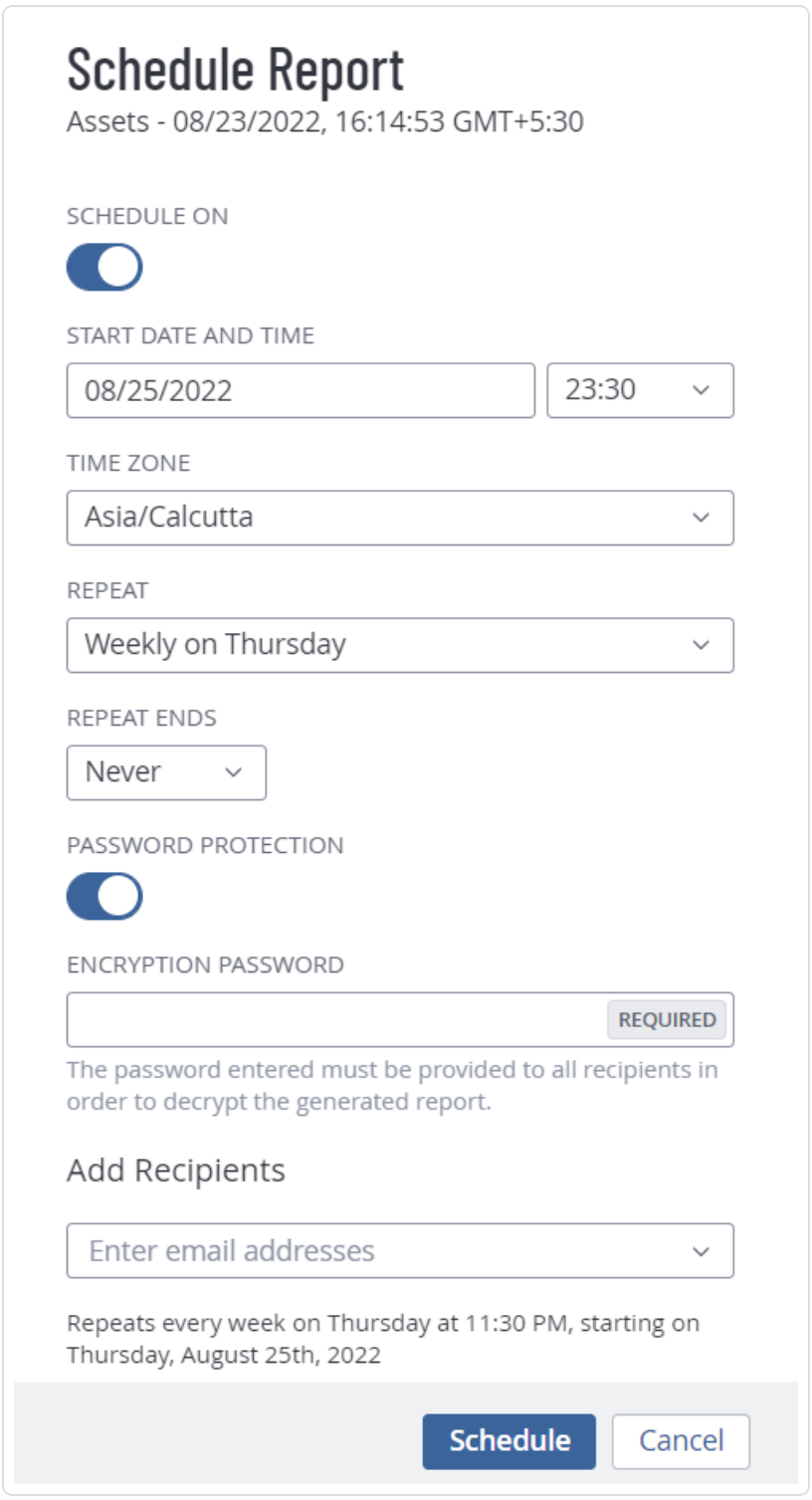
3. Do one of the following:

   - Right-click on the row for the report that you want to schedule.
   - In the action bar, click on the **More** ⋮ button.
   - In the **Actions** column, click the ⋮ button in the row for the report that you want to schedule.

     A menu appears.

4. Click **Schedule**.

   The **Schedule Report** plane appears.



5. Modify the report schedule settings.

Setting	Default	Description
Schedule On	off	A toggle that specifies whether the report is scheduled. By default, reports are not scheduled. When you disable the **Schedule** toggle, the other schedule settings remain hidden. Click the toggle to enable the schedule and view the remaining **Schedule** settings.
Start Date and Time	varies	Specifies the exact date and time when Tenable Vulnerability Management launches the report. The starting date defaults to the date when you create the schedule. The starting time is the nearest half-hour interval. For example, if you create the report schedule on 09/31/2022 at 9:12 AM, Tenable Vulnerability Management sets the default starting date and time to 09/31/2022 and 09:30.
Time Zone	varies	The time zone of the value set for **Start Date and Time**.
Repeat	Once	Specifies how often Tenable Vulnerability Management launches the report. Reports run at the time specified in **Start Date and Time**. • **Once**: Schedule the report to run once. • **Daily**: Schedule the report to run daily. • **Weekly**: Schedule the report to run on a weekly basis. **Note:** The report runs on the day of the week that the schedule begins. For example, if you schedule the report to first run on Monday, 2/14/2021, the report runs on Monday every week.

		• **Monthly**: Schedule the report to run on a monthly basis. **Note:** The report runs on the day of the week that the schedule begins. For example, if you schedule the report to first run on Monday, 2/14/2021, the report runs on the second Monday of every month. • **Custom**: Schedule the report to run on a custom interval, based on a specific number of days, weeks, or months. • **Yearly**: Schedule the report to run on a yearly basis.
Repeat Ends	Never	• **On:** If you select this option, the **End Date** setting appears, where you can select the date you want the report schedule to end. • **Never:** The report runs on the schedule until you modify the report schedule.
Password Protection	Off	A toggle that specifies whether the report schedule is password protected. To set a password for the report: a. Click the **Password Protection** toggle to enable password protection for the report. b. In the **Encryption Password** box, type the password for the report. **Note**: Make sure that you provide this password to the recipients to open the report.
Add Recipients		In this box, type one or more email recipients with whom you want to send the report to. Be sure to press enter

		after each email address entry.

6. Click **Schedule**.

   Tenable Vulnerability Management schedules the report and the recipients receive the report as an email. If you enable the password protection toggle, the recipient must provide the password when prompted.

Email Report Results

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

To share report results:

1. In the **Add Recipients** box, type one or more email recipients for the report results, pressing enter after each entry.

   The recipients you select receive an email with a PDF of the report results.

2. In the **Encryption Password** box, type the password for the generated report.

   Important: Make sure that you provide this password to the recipients to open the report.

   Note: If you provide a password at the time of scheduling the report, Tenable Vulnerability Management applies the same password when emailing the report. For reports for which passwords are applied at the time of scheduling, the **Encryption Password** box appears disabled with a message at the bottom that states that the password is the same as one created during the schedule process.

3. Click **Email**.

   The report results are shared as an email and the **Reports** page appears. If you add a password for the report, the recipient must enter the password when prompted.

Edit a Report Schedule

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

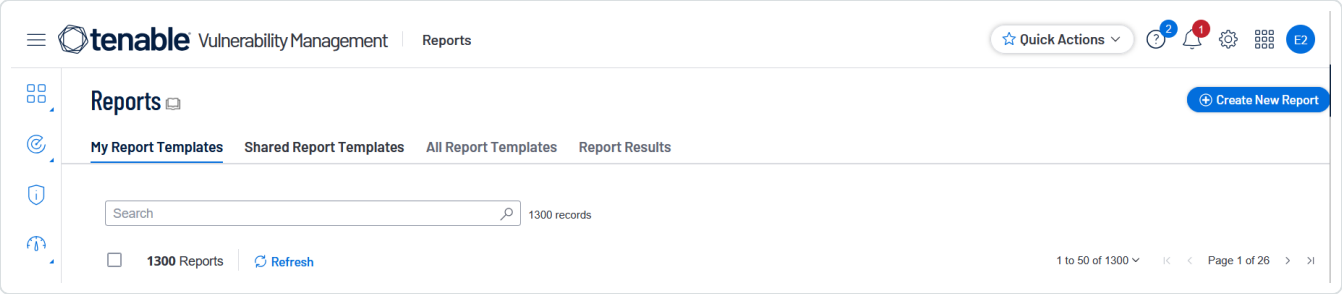
Before You Begin

You can only edit a report schedule if you are the owner, a user with an administrator account, or you have been given the **Can configure** permission for that report.

To edit a report schedule:

1. In the left navigation, click **Reports**.

   The **Reports** page appears.



2. Select the report for which you want to edit the schedule:

Scope	Action
Edit a single report schedule	To edit a report schedule from the **Reports** page: a. On the **My Report Templates** or **All Report Templates** tab, right-click the row for the report you want to edit. -or- On the **My Report Templates** or **All Report Templates** tab, in the **Actions** column, click the ⋮ button in the row for the report you want to edit. The action buttons appear in the row. b. Click **Schedule**.

   The **Schedule Report** pane appears.

3. Modify the report schedule settings.
4. Click **Schedule**.

   Tenable Vulnerability Management saves the report schedule and the **Reports** page appears.

Delete a Report

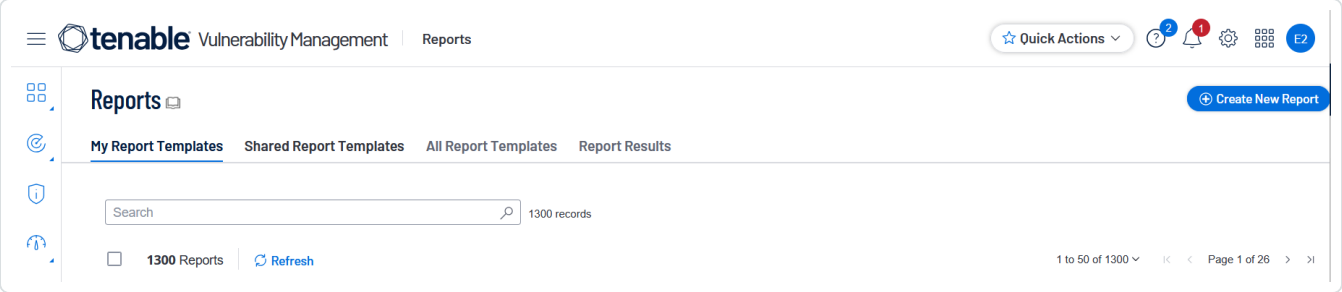
Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

You can only delete a report if you are the owner or a user with an administrator account.

To delete a report:

1. In the left navigation, click **Reports**.

   The **Reports** page appears.



2. Select the reports you want to delete.

Note: This procedure is applicable for both **Report Results** and **Report Templates**.

Scope	Action
Delete multiple	To delete reports:

reports	a. Select the check box for each report you want to delete. The action bar appears at the top of the list. b. In the action bar, click **Delete**.
Delete a single report	To delete a single report: a. Right-click the row for the report you want to delete. -or- Select the check box next to the report you want to delete. Tenable Vulnerability Management enables **More** in the action bar. -or- In the **Actions** column, click the ⋮ button in the row for the report you want to delete. The action buttons appear in the row. b. Click **Delete**.

The **Delete Reports** dialog box appears.

3. Click **Delete**.

   Tenable Vulnerability Management deletes the report permanently.

Exports

From the **Exports** page, you can view and configure your Scheduled Exports and Export Activity.

To view the **Exports** page, do one of the following:

1. In the left navigation, click **Exports**.

   The **Exports** page appears.

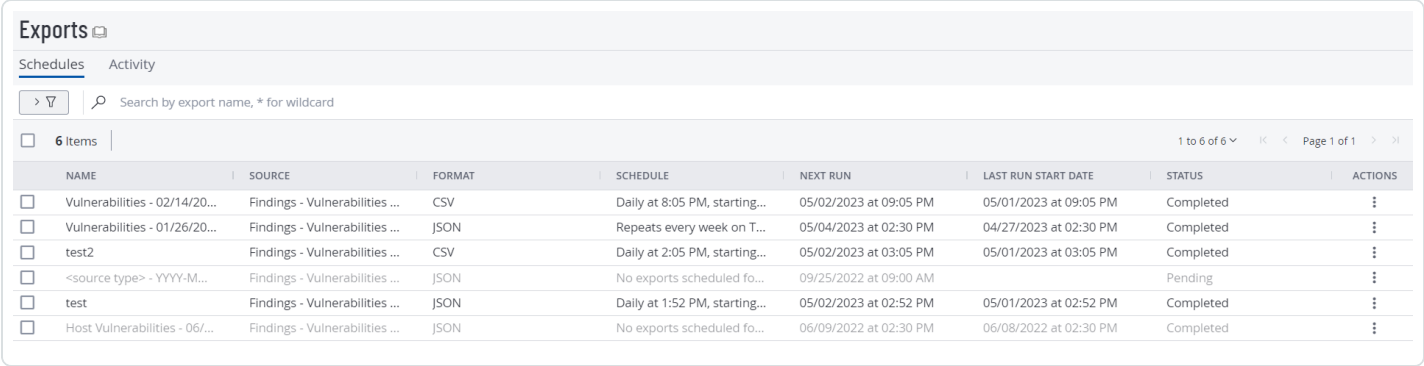
-or-

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears.



Export information on this page comes from the following sources:

- **Assets** – Information about all assets included on your Tenable Vulnerability Management license. For more information, see Export Findings or Assets.
- **Assets Host** –Information about assets Tenable Vulnerability Management identified on your host during a scan. For more information, see Host Assets and Export Findings or Assets.
- **Findings - Vulnerabilities - Host** – Information about the vulnerability findings Tenable Vulnerability Management identified on your host during a scan. For more information, see Export Findings or Assets.

- **Users** – Information about the users assigned to your account. For more information, see Export Users.

For more information, see the following topics:

Scheduled Exports

Export Activity

Scheduled Exports

The **Scheduled Export** page displays details about the exports on your account that include a schedule.

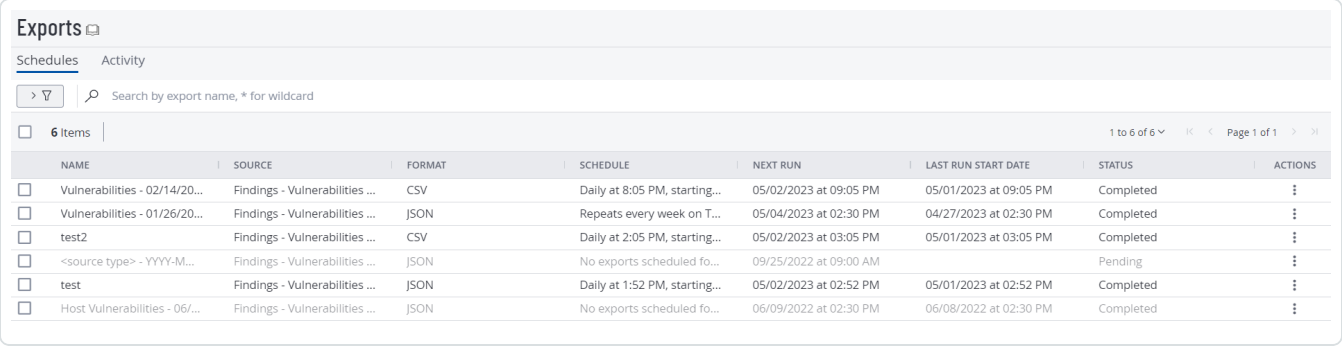
> **Note**: You can retain up to 1000 export schedules on your Tenable Vulnerability Management instance.

To view your scheduled reports export:

- In the left navigation, click → **Export**.

  The **Export** page appears.

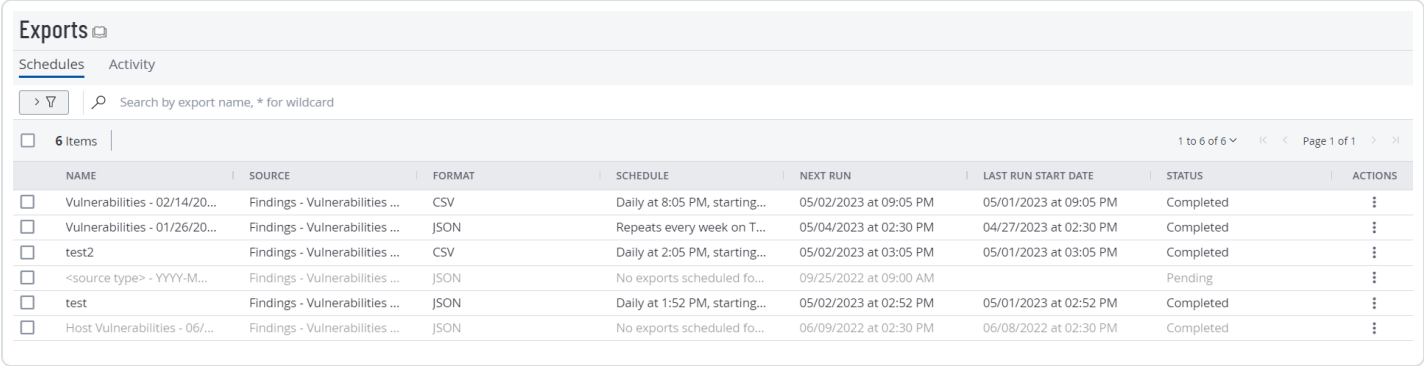
  The **Schedules** tab shows by default.



Export information on this page comes from the following sources:

- **Assets** – Information about all assets included on your Tenable Vulnerability Management license. For more information, see Export Findings or Assets.
- **Assets Host** –Information about assets Tenable Vulnerability Management identified on your host during a scan. For more information, see Host Assets and Export Findings or Assets.

- **Findings - Vulnerabilities - Host** – Information about the vulnerability findings Tenable Vulnerability Management identified on your host during a scan. For more information, see Export Findings or Assets.
- **Users** – Information about the users assigned to your account. For more information, see Export Users.



On the **Scheduled Exports** page, you can do the following:

- View Your Scheduled Exports
- Disable a Scheduled Export
- Enable a Disabled Scheduled Export
- Edit a Scheduled Export
- Delete a Scheduled Export

Note: Export expiration is set via the **Settings** section. For more information, see General Settings.

View Your Scheduled Exports

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Exports** page, you can view all the scheduled exports on your account.

Note: You can retain up to 1000 export schedules on your Tenable Vulnerability Management instance.

To view your scheduled exports:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

Schedules Table

The **Schedules** table contains the following information about your scheduled exports:

Column	Description
Name	The name of the scheduled export file.
Source	The data source for the scheduled export in Tenable Vulnerability Management. Possible sources include: • **Assets** – Information about all assets included on your Tenable Vulnerability Management license. • **Assets Host** –Information about assets Tenable Vulnerability Management identified on your host during a scan. • **Findings - Vulnerabilities - Host** – Information about the vulnerability findings Tenable Vulnerability Management identified on your host during a scan. • **Users** – Information about the users assigned to your account.
Format	The format of the export file, either CSV or JSON.
Schedule	The date, time, and frequency on which your export runs.
Next Run	The date and time when the export is scheduled to run next.
Last Run Start Date	The date and time when Tenable Vulnerability Management last began the export.
Status	The status of the most recent scheduled export.

Actions	The actions you can perform with the scheduled export, including the following: • Disable one or more scheduled exports. • Enable one or more disabled scheduled exports. • Delete one or more scheduled exports.

Disable a Scheduled Export

Required User Role: Administrator

Disabling an scheduled export prevents Tenable Vulnerability Management from automatically creating exports based on the export schedule. You can enable a disabled scheduled export, as described in Enable a Disabled Scheduled Export.

Note: Disabling a scheduled export does not remove the scheduled export from the **Schedules** table or from the list of exports that count against your 1000 scheduled export limit. To remove a scheduled export from your account, you must delete the scheduled export.

To disable a scheduled export:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

4. Do one of the following:

   #### To disable a single scheduled export:

   a. In the **Schedules** table, in the row for the scheduled export you want to disable, click the ⋮ button.

      The action buttons appear in the row.

   b. In the row, click the ⊘ **Disable** button.

To disable multiple scheduled exports:

a. In the **Schedules** table, select the check box for each scheduled export you want to disable.

> **Note**: You can disable up to 10 export schedules simultaneously.

The action bar appears at the top of the table.

b. In the action bar, click the ⊘ **Disable** button.

A success message appears.

Tenable Vulnerability Management disables the selected scheduled export or exports.

In the **Schedules** table, disabled scheduled exports appear in gray.

Enable a Disabled Scheduled Export

> **Required User Role:** Administrator

When you disable a scheduled export, you can enable the scheduled export again to resume the export cadence specified in the schedule.

To enable a disabled scheduled export:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

4. Do one of the following:

   ### To enable a single scheduled export:

   a. In the **Schedules** table, in the row for the scheduled export you want to enable, click the ⋮ button.

   The action buttons appear in the row.

b. In the row, click the **Enable** button.

To enable multiple scheduled exports:

a. In the **Schedules** table, select the check box for each disabled scheduled export that you want to enable.

> **Note**: You can enable up to 10 export schedules simultaneously.

The action bar appears at the top of the table.

b. In the action bar, click the **Enable** button.

A success message appears.

Tenable Vulnerability Management enables the selected scheduled export or schedules.

In the **Schedules** table, enabled scheduled exports appear in black.

Edit a Scheduled Export

> **Required User Role:** Administrator

On the **Exports** page, you can edit a scheduled export, as long as the export job is not currently running. If you are not a Tenable administrator, you can only edit exports you have created.

To edit a scheduled export:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. On the right, in the actions menu click **Edit** .

   The **Export** plane appears.

4. Edit the export options as follows.

Option	Description
Name	Type a custom name for your export.
Formats	Select an export format: • **CSV** – A CSV file that you can open in a spreadsheet application such as Microsoft Excel. **Note**: For findings exports, Tenable Vulnerability Management automatically trims cells longer than 32,000 characters so they appear correctly in Microsoft Excel. Select **Untruncated Data** to disable this. **Note:** If your export file contains a cell that starts with any of the following characters (=, +, -, @), Tenable Vulnerability Management adds a single quote (') at the beginning of the cell. For more information, see the Knowledge Base. • **JSON** – A JSON file containing a nested list of findings, with no empty fields.
Configurations	Select the fields to include: • Under **Select Field Set**, search for or select the fields to add to your export. • To view only selected fields, click **View Selected**. • In the **Expiration** box, type the number of days before the export file ages out.
Schedule	Turn on the **Schedule** toggle to schedule your export: a. In the **Start Date and Time** section, choose the date and time for the export. b. In the **Time Zone** drop-down, choose a time zone. c. In the **Repeat** drop-down, choose the cadence on which you

	want the export to repeat (for example, daily). d. In the **Repeat Ends** drop-down, choose the date when exports end. If you select **Never**, the export repeats until you modify or delete it.
Email Notifications	Turn on the **Email Notification** toggle to send email notifications: a. In the **Add Recipients** box, type the emails to notify. b. In the **Password** box, type a password for the export file. Share this password with the recipients so they can download the export file.

5. Click **Schedule Export**.

   The system saves the updated export.

Delete a Scheduled Export

> **Required User Role:** Administrator

On the **Exports** page, you can delete one or more scheduled exports from your Tenable Vulnerability Management instance.

> **Note**: Deleting a scheduled export removes the schedule from your Tenable Vulnerability Management instance entirely. If you want to instead suspend a scheduled export, you can disable the schedule.

To delete a scheduled export:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

4. Do one of the following:

   #### To delete a single scheduled export:

a. In the **Schedules** table, in the row for the scheduled export you want to delete, click the ⋮ button.

   A menu appears.

b. Click the **Delete** button.

To delete multiple scheduled exports:

a. In the **Schedules** table, select the check box for each scheduled export you want to delete.

   > **Note**: You can delete up to 10 export schedules simultaneously.

   The action bar appears at the top of the table.

b. In the action bar, click the **Delete** button.

Tenable Vulnerability Management deletes the selected scheduled export or exports. Deleted scheduled exports no longer appear in the **Schedules** table.

Export Activity

On the **Export Activity** tab, you can view all the exports created on your account. You can see the source, type, format, status, size, creation date, and author for each export.

> **Note:** Export expiration is set via the **Settings** section. For more information, see General Settings.

> **Note**: By default, Tenable Vulnerability Management allows you to store up to 500 MB of export data at a time. Once you reach this limit, you cannot create new exports until you delete some of your existing export data. To increase your export storage limit, contact your Tenable representative.

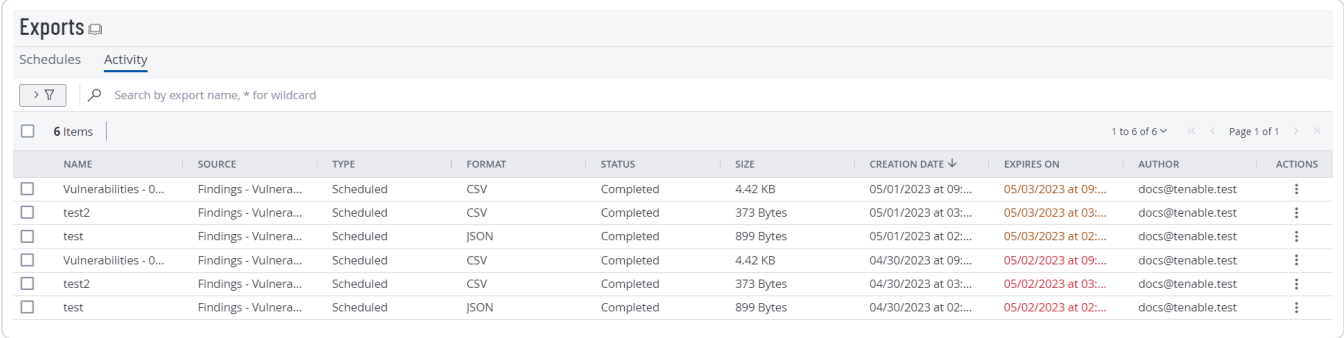
To view your export activity:

- In the left navigation, click **Export**.

  The **Export** page appears.

- Click the **Activity** tab.

The **Activity** page appears.



This page displays a table with all the exports on your Tenable Vulnerability Management account.

Activity Table

The **Activity** table contains the following information about your exports:

Column	Description
Name	The name of the export file.
Source	The data source for the export in Tenable Vulnerability Management. The possible sources are: • **Assets** – Information about all the assets on your Tenable Vulnerability Management license. • **Assets Host** –Information about assets Tenable Vulnerability Management identified on your host during a scan. • **Findings - Vulnerabilities - Host** – Information about the vulnerability findings Tenable Vulnerability Management identified on your host during a scan. • **Users** – Information about the users assigned to your account.
Type	The type of export, either manual or scheduled.
Format	The format of the export file, either CSV or JSON.
Status	The status of the export. The possible statuses are: • **Pending** – Tenable Vulnerability Management is initiating the export

	process. • **Running** – Tenable Vulnerability Management is preparing the requested file. • **Completed** – Tenable Vulnerability Management has successfully completed the export process. The export file is now available to download. • **Canceled** – Tenable Vulnerability Management canceled the export process. A **Canceled** status appears when a user stops a pending or running export. • **Failed** – The export process failed.
Reason	The reason the export attempt failed. By default, the **Reason** column is hidden. For information about how to add the column to the table, see Tables. A reason value appears only if the export status is **Failed**.
Size	The size of the export file. A size value appears only if the export status is **Completed**.
Creation Date	The date and time a user initiated the export.
Completion Date	The date and time when the export process completed.
File Name	The name of the CSV or JSON export file.
Expires On	The date and time the export expires. **Note:** The default export expiration is set in General Settings
Author	The user who initiated the export.
Actions	The actions you can perform with the export, including the following: • Download an export file.

	• Renew the expiration date for one or more exports. • Delete one or more export files. • Export your export activity.

On the **Export Activity** page, you can perform the following actions:

- Filter your Exports
- Renew an Export Expiration Date
- Stop an Export
- Download Export Activity
- Export your Export Activity
- Delete an Export

Note: Export expiration is set via the **Settings** section. For more information, see .

Filter your Exports

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Exports** page, you can filter the export data for your Tenable Vulnerability Management instance.

To filter your exports:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. (Optional) To filter your export activity data, click the **Activity** tab.

The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. In the upper-left corner, click the ▽ button.

   The filters plane expands. The plane displays a list of default filter options.

5. Click **Edit Filters**.

   A drop-down box appears listing all the filter options.

6. Select or deselect the filters you want to add or remove. For detailed list of available filters, see Export Filters.

7. Click outside the filter drop-down box.

   The drop-down box closes.

8. For each selected filter, in the first text box, select an operator.

9. In the second text box, select or type a value for the filter.

   Note: You can select up to five different values for each filter to apply to your exports.

   Note: If a filter you select has generic options, those options appear below the filter. If the filter requires a specific, unique value, you must type the value.

   Tip: When you type a value for your filter, you can use a wild card character (*****) to stand in for a section of text anywhere in the value. For example, if you want the filter to include all values that end in 1, type **1*. If you want the filter to include all values that begin with 1, *type 1**. If you want the filter to include all values with a 1 somewhere between the first and last characters, type **1**.

10. (Optional) To clear the value of a filter:

    a. Hover over the filter you want to clear.

       An interactive window appears over the filter.

    b. In the window, click **Clear** to remove the value provided in the filter box.

       Tenable Vulnerability Management clears the filter value.

11. (Optional) To remove a filter:

a. Hover over the filter you want to remove.

   An interactive window appears over the filter.

b. In the window, click **Remove** to remove the filter.

   Tenable Vulnerability Management removes the filter.

12. Click **Apply**.

    Tenable Vulnerability Management filters your export data.

Export Filters

On the **Exports** page, you can filter your export data using following filters:

Note: The available filters vary based on the type of data you want to export.

Filter	Export Data Type	Description
Name	scheduled exports, export activity	The name you assigned to the export in Tenable Vulnerability Management. This filter is selected by default.
Size	export activity	The size of the export file in bytes. This filter is selected by default.
Source	scheduled exports, export activity	The area of Tenable Vulnerability Management to which the export applies. This filter is selected by default.
Status	scheduled exports, export activity	The current status of the export. Possible options are: • **Pending** • **Running** • **Canceled** • **Failed**

		• **Completed** This filter is selected by default.
Author	export activity	The user who created the export.
Completion Date	export activity	The date on which Tenable Vulnerability Management completed the export. This filter applies only to exports with a **Completed** status.
Creation Date	scheduled exports, export activity	The date on which a user on your instance created the export.
Expires On	export activity	Indicates when the export file expires. The filter value can be a date, date range, or number of days until the export file expires.
File Name	export activity	The name of the export file.
Format	scheduled exports, export activity	The export file type. Possible options are: • CSV • JSON
Reason	export activity	The reason the export failed. This filter applies only to exports with a **Failed** status.
Next Run	scheduled exports	The date and time on which the next export is scheduled.
Last Run Start Date	scheduled exports	The date and time on which Tenable Vulnerability Management last initiated the export.
Last Run Completion Date	scheduled exports	The date and time on which Tenable Vulnerability Management last completed the export.
Created By	scheduled exports	The user who created the export.

Updated Date	scheduled exports	The date and time on which a user last updated the export.
Updated By	scheduled exports	The user who last updated the export.

Renew an Export Expiration Date

Required User Role: Administrator

On the **Exports** page, you can reset the expiration date for any export on your Tenable Vulnerability Management instance.

Note: You can reset the expiration date for only one export at a time.

Tip: You can also configure your default export expiration settings on the General Settings page.

To reset the expiration date for an export:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. Do one of the following:

   - In the exports table, right-click the row for the export for which you want to reset the expiration date.

     The action options appear next to your cursor.

- In the exports table, in the **Actions** column, click the ⋮ button in the row for the export for which you want to reset the expiration date.

  The action buttons appear in the row.

5. Click **Renew**.

   Tenable Vulnerability Management resets the expiration date of the export to the default expiration period you have configured in Settings>General Settings.

Stop an Export

Required User Role: Administrator

On the **Exports** page, you can stop one or more pending or running exports on your Tenable Vulnerability Management instance.

Note:You cannot stop an export that has already been completed, canceled, or failed.

To stop a pending or running export:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

5. Select the exports that you want to stop:

Stop Scope	Action
Selected exports	To stop selected exports:

	Tip: You can stop up to 10 exports simultaneously. a. In the exports table, select the check box for each export you want to stop. The action bar appears at the top of the table. b. In the action bar, click **Stop**.
A single export	To stop a single export: a. In the exports table, right-click the row for the export you want to stop. -or- In the exports table, in the **Actions** column, click the ⋮ button in the row for the export you want to stop. The action buttons appear in the row. b. Click **Stop**.

Download Export Activity

Required User Role: Administrator

On the **Exports** page, you can download an export file on your Tenable Vulnerability Management instance.

Note: You can download only one export file at a time.

Note:You can download the export file only if the export's status is **Completed**.

To download an export file:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

The **Exports** page appears. By default, the **Schedules** tab is active.

3. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

5. Do one of the following:

   - In the exports table, right-click the row for the export file you want to download.

     The action options appear next to your cursor.

   - In the exports table, in the **Actions** column, click the ⋮ button in the row for the export file you want to download.

     The action buttons appear in the row.

6. Click **Download**.

   Tenable Vulnerability Management downloads the export file to your computer.

Export your Export Activity

Required User Role: Administrator

On the **Exports** page, you can export data for the export activity on your Tenable Vulnerability Management instance.

To export your export activity data:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. Click the **Activity** tab.

The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

5. Select the exports that you want to export:

Export Scope	Action
Selected exports	To export selected exports: a. In the exports table, select the check box for each export you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 exports, select all the exports in the list and then click [→ **Export**.
A single export	To export a single export: a. In the exports table, right-click the row for the export you want to export. The action options appear next to your cursor. -or- In the exports table, in the **Actions** column, click the ⋮ button in the row for the export you want to export. The action buttons appear in the row. b. Click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  > **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

6. In the **Name** box, type a name for the export file.
7. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of exports. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of exports. Empty fields are not included in the JSON file.

8. In the **Configurations** section, select the fields you want to include in the export file by selecting the check box next to any field. Use the text box to search for a field.

   To view only the selected fields, click **View Selected**.

9. In the **Expiration** box, type the number of days before the export file expires.

   > **Note**: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

10. (Optional) To set a schedule for your export to repeat:

- Click the **Schedule** toggle.

  The **Schedule** section appears.

- In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
- In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
- In the **Repeat** drop-down box, select how often you want the export to repeat.
- In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

  > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

11. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

    - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

12. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

13. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Delete an Export

> **Required User Role:** Administrator

On the **Exports** page, you can delete one or more exports from your Tenable Vulnerability Management instance.

> **Note**:You can delete an export file only if the export's status is **Completed**, **Canceled**, or **Failed**.

To delete an export:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. (Optional) Refine the table data.

5. Select the exports that you want to delete:

Delete Scope	Action
Selected exports	To delete selected exports: **Tip**: You can delete up to 10 exports simultaneously. a. In the exports table, select the check box for each export you want to delete. The action bar appears at the top of the table. b. In the action bar, click **Delete**.
A single export	To delete a single export: a. In the exports table, right-click the row for the export you want to delete. -or- In the exports table, in the **Actions** column, click the ⋮ button in the row for the export you want to delete. The action buttons appear in the row. b. Click **Delete**.

Tenable Vulnerability Management removes the export from your account.

Remediation

Tracking all the items that need remediation can be a major effort. To facilitate the tracking of items to remediate, you can use the **Remediation** page to create two different methods to prioritize, distribute, and track vulnerability tasks in the environment.

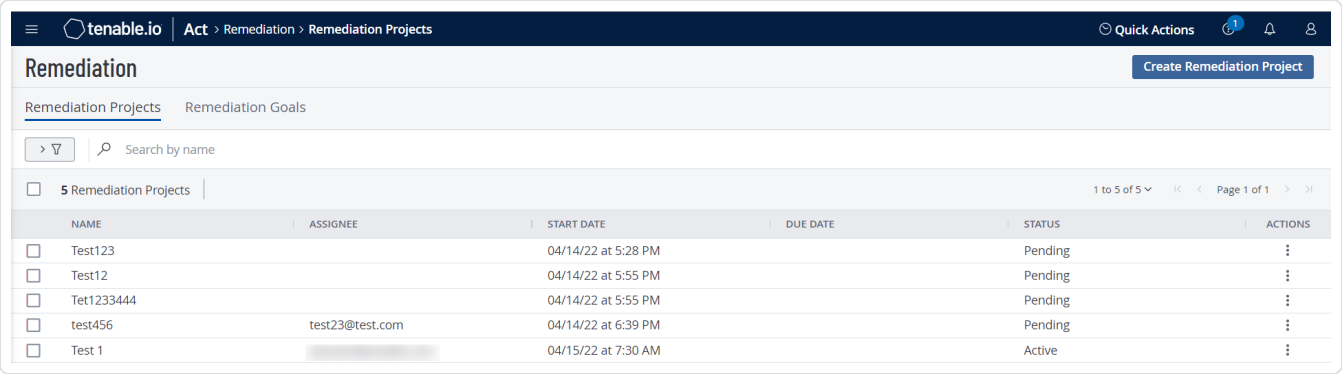
To access the Remediation page:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



View Remediations

Required Tenable Vulnerability Management User Role: Basic User, Scan Operator, Standard, Scan Manager, or Administrator

On the Remediation page, you can view your remediation projects or remediation goals.

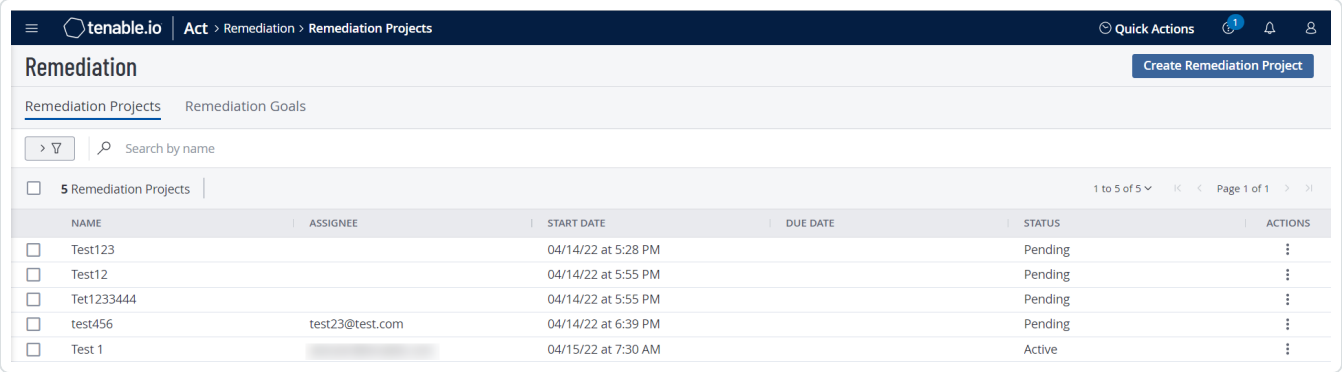
To view your remediation projects or goals:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Act** section, click **Remediation**.

The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Do one of the following:

   - View your remediation projects.

     The **Remediation Projects** tab is shown by default. The following table defines its columns:

Column	Description
Name	The name of the remediation project.
Assignee	The username of the user assigned to the remediation project.
Asset Tags	Asset tag(s) associated with the remediation project, which are added at project creation.
Start Date	The date and time on which the assigned user started the remediation project.
Due Date	The date and time on which the assigned user is expected to complete the remediation project.
Status	The status of the remediation project.
Actions	The actions you can take with the remediation project.

   - View your remediation goals.

To view your remediation goals, click the **Remediation Goals** tab. The following table defines its columns:

Column	Description
Name	The name of the remediation goal.
Type	Whether the goal is static or dynamic. The goal type depends on the due date option configured when you created the remediation goal.
Start Date	The date and time on which the remediation goal was started.
Due Date	The date and time on which the remediation goal must be complete.
Status	The status of the remediation goal.
Asset Tags	Asset tag(s) associated with the remediation project, which are added at project creation.
Actions	The actions you can take with the remediation goal.

4. (Optional) Refine your view with filters, as described in Remediation Filters.

Remediation Filters

Required Tenable Vulnerability Management User Role: Basic User, Scan Operator, Standard, Scan Manager, or Administrator

On the **Remediation** page, you can use filters to refine the remediation projects goals displayed.

Remediation Projects

The following table defines the Remediation Project filters:

Filter	Description
Asset Tags	Asset tag(s) associated with the project, which are added at project creation. Tenable Vulnerability Management only returns tags with a positive match, such as *Asset Tag is equal to Operating System: Windows*.
Assignees	The user(s) assigned to the remediation project.

Project Name	The name of the remediation project.
Project Status	The status of the remediation project.

Remediation Goals

The following table defines the Remediation Goals filters:

Filter	Description
Asset Tags	Asset tag(s) associated with the project, which are added at project creation. Tenable Vulnerability Management only returns tags with a positive match, such as *Asset Tag is equal to Operating System: Windows*.
Goal Name	The name of the remediation goal.
Goal Status	The status of the remediation goal.
Goal Type	Whether the goal is static or dynamic. The goal type depends on the due date option configured when you created the remediation goal.

Remediation Projects

A remediation project helps you organize and manage your remediation program. Remediation projects allow you to define the scope of work, prioritize your findings, assign projects to owners, and track the progress of your remediation tasks. The status of your remediation project lets you quickly visualize all your in-progress or closed remediation activities.

You can create the following types of remediation projects:

- **By fixed date** – A remediation project with a fixed scope that must be completed by the specified date.
- **Within number of days** – An open-scope or ongoing remediation project that must be completed within a specific period. This type of remediation project ensures that you always assign and track a certain type of critical vulnerability.

For more information, see Fixed-Scope and Ongoing Remediation Goals.

On the **Remediation Projects** page, you can perform the following tasks:

- Create a New Remediation Project
- Create a New Remediation Project From Findings
- View Remediation Project Details
- Activate a Remediation Project
- Edit a Remediation Project
- Suspend a Remediation Project
- Close a Remediation Project
- Export Remediation Projects
- Delete a Remediation Project

Create a New Remediation Project

Required Tenable Vulnerability Management User Role: Basic User, Scan Operator, Standard, Scan Manager, or Administrator

Note: You can also create a remediation project from **Explore** > **Findings**. For more information, see Create a remediation project from Findings.

You can create remediation projects to define the scope of work, prioritize your findings, assign projects to owners, and track the progress of your remediation tasks.

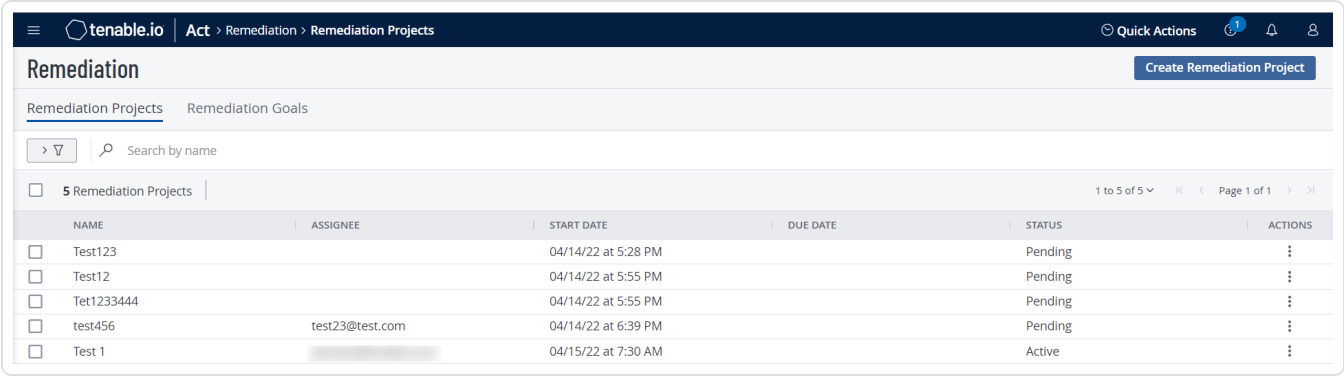
To create a new remediation project:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. In the upper-right corner, click **Create Remediation Project**.

   The **Create a Remediation Project** page appears.

   On the left side of the page, you can select from the following and click **Next** after each selection:

Option	Action
Name	• In the **Project Name** box, type a name for the project. • (Optional) In the **Description** box, type a description for the remediation project.
Scope	In the **Findings Filters** section, the following filters are selected by default. • **Risk Modified is not equal to Accepted** • **Severity: is not equal to Info** • **State: is not equal to Fixed** **Note**: When the **State: is not equal to Fixed** filter is applied, the progress bar shows 0%. To view the progress percentage of the remediation project, remove this filter. **Note**: You can select up to a maximum of five filters. You can modify the existing filters or add new filters to the list with **AND**

	and **OR** options. **Tip**: Tenable Vulnerability Management shows the findings count based on the filters in the **Scope**. For each filter you want to use to specify the project scope, do the following: 1. Under **Findings Filters**, click **Select Filters**. The **Select Filters** drop-down box appears. 2. Click the filter you want to apply. The filter appears in the **Finding Filters** box. 3. In the filter, click the v button. A list of filter value and operator options appears. 4. In the first drop-down box, select the operator you want to apply to the filter. 5. In the second drop-down box, select one or more values to apply to the filter. 6. Select **Match All** from the drop-down box. By default, Tenable Vulnerability Management sets the filter to **Match All**.
Assign	In the **Select Users or User Groups** drop-down box, select the users or groups to which you want to assign the remediation project.
Schedule	• In the **Start Date** box, select the date on which you want the assigned users and groups to be in the remediation project. • In the **Due Date** section, select one of the following: • **Within number of days** – The number of days within which the project must be complete.

	Note: For any remediation project with this option selected, the right-hand progress bar does not appear on the **Project Details** page. • **By fixed date** – The date by when you must complete the project. For more information, see Fixed-Scope and Ongoing Remediation Goals

4. Click **Save**.

   Tenable Vulnerability Management creates the remediation project.

   Note: Remediation projects do not automatically close even if all the tasks are complete or if the projects reach their due date. You have to close the project manually by changing the project status to **Closed** once it is complete.

Create a New Remediation Project From Findings

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

To create a new remediation project:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Explore** section, click **Findings**.

   The **Findings** page appears, showing a table that lists your findings. By default, the **Vulnerabilities** tab is active.

3. To create a remediation project, do one of the following:

   Note: The **Create Remediation Project** option is available when you have three or less than three selected filters. If you select more than three filters, Tenable Vulnerability Management does not show the **Create Remediation Project** option.

Create	Action
Remediation project for a single finding	a. Do one of the following: • Right-click the row of the finding for which you want to create the remediation project. The action options appear next to your cursor. • Select the check box for the finding for which you want to create the remediation project. In the action bar, Tenable Vulnerability Management enables **More** > ⊕ **Create Remediation Project**. • In the **Actions** column, click the ⋮ button in the row for which you want to create the remediation project. The action button appears in the row. b. Click **Create Remediation Project**.
Remediation project for multiple findings	a. Select the check box for the findings for which you want to create the remediation project. In the action bar, Tenable Vulnerability Management enables ⊕ **Create Remediation Project**. b. Click ⊕ **Create Remediation Project**.

4. The **Create a Remediation Project** page appears.

   On the left side of the page, you can select from the following and click **Next** after each selection:

Option	Action
Name	• In the **Project Name** box, type a name for the project.

	• (Optional) In the **Description** box, type a description for the remediation project.
Scope	In the **Findings Filters** section, the following filters are selected by default. You can modify the existing filters or add new filters to the list with **AND** and **OR** options. • **Asset ID: is equal to <asset ID>** • **Plugin ID: is equal to <plugin ID** • Filters selected on the **Findings** page **Tip**: Tenable Vulnerability Management shows the findings count based on the filters in the **Scope**. For each filter you want to use to specify the project scope, do the following: 1. Under **Findings Filters**, click **Select Filters**. The **Select Filters** drop-down box appears. 2. Click the filter you want to apply. The filter appears in the **Finding Filters** box. 3. In the filter, click the v button. A list of filter value and operator options appears. 4. In the first drop-down box, select the operator you want to apply to the filter. 5. In the second drop-down box, select one or more values to apply to the filter. 6. Select **Match All** from the drop-down box. By default, Tenable Vulnerability Management sets the filter to **Match All**.
Assign	In the **Select Users or User Groups** drop-down box, select the users or

	groups to which you want to assign the remediation project.

Schedule	• In the **Start Date** box, select the date on which you want the assigned users and groups to be in the remediation project.
	• In the **Due Date** section, select one of the following:
	  • **Within number of days** – The number of days within which the project must be complete.
	  • **By fixed date** – The date by when you must complete the project.

5. Click **Save**.

   Tenable Vulnerability Management creates the remediation project.

   Note: Remediation projects do not automatically close even if all the tasks are complete or if the projects reach their due date. You have to close the project manually by changing the project status to **Closed** once it is complete.

View Remediation Project Details

Required Tenable Vulnerability Management User Role: Basic User, Scan Operator, Standard, Scan Manager, or Administrator

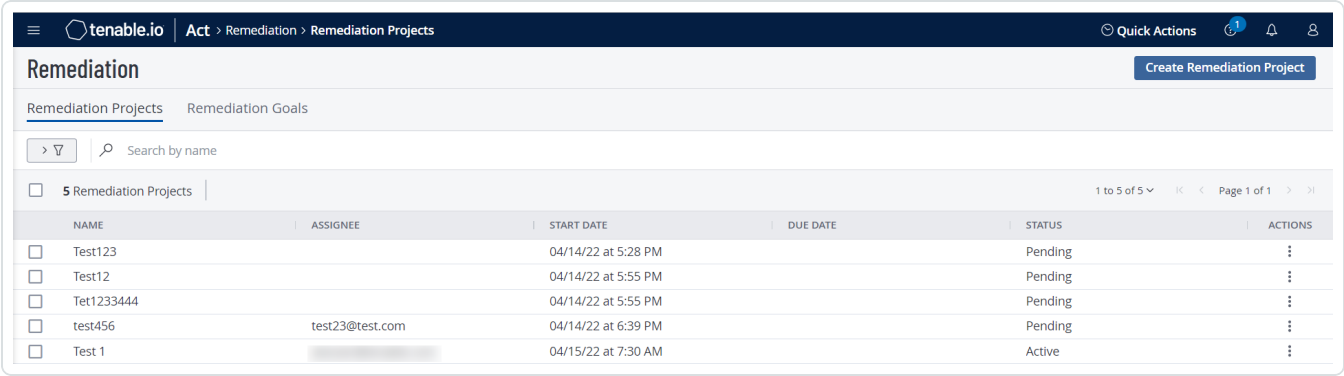
To view remediation project details:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.

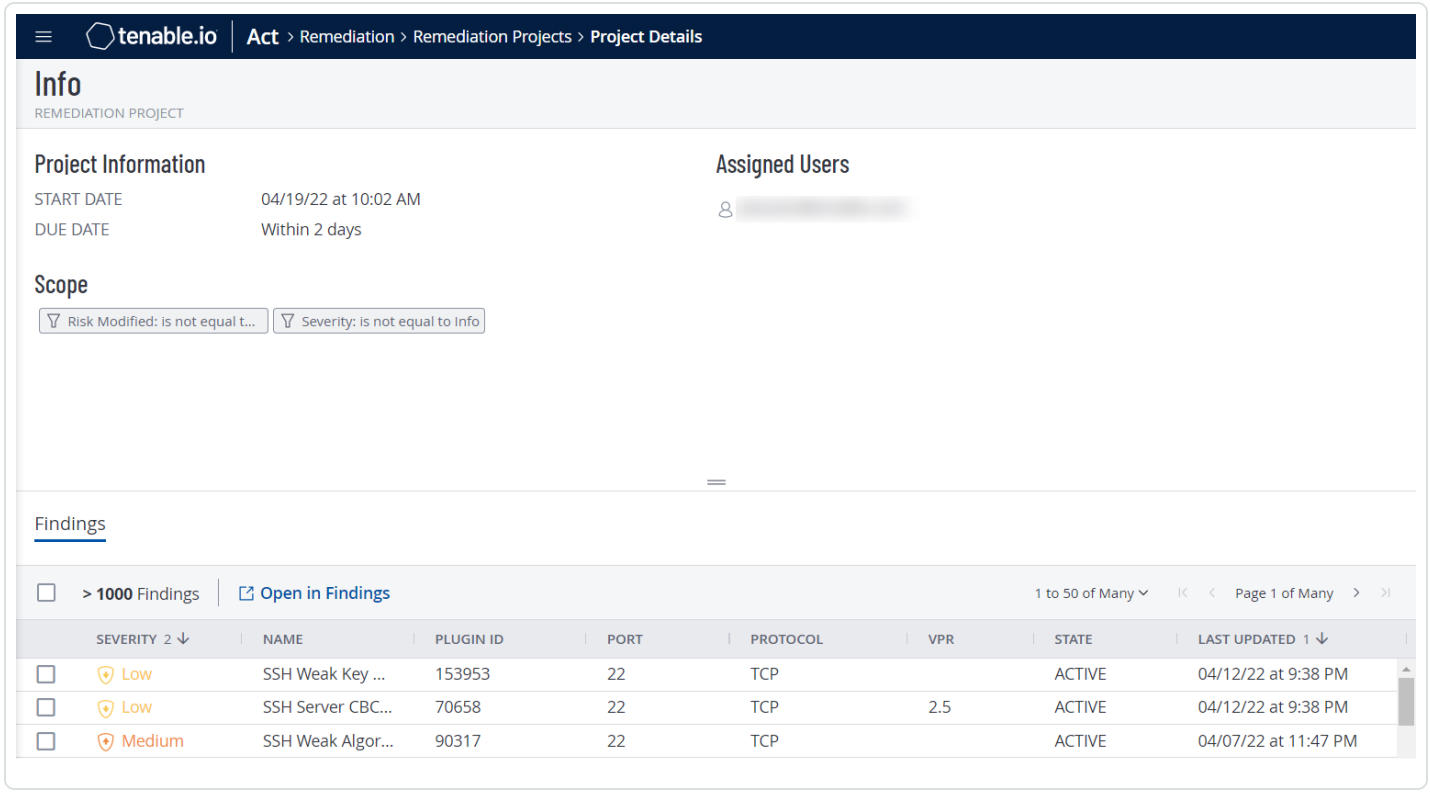


3. In the **Remediation Project** table, click the row for the remediation project whose details you want to view.

   The Remediation Project Details page appears.

Remediation Project Details

The **Project Details** page for remediations shows a high-level view of your remediation projects, details about the vulnerability findings specified in the remediation project configurations, and the current progress for each remediation project.



Note: Data on the **Project Details** page updates when you navigate away from or refresh the page.

Project Details

The **Project Details** page shows the following details about your remediation project:

Section	Description
Project Information	This section provides basic information about the remediation project including the **Start Date** and **Due Date** of the project.
Scope	This section shows the active filters applied to the remediation project. For more information, see Remediation Filters.
Assigned Users	A list of users assigned to the remediation project.
Findings	This section includes a table that lists all of your findings related to the remediation project. In this table, you can view the following information: • **Severity** – The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR. • **Name** – The name of the remediation finding. • **Plugin ID** – The ID of the plugin that identified the vulnerability. • **Port** – The port that the scanner used to connect to the asset where the scan detected the vulnerability. • **Protocol** – The protocol the scanner used to communicate with the asset where the scan detected the vulnerability. • **VPR** – The VPR Tenable calculated for the vulnerability. • **State** – The state of the vulnerability. • **Last Updated** – The date when a scan last found the vulnerability on an asset. • **Asset Name** – The name of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability

	Management. • **Actions** – In this column, click the ⋮ button to view a drop-down where you can: ◦ **Export** – Export to CSV or JSON, as described in Export from Explore Tables. In the Findings table you can also: • Refine the table data. • View your vulnerability details on the Findings page by clicking **Open in Findings**. • Export one or more findings: 1. Select the check box next to the Finding(s) you want to export. The action bar appears at the top of the table. 2. In the action bar, click [→ **Export**. For more information on configuring the export, see Export Remediation Projects.

Edit a Remediation Project

Required Tenable Vulnerability Management User Role: Basic User, Scan Operator, Standard, Scan Manager, or Administrator

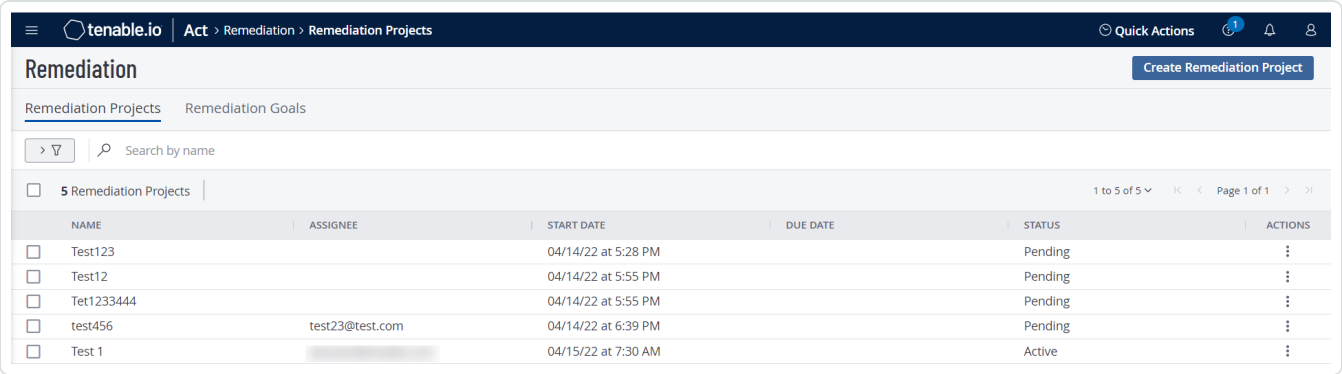
To edit a remediation project:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. To edit a remediation project:

    a. On the **Remediation Projects** page, do one of the following:

    - In the **Remediation Projects** table, right-click the row for the remediation project you want to edit.

      The action options appear next to your cursor.

    - In the **Remediation Projects** table, select the check box for the remediation project that you want to edit.

      The actions bar appears at the top of the table.

    - In the **Remediation Projects** table, in the **Actions** column, click the ⋮ button in the row for the project that you want to edit.

      The action button appears in the row.

4. Click **Edit**.

   The **Edit a Project** page appears.

5. Modify the remediation project settings.

6. Click **Save**.

   Tenable Vulnerability Management saves the remediation project and the **Remediation Projects** page appears.

Activate a Remediation Project

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

When you create a remediation project, it is in the **Pending** state. You must activate the project for it to start tracking the progress of the remediation project.

> **Note**: To activate a project, you must define the scope and assignee.

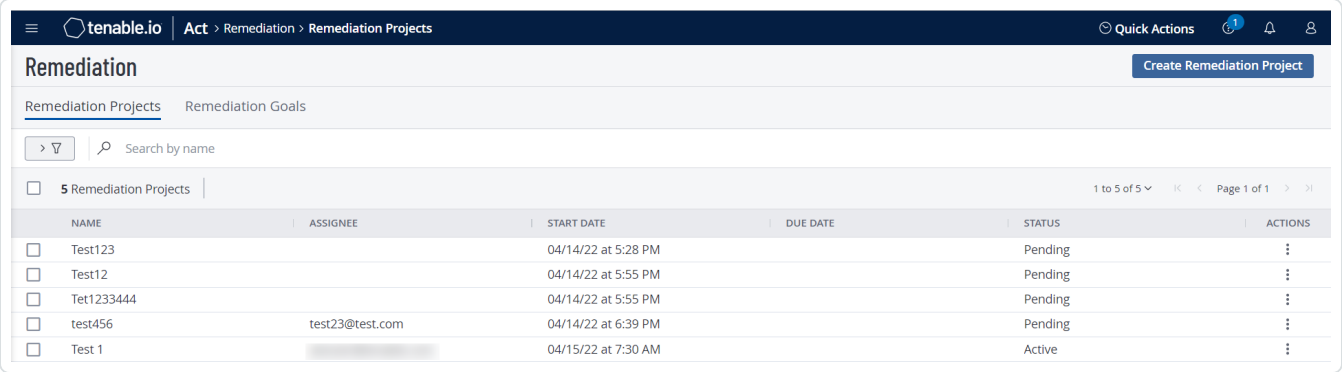
To activate a remediation project:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. In the **Remediation Projects** table, do one of the following:

   - In the **Remediation Projects** table, right-click the row for the remediation project you want to activate.

     The action options appear next to your cursor.

   - In the **Remediation Projects** table, select the check box for the remediation project that you want to activate.

     The actions bar appears at the top of the table.

   - In the **Remediation Projects** table, in the **Actions** column, click the ⋮ button in the row for the project that you want to activate.

     The action button appears in the row.

4. Click **Activate**.

Tenable Vulnerability Management activates the remediation project.

The **Remediation Projects** page appears and the **Status** column shows the project as **Active**.

Suspend a Remediation Project

Required Tenable Vulnerability Management User Role: Basic User, Scan Operator, Standard, Scan Manager, or Administrator

Suspending a remediation project temporarily stops the project from tracking the progress of the project. When you suspend a project, the status of the project remains the same until the project is activated.

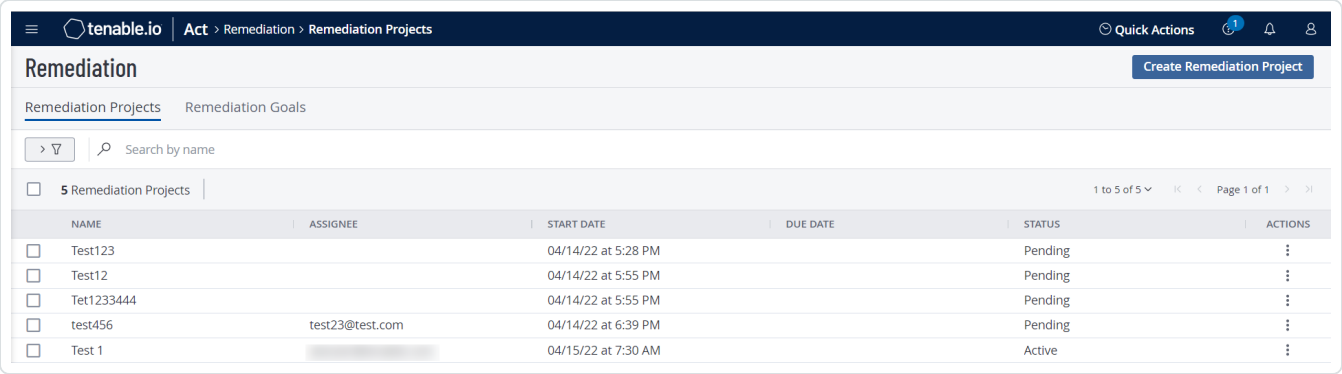
To suspend a remediation project:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Do one of the following:

   - In the **Remediation Projects** table, right-click the row for the remediation project you want to suspend.

     The action options appear next to your cursor.

- In the **Remediation Projects** table, select the check box for the remediation project that you want to suspend.

  In the action bar, Tenable Vulnerability Management enables **More** > **Suspend**.

- In the **Remediation Projects** table, in the **Actions** column, click the ⋮ button in the row for the project that you want to suspend.

  The action buttons appear in the row.

4. Click **Suspend**.

   Tenable Vulnerability Management suspends the remediation project.

   The **Remediation Projects** page appears and the **Status** column shows the project as **Suspended**.

Close a Remediation Project

> **Required Tenable Vulnerability Management User Role:** Basic User, Scan Operator, Standard, Scan Manager, or Administrator

A closed remediation project means that it has ended. But you can activate a closed project, if needed. Projects do not automatically close even if all the tasks are complete or if the projects reach their due date. You have to close the project manually by changing the project status to **Closed** once it is complete.

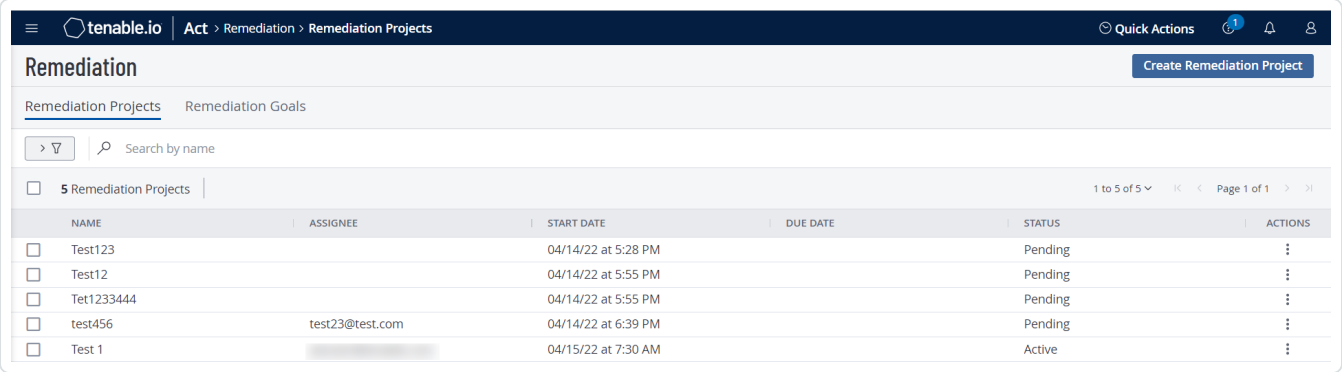
To close a remediation project:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Do one of the following:

   - In the **Remediation Projects** table, right-click the row for the remediation project you want to close.

     The action options appear next to your cursor.

   - In the **Remediation Projects** table, select the check box for the remediation project that you want to close.

     In the action bar, Tenable Vulnerability Management enables **More** > **Close**.

   - In the **Remediation Projects** table, in the **Actions** column, click the ⋮ button in the row for the project that you want to close.

     The action button appears in the row.

4. Click **Close**.

   Tenable Vulnerability Management closes the remediation project.

   The **Remediation Projects** page appears and the **Status** column shows the project as **Closed**.

Export Remediation Projects

On the **Remediation** page, you can export your remediation projects in CSV format.

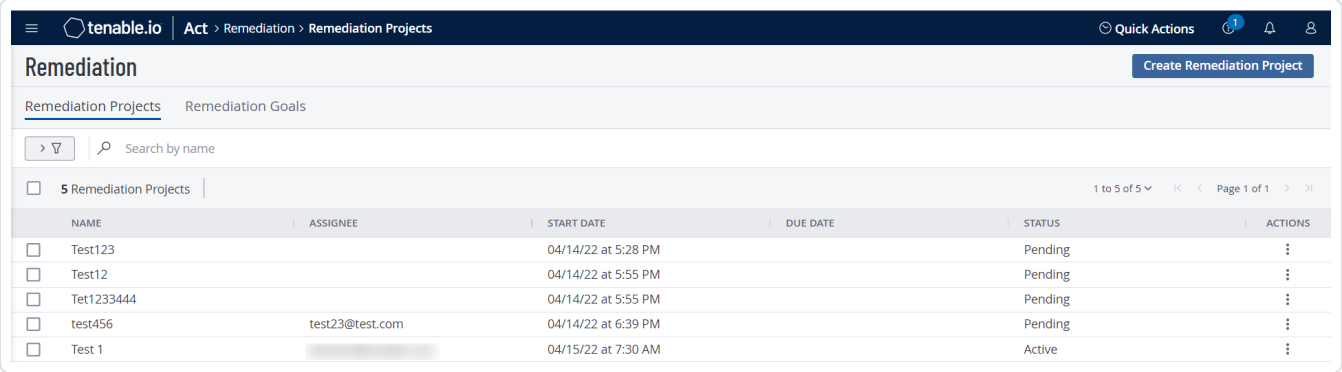
To export your remediation projects:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Act** section, click **Remediation**.

The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Do one of the following:

To export a single remediation project:

a. In the remediation projects table, right-click the row for the remediation project you want to export.

   The action options appear next to your cursor.

   -or-

   In the remediation projects table, in the **Actions** column, click the ⋮ button in the row for the remediation project you want to export.

   The action buttons appear in the row.

b. Click **Export**.

To export multiple remediation projects:

a. In the remediation projects table, select the check box for each remediation project you want to export.

   The action bar appears at the top of the table.

b. In the action bar, click [→ **Export**.

> **Note**: You can individually select and export up to 200 remediation projects. If you want to export more than 200 remediation projects, you must select all the remediation projects on

> our Tenable Vulnerability Management instance by selecting the check box at the top of the **Projects** table and then click [→ **Export**.

The **Export** plane appears.

4. In the **Name** box, type a name for the export file.
5. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of tag categories or values. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of tag categories or values. Tenable Vulnerability Management does not include empty fields in the JSON file.

6. (Optional) Deselect any fields you do not want to appear in the export file.
7. In the **Expiration** box, type the number of days before the export file ages out.

> **Note**: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

8. (Optional) To set a schedule for your export to repeat:
   - Click the **Schedule** toggle.

     The **Schedule** section appears.
   - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
   - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.

- In the **Repeat** drop-down box, select how often you want the export to repeat.
- In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

  > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

9. (Optional) To send email notifications on completion of the export:

   > **Note**: You can enable email notifications with or without scheduling exports.

   - Click the **Email Notification** toggle.

     The **Email Notification** section appears.
   - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
   - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

     > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

10. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

11. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Delete a Remediation Project

> **Required Tenable Vulnerability Management User Role:** Basic User, Scan Operator, Standard, Scan Manager, or Administrator

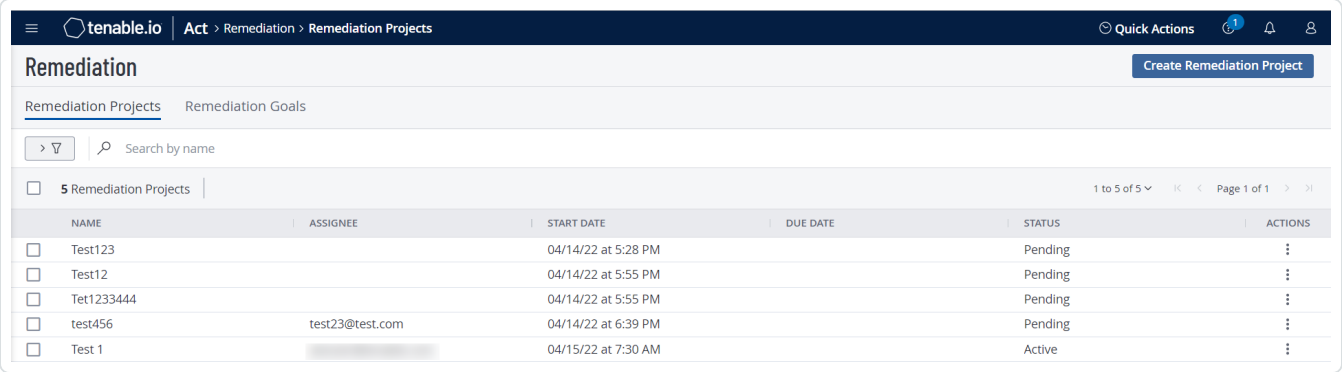
To delete a remediation project:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. To delete one or more remediation projects:

Delete	Action
A single remediation project	a. To delete a single remediation project: • In the **Remediation Projects** table, in the **Actions** column, click the ⋮ button in the row for the project that you want to delete. The action buttons appear in the row. • In the **Remediation Projects** table, select the check box next to the remediation project that you want to delete. In the action bar, Tenable Vulnerability Management enables **More** > **Delete**. • In the **Remediation Projects** table, right-click the row for the project that you want to delete. The action options appear next to your cursor. b. Click **Delete**.
Delete multiple remediation projects	a. In the **Remediation Projects** table, select more than one remediation projects that you want to delete. Tenable Vulnerability Management enables the **Delete** button in the action bar. b. Click **Delete**.

Tenable Vulnerability Management deletes the selected remediation projects.

Remediation Goals

A remediation goal allows you to measure the effectiveness of your remediation program. By setting a remediation goal, you can track whether your remediation projects are aptly tracking and closing critical findings within a specific period.

You can create the following types of remediation goals:

- **By fixed date** – A remediation goal that must be met by the specified date. Otherwise, the goal fails.
- **Within the number of days** – A remediation goal that must be met within a specific number of days. Tenable Vulnerability Management classifies this type of goal as a dynamic goal or a continuous goal.
- **Ongoing** – A continuous or dynamic goal that remains open until all findings of a specific scope are fixed.

On the **Remediation Goals** page, you can perform the following tasks:

- Create a New Remediation Goal
- View Remediation Goal Details
- Activate a Remediation Goal
- Edit a Remediation Goal
- Suspend a Remediation Goal
- Close a Remediation Goal
- Export Remediation Goals
- Delete a Remediation Goal

Fixed-Scope and Ongoing Remediation Goals

> **Required Tenable Vulnerability Management User Role:**Basic User, Scan Operator, Standard, Scan Manager, or Administrator

When creating a remediation goal, you can set the scope to be fixed or ongoing.

Fixed-scope goals – Applies to scenarios where a group of vulnerabilities or even just one vulnerability needs remediation in a certain period of time.

Ongoing (open-scope) goals – Applies to a scenario where you have to ensure that there is always an assigned owner to track a certain type of vulnerability, such as assigning all critical Tenable PCI ASV vulnerabilities needing remediation to owners.

To create remediation goals, see Create a New Remediation Goal.

Create a New Remediation Goal

Required Tenable Vulnerability Management User Role: Basic User, Scan Operator, Standard, Scan Manager, or Administrator

Remediation goals can be static or dynamic. Static remediation goals have a fixed due date, whereas dynamic goals do not have a fixed due date, but you must meet the goal within a specified time period or must be in an ongoing state.

For example, configure a dynamic remediation goal to ensure that Log4J findings must not exist in the system. You can configure this remediation goal as **Ongoing** and if the count of Log4J findings becomes greater than zero, then the goal fails.

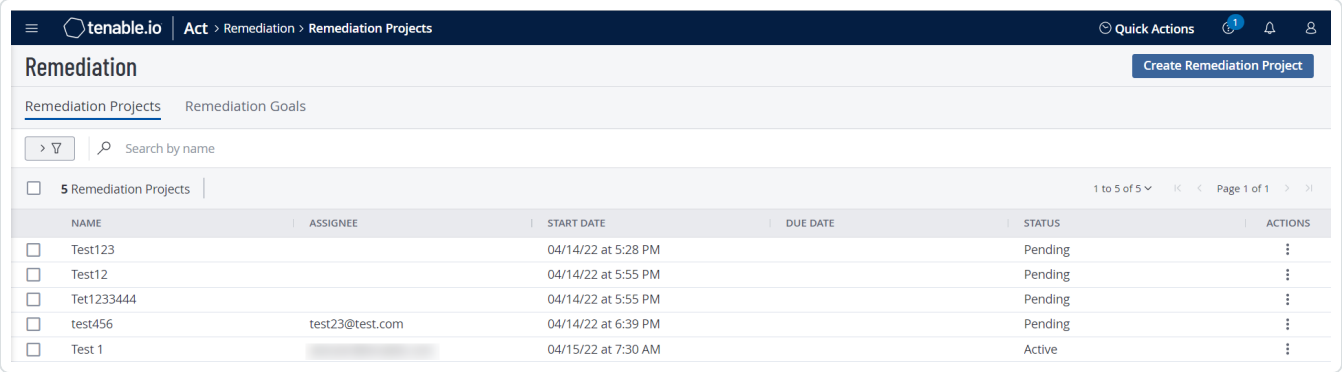
To create a new remediation goal:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

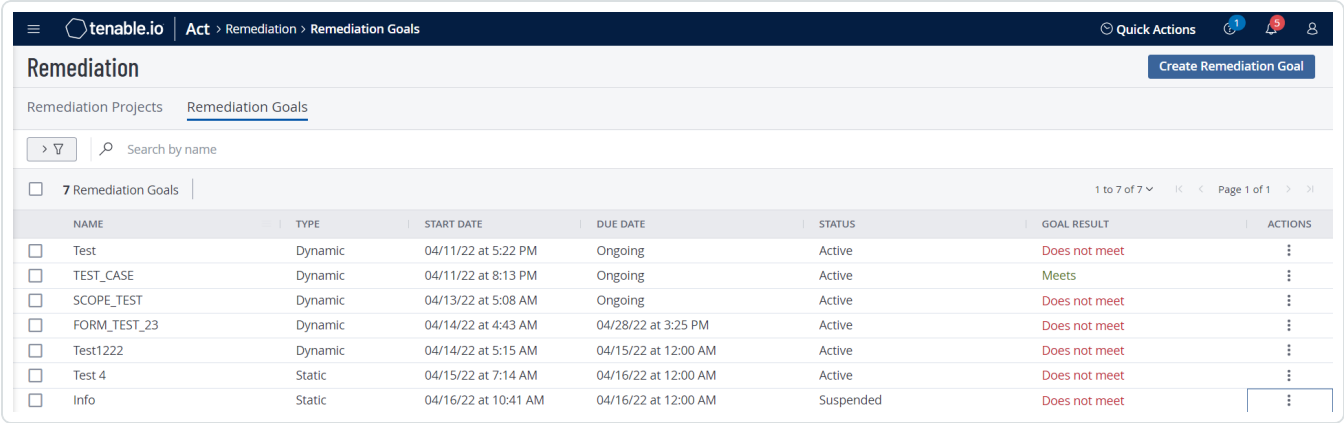
2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Click the **Remediation Goals** tab.

   The **Remediation Goals** page appears.



4. In the upper-right corner, click **Create Remediation Goal**.

   The **Create a Remediation Goal** page appears.

   On the left side of the page, you can select from the following and click **Next** after each selection:

Option	Actions
Name	• In the **Goal Name** box, type a name for the remediation goal. • In the **Description** box, type a description for the remediation goal.
Conditions	In the **Findings Filters** section, the following filters are selected by default. • **Severity is not equal to Info** • **State is not equal to Fixed** **Note**: You can select up to a maximum of five filters. You can modify the existing filters or add new filters to the list with **AND** and **OR** options. **Tip**: Tenable Vulnerability Management shows the findings count based on the filters in the **Scope**.

	1. Under **Findings Filters**, click **Select Filters**. The **Select Filters** drop-down box appears. 2. Click the filter you want to apply. The filter appears in the **Finding Filters** box. 3. In the filter, click the ⌄ button. A list of filter value and operator options appears. 4. In the first drop-down box, select the operator you want to apply to the filter. 5. In the second drop-down box, select one or more values to apply to the filter. 6. Select **Match All** from the drop-down box. By default, Tenable Vulnerability Management sets the filter to **Match All**.
Goal Due Date	Select and configure one of the following options: **Note**: Tenable Vulnerability Management determines the remediation goal type based on the due date option you configure. If you configure options for **Within number of days** or **Ongoing**,Tenable Vulnerability Management creates the goal as a dynamic goal. If you select **By fixed date**, Tenable Vulnerability Management creates the goal as a static type. • **Within number of days** – The number of days within which the goal must be complete. • **By fixed date** – The date by when you must complete the goal. • **Ongoing** – An ongoing goal is a remediation goal always in progress and must always be met. This option is selected by default. For more information, see Fixed-Scope and Ongoing Remediation Goals.

5. Click **Save**.

Tenable Vulnerability Management saves the remediation goal.

View Remediation Goal Details

Required Tenable Vulnerability Management User Role: Basic User, Scan Operator, Standard, Scan Manager, or Administrator

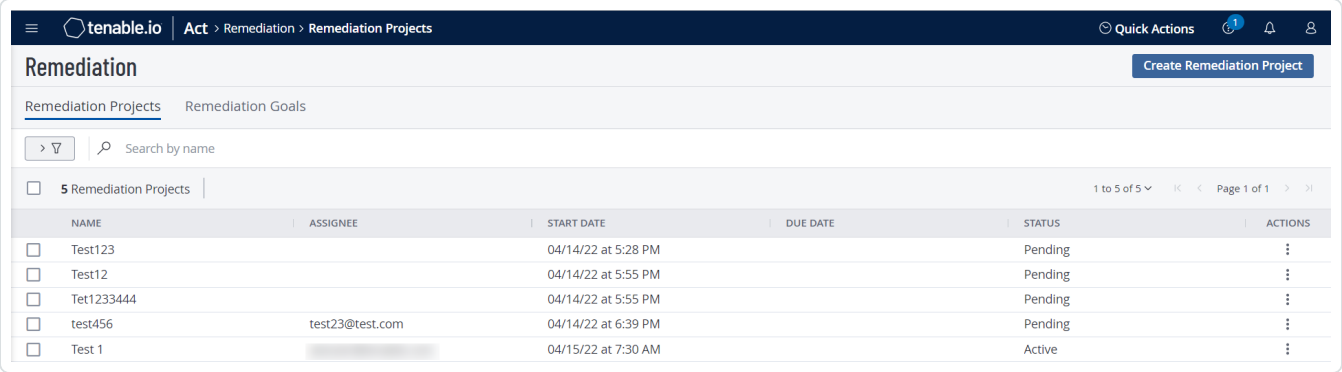
To view remediation goal details:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

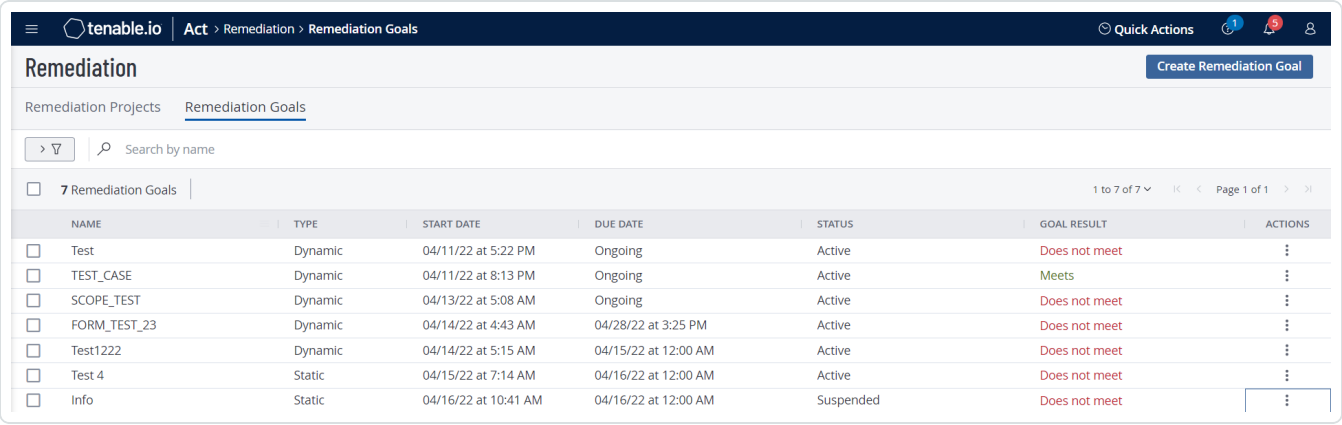
2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Click the **Remediation Goals** tab.

   The **Remediation Goals** page appears.



4. In the **Remediation Goals** table, click any row for which you want to view the details.

   The **Goal Details** page appears.

The **Goal Details** page shows the following details about your remediation goal:

Section	Description
Goal Information	The type, start date, and due date of the remediation goal.
Measure of Success	The filters assigned for findings. If the number of instances that match the filter is zero, it indicates that the remediation goal is a success.
Findings	• Refine the table data. • Export your host vulnerability findings. • View your vulnerability details on the Findings page by clicking **Open in Findings**.
Progress	The overall progress of the remediation goal. You can view the following information in this section: **Note**: These parameters are applicable only for goals that have a fixed due date (Static goals). For dynamic remediation goals, Tenable Vulnerability Management does not show the progress bar. • **Created on** – The date and time on which the remediation goal is created. • **Remediated** – The number of remediated findings. • **Resurfaced** – The number of findings that have reappeared after remediation.

Edit a Remediation Goal

Required Tenable Vulnerability Management User Role: Basic User, Scan Operator, Standard, Scan Manager, or Administrator

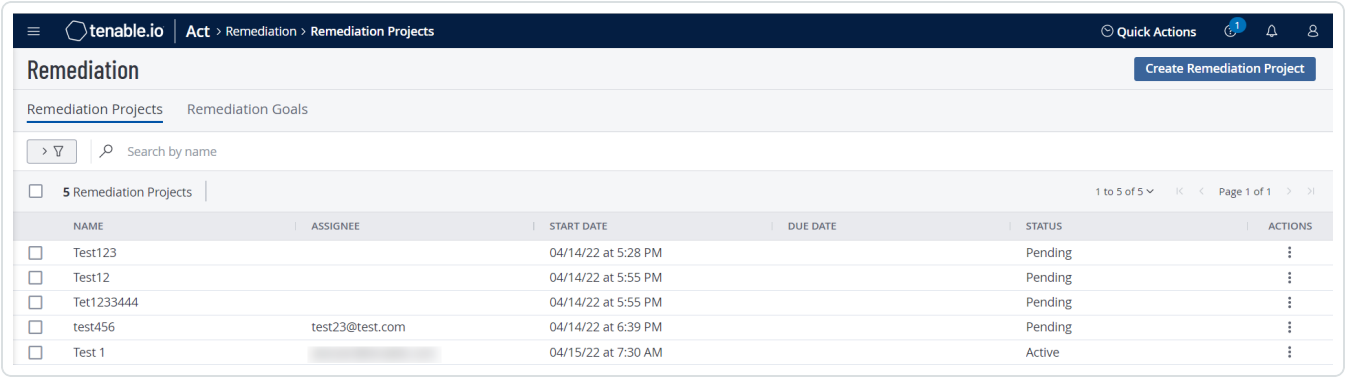
To edit a remediation goal:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

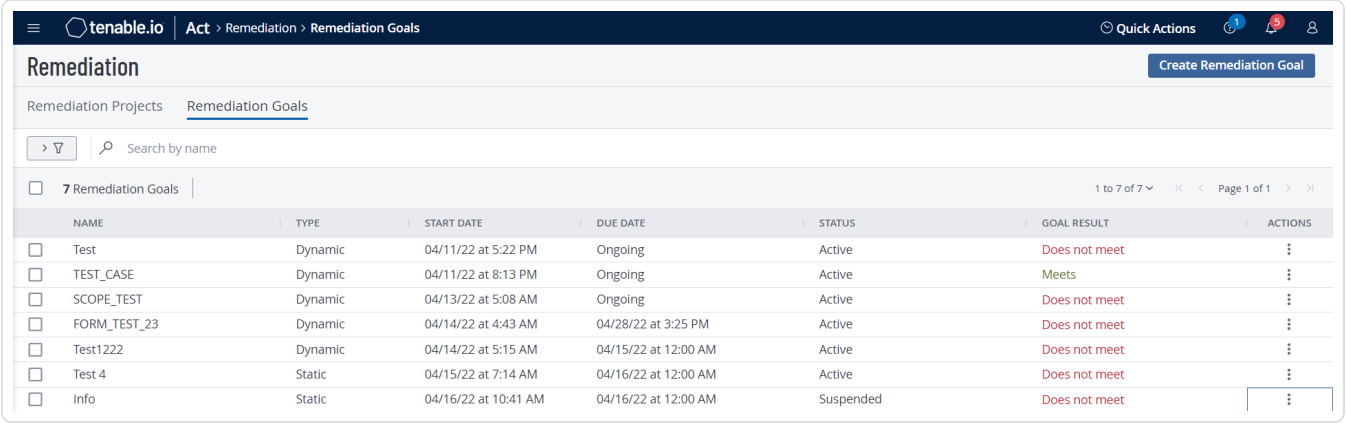
2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Click the **Remediation Goals** tab.

   The **Remediation Goals** page appears.



4. Do one of the following:

   - In the **Remediation Goals** table, right-click the row for the remediation goal you want to edit.

     The action options appear next to your cursor.

- In the **Remediation Goals** table, select the check box for the remediation goal you want to edit.

  The action bar appears at the top of the table.

- In the **Remediation Goals** table, in the **Actions** column, click the ⋮ button in the row for the goal you want to edit.

  The action button appears in the row.

5. Click **Edit**.

   The **Edit a Goal** page appears.

6. Modify the remediation goal settings.
7. Click **Save**.

   Tenable Vulnerability Management saves the remediation goal.

   The **Remediation Goals** page appears.

Activate a Remediation Goal

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

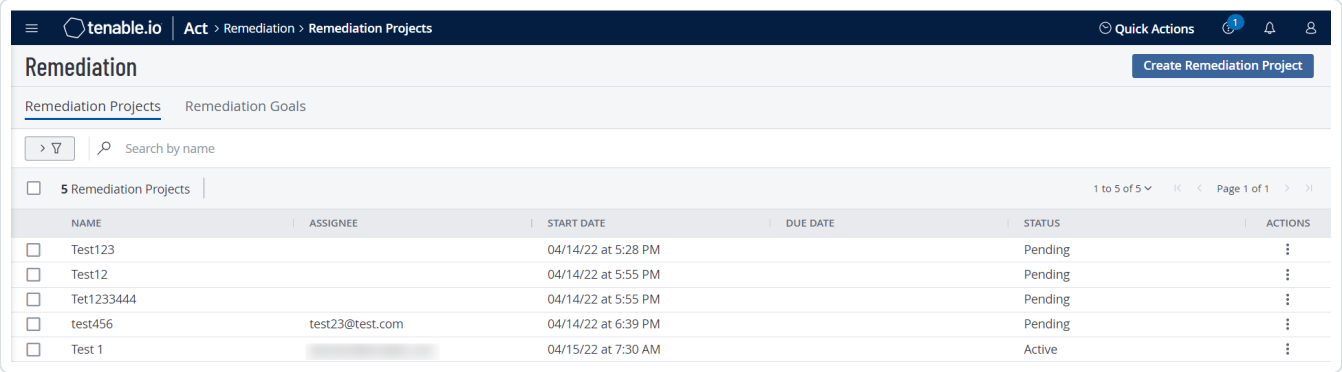
To activate a remediation goal:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

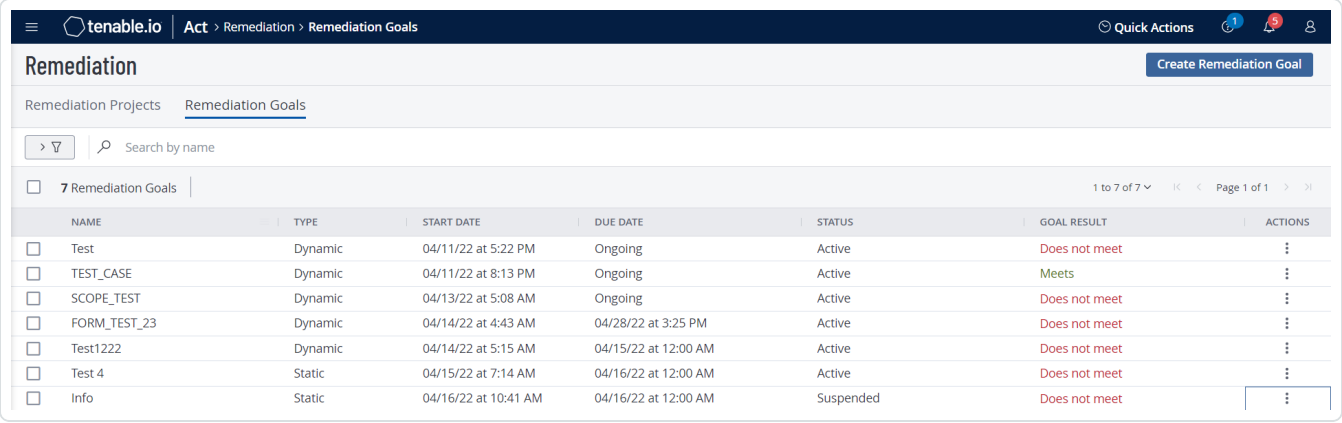
2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Click the **Remediation Goals** tab.

   The **Remediation Goals** page appears.



4. Do one of the following:

   - In the **Remediation Goals** table, right-click the row for the remediation goal you want to activate.

     The action options appear next to your cursor.

   - In the **Remediation Goals** table, select the check box for the remediation goal you want to activate.

     The action bar appears at the top of the table.

   - In the **Remediation Goals** table, in the **Actions** column, click the ⋮ button in the row for the goal you want to activate.

     The action button appears in the row.

5. Click **Activate**.

Tenable Vulnerability Management activates the remediation goal.

The **Remediation Goals** page appears and the **Status** column shows the project as **Active**.

Suspend a Remediation Goal

Required Tenable Vulnerability Management User Role: Basic User, Scan Operator, Standard, Scan Manager, or Administrator

You can temporarily suspend a goal and reactivate it any point of time.

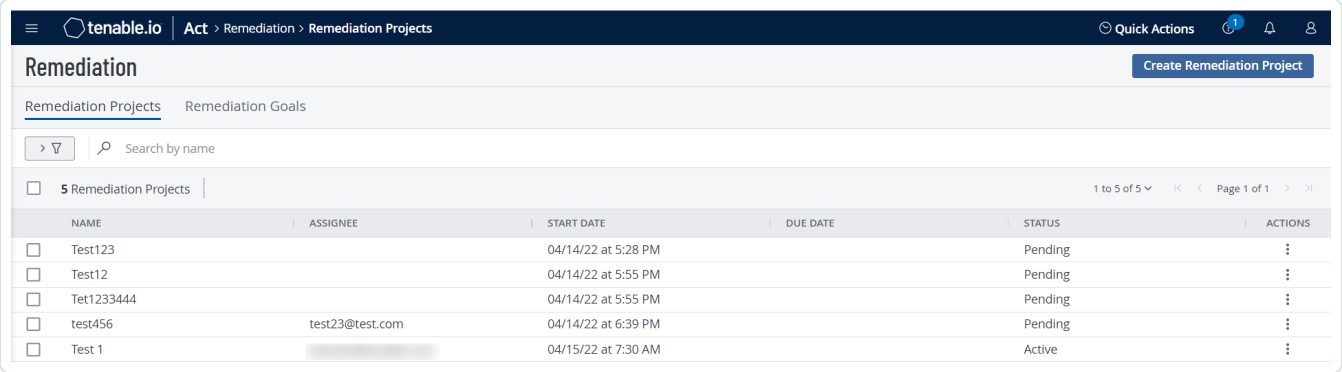
To suspend a remediation goal:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

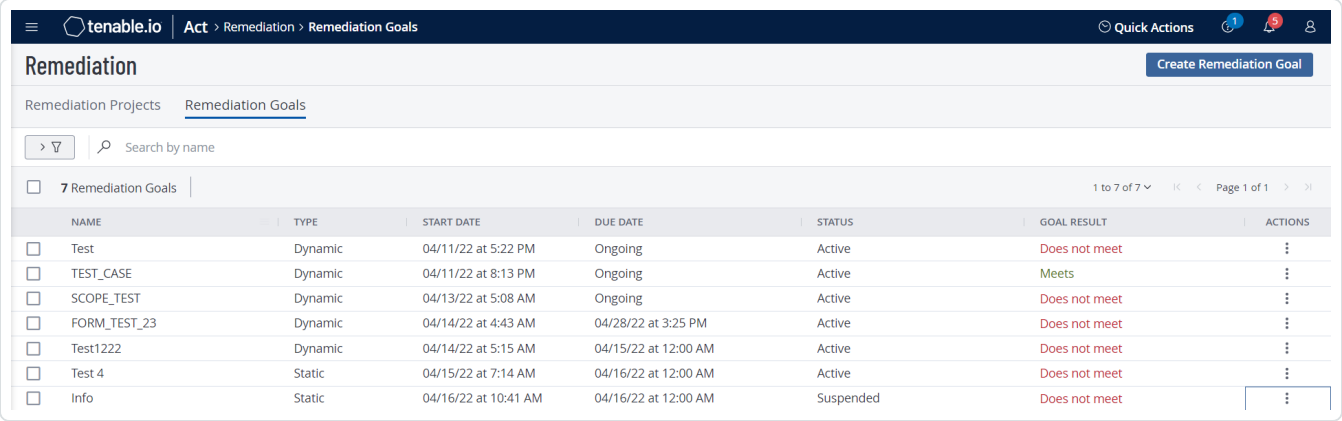
2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Click the **Remediation Goals** tab.

   The **Remediation Goals** page appears.



4. Do one of the following:

   - In the **Remediation Goals** table, right-click the row for the remediation goal you want to suspend.

     The action options appear next to your cursor.

   - In the **Remediation Goals** table, select the check box for the remediation goal you want to suspend.

     In the action bar, Tenable Vulnerability Management enables **More** > **Suspend**.

   - In the **Remediation Goals** table, in the **Actions** column, click the ⋮ button in the row for the goal you want to suspend.

     The action button appears in the row.

5. Click **Suspend**.

   Tenable Vulnerability Management suspends the remediation goal.

   The **Remediation Goals** page appears and the **Status** column shows the goal as **Suspended**.

Close a Remediation Goal

> **Required Tenable Vulnerability Management User Role:** Basic User, Scan Operator, Standard, Scan Manager, or Administrator

A closed remediation goal means that it has ended. But you can activate a closed goal, if needed.

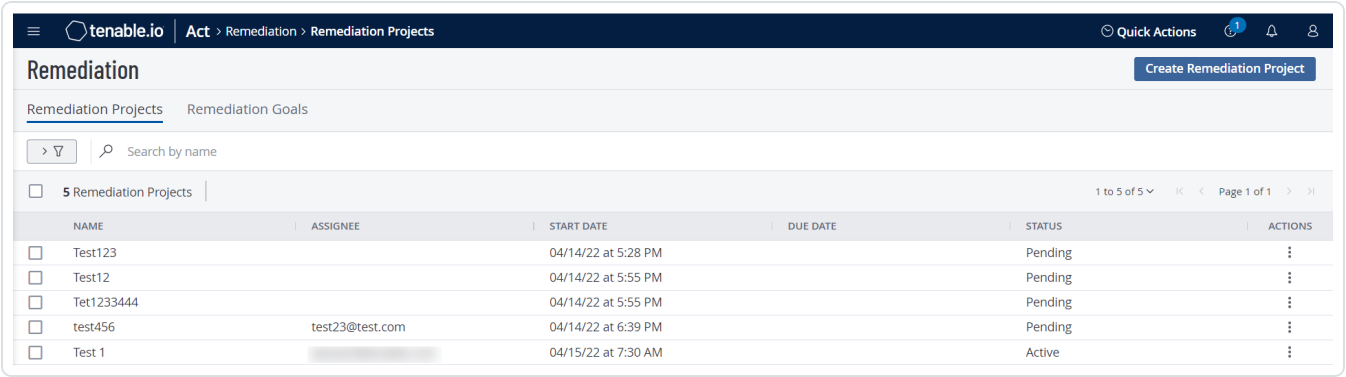
To close a remediation goal:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

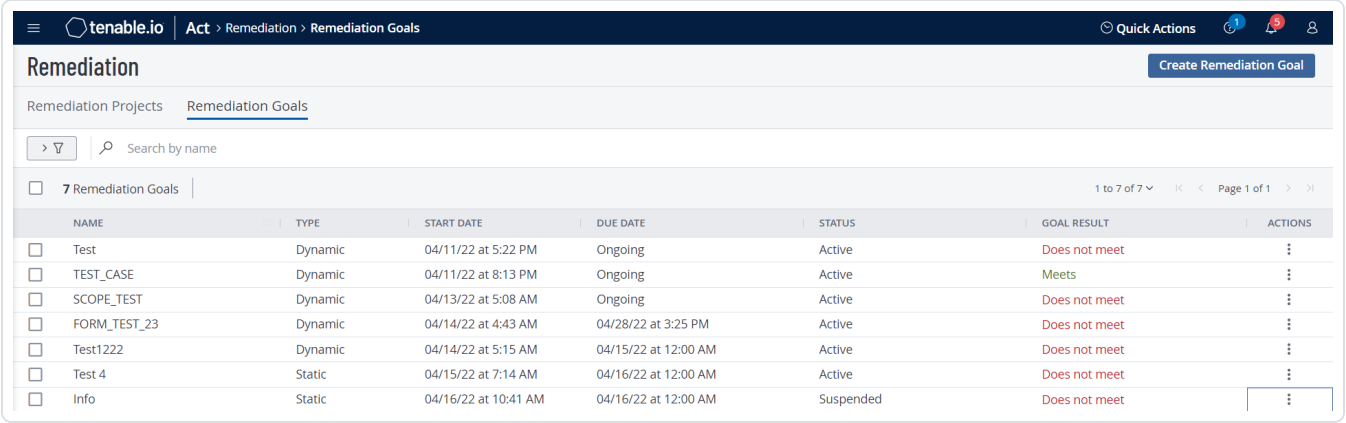
2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Click the **Remediation Goals** tab.

   The **Remediation Goals** page appears.



4. Do one of the following:

   - In the **Remediation Goals** table, right-click the row for the remediation goal you want to close.

     The action options appear next to your cursor.

- In the **Remediation Goals** table, select the check box for the remediation goal you want to close.

  In the action bar, Tenable Vulnerability Management enables **More** > **Close**.

- In the **Remediation Goals** table, in the **Actions** column, click the ⋮ button in the row for the goal you want to close.

  The action button appears in the row.

5. Click **Close**.

   Tenable Vulnerability Management closes the remediation goal.

   The **Remediation Goals** page appears and the **Status** column shows the project as **Closed**.

Export Remediation Goals

On the **Remediation** page, you can export your remediation goals in CSV format.

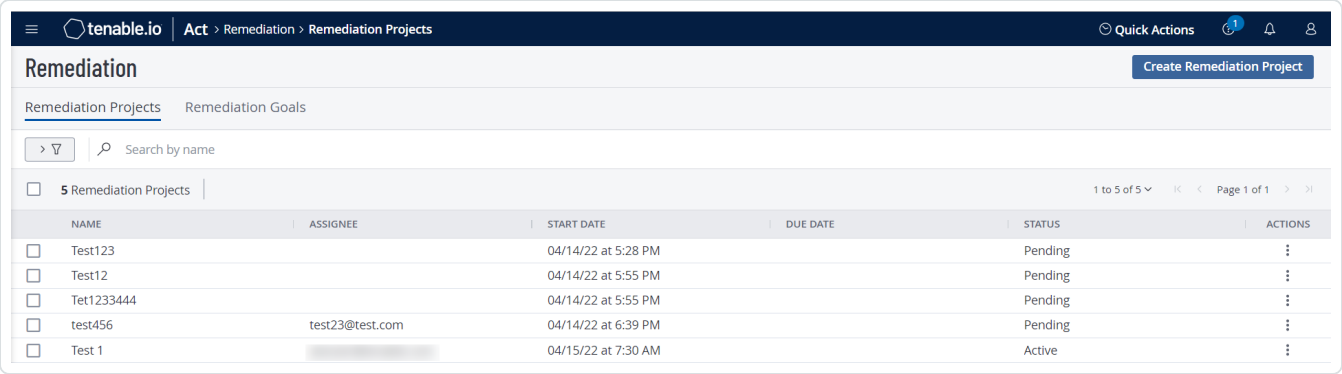
To export your remediation goals:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

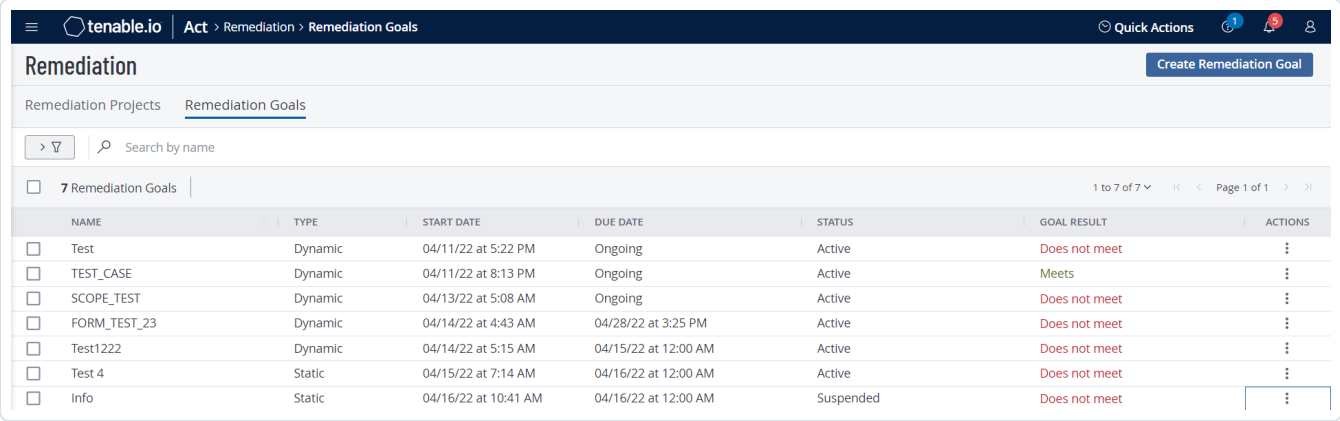
2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Click the **Remediation Goals** tab.

   The **Remediation Goals** page appears.



4. Do one of the following:

To export a single remediation goal:

a. In the remediation goals table, right-click the row for the remediation goal you want to export.

   The action options appear next to your cursor.

   -or-

   In the remediation goals table, in the **Actions** column, click the ⋮ button in the row for the remediation goal you want to export.

   The action buttons appear in the row.

b. Click **Export**.

To export multiple remediation goals:

a. In the remediation goals table, select the check box for each remediation goal you want to export.

   The action bar appears at the top of the table.

b. In the action bar, click [→ **Export**.

> **Note**: You can individually select and export up to 200 remediation goals. If you want to export more than 200 remediation goals, you must select all the remediation goals on your Tenable Vulnerability Management instance by selecting the check box at the top of the **Goals** table and then click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  > **Note**: By default, Tenable Vulnerability Management selects all fields.

- A text box to set the number of days before the export age outs.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

5. In the **Name** box, type a name for the export file.
6. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of tag categories or values. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.

7. (Optional) Deselect any fields you do not want to appear in the export file.
8. In the **Expiration** box, type the number of days before the export file age outs.

   > **Note**: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

9. (Optional) To set a schedule for your export to repeat:

   - Click the **Schedule** toggle.

     The **Schedule** section appears.

- In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
- In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
- In the **Repeat** drop-down box, select how often you want the export to repeat.
- In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

  Note: If you select never, the schedule repeats until you modify or delete the export schedule.

10. (Optional) To send email notifications on completion of the export:

    Note: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.
    - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      Note: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

11. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

12. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Delete a Remediation Goal

Required Tenable Vulnerability Management User Role: Basic User, Scan Operator, Standard, Scan Manager, or Administrator

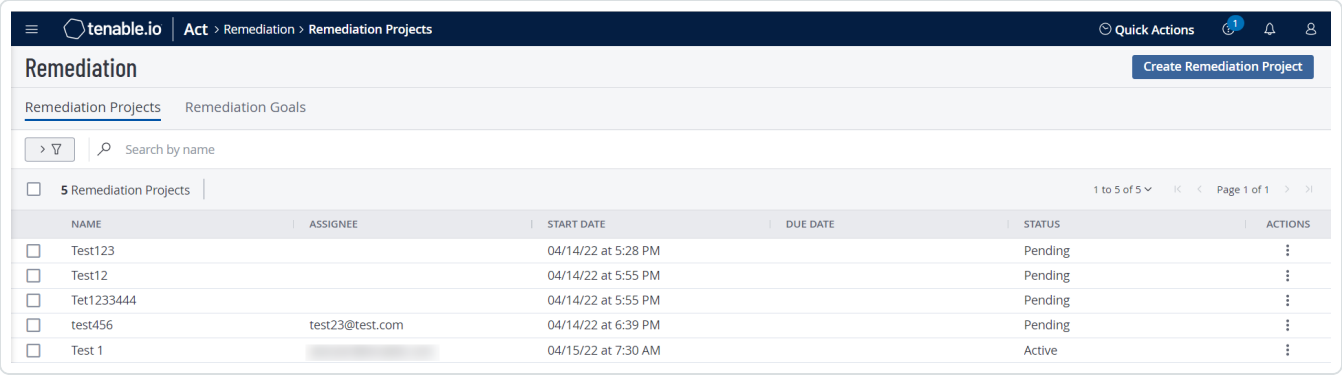
To delete a remediation goal:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

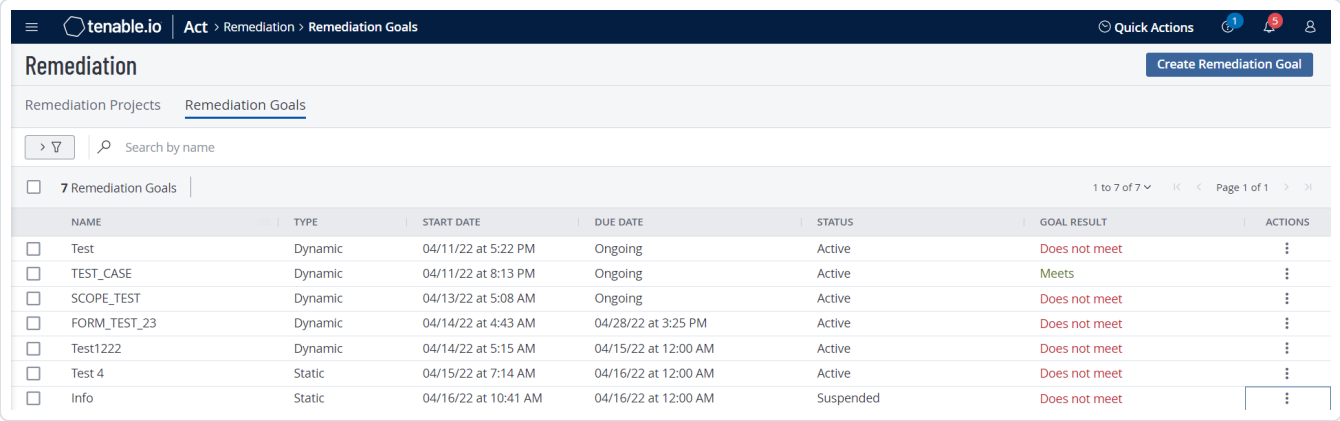
2. In the left navigation plane, in the **Act** section, click **Remediation**.

   The **Remediation** page appears. By default, the **Remediation Projects** tab is active.



3. Click the **Remediation Goals** tab.

   The **Remediation Goals** page appears.



4. To delete one or more remediation goals:

Delete	Action
A single remediation goal	a. Do one of the following: • In the remediation goals table, in the **Actions** column, click the ⋮ button in the row for the goal you want to delete. The action buttons appear in the row. • In the remediation goals table, select the check box next to the remediation goal that you want to delete. In the action bar, Tenable Vulnerability Management enables **More** > **Delete**. • In the remediation goals table, right-click the row for the goal you want to delete. The action options appear next to your cursor. b. Click **Delete**.
Multiple remediation goals	a. In the **Remediation Goals** table, select more than one remediation goals that you want to delete. Tenable Vulnerability Management enables the **Delete** button in the action bar. b. Click **Delete**.

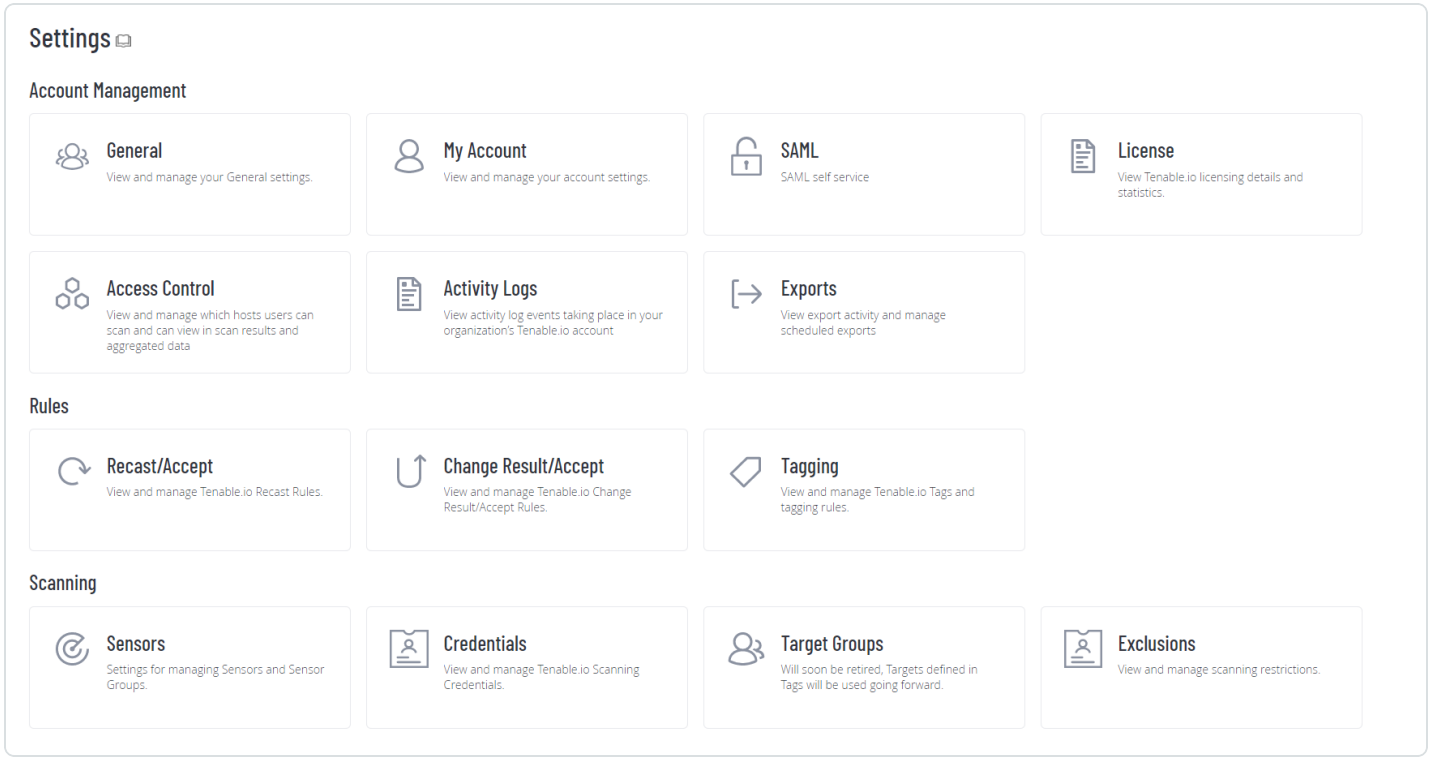
Tenable Vulnerability Management deletes the selected remediation goals.

Settings

On the **Settings** page, you can manage settings that affect your Tenable Vulnerability Management experience across a range of categories.

For example, in **My Account**, you can enable two-factor authentication or change your organization's user groups and permissions. In **Tags**, you can view and edit Tenable Vulnerability Management tags and tagging rules. Finally, in **Cloud Connectors**, you can manage the third-party data connectors that integrate Tenable Vulnerability Management with other platforms.

Note: Your user role and associated privileges determine the tiles that appear on the **Settings** page. For more information, see Roles.



This section contains complete documentation for the **Settings** page and is organized to match the Tenable Vulnerability Management interface. It contains the following topics:

- General Settings
- SAML
- License Information
- Access Control

- Activity Logs
- Access Groups
- Language
- Exports
- Recast Rules
- Tags
- Sensors
- Restart the agents
- Rebuild or reset the agent plugins
- Upgrade or downgrade the agent version
- Credentials
- Exclusions
- Connectors

General Settings

> **Required User Role:** Administrator

On the **General** page, you can configure general settings for your Tenable Vulnerability Management instance.

To access general settings:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

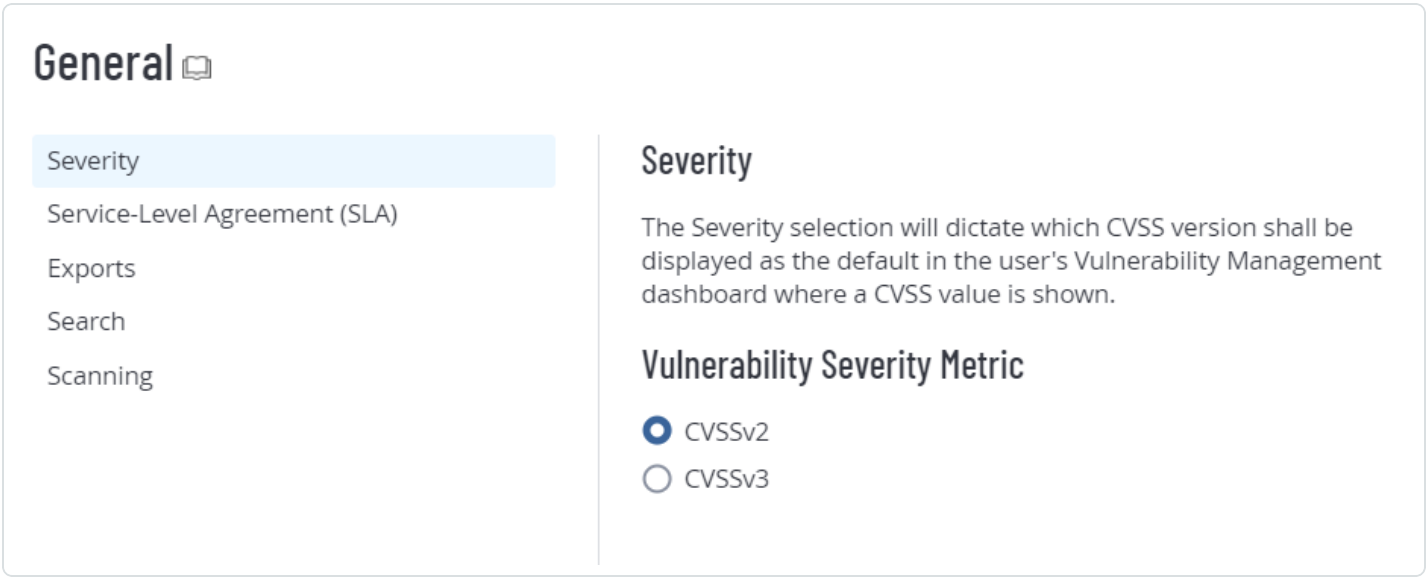
2. Click the **General** tile.

   The **General** page appears. By default, the **Severity** tab is active.

Here, you can configure the following options:

Severity

By default, Tenable Vulnerability Management uses CVSSv2 scores to calculate severity for individual vulnerability instances. If you want Tenable Vulnerability Management to calculate the severity of vulnerabilities using CVSSv3 scores (when available), you can configure your severity metric setting.



Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

For information about severity and the ranges for CVSSv2 and CVSSv3, see CVSS vs. VPR.

Note: This setting does not affect the following:

- Tenable Web App Scanning vulnerabilities.
- Tenable Container Security vulnerabilities.
- The calculations displayed in the **SLA Progress: Vulnerability Age** widget. To modify your SLA severity, navigate to the **Service-Level Agreement (SLA)** tab on the **General** page.

Caution: When changing your CVSS severity metric setting, the new setting is only reflected in new findings that come into your system. Any existing findings only reflect the previous severity setting (unless otherwise recasted). For more information on recast rules, see Recast/Accept Rules.

To configure your severity setting:

1. On the **Severity** tab, select the metric that you want Tenable Vulnerability Management to use for severity calculations.

    - **CVSSv2** – Use CVSSv2 scores for all severity calculations.
    - **CVSSv3** – Use CVSSv3 scores, when available, for all severity calculations. Use CVSSv2 only if a CVSSv3 score is not available.

2. Click **Save**.

3. The system saves your change and begins calculating severity based on your selection.

    All vulnerabilities seen before the change retain their severity. After the change, all vulnerabilities seen during scans receive severities based on your new selection. Because of this, you could see two sightings of the same vulnerability have two different CVSS scores and severities.

    > **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

Service-Level Agreement (SLA)

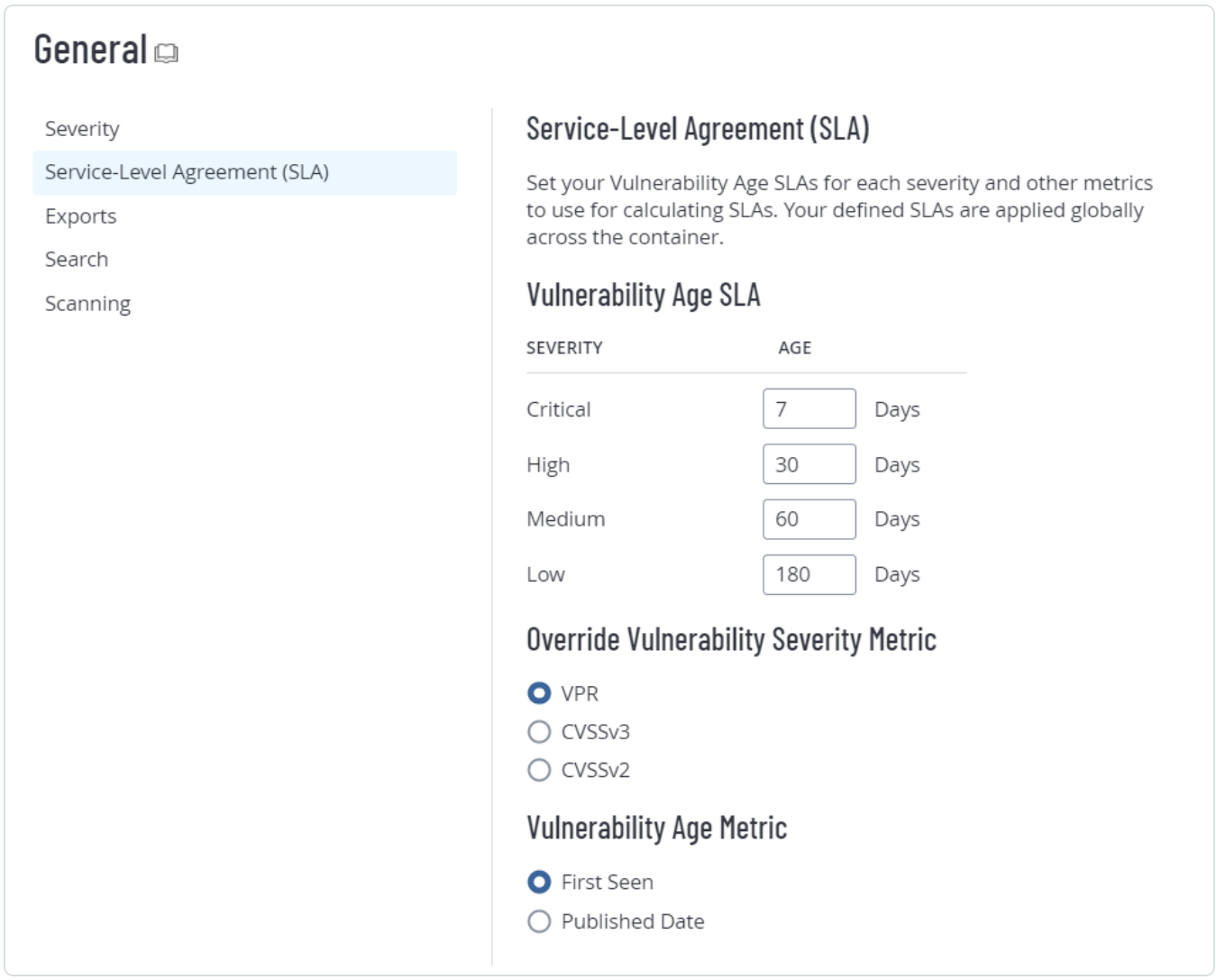
You can configure Service Level Agreement (SLA) settings to modify how Tenable calculates your SLA data.

You can view this data in the **SLA Progress: Vulnerability Age** widget on the **Vulnerability Management Overview** dashboard. For more information, see Vulnerability Management Dashboard.

To configure your SLA settings:

1. Click the **Service-Level Agreement (SLA)** tab.

    The SLA options appear.



2. Configure the following options:

Option	Default	Description/Actions
Vulnerability Age SLA	• **Critical** 7 days • **High** 30 days • **Medium** 60 days	To modify the number of days included for each severity, type an integer in the box next to **Critical**, **High**, **Medium**, or **Low**.

	• **Low** 180 days	
Override Vulnerability Severity Metric	VPR	Specifies whether Tenable uses VPR severity, CVSSv2 severity, or CVSSv3 severity to calculate SLA data. For more information about these metrics, see CVSS vs. VPR. **Note:** This option affects only the calculations displayed in the **SLA Progress: Vulnerability Age** widget. To modify the severity metric for all other areas of the product, navigate to the **Severity** tab on the **General** page.
Vulnerability Age Metric	First Seen	Specifies whether Tenable uses **First Seen** or **Published Date** to calculate SLA data.

3. Click **Save**.

   Tenable Vulnerability Management saves your SLA settings.

Language

On the **General** page, you can change the plugin language in your Tenable Vulnerability Management container to English, Japanese, Simplified Chinese, or Traditional Chinese. This setting affects all users in the container.

To change the plugin language:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **General** tile.

   The **General** tile appears. By default, the **Severity** tab is active.

4. Click the **Language** tab.

   The **Language** tab appears.

5. Under **Language**, select a new language.

   Tenable Vulnerability Management updates the plugin language for your container.

Export Expiration

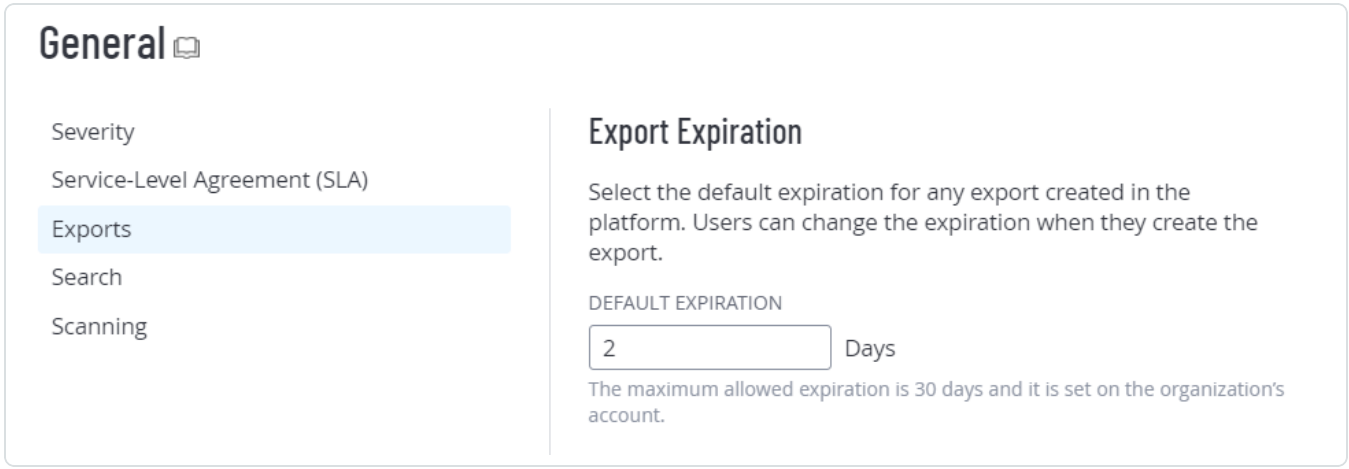
To configure your default export expiration:

When you create an export, you can set an expiration delay for the export file up to 30 calendar days, which is the maximum number of days that Tenable Vulnerability Management allows before your export files expire.

By default, any exports you create in Tenable Vulnerability Management have an expiration date of 30 days. If you want to decrease the number of days that Tenable Vulnerability Management allows before your export files expire, you can configure your default export expiration days.

1. Click the **Exports** tab.

   The **Export Expiration** options appear.



2. In the **Default Expiration** box, type the number of days you want to Tenable Vulnerability Management to allow before your exports expire.

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

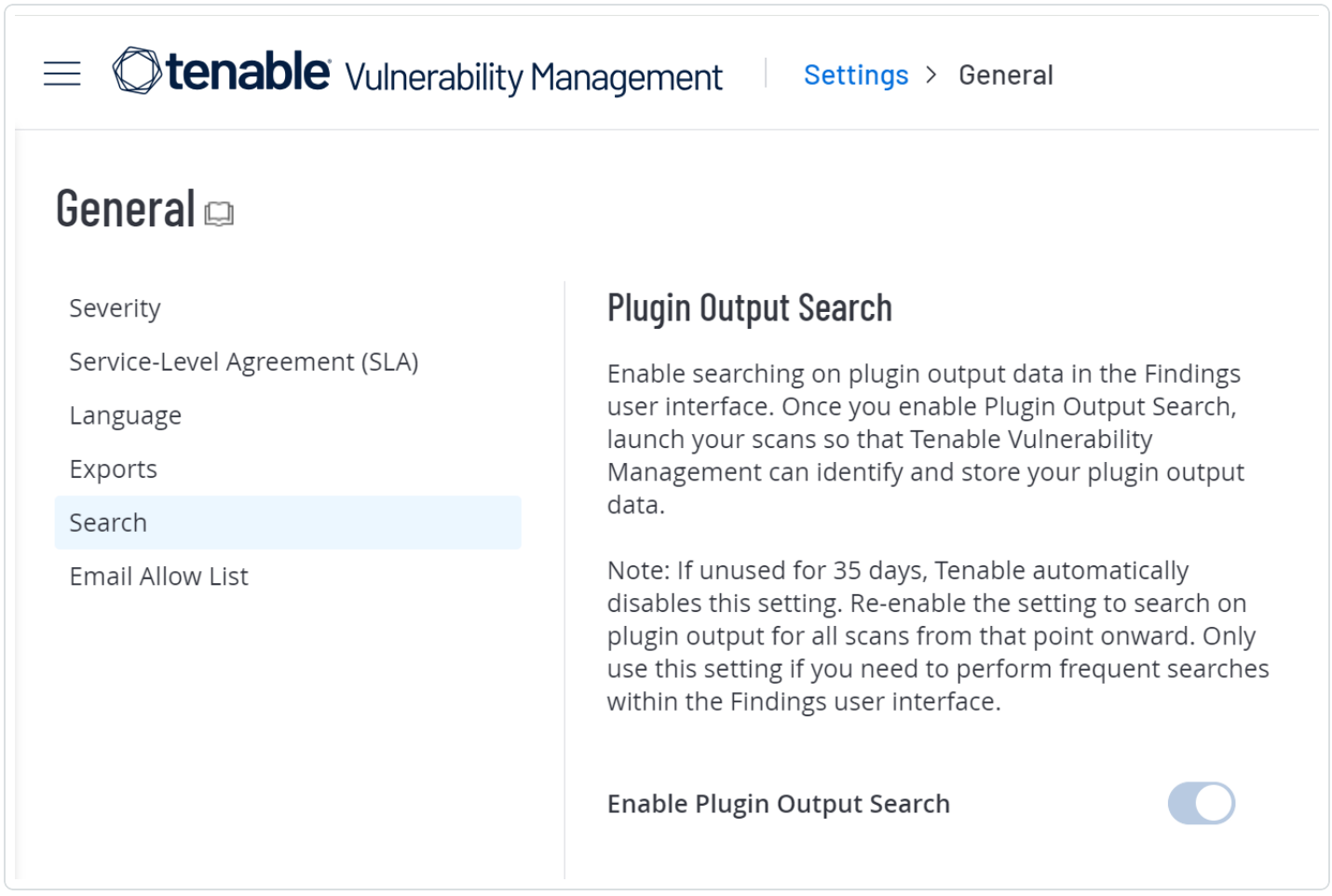
> **Note**: You must type the number of days as an integer between 1 and 30.

3. Click **Save**.

   Tenable Vulnerability Management saves your settings and updates the number of allowable days before your exports expire.

Search

Turn on **Enable Plugin Output Search** to store plugin output data each time you launch a scan. You can then filter vulnerability findings by plugin output and view that output on dashboards such as the AI/LLM Dashboard. Once you have enabled this setting, you must launch a scan to start storing the data.



> **Caution**: You cannot turn off **Enable Plugin Output Search** once you have turned it on, but the system automatically turns it off when it goes unused for 35 days.

Caution: Due to technical constraints in how the underlying system processes large data in JSON format, only the first 20,000,000 characters of raw plugin data are available when searching plugin output.

Email Allow List

In this section, type comma-separated email domains where the system can send export files, for example, *mycompany.com*. Once you add domains, users can *only* send exports to to those domains. An error appears when users try to email exports to unapproved domains.

Turn on the **Include Subdomains** toggle to include email subdomains: for example, *sales.mycompany.com*.

To learn more about the export types in Tenable Vulnerability Management, see Exports.

Note: When you turn on Email Allow List, it does not affect scan exports.

SAML

You can configure Tenable Vulnerability Management to accept credentials from your SAML identity provider (for example, Okta). This allows for an additional layer of security, where the SAML credentials are certified for use within Tenable Vulnerability Management. Once you enable SAML for a user, they can log in to Tenable Vulnerability Management directly through their identity provider, which automatically signs them in and redirects them to the Tenable Vulnerability Management landing page.

On the **SAML** page, you can view and manage your SAML credentials. You can also enable, disable, and add new configurations for users within your Tenable Vulnerability Management instance.

Tip: Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Vulnerability Management.

Note: Tenable Vulnerability Management supports SAML 2.0 configurations.

Note: Once SAML is configured for a user, they must log in using the IdP Tile or the URL provided in the SP metadata file (for example, cloud.tenable.com/SAML/XXXXXX) and log back out before they can access

he **Sign in via SSO** link on the Tenable Vulnerability Management login page. Additionally, any time you lear your browser cookies/cache, you must re-log in via the IdP tile or SP metadata file URL.

Important: Because Tenable Vulnerability Management cannot accept private keys to decrypt SAML assertions, Tenable Vulnerability Management does not support SAML assertion encryption. If you want to configure SAML authentication in Tenable Vulnerability Management, choose an identity provider that does not require assertion encryption and confirm that assertion encryption is not enabled.

SAML Details

On the **SAML** page, you can view a table that includes the following details about your SAML configurations:

Column	Description
UUID	The UUID that Tenable Vulnerability Management automatically generates when you create a new SAML configuration.
Description	A description for the SAML configuration.
Last Login	The date and time on which a user on your instance last successfully logged in via the SAML configuration. **Note**: The **Last Login** column shows a value only if Tenable Vulnerability Management has login data for the SAML identity provider.
Last Attempted Login	The date and time on which a user on your instance last attempted to log in via the SAML configuration. **Note**: The **Last Attempted Login** column shows a value only if Tenable Vulnerability Management has attempted login data for the SAML identity provider.
Certificate	The certificate for the SAML configuration. In the certificate column, you can complete the following tasks. • Click the button to copy the certificate to your clipboard. • Hover over the button to view the certificate expiration date.

	Note: Your identity provider determines the expiration date for your certificate.
Actions	An interactive column from which you can download the metadata.xml file that contains one or more security certificates for the configuration. To download the metadata.xml file: a. In the **Actions** column for the configuration from which you want to download a metadata.xml file, click the ⋮ button. An options menu appears. b. In the menu, click ⤓ **Download SP Metadata**. Tenable Vulnerability Management downloads the metadata.xml file to your computer.

View SAML Configurations

Required User Role: Administrator

To view your SAML configurations:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

   Tip: Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Vulnerability Management.

4. (Optional) Refine the table data. For more information, see Tables.

   The **SAML** table contains the following columns:

Column	Description
UUID	The UUID that Tenable Vulnerability Management automatically generates when you create a new SAML configuration.
Description	A description for the SAML configuration.
Last Login	The date and time on which a user on your instance last successfully logged in via the SAML configuration. **Note**: The **Last Login** column displays a value only if Tenable Vulnerability Management has login data for the SAML identity provider.
Last Attempted Login	The date and time on which a user on your instance last attempted to log in via the SAML configuration. **Note**: The **Last Attempted Login** column displays a value only if Tenable Vulnerability Management has attempted login data for the SAML identity provider.
Certificate	The certificate for the SAML configuration. In the certificate column, you can complete the following tasks. • Click the button to copy the certificate to your clipboard. • Hover over the button to view the certificate expiration date. **Note**: Your identity provider determines the expiration date for your certificate.
Actions	An interactive column from which you can download the metadata.xml file that contains one or more security certificates for the configuration. To download the metadata.xml file: 1. In the **Actions** column for the configuration from which you want to download a metadata.xml file, click the button. An options menu appears.

	2. In the menu, click ⭳ **Download SP Metadata**. Tenable Vulnerability Management downloads the metadata.xml file to your computer.

Add a SAML Configuration

Required User Role: Administrator

You can manually enter the details for your SAML configuration or you can upload a metadata.xml file that you download from your identity provider (IdP).

Note: Once SAML is configured for a user, they must log in using the IdP Tile or the URL provided in the SP metadata file (for example, cloud.tenable.com/SAML/XXXXXX) and log back out before they can access the **Sign in via SSO** link on the Tenable Vulnerability Management login page.

Important: Because Tenable Vulnerability Management cannot accept private keys to decrypt SAML assertions, Tenable Vulnerability Management does not support SAML assertion encryption. If you want to configure SAML authentication in Tenable Vulnerability Management, choose an identity provider that does not require assertion encryption and confirm that assertion encryption is not enabled.

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 Vulnerability Management. This includes the following high-level steps:

- Follow the steps described in your IdP's documentation to set up a SAML application for Tenable Vulnerability Management on your IdP account. Your IdP requires an entity ID and a reply URL for Tenable Vulnerability Management to set up the SAML application:
  - Entity ID/Audience URI– `TENABLE_IO_PLACEHOLDER`.
  - ACS/SSO URL/Login URL/Reply URL– `https://cloud.tenable.com/SAML/login/placeholder.com`.
- In your IdP account, download your metadata.xml file.

Note: Tenable does not currently support a SP-Initiated SAML flow. Because it must be initiated from the Identity Provider side, navigating directly to https://cloud.tenable.com does not allow SSO.

Important! All users must have an account configured in Tenable Vulnerability Management that matches their SSO login. You must ensure the SSO login matches the FULL Tenable account name (i.e., user@tenable.com).

To add a new SAML configuration:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the action bar, click ⊕ **Create**.

   The **SAML Settings** page appears.

5. Do one of the following:

   To provide configuration details by uploading the metadata.xml file from your IdP:

   a. In the first drop-down box, select **Import XML**.

      Note: **Import XML** is selected by default.

   b. The **Type** drop-down box specifies the type of identity provider you are using. Tenable Vulnerability Management supports SAML 2.0 (for example, Okta, OneLogin, etc.). This option is read-only.

   c. Under **Import**, click **Add File**.

      A file manager window appears.

   d. Select the metadata.xml file.

      The metadata.xml file is uploaded.

To manually create your SAML configuration using data from the metadata.xml file from your IdP:

a. In the first drop-down box, select **Manual Entry**.

   A **SAML** configuration form appears.

b. Configure the settings described in the following table:

Settings	Description
Enabled toggle	A toggle in the upper-right corner that indicates whether the SAML configuration is enabled or disabled. By default, the **Enable** setting is set to **Enabled**. Click the toggle to disable SAML configuration.
Type	Specifies the type of identity provider you are using. Tenable Vulnerability Management supports SAML 2.0 (for example, Okta, OneLogin, etc.). This option is read-only.
Description	A description for the SAML configuration.
IdP Entity ID	The unique entity ID that your IdP provides. **Note**: If you want to configure multiple IdPs for a user account, create a new configuration for each identity provider with separate identity provider URLs, entity IDs, and signing certificates.
IdP URL	The SAML URL for your IdP.
Certificate	Your IdP security certificate or certificates. **Note**: Security certificates are found in a metadata.xml file that your identity provider provides. You can copy the content of the file and paste it in the **Certificate** box.

Authentication Request Signing Enabled	A toggle that indicates whether authentication request signing is enabled. When this toggle is enabled, if: • a user is logged in via SAML and their session expires • a user logs out and tries to log back in directly via the Tenable Vulnerability Management interface rather than their IdP Tenable Vulnerability Management automatically signs the SAML authentication request that is sent to the IdP to log the user back in. **Note:** The authentication request can only be validated if the IdP is also configured to accept this setting. For more information, see the following resources: • Tenable SAML Quick Reference Guide • Manage Signing Certificates in Okta • Enforce Signed SAML Authentication Requests in Microsoft Entra ID • Edit a SAML Application in Ping Identity (**Enforce Signed AuthnRequest** option)
User Auto Provisioning Enabled	A toggle that indicates whether automatic user account creation is enabled or disabled.
IdP Assigns User Role at Provisioning	To assign a user role during provisioning, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access**

	Control > **Roles**.
IdP Resets User Role at Each Login	To assign a role each time a user logs in, overwriting the current role with the one chosen in your IdP, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**.
Group Management Enabled	Enable this toggle to allow the SAML configuration to manage user groups. You must enable this toggle for the **Managed by SAML** user group option to function successfully. For more information about this option, see Create a Group.

6. Click **Save**.

   Tenable Vulnerability Management saves your SAML configuration.

What to do next:

- Download the metadata.xml from Tenable Vulnerability Management using the **Download SP Metadata** option in the SAML Configurations table.
- Upload this file to the SAML application you created for Tenable Vulnerability Management with your SAML provider.

Tip: If you are having trouble configuring SAML, Tenable recommends trying one of the various third-party SAML debugging tools available online. You can also reach out to Tenable Support for further troubleshooting assistance.

Edit a SAML Configuration

Required User Role: Administrator

You can edit a SAML configuration on the **SAML** page.

Important: To avoid locking yourself out, ensure you have at least one admin user with access before updating SAML configurations. For example, if you disable the SAML configuration for your only admin user, you can no longer access and manage your application.

To edit a SAML configuration:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the SAML table, click the SAML configuration that you want to edit.

   The **SAML Settings** page appears.

5. (Optional) In the first drop-down box, select a different method to provide basic configuration details.

   - **Import XML** – Configure SAML authentication by uploading the metadata file your IdP provided, as described in Add a New SAML Configuration.
   - **Manual Entry** – Configure SAML authentication by manually configuring SAML options using data from the metadata.xml file your IdP provided, as described in Add a New SAML Configuration.

     Tenable Vulnerability Management updates the configuration options based on your selected source.

6. Update any of the configurable SAML settings described in the following table.

   Note: Some settings are read-only and cannot be modified.

   Note: The configuration options you can update depend on the source you select in the first drop-down box.

Settings	Source	Description
Enabled toggle	**Manual Entry**	Indicates whether the SAML configuration is enabled or disabled. By default, the setting is **Enabled**. In the upper-right corner, click the toggle to disable the SAML configuration.
Type	**Manual Entry** , **Import XML**	Specifies the type of identity provider you are using. Tenable Vulnerability Management supports SAML 2.0 (e.g., Okta, OneLogin, etc.).
UUID	**Entry**, **Import XML**	A unique identifier for your identity provider that Tenable Vulnerability Management automatically generates when you create a new SAML configuration. This box is read-only.
URL	**Manual Entry** , **Import XML**	The login URL that Tenable Vulnerability Management generates when you create a configuration. This box is read-only.
Entity ID	**Manual Entry** , **Import XML**	A unique identifier that Tenable Vulnerability Management generates when you create a configuration. This box is read-only.
Created	**Manual Entry** , **Import XML**	The time and date on which an administrator user created the configuration. This box is read-only.

Last Updated	**Manual Entry , Import XML**	The time and date on which an administrator user last updated the configuration. This box is read-only.
Description	**Manual Entry**	A description for the SAML configuration.
IdP Entity ID	**Manual Entry**	Your identity provider's unique entity ID. **Note**: If you want to configure multiple IdPs for a user account, create a new configuration for each identity provider, with separate identity provider URLs, entity IDs, and signing certificates.
IdP URL	**Manual Entry**	The SAML URL for your identity provider.
Certificate	**Manual Entry**	Your identity provider's security certificate or certificates. **Note**: Security certificates are found in a metadata.xml file that your identity provider provides. You can copy the content of the file and paste it in the **Certificate** box.
Authentication Request Signing Enabled	**Manual Entry**	A toggle that indicates whether authentication request signing is enabled. When this toggle is enabled, if: • a user is logged in via SAML and their session expires • a user logs out and tries to log back in directly via the Tenable Vulnerability Management interface rather than their IdP

		Tenable Vulnerability Management automatically signs the SAML authentication request that is sent to the IdP to log the user back in. **Note:** The authentication request can only be validated if the IdP is also configured to accept this setting. For more information, see the following resources: • Tenable SAML Quick Reference Guide • Manage Signing Certificates in Okta • Enforce Signed SAML Authentication Requests in Microsoft Entra ID • Edit a SAML Application in Ping Identity (**Enforce Signed AuthnRequest** option)
User Autoprovisioning Enabled	**Manual Entry**	A toggle that indicates whether automatic account user creation is enabled or disabled.
IdP Assigns User Role at Provisioning	**Manual Entry**	To assign a user role during provisioning, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value. To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**.
IdP Resets User Role at Each Login	**Manual Entry**	To assign a role each time a user logs in, overwriting the current role with the one chosen in your IdP, enable this toggle. In your SAML identity provider, add an attribute statement with **userRoleUuid** as the attribute name and the user role UUID as the attribute value.

		To obtain the UUID for a user role, go to **Settings** > **Access Control** > **Roles**.
Group Management Enabled	**Manual Entry**	Enable this toggle to allow the SAML configuration to manage user groups. You must enable this toggle for the **Managed by SAML** user group option to function successfully. For more information about this option, see Create a Group.
Import	**Import XML**	A metadata.xml file from your identity provider that contains one or more SAML certificates. To import a new metadata.xml file from your identity provider: a. Under **Import**, click **Add File**. A file explorer window appears. b. Select the metadata.xml file. The metadata.xml file is uploaded. **Note**: If your metadata.xml file contains multiple certificates, only the first one appears in the **Certificate** column for the configuration on the **SAML** page.

7. Click **Save**.

   Tenable Vulnerability Management saves the configuration.

   The **SAML** page appears with the updated configuration.

Disable a SAML Configuration

Required User Role: Administrator

Disabling a SAML configuration prevents users on your instance from using the SAML credentials in the configurations to log in to Tenable Vulnerability Management. You can enable a disabled SAML configuration as described in Enable a SAML Configuration.

Caution: When you disable a SAML configuration, users can no longer log in to Tenable Vulnerability Management using their SAML credentials. Make sure all users on your instance have an alternative method to log in to Tenable Vulnerability Management before you disable a SAML configuration.

To disable a SAML configuration:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the SAML table, click the SAML configuration that you want to disable.

   The **SAML Settings** page appears.

5. At the bottom of the page, click the **SAML Enable** toggle to disable the configuration.

6. Click **Save**.

   Tenable Vulnerability Management disables the SAML configuration. On the **SAML** page, the disabled configuration appears in light gray.

Note: You cannot disable a SAML configuration that is already disabled.

Enable a SAML Configuration

Required User Role: Administrator

You can enable a disabled a SAML configuration. For more information about SAML authentication in Tenable Vulnerability Management, see SAML.

Tip: Review the Tenable SAML Configuration Quick Reference Guide for a step-by-step guide of how to configure SAML for use with Tenable Vulnerability Management.

Note: Once SAML is configured for a user, they must log in using the IdP Tile or the URL provided in the SP metadata file (for example, cloud.tenable.com/SAML/XXXXXX) and log back out before they can access the **Sign in via SSO** link on the Tenable Vulnerability Management login page.

Before you Begin:

Configure your IdP to authenticate with Tenable Vulnerability Management. For more information, see the Tenable SAML Configuration Quick Reference Guide.

To enable a SAML configuration:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the SAML table, click the SAML configuration that you want to enable.

   Tip: Disabled configurations appear in light gray.

   The **SAML Settings** page appears.

5. At the bottom of the page, click the **SAML Enable** toggle to enable the configuration.

6. Click **Save**.

   Tenable Vulnerability Management enables the SAML configuration. On the **SAML** page, the enabled configuration appears in black.

Enable Automatic Account Provisioning

Required User Role: Administrator

When you manually configure or edit a SAML configuration, you can enable automatic user account provisioning. Automatic account provisioning allows users with credentials for the IdP named in the SAML configuration to create a Tenable Vulnerability Management account the first time they log in via the IdP.

> **Tip:** Review the Tenable SAML Configuration Quick-Reference guide for a step-by-step guide of how to configure SAML for use with Tenable Vulnerability Management.

Tenable Vulnerability Management creates automatically provisioned accounts with the following defaults:

- **Full name** – NameID
- **Username** – NameID
- **Email** – NameID
- **User role** – Basic

Tenable Vulnerability Management does not currently support any other claim types.

Before you Begin:

Configure your IdP to authenticate with Tenable Vulnerability Management. For more information, see the Tenable SAML Configuration Quick Reference Guide.

To enable automatic user account provisioning:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the SAML table, click the SAML configuration for which you want to enable automatic account provisioning.

The **SAML Settings** page appears.

5. At the bottom of the page, click the **User Autoprovisioning Enabled** toggle to enable automatic account provisioning.
6. Click **Save**.

   Tenable Vulnerability Management enables automatic account provisioning in the SAML configuration.

Disable Automatic Account Provisioning

> **Required User Role:** Administrator

Disabling automatic account provisioning prevents users from automatically creating Tenable Vulnerability Management account the first time they access the platform via their IdP. You can enable automatic account provisioning on a SAML configuration, as described in Enable Automatic Account Creation.

To disable automatic user account provisioning:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.
3. Click the **SAML** tile.

   The **SAML** page appears.
4. In the SAML table, click the SAML configuration for which you want to disable automatic account provisioning.
5. The **SAML Settings** page appears.
6. At the bottom of the page, click the **User Autoprovisioning Enabled** toggle to disable automatic account provisioning.
7. Click **Save**.

Tenable Vulnerability Management disables automatic account provisioning in the SAML configuration.

Delete a SAML Configuration

> **Required User Role:** Administrator

You can delete a SAML configuration on the **SAML** page. For more information about SAML authentication in Tenable Vulnerability Management, see SAML .

To enable a SAML configuration:

Before you begin:

- Disable the SAML configuration you want to delete.

To delete a SAML configuration:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **SAML** tile.

   The **SAML** page appears.

4. In the SAML table, select the check box for the SAML configuration that you want to delete.

5. In the action bar, click the **Delete** button.

   Tenable Vulnerability Management deletes the SAML configuration.

   > **Note:** Ensure that when you delete a SAML configuration, you also remove the related configuration in your IdP.

What to do next:

- Remove the related configuration from your identity provider's application.

License Information

On the **License Information** page, you can view a complete breakdown of your Tenable products and how many asset licenses they are using. You can view this information in multiple ways, including visual overviews by product or time period that enable you to spot trends such as temporary usage spikes or product misconfigurations.

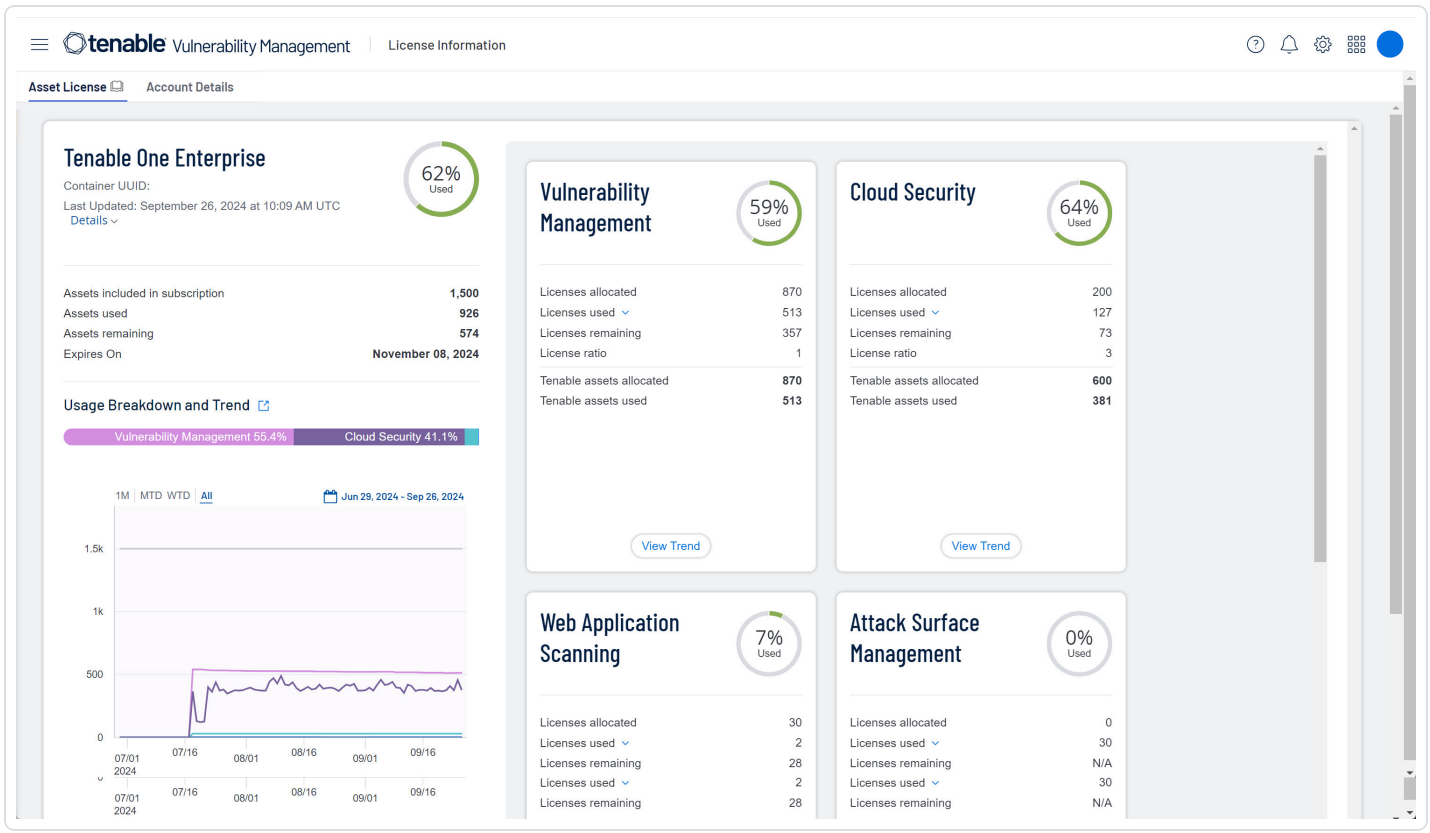
This page is broken down into two tabs:

- **Asset License** – License usage for all Tenable products in the current container.
- **Account Details** – Organization-level details such as your account information.

Tip: For details on how Tenable licenses work and how assets or resources are licensed in each product, see Licensing Tenable Products.

View the License Information Page

- To view the **License Information** page, in the top navigation bar, click ⚙ and on the page that appears, click **License**.



Asset License

View information about your Tenable licenses in the **Asset License** tab, which appears by default when you open the **License Information** page.

The **Asset License** tab shows license usage for products in the current Tenable container. Details appear in panels, separated by product. If you have Tenable One, to view its components, in the bottom-right corner, click **Show More**.

The following information appears on the **Asset License** tab:

Section	Description
Product summary	Name of the product and the unique identifier for your Tenable container, the date and time of the last update, and a ring chart which summarizes your asset license usage. Click **Details** to view the following: • **Site Name** – The cluster containing your installed products in Tenable's cloud. • **Region** – The geographic region in which your cluster is located. • **VM Plugin Set** – The version for the product's Nessus plugin set. • **VM Plugin Updated** – The date and time the Nessus plugin set was last updated. This section also contains the following: • **Assets included in subscription** – The number of Tenable asset licenses you have purchased for that product. • **Assets used** – The total number of asset licenses used or assessed from your product subscription. • **Overused assets** – If using more Tenable licenses than you have purchased, indicates that number, accounting for any license ratio. • **Expires On** – The date your license expires.
Usage Breakdown & Trend	See visual breakdowns of your asset license usage: • **Bar Chart** – (Tenable One only) View your total asset license use by

	Tenable One component in a bar chart. • **Usage Over Time** - View your asset license use over time in a line chart where the X-axis is the time period and the Y-axis is the number of asset licenses used. Filter the chart by time period. For Tenable One, below the chart, click a component to show or hide it.
Licenses allocated	The total number of your Tenable asset licenses allocated to a product.
Licenses used	The total number of Tenable asset licenses used in that product. If you have Tenable One, this number is the total of all asset licenses used across all Tenable One components. **Tip**: The type of asset you license varies by product. To learn more, see Tenable One Components.
Overused licenses	(Tenable One-only) If any, your license overage—that is, the number of extra licenses you are using. To learn more, see Tenable Cloud Overage Process.
License ratio	If any, the *ratio* against which the assets in your environment are multiplied to determine how many Tenable asset licenses you need to purchase. For example, if you have 1,000 assets to assign to Tenable Identity Exposure, you will need 500 Tenable asset licenses, since the ratio is *0.5*. To learn more, see Licensing Tenable One.
Tenable assets allocated	The total number of Tenable asset licenses you have assigned to a product, accounting for any ratio.
Tenable assets used	The total number of Tenable asset licenses used by that product, accounting for any ratio.

Account Details

View your account details in the **Account Details** tab, which contains information about your organization and your Tenable products. It is always the same, regardless of which Tenable container you are using.

Required User Role: Administrator

The **Account Details** tab contains the following information:

Section	Description
Account Information	View your account information: • **Account Name** – The name of your organization. • **Customer ID** – Your unique Tenable customer identification number. • **Tenable Contact Information** – The name and email of your Tenable customer success manager.
Tenable One Licenses	Under **Active Product Subscriptions**, view information about your Tenable One licenses, including version, your container's unique ID, your allocated assets, and your Tenable asset license's start and end dates. Also view a table with the following columns: • **Product Type** – The type of product (for example, Cloud). • **Activation Key** – The license key for your product. • **Site Name** – The cluster containing your installed products in Tenable's cloud. • **Region** – The geographic region in which your cluster is located. • **Assets Used** – The number of assets you have used. • **Assets Allocated** – The total number of assets available for all your Tenable One products. **Tip**: Next to a product, click the drop-down **>** to view information about your Tenable One components by **Product Type**, **Percent Allocated**, **Assets Used**, and **Assets Allocated**.
Standalone Product Licenses	Under **Active Product Subscriptions** view information about your standalone licenses.

Note: On-premise products such as Tenable Agent or Tenable Cloud Security do not appear here.

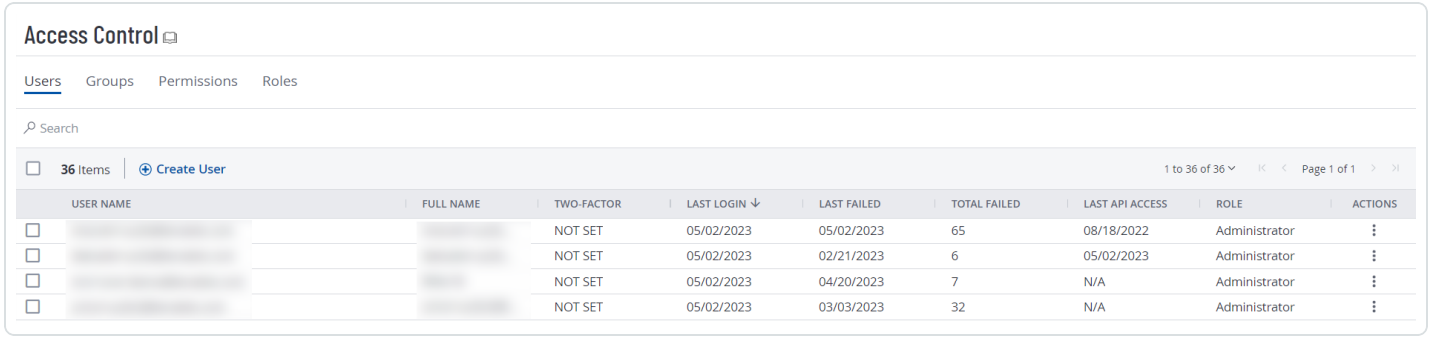
In a table, view the following:

- **Product Name** – The name of your Tenable product, for example Tenable PCI ASV.
- **Container UUID** – The unique ID for the container.
- **Activation Key** – The license key for your product.
- **Site Name** – The cluster containing your installed products in Tenable's cloud.
- **Region** – The geographic region in which your cluster is located.
- **Assets Used** – The number of assets you have used.
- **Assets Purchased** – The total number of assets you have purchased for that product.
- **Start Date** – The date your Tenable subscription started.
- **End Date** – The date your Tenable subscription ends.

Access Control

Required User Role: Administrator

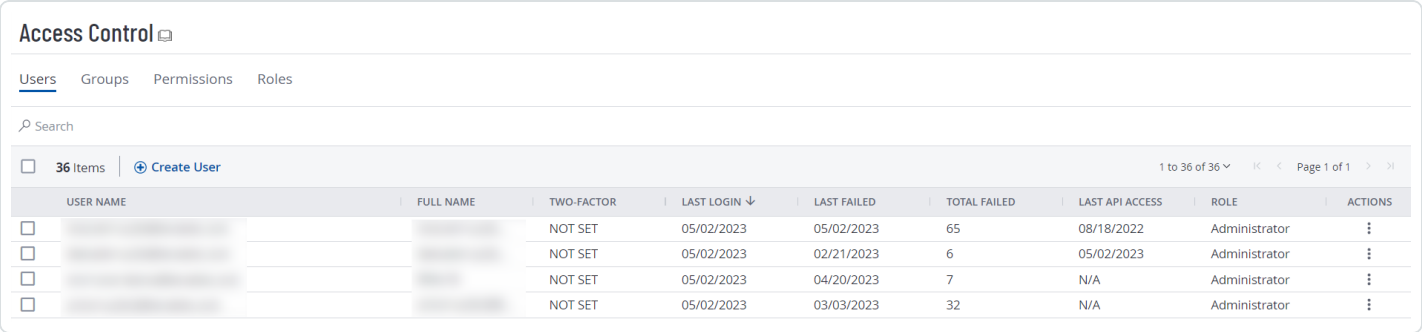
From the **Access Control** page, you can view and configure the list of users and groups on your account and the permissions assigned to them.



Users

Topics in this section have been modified to reflect feature updates in Tenable Vulnerability Management Key Enhancements. For more information, see Tenable Vulnerability Management Key Enhancements.

On the Access Control page, in the **Users** tab, administrator users can create and manage user accounts for an organization's resources in Tenable Vulnerability Management.



To view users and user data for your Tenable Vulnerability Management instance:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

3. The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

4. Click the **Users** tab.

   The **Users** page appears.

   The **Users** page displays a table of all Tenable Vulnerability Management user accounts. This documentation refers to that table as the *users table*.

Users Table

Column	Description
Name	The username for the account.

Full Name	The full name of the user.
Last Login	The date on which the user last successfully logged in to the Tenable Vulnerability Management interface.
Last Failed	The date on which the user failed to log in to the Tenable Vulnerability Management interface.
Total Failed	The total number of failed login attempts for the user. This number resets when either an administrator or the user resets the password for the user account.
Last API Access	The date on which the user last generated API keys.
Role	The role assigned to the user. For more information, see Roles.
Actions	The actions an administrator user can take with the user (e.g. export a user).

Create a User Account

Required User Role: Administrator

On the **Users** page, you can create an account for a new user.

Tip: Looking for account creation via a SAML IdP? See the SAML documentation.

Note: User accounts expire according to when the Tenable Vulnerability Management container they belong to was created. Tenable controls this setting directly. For more information, contact Tenable Support.

To create a user account:

1. In the left navigation, click **Settings**.

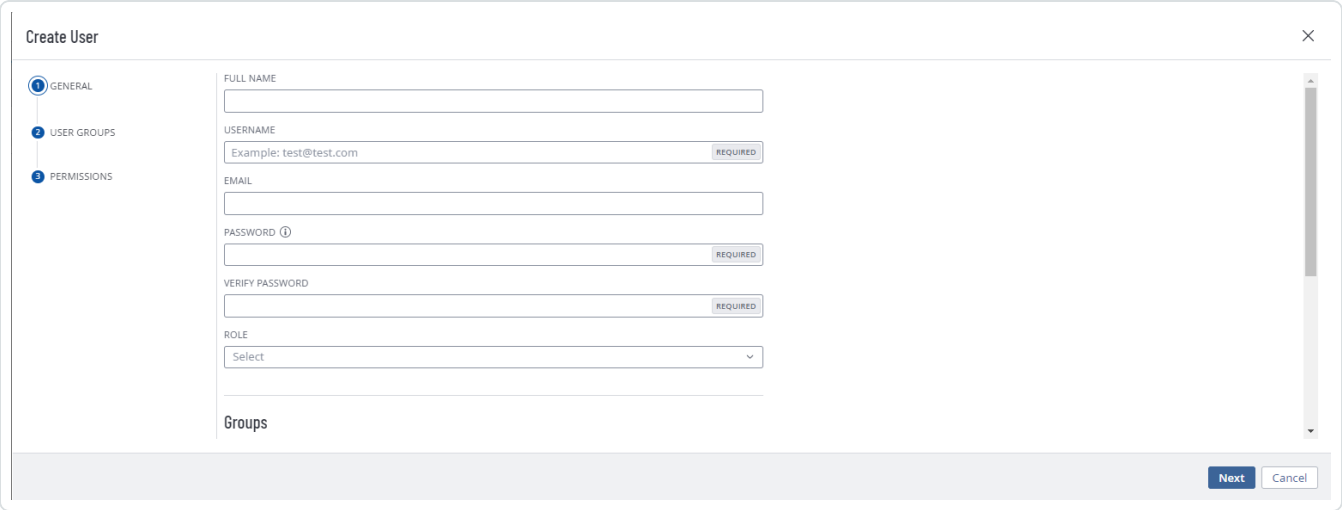
   The **Settings** page appears.

2. Click the **Access Control** tile.

The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the ⊕ **Create User** button.

   The **Create User** page appears.



4. Configure the following options:

> **Note**: To view and configure options in each section, you must select the section in the left menu.

Option	Action
General Section	
Full Name	Type the first and family name of the user.
Username	Type a valid username. A valid username must be in the format: *name@domain* where *domain* corresponds to a domain approved for your Tenable Vulnerability Management instance. **Note:** During initial setup, Tenable configures approved

	domains for your Tenable Vulnerability Management instance. To add domains to your instance, contact your Tenable representative. **Note:** Tenable Vulnerability Management usernames cannot include the following characters: ', !, #, $, %, ^, &, *, (,), /, \, |, {, }, [,], ", :, ;, ~, `, <, > and the comma "," itself.
Email	Type a valid email address in the format: *name@domain* where *domain* corresponds to a domain approved for your Tenable Vulnerability Management instance. This email address overrides the email address set in the **Username** box. If you leave this option empty, Tenable Vulnerability Management uses the **Username** value as the user's email address. **Note:** As an Administrator, you can create user accounts with email addresses from unapproved domains. Once a user account is created, you can only change the email address to another approved domain.
Password	Type a valid password. See Password Requirements for more information. In Tenable Web App Scanning, passwords must be at least 12 characters long and contain the following: • An uppercase letter • A lowercase letter • A number • A special character

Verify Password	Type the password again.
Role	In the drop-down box, select the role that you want to assign to the user.
Authentication	Select or deselect the available security setting options. When selected, these settings: **Note**: If you enable the **Password Access** or **SAML** options for a user with a custom role, the user automatically has basic access to your dashboards and widgets. • **API Key** – Allow the user to generate API keys. **Tip**: You can select only this setting to create an API-only user account. • **SAML** –Allow the user to log in to their account using a SAML single sign-on (SSO). For more information, see SAML. • **Username/Password** – Allow the user to log in to their account using a password. **Note**: If you deselect this option, you cannot select the MFA option. • **Two-Factor Required** – Require the user to provide two-factor authentication to log in to their account. **Tip**: You can configure two-factor authentication for your own account on the My Account page.
User Groups Section	
User Groups	Select the user group or groups to which you want to

	assign the user. By default, a new user belongs to the system-generated **All Users** user group, which assigns the user the **Basic** role. Add a user group: • Click anywhere in the **User Groups** box. A search box and drop-down list of roles appear. • (Optional) In the **Search** box, type a user group name. As you type, a list of user groups matching your search appears. • Click the user group you want to add. In the **User Groups** box, Tenable Vulnerability Management adds a label representing the user group. • Repeat these steps to add the user to another user group.
Permission Section	
Permissions	In the **Permissions** table, select the permission configurations you want to assign to the user.

5. Click **Save**.

   Note: If you assign permissions to the user, the button appears as **Add & Save**.

   Tenable Vulnerability Management lists the new user account on the users table.

Edit a User Account

Required User Role: Administrator

To edit a user account:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. In the users table, click the name of the user that you want to edit.

   The **Edit User** page appears.

4. Configure the following options:

Option	Action
Account Settings	
Full Name	Edit the first and last name of the user.
Username	You cannot edit this option.
Email	Type a valid email address in the format: *name@domain* where *domain* corresponds to a domain approved for your Tenable Vulnerability Management instance. This email address overrides the email address set in the **Username** box. If you leave this option empty, Tenable Vulnerability Management uses the **Username** value as the user's email address. **Note:** As an Administrator, you can create user accounts with email addresses from unapproved domains. Once a user account is created, you can only change the email address to another approved domain.
New Password	Type a valid password. See Password Requirements for more information. In Tenable Web App Scanning, passwords must be at least 12 characters long and contain the following:

	• An uppercase letter • A lowercase letter • A number • A special character
Role	In the drop-down box, select the role that you want to assign to the user.
Groups	
User Groups	Select the user group or groups to which you want to assign the user. The user inherits the roles and permissions associated with the user group.
security settings	Select or deselect the available security setting options. When selected, these settings: • **API** – Allow the user to generate API keys. **Tip**: You can select only this setting to create an API-only user account. • **SAML** –Allow the user to log in to their account using a SAML single-sign on (SSO). For more information, see SAML. • **Password Access** – Allow the user to log in to their account using a password. **Note**: If you deselect this option, you cannot select the MFA option. • **MFA** – Require the user to provide two-factor authentication to log in to their account. **Tip**: You can configure two-factor authentication for you own account on the My Account page.

5. (Optional) Generate API keys for the user.
6. Click **Save**.

Tenable Vulnerability Management saves the changes to the account.

View Your List of Users

Required User Role: Administrator

On the Access Control page, in the **Users** tab, you can view a list of all the users on your Tenable Vulnerability Management instance.

To view users and user data for your Tenable Vulnerability Management instance:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Users** tab.

   The **Users** tab appears, containing a table of all Tenable Vulnerability Management user accounts on your Tenable Vulnerability Management instance. This documentation refers to that table as the *users table*.

Users Table

On the users table, you can view the following information about users on your Tenable Vulnerability Management instance.

Column	Description
Name	The username for the account.
Last Login	The date on which the user last successfully logged in to the Tenable Vulnerability Management interface.
Last Failed	The date on which the user failed to log in to the Tenable Vulnerability Management interface.
Total	The total number of failed login attempts for the user.

Failed	This number resets when either an administrator or the user resets the password for the user account.
Last API Access	The date on which the user last generated API keys.
Role	The role assigned to the user. For more information, see Roles.
Actions	The actions an administrator user can take with the user (e.g. export a user).

Tenable Vulnerability Management Password Requirements

Tenable Vulnerability Management enforces the following password requirements for all accounts:

Password Criteria

Passwords must be at least 12 characters long and contain the following:

- An uppercase letter
- A lowercase letter
- A number
- A special character

Password Expiration

Tenable Vulnerability Management passwords do not expire.

Account Lockout

By default, after 5 failed login attempts, Tenable Vulnerability Management locks the user out of their account. When a user is locked out of their account, they can unlock their own account, or an administrator can reset their password.

Password History

You cannot reuse a current or former password.

Change Another User's Password

Required User Role: Administrator

To change the password for another user's account, you must be an administrator. To change your own password, see Change Your Password.

To change another user's password:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. In the users table, click the name of the user that you want to edit.

   The **Edit User** page appears.

4. In the **New Password** box, type a new password. See Password Requirements for more information.

5. Click **Save**.

   Tenable Vulnerability Management saves the new password for the user account.

Assist a User with Their Account

Required User Role: Administrator or Custom Role with appropriate privileges

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

As an administrator, you can use the user assist functionality to simulate being logged in as another account. While assisting a user account, you can perform operations in Tenable Vulnerability Management as that user without needing to obtain their password or having to log out of your administrator account.

Note: **User Assist** is available only for user accounts that have one or both of these authentication settings enabled:

- **Username/Password**

- **SAML**

To enable these security settings, see Edit a User Account.

To assist a user with their account:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. In the users table, click the check box for the user account you want to assist.

   The action bar appears at the top of the table.

   Note: You can select only one user to assist at a time.

4. In the action bar, click the button.

   Tenable Vulnerability Management refreshes and displays the default dashboard for the user you are assisting. While you are assisting the user, Tenable Vulnerability Management displays an overlay at the top of each page with the role of the user you are assisting.

To stop assisting a user with their account:

- At the top of any page, in the overlay that displays the role of the user you are assisting, click the button.

Generate Another User's API Keys

Required User Role: Administrator

The API keys associated with your user account enable you to access the API for all Tenable Vulnerability Management products for which your organization is licensed. These keys must be used to authenticate with the Tenable Vulnerability Management REST API.

Administrators can generate API keys for any user account. Other roles can generate API keys for their own accounts. For more information, see Generate API Keys.

Note: The API keys associated with your user account enable you to access the API for all Tenable Vulnerability Management products for which your organization is licensed. You cannot set separate keys for individual products. For example, if you generate API keys in Tenable Vulnerability Management, this action also changes the API keys for Tenable Web App Scanning and Tenable Container Security.

To generate API keys for another user:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. In the users table, click the name of the user that you want to edit.

   The **Edit User** page appears.

4. In the **API Keys** section, click **Generate API Keys**.

   Caution: Any existing API keys are replaced when you generate new API keys. You must update the applications where the previous API keys were used.

   A warning message appears.

5. Review the warning and click **Replace & Generate**.

   The **Generate API Keys** text box appears.

   The new access and secret keys for the account appear in the text box.

6. (Optional) Click **Re-generate API Keys**.

7. Copy the new access and secret keys to a safe location.

   Caution: Be sure to copy the access and secret keys before you navigate away from the **Edit User** page. After you close this page, you cannot retrieve the keys from Tenable Vulnerability Management.

Unlock a User Account

Tenable Vulnerability Management locks you out if you attempt to log in and fail 5 consecutive times.

Note: A user can be locked out of the user interface but still submit API requests if they are assigned the appropriate authorizations (api_permitted). For more information, see the Tenable Developer Portal.

You can unlock a user account in one of the following ways:

- If a user has access to the email address specified in the user account, they can unlock their own account.
- If a user no longer has access to that email address, another user with administrator privileges can reset the user's password.

Disable a User Account

Required User Role: Administrator

Important: Disabling a user account:

- does not disable scheduled reports for that user, nor does it prevent others from generating a report shared by the disabled user. For more information, see Reports.
- prevents the user from logging in.
- prevents the user's scans from running and aborts any ongoing scans owned by the user.

You can enable a disabled user account as described in Enable a User Account.

To disable a user account:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Select the user or users you want to disable:

- Select a single user:

  a. In the users table, in the row for the user account you want to disable, click the ⋮ button.

  The action buttons appear in the row.

  b. In the row, click the ⊘ button.

  A confirmation window appears.

- Select multiple users:

  a. In the users table, click the check box for each user you want to disable.

  The action bar appears at the bottom of the page.

  b. In the action bar, click the ⊘ button.

  A confirmation window appears.

4. In the confirmation window, click **Disable**.

   A success message appears.

   Tenable Vulnerability Management disables the selected user or users. In the users table, a disabled user appears in light gray.

   > **Note:** If the user you disable has a session in progress, they may continue to have limited access. However, once they log out, they cannot log back in.

Enable a User Account

> **Required User Role:** Administrator

When you disable a user account, you can enable an account again to restore a user's access.

To enable a user account:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Select the user or users you want to enable:

   ### Select a single user:

   a. In the users table, in the row for the user account you want to enable, click the ⋮ button.

      The action buttons appear in the row.

      > **Note**: Users appear grayed out while they are disabled.

   b. In the row, click the ✓ button.

      A confirmation window appears.

   ### Select multiple users:

   a. In the users table, click the check box for each user you want to enable.

      The action bar appears at the bottom of the page.

   b. In the action bar, click the ✓ button.

      A confirmation window appears.

4. In the confirmation window, click **Enable**.

   A success message appears.

   Tenable Vulnerability Management enables the selected user or users. In the users table, an enabled user appears in black.

Manage User Access Authorizations

Users can access Tenable Vulnerability Management using the following methods:

- Username and password login.
- Single sign-on (SSO). For more information, see SAML.
- Tenable Vulnerability Management REST API with API keys. For more information, see Generate Another User's API Keys.

When you create a new user, all access methods are authorized by default. Depending on your organization's security policies, you may need to disable certain access methods, for example, disable username and password login to enforce SSO.

Use the Tenable Vulnerability Management Platform API to view, grant, and revoke access authorizations for a user. For more information, see Get User Authorizations and Update User Authorizations in the Tenable Developer Portal.

Export Users

Required User Role: Administrator

On the **Users** page, you can export one or more users in CSV or JSON format.

To export your users:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Users** tab.

   The **Users** page appears. This page contains a table that lists all users for your Tenable Vulnerability Management instance.

4. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

5. Select the users that you want to export:

Export Scope	Action
Selected users	To export selected users: a. In the users table, select the check box for each user you want to export.

	The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 users, select all the users in the list and then click [→ **Export**.
A single user	To export a single user: a. In the users table, right-click the row for the user you want to export. The action options appear next to your cursor. -or- In the users table, in the **Actions** column, click the ⋮ button in the row for the user you want to export. The action buttons appear in the row. b. Click **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  Note: By default, all fields are selected.
- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

6. In the **Name** box, type a name for the export file.
7. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of users. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of users. Empty fields are not included in the JSON file.

8. (Optional) Deselect any fields you do not want to appear in the export file.
9. In the **Expiration** box, type the number of days before the export file expires.

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

10. (Optional) To set a schedule for your export to repeat:

    - Click the **Schedule** toggle.

      The **Schedule** section appears.

    - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
    - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
    - In the **Repeat** drop-down box, select how often you want the export to repeat.
    - In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

      Note: If you select never, the schedule repeats until you modify or delete the export schedule.

11. (Optional) To send email notifications on completion of the export:

    Note: You can enable email notifications with or without scheduling exports.

- Click the **Email Notification** toggle.

  The **Email Notification** section appears.

- In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
- (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

  > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

12. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

13. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Delete a User Account

> **Required User Role:** Administrator

Before you delete a user account, you must first disable the user account.

> **Caution:** Once you delete a user account, the account cannot be recovered and the action cannot be reversed.

> **Caution:** Tenable Web App Scanning does not support object migration. When you delete a Tenable Web App Scanning user, the application does not reassign objects belonging to the deleted users. Note that you cannot reassign a Tenable Web App Scanning scan to a new owner if its owner is deleted.

Caution: Before you delete a user account, reassign any associated Remediation projects. These will not be reassigned automatically.

The following table describes what objects are migrated, retained, or permanently deleted upon user deletion:

Object Type	Deleted	Notes
Audit Files in Scans	Yes	Permanently deleted
Scan Schedules	No	Migrated to the new object owner **Note:** Migrated scan schedules may be disabled if they rely on other permanently deleted objects, such as Audit files, Target Groups, or Unmanaged Credentials.
Historical Scan Results	No	Migrated to the new object owner
Scan Templates	No	Migrated to the new object owner
Unmanaged Credentials in Scans	Yes	Permanently deleted
Custom Dashboards/Widgets	Yes	Migrated to the new object owner
Managed Credentials	No	Retained (**Created By** value displays as **null**)
Tags	No	Retained (**Created By** value displays as **null**)
Recast/Accept Rules	No	Retained (**Owner** value displays as **Unknown User**)
Exclusions	No	Retained
System Target Groups	No	Retained
User Target Groups	No	Migrated to the new object owner
Saved Searches	Yes	Permanently deleted
Connectors	No	Retained

Object Type	Deleted	Notes
Sensors	No	Retained
Scheduled Exports	No	Migrated to the new object owner

To delete a user account:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

4. In the users table, in the row for the user account you want to delete, click the ⋮ button.

   A menu appears.

5. In the menu, click the 🗑 button.

   > **Note**: If a user is not disabled, then the 🗑 button does not appear. Disable the user before deleting them.

   > **Note:** You cannot delete the Default Administrator account. If you want to delete the Default Administrator account, you must contact Tenable Support.

   The user plane appears.

6. In the **Select New Object Owner** drop-down box, select the user to which you want to transfer any of the user's objects (e.g., scan results, user-defined scan templates).

7. Click 🗑 **Delete**.

   A confirmation message appears.

8. Click **Delete**.

   Tenable Vulnerability Management deletes the user and transfers any user objects to the user you designated.

User Groups

User groups allow you to manage user permissions for various resources in Tenable Vulnerability Management. When you assign users to a group, the users inherit the permissions assigned to the group. Your organization may utilize groups to provide permissions to batches of users based on the roles of those users and your organization's security posture.

To view your user groups:

1. In the left navigation, click **Settings**.

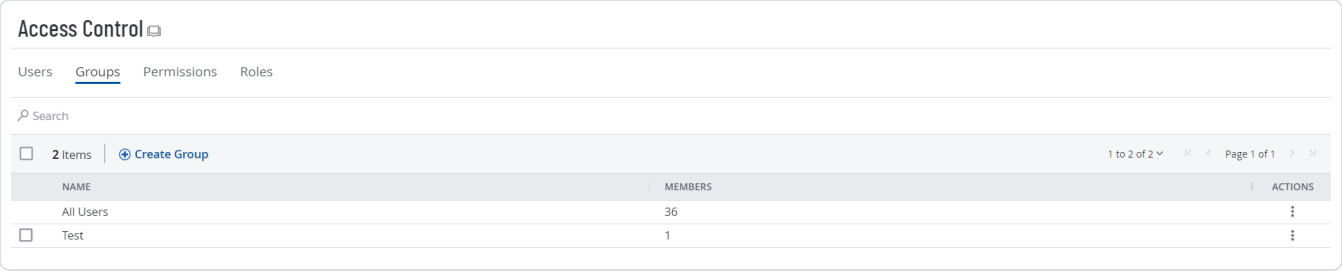
   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Groups** tab.

   The **Groups** page appears.



The **User Groups** page displays a table of all user groups in your Tenable Vulnerability Management instance. This documentation refers to that table as the *user groups table*.

The user groups table contains the following columns:

Column	Description
Name	The group name. You can define this name for all user groups except the

	Tenable-provided **All Users** and **Administrator** groups.
Members	The number of users assigned to the user group.
Actions	The actions you can take with the group.

On the **Groups** tab, you can perform the following actions:

- Create a Group
- Edit a Group
- Export Groups
- Delete a Group

Create a User Group

> **Required User Role:** Administrator

To create a user group:

1. In the left navigation, click **Settings**.

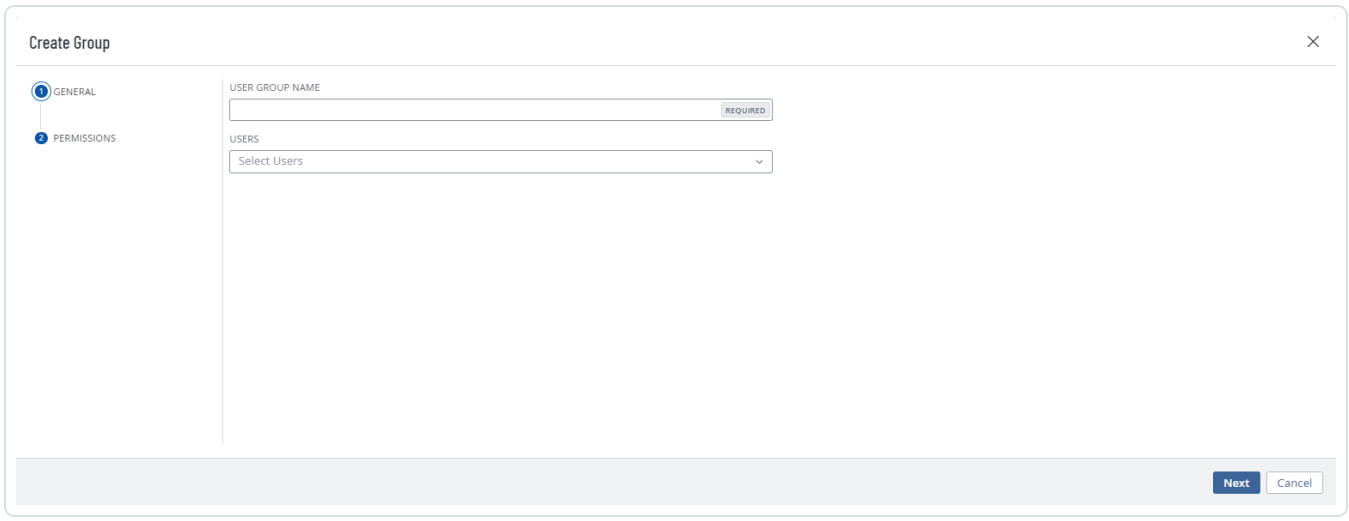
   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. At the top of the user group table, click the **Create User Group** button.

   The **Create Group** page appears.



4. In the **User Group Name** box, type a name for the new group.

5. (Optional) If you want to enable Tenable Vulnerability Management to automatically add users who log in using your SAML configuration to this user group, in the **General** section, select the **Managed by SAML** checkbox.

Important: For this feature to function successfully, you must also enable the Group Management Enabled toggle when creating/editing your SAML configuration. For more information on SAML configuration steps, see the SAML Quick Reference Guide.

Once you configure the related claim within your IdP, anytime a user logs in via your SAML configuration, Tenable Vulnerability Management automatically adds them to the specified user group.

6. Add users to the group:

a. For each user you want to add, click the Users drop-down box and begin typing a username.

   As you type, Tenable Vulnerability Management filters the list of users in the drop-down box to match your search.

b. Select a user from the drop-down box.

   Tenable Vulnerability Management adds the user to the list of users to be added to the user group.

   > **Tip:** To remove a user from the list of users to be added, roll over the user and click the ✕ button.

7. Click **Save**.

   Tenable Vulnerability Management creates the user group and adds the listed users as members.

   The **Groups** page appears, where you can view the new group listed in the user groups table.

Edit a User Group

> **Required User Role:** Administrator

To edit a group:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. In the user groups table, click the user group that you want to edit.

   The **Edit User Group** page appears.

4. Do any of the following:

- In the **User Group Name** box, type a new group name.
- Add users to the group:
  a. For each user you want to add, click the **Users** drop-down box and begin typing a username.

     As you type, Tenable Vulnerability Management filters the list of users in the drop-down box to match your search.

  b. Select a user from the drop-down box.

     Tenable Vulnerability Management adds the user to the list of users to be added to the user group.
- Remove a user from the group:
  a. In the **Users** list, click the ✕ button next to the user account you want to remove.

     Tenable Vulnerability Management removes the user from the **Users** list.
- Enable/disable the optional **Managed by SAML** option.

  (Optional) If you want to enable Tenable Vulnerability Management to automatically add users who log in using your SAML configuration to this user group, in the **General** section, select the **Managed by SAML** checkbox.

  > **Important:** For this feature to function successfully, you must also enable the Group Management Enabled toggle when creating/editing your SAML configuration. For more information on SAML configuration steps, see the SAML Quick Reference Guide.

  Once you configure the related claim within your IdP, anytime a user logs in via your SAML configuration, Tenable Vulnerability Management automatically adds them to the specified user group.
- Add or remove permissions from the group.

5. Click **Save**.

   Tenable Vulnerability Management saves the user group with any changes you made.

Export Groups

> **Required User Role:** Administrator

On the Access Control page, in the **Groups** tab, you can export one or more user groups in CSV or JSON format.

To export your user groups:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Groups** tab.

   The **Groups** tab appears, containing a table that lists all user groups in your Tenable Vulnerability Management instance.

4. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

5. Do one of the following:

   To export a single group:

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

      The action options appear next to your cursor.

      -or-

      In the groups table, in the **Actions** column, click the ⋮ button in the row for the group you want to export.

      The action buttons appear in the row.

   b. Click **Export**.

      The **Export** plane appears. This plane contains:

      - A text box to configure the export file name.
      - A list of available export formats.
      - A table of configuration options for fields to include in the exported file.

> **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.

To export multiple groups:

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

   The action bar appears at the top of the table.

b. In the action bar, click [→ **Export**.

   > **Note**: You can individually select and export up to 200 groups. If you want to export more than 200 groups, you must select all the groups on your Tenable Vulnerability Management instance by selecting the check box at the top of the groups table and then click [→**Export**.

   The **Export** plane appears. This plane contains:

   - A text box to configure the export file name.
   - A list of available export formats.
   - A table of configuration options for fields to include in the exported file.

     > **Note**: By default, all fields are selected.

   - A text box to set the number of days before the export expires.

The **Export** plane appear. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  > **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.

- A toggle to configure the export schedule.
- A toggle to configure the email notification.

6. In the **Name** box, type a name for the export file.
7. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of groups. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of groups. Empty fields are not included in the JSON file.

8. (Optional) Deselect any fields you do not want to appear in the export file.
9. In the **Expiration** box, type the number of days before the export file expires.

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

10. (Optional) To set a schedule for your export to repeat:
    - Click the **Schedule** toggle.

      The **Schedule** section appears.
    - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
    - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
    - In the **Repeat** drop-down box, select how often you want the export to repeat.

- In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

  > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

11. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

    - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.

    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

12. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

13. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Delete a Group

> **Required User Role:** Administrator

> **Note**: You cannot delete the Tenable-provided **Administrator** or **All Users** user group.

Before you begin:

- Remove all users from the user group. You cannot delete a user group that contains any users.

To delete one or more user groups:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Groups** tab.

   The **Groups** page appears. This page displays a table with all the user groups on your Tenable Vulnerability Management account.

4. Do one of the following:

   - To delete a single user group:

     a. In the user groups table, click the button for the user group you want to delete.

        A menu appears.

     b. Click the **Delete** button.

        A confirmation window appears.

   - To delete multiple user groups.

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

        The action bar appears at the top of the table.

     b. In the action bar, click the **Delete** button.

        A confirmation window appears.

5. In the confirmation window, click **Delete**.

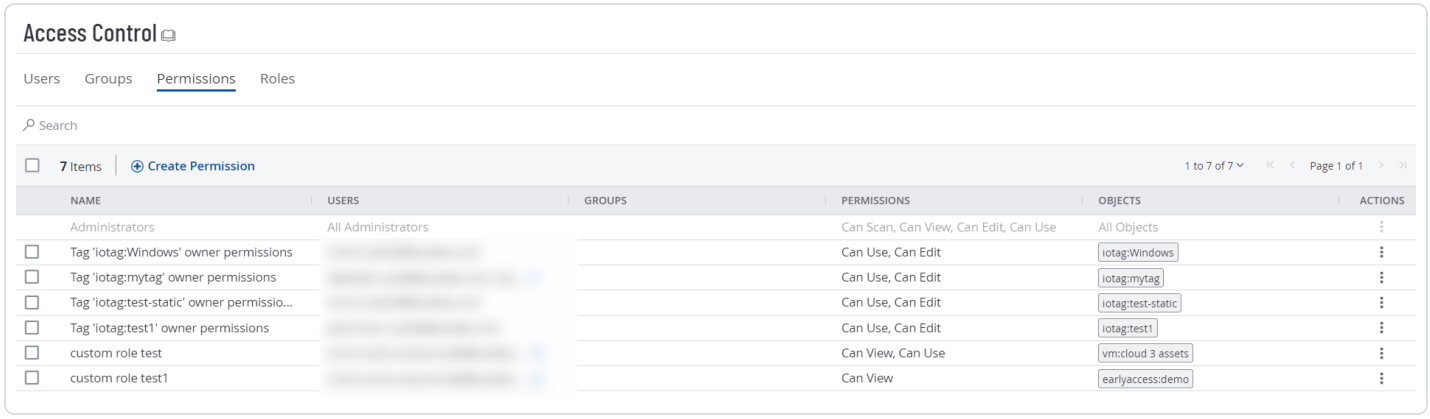
   Tenable Vulnerability Management deletes the selected user group or groups. The deleted group or groups no longer appear in the user groups table.

Permissions

Tenable Vulnerability Management allows you to create and manage configurations that determine which users on your organization's account can perform specific actions with the organization's resources and data. This documentation refers to these configurations as ***permission configurations***[1].

> **Note:** Tenable Web App Scanning does not handle permissions reliant on a tag.

On the **My Accounts** page, each user can view the permission configurations assigned to them. However, only administrator users can view or manage permission configurations for other users. For more information, see Tenable-Provided Roles and Privileges.



When you create a user or user group, you can assign existing permission configurations to them for assets that meet the criteria specified by a previously created tag. In Tenable Vulnerability Management, these assets and the tags that define them are called ***objects***[2].

---

[1] A configuration that administrators can create to determine what actions certain users and groups can perform with a given set of resources.

[2] In a permission configuration, an asset and the tag that defines it.

Roles vs. Permissions: What's the difference?

- Roles – Roles allow you to manage privileges for major functions in Tenable Vulnerability Management and control which Tenable Vulnerability Management modules and functions users can access.
- Permissions – Permissions allow you to manage access to your own data, such as Tags, Assets, and their Findings.

When you create a permission configuration, you must select one or more of the following predefined permissions. These permissions determine the actions users can take with the object or objects defined in the permission configuration.

Permission	Description
Can View	Allows a user or group with this permission to view the assets defined by the object.
Can Scan	Allows a user or group with this permission to scan the assets defined by the object. **Note:** For a manually entered target to be considered valid, it must meet the following criteria: • The user is an administrator OR • The user has at least Scan Operator role privileges, AND • If the target does not exist within the Tenable Vulnerability Management system, the user must have **CanScan** permissions on an object that refers to the target explicitly via IPv4, IPV6 or FQDN. If the object has more than one rule, the rules must be joined by the "Match Any" filter, OR • If the target already exists within the Tenable Vulnerability Management system, then it must be tagged by an object for which the user has **CanScan** permissions.
Can Edit	Allows a user or group with this permission to edit the tag that defines the object.
Can Use	Allows a user or group with this permission to use the tag that defines the

	object.

To view your permission configurations in Tenable Vulnerability Management:

1. In the left navigation, click **Settings**.

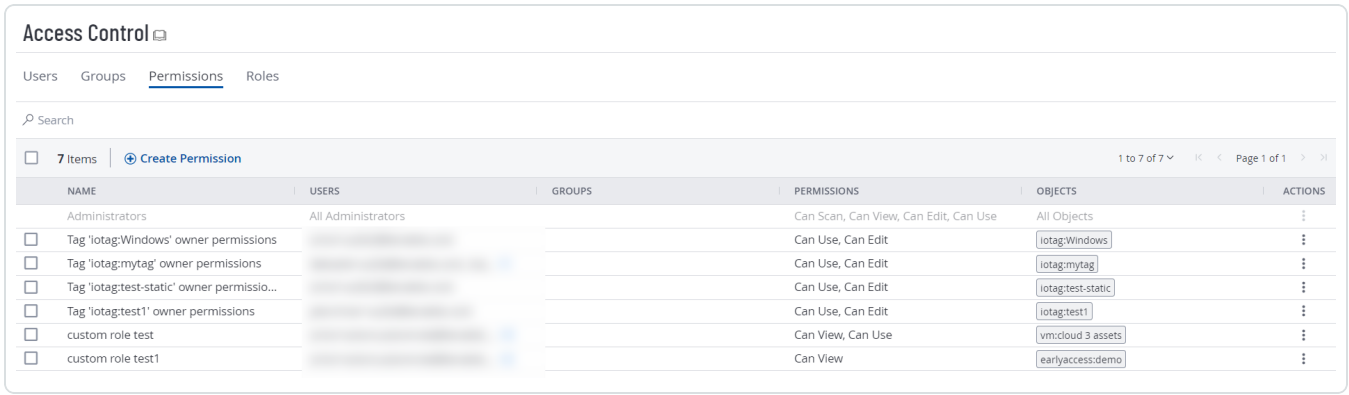
   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Permissions** tab.

   The **Permissions** tab appears. This tab contains a table that lists all of the permission configurations on your Tenable Vulnerability Management instance.



> **Note**:The first row of the permissions table contains a read-only entry for Administrators. This entry exists to remind you that Administrators have all permissions for every resource on your account. For more information, see Roles.

On the **Permissions** tab, you can perform the following actions:

- Create and Add a Permission Configuration
- Add a Permission Configuration to a User or Group
- Edit a Permission Configuration
- Export Permission Configurations

- Remove a Permission Configuration from a User or Group
- Delete a Permission Configuration

Create and Add a Permission Configuration

Required User Role: Administrator

When you create a permission configuration in Tenable Vulnerability Management, you can apply that configuration to one or more users or groups.

Before you begin:

- Create a user or group for your Tenable Vulnerability Management account.
- Create a tag for the object for which you want to create a permission.

To create and add a permission configuration to a user or group:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

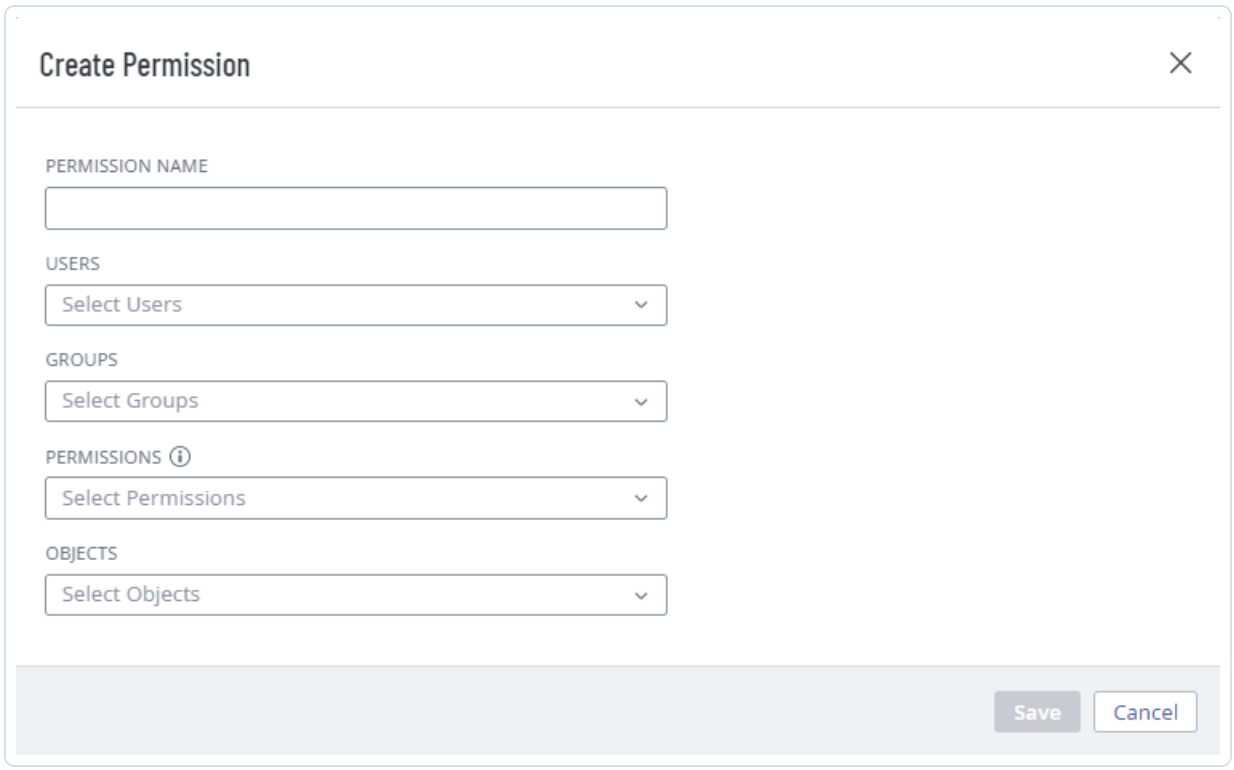
   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Permissions** tab.

   The **Permissions** tab appears. This tab contains a table that lists all of the permission configurations on your Tenable Vulnerability Management instance.

4. At the top of the table, click **Create Permission**.

   The **Create Permission** window appears.



5. In the **Permission Name** box, type a name for the permission configuration.
6. (Optional) In the **Users** drop-down box, select one or more users.

   Note: Although the **Users** box is optional, you cannot save the permission configuration unless at least one user or user group is selected.

7. (Optional) In the **Groups** drop-down box, select one or more user groups.

   Note: Although the **Groups** box is optional, you cannot save the permission configuration unless at least one user or user group is selected.

   Note: You can select **All Users** in the **Groups** drop-down box to assign the permission configuration to all users on your Tenable Vulnerability Management instance. However, Tenable recommends that you use caution when assigning the permission configuration to all users because doing so goes against security best practices.

8. In the **Permissions** drop-down box, select one or more permissions.

Caution: Adding the **Can Edit** permission to your permission configuration along with the **Can View** or **Can Scan** permission allows assigned users to change the scope of the assets they can view and scan. Tenable recommends that you combine the **Can Edit** permission with the **Can View** or **Can Scan** permission only for administrator users.

Note: If you select the **Can Edit** permission, Tenable Vulnerability Management automatically adds the **Can Use** permission.

9. In the **Objects** drop-down box, select one or more objects to which to apply the permission configuration.

   Note: The objects in the drop-down box are previously created tags that identify and define your assets. For more information, see Permissions.

   Tip: You can select **All Assets** to allow users and group to view or scan all the assets on your instance, regardless of whether the assets match any existing objects. You can also select **All Tags** to allow users and groups on your instance to edit or use all objects on your instance. For more information about objects, see Permissions.

10. Click **Save**.

    A confirmation message appears.

    Tenable Vulnerability Management saves your changes. The permission configuration appears on the **Permissions** tab.

Add a Permission Configuration to a User or Group

Required User Role: Administrator

Before you begin:

- Create a user or group for your Tenable Vulnerability Management account.
- Create a permission configuration.

To add a permission configuration to a user or group:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Do one of the following:

   - Add a permission configuration to a user:

     a. Click the **Users** tab.

        The **Users** tab appears. This tab contains a list of all the users on your Tenable Vulnerability Management instance.

     b. In the users table, click the user to which you want to add a permission configuration.

        The **Edit User** page appears.

     c. In the **Permissions** section, at the top of the table, click **Add Permissions**.

        The **Add Permissions** window appears.

     d. Select the check box next to one or more permission configurations.

     e. Click **Add**.

        The permission configuration appears in the **Permissions** table on the **Edit User** page.

   - Add a permission configuration to a user group:

     a. Click the **Groups** tab.

        The **Groups** tab appears. This tab contains a list of all the user groups on your Tenable Vulnerability Management instance.

     b. In the groups table, click the group to which you want to add a permission configuration.

The **Edit User Group** page appears.

c. In the **Permissions** section, at the top of the table, click **Add Permissions**.

The **Add Permissions** window appears.

d. Select the check box next to one or more permission configurations.

e. Click **Add**.

The permission configuration appears in the **Permissions** table on the **Edit User Group** page.

4. Click **Save**.

Tenable Vulnerability Management saves your changes and adds the permission configuration to the user or group.

Edit a Permission Configuration

Required User Role: Administrator

To edit a permission configuration:

1. In the left navigation, click ⚙ **Settings**.

The **Settings** page appears.

2. Click the **Access Control** tile.

The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Permissions** tab.

The **Permissions** tab appears. This tab contains a list of all the permission configurations on your Tenable Vulnerability Management instance.

4. In the table, click the permission configuration you want to edit.

The **Permission Details** page appears.

5. (Optional) In the **Permission Name** box, type a new name for the permission configuration.

6. (Optional) Add or remove users or user groups.

7. (Optional) Add or remove a permission:

   Caution: Adding the *Can Edit* permission to your permission configuration along with the *Can View* or *Can Scan* permission allows the users selected in the permission configuration to change the scope of the assets they can view and scan. Tenable recommends that you combine the *Can Edit* permission with the *Can View* or *Can Scan* permission only for administrator users.

   Note: If you select the **Can Edit** permission, Tenable Vulnerability Management automatically adds the **Can Use** permission.

   Note: You cannot assign permissions to user or groups for a given object that overlap with permissions assigned to them via another permission configuration. For example, if you selected the *Can Edit* permission for an object, but a user listed under **Users** already has the ability to edit that object based on an existing permission configuration, Tenable Vulnerability Management generates an error message and prevents you from saving the current permission configuration until you modify your selections to remove the redundancy.

   a. To add a permission, in the **Permissions** drop-down box, select one or more permissions.

   b. To remove a permission, in the **Permissions** drop-down box, click the ✕ button next to each permission you want to remove.

8. (Optional) Add or remove an object.

   a. To add an object, in the **Objects** drop-down box, select one or more objects.

   b. To remove an object, in the **Objects** drop-down box, click the ✕ button next to each object you want to remove.

9. Click **Save**.

   Tenable Vulnerability Management saves your changes. The updated permission configuration appears on the **Permissions** tab.

Export Permission Configurations

Required User Role: Administrator

On the **Permissions** page, you can export one or more permission configurations in CSV or JSON format.

To export your permission configurations:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Permissions** tab.

   The **Permissions** tab appears. This tab contains a table that lists all of the permission configurations on your Tenable Vulnerability Management instance.

   > **Note**:The first row of the permissions table contains a read-only entry for Administrators. This entry exists to remind you that Administrators have all permissions for every resource on your account. For more information, see Roles.

4. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

5. Do one of the following:

   ### To export a single permission configuration:

   a. In the permission configurations table, right-click the row for the permission configuration you want to export.

      The action options appear next to your cursor.

      -or-

      In the permission configurations table, in the **Actions** column, click the ⋮ button in the row for the permission configuration you want to export.

      The action buttons appear in the row.

   b. Click **Export**.

   ### To export multiple permission configurations:

a. In the permission configurations table, select the check box for each permission configuration you want to export.

   The action bar appears at the top of the table.

b. In the action bar, click **More**.

   A menu appears.

c. Click **Export**.

> **Note**: You can individually select and export up to 200 permission configurations. If you want to export more than 200 permission configurations, you must select all the permission configurations on your Tenable Vulnerability Management instance by selecting the check box at the top of the permission configurations table and then click **Export**.

The **Export** plane appears. This plane contains the following:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

> **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

6. In the **Name** box, type a name for the export file.
7. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of permission configurations. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs

	a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of permission configurations. Empty fields are not included in the JSON file.

8. (Optional) Deselect any fields you do not want to appear in the export file.
9. In the **Expiration** box, type the number of days before the export file expires.

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

10. (Optional) To set a schedule for your export to repeat:

    - Click the **Schedule** toggle.

      The **Schedule** section appears.

    - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
    - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
    - In the **Repeat** drop-down box, select how often you want the export to repeat.
    - In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

      Note: If you select never, the schedule repeats until you modify or delete the export schedule.

11. (Optional) To send email notifications on completion of the export:

    Note: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

- In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
- (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

  > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

12. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

13. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Remove a Permission Configuration from a User or Group

> **Required User Role:** Administrator

> **Note**: You cannot remove a permission configuration from the Tenable-provided **Administrator** or **All Users** user groups.

To remove a permission configuration from a user or user group:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. To remove a permission configuration from a user:

   - Do one of the following:

     - Remove the permission configuration via the **Users** tab:

       a. Click the **Users** tab.

          The **Users** tab appears. This tab contains a list of all the users on your Tenable Vulnerability Management instance.

       b. In the users table, click the user from which you want to remove a permission configuration.

          The **Edit User** page appears.

       c. In the **Permissions** table, in the **Actions** column, click the ⋮ button next to the permission configuration you want to remove.

       d. Click the **Remove** button.

          Tenable Vulnerability Management removes the permission configuration from the user.

       e. (Optional) Repeat for each user from which you want to remove a permission configuration.

     - Remove the permission via the **Permissions** tab:

       a. Click the **Permissions** tab.

          The **Permissions** tab appears. This tab contains a table that lists all of the permission configurations on your Tenable Vulnerability Management instance.

       b. In the table, click the permission configuration you want to remove.

          The **Permission Details** page appears.

c. Under **Users**, click the ✕ button next to each user from which you want to remove the permission configuration.

   Tenable Vulnerability Management removes the permission configuration from the **Users** list.

4. To remove a permission configuration from a user group:

   - Do one of the following:

     - Remove the permission configuration via the **Groups** tab:

       a. Click the **Groups** tab.

          The **Groups** tab appears. This tab contains a list of all the user groups on your Tenable Vulnerability Management instance.

       b. In the user groups table, click the group from which you want to remove a permission configuration.

          The **Edit User Group** page appears.

       c. In the **Permissions** table, in the **Actions** column, click the ⋮ button next to the permission configuration you want to remove.

       d. Click the **Remove** 🗑 button.

          Tenable Vulnerability Management removes the permission configuration from the user group.

       e. (Optional) Repeat for each user group from which you want to remove a permission configuration.

     - Remove the permission configuration via the **Permissions** tab:

       a. Click the **Permissions** tab.

          The **Permissions** tab appears. This tab contains a table that lists all of the permission configurations on your Tenable Vulnerability Management instance.

b. In the table, click the permission you want to remove.

   The **Permission Details** page appears.

c. Under **Groups**, click the ✕ button next to each user group from which you want to remove the permission configuration.

   Tenable Vulnerability Management removes the permission configuration from the **Groups** list.

5. Click **Save**.

   Tenable Vulnerability Management saves your changes and removes the permission from the user or group.

Delete a Permission Configuration

Required User Role: Administrator

Note: You cannot delete the default permission configuration.

To remove a permission configuration from a user or user group:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Permissions** tab.

   The **Permissions** tab appears. This tab contains a table that lists all of the permission configurations on your Tenable Vulnerability Management instance.

4. In the table, in the **Actions** column, click the ⋮ button next to the permission configuration you want to delete.

5. Click the **Delete** 🗑 button.

   Tenable Vulnerability Management deletes the permission configuration.

Roles

Roles allow you to manage privileges for major functions in Tenable Vulnerability Management and control which Tenable Vulnerability Management resources users can access in Tenable Vulnerability Management.

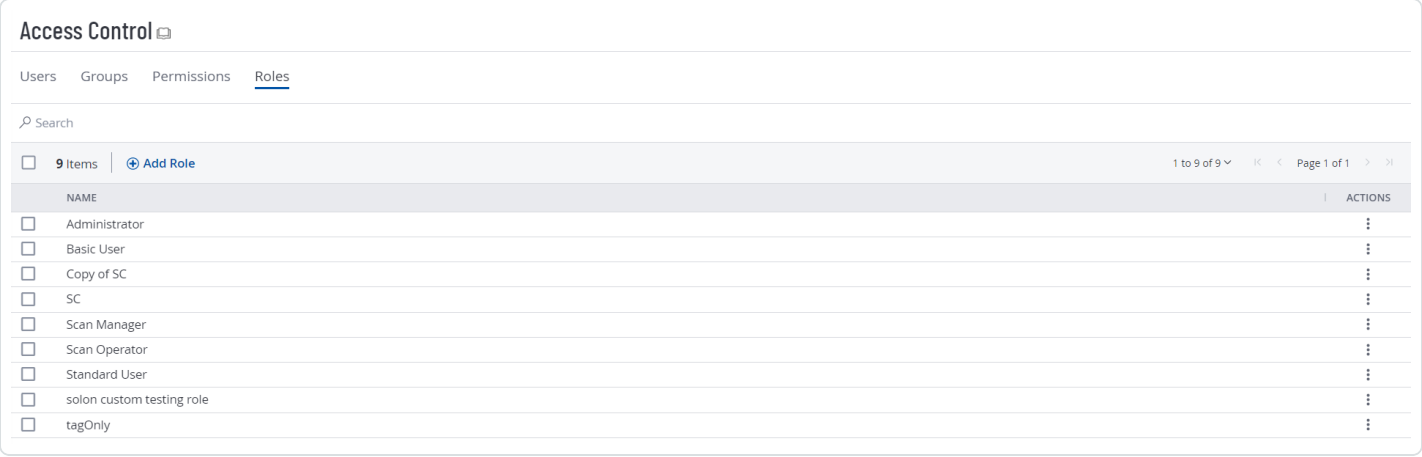
When you create a user, you must select a role for that user that broadly determine the actions the user can perform.

Note: You can further refine user access to specific resources by assigning permissions to individual users or groups. For more information, see Permissions.

Roles vs. Permissions: What's the difference?

- Roles – Roles allow you to manage privileges for major functions in Tenable Vulnerability Management and control which Tenable Vulnerability Management modules and functions users can access.
- Permissions – Permissions allow you to manage access to your own data, such as Tags, Assets, and their Findings.

On the **Roles** page, you can view all Tenable-provided roles and any custom roles created on your Tenable Vulnerability Management instance.



You can assign one of the following role types to users:

Role Type	Description
Tenable-Provided	Contains a predefined set of privileges determined by the Tenable Vulnerability Management product specified on your account license. Each

Roles and Privileges	role encompasses the privileges of lower roles and adds new privileges. Administrators have the most privileges. Basic users have the fewest.
Custom Roles	Contains a custom set of privileges that allow you to tailor user privileges and access to resources on your Tenable Vulnerability Management instance.

To view your user roles:

1. In the left navigation, click ⚙ **Settings**.

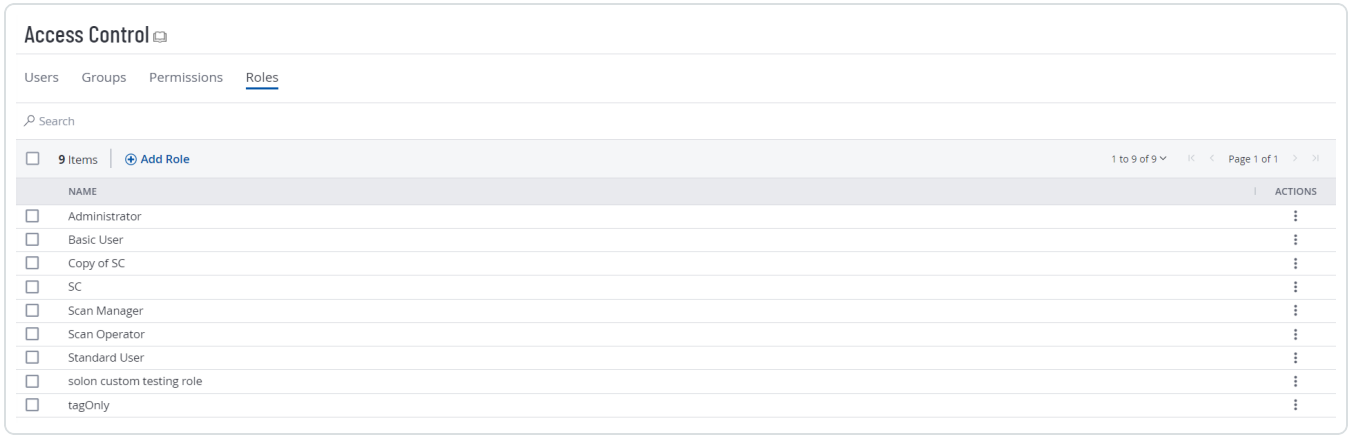
   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Roles** tab.

   The **Roles** page appears. This page contains a table that lists all the user roles available on your Tenable Vulnerability Management instance.



On the **Roles** page, you can complete the following actions:

- Create a Custom Role
- Duplicate a Role
- Edit a Custom Role

- Export Roles
- Delete a Custom Role

Tenable-Provided Roles and Privileges

The following tables describe privileges associated with each Tenable-provided user role, organized by function in their respective product.

Note: You can further refine user access to specific resources by assigning permissions to individual users or groups. For more information, see Permissions.

Tip: The following roles and privileges apply to commercial and Tenable FedRAMP Moderate environments, where appropriate.

Area	Tenable Vulnerability Management-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
Activity Logs	view, export	-	-	-	-
API Keys	view, modify	view, modify	view, modify	view, modify	view, modify
Account Settings	view, modify	view, modify	view, modify	view, modify	view, modify
Agents	view, delete	view, delete	-	-	-
Agent Freeze Windows	view, create, modify, delete	view, create, modify, delete	-	-	-
Agent Groups	view, create, modify, delete	view, create, modify, delete	-	-	-

Area	Tenable Vulnerability Management-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
Agent Settings	view, modify	view, modify	-	-	-
Assets	view, modify, export, delete	view, modify, export, delete	view, modify, export, delete	view, modify, export, delete	view, export
Connectors	view, create, modify, delete	-	-	-	-
Dashboards	view, create, modify, export, delete	view, create, modify, export, delete	view, create, modify, export, delete	view, create, modify, export, delete	view, create, modify, export, delete
Exclusions	view, import, export, delete	view, import, export, delete	-	-	-
Exports	view, modify, export, delete	-	-	-	-
Findings	view, export	view, export	view, export	view, export	view, export
General Settings	view, modify	-	-	-	-
Managed Credentials	view, create, modify, delete	view, create, modify,	view, create, modify,	view, create, modify,	view, create, modify,

Area	Tenable Vulnerability Management-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
		delete	delete	delete	delete
PCI Managing	view, import, export, create, modify, delete	-	-	-	-
Recast Rules	view, create, modify, delete	-	-	-	-
Reports	view, run, create, modify, delete	view, run, create, modify, delete	view, run, create, modify, delete	view, run, create, modify, delete	view
Scan Results	view, export, delete	view, export, delete	view, export, delete	view, export, delete	view, export, delete
Scans[1]	view, import, run, create, modify, delete	view, import, run, create, modify, delete	view, import, run, create, modify, delete	view, import, run, create[2], modify[3], delete	view[4], import
Scanner Groups	view, create, modify, delete	view, create, modify,	-	-	-

[1]User roles determine a user's abilities, but the permissions that a user has for a particular scan are dictated by scan permissions.

[2]Can create scans using existing user-defined policies that are shared with the user.

[3]Can manage scans using existing user-defined policies that are shared with the user.

[4]Can view list of scans, but not scan configuration details.

Area	Tenable Vulnerability Management-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
		delete			
Sensors	view, add, modify, delete	view, add, modify, delete	-	-	-
Shared Collections	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view
Tags[1]	view, create tag category, create tag value, delete, export, assign, unassign	view, create tag value, delete, assign, unassign	view, delete, assign, unassign[2]	view, delete, assign, unassign	view, assign, unassign
User Groups	view, create, modify, delete, export	-	-	-	-
Users	view, create, modify, delete	-	-	-	-

Area	Tenable Web App Scanning-Provided Roles and Privileges					
	Administrator	Scan Manager	Standard	Scan Operator		Basic
Dashboards	view, create,	view,	view,	view,	view	view

[1]Assigning and Unassigning tags can be done from the Asset Details page.

[2]Standard users must have the **Can Use** permission to view, delete, assign, and unassign tags.

Area	Tenable Web App Scanning-Provided Roles and Privileges					
	Administrator	Scan Manager	Standard	Scan Operator		Basic
	modify, delete	create, modify, delete	create, modify, delete	create, modify, delete		
Tenable-Provided Scan Templates	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view	-	-
Scans (also requires scan permissions)	view, import, create, modify, run, delete	view, import, create, modify, run, delete	view, create, modify, run, delete	view, create[1], modify[2], run, delete, move to trash	view	view
Managed Credentials	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete
Scan	view, create,	view,	view,	view,	-	-

[1]Can create scans using existing user-defined policies that are shared with the user.

[2]Can manage scans using existing user-defined policies or user templates that are shared with the user.

Area	Tenable Web App Scanning-Provided Roles and Privileges					
	Administrator	Scan Manager	Standard	Scan Operator		Basic
Permissions	modify, delete[1]	create, modify, delete[2]	create, modify, delete[3]	create, modify, delete[4]		
Scan Results (also requires scan permissions)	view, delete	view, delete	view, delete	view, delete	view, delete	view, delete

Area	Tenable Exposure Management-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
Settings	manage, read	read	read	read	read
Access to Asset Type	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity

[1]Administrator users can create, modify, and delete permissions for scans that any user on the account owns.
[2]Scan Manager users can create, modify, or delete permissions only on scans they own.
[3]Standard users can create, modify, or delete permissions only on scans they own.
[4]Scan Operator users can create, modify, or delete permissions only on scans they own.

Area	Tenable Exposure Management-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
Export	manage own	manage own	manage own	manage own	manage own
Exposure Card	create, share, read	create, share, read	create, share, read	share, read	read
Finding	manage, read	manage, read	read	read	read
Query	search, save	search, save	search, save	search	search
Tag	create, edit	create, edit	-	-	-
Third-Party Connectors	create, manage, read	-	-	-	-

Area	Tenable Identity Exposure-Provided Roles and Privileges	
	Administrator	Custom
Entire Application	Read, Edit, Create	Defined in-application

Area	Tenable Attack Surface Management-Provided Roles and Privileges			
	Business Administrator	Active User	Cloud Connector Manager	View-Only User
Inventory	manage, add, modify, delete	add, modify, leave	add, modify, leave	view
Suggestions	manage, add, modify, delete	manage, add, modify, delete	manage, add, modify, delete	view
Subscriptions	manage, add,	manage, add,	manage, add,	view

	modify, delete	modify, delete	modify, delete	
Dashboard	manage, add, modify, delete	manage, add, modify, delete	manage, add, modify, delete	view
Reports	manage, add, modify, delete	manage, add, modify, delete	manage, add, modify, delete	view
Txt Records	manage, modify, delete	manage, modify, delete	manage, modify, delete	view
Activity Logs	view	view	view	view
User Accounts	manage, modify, delete	-	-	-
Business	manage, modify	-	-	-
Cloud connectors	manage, add, modify, delete	view	manage, add, modify, delete	view

Note: By default, Tenable Attack Surface Management users created within Tenable One are mapped to a user role as documented in the Tenable Attack Surface Management User Guide.

Area	Tenable Cloud Security-Provided Roles and Privileges		
	Administrator	Collaborator	Viewer
Console Tabs	view	view	view
Reports	view, create, schedule, delete	view, create, schedule, delete	view, create
Inventory	view, manage, generate policy	view, manage, generate policy	-
Findings	view, share, manage, disable	view, share, manage	view, share
Administration	view, manage, audit	-	-

Area	Tenable PCI ASV-Provided Roles and Privileges	
	Administrator	Other
Entire Application	view, import, run, create, modify, delete	-

Custom Roles

You can create custom roles for users on your Tenable Vulnerability Management instance to give those users privileges that are specific to your organization's needs.

When you create a custom role, you can add all or some of the following privileges. You can also edit a custom role to remove privileges. Which privileges you can add to or remove from a role depend on the area of Tenable Vulnerability Management where each privilege applies.

> **Note**: A user's access to resources on the account may be limited by their permissions, regardless of their role.

- **Create** – Allows users to create an exposure card or a tag. This privilege is specific to Tenable Exposure Management.
- **Manage** – Allows the user to create, modify, and delete in the area where the privilege applies.

  > **Note**: When you add the **Manage** privilege to a custom role, Tenable automatically adds the **Read** privilege as well. You cannot disable the **Read** privilege unless you first disable the **Manage** privilege.

- **Manage All** – Allows the user to view, modify, and delete exports, including exports that others created.
- **Manage Own** – Allows the user to view, modify, and delete only exports that the user created.
- **Share** – Allows the user to share objects with other users or groups.

  > **Note**: If a custom role does not also have the **Read** permission enabled, they cannot access a list of other users with which to share objects. You can enable this permission in the **Access Control** section of the custom role configuration page.

- **Read** – Allows the user to view items in the area where the privilege applies.
- **Use** – Allows the user to use Tenable-provided scan templates during scan creation.

- **Import** – Allows the user to import Tenable Web App Scanning scan data. For more information, see the *Tenable Web App Scanning User Guide*.
- **Submit PCI** – Allows the user to submit the scan for PCI validation. For more information, see the *Tenable PCI ASV User Guide*.
- **Search** – Allows the user to search for a query where the privilege applies. This privilege is specific to the Attack Path section of Tenable Exposure Management.
- **Save** – Allows the user to save a query where the privilege applies. This privilege is specific to the Attack Path section of Tenable Exposure Management.
- **Cloud Resource** – Allows the user to access assets from **Cloud Resource** data sources. This privilege is specific to Tenable Exposure Management.
- **Computing Resource** – Allows the user to access assets from **Computing Resource** data sources. This privilege is specific to Tenable Exposure Management.
- **Identity** – Allows the user to access assets from **Identity** data sources. This privilege is specific to Tenable Exposure Management.
- **Web Application** – Allows the user to access assets from **Web Application** data sources. This privilege is specific to Tenable Exposure Management.

The following table describes the privilege options available for custom roles in different sections of Tenable Vulnerability Management.

> **Note**: When you create a custom role, you must include **Read** privileges for the **General Settings**, **License**, and **My Account** sections. If you do not include **Read** privileges for these sections, users assigned to the role cannot log in to Tenable Vulnerability Management.

Section	Privilege Options
Platform Settings	
Asset	Read
Findings	Read
My Account	Read, Manage
Access Control	Read, Manage

	Caution: Adding the **Manage** privilege in Access Control allows any user with that custom role to create an Administrator user, log in as that user, and change the privileges or permissions for any user on your Tenable Vulnerability Management instance, including their own. If you want to create a user account with the ability to manage your Access Control configurations, Tenable recommends that you assign that user the Administrator role. For more information, see Tenable-Provided Roles and Privileges.
Access Control Users	Read **Note:** Creating a **Shared Collection** role with the **Manage** privilege also enables the **Access Control UsersRead** privilege.
Activity Log	Read
General Setting	Read, Manage
License Information	Read
Tenable Attack Surface Management	
Business	Manage
Inventory	Manage **Note**: Selecting only the **Inventory** checkbox allows you to manage your inventory, but does not allow you access to the Administrator interface. For more information, see Tenable Attack Surface Management roles in the Tenable Attack Surface Management User Guide.
Vulnerability Management	
Dashboard	Manage, Share **Note**: Custom role privileges in the Dashboards section do not include the ability to export a dashboard. Assign a Tenable-provided role to a user if you want the user to be able to export dashboards.

	Note: All users can view the dashboards they create or that others share with them regardless of the privileges you assign to them.
Export	**Manage All**, **Manage Own**
Recast/Accept Rule	**Read**, **Manage** **Note:** Enabling these Recast/Accept Rule privileges grants access to recast rule operations for Tenable Vulnerability Management, Tenable Web App Scanning, and Host Audit findings.
Web App Scanning	
Web Application Scan	**Read**, **Manage**, **Import**, **Submit PCI** **Note:** For the **Submit PCI** privilege to function properly, you must also enable the **Enable PCI ASV** toggle when creating the custom role.
Tenable-Provided Scan Template	**Use** **Note:** For the **Use** privilege to function properly, you must also enable the **Manage** privilege in the **Web Application Scan** and/or **User-Defined Scan Template** sections.
User-Defined Scan Template	**Read**, **Manage**
Managed Credential	**Read**, **Manage** **Caution:** To restrict managed credential access in Legacy Tenable Web App Scanning, you must deselect the check boxes in this section AND the Managed Credential check boxes in the **Vulnerability Management** > **Scan** section of the custom role creation page. **Note:** In the Legacy Tenable Web App Scanning interface, custom role users must be assigned the **Manage** role to view managed credentials. In the new Tenable Web App Scanning interface, users can view managed credentials with the **Read** role alone.
Recast/Accept	**Read**, **Manage**

Rule	**Note:** Enabling these Recast/Accept Rule privileges grants access to recast rule operations for Tenable Vulnerability Management, Tenable Web App Scanning, and Host Audit findings.
Tenable Exposure Management	
Access to Asset Type	Cloud Resource, Computing Resource, Identity, Web Application
Inventory	Read
Export	Manage Own
Tag	Create, Edit
Export	Manage Own
Finding	Read, Manage
Query	Save, Search
Access to Asset Type	Cloud Resource, Computing Resource, Identity, Web Application
Export	Manage Own
Exposure Card	Read, Create, Share
Settings	Read, Manage
Scan	
Nessus/Agent Scan	Read, Manage, Submit PCI
Scan Exclusion	Read, Manage
Tenable-Provided Scan Template	Use
User-Defined Scan Template	Read, Manage

Managed Credential	**Read**, **Manage**
Target Group	**Read**, **Manage**
Shared Collection	**Read**, **Manage** **Note:** Creating a **Shared Collection** role with the **Manage** privilege also enables the **Access Control Users Read** privilege.

Create a Custom Role

Required User Role: Administrator

Note: Tenable applications do not currently support managing scans and sensors via Custom Roles.

To create a custom role:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Roles** tab.

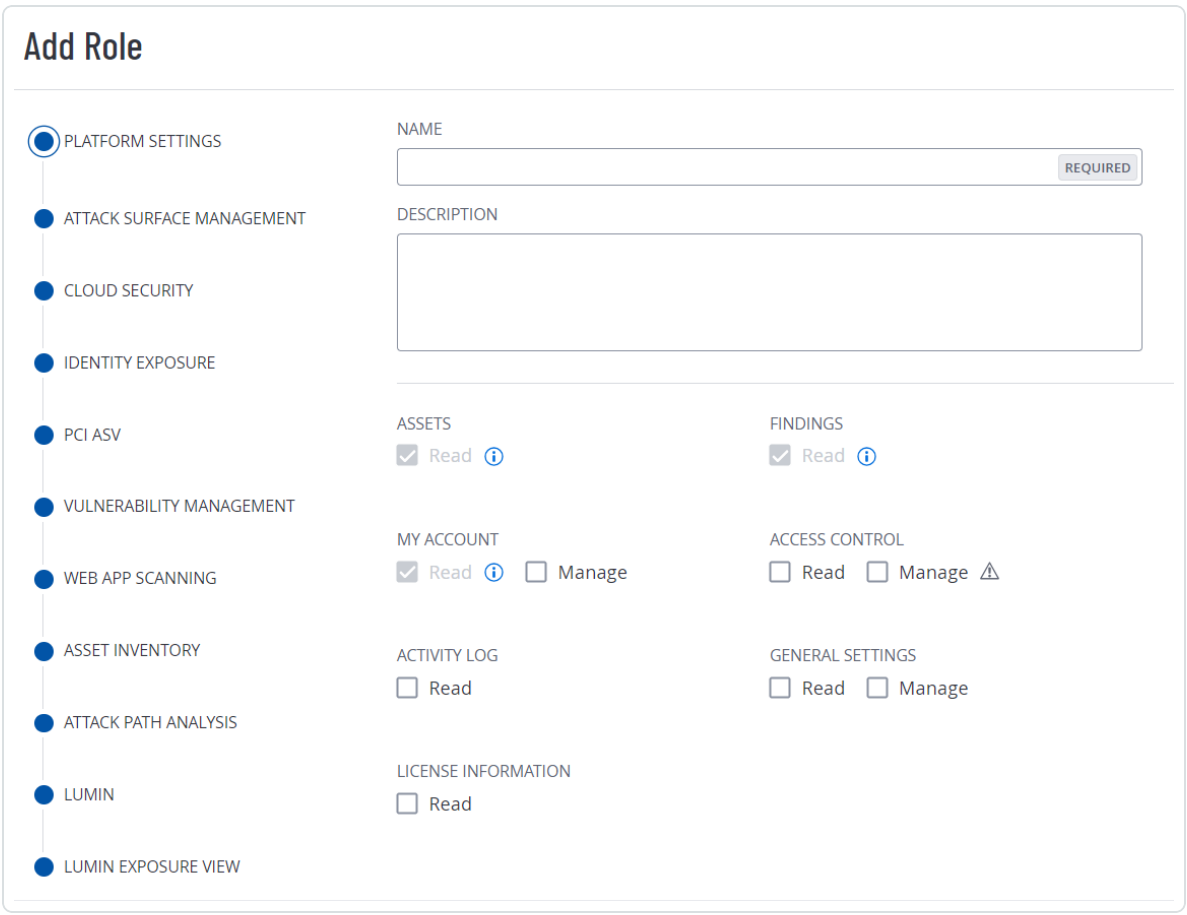
   The **Roles** page appears. This page contains a table that lists all the user roles available on your Tenable Vulnerability Management instance.

4. Do one of the following:

   - Duplicate and modify an existing role.
   - Add a new role:

     a. At the top of the table, click **Add Role**.

        The **Add Role** page appears.



b. In the **Name** box, type a name for your custom role.

c. (Optional) In the **Description** box, type a description for your custom role.

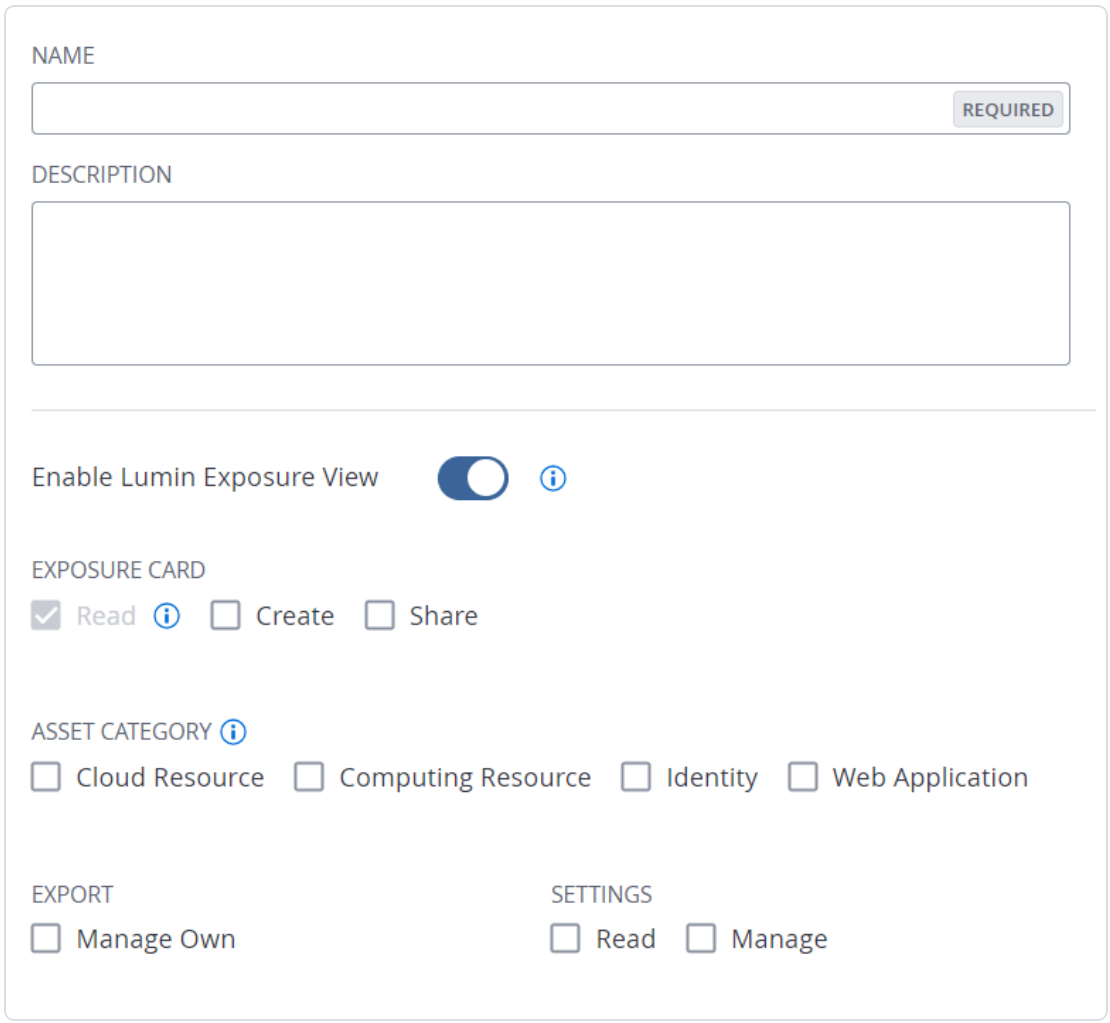
d. Determine the applications to which the custom role has access:

   i. In the left panel, click the application name.

      An **Enable** toggle appears.

   ii. Click the **Enable** toggle to enable or disable access to this application for the custom role you're creating.

      For some applications, privileges associated with the application appear.



iii. Select the checkbox for each privilege you want to add to your custom role. For more information about available privileges, see Custom Roles.

e. Click **Save**.

Tenable Vulnerability Management saves the role and adds it to the roles table.

Duplicate a Role

Required User Role: Administrator

You can create a custom role by duplicating any existing custom role and then modifying the new role configurations as desired.

Note: You cannot duplicate Tenable-provided roles.

To create a custom role via duplication:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Roles** tab.

   The **Roles** page appears. This page contains a table that lists all the user roles available on your Tenable Vulnerability Management instance.

4. In the roles table, select the check box next to the role you want to duplicate.

   The action bar appears at the top of the table.

5. In the action bar, click **More**.

   A menu appears.

6. Click **Duplicate**.

   A copy of the role appears in the table, with the prefix *Copy of* [role name].

7. Click the duplicated role.

   The **Roles Details** page appears. The name, description, and selected privileges for the duplicate role are copied from the original role.

8. Configure the role settings as described in Create a Custom Role.

9. Click **Save**.

   Tenable Vulnerability Management saves your changes to the duplicate role.

Edit a Custom Role

Required User Role: Administrator

Note: Tenable applications do not currently support managing scans and sensors via Custom Roles.

To edit a custom role:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Roles** tab.

   The **Roles** page appears. This page contains a table that lists all the user roles available on your Tenable Vulnerability Management instance.

4. In the roles table, click the role you want to edit.

   The **Roles Details** page appears.

5. Update one or more of the following configurations:

   - Name – In the **Name** box, type a new name for the role.
   - Description – In the **Description** box, type a description for the role.
   - Privileges – Under each Tenable Vulnerability Management area, select or deselect the check box next to each privilege you want to add to or remove from the role.

6. Click **Save**.

   Tenable Vulnerability Management saves your changes.

Delete a Custom Role

Required User Role: Administrator

Note: You can delete only custom roles. You cannot delete Tenable-Provided Roles and Privileges.

To delete a custom role:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Roles** tab.

   The **Roles** page appears. This page contains a table that lists all the user roles available on your Tenable Vulnerability Management instance.

4. In the table, in the **Actions** column, click the ⋮ button next to the role you want to delete.

5. Click the **Delete** 🗑 button.

   Tenable Vulnerability Management deletes the role and removes it from the roles table.

Export Roles

> **Required User Role:** Administrator

On the **Roles** page, you can export one or more user groups in CSV or JSON format.

To export your user roles:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **Roles** tab.

   The **Roles** page appears. This page contains a table that lists all the Tenable-provided and custom roles on your Tenable Vulnerability Management instance.

4. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

5. Do one of the following:

To export a single role:

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

   The action options appear next to your cursor.

   -or-

   In the roles table, in the **Actions** column, click the ⋮ button in the row for the role you want to export.

   The action buttons appear in the row.

b. Click **Export**.

To export multiple roles:

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

   The action bar appears at the top of the table.

b. In the action bar, click [→ **Export**.

> **Note**: You can individually select and export up to 200 roles. If you want to export more than 200 roles, you must select all the roles on your Tenable Vulnerability Management instance by selecting the check box at the top of the roles table and then click [→**Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  > **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.

- A toggle to configure the export schedule.
- A toggle to configure the email notification.

6. In the **Name** box, type a name for the export file.
7. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of roles. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of roles. Empty fields are not included in the JSON file.

8. (Optional) Deselect any fields you do not want to appear in the export file.
9. In the **Expiration** box, type the number of days before the export file expires.

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

10. (Optional) To set a schedule for your export to repeat:
    - Click the **Schedule** toggle.

      The **Schedule** section appears.
    - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
    - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
    - In the **Repeat** drop-down box, select how often you want the export to repeat.

- In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

  > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

11. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

    - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.

    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

12. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

13. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

API Access Security

Tenable Vulnerability Management allows you to restrict access to the Tenable Vulnerability Management API by specifying which IPv4 and/or IPv6 addresses can access the API. For more information about using the API, see the Tenable Vulnerability Management API Explorer documentation.

Caution: Unless your network assignments are restricted to only IPv4 addresses or only IPv6 addresses, you must specify allowed ranges for both IPv4 and IPv6 in order to avoid blocking some API traffic. It is not always predictable whether a given client will connect via IPv4 or IPv6.

To restrict Tenable Vulnerability Management API Access:

1. In the left navigation, click **Settings**.

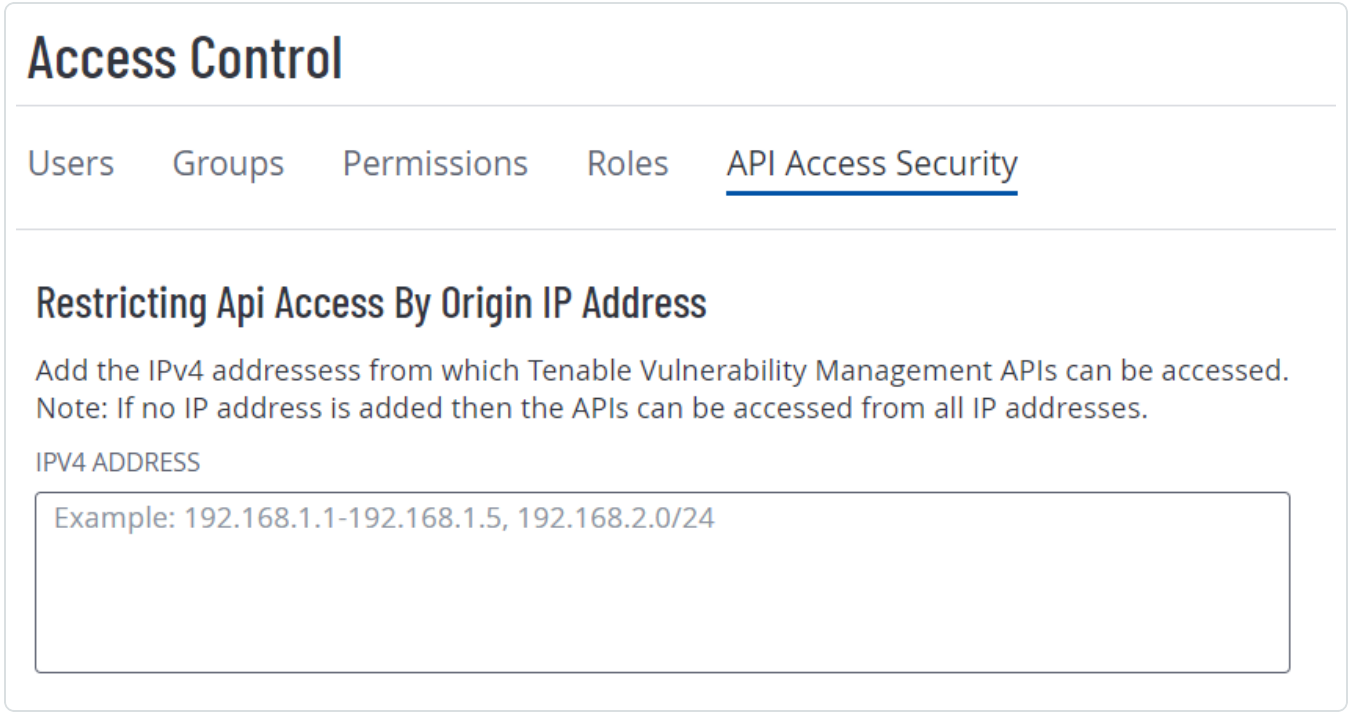
   The **Settings** page appears.

2. Click the **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Vulnerability Management account.

3. Click the **API Access Security** tab.

   The **API Access Security** options appear.



4. In the text box, type the IPv4 addresses to which you want to grant Tenable Vulnerability Management API access.

> **Tip:** The list can include discrete IP addresses, IP address ranges, and IP subnets. For example, `192.0.2.0, 198.51.100.4-198.51.100.10, 203.0.113.0/24` or `2001:db8:2e92:75f2:d40a:e290:10b3:c0f, 2001:db8:1e1f:46a1:e3cb:2110:22c6:0000-2001:db8:1e1f:46a1:e3cb:2110:22c6:ffff, 2001:0DB8::/32`.

5. Click **Save**.

   Tenable Vulnerability Management allows only the specified IPv4 addresses to access the Tenable Vulnerability Management API.

Activity Logs

> **Required User Role:** Administrator

In Tenable Vulnerability Management, the activity logs record user events that take place in your organization's Tenable Vulnerability Management account. For each event, the log includes information about:

- The action taken
- The time at which the action was taken
- The user ID
- The target entity ID

The activity log provides visibility into the actions that users in your organization take in Tenable Vulnerability Management, and can be helpful for identifying security issues and other potential problems. On the **Activity Logs** page, you can view a list of events for all users in your organization's Tenable Vulnerability Management account.

> **Important:** Tenable currently retains activity log data for 3 years, after which it is deleted from the Tenable database.

> **Tip**: To view the audit log via API, use the **Audit Log** endpoint as documented in the Tenable Developer Portal.

Logged Events

Activity log events include the following:

Action	Description
audit.log.view	The system received and processed an audit-log request.
session.create	The system created a session for the user. A user login triggers this event.
session.delete	The session aged out, or the user ended a session.
session.impersonation.end	An administrator ended a session where they impersonated another user.
session.impersonation.start	An administrator started a session where they impersonated another user.
user.authenticate.mfa	Two-factor authentication was successful, and login was allowed.
user.authenticate.password	The user authenticated a session start using a password.
user.create	An administrator created a new user account.
user.delete	An administrator deleted a user account.
user.impersonation.end	An administrator stopped impersonating another user.
user.impersonation.start	An administrator started impersonating another user.
user.logout	The user logged out of their session.
user.update	Either an administrator or the user updated a user account.

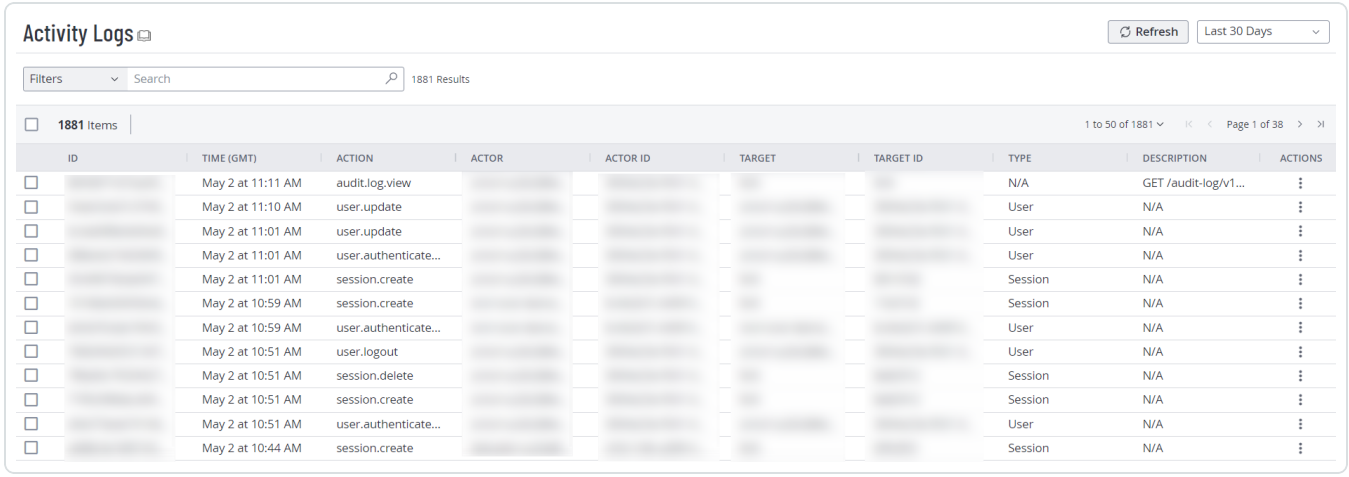
To view your activity logs:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Activity Logs** tile.

   The **Activity Logs** page appears. This page shows a list of activities associated with your organization's Tenable Vulnerability Management account.



3. (Optional) Refine the table data. For more information, see Tables.
4. (Optional) Apply a filter to the table:

Filter	Description
Actor ID	The ID of the account performing the action.
Target ID	The ID of the account affected by the action, if any.
Action	The type of action.
Date	The date the action was performed.

5. (Optional) To refresh the activity logs table, in the upper-right corner, click the **Refresh** button.
6. (Optional) Filter the table by a specific time period:
    - **Last 7 Days**
    - **Last 14 Days**
    - **Last 30 Days**
    - **Last 90 Days**
    - **All**

What to do next:

- (Optional) Export one or more activity logs.

Export Activity Logs

Required User Role: Administrator

On the **Activity Logs** page, you can export one or more activity logs in CSV or JSON format.

To export your activity logs:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Activity Logs** tile.

   The **Activity Logs** page appears. This page shows a list of activities associated with your organization's Tenable Vulnerability Management account.

3. (Optional) Refine the table data. For more information, see Filter a Table.

4. Select the activity logs that you want to export:

Export Scope	Action
Selected activity logs	To export selected activity logs: a. In the activity logs table, select the checkbox for each activity log you want to export. The action bar appears at the top of the table. b. In the action bar, click **Export**. **Note:** The **Export** link is available for up to 200 selections. If you want to export more than 200 activity logs, select all the activity logs in the list and then click **Export**.
A single activity log	To export a single activity log: a. In the activity logs table, right-click the row for the activity log you want to export.

	The action options appear next to your cursor. -or- In the activity logs table, in the **Actions** column, click the ⋮ button in the row for the activity log you want to export. The action buttons appear in the row. b. Click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  > **Note**: By default, all fields are selected.

- A text box to set the number of days before the export ages out.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

5. In the **Name** box, type a name for the export file.
6. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of activity logs. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of activity logs. Empty fields are not included in the JSON file.

7. (Optional) Deselect any fields you do not want to appear in the export file.
8. In the **Expiration** box, type the number of days before the export file ages out.

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

9. (Optional) To set a schedule for your export to repeat:

   - Click the **Schedule** toggle.

     The **Schedule** section appears.

   - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
   - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
   - In the **Repeat** drop-down box, select how often you want the export to repeat.
   - In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

     Note: If you select never, the schedule repeats until you modify or delete the export schedule.

10. (Optional) To send email notifications on completion of the export:

    Note: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

    - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      Note: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

11. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

12. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file from the Exports page.

Access Groups

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Note: System target group permissions that controlled viewing scan results and scanning specified targets have been migrated to access groups. For more information, see Scan Permissions Migration.

With access groups, you can control which users or groups in your organization can:

- View specific assets and related vulnerabilities in aggregated scan result views.
- Run scans against specific targets and view individual scan results for the targets.

An access group contains assets or targets as defined by the rules you set. Access group rules specify identifying attributes that Tenable Vulnerability Management uses to associate assets or targets with the group (for example, an AWS Account ID, FQDN, or IP address). By assigning permissions in the access group to users or user groups, you grant the users view or scan permissions for assets or targets associated with the access group.

Note: When you create or edit an access group, Tenable Vulnerability Management may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.

You can view the status of this assignment process in the **Status** column of the access groups table on the **Access Groups** page.

Only administrators can view, create, and edit access groups. As a user assigned any other role, you can see the access groups to which you belong and the related rules, but not the other users that are in the access group.

> **Note**: The **Access Group** tile appears only if you have one or more assigned access groups or if you are an administrator and users on your Tenable Vulnerability Management are assigned to access groups. Once you convert all your access groups to permission configurations, the **Access Group** tile will no longer appear on your account.

By default, all users have **No Access** to all assets on your Tenable Vulnerability Management instance. Therefore, if you want to assign permissions for assets, you must create an access group and configure user permissions for the group.

> **Note:** Tenable Vulnerability Management applies dynamic tags to any assets, regardless of access group scoping. As a result, it may apply tags you create to assets outside of the access groups to which you belong.

Your organization can create up to 5,000 access groups.

Transition to Permission Configurations

> **Required User Role:** Administrator

> Tenable is converting all access groups into permission configurations. As this conversion runs, you may notice your existing access groups undergoing changes. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance. For more information, see Transition to Permission Configurations.

Tenable Vulnerability Management has consolidated and moved user and group management to the **Access Control** page to make access management more intuitive and efficient.

As part of this effort, Tenable Vulnerability Management is replacing Access Groups with Permissions, a feature that allows you to create permission configurations. These permission configurations use tags to determine which users and groups on your Tenable Vulnerability Management instance can perform specific tasks with your organization's resources.

Previously, you had to create access groups to customize access settings for users on your instance. When you create a permission configuration, you can view and manage access settings for users and groups on the **Access Control** page, where you manage users and groups.

Tenable Vulnerability Management plans to retire access groups once all existing access groups are converted into permissible configurations. Tenable Vulnerability Management encourages you to use permission configurations to manage user access to your resources.

What to Expect

As Tenable Vulnerability Management converts your access group data into permission configurations, you may notice the following changes:

- Tenable Vulnerability Management has split up your access groups that have more than one access group type and recreated them as separate groups based on type. For more information about access group types, see Access Group Types.
- Tenable Vulnerability Management has converted all your **Scan Target** type access groups into **Manage Assets** type access groups.
- Tenable Vulnerability Management has updated access group rule filters to match tag rule filters and operators.
- For each access group on your instance that is based on rules instead of tags, Tenable Vulnerability Management has created tags based on the access group rules and updated the groups to reference the new tags. For more information about tag rules, see Tag Rules.
- For each access group on your install, Tenable Vulnerability Management has created permission configurations based on the rules and user permissions defined in that access group.

Task Parity

The following table lists common tasks you may perform on the **Access Groups** page and their equivalent tasks on the **Permissions** page.

Access Groups	Permissions
Create an Access Group	Create and Add a Permission Configuration
View Your Assigned Access Groups	View Your Account Details
Edit an Access Group	Edit a Permission Configuration
Configure User Permissions for an	• Add a Permission Configuration to a User or

Access Group	Groups • Remove a Permission Configuration from a User or Group
Delete an Access Group	Delete a Permission Configuration

Convert an Access Group to a Permission Configuration

Required User Role: Administrator

Tenable is converting all access groups into permission configurations. As this conversion runs, you may notice your existing access groups undergoing changes. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance. For more information, see Transition to Permission Configurations.

On the **Access Groups** page, you can convert your existing access groups into permission configurations.

Note: Once you convert an access group into a permission configuration, you cannot revert the converted permission configuration into an access group.

Note: The **Access Group** tile appears only if you have one or more assigned access groups or if you are an administrator and users on your Tenable Vulnerability Management are assigned to access groups. Once you convert all your access groups to permission configurations, the **Access Group** tile will no longer appear on your account.

To convert an access group into a permission configuration:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Groups** tile.

   The **Access Groups** page appears. This page contains a table that lists the access groups to which you have access.

3. In the access groups table, select the check box for the access group you want to convert.

   The action bar appears at the top of the table.

4. Click **Migrate To Permissions**.

   A confirmation message appears.

5. In the confirmation window, click **Migrate To Permissions**.

   Tenable Vulnerability Management begins converting your access group into a permission configuration.

   Tenable Vulnerability Management updates the **Status** column for the access group to reflect the current migration status.

Access Group Types

> Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

You can create the following types of access groups. Select an access group type based on the identifiers for the targets you want to scan.

Type	Description
Manage Assets	Users can view the asset records created during previous scans and scan the associated targets for those assets. Use this type of access group if the targets you want to view and scan have been scanned before and can be best identified using tags based on asset attributes (for example, operating system or AWS Account ID).
Scan Targets	Users can scan targets associated with the access group and view the results of those scans. Use this type of access group if the targets you want to view and scan have never been scanned before and can only be identified using certain asset identifiers (specifically, FQDN, IPv4 address, or IPv6 address).

> **Note:** The access group type names do not represent a limitation on the user actions that each group controls in relation to the specified targets. For both **Manage Assets** and **Scan Targets** groups, you can grant user permissions to view analytical results for the specified targets in dashboards, to scan the

specified targets, or to both view and scan. For more information on user permissions, see Configure User Permissions for an Access Group.

Tip: You can add a user to both access group types if you want to allow the user to scan both types of scan targets.

Restrict Users for All Assets Group

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

The **All Assets** group is the default, system-generated access group to which all assets belong.

By default, the following conditions are true:

- The **All Users** user group, which contains all users in your organization, is assigned to the **All Assets** access group.
- The permissions for the **All Users** group are set to **Can View** and **Can Scan**.

If you do not want all users to scan all assets and view the individual and aggregated results, you must set the permissions for the **All Users** group to **No Access**. Optionally, you can then add specific users or to provide individuals with access to all assets.

Note: When you create or edit an access group, Tenable Vulnerability Management may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.

You can view the status of this assignment process in the **Status** column of the access groups table on the **Access Groups** page.

To restrict user permissions for the **All Assets** group:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Groups** tile.

   The **Access Groups** page appears. This page contains a table that lists the access groups to which you have access.

3. In the access groups table, click the **All Assets** group.

   The **Edit All Assets Access Group** page appears.

4. In the **Users & Groups** section, locate the listing for the **All Users** group.

5. Remove both the **Can Edit** and **Can Scan** labels from the **All Users** group listing:

   a. Roll over the label.

      The ✕ button appears on the label.

   b. Click the ✕ button.

      Tenable Vulnerability Management removes the label.

   Note: When configuring permissions for the **All Users** user group, Tenable recommends keeping the following in mind:

   - If you retain the permissions for **All Assets** as **Can View**, all users can view scan results for all assets or targets for your organization.
   - If you set the permissions for **All Assets** to **Can Scan**, all users can scan all assets or targets for your organization and view the related scan results.

6. (Optional) Configure user permissions for each user or group you want to add to the **All Assets** group.

7. Click **Save**.

   The **Access Groups** page appears. Access to the **All Assets** group is restricted to the user(s) or group(s) you added.

Create an Access Group

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

You can create an access group to group assets based on rules, using information such as an AWS Account ID, FQDN, IP address, and other identifying attributes. You can then assign permissions for users or user groups to view or scan the assets in the access group.

To create an access group:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Groups** tile.

   The **Access Groups** page appears. This page contains a table that lists the access groups to which you have access.

3. In the upper-right corner of the page, click the **Create Access Group** button.

   The **Create Access Group** page appears.

4. In the **General** section, in the **Name** box, type a name for the access group.

   Note: The name must be unique within your organization.

5. In the **Type** section, select the appropriate access group type based on the type of targets you want to scan.

   If you create an access group of one type, then change the type during configuration, Tenable Vulnerability Management prompts you to confirm the action. If you confirm, Tenable Vulnerability Management clears any previously added rule filters.

6. In the **Rules** section, add rules for the access group.

   Access group rules specify the conditions Tenable Vulnerability Management evaluates when determining whether to include assets or targets in the access group.

   Note: You can add up to 1,000 rules per access group.

a. In the **Category** drop-down box, select an attribute to filter assets or targets.

b. In the **Operator** drop-down box, select an operator.

Possible operators include:

• **is equal to**: Tenable Vulnerability Management matches the rule to assets or targets based on an exact match of the specified term.

> **Note:** Tenable Vulnerability Management interprets the operator as 'equals' for rules that specify a single IPv4 address, but interprets the operator as 'contains' for rules that specify an IPv4 range or CIDR range.

• **contains**: Tenable Vulnerability Management matches the rule to assets or targets based on a partial match of the specified term.

• **starts with**: Tenable Vulnerability Management matches the rule to assets or targets that start with the specified term.

• **ends with**: Tenable Vulnerability Management matches the rule to assets or targets that end with the specified term.

c. In the text box, type a valid value for the selected category.

> **Tip:** You can enter multiple values separated by commas. For **IPV4 Address**, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

d. (Optional) To add another rule, click the ⊕ **Add** button.

> **Note:** If you configure multiple rules for an access group, the access group includes assets or targets that match *any* of the rules. For example, if you configure two rules -- one that matches on the **Network Name** attribute and one that matches on **IPv4 Address**, the access group includes any assets in the specified network, plus any asset with the specified IPv4 address, regardless of whether that asset belongs to the specified network.

7. In the **Users & Groups** section, configure user permissions for the access group.

8. Click **Save**.

Tenable Vulnerability Management creates the access group. The **Access Groups** page appears.

> **Note:** When you create or edit an access group, Tenable Vulnerability Management may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.
>
> You can view the status of this assignment process in the **Status** column of the access groups table on the **Access Groups** page.

Configure User Permissions for an Access Group

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

You can configure access group permissions for individual users or a user group. If you configure access group permissions for a group, you assign all users in that group the same permissions. For more information, see User Groups.

You can assign the following access group permissions to a user or user group:

- **No Access** – (**All Users** user group only) No users (except for users or groups you specifically assign permissions) can scan the assets or targets specified in the access group. Also, no users can view related individual or aggregated scan results for the specified assets or targets.
- **Can View** – The user's view in aggregated scan results (workbenches/dashboards) includes data from scans of the assets or targets specified in the access group. If you assign this permission to the **All Users** group for the access group, all users can view aggregated scan results for the assets or targets in the access group.
- **Can Scan** – Users can scan assets or targets specified in the access group and view individual scan results for the assets or targets. If you do not have this permission, Tenable Vulnerability Management does not prevent you from configuring a scan using assets or targets specified in the access group; however, the scanner does not scan the assets or targets. If you assign this permission to the **All Users** group for the access group, all users can scan the assets or targets in the access group and view the related individual scan results.

User permissions in an access group are cumulative, rather than hierarchical. To allow a user to scan an asset or target *and* view results for that asset or target in aggregated results, you must set the user's permissions in the access group to both **Can View** and **Can Scan**.

Tip: To run scans auditing cloud infrastructure, configure a **Scan Target** access group that includes the target 127.0.0.1, and set user permissions to **Can Scan**.

To configure user permissions for an access group:

1. Create or edit an access group.
2. In the **Users & Groups** section, do any of the following:
   - Edit permissions for the **All Users** user group.

     The default values for the **All Users** user group depends on the access group:

     - For the **All Assets** access group, Tenable Vulnerability Management assigns **Can View** and **Can Scan** permissions to the **All Users** group by default. Tenable recommends you restrict these permissions during initial configuration.
     - For all other access groups, Tenable Vulnerability Management assigns **No Access** permissions to the **All Users** group by default. For these access groups, set permissions for the **All Users** group as follows:
       a. Next to the permission drop-down for the **All Users** group, click the button.
       b. Click **Can View**.
       c. Next to the permission drop-down, click the button again.
       d. Click **Can Scan**.
       e. Click **Save**.

       Tenable Vulnerability Management allows any user to view or scan the assets or targets in the group.
   - Add a user to the access group.

a. In the search box, type the name of a user or group.

   As you type, a filtered list of users and groups appears.

b. Select a user or group from the search results.

   Tenable Vulnerability Management adds the user to the access group with the default **Can View** permissions and adds the related label to the user listing.

c. (Optional) Add **Can Scan** permissions for the user.

   i. Next to the permission drop-down for the user or group, click the ⌄ button.

   ii. Click **Can Scan**.

   Tenable Vulnerability Management adds a **Can Scan** label to the user listing.

d. Click **Save**.

   Tenable Vulnerability Management adds the user to the access group.

- Add permissions for an existing user.

a. Locate the user or group you want to edit.

b. Next to the permission drop-down for the user or group, click the ⌄ button.

c. Click **Can View** or **Can Scan** as appropriate.

   Tenable Vulnerability Management adds a label representing the new permission to the user listing.

d. Click **Save**.

   Tenable Vulnerability Management saves your changes to the access group.

- Remove permissions from an existing user.

a. Locate the user or group you want to edit.

b. In the label representing the permission you want to remove, click the ✕ button.

   Tenable Vulnerability Management removes the permission label from the user listing.

If you remove the last permission for the **All Users** group, Tenable Vulnerability Management sets the group permissions to **No Access**.

If you remove the last permission for an individual user or group, Tenable Vulnerability Management prompts you to remove the user from the access group.

- Remove a user from the access group.
  a. Click the ✕ button next to the user or user group you want to delete.

     The user or group disappears from the **Users & Groups** list.

  b. Click **Save**.

     Tenable Vulnerability Management saves your changes to the access group.

Edit an Access Group

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

You can edit rules for an existing access group, as well as add or remove users and user groups assigned to the access group.

Note: You cannot edit the name or rules for the system-generated **All Assets** access group.

To edit an access group:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Access Groups** tile.

   The **Access Groups** page appears. This page contains a table that lists the access groups to which you have access.

3. In the access groups table, click the access group you want to edit.

   The **Edit Access Group** page appears.

4. In the **General** section, in the **Name** box, type a new name for the access group.

5. In the **Type** section, edit the access group type.

   a. Select the access group type to which you want to change.

      Tenable Vulnerability Management prompts you to confirm the action.

   b. Click **Confirm**.

      Tenable Vulnerability Management clears any previously added rule filters.

6. In the **Rules** section, edit the access group rules.

   Access group rules specify the conditions Tenable Vulnerability Management evaluates when determining whether to include assets or targets in the access group.

   - To edit an existing rule, modify the category, operator, and/or value as needed.
   - To delete an existing rule, click the ✕ button next to the rule.
   - To add a new rule, click ⊕ **Add** and create a new rule.

7. In the **Users & Groups** section, configure user permissions for the access group.

8. Click **Save**.

   Tenable Vulnerability Management updates the access group with your changes. The **Access Groups** page appears.

   > **Note:** When you create or edit an access group, Tenable Vulnerability Management may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.
   >
   > You can view the status of this assignment process in the **Status** column of the access groups table on the **Access Groups** page.

View Assets Not Assigned to an Access Group

> Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that

you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

If an asset does not match any access group rules, Tenable Vulnerability Management does not assign the asset to any access group. These unassigned assets are only visible to users in the **All Assets** group. If your organization limits membership in the **All Assets** group, users who are not members of the **All Assets** group are unable to see these unassigned assets, but this limited visibility may not be immediately obvious to them. If you are a member of the **All Assets** group, you can use a filter to identify these unassigned assets.

To view assets that are not assigned to an access group:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Asset View** section, click **Assets**.

   The **Assets** page appears.

3. Create a filter with the following settings:

   - Category: **Belongs to Access Group**
   - Operator: **is equal to**
   - Value: **false**

4. Click **Apply**.

   The assets table updates to display all assets that are not assigned to an access group.

View Your Assigned Access Groups

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

As an administrator, you can view the rules and assigned users and user groups for any access group. You can also edit access group parameters.

As a user in any other role, you can view your assigned access groups. This view includes the rules associated with each access group, but excludes the other users or user groups assigned to the access group. You cannot edit any access group settings.

Note: The **Access Group** tile appears only if you have one or more assigned access groups or if you are an administrator and users on your Tenable Vulnerability Management are assigned to access groups. Once you convert all your access groups to permission configurations, the **Access Group** tile will no longer appear on your account.

To view your assigned access groups:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Access Groups** tile.

   The **Access Groups** page appears. This page contains a table that lists the access groups to which you have access.

3. The **Access Groups** page contains a table that includes the following information:

   - **Name** – The access group name.
   - **Owner** – The access group owner.
   - **Permission Type** – The access group type.
   - **Last Modified** – The date on which a user in your organization last changed the access group configuration.
   - **Last Modified By** – The user in your organization who last changed the access group configuration.

- **Status** – The status of the Tenable Vulnerability Management process matching assets to the access group. Possible values are **Processing** or **Completed**. To view the percentage complete for an ongoing process, roll over the Processing status.

4. (Optional) Click an access group to view more details.

   The **Edit Access Group** page appears.

   For administrators, this page contains both rules and assigned users and user groups, and you can edit all access group parameters.

   For users in any other role, this page contains rules only, and you cannot edit the rules.

Delete an Access Group

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

Note: You cannot delete the system-generated **All Assets** group.

To delete one or more access groups:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Access Groups** tile.

   The **Access Groups** page appears. This page contains a table that lists the access groups to which you have access.

3. Select the access groups you want to delete:

- Select a single access group:

  a. In the access groups table, roll over the access group you want to delete.

     The action buttons appear in the row.

  b. Click the button.

     A confirmation window appears.

- Select multiple access groups:

  a. In the access groups table, select the check boxes next to the access groups you want to delete.

     The action bar appears at the bottom of the page.

  b. In the action bar, click the button.

     A confirmation window appears.

4. In the confirmation window, click the **Delete** button.

   Tenable Vulnerability Management deletes the selected access group or groups and updates the access group table.

Access Group Rule Filters

> Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

You can use the filters described in the following sections to create rules for access groups. For more information, see:

- Tenable-provided Filters
- Guidelines for Tenable-provided Filters
- Tag Filters

Tenable-provided Filters

The last two columns in the following table indicate whether you can use the filter with the **Manage Assets** or **Scan Targets** group type.

Filter	Description	Manage Assets	Scan Targets
AWS Account ID	The canonical user identifier for the Amazon Web Services (AWS) account associated with the asset. For more information, see "AWS Account Identifiers" in the AWS documentation.	yes	no
AWS Availability Zone	The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see "Regions and Availability Zones" in the AWS documentation.	yes	no
AWS EC2 AMI ID	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.	yes	no
AWS EC2 Instance ID	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.	yes	no
AWS EC2 Name	The name of the virtual machine instance in Amazon EC2.	yes	no
AWS EC2 Product Code	The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2.	yes	no
AWS Region	The region where AWS hosts the virtual machine instance, for example, 'us-east-1'. For more information, see	yes	no

	"Regions and Availability Zones" in the AWS documentation.		
AWS Security Group	The security group to which you have assigned the virtual machine instance in Amazon EC2. For more information, see Security Groups in the Amazon Virtual Private Cloud User Guide.	yes	no
AWS Subnet ID	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.	yes	no
AWS VPC ID	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.	yes	no
Azure Resource ID	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.	yes	no
Azure VM ID	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see "Accessing and Using Azure VM Unique ID" in the Microsoft Azure documentation.	yes	no
FQDN/Hostname	One of the following: • The fully-qualified domain name of the asset. • The hostname of the asset.	yes	yes
Google Cloud	The unique identifier of the virtual	yes	no

Instance ID	machine instance in Google Cloud Platform (GCP).		
Google Cloud Project ID	The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see "Creating and Managing Projects" in the GCP documentation.	yes	no
Google Cloud Zone	The zone where the virtual machine instance runs in GCP. For more information, see "Regions and Zones" in the GCP documentation.	yes	no
IPv4 Address	An IPv4 address for the asset. For this filter, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).	yes	yes
IPv6 Address	An IPv6 address for the asset.	no	yes
MAC Address	The MAC address of the asset.	yes	no
NetBIOS Name	The NetBIOS name for the asset.	yes	no
Network Name	The name of the network to which the asset belongs.	yes	no
Operating System	The operating system installed on the asset.	yes	no
Qualys Asset ID	The Asset ID of the asset in Qualys. For more information, see the Qualys documentation.	yes	no
Qualys Host ID	The Host ID of the asset in Qualys. For more information, see the Qualys	yes	no

	documentation.		
ServiceNow Sys ID	The unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.	yes	no

Guidelines for Tenable-provided Filters

- When configuring rules for **Scan Targets** access groups, the asset attribute type must match the target format used in the related scan. For example, if a **Scan Targets** access group rule filters on the **FQDN/Hostname** attribute, the related scan succeeds if the scan target is specified in FQDN or hostname format, but fails if the scan target is specified in IPv4 address format.

Tag Filters

In Tenable Vulnerability Management, tags allow you to add descriptive metadata to assets that helps you group assets by business context. For more information, see Tags.

You can use the tags you create to assign assets to **Manage Assets** access groups.

To add a tag filter to a rule:

1. In the **Category** drop-down box, select **Tags**.
2. In the **Operator** drop-down box, select **contains**.
3. In the text box, type the tag category and value you want to search for in the following format:

   ```
   Category Name:Value Name
   ```

4. Continue creating rules and/or save the access group as described in Create an Access Group.

Note: Tag categories with 100,000 or more associated values cannot be applied as a rule to access groups.

Scan Permissions Migration

System target group permissions that controlled whether users can scan specified targets have been migrated to access groups.

> **Note**: Tenable plans to deprecate access groups in the near future. Currently, you can still create and manage access groups. However, Tenable recommends that you instead use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance.

This migration affects your existing Tenable Vulnerability Management configuration as follows:

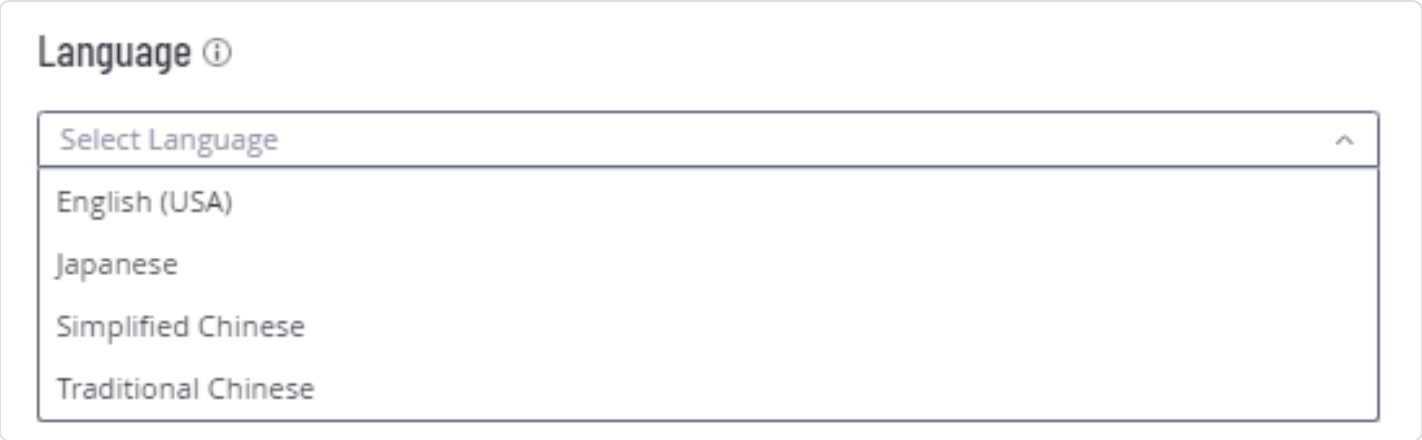
Component	Action
Existing access group	Tenable Vulnerability Management: • Updates any existing access group to an access group of the **Manage Assets** type. • Replaces the **All Users** toggle with a default **All Users** group. • Assigns **Can View** permissions to any existing users or user groups that currently have view access.
Existing system target groups	For each existing system target group, Tenable Vulnerability Management: • Creates a new access group with a type of **Scan Targets**. This access group specifies the same scan targets as the existing system target group. Tenable Vulnerability Management lists `migration` as the owner of the migrated access groups. • Moves any user with **Can Scan** permissions in the system target group to the new access group, and assigns the user **Can Scan** permissions for that access group. To ensure users can view results for the targets, configure **Can View** permissions for users in the access group. **Note:** This migration does *not* delete existing system target groups. The migration removes only the **Can Scan** permissions from the system target groups. **Note:** If, at the time of migration, an existing target group includes scan

	permissions, a **Scan** label may appear for the group in the **Permissions** column of the target groups table in the new Tenable Vulnerability Management user interface. This label indicates historical scan permissions only; access groups specify the current scan permissions.
Existing scan configurations, dashboard filters, and saved searches	Existing scan configurations retain the system target group as a target setting. Existing dashboard filters and saved searches retain the system target group as a filter setting. If you have **Can Use** permissions for a system target group, you can continue to use the system target group to specify a group of targets in a scan configuration and to use the system target group in filters for dashboards and searches. However, to specify which users can view scan results for the targets, configure **Can View** permissions in the appropriate access group.

Language

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Language** page, you can change the user interface language in your Tenable Vulnerability Management container. This setting only affects your own user account.



To change the user interface language:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Language** tile.

   The **Language** tile appears.

3. Under **User Interface Language**, select the language you want to switch to.

   Tenable Vulnerability Management updates the user interface language for your account.

Exports

From the **Exports** page, you can view and configure your Scheduled Exports and Export Activity.

To view the **Exports** page, do one of the following:

1. In the left navigation, click **Exports**.

   The **Exports** page appears.

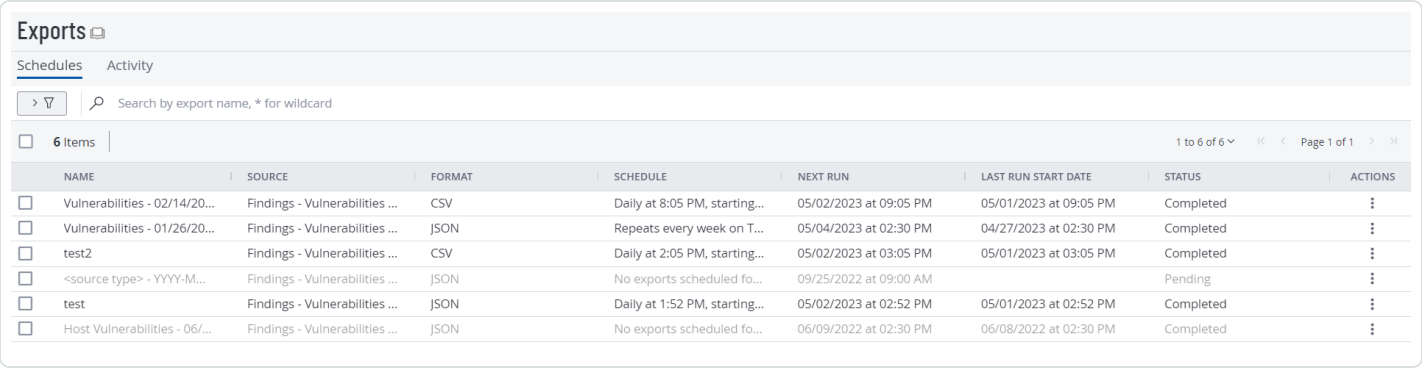
-or-

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears.



Export information on this page comes from the following sources:

- **Assets** – Information about all assets included on your Tenable Vulnerability Management license. For more information, see Export Findings or Assets.
- **Assets Host** –Information about assets Tenable Vulnerability Management identified on your host during a scan. For more information, see Host Assets and Export Findings or Assets.
- **Findings - Vulnerabilities - Host** – Information about the vulnerability findings Tenable Vulnerability Management identified on your host during a scan. For more information, see Export Findings or Assets.
- **Users** – Information about the users assigned to your account. For more information, see Export Users.

For more information, see the following topics:

Scheduled Exports

The **Scheduled Export** page displays details about the exports on your account that include a schedule.

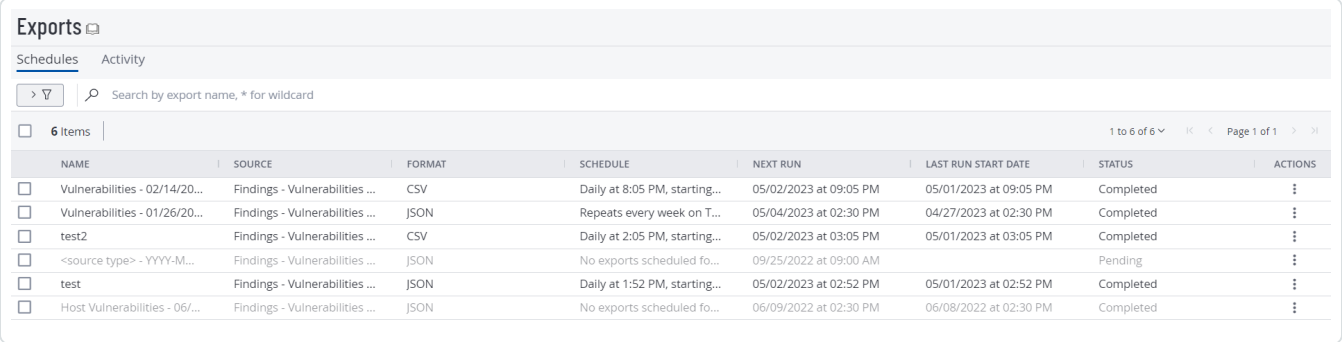
> **Note**: You can retain up to 1000 export schedules on your Tenable Vulnerability Management instance.

To view your scheduled reports export:

- In the left navigation, click **Export**.

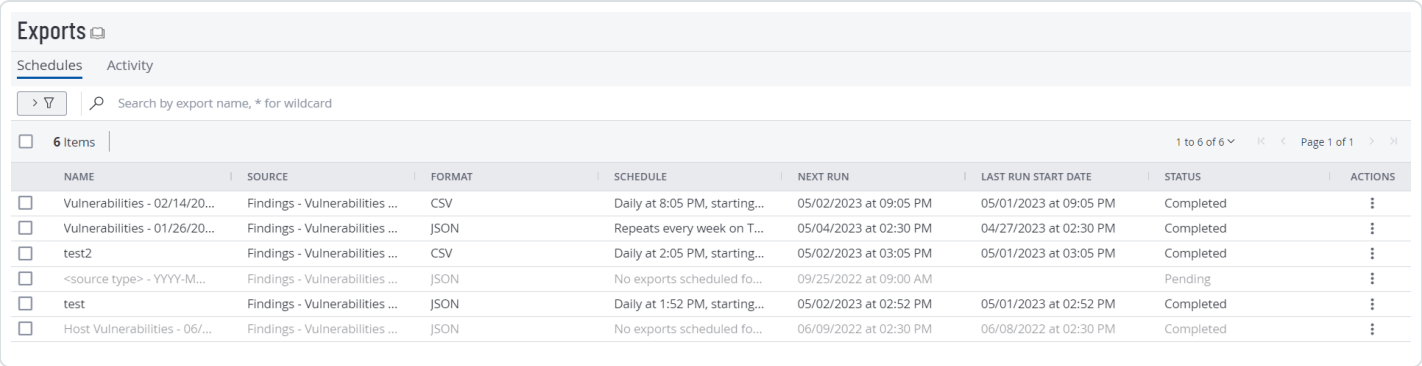
  The **Export** page appears.

  The **Schedules** tab shows by default.



Export information on this page comes from the following sources:

- **Assets** – Information about all assets included on your Tenable Vulnerability Management license. For more information, see Export Findings or Assets.
- **Assets Host** –Information about assets Tenable Vulnerability Management identified on your host during a scan. For more information, see Host Assets and Export Findings or Assets.
- **Findings - Vulnerabilities - Host** – Information about the vulnerability findings Tenable Vulnerability Management identified on your host during a scan. For more information, see Export Findings or Assets.
- **Users** – Information about the users assigned to your account. For more information, see Export Users.



On the **Scheduled Exports** page, you can do the following:

- View Your Scheduled Exports
- Disable a Scheduled Export
- Enable a Disabled Scheduled Export
- Edit a Scheduled Export
- Delete a Scheduled Export

Note: Export expiration is set via the **Settings** section. For more information, see General Settings.

View Your Scheduled Exports

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Exports** page, you can view all the scheduled exports on your account.

Note: You can retain up to 1000 export schedules on your Tenable Vulnerability Management instance.

To view your scheduled exports:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

Schedules Table

The **Schedules** table contains the following information about your scheduled exports:

Column	Description
Name	The name of the scheduled export file.
Source	The data source for the scheduled export in Tenable Vulnerability Management. Possible sources include: • **Assets** – Information about all assets included on your Tenable Vulnerability Management license. • **Assets Host** –Information about assets Tenable Vulnerability Management identified on your host during a scan. • **Findings - Vulnerabilities - Host** – Information about the vulnerability findings Tenable Vulnerability Management identified on your host during a scan. • **Users** – Information about the users assigned to your account.
Format	The format of the export file, either CSV or JSON.
Schedule	The date, time, and frequency on which your export runs.
Next Run	The date and time when the export is scheduled to run next.

Last Run Start Date	The date and time when Tenable Vulnerability Management last began the export.
Status	The status of the most recent scheduled export.
Actions	The actions you can perform with the scheduled export, including the following: • Disable one or more scheduled exports. • Enable one or more disabled scheduled exports. • Delete one or more scheduled exports.

Disable a Scheduled Export

Required User Role: Administrator

Disabling an scheduled export prevents Tenable Vulnerability Management from automatically creating exports based on the export schedule. You can enable a disabled scheduled export, as described in Enable a Disabled Scheduled Export.

Note: Disabling a scheduled export does not remove the scheduled export from the **Schedules** table or from the list of exports that count against your 1000 scheduled export limit. To remove a scheduled export from your account, you must delete the scheduled export.

To disable a scheduled export:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

4. Do one of the following:

   #### To disable a single scheduled export:

a. In the **Schedules** table, in the row for the scheduled export you want to disable, click the ⋮ button.

   The action buttons appear in the row.

b. In the row, click the ⊘ **Disable** button.

To disable multiple scheduled exports:

a. In the **Schedules** table, select the check box for each scheduled export you want to disable.

   > **Note**: You can disable up to 10 export schedules simultaneously.

   The action bar appears at the top of the table.

b. In the action bar, click the ⊘ **Disable** button.

A success message appears.

Tenable Vulnerability Management disables the selected scheduled export or exports.

In the **Schedules** table, disabled scheduled exports appear in gray.

Enable a Disabled Scheduled Export

> **Required User Role:** Administrator

When you disable a scheduled export, you can enable the scheduled export again to resume the export cadence specified in the schedule.

To enable a disabled scheduled export:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

4. Do one of the following:

To enable a single scheduled export:

a. In the **Schedules** table, in the row for the scheduled export you want to enable, click the ⋮ button.

   The action buttons appear in the row.

b. In the row, click the ✓ **Enable** button.

To enable multiple scheduled exports:

a. In the **Schedules** table, select the check box for each disabled scheduled export that you want to enable.

   > **Note**: You can enable up to 10 export schedules simultaneously.

   The action bar appears at the top of the table.

b. In the action bar, click the ✓ **Enable** button.

A success message appears.

Tenable Vulnerability Management enables the selected scheduled export or schedules.

In the **Schedules** table, enabled scheduled exports appear in black.

Edit a Scheduled Export

> **Required User Role:** Administrator

On the **Exports** page, you can edit a scheduled export, as long as the export job is not currently running. If you are not a Tenable administrator, you can only edit exports you have created.

To edit a scheduled export:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. On the right, in the actions menu ⋮ click **Edit** .

   The **Export** plane appears.

4. Edit the export options as follows.

Option	Description
Name	Type a custom name for your export.
Formats	Select an export format: • **CSV** – A CSV file that you can open in a spreadsheet application such as Microsoft Excel. **Note**: For findings exports, Tenable Vulnerability Management automatically trims cells longer than 32,000 characters so they appear correctly in Microsoft Excel. Select **Untruncated Data** to disable this. **Note:** If your export file contains a cell that starts with any of the following characters (=, +, -, @), Tenable Vulnerability Management adds a single quote (') at the beginning of the cell. For more information, see the Knowledge Base. • **JSON** – A JSON file containing a nested list of findings, with no empty fields.
Configurations	Select the fields to include: • Under **Select Field Set**, search for or select the fields to add to your export. • To view only selected fields, click **View Selected**. • In the **Expiration** box, type the number of days before the export file ages out.
Schedule	Turn on the **Schedule** toggle to schedule your export: a. In the **Start Date and Time** section, choose the date and time

	for the export. b. In the **Time Zone** drop-down, choose a time zone. c. In the **Repeat** drop-down, choose the cadence on which you want the export to repeat (for example, daily). d. In the **Repeat Ends** drop-down, choose the date when exports end. If you select **Never**, the export repeats until you modify or delete it.
Email Notifications	Turn on the **Email Notification** toggle to send email notifications: a. In the **Add Recipients** box, type the emails to notify. b. In the **Password** box, type a password for the export file. Share this password with the recipients so they can download the export file.

5. Click **Schedule Export**.

   The system saves the updated export.

Delete a Scheduled Export

> **Required User Role:** Administrator

On the **Exports** page, you can delete one or more scheduled exports from your Tenable Vulnerability Management instance.

> **Note**: Deleting a scheduled export removes the schedule from your Tenable Vulnerability Management instance entirely. If you want to instead suspend a scheduled export, you can disable the schedule.

To delete a scheduled export:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.
4. Do one of the following:

   To delete a single scheduled export:

   a. In the **Schedules** table, in the row for the scheduled export you want to delete, click the ⋮ button.

      A menu appears.

   b. Click the **Delete** button.

   To delete multiple scheduled exports:

   a. In the **Schedules** table, select the check box for each scheduled export you want to delete.

      > **Note**: You can delete up to 10 export schedules simultaneously.

      The action bar appears at the top of the table.

   b. In the action bar, click the **Delete** button.

   Tenable Vulnerability Management deletes the selected scheduled export or exports. Deleted scheduled exports no longer appear in the **Schedules** table.

Export Activity

On the **Export Activity** tab, you can view all the exports created on your account. You can see the source, type, format, status, size, creation date, and author for each export.

> **Note:** Export expiration is set via the **Settings** section. For more information, see General Settings.

> **Note**: By default, Tenable Vulnerability Management allows you to store up to 500 MB of export data at a time. Once you reach this limit, you cannot create new exports until you delete some of your existing export data. To increase your export storage limit, contact your Tenable representative.

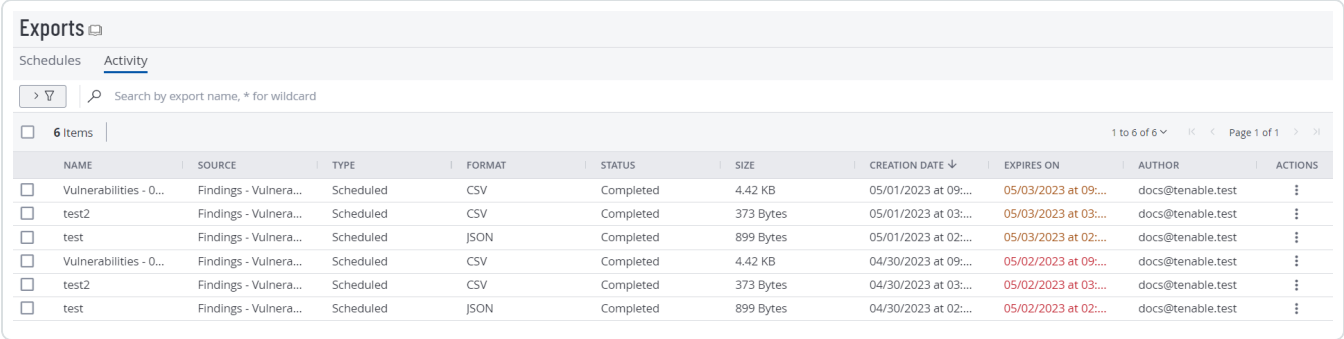
To view your export activity:

- In the left navigation, click **Export**.

  The **Export** page appears.

- Click the **Activity** tab.

  The **Activity** page appears.



This page displays a table with all the exports on your Tenable Vulnerability Management account.

Activity Table

The **Activity** table contains the following information about your exports:

Column	Description
Name	The name of the export file.
Source	The data source for the export in Tenable Vulnerability Management. The possible sources are: • **Assets** – Information about all the assets on your Tenable Vulnerability Management license. • **Assets Host** –Information about assets Tenable Vulnerability Management identified on your host during a scan. • **Findings - Vulnerabilities - Host** – Information about the vulnerability findings Tenable Vulnerability Management identified on your host during a scan. • **Users** – Information about the users assigned to your account.

Type	The type of export, either manual or scheduled.
Format	The format of the export file, either CSV or JSON.
Status	The status of the export. The possible statuses are: • **Pending** – Tenable Vulnerability Management is initiating the export process. • **Running** – Tenable Vulnerability Management is preparing the requested file. • **Completed** – Tenable Vulnerability Management has successfully completed the export process. The export file is now available to download. • **Canceled** – Tenable Vulnerability Management canceled the export process. A **Canceled** status appears when a user stops a pending or running export. • **Failed** – The export process failed.
Reason	The reason the export attempt failed. By default, the **Reason** column is hidden. For information about how to add the column to the table, see Tables. A reason value appears only if the export status is **Failed**.
Size	The size of the export file. A size value appears only if the export status is **Completed**.
Creation Date	The date and time a user initiated the export.
Completion Date	The date and time when the export process completed.
File Name	The name of the CSV or JSON export file.
Expires On	The date and time the export expires. **Note:** The default export expiration is set in General Settings

Author	The user who initiated the export.
Actions	The actions you can perform with the export, including the following: • Download an export file. • Renew the expiration date for one or more exports. • Delete one or more export files. • Export your export activity.

On the **Export Activity** page, you can perform the following actions:

- Filter your Exports
- Renew an Export Expiration Date
- Stop an Export
- Download Export Activity
- Export your Export Activity
- Delete an Export

Note: Export expiration is set via the **Settings** section. For more information, see .

Filter your Exports

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

On the **Exports** page, you can filter the export data for your Tenable Vulnerability Management instance.

To filter your exports:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

The **Exports** page appears. By default, the **Schedules** tab is active.

3. (Optional) To filter your export activity data, click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. In the upper-left corner, click the ▽ button.

   The filters plane expands. The plane displays a list of default filter options.

5. Click **Edit Filters**.

   A drop-down box appears listing all the filter options.

6. Select or deselect the filters you want to add or remove. For detailed list of available filters, see Export Filters.

7. Click outside the filter drop-down box.

   The drop-down box closes.

8. For each selected filter, in the first text box, select an operator.

9. In the second text box, select or type a value for the filter.

   Note: You can select up to five different values for each filter to apply to your exports.

   Note: If a filter you select has generic options, those options appear below the filter. If the filter requires a specific, unique value, you must type the value.

   Tip: When you type a value for your filter, you can use a wild card character (*****) to stand in for a section of text anywhere in the value. For example, if you want the filter to include all values that end in 1, type **1*. If you want the filter to include all values that begin with 1, *type 1**. If you want the filter to include all values with a 1 somewhere between the first and last characters, type **1**.

10. (Optional) To clear the value of a filter:

    a. Hover over the filter you want to clear.

       An interactive window appears over the filter.

b. In the window, click **Clear** to remove the value provided in the filter box.

Tenable Vulnerability Management clears the filter value.

11. (Optional) To remove a filter:

a. Hover over the filter you want to remove.

An interactive window appears over the filter.

b. In the window, click **Remove** to remove the filter.

Tenable Vulnerability Management removes the filter.

12. Click **Apply**.

Tenable Vulnerability Management filters your export data.

Export Filters

On the **Exports** page, you can filter your export data using following filters:

Note: The available filters vary based on the type of data you want to export.

Filter	Export Data Type	Description
Name	scheduled exports, export activity	The name you assigned to the export in Tenable Vulnerability Management. This filter is selected by default.
Size	export activity	The size of the export file in bytes. This filter is selected by default.
Source	scheduled exports, export activity	The area of Tenable Vulnerability Management to which the export applies. This filter is selected by default.
Status	scheduled exports, export activity	The current status of the export. Possible options are: • **Pending**

		• **Running** • **Canceled** • **Failed** • **Completed** This filter is selected by default.
Author	export activity	The user who created the export.
Completion Date	export activity	The date on which Tenable Vulnerability Management completed the export. This filter applies only to exports with a **Completed** status.
Creation Date	scheduled exports, export activity	The date on which a user on your instance created the export.
Expires On	export activity	Indicates when the export file expires. The filter value can be a date, date range, or number of days until the export file expires.
File Name	export activity	The name of the export file.
Format	scheduled exports, export activity	The export file type. Possible options are: • **CSV** • **JSON**
Reason	export activity	The reason the export failed. This filter applies only to exports with a **Failed** status.
Next Run	scheduled exports	The date and time on which the next export is scheduled.
Last Run Start Date	scheduled exports	The date and time on which Tenable Vulnerability Management last initiated the export.
Last Run	scheduled exports	The date and time on which Tenable Vulnerability Management last completed the export.

Completion Date		
Created By	scheduled exports	The user who created the export.
Updated Date	scheduled exports	The date and time on which a user last updated the export.
Updated By	scheduled exports	The user who last updated the export.

Renew an Export Expiration Date

Required User Role: Administrator

On the **Exports** page, you can reset the expiration date for any export on your Tenable Vulnerability Management instance.

Note: You can reset the expiration date for only one export at a time.

Tip: You can also configure your default export expiration settings on the General Settings page.

To reset the expiration date for an export:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. Do one of the following:

- In the exports table, right-click the row for the export for which you want to reset the expiration date.

  The action options appear next to your cursor.

- In the exports table, in the **Actions** column, click the ⋮ button in the row for the export for which you want to reset the expiration date.

  The action buttons appear in the row.

5. Click **Renew**.

   Tenable Vulnerability Management resets the expiration date of the export to the default expiration period you have configured in Settings>General Settings.

Stop an Export

> **Required User Role:** Administrator

On the **Exports** page, you can stop one or more pending or running exports on your Tenable Vulnerability Management instance.

> **Note**:You cannot stop an export that has already been completed, canceled, or failed.

To stop a pending or running export:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

5. Select the exports that you want to stop:

Stop Scope	Action
Selected exports	To stop selected exports: **Tip**: You can stop up to 10 exports simultaneously. a. In the exports table, select the check box for each export you want to stop. The action bar appears at the top of the table. b. In the action bar, click **Stop**.
A single export	To stop a single export: a. In the exports table, right-click the row for the export you want to stop. -or- In the exports table, in the **Actions** column, click the ⋮ button in the row for the export you want to stop. The action buttons appear in the row. b. Click **Stop**.

Download Export Activity

Required User Role: Administrator

On the **Exports** page, you can download an export file on your Tenable Vulnerability Management instance.

Note: You can download only one export file at a time.

Note:You can download the export file only if the export's status is **Completed**.

To download an export file:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

5. Do one of the following:

   - In the exports table, right-click the row for the export file you want to download.

     The action options appear next to your cursor.

   - In the exports table, in the **Actions** column, click the ⋮ button in the row for the export file you want to download.

     The action buttons appear in the row.

6. Click **Download**.

   Tenable Vulnerability Management downloads the export file to your computer.

Export your Export Activity

> **Required User Role:** Administrator

On the **Exports** page, you can export data for the export activity on your Tenable Vulnerability Management instance.

To export your export activity data:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

The **Exports** page appears. By default, the **Schedules** tab is active.

3. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

5. Select the exports that you want to export:

Export Scope	Action
Selected exports	To export selected exports: a. In the exports table, select the check box for each export you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 exports, select all the exports in the list and then click [→ **Export**.
A single export	To export a single export: a. In the exports table, right-click the row for the export you want to export. The action options appear next to your cursor. -or- In the exports table, in the **Actions** column, click the ⋮ button in the row for the export you want to export. The action buttons appear in the row. b. Click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  > **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

6. In the **Name** box, type a name for the export file.
7. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of exports. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of exports. Empty fields are not included in the JSON file.

8. In the **Configurations** section, select the fields you want to include in the export file by selecting the check box next to any field. Use the text box to search for a field.

   To view only the selected fields, click **View Selected**.

9. In the **Expiration** box, type the number of days before the export file expires.

   > **Note**: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

10. (Optional) To set a schedule for your export to repeat:

    - Click the **Schedule** toggle.

      The **Schedule** section appears.

    - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
    - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
    - In the **Repeat** drop-down box, select how often you want the export to repeat.
    - In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

      > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

11. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

    - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

12. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

13. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Delete an Export

> **Required User Role:** Administrator

On the **Exports** page, you can delete one or more exports from your Tenable Vulnerability Management instance.

> **Note**:You can delete an export file only if the export's status is **Completed**, **Canceled**, or **Failed**.

To delete an export:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

3. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

4. (Optional) Refine the table data.

5. Select the exports that you want to delete:

Delete Scope	Action
Selected exports	To delete selected exports: **Tip**: You can delete up to 10 exports simultaneously. a. In the exports table, select the check box for each export you want to delete. The action bar appears at the top of the table. b. In the action bar, click **Delete**.
A single export	To delete a single export: a. In the exports table, right-click the row for the export you want to delete. -or- In the exports table, in the **Actions** column, click the ⋮ button in the row for the export you want to delete. The action buttons appear in the row. b. Click **Delete**.

Tenable Vulnerability Management removes the export from your account.

Recast Rules

In Tenable Vulnerability Management, you can customize Tenable's risk management framework to fit the needs of your organization. To do this, you create rules that modify the severity of vulnerabilities or the results of host audits—or hide them from your scan results.

Example

Imagine you have an asset featuring an FTP with an open vulnerability. You no longer need FTP, so you shut down the service. Now, Tenable Vulnerability Management cannot verify the vulnerability

as patched, so it continues to appear in your Findings list. You can use a recast or accept rule to ignore this vulnerability finding without needing to delete the asset and begin a fresh scan.

To access the Accept/Recast Rules page:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Recast** tile.

   The **Accept/Recast Rules** page appears.

Here, you can view the following information about your accept and recast rules:

- **Action** – An icon that indicates the type of rule, for example (Accept) or (Recast).

  Tip: To learn about these rule types, see About Recast and Accept Rules.

- **Vulnerability** – The name of the vulnerability associated with the rule.
- **Plugin ID** – The plugin ID associated with the vulnerability.
- **Original Severity** – The original severity of the vulnerability before the rule was applied.
- **New Severity** – The new severity of the vulnerability after the rule was applied.
- **Targets** – The IP addresses/hostnames targeted by the rule.
- **Owner** – The Tenable Vulnerability Management user who created the rule.
- **Expires** – The date and time on which the rule expires. If the rule does not expire, this column is blank.
- **Created** – The date and time at which the rule was created.
- **Last Updated** – The date and time at which the rule was last updated by a user.
- **Actions** – Click the button to view actions you can take with the rule. For more information, see Manage Recast Rules.

This documentation explains how to create recast rules, when to use them, and how to manage them. For more information, see the following topics:

- About Recast and Accept Rules
- About Change Result and Accept Rules
- Create Recast Rules from Settings
- Create Recast Rules from the Findings Page
- Manage Recast Rules

About Recast and Accept Rules

On the **Accept/Recast Rules** page in the **Vulnerabilities** tab, you can create both *Recast* and *Accept* rules. While Recast rules modify the severity of all findings that correspond to a Plugin ID, Accept rules hide the findings instead. These rules do not modify historical scan results and you can only use them on host vulnerabilities.

Why would I use these?

Imagine you have an asset featuring an FTP with an open vulnerability. You no longer need FTP, so you shut down the service. Now, Tenable Vulnerability Management cannot verify the vulnerability as patched, so it continues to appear in your Findings list. You can use a recast or accept rule to ignore this vulnerability finding without needing to delete the asset and begin a fresh scan.

Recast Rules

Recast rules target a specific Plugin ID and its findings, for all your assets or some. You can set Recast rules to expire. When Recast rules expire, findings revert to their original severity.

You can check which findings have a Recast rule. To do this, on the **Findings** workbench, use the the **Risk Modified** filter with a value of **Recast**.

Recast findings are labeled in the user interface. On the **Findings** workbench in the **Severity** column, ⟳ appears. On the **Findings Details** page, in the top-right corner, a **Recast** label appears.

> **Note**: If using Tenable Vulnerability Management without Tenable One, targeted findings do not change your VPR, CES, or AES scores.

Example Recast Rule

Let's say you have a group of internal servers that use self-signed SSL certificates. Your scans report vulnerabilities from plugin 51192, *SSL Certificate Cannot Be Trusted*, which has a Medium severity. You know the servers use self-signed certificates, so you create the following rule to lower the severity:

- **Action** – Recast
- **Vulnerability Plugin ID** – 51192
- **New Severity** – Info
- **Targets** – Custom
- **Target Hosts** – 192.0.2.1 - 192.0.2.10
- **Expires** – Never

Accept Rules

Accept rules work the same way as Recast rules, but accept the risk and hide the findings. You can set Accept rules to expire. When Accept rules expire, their findings reappear on the **Findings** workbench.

To view hidden findings from Accept rules, on the **Findings** workbench, use the **Risk Modified** filter with a value of **Accepted**. Accepted findings appear with in the **Severity** column and, at the top-left corner of the **Findings Details** page, with an **Accepted** label.

> **Note**: Findings from Accept rules do not affect VPR, AES, or CES scores.

Example Accept Rule

For the same internal servers using self-signed SSL certificates, let's say you want to remove any scan results for plugin 51192 instead of lowering the severity of the vulnerability. You create the following rule:

- **Action** – Accept
- **Vulnerability Plugin ID** – 51192
- **Targets** – Custom

- **Target Hosts** – 192.0.2.1 - 192.0.2.10
- **Expires** – Never

About Change Result and Accept Rules

On the **Accept/Recast Rules** page in the **Host Audits** tab, you can create both *Change Result* and *Accept* rules. While Change Result rules modify the results of a host audit, Accept rules hide the findings instead. These rules do not modify historical scan results and you can only use them on Host Audit findings.

Change Result Rules

Change Result rules use an Audit File and an Audit Name and modify finding results to a value you specify. You can use Change Result rules on some or all assets or some and set them to expire. When Change Result rules expire, findings revert to their original result.

To view findings for a Change Result rule, on the **Findings** workbench in the **Host Audits** tab, use the **Results Modified** filter with a value of **Result Changed**.

Example Change Result Rule

In the following example, you create a rule to address host audit findings from a HIPAA audit. Since only some assets contain Protected Health Information (PHI), the rule changes results to Passed on assets without PHI:

- **Action** – Change Result
- **Category** – Custom
- **Audit File** – HIPAA_Security_Rule_v1.1.0.audit
- **Audit Name** – Check HIPAA Security
- **Original Result** – Failed
- **New Result** – Passed
- **Targets** – Custom
- **Target Hosts** – 192.0.2.1 - 192.0.2.10
- **Expires** – Never

Accept Rules

Accept rules hide findings instead of changing their results –useful when you want to keep a clean audit list with actionable items. Like Change Result rules, you can apply Accept rules to to some or all assets and set them to expire. When Accept rules expire, targeted findings reappear on the **Findings** workbench.

To view findings for an Accept rule, on the **Findings** workbench in the **Host Audits** tab, use the **Results Modified** filter with a value of **Accepted**.

Example Accept Rule

In the following example, you create a rule to accept host audit findings for Windows machines with disabled built-in firewalls, since your endpoint security package provides its own firewall:

- **Action** – Accept
- **Category** – Windows
- **Audit File** – CIS_Microsoft_Windows_11_Enterprise_v3.0.0_L1.audit
- **Audit Name** –Hide Windows Firewall Findings
- **Original Result** – Failed
- **Targets** – All
- **Expires** – Never

Create Recast Rules from Settings

In **Settings** > **Recast**, you can create rules to modify or accept vulnerability or host audit findings from the **Findings** workbench. You can also create these rules directly from the **Findings** workbench, as described in Create Recast Rules from Findings.

Here, you can create the following rule types:

Rule	Description
Recast	In the **Vulnerabilities** tab, modify the severity of vulnerability findings based on their Plugin ID.
Accept (for host	In the **Vulnerabilities** tab, accept the risk of vulnerability findings and

vulnerabilities)	hide them from the **Findings** workbench.
Change Result	In the **Host Audits** tab, modify the Result of host audit findings, for example by changing Failed results to Passed.
Accept (for host audits)	In the **Host Audits** tab, accept the Result of host audit findings and hide them from the the **Findings** workbench.

Create a Recast or Accept Rule

To create a Recast or Accept rule:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click **Recast**.

   The **Accept/Recast Rules** page appears.

3. In the upper-right corner, click **Add Rule**.

   The **Add Recast Rule** pane appears.

4. Configure the following options:

Option	Description
Action	Click **Accept** or **Recast**. To learn about these rule types, see About Recast and Accept Rules.
Vulnerability Plugin ID	Type the Tenable Plugin ID for the vulnerability, for example *70658*.
New Severity	(Recast rules only) Select the severity you want to change the corresponding vulnerability to, for example *Low*.
Targets	Select **All** or **Custom**. If the rule will override other rules, a warning appears. The most recently created rule trumps other rules.
Target Hosts	For **Custom** targets, enter up to 1000 comma-separated IPv4

	addresses or ranges, hostnames, Classless Inter-Domain Routing (CIDR) notations, or fully qualified domain names (FQDNs). **Caution**: If you target findings by IP address and have multiple networks, the rule matches findings on all your networks. For more information, see Networks.
Expires	Select **After** or **Never**. If you select **After**, type a number of days or a date when the rule will expire.
Comments	Type comments to provide rule details.
Report as False Positive to Tenable	(Optional) (Accept rules only) Turn on this toggle when a plugin generates inaccurate findings and you want Tenable to review the results.

5. Click **Save**.

   The system processes the rule, which may take time if many findings are targeted. When complete, the rule appears in the **Vulnerabilities** tab and the system updates the **Findings** workbench.

Create a Change Result or Accept Rule

Caution: For best performance, the system supports a maximum of *5000* Change Result and Accept rules in each container, total.

To create a Change Result or Accept rule:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click **Recast**.

   The **Accept/Recast Rules** page appears.

3. Click the **Host Audits** tab.

4. In the upper-right corner, click **Add Rule**.

The **Add Change Result Rule** pane appears.

5. Configure the following options:

Option	Description
Action	Click **Accept** or **Change Result**. To learn about these rule types, see About Change Result and Accept Rules.
Category	Select a category for the new rule, for example, *Windows*.
Audit File	Select an audit file to run against your assets, for example, *CIS_MS_Windows_11_Enterprise_Level_1_v1.0.0.audit*.
Audit Name	Type an audit name, for example, *9.3.1 Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)'*.
Original Result	Select the original result of the host audit, for example, *Failed*.
New Result	(Change Result rules only) Select the result to change the targeted findings to.
Targets	(Optional) Select **Custom**. If the rule will override other rules, a warning appears. The most recently created rule trumps other rules.
Target Hosts	For **Custom** targets, type a comma-separated list of IPv4 addresses or ranges, hostnames, Classless Inter-Domain Routing (CIDR) notation, or fully qualified domain names (FQDNs). The system supports up to 100 items.
Expires	(Optional) Select **After** or **Exact Date**. Then, type a number of days or a date when the rule will expire.
Comments	Type comments to provide rule details.

6. Click **Save**.

The system processes the rule, which may take time if many findings are targeted. When complete, the rule appears in the **Vulnerabilities** tab and the system updates the **Findings** workbench.

Manage Recast Rules

On the **Accept/Recast Rules** page, you can edit, delete, or export rules.

Edit a Recast Rule

To edit a rule:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click **Recast**.

   The **Recast/Accept Rules** page appears.

3. In the **Vulnerabilities** or **Host Audits** tab, click the rule to edit.

   The **Edit Rule** plane appears.

4. Edit the rule. To review available options, see Create Recast Rules from Settings.

5. Click **Save**.

   The system applies your changes. If the rule targets a large number of findings, this may take a few minutes.

Delete a Recast Rule

To delete a rule:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click **Recast**.

   The **Recast/Accept Rules** page appears.

3. In the **Vulnerabilities** or **Host Audits** tab, in the **Actions** column, click .

   A drop-down appears.

4. In the drop-down, click **Delete**.

5. In the confirmation that appears, click **Delete** again.

   The system deletes the rule.

Export a Recast Rule

To export a recast or accept rule:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click **Recast**.

   The **Recast/Accept Rules** page appears.

3. In the **Vulnerabilities** or **Host Audits** tab, in the **Actions** column, click ⋮.

   A drop-down appears.

4. In the drop-down, click **Export**.

   The **Export** plane appears. Set options as follows:

Option	Description
Name	Type a name for the export.
Formats	Select an export format: • **CSV** - A CSV file that you can open in a spreadsheet application. **Note**: The system trims cells longer than 32,000 characters so they appear correctly in Microsoft Excel. This is uncommon, except with verbose outputs such as those from service enumeration plugins. • **JSON** - A JSON file that conains a nested list of findings, with no empty fields.
Configurations	Select the fields to include. Toggle between **View Selected** and

	View All or search for fields to add them.
Expiration	(Optional) Type the number of days before the export file ages out.
Schedule	(Optional) Turn on the **Schedule** toggle and set the following options: • **Start Date and Time** – Select the date and time for the export. • **Time Zone** – Select a time zone. • **Repeat** – Select the cadence on which you want the export to repeat. • **Repeat Ends** – Select the date when exports end. If you select **Never**, the export repeats until you modify or delete it.
Email Notifications	(Optional) Turn on the **Email Notification** toggle and set the following options: • **Add Recipients** – Type the emails to send export files to. • **Password** –Type a password for the export file.

5. Click **Export**.

   The system processes the export. When processing completes, the file downloads to your computer. If you leave the page, the completed export appears in **Settings** > **Exports**.

Tags

You can add your own business context to assets by tagging them with descriptive metadata in Tenable Vulnerability Management. An asset tag is primarily composed of a *Category*:*Value* pair. For example, if you want to group your assets by location, create a *Location* category with the value *Headquarters*. You can then manually apply the tag to individual assets, or you can add rules to the tag that enable Tenable Vulnerability Management to apply the tag automatically to matching assets.

Important: Due to differences in the asset source, asset counts within the **Tags** section may not match the asset counts within the **Assets** section of Tenable Vulnerability Management.

For more information about tag structure and related best practices, see:

- Tag Format and Application
- Considerations for Tags with Rules
- Examples: Asset Tagging

Note: If you want to create tags without individual categories, Tenable recommends that you add the generic category *Category*, which you can use for all your tags.

To view your tags:

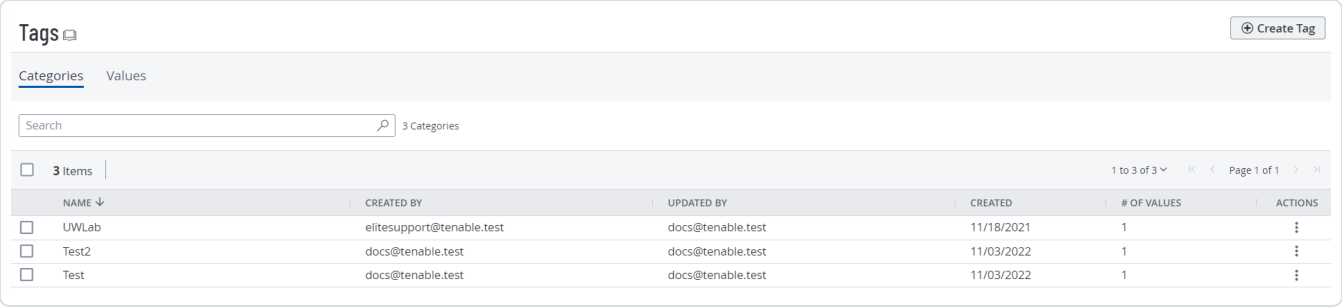
1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.



3. Do one of the following:

   To view the categories to which all the tags in your Tenable Vulnerability Management instance are assigned:

a. View your tag categories and relevant data about them in the **Categories** table:

Column	Description
Name	The name of the tag.
Created By	The username of the user who created the tag.
Last Used By	The username of the user who most recently created or edited the tag value or category.
Created	The date on which the tag was created.
# of Values	The number of tag values associated with the tag category.
Actions	The actions you can perform with the tag.

To view all the tags in your Tenable Vulnerability Management instance:

a. Click the **Values** tab.

The **Values** page appears, containing a table of all the tags on your Tenable Vulnerability Management instance.

b. View your tags and relevant data about them in the **Values** table:

Column	Description
Name	The name of the tag.
Created By	The username of the user who created the tag.
Updated By	The username of the user who last updated the tag category or value.
Created	The date on which the tag was created.
Applied	Indicates whether the tag is applied **Manually** or **Automatically**.
Last Processed	The date and time when Tenable Vulnerability Management last processed the scan and applied it to all relevant assets.

Assessment	Indicates whether Tenable Vulnerability Management has finished identifying and apply the tag to all matching assets.
Actions	The actions you can perform with the tag.

Examples: Asset Tagging

See the following configuration examples to tag assets for common use cases. For general information about tags, see Tags.

- Example: Automatically Tag by Installed Software
- Example: Manually Tag by Priority

Example: Automatically Tag by Installed Software

Your company manages assets that run on two software types: Oracle and Wireshark. Your company assigns asset ownership to employees based on the software type. Employees must resolve any vulnerabilities identified on assets with the software type they manage.

As an administrator, you can create an automatic tag for each software type. Then, employees can search for assets by the **Installed Software** tag and filter Tenable Vulnerability Management assets by the software type they manage.

> **Note:** For more precise results, set the tag value to the appropriate NVD Common Platform Enumeration (CPE), for example, `cpe:/a:microsoft:office`.

To automatically tag assets by installed software:

1. Create and automatically apply a tag for Oracle assets using the following settings:

Option	Value
Category	*Installed Software*
Value	*Oracle*
Rules	Enabled, with the following rule specified: • **Match All** • **Category**: *Installed Software* • **Operator**: *is equal to* • **Value**: *Oracle*

2. Create and automatically apply a tag for Wireshark assets using the following settings:

Option	Value
Category	*Installed Software*
Value	*Wireshark*
Rules	Enabled, with the following rule specified: • **Match All** • **Category**: *Installed Software* • **Operator**: *is equal to* • **Value**: *Wireshark*

3. Instruct employees to use the new tags to filter assets in the assets table or to search for assets from the tags table.

Example: Manually Tag by Priority

Your company owns sensitive assets and you want employees to prioritize addressing vulnerabilities on these assets first, regardless of the asset's other attributes (for example, the asset's VPR).

To make sure employees view and mediate these sensitive assets first, you can create a **High Priority** tag and manually add it to assets that you want employees to prioritize. Then, employees can search for assets using the **High Priority** tag to filter by the highest priority assets they manage.

To manually tag assets by priority:

1. Create a tag for your highest priority assets using the following settings:

Option	Value
Category	*Priority*
Value	*High Priority*
Value Description	A custom description about the urgency of remediating the vulnerabilities on assets with this tag.

2. Apply the tag manually to your highest priority assets.
3. Instruct employees to use the new tag to filter assets in the assets table or to search for assets from the tags table.

Tag Format and Application

An asset tag is primarily composed of a *Category*:*Value* pair. For example, if you want to group your assets by location, create a *Location* category with the value *Headquarters*.

> **Note:** If you want to create tags without individual categories, Tenable recommends that you add the generic category *Category*, which you can use for all your tags.

Tag membership is reevaluated:

- When you update or create a tag
- When Tenable Vulnerability Management imports data
- Every 12 hours

Manual Tags vs. Automatic Tags

When you create a tag, Tenable Vulnerability Management automatically applies it to the assets on your instance that match the tags rules. These automatically applied tags are sometimes called

dynamic tags. When you create an automatic tag, Tenable Vulnerability Management applies that tag to all your current assets and any new assets added to your organization's account. Tenable Vulnerability Management also regularly reviews your assets for changes to their attributes and adds or removes automatic tags accordingly.

Note: When you create or edit an automatic tag, Tenable Vulnerability Management may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

You can also create a tag without rules and then manually apply the tag to individual assets. Alternatively, you can manually apply an automatic tag to additional assets that may not meet the rules criteria for that tag. These manually applied tags are sometimes called *static tags*.

Manual tags appear with the icon, whereas automatic tags appear with the icon.

See the following examples for clarification:

Scenarios	Tag Type	Tag Icon
You create a tag with *Location*:*Headquarters* as the *Category*:*Value* pair, but you do not add any tag rules. Later, you add the tag to assets located at your headquarters.	Manual	
You create a tag with *Location*:*Headquarters* as the *Category*:*Value* pair, and you specify an IP address range in the tag rules. Tenable Vulnerability Management then automatically applies the tag to all existing or new assets within that IP address range.	Automatic	
When removing a tag it will display the icon appropriate to how the tag was applied. For example, if you manually apply an automatic tag to a host, when editing the tag selections on the host, the tag appears as manual rather than automatic.	N/A	N/A

Create a Manual or Automatic Tag

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Note: When you create a tag from the **Tagging** page, you can select from a list of generic asset filters to create tag rules. If you want to create a tag based on filters that are specific to certain asset types, Tenable recommends that you create a tag from the **Assets** page, where you can select additional filters that are specific to each asset type.

Note: Tenable Web App Scanning does not handle permissions reliant on a tag.

On the **Create Tag** page, you can create one of the following types of tags:

- Manual – You can create and save a tag to manually apply to individual assets at any time. Tenable does not automatically apply manual tags to assets.
- Automatic – You can create a tag and add Tag Rules that Tenable Vulnerability Management uses to identify and tag matching assets. Tenable Vulnerability Management automatically applies the tag to assets identified by the rule at specific intervals.

  Important: You must add a tag rule to the tag in order for Tenable Vulnerability Management to identify and tag the appropriate assets.

  Tip: If your tags fail to apply, the tag rules you configured likely returned too many assets for Tenable Vulnerability Management to process. For example, a long list of Fully Qualified Domain Names (FQDNs) with wildcards would cover a large number of assets. When this happens, Tenable recommends reducing the number of assets through stricter tag rules. If needed, you can then use an additional tag to join each list.

For more information, see Considerations for Tags with Rules.

Note: You can create up to 100 tag categories, and each category can have up to 100,000 tags.

To create a tag from the **Tags** page:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

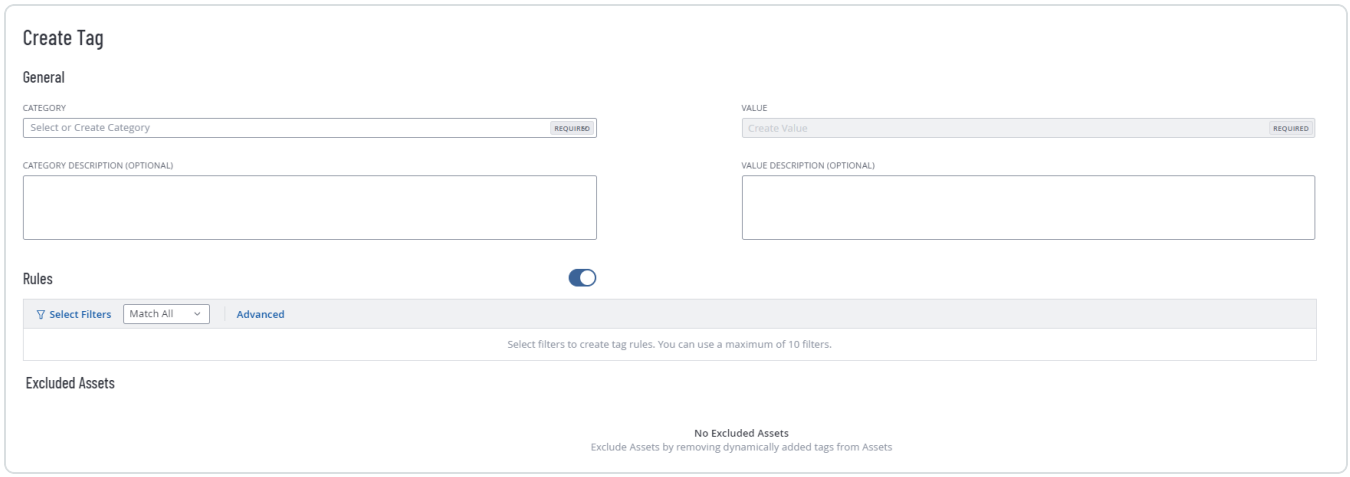
2. Click the **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

3. In the upper-right corner of the page, click the ⊕ **Create Tag** button.

   The **Create Tag** page appears.



4. Click the **Category** drop-down box.
5. In the **Add New Category** box, type a category.

   As you type, the list filters for matches.
6. From the drop-down box, select an existing category, or if the category is new, click **Create "***category name***"**.

   Note: You can create a maximum of 100 categories for your Tenable Vulnerability Management instance.
7. (Optional) In the **Category Description** box, type a description of the tag category.
8. In the **Value** box, type a name for the tag.

   Note: Tag names cannot include commas or be more than 50 characters in length.

   Tip: Tenable recommends that you provide a tag name that directly corresponds with the tag category. For example, if the category is *Location*, *Headquarters* would be an appropriate value.
9. (Optional) In the **Value Description** box, type a description for the new tag.
10. Do one of the following:

    To save the tag as a manual tag:

a. Click **Save**.

   Tenable Vulnerability Management saves the tag to the tags table.

b. (Optional) Manually add the tag to one or more assets.

To save and apply the tag automatically:

a. Create a tag rule.

b. Click **Save**.

   Tenable Vulnerability Management creates the tag, evaluates existing assets, and automatically applies the tag to assets that match the tag rules.

> **Note:** When you create an automatic tag, Tenable Vulnerability Management may take a few minutes to apply the tag and update any excluded assets, depending on the system load and the number of assets.

> **Tip:** When you create a tag, Tenable Vulnerability Management automatically creates and assigns "*Tag:value* owner permissions" that allow you to manage the tag. If you are an administrator, you can give other users or groups this permission via the Permissions page.

Considerations for Tags with Rules

Automatic Application

Tenable Vulnerability Management evaluates assets against tag rules in the following situations:

- When you add a new asset (via scan, connector import, or leveraging the Tenable Vulnerability Management API), Tenable Vulnerability Management evaluates the asset against your tag rules.
- When you create or update a tag rule, Tenable Vulnerability Management evaluates your assets against the tag rule.

  > **Note:** When you create or edit a tag rule, Tenable Vulnerability Management may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

- When you update an existing asset, Tenable Vulnerability Management re-evaluates the asset and removes the tag if the asset's attributes no longer match the tag rules.

Manual Application

If you manually apply a tag that has been configured with rules, Tenable Vulnerability Management excludes that asset from any further evaluation against the rules.

Tag Rules

Tag rules allow Tenable Vulnerability Management to automatically apply tags you create to the assets on your instance that match the tags rules. These automatically applied tags are called *dynamic* or *automatic* tags.

Tag rules are composed of one or more filter-value pairs based on asset attributes. When you create a rule and add it to a tag, Tenable Vulnerability Management applies the tag to all assets on your instance that match the tag rule.

> **Note:** Tenable Vulnerability Management supports a maximum of 35 rules per tag. This limit means that you can specify a maximum of 35 **and** or **or** conditions for a single tag value. Additionally, Tenable Vulnerability Management supports a default maximum of 25 values per individual tag rule. For IPv4, IPv6, and FQDNs, Tenable Vulnerability Management supports a maximum of 1,024 values per individual tag rule.

For more information about automatic tags, see:

- Tag Format and Application
- Considerations for Tags with Rules

In the **Tags** section, you can complete the following tasks with tag rules:

- Create a Tag Rule
- Edit a Tag Rule
- Delete A Tag Rule

Create a Tag Rule

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

> **Required Tenable Vulnerability Management Permission:** Can Edit, Can Use permission for applicable asset tags.

When you create or edit a tag to apply automatically, you must create and apply rules to the tag using tag rules filters. You can create a tag rule in either **Basic** or **Advanced** mode.

Caution: If you create a tag rule in **Basic** mode and then switch to **Advanced** mode, the rules you created appear in the **Advanced** mode format. However, if you switch from **Advanced** mode to **Basic** mode, Tenable Vulnerability Management removes all rules from the rules section.

Note: When you create a tag from the **Tagging** page, you can select from a list of generic asset filters to create tag rules. If you want to create a tag based on filters that are specific to certain asset types, Tenable recommends that you create a tag from the **Assets** page, where you can select additional filters that are specific to each asset type.

Note: Tenable Web App Scanning does not handle permissions reliant on a tag.

For more information about applying tags automatically, see Considerations for Tags with Rules.

Before you begin:

- Create or edit a tag.

To create and add a rule to a tag:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

3. Click the **Values** tab.

   The **Values** page appears, containing a table of all the tags on your Tenable Vulnerability Management instance.

4. Click the **Rules** toggle to enable the rule settings.

   The **Rules** section appears.

5. For each tag rule you want to create, do one of the following:

Note: **Basic** mode is active by default.

To create a tag rule in Basic mode:

a. In the **Rules** section, click **Select Filters**.

A drop-down box appears, listing the tag rule filter options.

Note: Each tag rule filter has different limits on the number of values you can apply to a single filter. For information about those limits, see Tag Rules Filters.

b. Select a filter.

The filter you select appears in the **Rules** section.

c. Click outside the drop-down box.

The drop-down box closes.

d. In the filter, click the button.

The filter expands.

e. In the first drop-down box, select the operator you want to apply to the filter.

f. In the second drop-down box, select or type one or more values for the filter.

g. **Determine whether you want to Match Any or Match All assets:**

In the **Rules** section, in the **Match Any** drop-down box, do one of the following:

- To apply the tag to assets that match any one of the defined rules, select **Match Any**.

  An **OR** operator appears between each rule.

  If an asset matches one or more of the filters defined in the tag rule, Tenable Vulnerability Management applies the tag to that asset.

- To apply the tag only to assets that match all of the filters defined in the tag rule, select **Match All**.

  An **AND** operator appears between each rule.

  If an asset matches every individual filter defined within the rule, Tenable Vulnerability Management applies the tag to that asset.

  > **Important:** If you select **Match All** and separate the values by commas, Tenable Vulnerability Management processes the string using OR logic, similar to the **Match Any** option.

h. (Optional) To create another rule, repeat the steps to create a tag rule in **Basic** mode.

To create a tag rule in Advanced mode:

a. In the **Rules** section, click **Advanced**.

   A text box appears.

b. Place your cursor in the text box.

   A drop-down box appears, listing the tag rule filter options.

   > **Note**: Each tag rule filter has different limits on the number of values you can apply to a single filter. For information about those limits, see Tag Rules Filters.

   > **Note:** If there is a typo in the tag rule, an error appears in the **Rules** box with a description of the issue.

c. Select or type the filter you want to apply.

   > **Tip:** You can use the arrow keys to navigate filter drop-down boxes, and press the **Enter** key to select an option.

   The filter appears in the text box.

   An operator drop-down box appears to the right of the filter.

d. Select one of the following operators. Available operators depend on the filter you select:

Note: If you want to filter on a value that starts with (') or ("), or includes (*) or (,), then you must wrap the value in quotation marks (").

Operator	Description
exists	Filters for items for which the selected filter exists.
does not exist	Filters for items for which the selected filter does not exist.
is equal to	Filters for items that match the filter value.
is not equal to	Filters for items that do not include the filter value.
is greater than **is greater than or equal to**	Filters for items with a value greater than the specified filter value. If you want to include the value you specify in the filter, then use the **is greater than or equal to** operator.
is less than **is less than or equal to**	Filters for items with a value less than the specified filter value. If you want to include the value you specify in the filter, then use the **is less than or equal to** operator.
within last	Filters for items with a date within a number of hours, days, months, or years before today. Type a number, then select a unit of time.
after	Filters for items with a date after the specified filter value.
before	Filters for items with a date before the specified filter value.
older than	Filters for items with a date more than a number of hours, days, months, or years before today. Type a number, then select a unit of time.

Operator	Description
is on	Filters for items with a specified date.
between	Filters for items with a date between two specified dates.
contains	Filters for items that contain the specified filter value.
does not contain	Filters for items that do not contain the specified filter value.
wildcard	Filters for items with a wildcard (*****) as follows: • **Begin or end with** – Filters for values that begin or end with text you specify. For example, to find all values that begin with "1", type *1**. To find all values that end in "1", type **1*. • **Contains** –Filters for values that contain text you specify. For example, to find all values with a "1" between the first and last characters, type **1**. • **Turn off case sensitivity** – Filters for values without case sensitivity. For example, to search for findings with a **Plugin Name** of "TLS Version 1.2 Protocol Detection" *or* "tls version 1.2 protocol detection", type **tls version 1.2 protocol detection*.

e. Where applicable, to the right of the operator, select or type a value for the filter.

> **Tip:** Some text filters support the character (*****) as a wildcard to stand in for a section of text in the filter value. For example, if you want the filter to include all values that end in 1, type **1*. If you want the filter to include all values that begin with 1, *type 1**.
>
> You can also use the wildcard operator to filter for values that contains certain text. For example, if you want the filter to include all values with a 1 somewhere between the first and last characters, type **1**.

f. Press the **Space** key.

A **CONDITIONS** drop-down box appears, with **AND** and **OR** as options:

- Select **OR** to "match any" assets tagged by the rule. If an asset matches one or more of the filters defined in the tag rule, Tenable Vulnerability Management applies the tag to that asset.
- Select **AND** to "match all" assets tagged by the rule. If an asset matches every individual filter defined within the rule, Tenable Vulnerability Management applies the tag to that asset.

  Important: If you select **AND** and separate the values by commas, Tenable Vulnerability Management processes the string using OR logic, similar to the **OR** option.

g. (Optional) To create more rules for the tag, repeat steps c-f.

6. Click **Save**.

   Tenable Vulnerability Management creates the rule and applies it to the tag.

Tip: When you create a tag, Tenable Vulnerability Management automatically creates and assigns "*Tag:value* owner permissions" that allow you to manage the tag. If you are an administrator, you can give other users or groups this permission via the Permissions page.

Edit a Tag Rule

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Required Tenable Vulnerability Management Permission: Can Edit, Can Use permission for applicable asset tags.

Once you create an automatic tag, you can edit the rules that apply to the tag from the **Edit Value** page.

Note: When you edit rules from the **Tagging** page, you can select from a list generic asset filters to create tag rules. However, if you want to add filters that are specific to a certain asset type (e.g., web application assets), Tenable recommends that you edit the tag from the **Assets** page, where you can select filters that are specific to each asset type.

Before you begin:

- Create an automatic tag.

To edit a tag rule:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

3. Click the **Values** tab.

   The **Values** page appears, containing a table of all the tags on your Tenable Vulnerability Management instance.

4. In the tags table, click the tag for which you want to edit a tag rule.

   The **Edit Value** page appears.

   > **Tip**: You can also navigate to the **Edit Value** page from the **Edit Category** page by clicking the tag you want to review in the **Values** table.

5. Click the **Rules** toggle to enable the rule settings.

   The **Rules** section appears.

6. In the **Rules** section, in the rule filter you want to edit, click the ⌄ button.

   A drop-down box appears with the lists of rule values previously selected for that filter.

   > **Note:** You can apply up to 10 filters to a tag rule.

7. (Optional) In the first drop-down box, select a new operator.

8. (Optional) In the second box, add or remove a rule value.

   > **Note**: If the rule filter has selectable options (e.g., dates ranges), those options appear below the filter. Otherwise, you must type the value.

9. Click outside the rules drop-down box.

   The drop-down box closes.

10. Click **Save**.

Tenable Vulnerability Management save your changes, evaluates existing assets, and automatically applies the tag to assets that match the updated tag rules.

> **Note:** Tenable Vulnerability Management may take some time to apply the tag to assets, depending on the system load and the number of assets.

Delete A Tag Rule

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

> **Required Tenable Vulnerability Management Permission:** Can Edit, Can Use permission for applicable asset tags.

When you delete a rule from an automatic tag, Tenable Vulnerability Management removes the tag from any assets that match the tag rule. When you delete all rules from an automatic tag, the tag becomes a manual tag.

To delete a tag rule:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

3. On the **Tags** page, click the **Values** tab.

   The **Values** page appears, containing a table with all the tags on your Tenable Vulnerability Management instance.

4. In the tags table, click the tag from which you want to delete a tag rule.

   The **Edit Value** page appears.

   > **Tip**: You can also navigate to the **Edit Value** page from the **Edit Category** page by clicking the tag you want to review in the **Values** table.

5. In the **Rules** section, in the rule you want to delete, click the ✕ button.

   The rule disappears from the **Rules** section.

6. Click **Save**.

   Tenable Vulnerability Management saves and applies your changes.

Tag Rules Filters

Note: If there is a typo in the tag rule, an error appears in the **Rules** box with a description of the issue.

Note: Tenable Vulnerability Management supports a maximum of 35 rules per tag. This limit means that you can specify a maximum of 35 **and** or **or** conditions for a single tag value. Additionally, Tenable Vulnerability Management supports a default maximum of 25 values per individual tag rule. For IPv4, IPv6, and FQDNs, Tenable Vulnerability Management supports a maximum of 1,024 values per individual tag rule.

On the **Tags** page, you can select from the following filters to create rules for an automatic tag:

Filter	Description
Account ID	The unique identifier assigned to the asset resource in the cloud service that hosts the asset.
ACR	(Requires Tenable Lumin license) The asset's ACR (Asset Criticality Rating).
ACR Severity	(Requires Tenable Lumin license) (Requires Tenable One or Tenable Lumin license) The ACR category of the ACR calculated for the asset.
AES	(Requires Tenable Lumin license)The Asset Exposure Score (AES) calculated for the asset.
AES Severity	(Requires Tenable Lumin license) (Requires Tenable Lumin license) The AES category of the AES calculated for the asset.
Agent Name	The name of the Tenable Nessus agent that scanned and identified the asset.
ARN	The Amazon Resource Name (ARN) for the asset.

ASN	The Autonomous System Number (ASN) for the asset.
Assessed vs. Discovered	Specifies whether Tenable Vulnerability Management scanned the asset for vulnerabilities or if Tenable Vulnerability Management only discovered the asset via a discovery scan. Possible values are: • **Assessed** • **Discovered Only**
Asset ID	The asset's unique identifier.
AWS Availability Zone	The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see Regions and Zones in the AWS documentation.
AWS EC2 AMI ID	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Instance ID	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Name	The name of the virtual machine instance in Amazon EC2.
AWS EC2 Product Code	The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2.
AWS Instance State	The state of the virtual machine instance in AWS at the time of the scan. For possible values, see InstanceState in the Amazon Elastic Compute Cloud Documentation.
AWS Instance Type	The type of virtual machine instance in Amazon EC2. Amazon EC2 instance types dictate the specifications of the instance (for example, how much RAM it has). For a list of possible values, see Amazon EC2 Instance Types in the AWS documentation.
AWS Owner ID	A UUID for the Amazon AWS account that created the virtual machine instance. This attribute only appears for Amazon EC2 instances. For more information, see View AWS Account Identifiers in the AWS

	documentation
AWS Region	The region where AWS hosts the virtual machine instance, for example, `us-east-1`.
AWS Security Group	The AWS security group (SG) associated with the Amazon EC2 instance.
AWS Subnet ID	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.
AWS VPC ID	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud Documentation.
Azure Resource Group	The name of the resource group in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure Resource ID	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager documentation.
Azure Resource Type	The resource type of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure Subscription ID	The unique subscription identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure VM ID	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see the Azure Resource Manager documentation.
BIOS ID	The NetBIOS name for the asset.
Cloud Provider	The name of the cloud provider that hosts the asset.
Created Date	The time and date when Tenable Vulnerability Management created the asset record.
Custom Attribute	A filter that searches for custom attributes via a category-value pair. For

	more information about custom attributes, see the Tenable Developer Portal.
Deleted	Specifies whether the asset has been deleted.
Deleted Date	The date when a user deleted the asset record or the number of days since a user deleted the asset. When a user deletes an asset record, Tenable Vulnerability Management retains the record until the asset ages out of the license count.
DNS (FQDN)	The fully-qualified domain name of the asset host. **Note:** This does not apply to Web Application assets, for which you must use the **Name** filter.
Domain	The domain which has been added as a source or discovered by ASM as belonging to a user.
First Seen	The date and time when a scan first identified the asset.
Google Cloud Instance ID	The unique identifier of the virtual machine instance in Google Cloud Platform (GCP).
Google Cloud Project ID	The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see Creating and Managing Projects in the GCP documentation.
Google Cloud Zone	The zone where the virtual machine instance runs in GCP. For more information, see Regions and Zones in the GCP documentation.
Has Plugin Results	Specifies whether the asset has plugin results associated with it.
Host Name (Domain Inventory)	The host name for assets found during attack surface management scans; only for use with Domain Inventory assets.
Hosting Provider	The hosting provider for the asset.
IaC Resource Type	The Infrastructure as Code (IAC) resource type of the asset.
Installed Software	A list of Common Platform Enumeration (CPE) values that represent applications identified on an asset from a scan. This field supports the

	CPE 2.2 format. For more information, see the Component Syntax section of the CPE Specification documentation. For assets identified in Tenable scans, this field only contains data when a scan using Tenable Nessus Plugin 45590 has evaluated the asset.
IPv4 Address	The IPv4 address associated with the asset record.. This filter supports multiple asset identifiers as a comma-separated list (for example, hostname_example, example.com, 192.168.0.0). For IP addresses, you can specify individual addresses, CIDR notation (for example, 192.168.0.0/24), or a range (for example, 192.168.0.1-192.168.0.255). **Note:** A CIDR mask of /0 is not supported for this parameter, because that value would match all IP addresses. If you submit a /0 value for this parameter, Tenable Vulnerability Management returns a 400 Bad Request error message. **Note:** Ensure the tag filter value does not end in a period.
IPv6 Address	An IPv6 address that a scan has associated with the asset record. This filter supports multiple asset identifiers as a comma-separated list. The IPV6 address must be an exact match. (for example, 0:0:0:0:0:ffff:c0a8:0). **Note:** Ensure the tag filter value does not end in a period.
Is Attribute	Specifies whether the asset is an attribute.
Is Auto Scale	Specifies whether the asset scales automatically.
Is Unsupported	Specifies whether the asset is unsupported in Tenable Vulnerability Management.
Last Audited	The time and date at which the asset was last audited.
Last Authenticated	The date and time of the last authenticated scan run against the asset.

Scan	An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field.
Last Licensed Scan	The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on how licenses work, see Tenable Vulnerability Management Licenses.
Last Seen	The date and time of the scan that most recently identified the asset.
Licensed	Specifies whether the asset is included in the asset count for the Tenable Vulnerability Management instance.
MAC Address	A MAC address that a scan has associated with the asset record.
Mitigation Last Detected	The date and time of the scan that last identified mitigation software on the asset.
Name	The asset identifier that Tenable Vulnerability Management assigns based on the presence of certain asset attributes in the following order: 1. Agent Name (if agent-scanned) 2. NetBIOS Name 3. FQDN 4. IPv6 address 5. IPv4 address For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.
NetBIOS Name	The NetBIOS name for the asset.
Network	The name of the network object associated with scanners that identified the asset. The default name is **Default**. For more information, see

	Networks.
Open Ports	Open ports on the asset.
Operating System	One of the operating system(s) that a scan identified on the asset.
Port	The port associated with the asset.
Public	Specifies whether the asset is available on a public network.
Record Type	The asset type.
Region	The cloud region where the asset runs.
Repositories	Any code repositories associated with the asset.
Resource Category	The name of the category to which the cloud resource type belongs (for example, object storage or virtual network).
Resource Tags (By Key)	Tags synced from a cloud source, such as Amazon Web Services (AWS), matched by the tag key (for example, Name).
Resource Tags (By Value)	Tags synced from a cloud source, such as Amazon Web Services (AWS), matched by the tag value.
Resource Type	The asset's cloud resource type (for example, network, virtual machine).
ServiceNow Sys ID	Where applicable, the unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.
Source	The source of the scan that identified the asset. Possible filter values are: • AWS • AWS FA • Azure • AZURE FA • Cloud Connector

	• Cloud IAC • Cloud Runtime • GCP • Nessus Agent • Nessus Scan • NNM • ServiceNow • WAS
SSL/TLS	Specifies whether the application on which the asset is hosted uses SSL/TLS public-key encryption.
System Type	The system types as reported by Plugin ID 54615. For more information, see Tenable Plugins.
Tags	Asset tags, entered in pairs of `category` and `value` (for example Network: Headquarters). This includes the space after the colon (:). If there is a comma in the tag name, insert a backslash (\) before the comma. If your tag name includes double quotation marks (" "), use the UUID instead. You can add a maximum of 100 tags. For more information, see Tags.
Target Groups	The target group to which the asset belongs. This attribute is empty if the asset does not belong to a target group. For more information, see Target Groups.
Tenable ID	The UUID of the agent present on the asset.
Terminated	Specifies whether or not the asset is terminated.
Type	The system type on which the asset is managed. Possible filter values are: • **Cloud Resource**

	• Container • Host • Cloud
Updated Date	The time and date when a user last updated the asset.
VPC	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.

Create a Tag via Asset Filters

Required User Role: Administrator

When you filter your assets, you can use the filters as tag rules to create a new automatic tag.

After you create the tag, Tenable Vulnerability Management automatically applies the tag to any assets identified through those filters.

You can also create a manual or automatic tag for your assets from the **Tagging** page.

To create a tag using asset filters:

1. In the left navigation, click **Assets**.

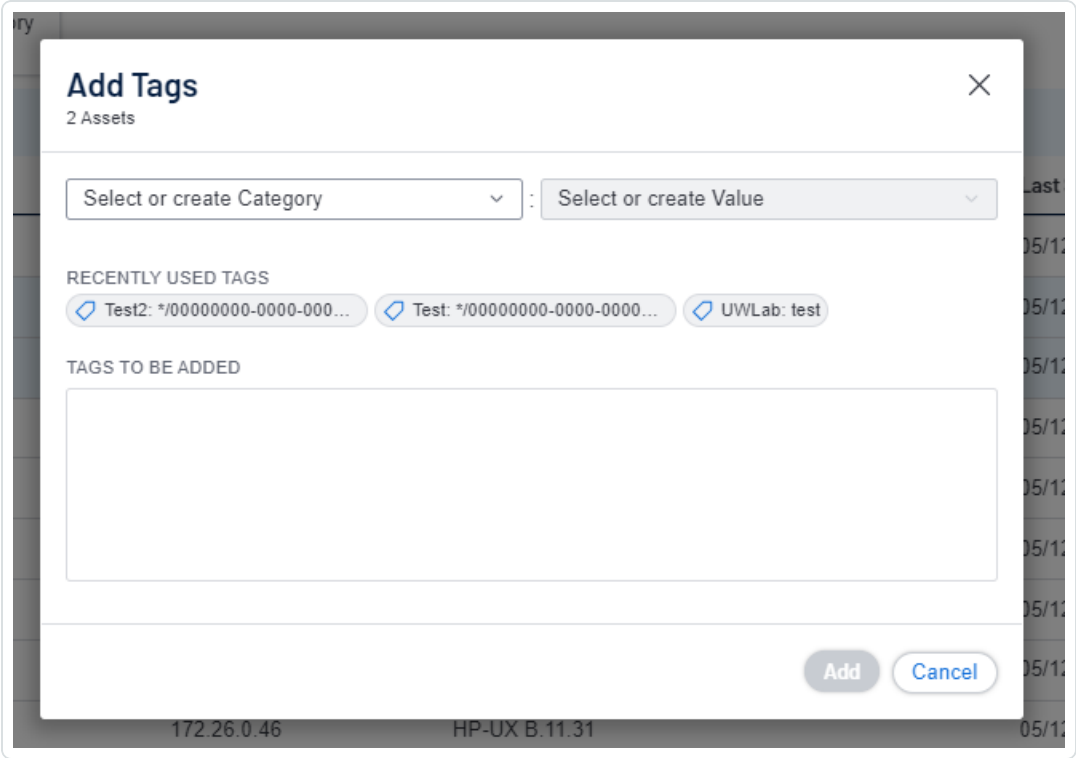
   The **Assets** workbench appears.

2. Filter the table, selecting and deselecting filters based on the rules you want to add to or remove from your tag.

   The filters you selected appear in the header above the filter plane.

3. In the header, to the left of the first filter, click **Add Tags**.

   The **Add Tags** window appears.



4. Under **Create/Select Tag**, in the first drop-down box, type a category.

   As you type, the list filters for matches.

5. In the drop-down box, select an existing category, or if the category is new, click **Create "*category*"**.

   Tip: You can create a generic tag category and apply to different tag values to group your tags. For example, if you create a *Location* category, you can apply it to multiple values such as *Headquarters* or *Offshore* to create a group of location tags.

6. Under **Create/Select Tag**, in the second drop-down box, type a value for your new tag.

7. In the drop-down box, click **Create "*value*"**.

8. Click **Save**.

   Tenable Vulnerability Management saves the tag and applies it to applicable assets on your account.

   Note: It can take up to several minutes for Tenable Vulnerability Management to apply a tag to the applicable assets.

Edit a Tag or Tag Category

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Required Tenable Vulnerability Management Permission: Can Edit, Can Use permission for applicable asset tags.

In the **Tagging** section, you can edit one or more components of a tag, including the category to which the tag belongs as well as the tag's name and description and any rules applied to the tag.

To edit a tag or tag category:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

3. To edit an individual tag:

   a. On the **Tags** page, click the **Values** tab.

      The **Values** page appears, containing a table with all the tags on your Tenable Vulnerability Management instance.

   b. In the **Values** table, click the tag you want to edit.

      The **Edit Value** page appears.

      Tip: You can also navigate to the **Edit Value** page from the **Edit Category** page by clicking the tag you want to review in the **Values** table.

   c. (Optional) In the **Value** box, edit the tag name.

   d. (Optional) In the **Value Description (Optional)** box, edit the tag description.

   e. (Optional) Configure the tag rules.

4. To edit the tag category:

> **Note**: When you edit a tag category, Tenable Vulnerability Management changes the category for all the tags in that category.

a. In the tag categories table, click the category you want to edit.

   The **Edit Category** page appears.

b. In the tag categories table, click the category you want to edit.

   The **Edit Category** page appears.

c. (Optional) To edit the name, in the **Category** box, type a new name.

d. (Optional) To edit the description, in the **Category Description** box, type a new description.

5. Click **Save**.

   Tenable Vulnerability Management saves and applies your changes.

Edit a Tag via Asset Filters

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

> **Required Tenable Vulnerability Management Permission:** Can Edit, Can Use permission for applicable asset tags.

On the **Assets** page, you can use asset filters to edit a tag's rules, category, and value.

To edit a tag using asset filters:

1. In the left navigation, click **Assets**.

   The **Assets** workbench appears.

2. Filter the table, selecting and deselecting filters based on the rules you want to add to or remove from your tag.

   The filters you applied appear in the header above the filter plane.

3. In the header, to the left of the first filter, click the button.

The **Tag Matching Assets** window appears.

4. Do one of the following:
   - To edit a recently used tag:
     a. Under **Recently Used Tags**, click the tag you want to edit.

        The tag category appears in the **Select or create Category** drop-down box.

        The tag value appears in the **Select or create Value** drop-down box.
   - To edit any other tag:
     a. In the **Select or create Category** drop-down box, type a category name.

        As you type, the list filters for matches.

     b. Select the category for the tag you want to edit.

     c. In the **Select or create Value** drop-down box, type a value name.

        As you type, the list filters for matches.

     d. In the drop-down box, select the value for the tag you want to edit.
5. (Optional) To edit the tag category:
   a. In the **Select or create Category** drop-down box, type a new name for your category.

      Create "*category***"** appears in the drop-down box.

   b. In the drop-down box, select **Create "***category***"**.

      The new category name appears selected in the drop-down box.
6. (Optional) To edit the tag value:
   a. In the **Select or create Value** drop-down box, type a new value for your tag.

      Create "*value***"** appears in the drop-down box.

   b. In the drop-down box, select **Create "***value***"**.

      The new value name appears selected in the drop-down box.

7. (Optional) In the **Chosen Search Filters for Tag** box, click the ✕ inside any filters you want to remove from the tag.
8. Click **Save**.

   Tenable Vulnerability Management saves your edits.

Add a Tag to an Asset

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

> **Required Tenable Vulnerability Management Permission:** Can Use permission for applicable asset tags.

After you create a tag, you can manually apply it to one or more assets on your Tenable Vulnerability Management instance.

To add a tag to an asset:

1. View your assets list.
2. Do one of the following:

   ### To add a tag to a single asset:

a. Select the page where you want to add the tag:

Location	Action
Assets page	To add a tag from the **Assets** page: a. In the assets table, right-click the row for the asset to which you want to add a tag. The action options appear next to your cursor. -or- In the assets table, in the **Actions** column, click the ⋮ button for the asset to which you want to add a tag. The action buttons appear in the row. b. Click **Add Tags**.
Asset Details page preview plane	To add a tag from the **Asset Details** page: a. In the assets table, click the row for the asset to which you want to add a tag. The preview plan for the asset's **Asset Details** page appears. b. In the left section of the preview plane, next to **Tags**, click the ⊕ button.
Asset Details page	To add a tag from the **Asset Details** page: a. View the **Asset Details** page for the asset from which you want to remove the tag. The **Asset Details** page appears. b. In the upper-right corner, click the **Actions** button.

	The actions menu appears. c. In the actions menu, click **Add Tag**. -or- On the left side of the page, next to **Tags**, click the ⊕ button.

The **Add Tags** window appears.

b. Click **Add**.

The assets table appears. A confirmation message also appears. Tenable Vulnerability Management adds the tags specified in **Tags to be Added** to the assets.

To add a tag to multiple assets:

a. In the assets table, select the check box for each asset to which you want to add a tag.

The action bar appears at the top of the table.

b. Click **Add Tags**.

The assets table appears. A confirmation message also appears. Tenable Vulnerability Management adds the tags specified in **Tags to be Added** to the assets.

3. Do one of the following:

To add a recently used tag:

- Under **Recently Used Tags**, select the tag you want to add.

The tag appears in the **Tags to be Added** box.

> **Tip:** To remove a tag from **Tags to be Added**, roll over the tag and click the ✕ button.

To add a new or existing tag:

a. In the **Category** box, type a category.

As you type, the list filters for matches.

b. From the drop-down box, select an existing category, or if the category is new, click **Create "***category name***"**.

> **Tip**: You can create a generic tag category and apply to different tag values to group your tags. For example, if you create a *Location* category, you can apply it to multiple values such as *Headquarters* or *Offshore* to create a group of location tags.

c. In the **Value** box, type a value.

As you type, the list filters for matches.

d. From the drop-down box, select an existing value, or if the value is new, click **Create "***value***"**.

> **Note:** The system does not save new tags you create by this method until you add the new tags to the asset.

The tag appears in the **Tags to be Added** box.

> **Tip:** To remove a tag from **Tags to be Added**, roll over the tag and click the ✕ button.

4. Click **Add**.

The assets table appears. A confirmation message also appears. Tenable Vulnerability Management adds the tags specified in **Tags to be Added** to the assets.

Remove a Tag from an Asset

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

> **Required Access Group Permissions**: Can View, Can Edit

When you manually add a tag to an asset or create a tag that Tenable Vulnerability Management automatically applies to that asset based on the tag's rules, you can manually remove from the asset if you want to exclude the asset from the tag's scope.

To remove a tag from an asset:

1. View your assets list.
2. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.
3. Do one of the following:

To remove a tag from single asset:

Select the page where you want to remove the tag from the asset:

Location	Action
Assets page	To remove a tag from an asset on the **Assets** page: a. In the assets table, right-click the row for the asset from which you want to remove a tag. The action options appear next to your cursor. -or- In the assets table, in the **Actions** column, click the ⋮ button for the asset from which you want to remove a tag. The action buttons appear in the row. b. Click **Remove Tags**. The **Remove Tags** window appears. c. Under **Current Tags**, roll over the tag you want to remove and click the ✕ button. The tag appears in the **Tags To Be Removed** box. **Tip:** To remove a tag from **Tags to be Removed**, roll over the tag and click the ✕ button.
Asset Details page	To remove a tag from an asset on the **Asset Details** page: a. View the **Asset Details** page for the asset from which you want to remove the tag.

b. Do one of the following:

- On the left side of the page, in the **Tags** section, roll over the tag you want to remove and click the ✕ button.
- To remove the tag via the **Actions** menu:

  i. In the upper-right corner, click the **Actions** button.

  The actions menu appears.

  ii. In the actions menu, click **Remove Tags**.

  The **Remove Tags** window appears.

  iii. Under **Current Tags**, roll over the tag you want to remove and click the ✕ button.

  The tag appears in the **Tags To Be Removed** box.

  > **Tip:** To remove a tag from **Tags to be Removed**, roll over the tag and click the ✕ button.

To remove a tag from multiple assets:

a. Search your assets by the tag you want to remove.

b. Do one of the following:

- To remove the tag from selected assets, in the assets table, select the check box next to each asset from which you want to remove the tag.
- To remove the tag from all your assets:

  i. In the assets table header row, select the check box next to the total number of assets.

  The action bar appears at the top of the table.

  All assets on the page are selected.

ii. Click **Select all [***total number of tagged assets***] assets**.

> **Note**: If you do not select all the tagged assets, Tenable Vulnerability Management removes the tag from the assets on only the current page.

c. In the action bar, click the **More** button.

A menu appears.

d. In the actions menu, click **Remove Tags**.

The **Remove Tags** window appears.

e. Under **Current Tags**, roll over the tag you want to remove and click the button.

The tag appears in the **Tags To Be Removed** box.

> **Tip:** To remove a tag from **Tags to be Removed**, roll over the tag and click the button.

4. Click **Remove**.

Tenable Vulnerability Management removes the selected tag from the assets.

Export Tags

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

On the **Tags** page, you can export tag categories and values in CSV or JSON format.

To export tag categories or values:

1. In the left navigation, click **Settings**.

The **Settings** page appears.

2. Click the **Tagging** tile.

The **Tags** page appears. On this page, you can view your asset tag categories and values.

The **Categories** tab is active.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

Note: You cannot filter the tables on the **Tags** page.

4. Do one of the following:

   To export tag categories:

   a. Select the tag categories that you want to export:

Export Scope	Action
Selected tag categories	To export selected tag categories: a. In the categories table, select the check box for each tag category you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 tag categories, select all the tag categories in the list and then click [→ **Export**.
A single tag category	To export a single tag category: a. In the categories table, right-click the row for the tag category you want you want to export. The action options appear next to your cursor. -or- In the categories table, in the **Actions** column, click the ⋮ button in the row for the tag category you want to export. The action buttons appear in the row. b. Click **Export**.

   To export tag values:

a. Click the **Values** tab.

   The **Values** tab appears. This tab consists of a table that contains all your tag values.

b. Select the tag values that you want to export:

Export Scope	Action
Selected tag values	To export selected tag values: a. In the values table, select the check box for each tag value you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 tag values, select all the tag values in the list and then click [→ **Export**.
A single tag value	To export a single tag value: a. In the categories table, right-click the row for the tag value you want you want to export. The action options appear next to your cursor. -or- In the values table, in the **Actions** column, click the ⋮ button in the row for the tag value you want to export. The action buttons appear in the row. b. Click **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  Note: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

5. In the **Name** box, type a name for the export file.
6. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of tag categories or values. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of tag categories or values. Empty fields are not included in the JSON file.

7. (Optional) Deselect any fields you do not want to appear in the export file.
8. In the **Expiration** box, type the number of days before the export file expires.

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

9. (Optional) To set a schedule for your export to repeat:

   - Click the **Schedule** toggle.

     The **Schedule** section appears.

- In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
- In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
- In the **Repeat** drop-down box, select how often you want the export to repeat.
- In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

  > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

10. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.
    - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

11. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

12. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Delete a Tag Category

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Required Tenable Vulnerability Management Permission: Can Edit, Can Use permission for applicable asset tags.

When you delete a tag category, Tenable Vulnerability Management deletes any tags created under that category and removes those tags from all assets where they were applied.

Caution: When you delete a tag category, all associated values and assignments are also deleted. If you want to remove a specific tag, see Delete a Tag .

To delete a tag category:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

3. Click the **Categories** tab.

   The tag categories table appears.

4. To delete one tag category:

   a. In the tags table, in the **Action** column , click the ⋮ button.

      A menu appears.

b. Click the **Delete** button.

   A confirmation window appears, asking if you are sure that you want to delete the category and all associated tags and assignments.

To delete multiple tag categories:

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

   The action bar appears at the bottom of the page.

b. In the action bar, click the **Delete** button.

   A confirmation window appears, asking if you are sure that you want to delete the category and all associated tags and assignments..

5. Click **Delete**.

   Tenable Vulnerability Management deletes the tag category and any associated tags, and removes those tags from all assets where you applied them.

Delete a Tag

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

> **Required Tenable Vulnerability Management Permission:** Can Edit, Can Use permission for applicable asset tags.

When you delete a tag, Tenable Vulnerability Management removes that specific tag from all assets where you applied the tag.

To delete one or more tags:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

The **Categories** tab is active.

3. Delete a one or more tags:

Scope of Deletion	Action
A single tag	To delete a single tag: a. Click the **Values** tab. The **Values** tab appears, displaying a table with all the tags on your Tenable Vulnerability Management instance in *Category:Value* format. b. In the tags table, right-click the row for the tag you want to delete. The action options appear next to your cursor. -or- In the tags table, in the **Actions** column, click the ⋮ button for the tag you want to delete. The action buttons appear in the row. c. Click **Delete**.
Multiple tags	To delete multiple tags: a. Click the **Values** tab. The **Values** tab appears, displaying a table with all the tags on your Tenable Vulnerability Management instance in *Category:Value* format. b. In the tags table, select the check box for each tag you want to delete. The action bar appears at the top of the table. c. In the action bar, click **Delete**.

	-or- Delete all tags in a category by deleting the tag category.

4. Click the **Values** tab.
5. To delete one tag:
   a. In the tags table, roll over the tag you want to delete.

      The action buttons appear in the row.

   b. Click the **Delete** button.

      A confirmation window appears.

   To delete multiple tags:

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

      The action bar appears at the bottom of the page.

   b. In the action bar, click the **Delete** button.

      A confirmation window appears.

6. Click **Confirm**.

   Tenable Vulnerability Management deletes the tag and removes it from all assets where you applied the tag.

Search for Assets by Tag from the Tags Table

Required Tenable Vulnerability Management User Role: Scan Operator, Standard, Scan Manager, or Administrator

You can see which assets have a specific tag applied by searching for assets by tag.

To search for assets by tag from the tags table:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

3. Click the **Values** tab.
4. In the table, click the ⋮ button.

   The actions menu appears.

5. Click **Search by Tag**.

   The **Assets** page appears and displays the assets table filtered by the tag you selected.

Sensors

Tenable Vulnerability Management supports the following sensor types:

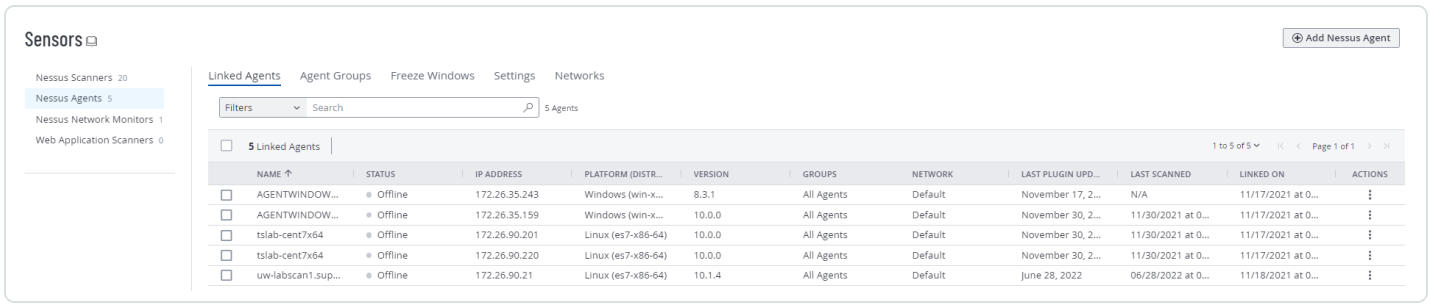
- Tenable-provided *regional cloud sensors*. For more information, see Cloud Sensors.
- Manually configured *linked sensors* (Tenable Nessus scanners, Tenable Network Monitor instances, Tenable Web App Scanning sensors, and Tenable Agents). For more information, see Linked Sensors.

Tip: For information on other ways to ingest data into Tenable Vulnerability Management, see the Data Ingestion in Tenable Vulnerability Management quick reference guide.

Agents

Agents increase scan flexibility by making it easy to scan assets without needing ongoing host credentials or assets that are offline. Agents allow for large-scale concurrent scanning with little network impact.

After you install a Tenable Agent on a host and link the agent to Tenable Vulnerability Management, the agent appears on the Tenable Vulnerability Management **Linked Agents** page.



Note: If you assign one or more agents to a network and any of those agents are already assigned to another custom network, a confirmation message appears indicating that, by adding agents to this network, they are reassigned from their previous networks.

Agents send the following information to Tenable Vulnerability Management:

- Version information (agent version, host architecture)
- Versions of installed Tenable plugins
- OS information (for example, `Microsoft Windows Server 2008 R2 Enterprise Service Pack 1`)
- Tenable asset IDs (for example, `/etc/tenable_tag` on Unix, `HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\TAG` on Windows)
- Network interface information (network interface names, MAC addresses, IPv4 and IPv6 addresses, hostnames and DNS information if available)
- Hostname if `update_hostname` is set to `yes` (see Tenable Agent Advanced Settings for more information)
- AWS EC2 instance metadata, if available:

  Note: Tenable Agent connect to 169.254.169.254 to provide AWS metadata to Tenable Vulnerability Management; traffic between Tenable Agent and 169.254.169.254 is normal and expected behavior.

  - `privateIp`
  - `accountId`
  - `imageId`
  - `region`

- instanceType
- availabilityZone
- architecture
- instanceId
- local-hostname
- public-hostname
- public-ipv4
- mac
- iam/security-credentials/
- public-keys/0/openssh-key
- security-groups

Note: Agents check in on start, after a restart, and whenever metadata is updated (no more than every 10 minutes).

Tip: For information on other ways to ingest data into Tenable Vulnerability Management, see the Data Ingestion in Tenable Tenable Vulnerability Management quick reference guide.

Agent Settings

On your agent's manager, you can configure global agent settings to specify agent and freeze window settings for all your linked agents. For more information on creating, modifying, and deleting freeze windows, see Freeze Windows.

You can also adjust log level, performance level, automatic hostname update, and automatic version update settings for individual agents. For more information, see Modify Remote Agent Settings .

Modify Remote Agent Settings

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

In Tenable Vulnerability Management, you can modify settings for individual agents (versions 7.6 and later) on the **Linked Agents** tab. For information on editing similar settings in the command line interface, see Advanced Settings in the *Tenable Agent User Guide*.

Note: In addition to using the following procedure, you can manually update agents through the command line. For more information, see the *Tenable Agent User Guide*.

To modify remote agent settings in Tenable Vulnerability Management:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. (Optional) Search for a specific agent or filter the agents in the table, as described in Filter Agents in the *Tenable Agent Deployment and User Guide*.

6. Do one of the following:

   ### To edit a single agent:

   a. In the agents table, in the row for the agent you want to edit, click the button.

      The **Edit Agent** window appears.

   b. Edit the agent settings:

Setting	Description	Default	Values
Nessus Agent Log Level	The logging level of the `backend.log` log file, as indicated by a set of log tags that determine what information to include in the log.	`normal`	• `normal` - Changes the backend.log logging level to `normal` and sets log tags to `"log", "info",`

	If you manually edited `log.json` to set a custom set of log tags for `backend.log`, this setting overwrites that content. For more information, see log.json Format in the *Tenable Nessus User Guide*.		`"warn", "error", "trace"` • `debug` - Changes the backend.log logging level to `debug` and sets log tags to `"log", "info", "warn", "error", "trace", "debug"` • `verbose` - Changes the backend.log logging level to `verbose`and sets log tags to `"log", "info", "warn", "error", "trace", "debug", "verbose"`
Plugin Compilation Performance	Sets plugin compilation	`high`	`low`, `medium`, or `high`

	performance, which affects CPU usage. Low performance slows down plugin compilation, but reduces the agent's CPU consumption. Setting the performance to medium or high means that plugin compilation completes more quickly, but the agent consumes more CPU. For more information, see Agent CPU Resource Control in the *Tenable Agent Deployment and User Guide*.		
Scan Performance	Sets scan performance, which affects CPU usage. Low performance slows down scans, but reduces the agent's CPU consumption. Setting the performance to	`high`	`low`, `medium`, or `high`

	medium or high means that scans complete more quickly, but the agent consumes more CPU. For more information, see Agent CPU Resource Control in the *Tenable Agent Deployment and User Guide*.		
Nessus Agent Update Plan	Sets the agent's update plan to determine what version the agent automatically updates to. **Note:** If you assign an agent an agent profile, the agent profile version overrides the **Nessus Agent Update Plan**. If you assign an agent a freeze window, the freeze window overrides both the **Nessus Agent Update Plan** and the agent profile.	`Keep up to date with GA releases`	`Keep up to date with GA releases`, `Opt in to Early Access releases`, or `Delay updates`, `staying on the last stable release`

	In this case, the agent remains on its current version and no software updates occur for that agent as long as the agent is assigned to the freeze window.		
Automatic Hostname Update	When enabled, when the hostname on the endpoint is modified the new hostname will be updated in the agent's manager. This feature is disabled by default to prevent custom agent names from being overridden.	no	yes or no
Offline Agent Scan Trigger Execution Threshold	Specifies the number of days an agent can be offline before rule-based scans stop executing.	14	Integers 1-48
Maximum Scans Per Day	Specifies the maximum number of scans to run on the agent per day.	10	Integers 1 or more

c. Click **Save**.

Tenable Vulnerability Management saves your settings, and the changes take effect the next time the agent checks in. For online agents, this can take up to 45 minutes.

If necessary for the setting changed, the agent restarts the next time it becomes idle.

To edit multiple agents:

a. Do one of the following:

- In the agents table, select the check box next to each agent you want to edit.
- In the table header, select the check box to select the entire page.

The action bar appears at the bottom of the page.

> **Tip:** In the action bar, select **Select All Pages** to select all linked agents.

b. In the action bar, click the ✎ button.

The **Edit Agents** window appears.

c. Edit the agent settings:

Setting	Description	Default	Values
Nessus Agent Log Level	The logging level of the `backend.log` log file, as indicated by a set of log tags that determine what information to include in the log. If you manually edited `log.json` to set a custom set of log tags for `backend.log`, this setting overwrites that content.	`normal`	• `normal` - Sets log tags to `"log", "info", "warn", "error", "trace"` • `debug` - Sets log tags to `"log", "info", "warn", "error", "trace",`

	For more information, see log.json Format in the *Tenable Nessus User Guide*.		`"debug"` • `verbose` - Sets log tags to `"log"`, `"info"`, `"warn"`, `"error"`, `"trace"`, `"debug"`, `"verbose"`
Plugin Compilation Performance	Sets plugin compilation performance, which affects CPU usage. Low performance slows down plugin compilation, but reduces the agent's CPU consumption. Setting the performance to medium or high means that plugin compilation completes more quickly, but the agent consumes more CPU. For more information, see Agent CPU Resource Control in	[[[Undefined variable Agent.Agent]]] 10.8.3 and later – `medium` [[[Undefined variable Agent.Agent]]] 10.8.2 and earlier – `high`	`low`, `medium`, or `high`

	the *Tenable Agent Deployment and User Guide*.		
Scan Performance	Sets scan performance, which affects CPU usage. Low performance slows down scans, but reduces the agent's CPU consumption. Setting the performance to medium or high means that scans complete more quickly, but the agent consumes more CPU. For more information, see Agent CPU Resource Control in the *Tenable Agent Deployment and User Guide*.	`high`	`low`, `medium`, or `high`
Automatic Hostname Update	When enabled, when the hostname on the endpoint is modified the new hostname will be updated in the agent's manager.	`no`	`yes` or `no`

	This feature is disabled by default to prevent custom agent names from being overridden.		
Nessus Agent Update Plan	Sets the agent's update plan to determine what version the agent automatically updates to. **Note:** If you assign an agent an agent profile, the agent profile version overrides the **Nessus Agent Update Plan**. If you assign an agent a freeze window, the freeze window overrides both the **Nessus Agent Update Plan** and the agent profile. In this case, the agent remains on its current version and no software updates	`Keep up to date with GA releases`	`Keep up to date with GA releases`, `Opt in to Early Access releases`, or `Delay updates, staying on the last stable release`

	occur for that agent as long as the agent is assigned to the freeze window.		
Offline Agent Scan Trigger Execution Threshold	Specifies the number of days an agent can be offline before rule-based scans stop executing.	14	Integers 1-48
Maximum Scans Per Day	Specifies the maximum number of scans to run on the agent per day.	10	Integers 1 or more

d. Click **Save.**

Tenable Vulnerability Management saves your settings, and the changes take effect the next time the agent checks in. For online agents, this can take up to 45 minutes.

If necessary for the setting changed, the agents restart the next time they become idle.

Modify Global Agent Settings

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Use this procedure to edit agent settings in Tenable Vulnerability Management.

To modify global agent settings in Tenable Vulnerability Management:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. Select **Settings** in the drop-down box.

   The **Settings** page appears.

4. Edit the settings as necessary:

Option	Description
Inactive Agents	
Unlink agents that have been inactive for *X* days	Specifies the number of days an agent can be inactive before the manager unlinks the agent. After the specified number of days, the agent is unlinked, but the corresponding agent data is not removed from the manager. Tenable Vulnerability Management automatically tracks unlinked agents and related data for the number of days specified in this option. You cannot turn off this tracking. **Note:** Inactive agents that were automatically unlinked by Tenable Vulnerability Management do *not* automatically relink if they come back online.
Override Freeze Windows	
Exclude all agents from software updates	Enable this option to prevent all linked agents from receiving software updates at any time. This option takes precedence over any existing freeze windows. Agents continue to receive plugin updates and perform scheduled scans if you enable this setting.

5. Click **Save**.

   Tenable Vulnerability Management saves your changes.

Agent Groups

You can use agent groups to organize and manage the agents linked to Tenable Vulnerability Management. You can add an agent to more than one group, and configure scans to use these groups as targets.

Use the following processes to create and manage agent groups:

- Create an Agent Group
- Add an Agent to an Agent Group
- Edit an Agent Group
- Delete an Agent Group
- Remove an Agent from an Agent Group
- View Agents in an Agent Group
- Agent Group Filters

Create an Agent Group

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

You can use agent groups to organize and manage the agents linked to your account. You can add an agent to more than one group and configure scans to use these groups as targets.

Use this procedure to create an agent group in Tenable Vulnerability Management.

To create a new agent group:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the drop-down box, select **Agent Groups**.

   The list of agent groups appears.

4. Click ⊕ **Add Agent Group**.

   The agent group settings plane appears.

5. In the **Group Name** box, type a name for the new agent group.

6. Configure user permissions for the agent group.

7. Click **Save**.

   The new agent group appears in the table.

What to do next:

- Use the agent group in an agent scan configuration.

Add an Agent to an Agent Group

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to add an agent to an agent group in Tenable Vulnerability Management. You can also add agents to a group when you modify an agent group.

To add an agent to agent groups:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the drop-down box, select **Agent Groups**.

   The list of agent groups appears.

4. (Optional) Search for a specific agent or filter the agents in the table. For filter descriptions, see Agent Filters.

5. Do one of the following:

   - To add a single agent to agent groups:

     a. In the agents table, roll over the agent you want to add.

        The action buttons appear in the row.

b. Click the 🗁 button.

The **Add to Groups** plane appears.

- To add multiple agents to agent groups, do one of the following:
  - In the agents table, select the check box next to each agent you want to add.
  - In the table header, select the check box to select the entire page.

  The action bar appears at the bottom of the page.

  > **Tip:** In the action bar, select **Select All Pages** to select all linked agents.

  a. In the action bar, click the 🗁 button.

  The **Add to Groups** plane appears.

6. Do one of the following:
   - If there are existing agent groups, select one:
     a. In the search box, search by agent group name.
     b. Click the agent group you want to select.
   - If there are no existing agent groups, create one:
     a. Click **add a new group**.

     The agent group settings plane appears.

     b. In the text box, type the name of the new group.
     c. In the **Users & Groups** section, set the user permissions for the new group.
     d. Click **Save**.

     The **Add to Groups** plane reappears. The new group appears in the selection list.
7. Click **Save** to save your changes.

   Tenable Vulnerability Management adds the agent to the selected group or groups.

Edit an Agent Group

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to modify an agent group in Tenable Vulnerability Management

To modify an agent group:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the drop-down box, select **Agent Groups**.

   The list of agent groups appears.

4. (Optional) Search for a specific agent group or filter the agent groups in the table. For filter descriptions, see Agent Group Filters.

5. Edit agent group settings:

   a. In the agents table, do one of the following:

      - In the **Actions** column, click the ⋮ icon for the agent you want to edit.

        The action options appear in the row.

      - Right-click the agent you want to edit.

        The action options appear next to your cursor.

      - Select the check box next to the agent you want to edit.

        The action bar appears at the top of the table.

   b. Click the **Edit** button.

      The **Edit Agent Group** plane appears.

   c. In the box, type a new name for the agent group.

   d. Configure user permissions for the agent group.

e. Click **Save** to save your changes.

   Tenable Vulnerability Management saves your changes.

6. Assign agents to an agent group:

   a. Click the row of the agent group where you want to add agents.

      The agent group details page appears.

   b. In the upper-right corner, click ⊕ **Assign Agents**.

      The assign agents page appears.

   c. (Optional) Search for a specific agent or filter the agents in the table. For filter descriptions, see Agent Filters.

   d. In the agents table, select the check boxes next to the agents you want to add to the agent group.

   e. Click **Assign**.

      Tenable Vulnerability Management adds the agents to the agent group, and the details page appears.

Delete an Agent Group

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to delete an agent group in Tenable Vulnerability Management.

To delete an agent group:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the drop-down box, select **Agent Groups**.

The list of agent groups appears.

4. (Optional) Search for a specific agent group or filter the agent groups in the table. For filter descriptions, see Agent Group Filters.
5. In the agents table, do one of the following:
   - In the row for the agent group you want to delete, in the Actions column, click the ⋮ button.

     The action options appear in the row.
   - Right-click the agent you want to delete.

     The action options appear next to your cursor.
   - Select the check box for the agent you want to delete.

     The action bar appears at the top.
6. Click **Delete**.

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

   Tenable Vulnerability Management deletes the agent group.

Remove an Agent from an Agent Group

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to remove an agent or agents from an agent group in Tenable Vulnerability Management.

To remove an agent from an agent group:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.
2. Click the **Nessus Agents** tab.

The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the drop-down box, select **Agent Groups**.

   The list of agent groups appears.

4. (Optional) Search for a specific agent group or filter the agent groups in the table. For filter descriptions, see Agent Group Filters.

5. In the agent groups table, click the agent group you want to modify.

   The **Group Details** page appears.

6. Remove selected agent groups.

To remove	Action
A single agent group	a. Do one of the following: • In the agents table, right-click the agent group you want to remove. The action buttons appear in the row. • In the row of the agent group you want to remove, in the **Actions** column, click the ⋮ button. The action buttons appear in the row. • Select the check box next to the agent group you want to remove. Tenable Vulnerability Management enables **More** > **Remove from Group**. b. Click **Remove from Group**.
Multiple agent groups	a. Do one of the following: • In the agents table, select the check box next to each agent you want to remove. • In the table header, select the check box to select the

	entire page. Tenable Vulnerability Management enables **More** > **Remove Selected from Group**. b. Click **Remove Selected from Group**.

Tenable Vulnerability Management removes the agent or agents from the group.

View Agents in an Agent Group

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Use this procedure to view agents in an agent group in Tenable Vulnerability Management.

To view agents in an agent group in the new interface:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the drop-down box, select **Agent Groups**.

   The list of agent groups appears.

4. (Optional) Search for a specific agent or filter the agents in the table. For filter descriptions, see Agent Filters.

5. In the agent groups table, click the agent group you want to view.

   The **Group Details** page appears. This page contains a table listing the agents assigned to the group.

Agent Group Filters

You can use the filters listed below to filter agent groups in the **Agent Groups** tab.

Category	Operator	Value

Name	is equal to is not equal to contains does not contain	In the text box, type the name of the agent group.
Creation Date	earlier than later than on not on	In the text box, type the date on which the agent group was created.
Last Modified	earlier than later than on not on	In the text box, type the date on which the agent group was last modified. Modifications include: • You modified the agent name or description. • You added an agent to the group. • You removed an agent from the group.

Agent Profiles

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

You can use agent profiles to apply a specific version to your linked agents. This can be helpful for testing; for example, you may want to schedule a testing period on a subset of your agents before upgrading all your agents to a new version.

An agent profile allows you to apply a newer version to a subset of your agents for a limited time, and more broadly, allows you to upgrade and downgrade agents to different versions easily. You can only assign an agent to one profile.

There are two types of agent profile:

- **Default** – The profile to which an agent or agent group belongs to unless you assign it to a custom profile. You cannot copy, delete, or edit the name and description of the **Default** profile.
- Custom profiles – A custom profile that you create. Custom profiles allow you to associate and configure different agents and agent groups based on your business needs.

Note: You cannot set agent profiles to versions earlier than 10.4.1. Agent profiles do not affect agents on versions earlier than 10.4.1.

Note: The agent profile version overrides the agent's Nessus Agent update plan setting. If you assign the agent a freeze window, the freeze window overrides both the Nessus Agent update plan and the agent profile. In this case, the agent remains on its current version and no software updates occur for that agent as long as the agent is assigned to the freeze window.

To manage agent profiles:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. Above the linked agents table, click **Profiles**.

   The **Profiles** page appears.

Use the following procedures to manage your agent profiles:

Create an agent profile:

Note: You cannot create an agent profile for an end-of-life (EOL) Tenable Agent version.

To create an agent profile:

1. On the **Profiles** page, click ⊕ **Add Agent Profile**.

   The **Create Agent Profile** page appears.

2. Configure the following settings for the agent profile:

Setting	Required	Default	Description
Name	Yes	n/a	The agent profile name.
Description	No	n/a	The agent profile description.
Agent Version	Yes	**None**	The version that agents assigned to the profile are upgraded or downgraded to. You can set the agent profile to stay on the latest major version release (for example, 10.x) or the latest minor version release (for example, 10.8.x), or you can set the agent profile to a specific patch release (for example, 10.8.1).
Open Agent Port (Advanced Asset Identification)	No	Disabled	Determines whether agents designate an open agent port on your scan targets and, if so, which port is opened. Enabling **Open Agent Port** allows Tenable scanners to identify scan targets that host the agents assigned to this profile. These hosts then appear as a single asset regardless of whether they are the target of a scanner's network scan or are generating agent scans. This helps minimize asset duplication in your network. To learn more

			about the **Open Agent Port**, see Configure Agent Profiles to Avoid Asset Duplication in Tenable Vulnerability Management in the *Tenable Agent User Guide*. **Note:** Configuring the **Open Agent Port** permits your network scanners to probe each target system on the port you select. **Note:** Only agents version 10.6.0 and later can use the **Open Agent Port** setting. The setting does not apply to any agent on an earlier version.
Plugin Update Setting	Yes	**Auto update to latest**	Determines what plugins Tenable Vulnerability Management installs on agents during the daily plugin update. Choose from the following options: • **Auto update to latest** – (Default) Update agents with the latest plugin set. • **Delay plugin updates by days** – Update agents with a delayed plugin set. The plugin set can be delayed by a minimum of

			one day and a maximum of 30 days. If multiple plugin sets were published on the configured day, Tenable Vulnerability Management installs the latest set of that day. • **Select plugin set from the last 30 days** – Update agents with a specific plugin set from the last 30 days. Tenable Vulnerability Management uses this plugin set until you choose another plugin set or update plan setting. **Note:** This setting only applies to agents on version 10.7.0 and later. **Note:** If an agent assigned to the agent profile has a later plugin set version than the plugin set version offered by **Plugin Update Setting**, the agent retains the newer set. In other words, you cannot use this setting to downgrade agent plugin sets.

Disable Agent Version Update	Yes	Disabled	Determines whether Tenable Vulnerability Management prevents the agents from receiving software updates. This setting overrides any scheduled freeze windows.
Enable Continuous Assessment Scan	Yes	Disabled	Determines whether the agents can perform continuous assessment scanning on their hosts. Continuous assessment scanning provides continuous monitoring and reporting of vulnerability status changes on your hosts. For more information, see Continuous Assessment Scanning. **Note:** Continuous assessment scanning is only available for Tenable Agents on Linux hosts. **Note:** Continuous assessment scanning requires a system user to run under. When continuous assessment is first started on an agent, the agent automatically creates a system user called **tenable_tua_comm**. The tenable_tua_comm user is a locked system user and cannot be used for logging in.

			Caution: Agents that have NIAP mode enforced cannot perform continuous assessment scanning. For more information on NIAP mode, see Configure Tenable Agent for NIAP Compliance and Tenable Agent CLI Commands in the *Tenable Agent User Guide*.
Baseline Scan Frequency	No, unless **Enable Continuous Assessment Scan** is selected	n/a	Configures how often you would like the agents to perform a full software inventory scan via continuous assessment scanning in days. You can choose any integer between **1** and **14**. This option only appears when you select **Enable Continuous Assessment Scan**.

3. Under **Assign Agents**, select the checkboxes next to the agents you want to assign.
4. Click **Create**. The agents' versions update the next time they check in with Tenable Vulnerability Management, which can take up to 24 hours.

View an agent profile ID:

You can link an agent to a profile by running the `nessuscli agent link` command and specifying the optional `--profile-uuid` argument. You can also link an agent to a profile during deployment by specifying the `profile-uuid` in the *config.json file*. Use the following procedure to view a profile's `--profile-uuid`.

To view an agent profile ID:

1. On the **Profiles** page, double-click the agent profile that you want to view the ID of.

   The **Sensor Profile Details** page appears.

2. In the **Details** tab, view the `--profile-uuid` under **Agent Profile ID**. You can click to copy the ID to your clipboard.

Edit an agent profile:

To edit an agent profile:

1. On the **Profiles** page, double-click the profile that you want to edit.

   The **Sensor Profile Details** page appears.

2. Edit the agent profile as needed:

Setting	Required	Default	Description
Name	Yes	n/a	The agent profile name.
Description	No	n/a	The agent profile description.
Agent Version	Yes	**None**	The version that agents assigned to the profile are upgraded or downgraded to. You can set the agent profile to stay on the latest major version release (for example, 10.x) or the latest minor version release (for example, 10.8.x), or you can set the agent profile to a specific patch release (for example, 10.8.1).
Open Agent Port (Advanced Asset Identification)	No	Disabled	Determines whether agents designate an open agent port on your scan targets and, if so, which port is opened.

			Enabling **Open Agent Port** allows Tenable scanners to identify scan targets that host the agents assigned to this profile. These hosts then appear as a single asset regardless of whether they are the target of a scanner's network scan or are generating agent scans. This helps minimize asset duplication in your network. To learn more about the **Open Agent Port**, see Configure Agent Profiles to Avoid Asset Duplication in Tenable Vulnerability Management in the *Tenable Agent User Guide*. **Note:** Configuring the **Open Agent Port** permits your network scanners to probe each target system on the port you select. **Note:** Only agents version 10.6.0 and later can use the **Open Agent Port** setting. The setting does not apply to any agent on an earlier version.
Plugin Update Setting	Yes	**Auto update to latest**	Determines what plugins Tenable Vulnerability Management installs on agents during the daily plugin update.

			Choose from the following options: • **Auto update to latest** – (Default) Update agents with the latest plugin set. • **Delay plugin updates by days** – Update agents with a delayed plugin set. The plugin set can be delayed by a minimum of one day and a maximum of 30 days. If multiple plugin sets were published on the configured day, Tenable Vulnerability Management installs the latest set of that day. • **Select plugin set from the last 30 days** – Update agents with a specific plugin set from the last 30 days. Tenable Vulnerability Management uses this plugin set until you choose another plugin set or update plan setting. **Note:** This setting only applies

			to agents on version 10.7.0 and later. **Note:** If an agent assigned to the agent profile has a later plugin set version than the plugin set version offered by **Plugin Update Setting**, the agent retains the newer set. In other words, you cannot use this setting to downgrade agent plugin sets.
Disable Agent Version Update	Yes	Disabled	Determines whether Tenable Vulnerability Management prevents the agents from receiving software updates. This setting overrides any scheduled freeze windows.
Enable Continuous Assessment Scan	Yes	Disabled	Determines whether the agents can perform continuous assessment scanning on their hosts. Continuous assessment scanning provides continuous monitoring and reporting of vulnerability status changes on your hosts. For more information, see Continuous Assessment Scanning. **Note:** Continuous assessment scanning is only available for Tenable Agents on Linux

			hosts. **Note:** Continuous assessment scanning requires a system user to run under. When continuous assessment is first started on an agent, the agent automatically creates a system user called **tenable_tua_comm**. The tenable_tua_comm user is a locked system user and cannot be used for logging in. **Caution:** Agents that have NIAP mode enforced cannot perform continuous assessment scanning. For more information on NIAP mode, see Configure Tenable Agent for NIAP Compliance and Tenable Agent CLI Commands in the *Tenable Agent User Guide*.
Baseline Scan Frequency	No, unless **Enable Continuous Assessment Scan** is selected	n/a	Configures how often you would like the agents to perform a full software inventory scan via continuous assessment scanning in days. You can choose any integer between **1** and **14**. This option only appears when you select **Enable Continuous Assessment Scan**.

3. Click **Save**.

Tenable Vulnerability Management saves your changes. The agents' versions update the next time they check in with Tenable Vulnerability Management, which can take up to 24 hours.

Copy an agent profile:

Copy an agent profile to create a duplicate of the existing agent profile. You can then use the duplicate to set up a new agent profile.

To copy an agent profile:

1. On the **Profiles** page, click ⋮ in the row of the profile that you want to copy.

   A menu appears.

2. Click **Copy**.

   Tenable Vulnerability Management creates a new profile with "Copy of" appended to the profile name.

Delete an agent profile:

Delete an agent profile if you no longer need the agent profile. You cannot undo an agent profile deletion.

To delete an agent profile:

1. On the **Profiles** page, click ⋮ in the row of the profile that you want to delete.

   A menu appears.

2. Click **Delete**.

   The **Delete Agent Profile** window appears.

3. Click **Delete** to confirm the deletion.

   Tenable Vulnerability Management deletes the agent profile and removes all the linked agents from the profile.

What to do next:

- Add or Remove Agents from Agent Profiles

Add or Remove Agents from Agent Profiles

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Use the following procedures to add an agent to an agent profile or remove an agent from an agent profile in Tenable Vulnerability Management. You can also add and remove agents from profiles from the **Sensor Profile Details** page. For more information, see Edit an agent profile.

In addition to using the Tenable Vulnerability Management user interface, you can link an agent to a profile by running the `nessuscli agent link` command and specifying the optional `--profile-uuid` argument. You can link an agent to a profile during deployment by specifying the `profile-uuid` in the *config.json file*. To find a profile's `profile-uuid`, see View an agent profile ID.

Note: The agent profile version overrides the agent's Nessus Agent update plan setting. If you assign the agent a freeze window, the freeze window overrides both the Nessus Agent update plan and the agent profile. In this case, the agent remains on its current version and no software updates occur for that agent as long as the agent is assigned to the freeze window.

Apply an agent profile to an agent

To apply an agent profile to an agent:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. Do one of the following:

   - To assign a single agent to an agent profile:

     a. Click ⋮ in the row of the agent that you want to assign to the profile.

        The action buttons appear in the row.

     b. Click **Apply Agent Profile**.

        The **Select Agent Profile** window appears.

c. In the table, select the checkbox of the agent profile that you want to assign the agent to.

d. Click **Apply**.

Tenable Vulnerability Management assigns the agent to the agent profile.

- To assign multiple agents to an agent profile, do one of the following:
  - In the agents table, select the check box next to each agent you want to add.
  - In the table header, select the check box to select the entire page.

  The action bar appears at the bottom of the page.

  > **Tip:** In the action bar, select **Select All Pages** to select all linked agents.

  a. In the action bar, click **Apply Agent Profile**.

  The **Select Agent Profile** window appears.

  b. In the table, select the checkbox of the agent profile that you want to assign the agents to.

  c. Click **Apply**.

  Tenable Vulnerability Management assigns the agents to the agent profile. The agents' versions update within 24 hours of the profile application.

Remove an agent profile from an agent

To remove an agent profile from an agent:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. Do one of the following:

- To remove a single agent from an agent profile:

  a. Click ⋮ in the row of the agent that you want to assign to the profile.

     The action buttons appear in the row.

  b. Click **Remove Agent Profile**.

     The **Remove Agent Profile** window appears.

  c. Click **Remove** to confirm.

     Tenable Vulnerability Management removes the agent from the agent profile.

- To remove multiple agents from an agent profile, do one of the following:

  - In the agents table, select the check box next to each agent you want to add.
  - In the table header, select the check box to select the entire page.

  The action bar appears at the bottom of the page.

  > **Tip:** In the action bar, select **Select All Pages** to select all linked agents.

  a. In the action bar, click **Remove Agent Profile**.

     The **Remove Agent Profile** window appears.

  b. Click **Remove** to confirm.

     Tenable Vulnerability Management removes the agents from the agent profile or profiles. The agents' versions update within 24 hours of the profile removal.

What to do next:

- Manage agent profiles

Freeze Windows

Freeze windows allow you to schedule times where certain agent activities are suspended for all linked agents. This activity includes:

- Receiving and applying software updates

Freeze windows do not prevent linked agents from:

- Receiving plugin updates
- Installing or executing agent scans

Note: Freeze windows override both agent profiles and the Nessus Agent update plan. If you assign an agent to a freeze window and enable the freeze window, any version updates that would normally occur due to an agent's agent profile or the agent's update plan are blocked.

To create and manage freeze windows:

- Create a Freeze Window
- Modify a Freeze Window
- Enable or Disable a Freeze Window
- Delete a Freeze Window

Create a Freeze Window

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Use this procedure to create freeze windows.

Freeze windows will apply to all linked agents and will prevent the agents from receiving and applying software updates during scheduled windows. Agents still receive plugin updates and continue performing scheduled scans during these windows.

To create a freeze window for linked agents:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the drop-down box, select **Freeze Windows**.
4. Click ⊕ **New Freeze Window**.

The **New Freeze Window** plane appears.

5. Configure the options as necessary.
6. Click **Save**.

   The freeze window is saved and appears on the **Freeze Windows** psge.

Edit a Freeze Window

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to manage a freeze window for agent scanning in Tenable Vulnerability Management.

To edit a freeze window:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the drop-down box, select **Freeze Windows**.

   The list of freeze windows appears.

4. In the freeze window table, click the freeze window you want to modify.

   The **Update a Freeze Window** page appears.

5. Edit the options as necessary.
6. Click **Save** to save your changes.

   Tenable Vulnerability Management saves the changes to the freeze window.

Enable or Disable a Freeze Window

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to enable or disable a freeze window for linked agents in Tenable Vulnerability Management.

To enable or disable a freeze window for linked agents in the new interface:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the drop-down box, select **Freeze Windows**.

4. Search for the freeze window you want to enable or disable.

5. In the row for the freeze window you want to enable or disable, click the **Status** toggle.

   The freeze window is enabled or disabled and a confirmation window appears.

Export Freeze Windows

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

On the **Sensors** page, you can export one or more freeze windows in CSV or JSON format.

To export your freeze windows:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the drop-down box, select **Freeze Windows**.

   The list of freeze windows appears.

4. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

5. Export selected freeze windows.

Scope	Action
To export a single freeze window	a. In the freeze windows table, do one of the following: • Right-click the row for the freeze window you want to export. The action options appear in the row. • In the **Actions** column, click the ⋮ button in the row for the freeze window you want to export. The action options appear in the row. • Select the check box for the freeze window you want to export The action bar appears at the top of the table. b. Click [→ **Export**.
To export multiple freeze windows	a. In the freeze windows table, select the check box for each freeze window you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note**: You can individually select and export up to 200 freeze windows. If you want to export more than 200 freeze windows, you must select all the freeze windows on your Tenable Vulnerability Management instance by selecting the check box at the top of the freeze windows table and then click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

> **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the email notification.

6. In the **Name** box, type a name for the export file.
7. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of freeze windows. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of freeze windows. Empty fields are not included in the JSON file.

8. (Optional) Deselect any fields you do not want to appear in the export file.
9. In the **Expiration** box, type the number of days before the export file expires.

> **Note**: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

10. (Optional) To send email notifications on completion of the export:

> **Note**: You can enable email notifications with or without scheduling exports.

- Click the **Email Notification** toggle.

  The **Email Notification** section appears.

- In the **Add Recipients** box, type the email addresses to which you want to send the export notification.

- (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

  > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

11. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

12. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the Export Management View.

Delete a Freeze Window

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

Use this procedure to delete a freeze window for agent scanning in Tenable Vulnerability Management.

To delete a freeze window for agent scanning:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the drop-down box, select **Freeze Windows**.

   The list of freeze windows appears.

4. Delete the selected freeze windows:

Scope	Action
Delete a single freeze window	a. In the freeze window table, do one of the following: • Right-click the window you want to delete. The action options appear in the row. • In the **Actions** column, click the ⋮ button in the row for the freeze window you want to delete. The action options appear in the row. • Select the check box for the freeze window you want to delete. The action bar appears at the top of the table. b. Click **Delete**. A confirmation window appears.
Delete multiple freeze windows	a. In the freeze windows table, select the check box next to each window you want to delete. The action bar appears at the top of the table. b. Click **Delete**. A confirmation window appears.

5. Click **Delete** to confirm the deletion.

   Tenable Vulnerability Management deletes the selected freeze window or windows.

Retrieve the Tenable Agent Linking Key

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

Before you begin the Tenable Agents installation process, you must retrieve the agent linking key from Tenable Vulnerability Management.

To retrieve the agent linking key:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. Click **Add Nessus Agent**.

   The **Add Agent** plane appears.

4. Click the **Copy** button to copy the **Linking Key**.

   A **Linking key copied to clipboard** confirmation message appears.

What to do next:

- Install Tenable Agent

Download Linked Agent Logs

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

In Tenable Vulnerability Management, you can request and download a log file containing logs and system configuration data from any of your linked agents. This information can help you troubleshoot system problems and easily provide data for Tenable Support.

You can store a maximum of five log files from each agent. Once the limit is reached, you must remove an old log file to download a new one. After you request an agent log file, Tenable Vulnerability Management retains the log file for seven days.

Note: You can only download agent logs when the agent is online. The Tenable Vulnerability Management **Logs** tab disappears when the selected agent is offline.

Tip: If Tenable Vulnerability Management identifies your agent as offline unexpectedly, Tenable recommends running the `nessuscli bug-report-generator` command on the agent to troubleshoot.

To download logs from a linked agent in Tenable Vulnerability Management:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the agents table, click the agent for which you want to download logs.

   The details page for that agent appears.

4. Click the **Logs** tab.

   A table shows any previously downloaded logs.

5. In the upper-right corner, click **Request Logs**.

   > **Note:** If you have reached the maximum of five log files, the **Request Logs** button is disabled. Remove an existing log before downloading a new one.

   Tenable Vulnerability Management requests the logs from the agent the next time it checks in, which may take several minutes. You can view the status of the request in the user interface until the download is complete.

   Once you request agent logs, Tenable Vulnerability Management retains the logs for seven days.

6. To download the log file, click the button.

   The system downloads the log file.

To remove an existing log:

1. In the row of the log you want to remove, click the button.

   A confirmation window appears.

2. In the confirmation window, click **Delete**.

   Tenable Vulnerability Management deletes the log and removes it from the table.

To cancel a pending or failed log request:

- In the row of the pending or failed log request that you want to cancel, click the ⏸ button.

  Tenable Vulnerability Management cancels the log request and removes it from the table.

Restart an Agent

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

In Tenable Vulnerability Management, you can restart linked agents (versions 7.6 and later) on the **Linked Agents** tab.

To restart an agent:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. (Optional) Search for a specific agent or filter the agents in the table.

6. Do one of the following:

   ##### To restart a single agent:

   a. In the agents table, in the row for the agent you want to restart, click the ↻ button.

      The **Restart Agent** window appears.

   b. Select one of the following **Restart Types**:

Restart Type	Description
Soft	Restart the agent backend without restarting the service.
Hard	Restart the agent backend and service.
Idle	Restart the agent backend and service when the agent is not running a scan.

c. Click **Save**.

Tenable Vulnerability Management saves your settings, and the changes take effect the next time the agent checks in. For online agents, this can take up to 45 minutes.

To restart multiple agents:

a. Do one of the following:

- In the agents table, select the check box next to each agent you want to restart.
- In the table header, select the check box to select the entire page.

The action bar appears at the bottom of the page.

> **Tip:** In the action bar, select **Select All Pages** to select all linked agents.

b. In the action bar, click the ↻ button.

The **Restart Agents** window appears.

c. Select one of the following **Restart Types**:

Restart Type	Description
Soft	Restart the agent backend without restarting the service.
Hard	Restart the agent backend and service.
Idle	Restart the agent backend and service when the agent is not running a scan.

d. Click **Save**.

Tenable Vulnerability Management saves your settings, and the changes take effect the next time the agent checks in. For online agents, this can take up to 45 minutes.

Unlink an Agent

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

When you manually unlink an agent, the agent is removed from the **Agents** page, but the system retains related data for the period of time specified in agent settings. When you manually unlink an agent, the agent does not automatically relink to Tenable Vulnerability Management.

> **Tip:** You can configure agents to automatically unlink if they are inactive for a certain number of days, as described in agent settings.

To unlink agents in Tenable Vulnerability Management:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. (Optional) Search for a specific agent or filter the agents in the table. For filter descriptions, see Agent Filters.

4. Select the agent you want to unlink:

Scope	Action
Unlink a single agent	To unlink an agent from the **Nessus Agents** tab: a. In the agents table, right-click the row for the agent you want to unlink. -or- In the row of the agent you want to unlink, in the **Actions** column, click the ⋮ button. The action buttons appear in the row. -or- Select the check box next to the agent you want to unlink. In the action bar, Tenable Vulnerability Management enables **More** > **Unlink Selected**. b. Click **Unlink** or **Unlink Selected**, as applicable.
Unlink multiple agents	To unlink multiple agents from the **Nessus Agents** tab: a. Select the check box next to the agents you want to unlink. In the action bar, Tenable Vulnerability Management enables **More** > **Unlink Selected**. b. Click **Unlink Selected**.

Tenable Vulnerability Management unlinks the agents.

Rename an Agent

You can rename your linked agents from the **Sensors** menu. This can be helpful for making agents more recognizable to other users.

To rename an agent:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. Click the row of the agent you want to rename.

   The agent **Details** page appears.

4. Click the button next to the agent name.

5. Edit the agent name.

6. Click the button next to the agent name.

   Tenable Vulnerability Management saves the new agent name and updates any related tables with the new name.

View Linked Agent Health Events

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

In Tenable Vulnerability Management, you can view information about the health of the Tenable Agent software on your installed endpoints linked to Tenable Vulnerability Management. You can use the agent health information to troubleshoot agent issues, or you can forward the agent health information to Tenable support.

Tenable Vulnerability Management-linked agents provide health event updates every 60 minutes by default.

To view a linked agent's health events in Tenable Vulnerability Management:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. In the agents table, click the agent for which you want to view health events.

   The details page for that agent appears.

4. Click the **Agent Health Events** tab.

   A table shows the linked agent's health events. Tenable Vulnerability Management shows the events in the detected order (the newest event shows at the top of the table). The table shows the following information about each health event:

Column	Description

Type	The agent health event type:
	• **Comms Backoff State** (related to continuous assessment scanning)
	  • Check Frequency – Every hour
	  • Possible States – **HEALTHY** (last Tenable Vulnerability Management upload was successful), **WARNING** (last Tenable Vulnerability Management upload was not successful), **CRITICAL** (last Tenable Vulnerability Management upload was not successful and received a 409 error)
	• **Comms Waiting Batches** (related to continuous assessment scanning)
	  • Check Frequency – Every hour
	  • Possible States – **HEALTHY** (0-9 events waiting to upload), **WARNING** (10-39 events waiting to upload), **CRITICAL** (> 39 events waiting to upload)
	• **Module Asset Identity**
	  • Check Frequency – Every 60 seconds
	  • Possible States – **HEALTHY**, **CRITICAL** (the open agent

port service is not working, even though it is configured for the agent profile)

- **Module Runtime Scan** (related to continuous assessment scanning)
  - Check Frequency – Every 60 seconds
  - Possible States – **HEALTHY**, **CRITICAL** (the continuous assessment scanning service is not working, even though it is configured for the agent profile)
- **Module Comms** (related to continuous assessment scanning)
  - Check Frequency – Every 60 seconds
  - Possible States – **HEALTHY**, **CRITICAL** (the agent cannot successfully send continuous assessment scanning data to Tenable Vulnerability Management)
- **Plugin Compilation**
  - Check Frequency – Once upon agent startup
  - Possible States – **HEALTHY**, **CRITICAL** (agent plugin compilation failure)
- **Plugin Disk Usage**

  Note: This event only shows for Tenable Agents on version 10.8.0 or later.

  - Check Frequency – Once upon agent startup
  - Possible States – **HEALTHY**, **WARNING** (< 2,000 MB disk space remaining)
- **Plugin Integrity Checks**
  - Check Frequency – Every 24 hours
  - Possible States – **HEALTHY**, **CRITICAL** (the plugins

	database failed an integrity check)
	• **Plugin Updates**
	  • Check Frequency – Every 24 hours, or whenever the agent plugins are updated
	  • Possible States – **HEALTHY**, **CRITICAL** (the agent cannot successfully update plugins)
	• **System Disk Usage**
	  • Check Frequency – Every 60 seconds
	  • Possible States – **HEALTHY**, **WARNING** (< 350 MB disk space remaining), **CRITICAL** (< 150 MB disk space remaining)

Status	• **Healthy** – The health event is healthy and requires no action. • **Warning** – The health event is unhealthy and may cause minimal impact on the agent's performance. • **Critical** – The health event is unhealthy and may cause a major impact on the agent's performance. Tenable recommends working to resolve any **Critical** health events. • **Unknown** – The health event status is currently unknown.
Summary	The summary of the health event's current status. For more information about negative health events, see the **Recommended Action** column of the Health Event Troubleshooting table.
Last Updated	The date and time at which Tenable Vulnerability Management last updated the health event.
Resolved	Indicates whether the health event was resolved (in other words, whether the event recently changed from **Warning** or **Critical** to **Healthy**).

	If this column shows **N/A**, Tenable Vulnerability Management has not recently detected a health problem for the **Type**.
Previous Status	The previous health event status before the **Last Updated** date and time. • **Healthy** – The health event is healthy and requires no action. • **Warning** – The health event is unhealthy and may cause minimal impact on the agent's performance. • **Critical** – The health event is unhealthy and may cause a major impact on the agent's performance. Tenable recommends working to resolve any **Critical** health events. • **Unknown** – The health event status is currently unknown.
Previous Summary	The summary of the health event's **Previous Status**.
Previously Updated	The date and time at which Tenable Vulnerability Management previously updated the event before the **Last Updated** date and time.

Health Event Troubleshooting

Event Type	Negative Event Summary	Recommended Action
Comms Backoff State	• *There are __ items waiting to upload."*	Contact Tenable support.
Comms Waiting Batches	• *Service is in a temporary backoff*	Contact Tenable support.

	due to <error code>. • *Service is in a 24 hour backoff due to code 409.*	
Module Asset Identity	• *Incorrect module state.*	Check to see if IPv6 is disabled on the agent host by viewing the following log file: • Linux – `/opt/nessus_agent/var/nessus/mod/com.tenable.agent_identifier_service/data/com.tenable.agent_identifier_service.log` • Windows – `C:\ProgramData\Tenable\Nessus Agent\nessus\mod\com.tenable.agent_identifier_service\data\com.tenable.agent_identifier_service.log` • macOS – `/Library/NessusAgent/run/var/nessus/mod/com.tenable.agent_identifier_service/data/com.tenable.agent_identifier_service.log` If you see the following messages, IPv6 has been disabled, and you must enable it for the asset identity module to run properly. `[2024-12-05 19:29:48 +0000][2970.0][severity=INFO] : Launching asset UUID service on port XXXX`

		<pre>[2024-12-05 19:29:48 +0000][2970.0][severity=INFO] : Unable to create socket: Address family not supported by protocol
		[2024-12-05 19:29:48 +0000][2970.0][severity=INFO] : Socket was not opened.
		[2024-12-05 19:29:48 +0000][2970.0][severity=INFO] : Socket not valid</pre>
		Note: On all operating systems, the **Open Agent Port** agent profile setting in Tenable Vulnerability Management requires the operating system to have a basic level of IPv6 support, though IPv6 itself does not have to be enabled on any network interfaces. On Linux, this may cause problems in older Linux distributions following configuration guides that used to recommend disabling the Linux IPv6 driver via kernel boot parameters. On such a system, you can disable IPv6 via sysctl parameters in /etc/sysctl.conf, instead of disabling them on the kernel boot command line. This allows the asset UUID service to function without allowing IPv6 to be enabled on such a system.
		<pre>net.ipv6.conf.all.disable_ipv6 = 1
		net.ipv6.conf.default.disable_ipv6 = 1</pre>
		If you do not disable IPv6 using this method, you may experience negative health events related to the asset identity module.
		For more information, see Configure Agent Profiles to Avoid Asset Duplication in Tenable Vulnerability Management in the *Tenable Agent User Guide*.
		If the issue is unrelated to IPv6, contact Tenable support.

Module Runtime Scan	• *Incorrect module state.*	Contact Tenable support.
Module	• *Incorrect*	Contact Tenable support.

Comms	*module state.*	
Plugin Compilation	• *Plugin compilation failed for _ plugins. Failed plugin names: _*	Contact Tenable support.
Plugin Disk Usage	• *Nessus Agent plugin disk usage is abnormally high. Plugin disk usage is more than _ MB.*	Contact Tenable support.
Plugin Integrity Checks	• *The plugins database failed an integrity check. The Nessus Agent*	Wait for the plugin integrity checks to re-run after the full plugin update. If the problem persists, contact Tenable support.

	will try to resolve this by triggering a full plugin update. • *Plugin integrity check failed on the following files: _* • *Plugin integrity check failed on many files, including: _*	
Plugin Updates	• *The Nessus Agent could not update plugins because the download failed*	Allow the agent to retry the daily plugin update. If the problem persists, check your network and antivirus settings for any issues that may affect the agent's ability to download properly.

	due to an error. Failed plugin updates are retried daily. [Status code: _ / HTTP Status code: _] • *The Nessus Agent could not update plugins because the integrity check of the download failed. Failed plugin updates are retried daily.*	
System	• *Available*	Free the amount of disk space suggested in the event

Disk Usage	*disk space for the Nessus Agent is [getting low or critically low]. Free disk space is less than _ MB.*	summary.

Export Linked Agents

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

On the **Sensors** page, you can export one or more linked agents in CSV or JSON format.

To export your linked agents:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

4. Select the linked agents that you want to export:

Export Scope	Action

A single linked agent	To select and export a single linked agent: a. In the linked agents table, right-click the row for the linked agent you want to export. The action options appear in the row. -or- In the linked agents table, in the **Actions** column, click the ⋮ button in the row for the linked agent you want to export. The action options appear in the row. -or- In the linked agents table, select the check box of the agent you want to export. The action bar appears at the top of the table. b. Click [→ **Export**.
Multiple linked agents	To select and export multiple linked agents: a. In the linked agents table, select the check box for each linked agent you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 linked agents, select all the linked agents in the list and then click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.

- A table of configuration options for fields to include in the exported file.

  Note: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the email notification.

5. In the **Name** box, type a name for the export file.
6. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of linked agents.
JSON	A JSON file that contains a nested list of linked agents. Empty fields are not included in the JSON file.

7. (Optional) Deselect any fields you do not want to appear in the export file.
8. In the **Expiration** box, type the number of days before the export file expires.

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

9. (Optional) To send email notifications on completion of the export:

   Note: You can enable email notifications with or without scheduling exports.

   - Click the **Email Notification** toggle.

     The **Email Notification** section appears.

   - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
   - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

> **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

10. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

11. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Export Linked Agent Details

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

On the **Details** page for any linked agent, you can export details about your linked agent in CSV or JSON format.

To export details about a linked agent:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

4. In the linked agents table, click the linked agent for which you want to export details.

   The **Details** page appears.

5. In the upper-right corner, click [→ **Export**.

   The **Export** plane appears. This plane contains:

   - A text box to configure the export file name.
   - A list of available export formats.
   - A table of configuration options for fields to include in the exported file.

     > **Note**: By default, all fields are selected.

   - A text box to set the number of days before the export expires.
   - A toggle to configure the export schedule.
   - A toggle to configure the email notification.

6. In the **Name** box, type a name for the export file.
7. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of your linked agent details, organized by fields. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of your linked agent details, organized by fields. Empty fields are not included in the JSON file.

8. (Optional) Deselect any fields you do not want to appear in the export file.
9. In the **Expiration** box, type the number of days before the export file expires.

> **Note**: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

10. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

    - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.

    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

11. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

12. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

The `agents.csv` file exported from Tenable Vulnerability Management contains the following data:

Field	Description
Agent Name	The name of the agent.
Status	The status of the agent at the time of export. Possible values are `unlinked`,

	`online`, or `offline`.
IP Address	The IPv4 or IPv6 address of the agent.
Platform	The platform the agent is installed on.
Profile Name	The name of the agent's assigned agent profile.
Profile UUID	The UUID of the agent's assigned agent profile.
Groups	The names of any groups the agent belongs to.
Group IDs	The group IDs of any groups the agent belongs to.
Version	The version of the agent.
Last Plugin Update	The date (in ISO-8601 format) the agent's plugin set was last updated.
Agent ID	The ID of the agent.
Agent UUID	The UUID of the agent.
Linked On	The date (in ISO-8601 format) the agent was linked to Tenable Vulnerability Management.
Last Connect	The date (in ISO-8601 format) of the agent's last check-in.
Last Scanned	The date (in ISO-8601 format) the agent was last scanned.

Filter Agents

To filter agents in the agents table in Tenable Vulnerability Management

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. In the left navigation menu, click **Nessus Agents**.

   The **Linked Agents** page appears.

3. Above the agents table, click the **Filters** button.

The **Filters** pane appears.

4. Configure the options as necessary. Depending on the parameter you select, different options appear:

Category	Operator	Value
Distro	contains does not contain	In the text box, type the distribution name on which you want to filter.
IP Address	is equal to is not equal to contains does not contain	In the text box, type the IPv4 or IPv6 addresses on which you want to filter.
Last Connection Last Plugin Update Last Scanned	earlier than later than on not on	In the text box, type the date on which you want to filter.
Member of Group	is equal to is not equal to	From the drop-down list, select from your existing agent groups.
Name	is equal to is not equal to contains	In the text box, type the agent name on which you want to filter.

Category	Operator	Value
	does not contain	
Platform	contains does not contain	In the text box, type the platform name on which you want to filter.
Status	is equal to is not equal to	In the drop-down list, select an agent status.
Version	is equal to is not equal to contains does not contain	In the text box, type the version you want to filter.

5. Click **Apply**.

   The manager filters the list of agents to include only those that match your configured options.

Agent Filters

Tenable Vulnerability Management supports filtering agents by the following categories:

Category	Operator	Value
Distro	contains does not contain	In the text box, type the distribution name on which you want to filter.
IP Address	is equal to is not equal to	In the text box, type the IPv4 or IPv6 addresses on which you want to filter.

Category	Operator	Value
	contains does not contain	
Last Connection Last Plugin Update Last Scanned	earlier than later than on not on	In the text box, type the date on which you want to filter.
Member of Group	is equal to is not equal to	From the drop-down list, select from your existing agent groups.
Name	is equal to is not equal to contains does not contain	In the text box, type the agent name on which you want to filter.
Platform	contains does not contain	In the text box, type the platform name on which you want to filter.
Safe Mode	is equal to is not equal to	In the drop-down list, select whether you want to filter agents for which safe mode is **Enabled** or **Disabled**. You can also filter by **N/A** to filter the agents that do not have safe mode capabilities.
Status	is equal to	In the drop-down list, select an agent status.

Category	Operator	Value
	is not equal to	
UUID	is equal to is not equal to	In the text box, type the agent UUID that you want to filter. You can use either of the following agent UUID formats: • xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (for example, `885c5f3e-aca3-42bf-9355-ace1c71bfe9a`) • xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx (for example, `885c5f3eaca342bf9355ace1c71bfe9a`) You can find the agent's UUID by viewing the agent's details in the Tenable Vulnerability Management user interface, or by running the `# nessuscli agent status --show-uuid` command.
Version	is equal to is not equal to contains does not contain	In the text box, type the version you want to filter.

Agent Status

Tenable Agents can be in one of the following statuses:

Status	Description
Online	The host that contains the Tenable Agent is currently connected and in communication with Tenable Vulnerability Management.
Offline	The host that contains the Tenable Agent is currently powered down or not connected to a network.

Status	Description
	In Tenable Vulnerability Management, the **Offline** status appears after the agent has not been connected for two hours.
Initializing	The Tenable Agent is in the process of checking in with Tenable Vulnerability Management.

Plugin Updates

The following table describes the behavior of differential plugin updates for agents linked to Tenable Vulnerability Management:

Linked	Differential Update	Full Update
Tenable Vulnerability Management	The agent requests differential updates from Tenable Vulnerability Management once every 24 hours.	The agent performs a full plugin update at scan time whenever the agent needs all plugin sets for certain scan policies. The agent also deletes unused plugin sets after a configurable amount of time. After the amount of time passes, the agent performs a full update and deletes the unused plugin sets. For more information, see the `days_to_keep_unused_plugins` advanced setting.

Connection Disruptions

In the event of agent connectivity disruption in Tenable Vulnerability Management, the agent tests connectivity approximately every 30 minutes.

Once connectivity is restored, the agent attempts to upload the scan result. After three failed upload attempts, the agent stops attempting.

- When using a scan window, once an agent completes a scan, it uploads its scan results. As long as the window is active, Tenable Vulnerability Management accepts the results. If the

agent fails to upload its scan results during the window, the results are discarded. The agent re-scans and re-uploads during the next window.

- When using a triggered scan, once an agent completes a scan, it uploads its scan results. If there are connectivity interruptions during transmission, the agent waits until connectivity is restored and attempts to upload the scan result. If the agent fails to upload the result three times, the agent re-scans and re-uploads the results upon the next trigger.

  An agent that is offline for an extended time continues to scan if the trigger is met, replaces the previous scan results, and uploads the results once connectivity is restored.

  > **Tip:** You can use the **Offline Agent Scan Trigger Execution Threshold** agent setting configure the number of days an agent can be offline before it stops executing triggered scans. For more information, see Modify Remote Agent Settings .

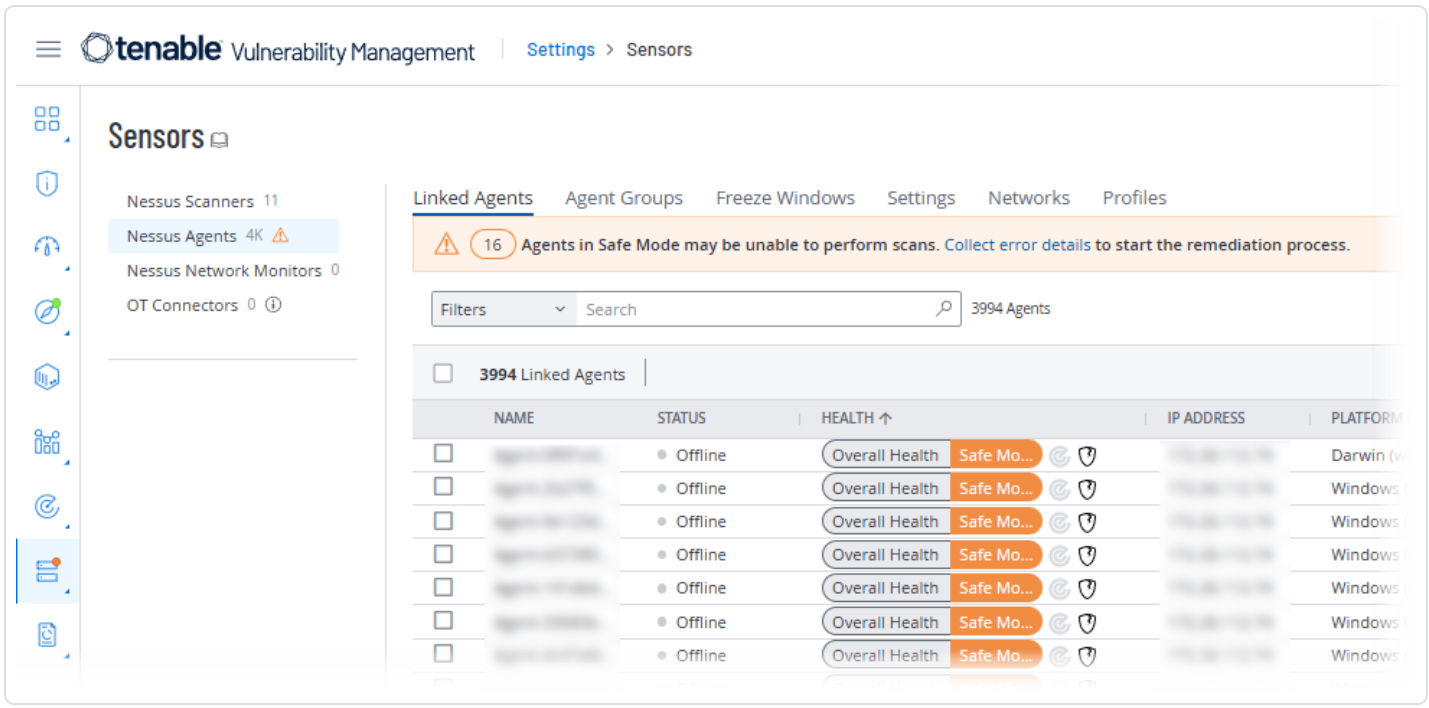
Agent Safe Mode

When Tenable Agent experiences an error, the agent automatically enters *safe mode*. While the agent is in safe mode, it cannot compile plugins or run scans, but it maintains connection with Tenable Vulnerability Management so that your organization can see that an error occurred, work to remediate the error, and remotely recover the agent.

For a deeper explanation of agent safe mode, see Safe Mode in the *Tenable Agent User Guide*.

> **Note:** Agents on an earlier version than 10.9.0 do not have safe mode capabilities.

When a linked agent enters safe mode, Tenable Vulnerability Management notifies you on the **Sensors** menu icon and the **Nessus Agents** > **Linked Agents** tab. The **Linked Agents** menu shows a banner describing how many agents are currently in safe mode, and each agent in safe mode is marked with **Overall Health: Safe Mode** in the **Health** column of the linked agents table.



To remediate and recover agents that are in safe mode, you can report agents that are in safe mode on connect.tenable.com for Tenable Support assistance, or you can use the **Linked Agents** menu to self-remediate.

Note: Tenable strongly recommends submitting a support ticket when one or more agents go into safe mode. Do this *before* attempting one of the following remediation actions and make sure to include a debug file for one of the agents that has entered safe mode. Doing so allows Tenable Support to identify the root cause of the issue and plan any fixes. Without a debug file, the root cause of the issue will remain unknown and unable to be addressed.

Report agents that are in safe mode

1. Go to **Sensors** > **Nessus Agents** > **Linked Agents**.
2. (Optional) Collect error details about the agent or agents by doing one of the following:
   - In the yellow safe mode banner, click **Collect error details**.
   - In the table row of one of the agents that are in safe mode, right-click or open the **Actions** menu, then select **Collect error details**.

   The **Error Details** window appears. Record the error details as needed.
3. Copy the error output text to your clipboard.

4. Go to connect.tenable.com and open a ticket. Be sure to include the error output text in the ticket description.

   Await instruction from Tenable Support.

Self-remediate agents that are in safe mode

Caution: If you choose to self-remediate without assistance from Tenable, Tenable highly recommends trying remediation methods on small subset of your agents before attempting them on large groups or all of your agents.

1. Go to **Sensors** > **Nessus Agents** > **Linked Agents**.
2. (Optional) View error details about the agent or agents by doing one of the following:
   - In the yellow safe mode banner, click **Collect Error Details**.
   - In the table row of one of the agents that are in safe mode, right-click or open the **Actions** menu, then select **Collect Error Details**.

   The **Error Details** window appears. Record the error details as needed.
3. Attempt to remediate the issue using one of the following methods: restarting the agent, rebuilding or resetting the agent plugins, or upgrading/downgrading the agent version.

   Generally, the agent re-enters safe mode within 90 minutes of restarting the agent if the issue is not solved. If your remediation action fixed the issue, the agent exits safe mode and remains out of safe mode. If you cannot remediate the issue, follow the *Report agents that are in safe mode* steps.

Restart the agents

Restarting the agent can remediate the issue if a previously undiscovered bug caused the agent to enter safe mode. You can restart an agent by simply exiting safe mode in the **Linked Agents** menu.

To restart the agent:

a. In the **Linked Agents** table, do one of the following:

   - To restart a single agent, click the ⋮ button in the agent's row.

     An action menu appears.

   - To restart multiple agents, select the checkbox of each agent you want to restart. Then, in the table click ⋮ **More**.

     An action menu appears.

b. Click [← **Exit Safe Mode**.

   The **Exit Safe Mode** window appears.

c. Click **Confirm**.

   The agent or agents restart and exit safe mode the next time they check in with Tenable Vulnerability Management, which may be up to 30 minutes after clicking **Confirm**.

Rebuild or reset the agent plugins

Rebuild or resetting the agent's plugins can remediate the issue if the agent enters safe mode after a plugin update.

Rebuilding agent plugins instructs the agent to locally rebuild its current plugin set. Resetting the agent plugins instructs the agent to download the latest plugins from Tenable Vulnerability Management and build them. Therefore, the plugin reset process may not complete until up to 12 hours later (the next time the agents connect with Tenable Vulnerability Management).

Once either process completes, the agent restarts and exits safe mode.

Generally, Tenable recommends attempting to rebuild agent plugins before attempting to reset agent plugins. This is because rebuilding plugins has a much smaller impact on network traffic.

> **Note:** If you rebuild plugins on many agents in a shared host environment, you may notice a CPU usage spike in that environment. If you reset plugins on many agents, you may notice a significant CPU usage spike.

To rebuild or reset the agent plugins:

a. In the **Linked Agents** table, do one of the following:

   - To restart a single agent, click the ⋮ button in the agent's row.

     An action menu appears.

   - To restart multiple agents, select the checkbox of each agent you want to restart. Then, in the table click ⋮ **More**.

     An action menu appears.

b. Depending on the action you want to perform, click **Rebuild Agent Plugins** or **Reset Agent Plugins**.

   A confirmation window appears.

c. Click **Confirm**.

   The agent or agents perform a plugin rebuild or plugin reset the next time they check in with Tenable Vulnerability Management, which may be up to 30 minutes after clicking **Confirm**.

Upgrade or downgrade the agent version

Upgrading or downgrading the agent can remediate the issue if a software version update caused the agent to enter safe mode. Once the upgrade or downgrade process is complete, the agent restarts and exits safe mode.

If you choose to upgrade or downgrade agents, the process may not complete until up to 12 hours later (the next time the agents connect with Tenable Vulnerability Management).

Networks

In larger enterprises, you can reduce the time and cost of setting up and maintaining locations by deploying environments with the same internal IP addresses. To disambiguate between assets that have the same IP addresses across environments, use networks in Tenable Vulnerability Management. Networks can also be used to logically separate assets for reporting, Role-Based Access Control (RBAC), and Tagging purposes.

If you deploy environments with the same internal IP addresses, create a network for each environment you have, and assign scanners and scanner groups to each network. When a scanner scans an asset, the associated network is added to the asset's details. You can filter assets by

network or create dynamic tags based on a network. Recast rules and access groups do not support networks.

A scanner or scanner group can only belong to one network at a time.

There are two types of networks:

- **Default network** – The network to which a scanner or scanner group belongs unless you assign it to a custom network.

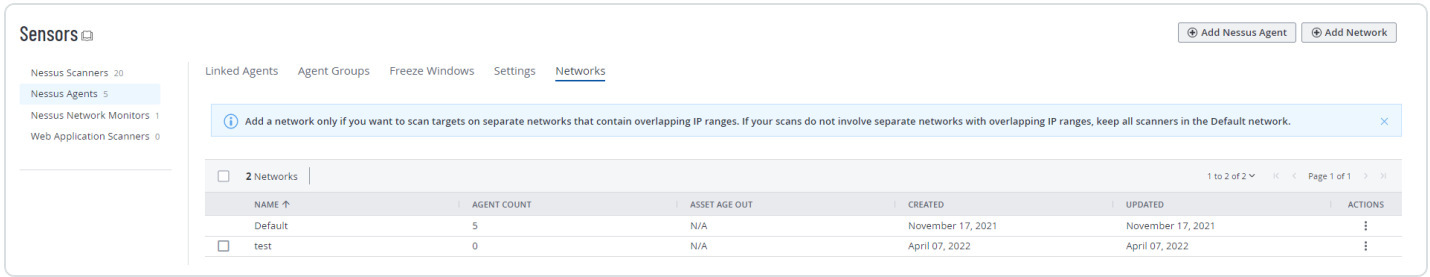
  You can view scanners in the default network, but you cannot add or remove scanners from the default network. If you remove a scanner or scanner group from a custom network, or if you delete a custom network, Tenable Vulnerability Management returns the scanner or scanner groups to the default network. Imported scans always belong to the default network.

  > **Note:** The following can only appear in the Default network:
  >
  > - Assets from AWS pre-authorized scanners
  > - Tenable Web App Scanning scanners

  > **Note:** If you move agents from a custom network to the **Default** network, you need to move the agents' associated assets to the **Default** network manually. Assets do not revert back to the **Default** network automatically. For more information, see Add an Agent to a Network and Move Assets to a Network via Settings.

- **Custom network** – A custom network that you create. Custom networks allow you to group and separate different scanners and assets based on your business needs. For example, you can create networks for different sub-organizations, external versus internal scanning, or ephemeral versus static scanning.

> **Caution:** Scanning an asset from a scanner that is not in the same network can create a duplicate asset record. If an asset is scanned by sensors in multiple networks, its network assignment will update to match the most recent scan. To avoid duplication and data inconsistency, make sure all scanners or scanner groups are assigned to the correct network. Only scan each asset using sensors from one network.



Create a Network

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Create a custom network only if you want to scan targets in separate environments that contain overlapping IP ranges. If your scans do not involve separate environments with overlapping IP ranges, keep all scanners in the **Default** network.

To create a new network:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Networks** tab.

   The list of networks appears.

3. Click **Add Network**.

   The **Settings** page appears.

4. Type a name for the network.

5. (Optional) Type a description for the network.

6. (Optional) Configure **Asset Age Out**:

   Note: By default, the **Asset Age Out** toggle is enabled and the value is set to 180 days. At that point, Tenable Vulnerability Management deletes all asset records and associated vulnerabilities. These cannot be recovered, and the deleted assets no longer count towards your license.

   - To change the number of days after which Tenable Vulnerability Management deletes unseen assets, in the **Delete Assets Not Seen in the Last** text box, type the number of days.
   - To disable the **Asset Age Out** toggle, click the toggle.

7. In the lower-right corner, click **Create**.

   Tenable Vulnerability Management creates the new network. The **Manage Scanners** page appears.

View or Edit a Network

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

To view or edit the configuration of an existing network:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Networks** tab.

   The list of networks appears.

3. In the **Networks** table, click the network to edit.

   The **Network Details** page appears with the **Settings** tab active.

4. Make changes to your network details:

   - Edit the network **Name** or **Description**. The name can contain any alphanumeric and special characters except < and >.
   - Turn on **Asset Age Out** to permanently delete host assets on your network that have not been seen on a scan for a specific number of days.

     Important: This setting only applies to host assets, and does not affect assets detected via your Cloud Native Application Protection Platform (CNAPP) license.

     a. In the text box that appears, type the number of days. The minimum value is 14 and the maximum value is 450.

     Caution: When you enable and save this option, Tenable Vulnerability Management immediately deletes assets. All asset records and associated vulnerabilities are deleted and cannot be recovered. The deleted assets no longer count towards your license.

     Note: You cannot age out assets which are older than 15 months (456 days). To delete these assets, filter for them on the **Assets** workbench and then delete them manually. For more information, see Delete Assets.

5. Click **Save**.

   Tenable Vulnerability Management saves your changes.

Add a Scanner to a Network

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

A scanner or scanner group is part of the default network unless you add it to a custom network. A scanner or scanner group can only be part of one network at a time.

You can only add a scanner group to a custom network if all scanners in that group belong to either the default network or the same custom network. If you try to add a scanner group that contains a scanner already assigned to a different custom network, Tenable Vulnerability Management prevents you from adding the scanner group to the network until you resolve the conflict.

You cannot add an AWS pre-authorized scanner to a network.

Before you begin:

- Create a new network.

  > **Note**: Tenable recommends moving scanners to a new network, rather than an existing network, to prevent unwanted asset merges. If the network where you move a scanner already contains asset records, and the identifiers for assets from the moved scanner match the identifiers already existing in the network, Tenable Vulnerability Management automatically merges those assets.

- If you want to move a scanner from one existing network to another existing network:
  - Note the IP addresses of the assets identified by the scanner you want to move.
  - Use the IP addresses to move the assets from the first network to the second network.
  - Add the scanner from the first network to the second network. Use the steps below to add a scanner.

To add a scanner or scanner group to a network:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Networks** tab.

   The list of networks appears.

3. In the networks table, click the network you want to add a scanner or scanner group to.

   The **Settings** page appears.

4. In the left navigation list, click **Manage Scanners**.

   A list of **Available Scanners to Add** and **Member Scanners in Network** appear.

5. In the row of the scanner or scanner group you want to add to the network, click the ⊕ button.

   Tenable Vulnerability Management determines whether there are any scanner group conflicts:

   If no conflicts are present, Tenable Vulnerability Management adds the scanner or scanner group to the network and moves it to the Member Scanners table.

   If any conflicts are present, Tenable Vulnerability Management displays a message. You need to remove a scanner from the scanner group to resolve the conflict. For more information about removing scanners from scanner groups, see Edit a Scanner Group.

   The scanner or scanner group appears in the **Member Scanners in Network**.

Remove a Scanner from a Network

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

If you remove a scanner or a scanner group from a custom network, Tenable Vulnerability Management reassigns it to the default network.

> **Tip:** If you want to delete a scanner group or remove a sensor from a scanner group, see Delete a Scanner Group and Remove a Sensor from a Scanner Group.

To remove a scanner or scanner group from a network:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Networks** tab.

The list of networks appears.

3. In the networks table, click the network where you want to remove a scanner or scanner group.

   The **Settings** page appears.

4. In the left navigation plane, click **Manage Scanners**.

   A list of **Available Scanners to Add** and **Member Scanners in Network** appear.

5. In the row of the scanner or scanner group you want to remove from the network, click the ✕ button.

   Tenable Vulnerability Management moves the scanner or scanner group to the default network. The scanner or scanner group appears in the **Available Scanners** list.

Add an Agent to a Network

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

An agent is part of the *Default* network unless you add it to a custom network. An agent can only be part of one network at a time.

Note: If you assign one or more agents to a network and any of those agents are already assigned to another custom network, a confirmation message appears indicating that, by adding agents to this network, they are reassigned from their previous networks.

Before you begin:

- Create a new network.

  Note: Tenable recommends moving agents to a new network, rather than an existing network, to prevent unwanted asset merges. If the network where you move an agent already contains asset records, and the identifiers for assets from the moved agent match the identifiers already existing in the network, Tenable Vulnerability Management merges those assets automatically.

- If you want to move an agent from one existing network to another existing network:
  - Note the IP addresses of the assets identified by the agent you want to move.
  - Use the IP addresses to move the assets from the first network to the second network.
  - Add the agent from the first network to the second network.

To add an agent to a network:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Do one of the following:

   - To add agents from the **Linked Agents** tab:

     a. Click the **Nessus Agents** tab.

        The list of agents appears and **Linked Agents** is selected in the drop-down box.

     b. Select an agent or agents in one of the following ways:

        - In the agents table, right-click the row for the agent you want to add.

          The action buttons appear in the row.

        - In the **Actions** column, click the button in the row for the freeze window you want to delete.

          The action buttons appear in the row.

        - In the agents table, select the check box next to each agent you want to add.

          The action bar appear at the top of the table.

        - In the table header, select the check box to select the entire page.

        The action bar appears at the bottom of the page.

     c. Click **Add to network** or **Add Selected to Network**, as applicable.

        The **Add to Network** plane appears.

     d. In the drop-down list, select the network to which you want to add the agent or agents.

     e. Click **Assign**.

        Tenable Vulnerability Management adds the agents to the selected network.

- To add agents from the **Networks** page:

  a. Click the **Networks** tab.

     The list of networks appears.

  b. In the networks table, click the network you want to add an agent to.

     The **Settings** page appears.

  c. In the left navigation list, click **Manage Agents**.

     Lists of both **Available Agents to Add** and **Member Agents in Network** appear.

  d. In the row of the agent to add to the network, click the ⊕ button.

     Tenable Vulnerability Management determines whether there are any agent group conflicts. Once you manually resolve the conflict, repeat the steps above.

     If there are no group conflicts, Tenable Vulnerability Management adds the agent to the network.

If you moved the agents from a custom network to the **Default** network, you need to move the agents' associated assets to the **Default** network manually. Assets do not revert back to the **Default** network automatically. For more information, see Move Assets to a Network via Settings.

To add an agent group to a network:

1. 1. In the left navigation, click **Sensors**.

      The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

3. Filter the agent table to view the agent group you want to add to a network:

   a. Click **Filters**.

   b. Select **Member of Group** from the **Category** drop-down list.

c. Select the agent group to add in the **Value** drop-down list.

d. Click **Apply**.

4. In the agent table header, select the check box to select the entire page.

   The action bar appears at the bottom of the page.

5. In the action bar, click the **Add selected to network**.

   The **Add to Network** plane appears.

6. In the drop-down, select the network to which you want to add the agent or agents.

7. Click **Assign**.

   Tenable Vulnerability Management adds the agents to the selected network.

   If you moved the agents from a custom network to the **Default** network, you need to move the agents' associated assets to the **Default** network manually. Assets do not revert back to the **Default** network automatically. For more information, see Move Assets to a Network via Settings.

Remove an Agent from a Network

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Before you begin:

- If you want to move an agent from one existing network to another existing network:
  - Note the IP addresses of the assets identified by the agent you want to move.
  - Use the IP addresses to move the assets from the first network to the second network.
  - Add the agent from the first network to the second network.

To remove an agent from a network:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Do one of the following:

- To remove agents from the **Linked Agents** tab:

  a. Click the **Nessus Agents** tab.

     The list of agents appears and **Linked Agents** is selected in the drop-down box.

  b. Select an agent or agents in one of the following ways:

     - In the agents table, right-click the row for the agent you want to remove.

       The action buttons appear in the row.

     - In the agents table, select the check box for the agent you want to remove.

       Tenable Vulnerability Management enables **Remove selected from network** in the action bar.

     - In the table header, select the check box to select the entire page.

       The action bar appears at the bottom of the page.

  c. Click **Remove from network** or **Remove selected from network**, as applicable.

     Tenable Vulnerability Management removes the agents from their networks and adds them to the *Default* network.

- To remove agents from the **Networks** tab:

  a. Click the **Networks** tab.

     The list of networks appears.

  b. In the networks table, select the network from which you want to remove an agent or agents.

     The **Settings** page appears.

  c. In the left navigation menu, click **Manage Agents**.

     Lists of both **Available Agents to Add** and **Member Agents in Network** appear.

  d. In the row of the agent to remove from the network, click the ✕ button.

Tenable Vulnerability Management removes the agent from the network and adds it to the *Default* network. <<ASK SME if same as scanner group conflicts -- refer to that doc if so.>>

Move Assets to a Network via Settings

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

When a scanner scans assets, the scanner automatically adds the network to which it belongs to the scanned assets' identifying details. However, if you want to change the network assets are assigned to, you can also manually move assets to a network.

Move assets to a new network before you run scans on the new network. If you move assets to a network where scans have already run, Tenable Vulnerability Management may create duplicate asset records that count against your license.

Tip: You can also move assets to a network via the **Explore** > **Assets** workbench.

Note: If you moved agents or agent groups from a custom network to the **Default** network, you need to move the agents' associated assets to the **Default** network manually. Assets do not revert back to the **Default** network automatically.

To move an asset or assets to a network from the **Networks** page:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Networks** tab.

   The list of networks appears.

3. In the networks table, do one of the following:

   - Right-click the network you want to move an asset or assets to.

     The action buttons appear in the row.

   - In the **Actions** column, click the ⋮ button in the row for the freeze window you want to

delete.

The action buttons appear in the row.

4. Click **Move assets**.

   The **Move Assets** page appears.

5. In the **Source Network** drop-down box, select the network you want to move an asset or assets to.

6. In the text box, do one of the following:

   - To search for a single asset, enter an IP address.
   - To search for multiple assets, enter a CIDR range or individual IP addresses separated by commas.

   Tenable Vulnerability Management shows the asset or assets that match your search criteria.

7. Do one of the following:

   - Move a single asset:

     a. In the assets table, do one of the following:

        - Right-click the asset you want to move. The action buttons appear in the row.
        - In the **Actions** column, click the ⋮ button in the row for the asset you want to move. The action buttons appear in the row.

     a. Click Move assets.

        Tenable Vulnerability Management moves the asset to the selected network.

   - Move selected assets:

     a. For each asset you want to select, roll over the icon.

        The check box for the asset appears.

     b. Click the check box.

        The action bar appears at the bottom of the page.

c. In the action bar, click the button.

Tenable Vulnerability Management moves the selected asset or assets from the source network to the destination network.

- Move all assets on the current page:

a. In the assets table header, click the check box.

Tenable Vulnerability Management selects all assets on the current page. The action bar appears at the bottom of the page.

b. In the action bar, click the button.

Tenable Vulnerability Management moves the selected assets from the source network to the destination network.

- Move all assets in the source network:

a. Roll over the icon of an asset.

The action bar appears at the bottom of the page.

b. In the action bar, click **Select All Assets**.

Tenable Vulnerability Management selects all assets in the source network.

c. In the action bar, click the button.

Tenable Vulnerability Management moves all assets from the source network to the destination network.

To move an asset or multiple assets to a network from the asset table:

1. In the upper-left corner, click the button.

   The left navigation plane appears.

2. In the left navigation bar, click **Assets**.

   The **Assets** dashboard appears, and displays the assets table.

3. (Optional) Refine the table data. For more information, see Tables.

4. (Optional) Apply a saved search filter.

5. Do one of the following:

   - Move a single asset:

     a. Roll over the asset you want to move.

        The action buttons appear in the row.

     b. Click the → button.

     c. The **Move** plane appears.

     d. In the **Default** drop-down box, select the network you want to move the asset to.

     e. Click the **Move** button.

     f. Tenable Vulnerability Management moves the asset to the selected network.

   - To move selected assets:

     a. For each asset you want to move, click the check box in the asset row.

        The action bar appears at the bottom of the page.

     b. In the action bar, click the → button.

        The **Move** plane appears.

     c. In the **Default** drop-down box, select the network you want to move the asset to.

     d. Click the **Move** button.

        Tenable Vulnerability Management moves the assets to the selected network.

   - To move all assets on the current page:

     a. Click the check box in the table header.

        The action bar appears at the bottom of the page.

     b. In the action bar, click the → button.

        The **Move** plane appears.

     c. In the **Default** drop-down box, select the network you want to move the asset to.

d. Click the **Move** button.

   Tenable Vulnerability Management moves the assets to the selected network.

- To move all assets:

  a. Click the check box in the table header.

  b. The action bar appears at the bottom of the page.

  c. In the action bar, click **Select All Assets**.

  > **Note:** If you click **Select All Assets**, all assets on the current page and any additional pages are selected.

  d. In the action bar, click **Move**.

  e. The **Move** plane appears.

  f. In the **Default** drop-down box, select the network you want to move the assets to.

  g. Click the **Move** button.

  h. Tenable Vulnerability Management moves the assets to the selected network.

> **Note:** Depending on the filter applied and the number of assets selected, it may take some time for Tenable Vulnerability Management to move all assets to the destination network.

Delete Assets in a Network

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

> **Tip:** If you want to remove an asset from a network but not delete the asset, see Move Assets to a Network via Settings.

Delete Assets Manually

If you manually delete an asset, Tenable Vulnerability Management no longer displays the asset in the default view of the assets table, deletes vulnerability data associated with the asset, and stops matching scan results to the asset. Manually deleted assets continue to count against your Tenable Vulnerability Management license until the assets age out after 14 days.

To delete assets manually:

- Delete an individual asset. For more information, see Delete Assets.
- Delete multiple assets using the Tenable Vulnerability Management API. For more information, see the Tenable Developer Portal.

Delete Assets Automatically

If you automatically delete assets in a network, Tenable Vulnerability Management permanently deletes the asset and all associated vulnerability data after a specified number of days. Automatically deleted assets do not count against your Tenable Vulnerability Management license.

To automatically delete assets, enable the **Asset Age Out** feature when you create or edit the network.

Export Networks

Required User Role: Administrator

On the **Sensors** page, you can export one or more networks.

To export a network:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Networks** tab.

   The list of networks appears.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

4. Select the networks that you want to export:

Export Scope	Action
Selected networks	To export selected networks: a. Select the check box for each network you want to export.

	The action bar appears at the top of the table. b. Click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 networks, select all the networks in the list and then click [→ **Export**.
A single network	To export a single network: a. In the networks table, right-click the row for the network you want to export. The action options appear next to your cursor. -or- In the networks table, in the **Actions** column, click the ⋮ button in the row for the network you want to export. The action options appear in the row. -or- Select the check box for the network you want to export. The action bar appears at the top of the table. The action buttons appear in the row. b. Click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  Note: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

5. In the **Name** box, type a name for the export file.
6. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of networks. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of networks. Empty fields are not included in the JSON file.

7. (Optional) Deselect any fields you do not want to appear in the export file.
8. In the **Expiration** box, type the number of days before the export file expires.

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

9. (Optional) To set a schedule for your export to repeat:
   - Click the **Schedule** toggle.

     The **Schedule** section appears.
   - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
   - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
   - In the **Repeat** drop-down box, select how often you want the export to repeat.

- In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

  > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

10. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

    - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.

    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

11. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

12. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file from the Exports page.

Delete a Network

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

- If you delete a network, assets that were in the deleted network still retain the network attribute.

- Tenable Vulnerability Management retains any asset records for the deleted network until the assets age out of your licensed assets count. You can still filter for assets that use the deleted network.
- You cannot create a new network that has the same name as a deleted network.

Before you begin:

Before you delete a network, consider the following:

- Consider moving assets to a different network before you delete the network. To move assets from a deleted network to another network, you must use the Tenable Vulnerability Management API.
- Tenable Vulnerability Management re-assigns any scanners or scanner groups in the deleted network to the default network. If you want to delete the scanners or scanner groups, see Remove a Sensor from a Scanner Group and Delete a Scanner Group.

To delete a network:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **Networks** tab.

   The list of networks appears.

3. Delete selected networks.

Delete Scope	Action
To delete a single network	To delete a single network: a. In the networks table, right-click the row for the network you want to delete. The action options appear next to your cursor. -or- In the networks table, in the **Actions** column, click the ⋮ button in the row for the network you want to delete. The action options appear in the row. -or- Select the check box for the network you want to delete. The action bar appears at the top of the table. b. Click **Delete**.
To delete multiple networks	To delete multiple networks: a. In the networks table, select the check box for the network you want to delete. The action bar appears at the top of the table. b. Click **Delete**.

Tenable Vulnerability Management deletes the network.

Linked Scanners

After you install a Tenable Nessus scanner, Tenable Network Monitor instance, Tenable Web App Scanning sensor, or Tenable Agent sensor, you can link it to Tenable Vulnerability Management.

Before you can use linked scanners in Tenable Vulnerability Management scans, you must:

1. Install the appropriate Tenable product on the sensor or the host you want to scan.

Sensor Type	More Information
Tenable Agent	• Environments • Install Tenable Agent in the *Tenable Agent Deployment and User Guide*
Tenable Network Monitor	• Environments • Install Tenable Network Monitor in the *Tenable Network Monitor User Guide* • Deploy or Install Tenable Container Security + Tenable Network Monitor in the *Tenable Core User Guide*
Tenable Nessus	• Environments • Install Tenable Nessus in the *Tenable Nessus User Guide* • Deploy or Install Tenable Core + Tenable Nessus in the *Tenable Core User Guide* **Note:** If a Tenable Nessus scanner has multiple NICs/interfaces, you may see multiple IPv4/IPv6 addresses for the scanner.
Tenable Web App Scanning	• Environments • Deploy or Install Tenable Core + Tenable Web App Scanning in the *Tenable Core User Guide*

2. Link the sensor to Tenable Vulnerability Management.

View Linked Scanners

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

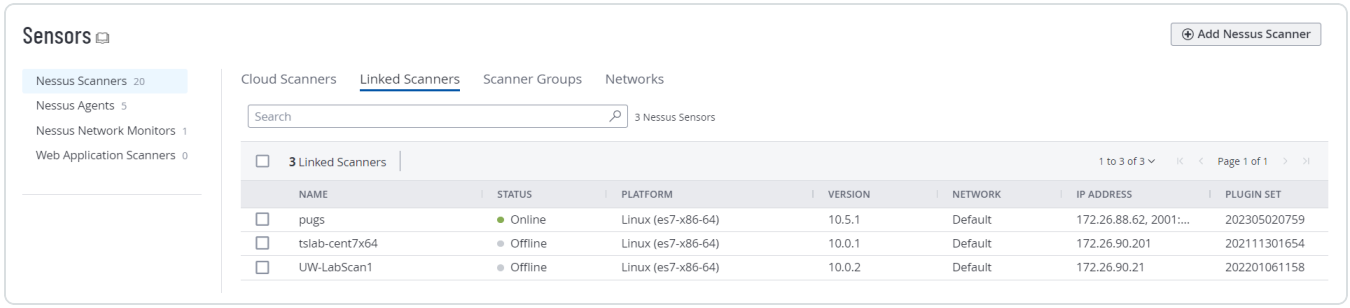
To view your linked scanners:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. To view a different type of linked scanners, in the top navigation bar, click the type of linked scanners you want to view.

   Tenable Vulnerability Management displays the selected type of linked scanners.



Rename a Linked Scanner

You can rename your linked scanners from the **Sensors** menu. This can be helpful for making linked scanners more recognizable to other users.

> **Note:** You cannot rename a cloud scanner. The cloud scanner names are managed by Tenable.

To rename a linked scanner:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the row of the scanner you want to rename.

   The scanner **Details** page appears.

3. Click the button next to the scanner name.

4. Edit the scanner name.

5. Click the button next to the scanner name.

Tenable Vulnerability Management saves the new scanner name and updates any related tables with the new name.

Download Linked Scanner Logs

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

In Tenable Vulnerability Management, you can request and download a log file containing logs and system configuration data from any of your linked scanners. This information can help you troubleshoot system problems and easily provide data for Tenable Support.

You can store a maximum of five log files from each scanner. Once the limit is reached, you must remove an old log file to download a new one.

Note: You can only download scanner logs when the scanner is online. The Tenable Vulnerability Management **Logs** tab disappears when the selected scanner is offline.

Tip: If Tenable Vulnerability Management identifies your scanner as offline unexpectedly, Tenable recommends running the `nessuscli bug-report-generator` command on the scanner to troubleshoot.

To download logs from a linked scanner in Tenable Vulnerability Management:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. In the linked scanners table, click the scanner for which you want to download logs.

   The details page for that scanner appears.

3. Click the **Logs** tab.

   A table shows any previously downloaded logs.

4. In the upper-right corner, click **Request Logs**.

   Note: If you have reached the maximum of five log files, the **Request Logs** button is disabled. Remove an existing log before downloading a new one.

The pending log appears as a row in the logs table. Tenable Vulnerability Management requests the logs from the scanner the next time it checks in, which may take several minutes.

5. In the row for an available log file, click the ⬇ button.

   Your system downloads the log file.

To remove an existing log:

1. In the row of the log you want to remove, click the 🗑 button.

   A confirmation window appears.

2. In the confirmation window, click **Delete**.

   Tenable Vulnerability Management deletes the log and removes it from the table.

To cancel a pending or failed log request:

- In the row of the pending or failed log request that you want to cancel, click the ⏸ button.

  Tenable Vulnerability Management cancels the log request and removes it from the table.

Export Linked Scanners

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

On the **Sensors** page, you can export one or more linked scanners in CSV or JSON format.

To export your linked scanners:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Do one of the following:

   - To export Tenable Nessus linked scanners, in the drop-down box, select the **Linked Scanners** tab.

The **Linked Scanners** page appears, displaying a table with all your Tenable Nessus linked scanners.

- To export Tenable Network Monitor linked scanners, click the **Nessus Network Monitors** tab.

  A table with all your Tenable Network Monitor linked scanners appears.

- To export Tenable Web App Scanning linked scanners, click the **Web App Scanners** tab.

  A table with your Tenable Web App Scanning linked scanners appears.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

4. Select the linked scanners that you want to export:

Export Scope	Action
A single linked scanner	To export a single linked scanner from the **Linked Scanners** page: a. In the linked scanners table, right-click the row for the linked scanner you want to export. -or- In the linked scanners table, in the **Actions** column, click the ⋮ button in the row for the linked scanner you want to export. The action buttons appear in the row. -or- Select the check box for the linked scanner you want to export. The action bar appears at the top of the table. b. Click [→ **Export**. To export from the **Details** page: a. In the linked scanners table, click the row for the linked scanner you

	want to export. The **Details** page appears. b. In the upper-right corner, click the [→ **Export** button.
Multiple linked scanners	To export multiple selected linked scanners: a. In the scanners table, select the check box for each linked scanner you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 scanners, select all the scanners in the list and then click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  Note: By default, all fields are selected.
- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

5. In the **Name** box, type a name for the export file.
6. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of linked scanners.

	Note: If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of linked scanners. Empty fields are not included in the JSON file.

7. In the **Expiration** box, type the number of days before the export file expires.

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

8. (Optional) To set a schedule for your export to repeat:

   - Click the **Schedule** toggle.

     The **Schedule** section appears.

   - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
   - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
   - In the **Repeat** drop-down box, select how often you want the export to repeat.
   - In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

     Note: If you select never, the schedule repeats until you modify or delete the export schedule.

9. (Optional) To send email notifications on completion of the export:

   Note: You can enable email notifications with or without scheduling exports.

   - Click the **Email Notification** toggle.

     The **Email Notification** section appears.

- In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
- (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

  > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

10. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

11. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Export Linked Scanner Details

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

On the **Details** page for any linked scanner, you can export details about your linked scanner in CSV or JSON format.

To export details for a linked scanner:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.
3. In the linked scanners table, click the linked scanner for which you want to export details.

The **Details** page appears.

4. In the upper-right corner, click [→ **Export**.

   The **Export** plane appears. This plane contains:

   - A text box to configure the export file name.
   - A list of available export formats.
   - A table of configuration options for fields to include in the exported file.

     > **Note**: By default, all fields are selected.

   - A text box to set the number of days before the export expires.
   - A toggle to configure the export schedule.
   - A toggle to configure the email notification.

5. In the **Name** box, type a name for the export file.
6. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of your linked scanner details, organized by fields. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of your linked scanner details, organized by fields. Empty fields are not included in the JSON file.

7. (Optional) Deselect any fields you do not want to appear in the export file.
8. In the **Expiration** box, type the number of days before the export file expires.

> **Note**: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

9. (Optional) To send email notifications on completion of the export:

   > **Note**: You can enable email notifications with or without scheduling exports.

   - Click the **Email Notification** toggle.

     The **Email Notification** section appears.

   - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.

   - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

     > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

10. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

11. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Differential Plugin Updates

The following table describes the behavior of differential plugin updates for Tenable Nessus scanners linked to Tenable Vulnerability Management.

Linked to	Differential Update	Full Update

Tenable Vulnerability Management	The scanner requests differential updates from Tenable Vulnerability Management once every 24 hours.	The scanner performs a full plugin update if it does not have plugins (for example, immediately after you link the scanner to Tenable Vulnerability Management).

Scanner Groups

You can use scanner groups to organize and manage the scanners linked to your Tenable Vulnerability Management instance. For example, you can add all sensors related to a specific geographical location to a group, for example, a group named "East Coast Scanners."

You can add a scanner to one or more scanner groups.

Important! Scanner group permissions do not override existing individual scanner permissions. For example, if you add a scanner with **Can Use** permissions to a scanner group with **Can Manage** permissions, that scanner retains its **Can Use** permissions.

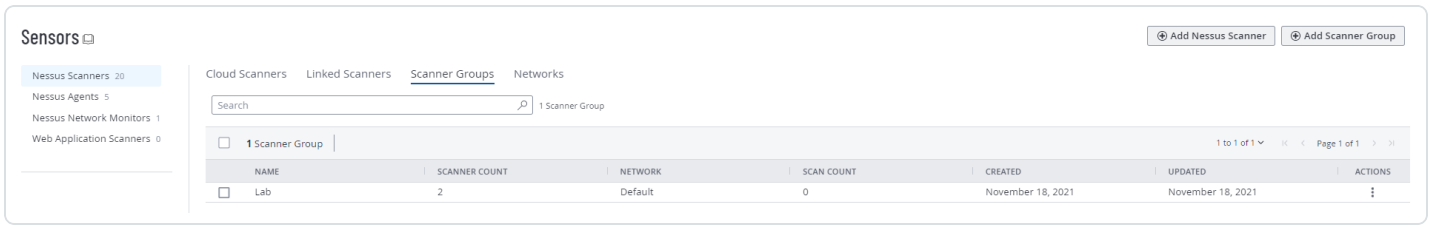
When you create a scan, you can select the scanner group to use to launch the scan. Alternatively, you can select **Auto-Select** to enable scan routing for the scan, which assigns scans to scanners based on the targets configured in scanner groups.

Tenable Vulnerability Management determines which scanner in a scanner group to use based on the following criteria:

- The scanner is active and has communicated to Tenable Vulnerability Management within the last 5 minutes.
- The scanner is running the lowest number of active scans and is scanning the lowest number of hosts.

Note: If your organization uses scan networks, you can only add scanners to scanner groups that belong to the same network. For more information, see Networks.

Note: If a remote scanner is part of a **Scanner Group** and is unlinked during its operations, the scan's operations complete, but Tenable Vulnerability Management does not include the unlinked scanner for future use.



Create a Scanner Group

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

To create a scanner group in the new interface:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. In the drop-down box, select **Scanner Groups**.

   The list of existing scanner groups you have permission to use or manage appears.

3. Click **Add Scanner Group**.

   The **Add Scanner Group** plane appears.

4. In the **Group Name** field, type a name for the group.

5. (Optional) In the **Targets for Scan Routing** box, type a comma-separated list of scan routing targets.

   Targets in the list must be in the supported formats.

   This list specifies the targets that scanners in this scanner group can scan if a scan is configured to use the **Auto-Select** scanner. For more information, see Example: Scan Routing.

   Note: You can specify up to 10,000 individual scan routing targets for an individual scanner group. For example, `192.168.0.1, example.com, *.example.net, 192.168.0.0/24` specifies four scan routing targets. To condense a scan routing target list, Tenable recommends using wildcard and range formats, instead of individual IP addresses.

6. (Optional) Configure user permissions for a scanner group.

By default, in any new scanner group, Tenable Vulnerability Management assigns the system-generated **All Users** group **Can Use** permissions.

7. Click **Save**.

   If **Targets for Scan Routing** specifies more than the maximum number of targets, an error message appears. Condense the scan routing targets by using wildcard and range formats instead of individual IP addresses, then try again to save the scanner group.

   In all other cases, the new group appears in the **Scanner Groups** list.

Modify a Scanner Group

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

To modify a scanner group:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. In the drop-down box, select **Scanner Groups**.

   The list of existing scanner groups you have permission to use or manage appears.

3. (Optional) Search the table for the group you want to modify. For more information, see Tables.

4. In the scanner group table, do one of the following:

   - In the **Actions** column of the scanner group you want to modify, click the ⋮ button.

     The action options appear in the row.

   - Right-click the scanner group you want to modify.

     The action options appear next to your cursor.

5. Click **Edit**.

   The **Edit Scanner Group** plane appears.

6. Modify any of the following settings:

Setting	Action
Name	Type a new name.
User and Group Permissions	Configure user permissions for the scanner group.

7. (Optional) In the **Targets for Scan Routing** box, type a comma-separated list of scan routing targets.

   Targets in the list must be in the supported formats.

   This list specifies the targets that scanners in this scanner group can scan if a scan is configured to use the **Auto-Select** scanner. For more information, see Example: Scan Routing.

   > **Note:** You can specify up to 10,000 individual scan routing targets for an individual scanner group. For example, `192.168.0.1, example.com, *.example.net, 192.168.0.0/24` specifies four scan routing targets. To condense a scan routing target list, Tenable recommends using wildcard and range formats, instead of individual IP addresses.

8. Click **Save**.

   If **Targets for Scan Routing** specifies more than the maximum number of targets, an error message appears. Condense the scan routing targets by using wildcard and range formats instead of individual IP addresses, then try again to save the scanner group.

   In all other cases, Tenable Vulnerability Management updates the scanner group with your changes.

To assign scanners to a scanner group:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Sensors** tile.

The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

4. (Optional) For Tenable Web App Scanning, click the **Web App Scanners** tab.

   The **Web App Scanners** tab appears and **Linked Scanners** is selected in the drop-down box.

5. In the drop-down box, select **Scanner Groups**.

   The list of existing scanner groups you have permission to use or manage appears.

6. In the scanner groups table, click the row of the scanner group where you want to add scanners.

   The **Group Details** page appears.

7. Click ⊕ **Assign Scanners**.

   The **Assign Scanner** page appears.

8. (Optional) Search the table for the scanner you want to assign. For more information, see Tables.

9. In the scanners table, select the check boxes next to the scanner or scanners you want to add to the scanner group.

10. Click **Assign**.

    If the assignment is successful, Tenable Vulnerability Management adds the scanner to the scanner group, and the **Group Details** page appears.
    If Tenable Vulnerability Management encounters any problems during processing, the **Assign Scanners** page remains active, and one of the following messages appears in the **Assignment** column of the affected scanner:

Possible Error Messages	Action
This sensor already exists in the scanner group.	Click **Cancel** to close the page.
An error occurred adding this sensor to the scanner group.	Click **Assign** again. If the processing still fails, contact Tenable Support.

Configure User Permissions for a Scanner Group

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

You can configure scanner group permissions for individual users or a user group. If you configure scanner group permissions for a user group, you assign all users in that group the same permissions. For more information, see User Groups.

Important! Scanner group permissions do not override existing individual scanner permissions. For example, if you add a scanner with **Can Use** permissions to a scanner group with **Can Manage** permissions, that scanner retains its **Can Use** permissions.

You can assign the following scanner group permissions to a user or user group:

- **No Access** – (**All Users** user group only) No users (except for users or groups you specifically assign permissions) can use the scanner group in scan configurations.
- **Can Use** – The user or user group can use the scanner group in scan configurations. The user or user group (assuming they have the **Scan Manager** or **Administrator** user role) can view but not edit the scanner group configuration.
- **Can Manage** – The user or user group can use the scanner group in scan configurations. The user or user group (assuming they have the **Scan Manager** or **Administrator** user role) can view and edit the scanner group configuration.

  Note: All users with the **Scan Manager** user role have **Can Manage** permissions for scanner groups, regardless of the scanner group permission they are assigned.

To configure user permissions for a scanner group:

1. Create or edit a scanner group.
2. During scanner group configuration, in the **Users & Groups** section, do any of the following:
   - Edit permissions for the **All Users** user group.
     a. Next to the permission drop-down for the **All Users** group, click the ⌄ button.
     b. Select a permissions level.
   - Add a user or user group to the scanner group.

a. In the **User & Groups** heading, click the ⊕ button.

   The **Add Users & Group** plane appears.

b. In the **Search** field, type or click the drop-down to find and add a user or group.

   > **Tip**: Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

   Added users and groups appear below the **Search** field.

c. Click the **Add** button.

   The scanner group plane appears.

   By default, Tenable Vulnerability Management assigns the added user or user group **Can Use** permissions.

- Edit permissions for an existing user or user group.

  a. Next to the permissions drop-down for the user or user group you want to edit, click the ⌄ button.

  b. Select a permissions level.

- Remove a user or user group from the scanner group.

  a. Roll over the user or group you want to remove.

  b. Click the ✕ button next to the user or user group.

     The user or group disappears from the **Users & Groups** list.

3. Click **Save**.

   Tenable Vulnerability Management saves your changes to the scanner group.

What to do next:

- Use the scanner group in a scan configuration.

Delete a Scanner Group

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

To delete one or more scanner groups:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. In the drop-down box, select **Scanner Groups**.

   The list of existing scanner groups you have permission to use or manage appears.

3. In the scanner groups table, select one or more scanner groups to delete:

Scope	Action
To delete a single scanner group	a. In the scanner groups table, do one of the following: • Select the check box for the scanner group you want to delete. The action bar appears at the top of the table. • Right-click the scanner group you want to delete. The action options appear next to your cursor. • In the **Actions** column, click the ⋮ button for the scanner group you want to delete. The action options appear in the row. b. Click **Delete**. A confirmation window appears.
To delete multiple scanner groups	a. In the scanner groups table, select the check boxes next to the scanner groups you want to delete. The action bar appears at the bottom of the page. b. In the action bar, click the **Delete** button. A confirmation window appears.

4. In the confirmation window, click the **Delete** button.

   Tenable Vulnerability Management deletes the group or groups you selected.

Add a Sensor to a Scanner Group

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

You can add the following types of sensors to a scanner group:

Sensor Type	Supported?
On-premises Tenable Nessus	yes
On-premises Tenable Web App Scanning	yes
Tenable Vulnerability Management cloud	no
Tenable Nessus sensor for Amazon Web Services (AWS)	no
Tenable Network Monitor (NNM)	no
Tenable Agent	no (see Agent Groups)

To add sensor to one or more scanner groups in the new interface:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. (Optional) Search for the scanner you want to add to a scanner group.

3. Select the scanners you want to add and the groups you want to add the scanners to:

Scope	Action
Add a single scanner to a group or groups	a. In the scanner group table, do one of the following: • Right-click the sensor you want to add to a scanner group. The action options appear next to the cursor.

	• In the **Actions** column, click the ⋮ button for the sensor you want to add to a scanner group. The action options appear in the row. • Select the check box for the sensor you want to add to a scanner group. Tenable Vulnerability Management enables **Add selected to Groups** in the action bar. b. Click 🗁 **Add to Groups**. The **Add to Groups** plane appears. c. In the search box, type the name of the scanner group where you want to add the scanner. d. In the drop-down box of matching groups, click a group. e. (Optional) Repeat steps c and d to add additional scanner groups.
Add multiple scanners to a group or groups	a. In the scanner table, select the check boxes next to the scanners you want to add to scanner groups. The action bar appears at the bottom of the page. b. Click the 🗁 **Add selected to Groups** button. The **Add to Groups** plane appears. c. In the search box, type the name of the scanner group where you want to add the scanner. d. In the drop-down list of matching groups, click a group. e. (Optional) Repeat steps c and d to add additional scanner groups.

4. Click **Save** to save your changes.

   Tenable Vulnerability Management adds the scanner or scanners to the selected group or groups and closes the **Add to Groups** plane.

Remove a Sensor from a Scanner Group

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

> **Required Tenable Web App Scanning User Role:** Scan Manager or Administrator

To remove a sensor from a scanner group in the new interface:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. In the drop-down box, select **Scanner Groups**.

   The list of existing scanner groups you have permission to use or manage appears.

3. (Optional) Search the table for the group you want to modify. For more information, see Tables.

4. In the scanner group table, click the scanner group you want to modify.

   The **Group Details** page appears. This page contains a table listing sensors assigned to this group.

5. (Optional) Search for the sensor you want to remove. For more information, see Tables.

6. Select the sensor or sensors you want to remove:

7. Select the sensors you want to remove:

Scope	Action
Remove a single sensor	a. In the sensors table, do one of the following: • Right-click the sensor you want to remove.

	The action options appear next to your cursor. • In the **Actions** column, click the ⋮ button for the sensor you want to remove. The action options appear in the row. • Select the check box for the sensor you want to remove. The action buttons appear at the top of the table. b. Click the **Remove from Group** button. A confirmation window appears.
Remove multiple sensors	a. In the sensors table, select the check box for each sensor you want to remove from the group. The action bar appears at the bottom of the page. b. In the action bar, click the **Remove from Group** button. A confirmation window appears.

8. In the confirmation window, click **Remove**.

   Tenable Vulnerability Management removes the sensor or sensors from the scanner group.

View Sensors in a Scanner Group

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Important! Scanner group permissions do not override existing individual scanner permissions. For example, if you add a scanner with **Can Use** permissions to a scanner group with **Can Manage** permissions, that scanner retains its **Can Use** permissions.

To view sensors assigned to a scanner group:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. In the drop-down box, select **Scanner Groups**.

   The list of existing scanner groups you have permission to use or manage appears.

3. (Optional) Search the table for the group you want to view. For more information, see Tables.

4. In the scanner group table, click the scanner group you want to view.

   The **Group Details** page appears. This page contains a table listing sensors assigned to this group.

View All Running Scans for a Sensor

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Note: You can only view all scans for sensors in Tenable Nessus scanner groups.

To view all running scans for a sensor:

1. View the sensors in the appropriate scanner group.

2. In the sensors table, click the sensor for which you want to view all scans.

   The scanner **Details** page appears.

3. Click the **Manage Scans** tab.

   Tenable Vulnerability Management shows a list of all scans the sensor is currently running.

OT Connectors

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

If your organization has OT Security and Tenable Vulnerability Management, you can allow OT Security to transmit assets and findings data to Tenable Vulnerability Management by setting up OT connectors. You can manage OT connectors from the Tenable Vulnerability Management **Sensors** page.

To open the **OT Connectors** menu in Tenable Vulnerability Management:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the **OT Connectors** tab.

   The list of linked OT connectors appears.

3. Use the following procedures to manage OT connectors:

Add an OT connector:

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

To add an OT connector:

1. Click ⊕ **Add OT Connector**.

   The **Add OT Connector** window appears.

2. Click **Generate**.

   Tenable Vulnerability Management shows the appropriate cloud site to link the OT connector to and generates an OT linking key.

   Note: You can use the linking key to link *one* OT connector, and you must use the linking key within two hours of generation. To link additional OT connectors, generate and use a new linking key for each connector.

3. Use the cloud site and linking key to link the connector to Tenable Vulnerability Management from the OT Security user interface. For more information, see the *OT Security User Guide*.

Modify an OT connector name or type:

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

To ensure that your OT connectors are recognizable and represent the correct types, you may need to modify the OT connector names and types in Tenable Vulnerability Management. You can choose from two types: **ICP** and **EM** (Enterprise Manager). For more information about the types, see the *OT Security User Guide*.

Note: Updating an OT connector name or type in Tenable Vulnerability Management does not cause any changes in OT Security.

To modify an OT connector name or type:

1. In the **OT Connectors** table, double-click the **Name** or **Type** cell to edit it.
2. Enter the new name or select the new type (**ICP** or **EM**).
3. Click out of the cell.

   Tenable Vulnerability Management saves your change.

Enable or disable an OT connector:

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

There may be some cases where you want to disable an OT connector temporarily and enable it at a later time. For example, you may want to disable an OT connector if OT Security begins sending data from an unwanted network to Tenable Vulnerability Management. Once the issue is resolved, you can re-enable the connector.

To enable or disable an OT connector:

1. In the OT Connectors table, click ⋮ in the row of the connector that you want to enable or disable.

   A drop-down menu appears.
2. If the connector is currently enabled, click **Disable**. If the connector is currently disabled, click **Enable**.

   If you enabled the connector, Tenable Vulnerability Management bolds the connector row text and updates the **Enabled** column to **Yes**. If you disabled the connector, Tenable Vulnerability Management grays the connector row text and updates the **Enabled** column to **No**.

Delete an OT connector:

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Delete an OT connector from Tenable Vulnerability Management if you no longer want the OT connector to send data to Tenable Vulnerability Management. For example, if you need to redeploy OT Security, you would need to delete any connector associated with the old deployment.

Tenable recommends that whenever you delete an OT connector from Tenable Vulnerability Management, you also delete the related connector in OT Security to ensure that Tenable Vulnerability Management and OT Security stay aligned.

Note: You cannot undo an OT connector deletion; if you want to relink the OT connector, you have to repeat the Add an OT connector process.

To delete an OT connector from Tenable Vulnerability Management:

1. In the OT Connectors table, click ⋮ in the row of the connector that you want to delete.

   A drop-down menu appears.

2. Click **Delete**.

   The **Delete OT Connector** window appears.

3. Click **Delete**.

   Tenable Vulnerability Management removes the connector from the table.

Cloud Sensors

By default, Tenable provides regional cloud sensors for use in Tenable Vulnerability Management. You can select these sensors when you create and launch scans.

The following table identifies each regional cloud sensor and, for allow list purposes, its IP address ranges. These IP address ranges are exclusive to Tenable.

Note: If you use cloud connectors or Tenable Exposure Management connectors, Tenable recommends allowlisting the IP addresses for the region in which the site resides.

Note: While these IP addresses are for outbound requests, only the **tenable.io** sensor group IP addresses are used for inbound cloud.tenable.com requests.

Tip: The cloud sensor and IP address information contained in the table below is also provided in JSON format for users that want to parse the data programmatically.

For Cloud IPs associated with Tenable Attack Surface Management, see Cloud Sensors in the *Tenable Attack Surface Management User Guide*.

Sensor Region	IPv4 Range	IPv6 Range
ap-northeast-1	13.115.104.128/25 35.73.219.128/25	2406:da14:e76:5b00::/56
ap-southeast-1	13.213.79.0/24 18.139.204.0/25 54.255.254.0/26	2406:da18:844:7100::/56
ap-southeast-2	13.210.1.64/26 3.106.118.128/25 3.26.100.0/24	2406:da1c:20f:2f00::/56
ap-south-1	3.108.37.0/24	2406:da1a:5b2:8500::/56
ca-central-1	3.98.92.0/25 35.182.14.64/26	2600:1f11:622:3000::/56
eu-west-1	3.251.224.0/24	2a05:d018:f53:4100::/56
eu-west-2	18.168.180.128/25 18.168.224.128/25 3.9.159.128/25 35.177.219.0/26	2a05:d01c:da5:e800::/56
eu-central-1	18.194.95.64/26 3.124.123.128/25 3.67.7.128/25 54.93.254.128/26	2a05:d014:532:b00::/56
me-central-1	51.112.93.0/24	2406:da17:524:dd00::/56
us-east-1	34.201.223.128/25 44.192.244.0/24	2600:1f18:614c:8000::/56

Sensor Region	IPv4 Range	IPv6 Range
	54.175.125.192/26	
us-east-2	13.59.252.0/25 18.116.198.0/24 3.132.217.0/25	2600:1f16:8ca:e900::/56
us-west-1	13.56.21.128/25 3.101.175.0/25 54.219.188.128/26	2600:1f1c:13e:9e00::/56
us-west-2	34.223.64.0/25 35.82.51.128/25 35.86.126.0/24 44.242.181.128/25 35.93.174.0/24	2600:1f14:141:7b00::/56
sa-east-1	15.228.125.0/24	2600:1f1e:9a:ba00::/56
static	162.159.129.83/32 162.159.130.83/32	2606:4700:7::a29f:8153 2606:4700:7::a29f:8253

Note: For troubleshooting Tenable Web App Scanning issues with Tenable Support, you may be asked to add the following IP range to your allow list:

- 13.59.250.76/32

Regional cloud sensors appear in the following groups:

- **US East Cloud Scanners**: A group of scanners from the us-east-1 (Virginia) or the us-east-2 (Ohio) ranges.
- **US West Cloud Scanners**: A group of scanners from the us-west-1 (California) or the us-west-2 (Oregon) ranges.
- **AP Singapore Cloud Scanners**: A group of scanners from the ap-southeast-1 (Singapore) range.
- **AP Sydney Cloud Scanners**: A group of scanners from the ap-southeast-2 (Sydney) range.

- **AP Tokyo Cloud Scanners**: A group of scanners from the ap-northeast-1 (Tokyo) range.
- **CA Central Cloud Scanners**: A group of scanners from the ca-central-1 (Canada) range.
- **EU Frankfurt Cloud Scanners**: A group of scanners from the eu-central-1 (Frankfurt) range.
- **UK Cloud Scanners**: A group of scanners from the eu-west-2 (London) range.
- **Brazil Cloud Scanners:** A group of scanners from the sa-east-1 (São Paulo) range.
- **India Cloud Scanners:** A group of scanners from the ap-south-1 (Mumbai) range.
- **Amazon GOV-CLOUD**: A group of scanners available for Federal Risk and Authorization Management Program (FedRAMP) environments.
- **US Cloud Scanner**: A group of scanners from the following AWS ranges:
    - us-east-1 (Virginia)
    - us-east-2 (Ohio)
    - us-west-1 (California)
    - us-west-2 (Oregon)
- **APAC Cloud Scanners**: A group of scanners from the following AWS ranges:
    - ap-northeast-1 (Tokyo)
    - ap-southeast-1 (Singapore)
    - ap-southeast-2 (Sydney)
    - ap-south-1 (Mumbai)
- **EMEA Cloud Scanners**: A group of scanners from the following AWS ranges:
    - eu-west-1 (Ireland)
    - eu-west-2 (London)
    - eu-central-1 (Frankfurt)
    - me-central-1 (UAE)
- **UAE Cloud Scanners**: A group of scanners from the me-central-1 range.

Note: If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.

Tenable FedRAMP Moderate Cloud Sensors

Important: For Tenable FedRAMP Moderate Cloud Sensors, you must ensure that you connect your sensors using *https://sensor.fedcloud.tenable.com/*.

- For cloud based network scans, add the following IP ranges to your allow list:
  - 3.32.43.0 - 3.32.43.31 (3.32.43.0/27)
  - 3.31.100.0/24
  - 2600:1f12:98d:c900::/56
- For internal scanner or agent communications, add the following IP ranges to your allow list:
  - 52.61.37.84
  - 15.200.117.191
  - 172.65.64.208
  - 172.65.64.209
  - 172.65.64.210
  - 172.65.64.211
  - 2606:4700:78::120:0:1200
  - 2606:4700:78::120:0:1201
  - 2606:4700:78::120:0:1202
  - 2606:4700:78::120:0:1203

Sensor Security

See the following sections to learn more about sensor security and encryption when using the Tenable Vulnerability Management platform:

- Sensor Overview
- Linking Keys
- Data Encryption

Sensor Overview

Sensors access Tenable Vulnerability Management through the following site: `<port> - sensor.cloud.tenable.com:443`. All sensors (Tenable Nessus scanners, Tenable Agents, Tenable Network Monitor) need access to `cloud.tenable.com:443`.

> **Note:** If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.

Depending on how you deploy and set up Tenable Nessus scanners and Tenable Network Monitor - you need to access their respective user interfaces for initial setup:

- Tenable Nessus – `<IP>:8834`
- Tenable Network Monitor – `<IP>:8835`

  > **Note:** If you are deploying Tenable Nessus or Tenable Network Monitor with Tenable Core, you also need access to the underlying virtual appliance interface: `<IP>:8000`.

Tenable Vulnerability Management uses a user interface, driven by Tenable's customer-facing APIs, for all operations. The sensors that connect to Tenable Vulnerability Management play a major role in your security, collecting vulnerability and asset information. Protecting this data and ensuring the communication paths are secure is a core function of Tenable Vulnerability Management.

Nessus sensors connect to the Tenable Vulnerability Management platform after securely authenticating and linking to Tenable Vulnerability Management (see Linking Keys in the following section to learn more). Once linked, Tenable Vulnerability Management manages all updates to ensure the sensors are always up to date.

Sensors always initial the traffic between sensors and Tenable Vulnerability Management, and the traffic is outbound-only over port 443. Traffic is encrypted via SSL communication using TLS 1.2+ (or version 1.2 when in NIAP mode) with a 4096-bit key. This removes the need for firewall changes and allows you to control the connections via firewall rules.

Note: To learn more about NIAP mode, see the following topics in their respective product user guides:

- Configure Tenable Nessus for NIAP Compliance
- Configure Tenable Agent for NIAP Compliance
- Configure Tenable Network Monitor for NIAP Compliance

Linking Keys

Tenable Vulnerability Management uses a linking key as an initial authentication token for sensors. The linking key allows you to create the initial link between your sensor (a Nessus scanner, Nessus Agent, or Tenable Network Monitor) and Tenable Vulnerability Management.

When the Tenable Vulnerability Management platform receives a link request from a sensor, it validates the presented linking key with valid linking keys. If it finds that it matches a valid linking key, Tenable Vulnerability Management allows the sensor to link.

Upon linking, Tenable Vulnerability Management randomly generates, saves, and sends a 256-bit length key to the sensor. This key is unique to the sensor.

Once the link process is complete, the sensor no longer needs or uses the linking key. Any future authentication is performed in the following ways:

- **Sensor-to-platform authentication**

  After the initial linking process, the sensor provides the 256-bit key to identify and authenticate its requests. These requests include, but are not limited to, requesting jobs, scan policies, plugin updates, scanner binary updates, and providing information back to Tenable Vulnerability Management, such as scan results or sensor health data.

- **Sensor-to-platform job communication**

  Sensors check in to Tenable Vulnerability Management every so often (different sensor types have different check-in frequencies). When a scan job is launched, Tenable Vulnerability Management generates a policy and encrypts it with a randomly generated 128-bit key. The sensor requests the policy from the platform. The policy is stored on disk, but the key resides only in memory. The controller uses the key to encrypt the policy, which includes the scan credentials.

Data Encryption

Tenable Vulnerability Management encrypts all data in all states with at least one level, using no less than AES-256:

- Data at rest – Tenable Vulnerability Management stores data on encrypted media using at least one level of AES-256 encryption. Some data classes include a second level of per-file encryption.
- Data in transport – Tenable Vulnerability Management uses TLS version 1.2+ with a 4096-bit key to encrypt data during transportation (including internal transports).
- Backed up or replicated data – Tenable Vulnerability Management stores volume snapshots and data replicas with the same level of encryption as their source: no less than AES-256. All replication is done within AWS. Tenable does not back up any data to physical, off-site media or physical systems.
- Index data – Tenable Vulnerability Management stores index data on encrypted media using at least one level of AES-256 encryption.

Tenable can rotate all the stored, encrypted data to a new key. Alternatively, you can switch to a new site to use a new key (in other words, Tenable does not reuse keys when provisioning a new site). Tenable manages the keys with AWS Key Management.

Link a Sensor

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Required Tenable Web App Scanning User Role: Scan Manager or Administrator

This procedure describes how to link a sensor to Tenable Vulnerability Management.

Linking a sensor to Tenable Vulnerability Management represents a one-time event in managing a sensor, unless you remove the sensor. After you link the sensor, the sensor connects to Tenable Vulnerability Management using unique credentials.

Once you copy the linking key in Tenable Vulnerability Management, you must paste the linking key in the appropriate location of the sensor user interface (for example, the Tenable Agent CLI or the Tenable Network Monitor **Cloud Settings** section). Expand the following sections for specific details.

Note: If you use the Tenable Vulnerability Management FedRAMP environment, Tenable recommends reviewing the following documents before you link sensors:

- Cloud Sensors (FedRAMP Moderate Cloud Sensors) – View the Tenable Vulnerability Management FedRAMP sensor connectivity IP ranges, which are different from non-FedRAMP environments.
- If you have policies that require you to enable NIAP compliance settings, view the following topics to configure your scanners and agents accordingly:
  - Configure Tenable Nessus for NIAP Compliance
  - Configure Tenable Agent for NIAP Compliance

Note: If you use domain allowlists for firewalls, Tenable recommends adding:

- * cloud.tenable.com (Commercial)
- *.fedcloud.tenable.com (FedRAMP)

(with the wildcard character) to the allowlist. This ensures communication with sensor.fed/cloud.tenable.com, which the scanner uses to communicate with Tenable Vulnerability Management. If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Agents, Tenable Web App Scanning scanners, or Tenable Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.

Note: Under certain circumstances, you may need to regenerate the linking key. See Regenerate a Linking Key for more information. To learn more about the sensor security and linking keys, see Sensor Security.

To link a sensor:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Then:

   To link a Tenable Agent sensor, click the **Nessus Agents** tab.

   Note: For troubleshooting agents in environments where Zscaler is used, see the Difficulties with Nessus Agents when Zscaler is in useTenable community article.

a. Click ⊕ **Add Agent**.

   The **Add Agent** plane appears.

b. Do one of the following:

   - To install and link Tenable Agent manually:

     a. In the **Linking Key** section, click **Copy**.

        A **Linking key copied to clipboard** confirmation message appears.

     b. Access the Tenable Agent instance that you want to link to Tenable Vulnerability Management.

     c. Use the copied linking key in the Tenable Agent CLI to link the sensor. For more information, see Install Tenable Agent in the *Tenable Agent Deployment and User Guide*.

   - (Windows only) To use a single command to install and link Tenable Agent:

     a. Under the **Installing Agent on Windows platforms** header, copy the command.

        The command contains the linking key and syntax required to install the agent, link the agent to Tenable Vulnerability Management, change the agent name, and add the agent to an agent group. For example:

        ```
        Invoke-WebRequest -Uri “https://cloud.tenable.com/install/
        {sensorType}/installer/ms-install-script.ps1” -OutFile “./ms-
        install-script.
        ps1"; & “./ms-install-script.ps1” -key “{linkingKey}” -type
        “{sensorType}” -name “<agent name>” -groups “<list of groups>“;
        Remove-Item -Path “./ms-install-script.ps1”
        ```

        Tip: For Tenable FedRAMP Moderate environments, use "fedcloud.tenable.com".

     b. In the command, replace *<agent name>* with the agent name.

> **Tip:** If you do not want to set a custom agent name, remove `-name "<agent name>"`. If you do not set a custom name, Tenable names the agent using the hostname of the machine on which you installed the agent.

c. In the command, replace `<list of groups>` with the agent group name or names.

> **Note:** The agent group name is case-sensitive and must match exactly. You must encase the agent group name in quotation marks (for example, `--groups="My Group"`).

> **Tip:** If you do not want to add the agent to an agent group, remove `-groups "<list of groups>"`.

d. As a user with administrative privileges, access the CLI of the Windows machine on which you want to install the agent.

e. Run the command.

Tenable Agent installs on your Windows machine, links to your instance of Tenable Vulnerability Management, and updates the agent name and agent group if necessary.

- (Linux only) To use a single command to install and link Tenable Agent:

a. Under the **Installing Agent on Linux platforms** header, copy the command.

The command contains the linking key and syntax required to install the agent, link the agent to Tenable Vulnerability Management, change the agent name, and add the agent to an agent group. For example:

```
curl -H 'X-Key:
abcd1234efgh5678ijkl9012mnop3456qrst7890uvwx1234yz5678abcd1234ef'
'https://cloud.tenable.com/install/agent?name=agent-
name&groups=agent-group' | bash
```

> **Note:** For Tenable FedRAMP Moderate environments, use "fedcloud.tenable.com".

b. In the command, replace *agent-name* with the agent name.

> **Tip:** If you do not want to set a custom agent name, remove `name=agent-name`. If you do not set a custom name, Tenable names the agent using the hostname of the machine on which you installed the agent.

c. In the command, replace *agent-group* with the agent group name.

> **Note:** The agent group name is case-sensitive and must match exactly. You must encase the agent group name in quotation marks (for example, `--groups="My Group"`).

> **Tip:** If you do not want to add the agent to an agent group, remove `groups=agent-group`.

d. As a user with administrative privileges, access the CLI of the Linux machine on which you want to install the agent.

e. Run the command.

Tenable Agent installs on your Linux machine, links to your instance of Tenable Vulnerability Management, and updates the agent name and agent group if necessary.

To link an Tenable Network Monitor instance, click the **Nessus Network Monitors** tab.

a. Click ⊕ **Add Nessus Network Monitor**.

The **Add Nessus Network Monitor** plane appears.

b. In the **Linking Key** section, click **Copy**.

A **Linking key copied to clipboard** confirmation message appears.

c. Access the Tenable Network Monitor instance that you want to link to Tenable Vulnerability Management.

d. Use the copied linking key in the Tenable Network Monitor user interface to link the sensor. For more information, see the NNM User Guide.

To link a Tenable Nessus sensor, click the **Nessus Scanners** tab.

a. Click ⊕ **Add Nessus Scanner**.

The **Add Nessus** plane appears.

b. Do one of the following:

- To install and link Tenable Nessus manually:

  a. In the **Linking Key** section, click **Copy**.

  A **Linking key copied to clipboard** confirmation message appears.

  b. Access the Tenable Nessus instance that you want to link to Tenable Vulnerability Management.

  c. Use the copied linking key in the Tenable Nessus user interface to link the sensor. For more information, see the Link to Tenable Vulnerability Management in the *Tenable Nessus User Guide*.

- (Windows only) To use a single command to install and link a Tenable Nessus scanner:

  a. Under the **One-Line Installation** instructions, copy the command.

  The command contains the linking key and syntax required to install the scanner, link the scanner to Tenable Vulnerability Management, change the scanner name, and add the scanner to a scanner group. For example:

```
Invoke-WebRequest -Uri
"https://cloud.tenable.com/install/scanner/installer/ms-install-
script.ps1" -OutFile "./ms-install-script.ps1"; & "./ms-install-
script.ps1" -key
"51cc161bfa7c62dd7fc90a63561a256306cda982e3edba9d7ebadc05f6a2118c"
-type "scanner" -name "<scanner name>" -groups "<list of groups>";
Remove-Item -Path "./ms-install-script.ps1"
```

> **Tip:** For Tenable FedRAMP Moderate environments, use "fedcloud.tenable.com".

b. In the command, replace `<scanner-name>` with the scanner name.

> **Tip:** If you do not want to set a custom scanner name, remove `-name "<scanner-name>"`. If you do not set a custom name, Tenable names the scanner using the hostname of the machine on which you installed the scanner.

c. In the command, replace `<list of groups>` with the scanner group name.

> **Note:** The scanner group name is case-sensitive and must match exactly.

> **Tip:** If you do not want to add the scanner to a scanner group, remove `-groups "<list of groups>"`.

d. As a user with administrative privileges, access the CLI of the Windows machine on which you want to install the scanner.

e. Run the command.

Tenable Nessus installs on your Windows machine, links to your instance of Tenable Vulnerability Management, and updates the scanner name and scanner group if necessary.

- (Linux only) To use a single command to install and link a Tenable Nessus scanner:

a. Under the **One-Line Installation** instructions, copy the command.

The command contains the linking key and syntax required to install the scanner, link the scanner to Tenable Vulnerability Management, change the scanner name, and add the scanner to a scanner group. For example:

```
curl -H 'X-Key:
abcd1234efgh5678ijkl9012mnop3456qrst7890uvwx1234yz5678abcd1234ef'
'https://cloud.tenable.com/install/scanner?name=scanner-
```

```
name&groups=scanner-group'| bash
```

Tip: For Tenable FedRAMP Moderate environments, use "fedcloud.tenable.com".

b. In the command, replace *scanner-name* with the scanner name.

Tip: If you do not want to set a custom scanner name, remove `name=scanner-name`. If you do not set a custom name, Tenable names the scanner using the hostname of the machine on which you installed the scanner.

c. In the command, replace *scanner-group* with the scanner group name.

Note: The scanner group name is case-sensitive and must match exactly.

Tip: If you do not want to add the scanner to a scanner group, remove `groups=scanner-group`.

d. As a user with administrative privileges, access the CLI of the Linux machine on which you want to install the scanner.

e. Run the command.

Tenable Nessus installs on your Linux machine, links to your instance of Tenable Vulnerability Management, and updates the scanner name and scanner group if necessary.

To link a Tenable Core + Tenable Web App Scanning instance, in the left navigation menu, click **Web App Scanners**.

a. Click ⊕ **Add Web Application Scanner**.

The **Add Web Application Scanner** plane appears.

b. In the **Linking Key** section, click **Copy**.

A **Linking key copied to clipboard** confirmation message appears.

c. Access the Tenable Core + Tenable Web App Scanning instance that you want to link to Tenable Vulnerability Management.

d. Use the copied linking key in the Tenable Core + Tenable Web App Scanning user interface to link the sensor. For more information, see the Tenable Core+Tenable Web App Scanning User Guide.

What to do next:

- Manage the sensor in Tenable Vulnerability Management (including disabling or re-enabling the sensor link).
- Select the sensor when configuring Tenable Vulnerability Management scans.

Regenerate a Linking Key

Required User Role: Administrator

Under certain circumstances, you may need to regenerate the linking key for your Tenable Vulnerability Management instance. For example, you may regenerate the key for security reasons if an employee with knowledge of the linking key leaves your organization.

Regenerating a linking key does not affect sensors that are currently linked to Tenable Vulnerability Management, because the linking key is only used to establish the initial link. After you link a sensor, the sensor connects to Tenable Vulnerability Management using unique credentials.

If your organization has hard-coded a linking key into implementation scripts, keep in mind the following:

- Be sure to replace the original key with the regenerated key to prevent script failure.
- Each Tenable Vulnerability Management instance uses a single linking key for all sensor types. If you regenerate the linking key while working with one type of sensor (for example, Tenable Nessus scanners), you also regenerate the linking key for the other sensor types. If you regenerate the linking key, be sure to update the implementation for scripts involving all types of sensors.

Note: To learn more about Tenable Vulnerability Management linking keys, see Sensor Security.

To regenerate a linking key for your Tenable Vulnerability Management instance:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click any sensor type tab (for example, **NNM**).

   The appropriate sensor page appears.

3. Click the **Add [Sensor Type]** button (for example, **Add NNM**).

   The appropriate sensor plane appears (for example, **Add NNM**).

4. In the **Add [Sensor Type]** plane, click the **Regenerate** button.

   A confirmation window appears.

5. In the confirmation window, click **Regenerate**.

   The **Regenerated Linking Key** message appears, and the new linking key replaces the original linking key in the **Add [Sensor Type]** plane.

What to do next:

- Link a sensor.

View Sensors and Sensor Groups

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Required Tenable Web App Scanning User Role: Scan Manager or Administrator

On the **Sensors** page, you can view your linked sensors: Tenable Vulnerability Management cloud sensors, your Tenable Nessus Scanners, Tenable Agents, Tenable Network Monitors, and Tenable Web App Scanning Scanners. You can also view your scanner groups and agent groups.

To view sensors and sensor groups:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Use the left navigation pane to choose what sensors to view:

    - **Nessus Scanners** – Cloud Scanners, Linked Scanners, Scanner Groups
    - **Nessus Agents** – Linked Agents, Agent Groups, Freeze Windows, Settings, Networks, Profiles
    - **Nessus Network Monitors**
    - **OT Connectors**
    - **Web Application Scanners** – Linked Scanners, Scanner Groups

    Each sensor page shows a list of your linked sensors or groups, along the basic information listed in the following table. Depending on what sensor you are viewing, you may not see all the columns described.

    You can also view the same information by clicking the sensor and viewing its details page.

Column	Description
Actions	The actions that you can perform for each sensor.
Created	The date on which the sensor group was created.
Groups	The group or groups to which the sensors belongs.
Health	The health status of the linked agent: • **Healthy** – The health event is healthy and requires no action. • **Warning** – The health event is unhealthy and may cause minimal impact on the agent's performance. • **Critical** – The health event is unhealthy and may cause a major impact on the agent's performance. Tenable recommends working to resolve any **Critical** health events. • **Unknown** – The health event status is currently unknown.

	For agents configured with continuous assessment scanning, the **Health** column also shows two health icons:
	• Runtime Scanning – Indicates the general health of the following vulnerability management-related agent events.
	  • **Module Comms**
	  • **Module Runtime Scan**
	  • **Comms Backoff State**
	• Vulnerability Management Scanning – Indicates the general health of the following vulnerability management-related agent events:
	  • **Plugin Compilation**
	  • **Plugin Disk Usage**
	  • **Plugin Integrity Checks**
	  • **Plugin Updates**
	  • **System Disk Usage**
	For more information about agent health, you can view an agent's **Linked Health Events** tab.

Hostname	The hostname of the sensor. **Note:** For Nessus Web Application Scanners, the hostname shows as **N/A**.
IP Address	The IP address of the sensor.
Last Modified	The date on which the sensor was last modified.
Last Plugin Update	The date on which the sensor's plugins were last updated.

Last Scanned	The date on which the sensor last performed a scan.
Linked On	The date on which the sensor was linked to Tenable Vulnerability Management.
Name	The name of the sensor.
Network	The network associated with the sensor or sensor group.
Platform	The platform associated with the sensor. **Note:** For Nessus Web Application Scanners, the platform shows as **N/A**.
Plugin Set	The plugin set of the sensor.
Profile	The agent profile to which the agent belongs.
Runtime Module	Indicates whether the agent is enabled with continuous assessment scanning.
Scanner Count	The number of scanners in the group.
Scans or **Scan Count**	The number of scans that the sensor or sensor group is currently running. **Note:** This value does not appear for Tenable Web App Scanning scans.
Status	The status of the sensor – **Online** or **Offline**.
Updated	The date on which the sensor group was last updated.
Version	The version of the sensor.

View Sensor Details

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

You can view details for both cloud sensors and linked sensors.

To view sensor details:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the sensor type tab you want to view.

   A table of sensors appears.

3. For **Nessus Scanners**, do one of the following:

   - In the drop-down box, select the **Cloud Scanners** tab to view cloud scanners connected to Tenable Vulnerability Management. For more information, see Cloud Sensors.
   - In the drop-down box, click the **Linked Scanners** tab to view on-premises scanners linked to Tenable Vulnerability Management. For more information, see Linked Scanners.

4. In the sensors table, click the sensor where you want to view details.

   The **Details** page appears.

   Depending on the sensor type, you can do the following in the **Details** page:

   - Click the **Settings** tab to modify sensor settings.
   - Click the **Permissions** tab to modify sensor permissions.

Edit Sensor Settings

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

You can edit certain settings for the following types of linked sensors:

- Tenable Network Monitor
- Tenable Nessus for Amazon Web Service (AWS)

To edit sensor settings in the new interface:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the appropriate sensor type tab.

   The sensor table appears.

3. If the sensor is a **Nessus Scanner**, do one of the following:

   - In the drop-down box, select the **Cloud Scanners** tab to view cloud scanners connected to Tenable Vulnerability Management. For more information, see Cloud Sensors.
   - In the drop-down box, select the **Linked Scanners** tab to view scanners linked to Tenable Vulnerability Management. For more information, see Linked Scanners

4. In the table of linked sensors, click the sensor for which you want to edit settings.

   The sensor details appear. By default, the **Overview** tab is active.

5. Click the **Settings** tab.

   The sensor settings appear.

6. Edit the sensor settings:

Setting	Sensor Type	Description
Report Frequency	NNM	Specifies the frequency, in minutes, that you want the sensor to report information to Tenable Vulnerability Management.
Software Update Type	NNM (5.6.1 and later only)	Specifies which components, if any, you want Tenable Network Monitor to automatically update. **All components** includes web server, HTML client, plugins, and engine.
Updates instances every	AWS	Specifies the frequency, in minutes, that you want the AWS sensor to report information

(minutes)		to Tenable Vulnerability Management about the instances it has access to.

7. In the lower-right corner of the page, click **Save**.

Edit Sensor Permissions

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

You can set the following Tenable Vulnerability Management user permissions levels in your sensor configuration:

- **No Access** – The user or group cannot use the scanner in scan configurations or edit the scanner configuration.
- **Can Use** – The user or group can use the scanner in scan configurations, but cannot edit the scanner configuration.
- **Can Manage** – The user or group can use the scanner in scan configurations and edit the scanner configuration.

Note: Cloud scanners always have the **Can Use** permission regardless of how you configure them.

To modify sensor permissions:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the appropriate sensor type tab.

   A sensors table appears.

3. If the sensor is a **Nessus Scanner**, click the **Linked Scanners** tab to view on-premises scanners linked to Tenable Vulnerability Management. For more information, see Linked Scanners.

4. In the table of linked sensors, click the sensor for which you want to set permissions.

The **Details** page appears. For all sensors except agents, the **Overview** tab is active by default.

5. Click the **Permissions** tab.

   Note: By default, any user in your Tenable Vulnerability Management instance can use the scanner.

6. Do any of the following:

   - To select a permissions level from the drop-down box for the **Default** user.
   - To specify permissions for an individual user or user group:

     a. In the **Add users or user groups** text box, type the name of a user or user group.

     As you type, Tenable Vulnerability Management searches for matches to existing users or user groups.

     b. In the search results, select a user or user group.

     c. In the permissions drop-down, select a permissions level for the user or user group you added.

7. In the lower-right corner of the page, click **Save**.

Enable or Disable a Sensor

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

To enable or disable a sensor:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the appropriate sensor type tab.

   The sensors table appears.

3. (Optional) If the sensor is a **Nessus Scanner**, select **Linked Scanners** in the drop-down box to view on-premises scanners linked to Tenable Vulnerability Management. For more information, see Linked Scanners.

4. In the table of linked sensors, do one of the following:

   - Right-click the sensor you want to enable or disable.

     The action options appear next to your cursor.

   - In the **Actions** column, click the ⋮ button you want to enable or disable.

     The action options appear in the row.

5. Do one of the following:

   - To enable a sensor, click the **Enable** button.
   - To disable a sensor, click the **Disable** button.

   Tenable Vulnerability Management enables or disables the sensor.

Remove a Sensor

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Note: You cannot remove cloud sensors.

To remove a sensor:

1. In the left navigation, click **Sensors**.

   The **Sensors** page appears. By default, the **Nessus Scanners** tab is active and **Linked Scanners** is selected in the drop-down box.

2. Click the appropriate sensor type tab.

   The sensor table appears.

3. For **Nessus Scanners**, select **Linked Scanners** in the drop-down box to view on-premises scanners linked to Tenable Vulnerability Management. For more information, see Linked Scanners.

4. In the table of linked sensors, do one of the following roll over the sensor you want to remove.

Scope	Action

Remove a sensor	a. In the sensors table, do one of the following: • Right-click the sensor you want to remove. The action options appear next to the cursor. • In the **Actions** column, click the ⋮ button for the sensor you want to remove. The action options appear in the row. • Select the check box next to the sensor you want to remove. The action bar appears at the top of the table. b. Click **Delete**. A confirmation window appears.
Remove multiple sensors	a. In the sensors table, select the check box for the sensors you want to remove. The action bar appears at the top of the table. b. Click **Delete**. A confirmation window appears.

5. Click **Delete** to confirm the removal.

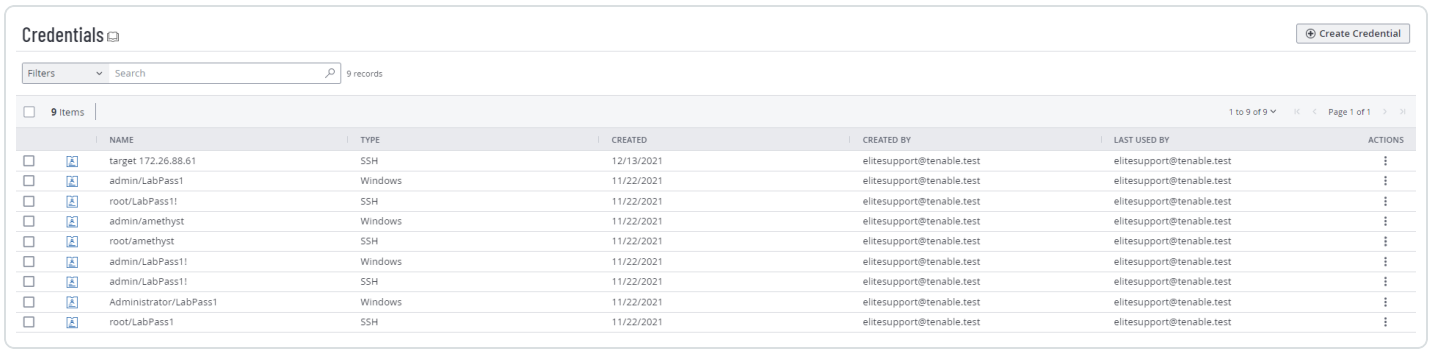
   Tenable Vulnerability Management removes the sensor from the list.

Credentials

> **Note:** This section describes creating and maintaining managed credentials. For more information about scan-specific or policy-specific credentials, see Credentials in Tenable Vulnerability Management Scans or Credentials in Tenable Web App Scanning Scans.

Managed credentials allow you to store credential settings centrally in a credential manager. You can then add those credential settings to multiple scan configurations instead of configuring credential settings for each individual scan.

You and users to whom you grant permissions can use managed credentials in scans. Credential user permissions control which users can use and edit managed credentials.



Create a Managed Credential

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

This topic describes creating a managed credential in the Tenable Vulnerability Management credential manager.

You can also create a managed credential during scan configuration, as well as convert a scan-specific credential to a managed credential. For more information, see Add a Credential to a Scan or Configure Credentials Settings in Tenable Web App Scanning.

To create a managed credential:

1. In the left navigation, click **Settings**.

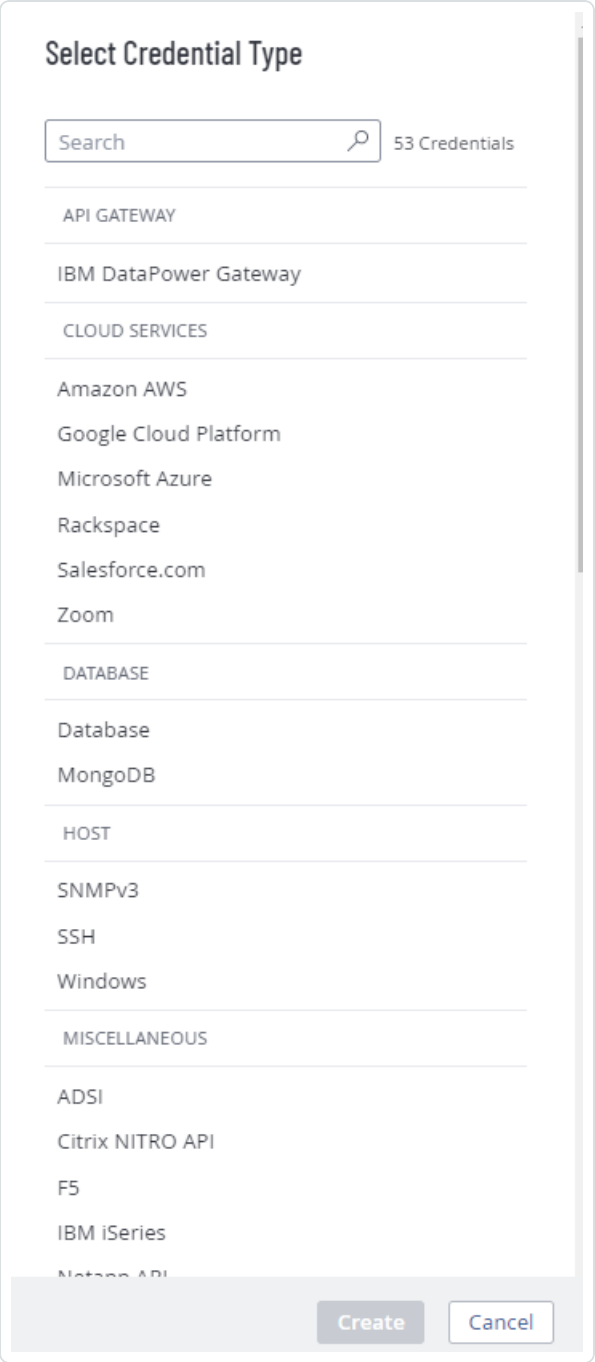
   The **Settings** page appears.

2. Click the **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

3. In the upper-right corner of the page, click the **Create Credential** button.

   The **Select Credential Type** plane appears.



4. Do one of the following:
    - Select one of the available credential types.
    - Click on a credential type in the category sections.

    The credential settings appear.
5. In the **Title** box, type a name for the credential.

6. (Optional) In the **Description** box, type a description for the credential.
7. Configure the settings for the credential type you selected.

   For more information about credential settings, see Credentials (Tenable Vulnerability Management) or Credentials (Tenable Web App Scanning).
8. Add user permissions.
9. Click **Save**.

   Tenable Vulnerability Management adds the credential to the credentials table in the **Credentials** page.

Edit a Managed Credential

> **Required Tenable Vulnerability Management User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

> **Required Tenable Web App Scanning User Role:** Basic, Scan Operator, Standard, Scan Manager, or Administrator

This topic describes editing a credential in the Tenable Vulnerability Management credential manager.

You can also edit managed credentials during scan configuration. For more information, see Add a Credential to a Scan for Tenable Vulnerability Management or Configure Credentials Settings in a Tenable Web App Scanning Scan for Tenable Web App Scanning.

You can edit any credentials where you have **Can Edit** permission.

To edit managed credentials:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.
2. Click the **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

3. Filter or search the credentials table for the credential you want to edit. For more information, see Tables.
4. In the credentials table, click the name of the credential you want to edit.

   The credential settings plane appears.
5. Do one of the following:
   - Edit the credential name or description.
     a. Roll over the name or description box.
     b. Click the button that appears next to the box.
     c. Make your changes.
     d. Click the button at the lower right corner of the box to save your changes.
   - Edit the settings for the credential type. For more information about these settings, see Credentials (Tenable Vulnerability Management) or Credentials (Tenable Web App Scanning).
   - Configure user permissions for the credential.
6. Click **Save**.

Configure User Permissions for a Managed Credential

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You configure user permissions for a managed credential separately from the permissions you configure for the scans where you use the credential.

You can configure credential permissions for individual users or a user group. If you configure credential permissions for a group, you assign all users in that group the same permissions. You may want to create the equivalent of a credential manager role by creating a group for the users you want to manage credentials. For more information, see User Groups.

If you create a managed credential, Tenable Vulnerability Management automatically assigns you **Can Edit** permissions.

To configure user permissions for a managed credential:

1. Create or edit a managed credential:

Location	Action
In the credential manager	create or edit
In a scan configuration	create or edit

2. Do one of the following:

   - Add permissions for a user or user group.

     a. In the credential settings plane, click the ⊕ button next to the **User Permissions** title.

        The **Add User Permission** settings appear.

     b. In the search box, type the name of a user or group.

        As you type, a filtered list of users and groups appears.

     c. Select a user or group from the search results.

     d. Click the ⌄ button next to the permission drop-down for the user or group.

     e. Select a permission level:

        - **Can Use** – The user can view the credential in the managed credentials table and use the credential in scans.
        - **Can Edit** – The user can view and edit credential settings, delete the credential, and use the credential in scans.

     f. Click **Add**.

     g. Click **Save**.

   - Edit permissions for a user or user group.

a. In the **User Permissions** section of the credential settings plane, click the ⌄ button next to the permission drop-down for the user or group.

b. Select a permission level:

- **Can Use** – The user can view the credential in the managed credentials table and use the credential in scans.
- **Can Edit** – The user can view and edit credential settings, delete the credential, and use the credential in scans.

c. Click **Save**.

- Delete permissions for a user or user group.

a. In the **User Permissions** section of the credential settings plane, roll over the user or group you want to delete.

b. Click the ✕ button next to the user or user group.

The user or group is removed from the **User Permissions** list.

c. Click **Save**.

Export Credentials

Required User Role: Administrator

On the **Credentials** page, you can export the data for one or more managed credentials.

Note: When you export credential data, authentication details such as usernames, passwords, or keys are not included in the export.

To export credential data:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.
4. Select the credentials that you want to export:

Export Scope	Action
Selected credentials	To export selected credentials: a. In the credentials table, select the check box for each credential you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 credentials, select all the credentials in the list and then click [→ **Export**.
A single credential	To export a single credential: a. In the credentials table, right-click the row for the credential you want to export. The action options appear next to your cursor. -or- In the credentials table, in the **Actions** column, click the ⋮ button in the row for the credential you want to export. The action buttons appear in the row. b. Click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

> **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

5. In the **Name** box, type a name for the export file.
6. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of credentials. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of credentials. Empty fields are not included in the JSON file.

7. (Optional) Deselect any fields you do not want to appear in the export file.
8. In the **Expiration** box, type the number of days before the export file expires.

> **Note**: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

9. (Optional) To set a schedule for your export to repeat:
   - Click the **Schedule** toggle.

     The **Schedule** section appears.
   - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.

- In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
- In the **Repeat** drop-down box, select how often you want the export to repeat.
- In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

  > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

10. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.
    - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

11. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

12. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file from the Exports page.

Delete a Managed Credential

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can delete any credentials where you have **Can Edit** permission.

To delete a managed credential:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

3. Filter or search the credentials table for the credential you want to delete. For more information, see Tables.

4. In the table, roll over the credential you want to delete.

   The action buttons appear in the row.

5. Click the button.

   The **Confirm Deletion** window appears.

6. Do one of the following:

   - If no scans use the credential, click **Delete**.
   - If any scans use the credential:

     a. Click **View Scans**.

        The **Scans** plane appears.

     b. Filter or search for scans that use the credential.

     c. Do one of the following:

- Click **Cancel** to cancel the deletion.
- Click **Delete** to confirm the deletion.

Exclusions

You can use exclusions to restrict the scanning of specific hosts based on a selected schedule.

Note: Exclusions do not apply to agent scans.

Note: If a target has been moved to a different network, you must update any related exclusions. Otherwise, the target may be blocked from scanning.

Important: Tenable does not recommend applying exclusions to PAM integration servers. This prohibits Tenable Vulnerability Management from accessing those credentials and, as a result, Tenable Vulnerability Management cannot run scans using them.

For more information on exclusions, see the following topics:

Create an Exclusion

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Note: Exclusions do not apply to agent scans.

Important: Tenable does not recommend applying exclusions to PAM integration servers. This prohibits Tenable Vulnerability Management from accessing those credentials and, as a result, Tenable Vulnerability Management cannot run scans using them.

To create an exclusion:

1. In the left navigation, click ⚙ **Settings**.

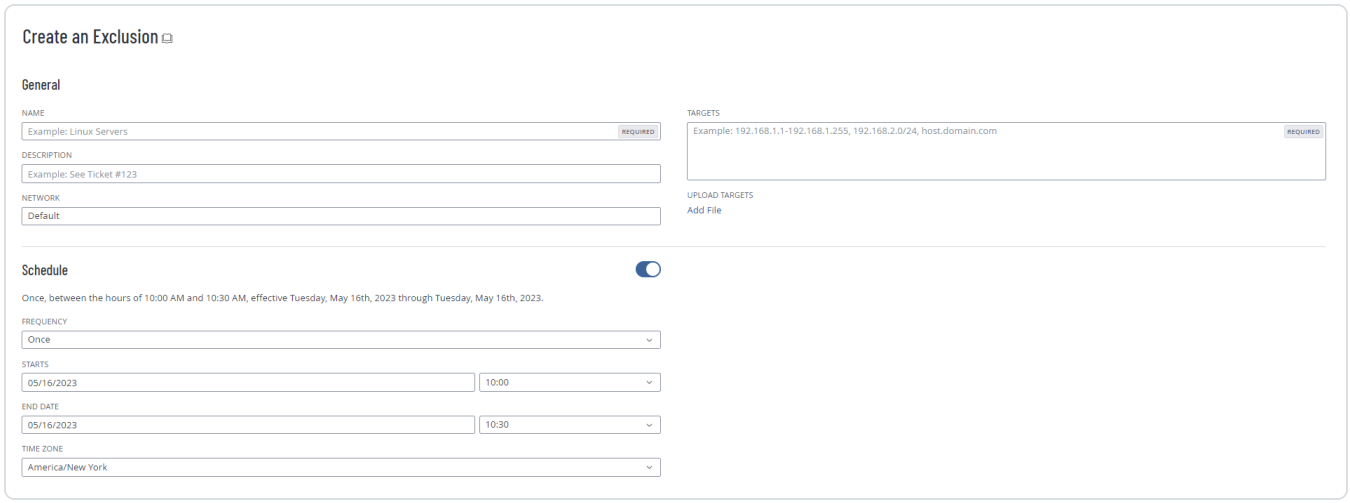
   The **Settings** page appears.

2. Click the **Exclusions** tile.

   The **Exclusions** page appears.

3. In the upper-right corner of the page, click the ⊕ **Create Exclusion** button.

   The **Create an Exclusion** page appears.



4. Set the exclusion settings.
5. Click **Save**.

   Tenable Vulnerability Management saves the exclusion and applies the exclusion to the selected scan targets.

Edit an Exclusion

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

To edit an exclusion:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Exclusions** tile.

   The **Exclusions** page appears.

3. In the exclusions table, click the exclusion you want to edit.

   The **Update an Exclusion** page appears.

4. Edit the exclusion settings.

5. Click **Save**.

   Tenable Vulnerability Management saves the exclusion, and the **Exclusions** page appears.

Import an Exclusion

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

You can import an exclusion as a `.csv` file.

Note: When you import an exclusion, Tenable Vulnerability Management automatically assigns it to the default network. After import, you can move the exclusion to a custom network.

Before you begin:

- Create a `.csv` file in the specified format.

To import an exclusion:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exclusions** tile.

   The **Exclusions** page appears.

3. In the upper-right corner of the page, click the **Import** button.

   Your operating system's file manager appears.

4. Select a `.csv` file to import.

   Tenable Vulnerability Management imports the file and adds the exclusions to the exclusions table.

Exclusion Import File

You can import one or more exclusions as a `.csv` file.

Note: Tenable does not recommend opening the `.csv` file in Microsoft Excel, as Excel can add additional characters to the file that Tenable Vulnerability Management cannot recognize.

This file is composed of a header and at least one line of data. Separate each line in the file with a new line break.

Header (Optional)

A header line in the file is optional. If included, the header must be the first line in the file and be formatted as follows:

```
id,name,description,members,creation_date,last_modification_date
```

Note: There are no spaces after the commas.

Data (Required)

Each data line in the file represents one exclusion configuration. Data lines must be separated from each other by a new line break. The file must include at least one data line.

Each data line is a comma-separated string of fields described in the following.

Note: Optional fields can be blank, but the associated comma separator must be present in the data line.

Field	Description	Required
id	An integer that uniquely identifies the exclusion.	No
name	The name of the exclusion. You can use any combination of alphanumeric characters or symbols.	Yes
description	A description for the exclusion.	Yes
members	The target or targets where you want the scan exclusion to apply. This value can have the following formats: • A hostname (example.com) • An IP address (192.0.2.57) • An IP range (192.0.2.57-192.0.2.67)	Yes

	• A comma-separated list of multiple hostnames, IP addresses, or IP ranges, bracketed by quotation marks ("192.0.2.57,192.0.2.177,192.0.2.8")	
creation_date	The Unix timestamp that Tenable Vulnerability Management uses as the creation date for the imported exclusion.	No
last_ modification_ date	The Unix timestamp that Tenable Vulnerability Management uses as the last modification date for the exclusion.	No

Example

```
id,name,description,members,creation_date,last_modification_date
1,Exclusion Rule 1,routers,"192.0.2.57,192.0.21.177,192.0.28",1561643735,1561643785
2,Exclusion Rule 2,workstations,192.0.257-192.0.267,1561643735,1561643785
```

Export an Exclusion

Required User Role: Administrator

On the **Exclusions** page, you can export one or more scanning exclusions.

To export an exclusion:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exclusions** tile.

   The **Exclusions** page appears. This page displays a list of exclusions configured on your Tenable Vulnerability Management account.

3. (Optional) Refine the table data. For more information, see Interact with a Customizable Table.

4. Select the exclusions that you want to export:

Export Scope	Action
Selected exclusions	To export selected exclusions: a. In the exclusions table, select the check box for each exclusion you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 exclusions, select all the exclusions in the list and then click [→ **Export**.
A single exclusion	To export a single exclusion: a. In the exclusions table, right-click the row for the exclusion you want to export. The action options appear next to your cursor. -or- In the exclusions table, in the **Actions** column, click the ⋮ button in the row for the exclusion you want to export. The action buttons appear in the row. b. Click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

Note: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

5. In the **Name** box, type a name for the export file.
6. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of exclusions. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of exclusions. Empty fields are not included in the JSON file.

7. (Optional) Deselect any fields you do not want to appear in the export file.
8. In the **Expiration** box, type the number of days before the export file expires.

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

9. (Optional) To set a schedule for your export to repeat:
   - Click the **Schedule** toggle.

     The **Schedule** section appears.
   - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
   - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
   - In the **Repeat** drop-down box, select how often you want the export to repeat.

- In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

  > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

10. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

    - In the **Add Recipients** box, type the email addresses to which you want to send the export notification.

    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      > **Note**: Tenable Vulnerability Management sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

11. Click **Export**.

    Tenable Vulnerability Management begins processing the export. Depending on the size of the exported data, Tenable Vulnerability Management may take several minutes to process the export.

    When processing completes, Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

12. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file from the Exports page.

Delete an Exclusion

> **Required Tenable Vulnerability Management User Role:** Scan Manager or Administrator

To delete an exclusion:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Exclusions** tile.

   The **Exclusions** page appears.

3. Select the exclusion or exclusions you want to delete:

   - Select a single exclusion.

     a. In the exclusions table, roll over the exclusion you want to delete.

        The action buttons appear in the row.

     b. In the row, click the button.

        A confirmation window appears.

   - Select multiple exclusions.

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

        The action bar appears at the bottom of the page.

     b. In the action bar, click the button.

        A confirmation window appears.

4. In the confirmation window, click **Delete**.

   Tenable Vulnerability Management deletes the selected exclusion or exclusions.

Exclusion Settings

Note: Exclusions do not apply to agent scans.

Setting	Description
Settings	
Name	Specifies a name for the exclusion.
Description	Specifies a description for the exclusion.

Setting	Description
Targets	Specifies targets that you want excluded from scans. You cannot use the **Targets** setting if you already specified targets with the **Upload Targets** setting. Ways that you can list targets include, but are not limited to: • a single IP address • an IP range • a list of IP addresses, separated by commas For more information on how you can list targets, see Scan Targets. **Tip:** The **Targets** setting supports excluding specific ports per IP address by typing IP:Port entries. **Note:** If a target has been moved to a different network, you must update any related exclusions. Otherwise, the target may be blocked from scanning.
Network	Specifies the network that the targets belong to: either **Default** or a custom network. **Note:** Tenable Web App Scanning scan targets always belong to the default network.
Upload Targets	Uploads a text file with host names or IP ranges, separated by commas, that you want excluded from scans. You cannot use the **Upload Targets** setting if you already specified targets with the **Targets** setting.
Schedule	
Enabled	Enables or disables a schedule for when the exclusion is enabled. When disabled, the exclusion is set to **Always On**. When enabled, you can configure the following settings, which set a frequency and schedule for when the exclusion is enabled.

Setting	Description
Summary	A summary of the selections for the **Frequency**, **Starts**, and **Ends** settings.
Frequency	A drop-down box that contains the following options: **Once**, **Daily**, **Weekly**, **Monthly**, and **Yearly**.
Starts	Two drop-down boxes in which you can select a date and time when the exclusion begins. **Tip:** To select a more granular start time, manually type the desired time in the box, then click **Create**. **Note:** Tenable Vulnerability Management does not support an exclusion that starts and ends at 00:00 - 00:00.
Ends	Two drop-down boxes in which you can select a date and time when the exclusion ends. **Tip:** To select a more granular end time, manually type the desired time in the box, then click **Create**. **Note:** Tenable Vulnerability Management does not support an exclusion that starts and ends at 00:00 - 00:00.
Time Zone	A drop-down box with a search bar in which you can select a time zone for the selected dates and times.

Connectors

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Tenable Vulnerability Management uses connectors, including third-party data connectors, to import assets from other platforms. Tenable Vulnerability Management supports connectors for Tenable Vulnerability Management and Tenable Container Security.

Tenable Vulnerability Management Connectors

Vulnerability Management includes connectors for AWS, GCP, and Microsoft Azure. To use Tenable Vulnerability Management connectors to scan your assets, you must first configure the platform the connector integrates with, then create the connector, as described in the appropriate section for your platform:

- Amazon Web Service (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

After you configure platforms and create connectors, you can manage connectors from the **Settings** page in Tenable Vulnerability Management.

Note: When using cloud connectors. Tenable recommends allowlisting the IP addresses for the region in which the Tenable Vulnerability Management site resides.

The licensing implications are as follows:

- Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities. Discovery through the connector is free.
- Assets discovered through the connectors that did become licensed fall off the license the day after the asset was terminated. This event can be observed via the connector.
- When an asset is terminated, Tenable Vulnerability Management stops matching scan results to the asset. The asset is also deleted from the default view of the assets table.

- When an asset is deleted, Tenable Vulnerability Management purges the asset and any associated findings in Explore, and releases the asset's license. For more information, see Delete Assets.

Tip: For information on other ways to ingest data into Tenable Vulnerability Management, see the Data Ingestion in Tenable Vulnerability Management quick reference guide.

Supported Plugins

To view the supported plugins for AWS and Azure, see the Tenable Plugins page.

Amazon Web Services Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

The Amazon Web Services (AWS) connector provides real-time visibility and inventory of EC2 instances in your AWS account.

To import and analyze information about EC2 instances in AWS, you must first configure AWS to support your connector configuration, then create an AWS connector in Tenable Vulnerability Management.

You can create an AWS connector to discover AWS assets and import them to Tenable Vulnerability Management. Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities.

Alternatively, you can run a Tenable Nessus scanner or agent scan, which runs plugins locally on the host.

Note: The AWS connector performs two types of imports:

- **Full Sync**: Occurs when the AWS connector describes all EC2 instances in your account and imports them to Tenable Vulnerability Management.
- **Partial Sync**: Occurs when the AWS connector reads all cloud trail events and imports any created or terminated EC2 instances since the previous sync.

The AWS connector performs up to 47 partial syncs and one full sync in a 24-hour period. When you set a new schedule, the AWS resets and triggers another full sync.

Goal	Connector Type
Discover AWS assets The cloud connector discovers AWS assets without assessing them for vulnerabilities. Optionally, you can scan discovered assets later using a Tenable Nessus scanner or agent scan. For more information, see AWS Cloud Connector (Discovery Only).	• Keyless authentication (recommended) • Key-based authentication

To manage existing AWS connectors, see Manage Connectors.

Tip: For descriptions of common connector errors, see Connectors in the Tenable Developer Portal.

AWS Cloud Connector (Discovery Only)

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

The Amazon Web Services (AWS) cloud connector provides real-time visibility and inventory of EC2 assets in AWS accounts.

You can create an AWS connector to discover AWS assets and import them to Tenable Vulnerability Management. Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities.

This connector uses the `tenableio-connector` role permissions to collect information on EC2 instances in the AWS account.

You can create AWS connectors for discovery with either of the following configurations:

- Recommended: AWS Connector with Keyless Authentication (Discovery Only)
- AWS Connector with Key-based Authentication

Supported Regions

The following regions are supported for AWS Discovery Connectors:

- `us-east-1`, US East (N. Virginia)
- `us-east-2`, US East (Ohio)
- `us-west-1`, US West (N. California)
- `us-west-2`, US West (Oregon)
- `ca-central-1`, Canada (Central)
- `ap-south-1`, Asia Pacific (Mumbai)
- `ap-northeast-1`, Asia Pacific (Tokyo)
- `ap-northeast-2`, Asia Pacific (Seoul)
- `ap-southeast-1`, Asia Pacific (Singapore)
- `ap-southeast-2`, Asia Pacific (Sydney)
- `ap-southeast-3`, Asia Pacific (Jakarta)
- `eu-central-1`, EU (Frankfurt)
- `eu-west-1`, EU (Ireland)
- `eu-west-2`, EU (London)
- `eu-west-3`, EU (Paris)
- `me-south-1`, Middle East (Bahrain)
- `ap-east-1`, Asia Pacific (Hong Kong)
- `af-south-1`, Africa (Cape Town)
- `eu-south-1`, Europe (Milan)
- `sa-east-1`, South America (São Paulo)

AWS Connector with Keyless Authentication (Discovery Only)

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

The Amazon Web Services (AWS) Connector provides real-time visibility and inventory of EC2 assets in AWS accounts.

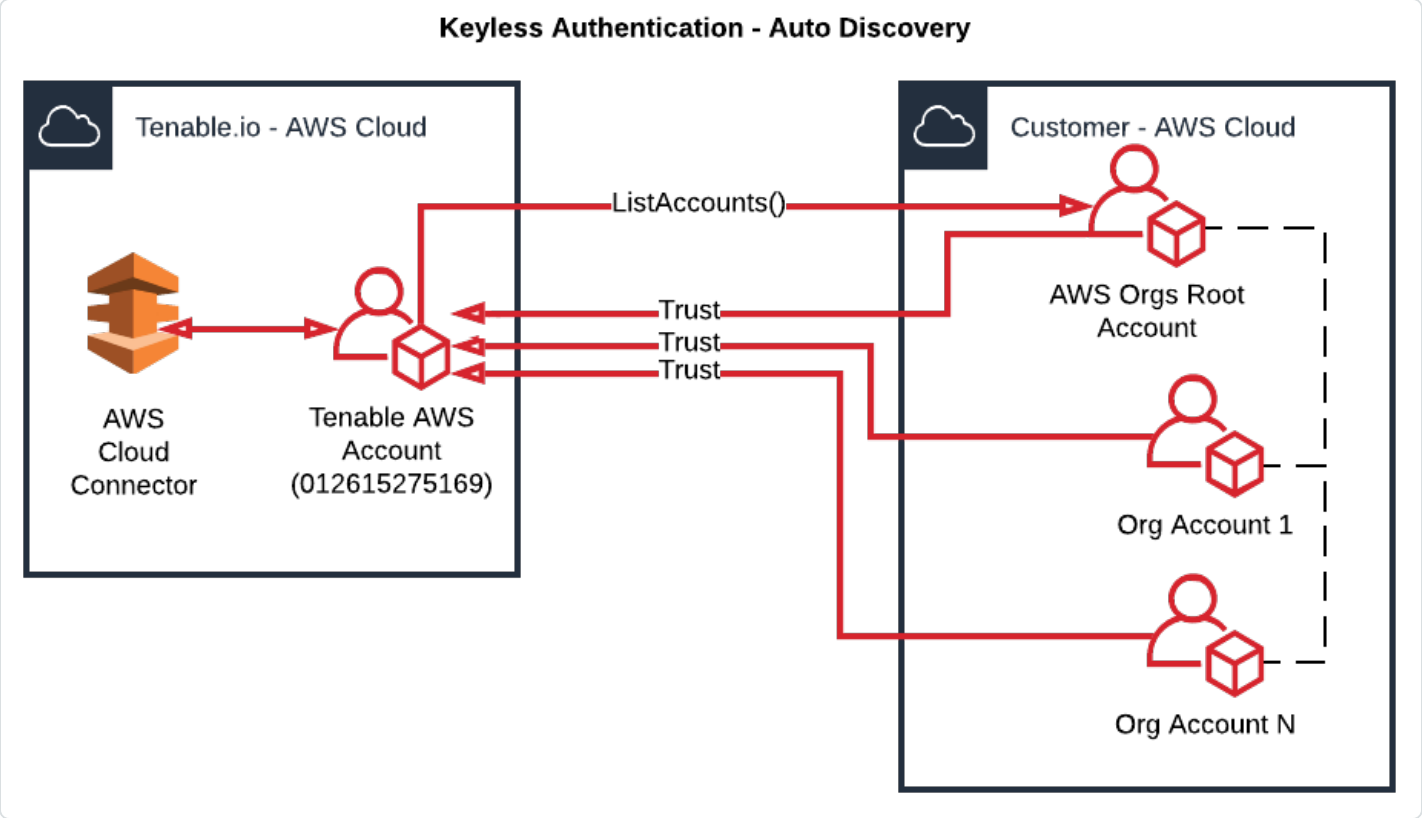
You can create an AWS connector to discover AWS assets and import them to Tenable Vulnerability Management. Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities.

Keyless Authentication

Tenable Vulnerability Management AWS connectors support keyless authentication via AWS role delegation. Keyless authentication via AWS role delegation allows the automatic discovery of your AWS assets. To use keyless authentication, you must establish a trust relationship between your AWS accounts and the Tenable AWS account. In this scenario, your AWS accounts communicate with a trusted Tenable AWS account that communicates with your AWS connector.

Automatic Discovery of AWS Accounts

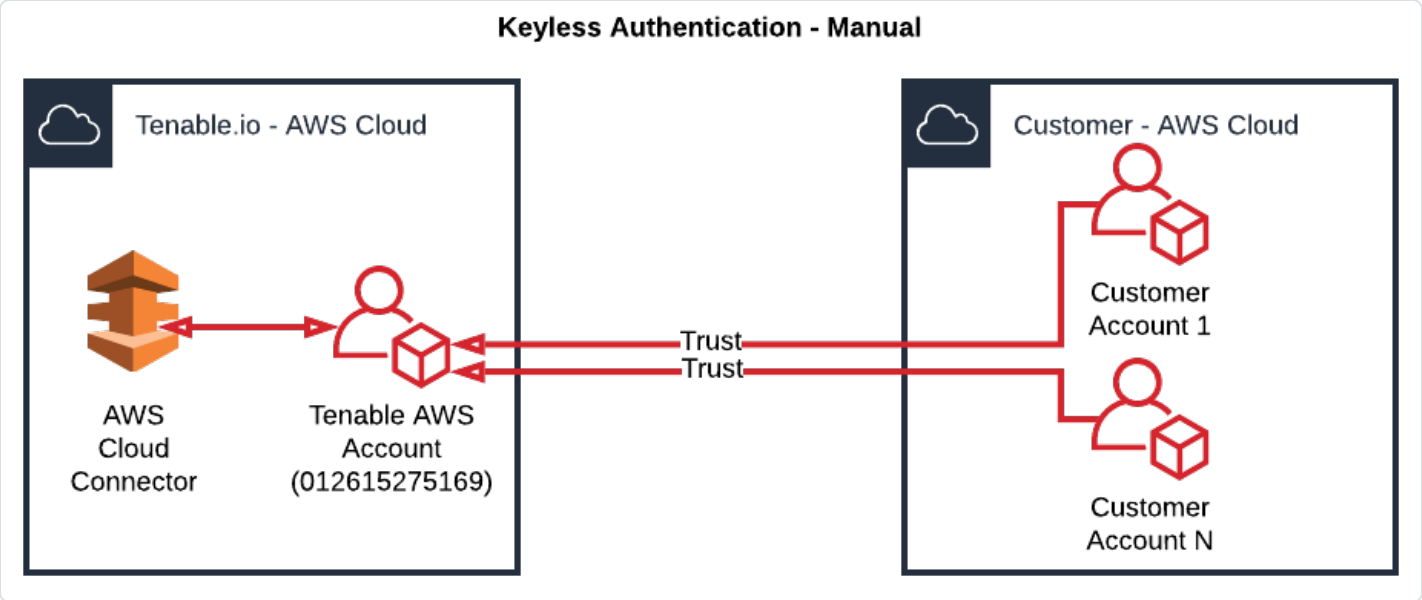
If you want to allow the Tenable AWS Account to automatically find other AWS accounts in your organization, use keyless authentication with auto account discovery. You must enable AWS Organizations and assign a `ListAccounts` policy, which then discovers other AWS accounts and establishes trust relationships as shown in the following diagram.



For more information about setting up AWS Organizations, see the AWS documentation.

Manual Linking of AWS Accounts

If you do not want to use auto account discovery or if you are not using AWS Organizations, you can manually configure linked AWS accounts, as shown in the following diagram.



To configure and create an AWS connector with keyless authentication:

1. Configure AWS for Keyless Authentication (Discovery Only)
2. Create an AWS Connector with Keyless Authentication (Discovery Only)

Configure AWS for Keyless Authentication (Discovery Only)

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

Before you create a discovery-only connector with keyless authentication, you must first configure AWS. For more information on linking AWS accounts and establishing trust relationships, see AWS Connector with Keyless Authentication (Discovery Only)

Before you begin:

1. On your AWS account, enable CloudTrail.
2. Create a trail if one does not already exist.
3. In the trail, turn on **All** or **Write Only** Management Events, as well as logging.

   Note: When an AWS connector is used to import assets, Tenable queries all the CloudTrails for that connector and determine the set of all regions that those CloudTrails receive events for. That set of regions is then used when making calls to the EC2 and CloudTrail APIs.

To manually configure AWS for a discovery-only connector with keyless authentication:

1. Obtain your Tenable Vulnerability Management container ID, as described in License Information.
2. In your AWS account, create a role named *tenableio-connector* to delegate permissions to an IAM user:

   Tip: For more information, see the Amazon AWS documentation.

   a. In the navigation pane of the AWS console, click **Roles** > **Create role**.

   b. For role type, click **Another AWS account**.

   c. For **Account ID**, type the ID `012615275169`.

      Note: `012615275169` is the account ID of the Tenable AWS account that you will be establishing a trust relationship with to support AWS role delegation.

d. Select the **Require external ID** check box, and type the Tenable Vulnerability Management container ID that you obtained in step 1.

e. Click **Next: Add Permissions**.

f. Create or reuse a policy with the following permissions:

AWS Service	Permission
Amazon EC2	• DescribeInstances
AWS CloudTrail	• DescribeTrails • GetEventSelectors • GetTrailStatus • ListTags • LookupEvents
AWS Organizations	• ListAccounts **Note:** The `ListAccounts` permission is required for Tenable Vulnerability Management to automatically discover AWS accounts. If you do not use auto account discovery, you do not need this permission.

Note: Tenable recommends that you set **Amazon Resource Name** to * (all resources) for each AWS Service.

   a. Click **Next: Tags**.

   b. (Optional) Add any desired tags.

   c. Create **Policy**.

g. Click **Next: Review**.

h. In the **Role name** box, type *tenableio-connector*.

Caution: The role must be named *tenableio-connector* for the connector to work.

i. Review the role, ensuring that the role name is *tenableio-connector*, and then click **Create role**.

j. Viewing the new *tenableio-connector* role, click the **Trust Relationship** tab.

k. Click **Edit Trust Relationship**.

   The policy document appears in a text box.

l. At the **AWS** line of the text box, replace `arn:aws:iam::012615275169:root` with `arn:aws:iam::012615275169:role/keyless_connector_role`.

m. Click **Update Trust Policy**.

What to do next:

- Create an AWS Connector with Keyless Authentication (Discovery Only)

Create an AWS Connector with Keyless Authentication (Discovery Only)

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

> **Required User Role:** Administrator

You can create an AWS connector to discover AWS assets and import them to Tenable Vulnerability Management. Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities.

Before you begin:

- Configure AWS for Keyless Authentication (Discovery Only)

To create an AWS connector with keyless authentication for discovery only:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

3. In the upper-right corner of the page, click the **Create Cloud Connector** button.

   The cloud connector selection plane appears.

4. In the **Cloud Connectors** section, click **Amazon Web Services**.

   The connector creation plane appears.

5. In the **Connector Name** box, type a name to identify the connector.

6. In the **Account ID** box, type your primary AWS account ID.

7. (Optional) Click **Create Stack** to deploy a Cloud Formation Template (CFT) to your AWS account.

> **Note:** For discovery-only connectors, skip the stack creation steps in the user interface only if you have manually configured *tenableio-connector* role in your AWS account. The stack configures parameters, policies, and roles required for using the Tenable Vulnerability Management connector.

8. (Optional) To expand more cloud connector settings, click **Cloud Connector Advanced Settings**.

    a. (Optional) Use the **Auto Account Discovery** toggle to enable or disable automatic discovery of linked accounts and CloudTrails.

    > **Note**: Make sure that you create a *tenableio-connector* role either manually or via CFT for each linked account.

    b. (Optional) If you disabled **Auto Account Discovery**, do any of the following:

    - To manually add AWS accounts, next to **Accounts for Cloud Assessment**, click ⊕.
    - To manually add AWS CloudTrails, next to **AWS CloudTrails for Cloud Assessment**, click ⊕.

    c. (Optional) In the **Select or Create Network** drop-down box, select an existing network to which the connector should be added.

    When the connector discovers an asset, the associated network is added to the asset's details. For more information, see Networks.

    d. (Optional) Use the **Cloud Connector Schedule** toggle to enable or disable scheduled imports.

    By default, Tenable Vulnerability Management requests new and updated asset records every 1 day.

    If enabled:

    i. In the text box, type the frequency with which Tenable Vulnerability Management sends data requests to the AWS server.

ii. In the drop-down box select **Minutes**, **Hours**, or **Days**.

> **Note**: When you schedule a connector configuration to sync every 30 minutes, a discovery job is placed in a queue every 30 minutes. The results of the discovery job become available in the Tenable Vulnerability Management interface and logs depending on the workload for the connector services. So, the results of the discovery job can take more than 30 minutes depending on the queue.

9. Do one of the following:

   - To save the connector, click **Save**.
   - To save the connector and import your assets from AWS, click **Save & Import**.

   Tenable Vulnerability Management imports your assets from AWS. There may be a short delay before your assets appear.

What to do next:

- View assets to see assets that were discovered by the connector.

AWS Connector with Key-based Authentication

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

The Amazon Web Services (AWS) Connector provides real-time visibility and inventory of EC2 assets in AWS accounts.

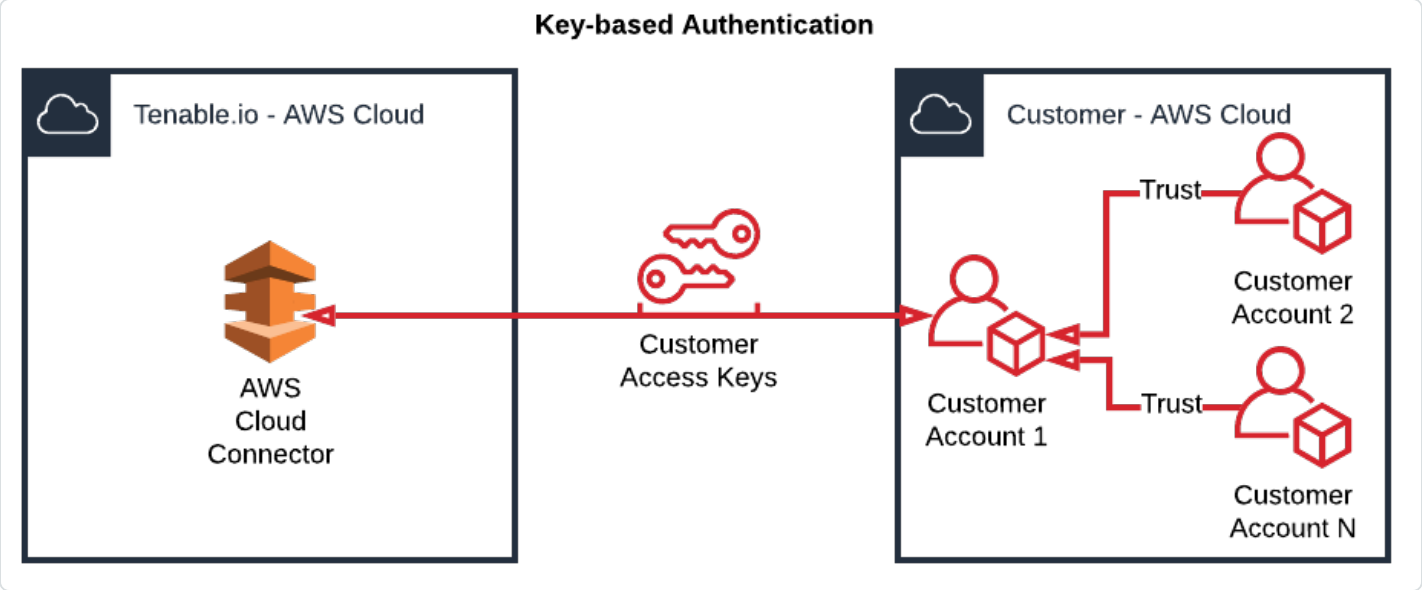
You can create an AWS connector to discover AWS assets and import them to Tenable Vulnerability Management. Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities.

Key-based Authentication

Tenable Vulnerability Management AWS connectors support key-based authentication that uses an IAM user with permissions and a secret key and access key. In this scenario, the Tenable Vulnerability Management AWS connector authenticates with your primary AWS account via a secret key and an access key. Additionally, you can manually configure secondary linked AWS accounts with trust relationships to your primary AWS account., as shown in the diagram below.

For more information about other AWS authentication options, see Amazon Web Services Connector.

Note: AWS connectors configured with key-based authentication do not support the automatic discovery of AWS accounts. Additionally, key-based authentication is not recommended.



To fully configure AWS key-based authentication with Tenable Vulnerability Management:

1. In AWS, configure your primary AWS account to support key-based authentication for your connectors, as described in Configure AWS for Key-based Authentication.
2. (Optional) In AWS, manually configure linked AWS accounts, as described in Configure Linked AWS Accounts (Key-based).
3. In Tenable Vulnerability Management, create your AWS connector, as described in Create an AWS Connector with Key-based Authentication.

Configure AWS for Key-based Authentication

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

Before you begin:

- Enable CloudTrail and create a trail if one does not already exist.

  Note: You must turn on **All** or **Write Only** Management Events, as well as logging for the trail.

To configure AWS to support Tenable Vulnerability Management connectors via an IAM user with permissions (key-based authentication):

1. Use the Policy Generator to create an IAM permission policy for integration with Tenable Vulnerability Management.
2. Add the following permissions to the policy:

AWS Service	Permission
EC2	• DescribeInstances
CloudTrail	• DescribeTrails • GetEventSelectors • GetTrailStatus • ListTags • LookupEvents

   Tenable recommends that you set **Amazon Resource Name** to * (all resources) for each AWS Service.
3. Create an IAM user with programmatic access.
4. Assign the policy you created in Step 2 to the IAM user.
5. Obtain Access and Secret keys.

(Optional) To configure linked AWS accounts:

- Link AWS Accounts

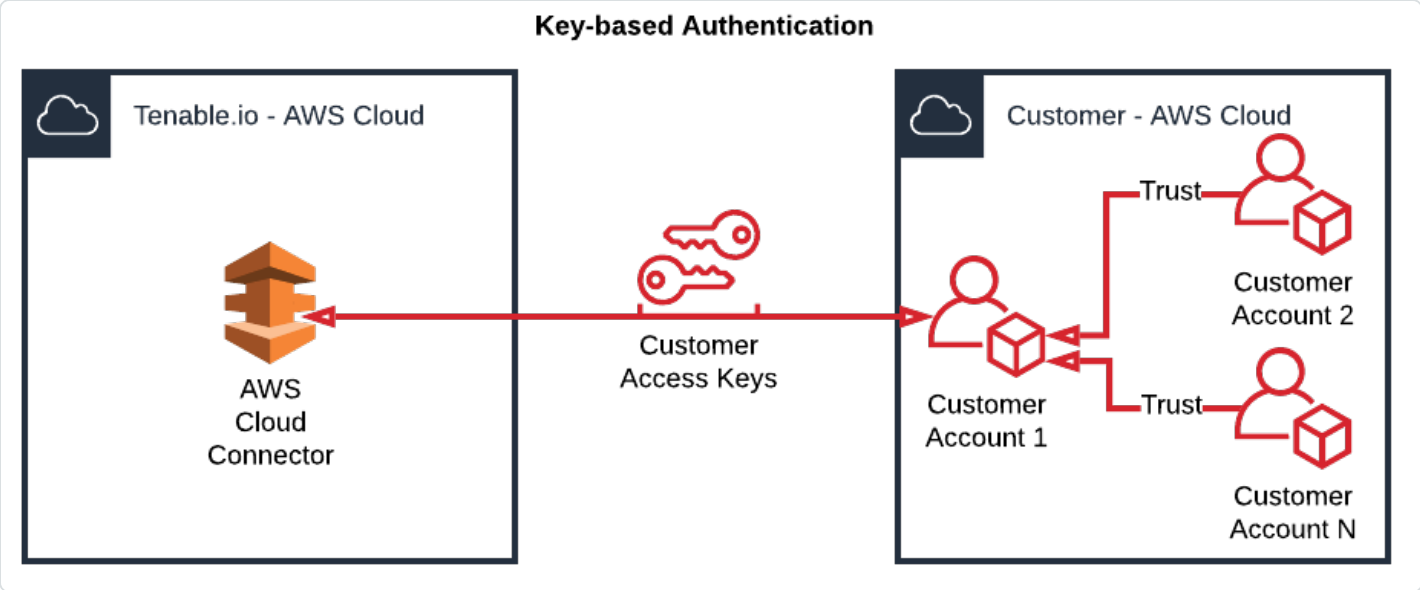
What to do next:

- Create an AWS connector with Keyed Authentication.

Configure Linked AWS Accounts for Key-based Authentication

Required User Role: Administrator

This section assumes that access keys have already been generated for the primary account, and explains how to configure linked AWS accounts as depicted in the diagram below.



Before you begin:

- Configure the primary AWS account.
- Record the Account ID for the primary AWS account.

To configure linked AWS accounts:

1. Obtain your Tenable Vulnerability Management container ID, as described in License Information.
2. In your AWS account, create a role named **tenableio-connector** to delegate permissions to an IAM user, as described in the Amazon AWS documentation.
    a. In the navigation pane of the console, click **Roles > Create role**.
    b. For role type, click **Another AWS account**.
    c. For **Account ID**, type the AWS account ID of the primary AWS account.

d. Select the **Require external ID** check box, and type the Tenable container ID that you obtained in Step 1.

e. Click **Next: Permissions**.

f. Create or reuse a policy with the following permissions:

AWS Service	Permission
Amazon EC2	• DescribeInstances
AWS CloudTrail	• DescribeTrails • GetEventSelectors • GetTrailStatus • ListTags • LookupEvents

Tenable recommends that you set **Amazon Resource Name** to * (all resources) for each AWS Service.

g. Click **Next: Tagging**.

h. (Optional) Add any desired tags.

i. Click **Next: Review**.

j. In the **Role name** box, type **tenableio-connector**.

Caution: The role *must* be named **tenableio-connector** for the connector to work.

k. Review the role, ensuring that the role name is **tenableio-connector**, and then click **Create role**.

l. Record the **Role ARN** for the created role. You need the Role ARN for the next section of the configuration.

To configure the primary AWS account:

Note: For more detailed steps, see the Amazon documentation: Accessing and Administering the Member Accounts in Your Organization.

1. Create a policy that has permission to use the AWS Security Token Service (AWS STS) AssumeRole API (*sts:AssumeRole*) action.
    a. Navigate to **Policies** and then click **Create Policy**.
    b. For **Service**, choose **STS**.
    c. For **Actions**, type **`AssumeRole`** in the **Filter** box and then select the check box next to it when it appears.
    d. Click **You chose actions that require the role resource type**.
    e. Click **Add ARN**.
    f. In the **Specify ARN for role** field, paste the ARN recorded for the role created in the linked account(s).
    g. Click **Add**.
    h. Click **Review policy**.
    i. In the **Name** field, type a unique name for your policy.
    j. Click **Create Policy**.
2. Add the policy created in step 1 to a user or group associated with the access keys used when you created your connector.
    a. Click the **Add Permissions** button.
    b. Select the **Attach existing policies directly** check box.
    c. Find the policy with `sts:AssumeRole` that was created in step 1.
    d. Click **Next: Review**.
    e. Click **Add permissions**.

Create an AWS Connector with Key-based Authentication

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

Before you begin:

- Complete the required AWS configuration steps for key-based authentication.

To create an AWS connector:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

3. In the upper-right corner of the page, click the **Create Cloud Connector** button.

   The cloud connector selection plane appears.

4. In the **Cloud Connectors** section, click **AWS - Keyed setup**.

   The cloud connector creation plane appears.

5. In the **Connector Name** box, type a name to identify the connector.

6. In the **Access Key** box, type the access key that you obtained when configuring AWS.

7. In the **Secret Key** box, type the secret key that corresponds to the access key you used.

8. In the **Select or Create Network** drop-down box, select an existing network for your connector or click the ⊕ button to create a new network.

   Note: Networks help to avoid IP address collisions between cloud assets and Nessus-discovered assets. Tenable recommends creating a network for each connector type in use to prevent asset records in different cloud environments from overwriting each other. For more information about the network feature, see Networks.

9. Use the **Cloud Connector Schedule** toggle to enable or disable scheduled imports.

   > **Note:** By default, Tenable Vulnerability Management requests new and updated asset records every 1 hour.

   If enabled:

   - In the **Import** text box, type the frequency with which Tenable Vulnerability Management sends data requests to the AWS server.
   - In the drop-down box select *Minutes*, *Hours*, or *Days*.

     > **Note**: When you schedule a connector configuration to sync every 30 minutes, a discovery job is placed in a queue every 30 minutes. The results of the discovery job become available in the Tenable Vulnerability Management interface and logs depending on the workload for the connector services. So, the results of the discovery job can take more than 30 minutes depending on the queue.

10. Do one of the following:

    - To save the connector, click **Save**.
    - To save the connector and import your assets from AWS, click **Save & Import**.

    > **Note:** There may be a short delay before your assets appear in Tenable Vulnerability Management.

Microsoft Azure Connector

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

The Microsoft Azure Connector provides real-time visibility and inventory of assets in Microsoft Azure accounts.

To import and analyze information about assets in Microsoft Azure, you must configure Azure to support connectors and then create an Azure connector in Tenable Vulnerability Management.

> **Note:** If your Azure deployment includes Azure instances in the Azure China or Azure Government regions, Tenable Vulnerability Management cannot connect to those instances.

Alternatively, you can run a Nessus scanner or agent scan, both of which run plugins locally on the host.

Note: The Microsoft Azure Connector in Tenable Vulnerability Management does not support Virtual Machine Scale Sets (VMSS) hosts, which Tenable Cloud Security supports.

Goal	Connector Type
Discover Microsoft Azure assets The cloud connector discovers Azure assets without assessing them for vulnerabilities. Optionally, you can scan discovered assets later using a Nessus scanner or agent scan. This connector uses an Azure Application to collect information on Virtual Machines in the Azure subscription. To analyze assets via a Microsoft Azure connector: 1. Configure your Azure account to support your connectors, as described in Configure Microsoft Azure (Discovery Only). 2. Create your Azure connector, as described in Create a Microsoft Azure Connector.	Discovery Connector

Note: To manage existing Microsoft Azure connectors, see Manage Connectors. in the Tenable Vulnerability Management User Guide.

Tip: For common connector errors, see Connectors in the Tenable Developer Portal.

Configure Microsoft Azure (Discovery Only)

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Before you can use Tenable Vulnerability Management Azure connectors, you must perform several steps in Microsoft Azure.

Note: If your Azure deployment includes Azure instances in the Azure China or Azure Government regions, Tenable Vulnerability Management cannot connect to those instances.

To configure Microsoft Azure:

1. Create an Azure Application if one does not already exist.

   > **Note:** The Azure Application ID and Client Secret are obtained during this step.

2. Obtain the Azure Tenant ID (Directory ID).
3. Obtain the Azure Subscription ID.
4. Grant the Azure Application reader role permissions.
5. (Optional) Link Additional Azure Subscriptions to your Azure Application.

What to do next:

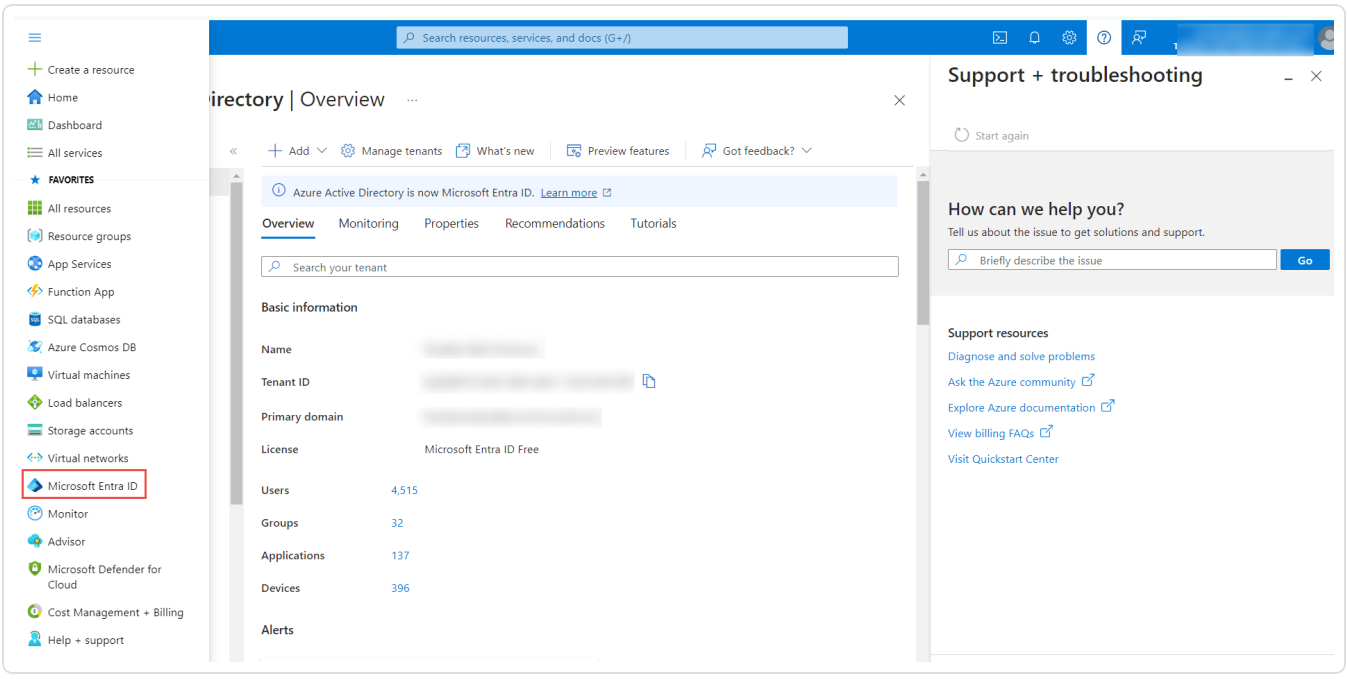
- Create an Azure connector.

Create Azure Application

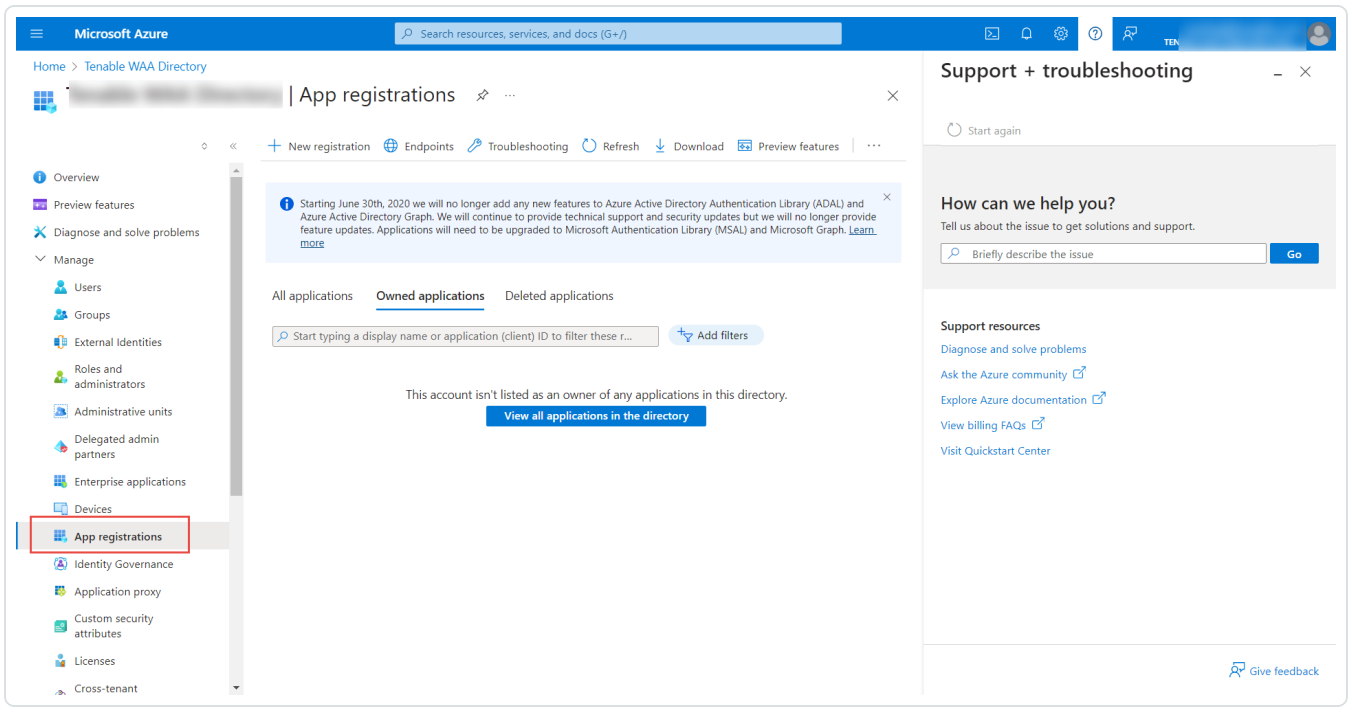
> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

To create an Azure Application for an Azure Tenable Vulnerability Management connector:

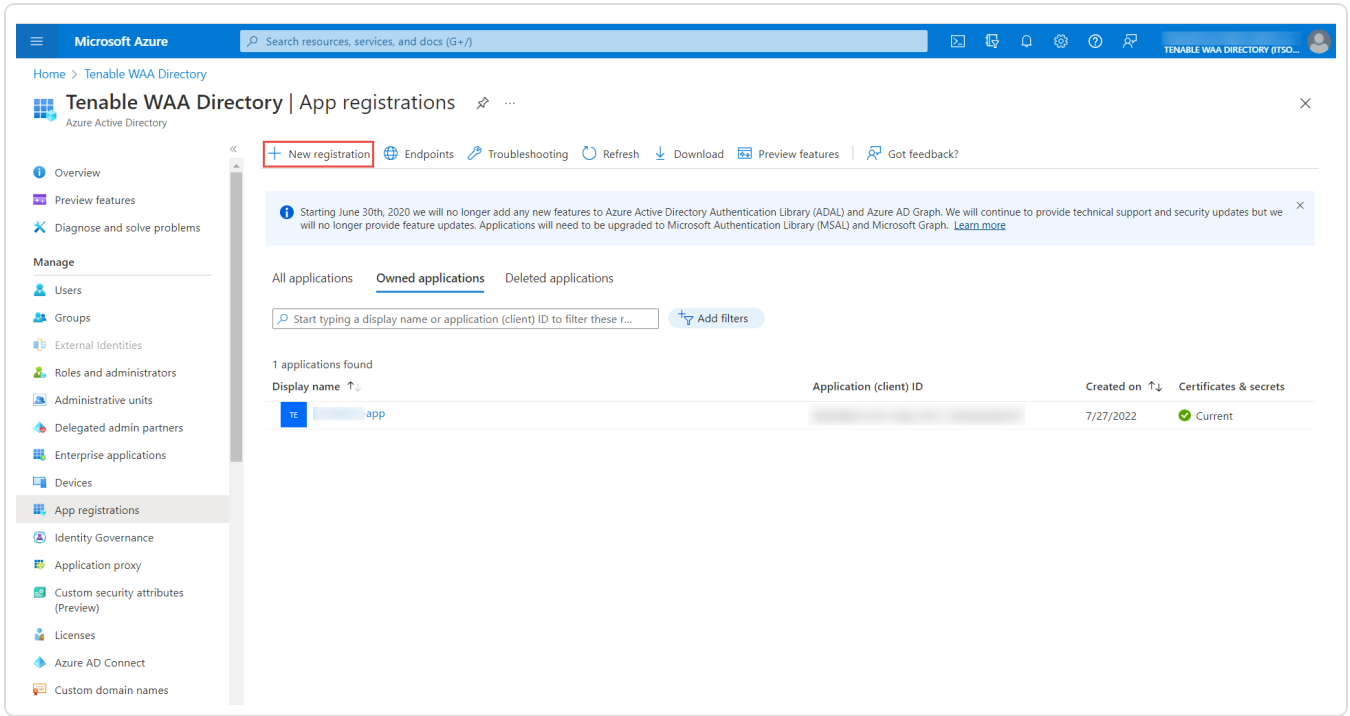
1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click **Microsoft Entra ID**.



3. Click **App registrations**.



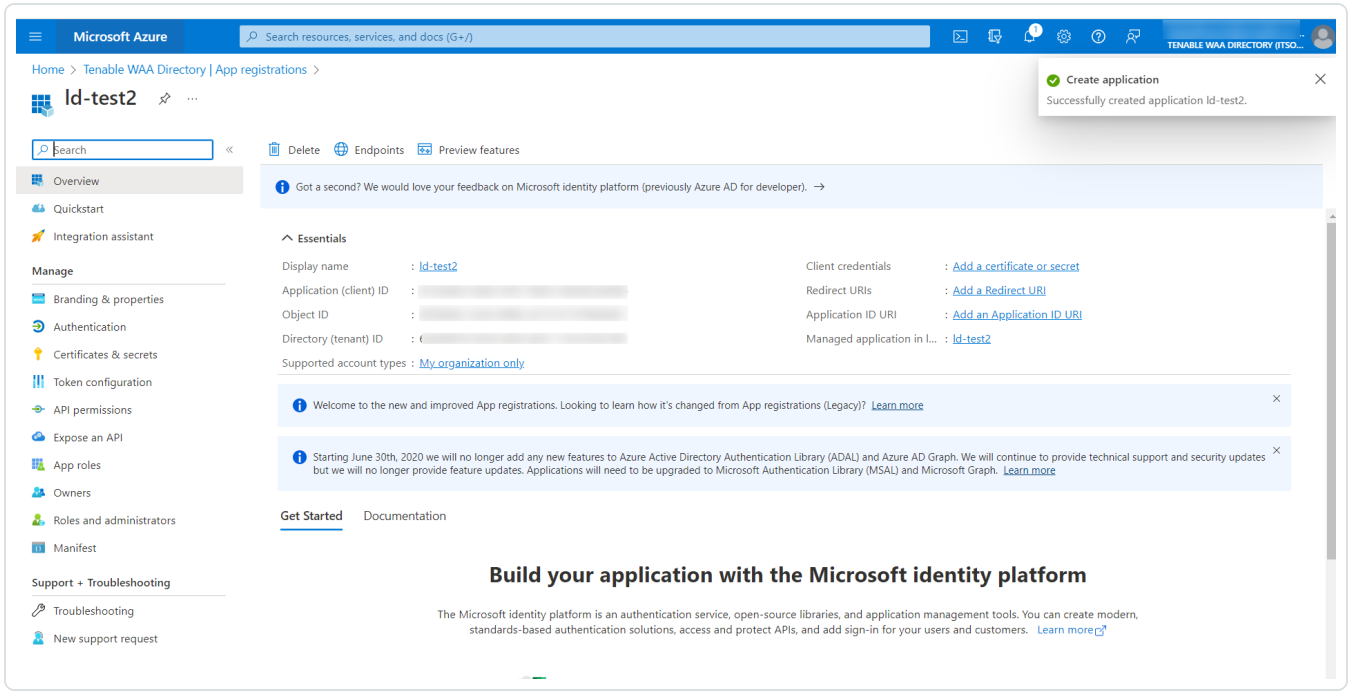
4. To add a new application, click **New registration**.



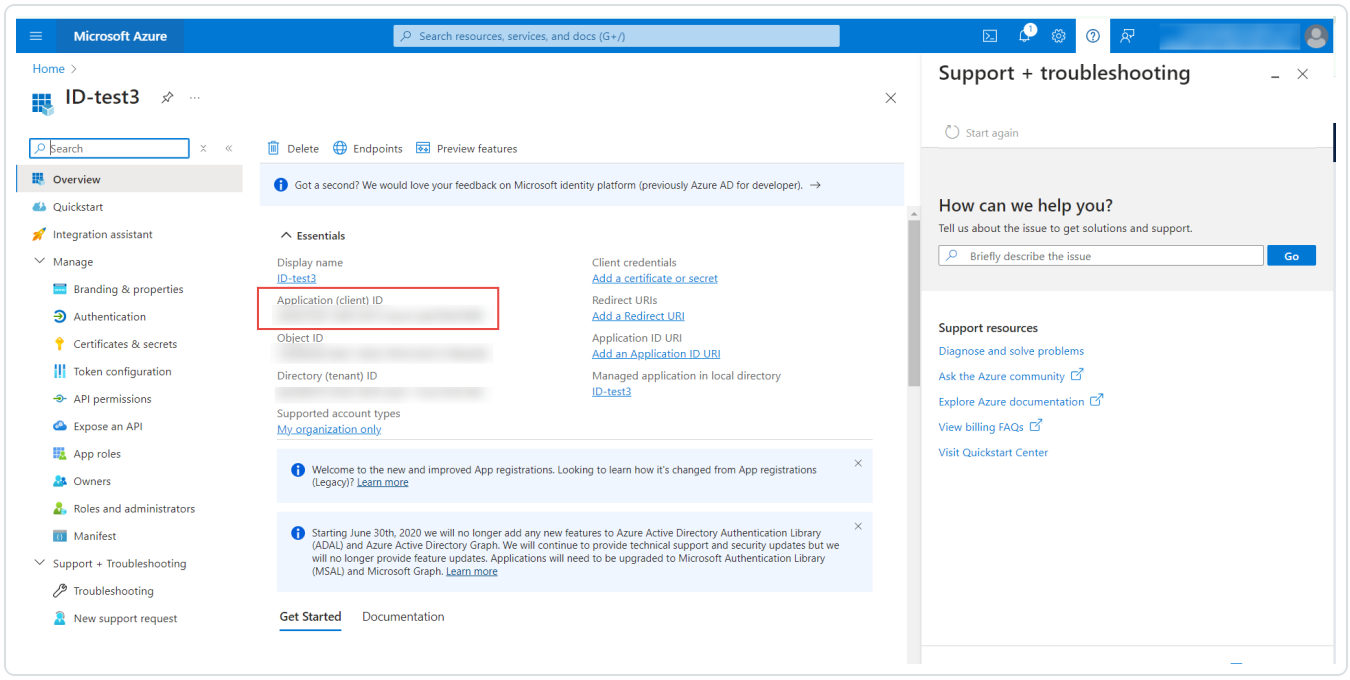
5. In the **Name** box, enter a descriptive name for the application.

6. In the **Supported Account types** section, choose one of the three options to specify the type of accounts that can access the API.
7. (Optional) In the **Redirect URI** section, select either **Web** or **Public client (mobile & desktop)** from the drop-down, and then enter the URI in the text box.
8. Click **Register** to finalize the settings and create the application.

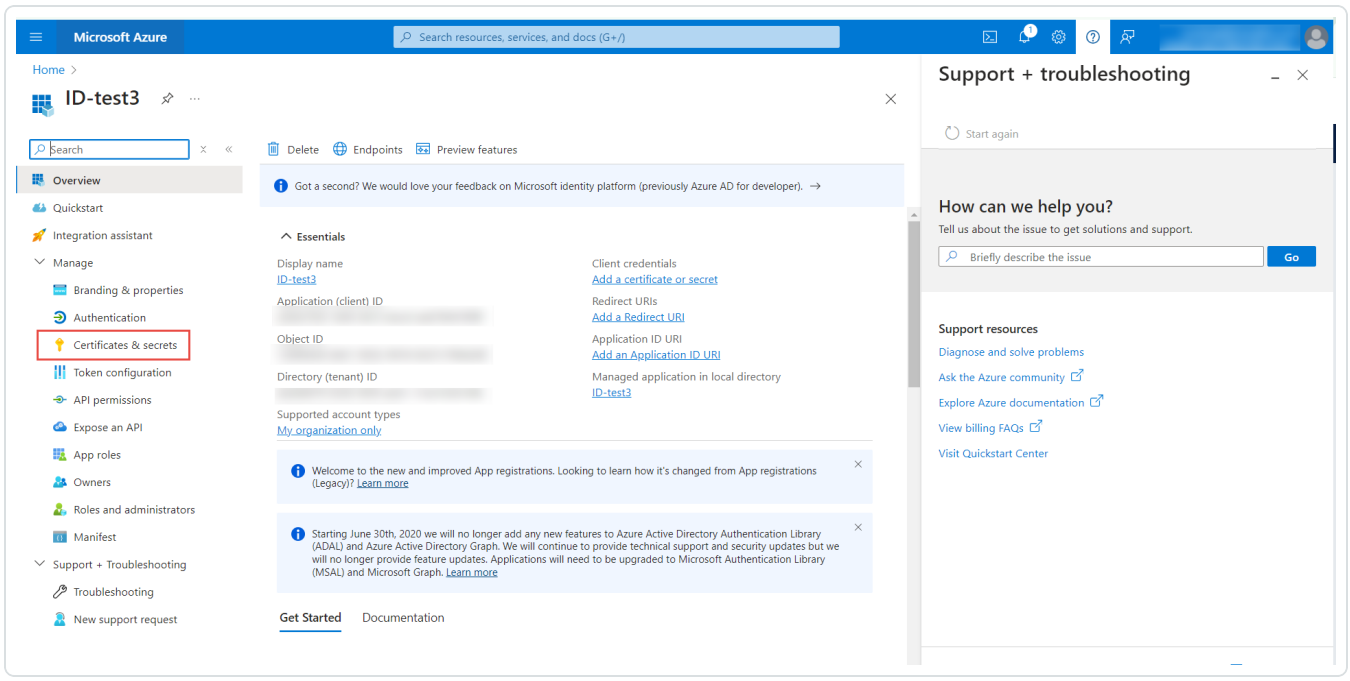
   A success message appears at the top of the page stating that the new application has been created, and the page is redirected to the **Overview page** for the application.



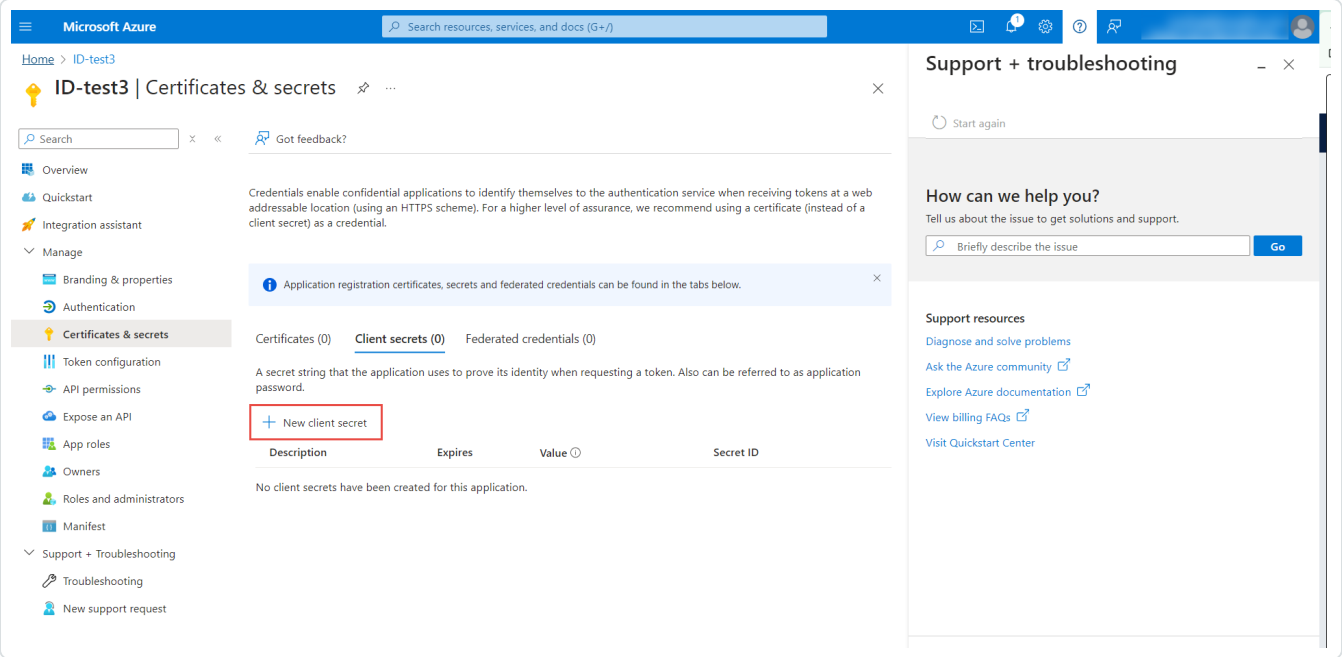
9. Copy the **Application (client) ID**. This information is used to configure a connector with Tenable Vulnerability Management.



10. In the **Manage** section for the application, click **Certificates & secrets**.

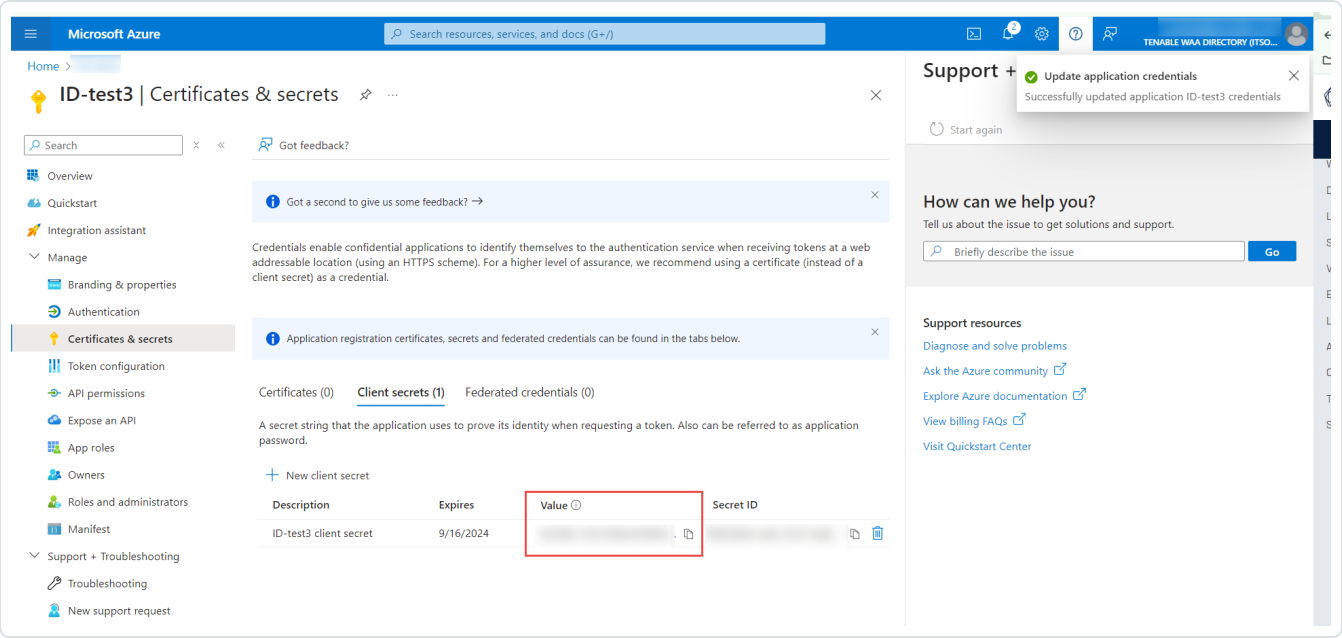


11. In the **Client Secrets** section, click **+ New client secret**.



12. In the **Description** box, type a description for the client secret.
13. For the **Expires** option, select an expiration date.
14. Click the **Add** button.

    The new client secret is added.
15. Copy or make a note of the client secret value.



Later, you will need this client secret to configure a connector with Tenable Vulnerability Management.

What to do next:

- Obtain the Azure Tenant ID (Directory ID)

Obtain Azure Tenant ID (Directory ID)

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

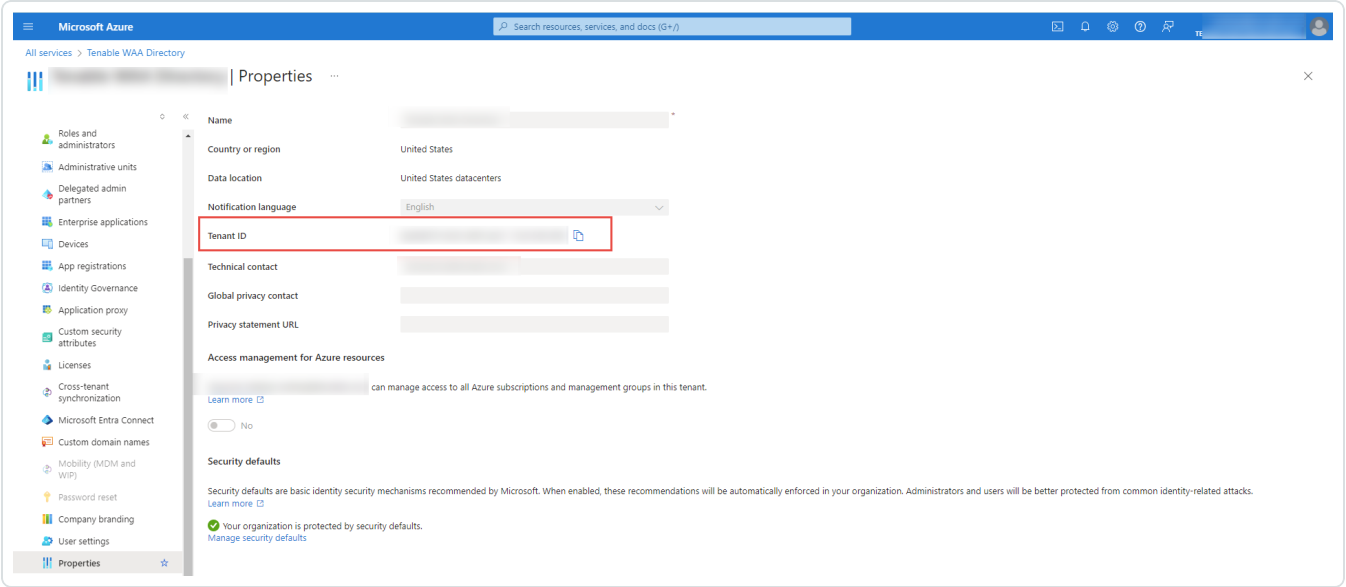
To obtain your Tenant ID for an Azure Tenable Vulnerability Management connector:

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click **Microsoft Entra ID**.

   The **Directory Overview** page appears.
3. In the **Manage** section, click **Properties**.

   The **Directory properties** page appears.
4. Copy the **Directory ID**.

> **Note:** The Tenant ID and Directory ID are the same.



What to do next:

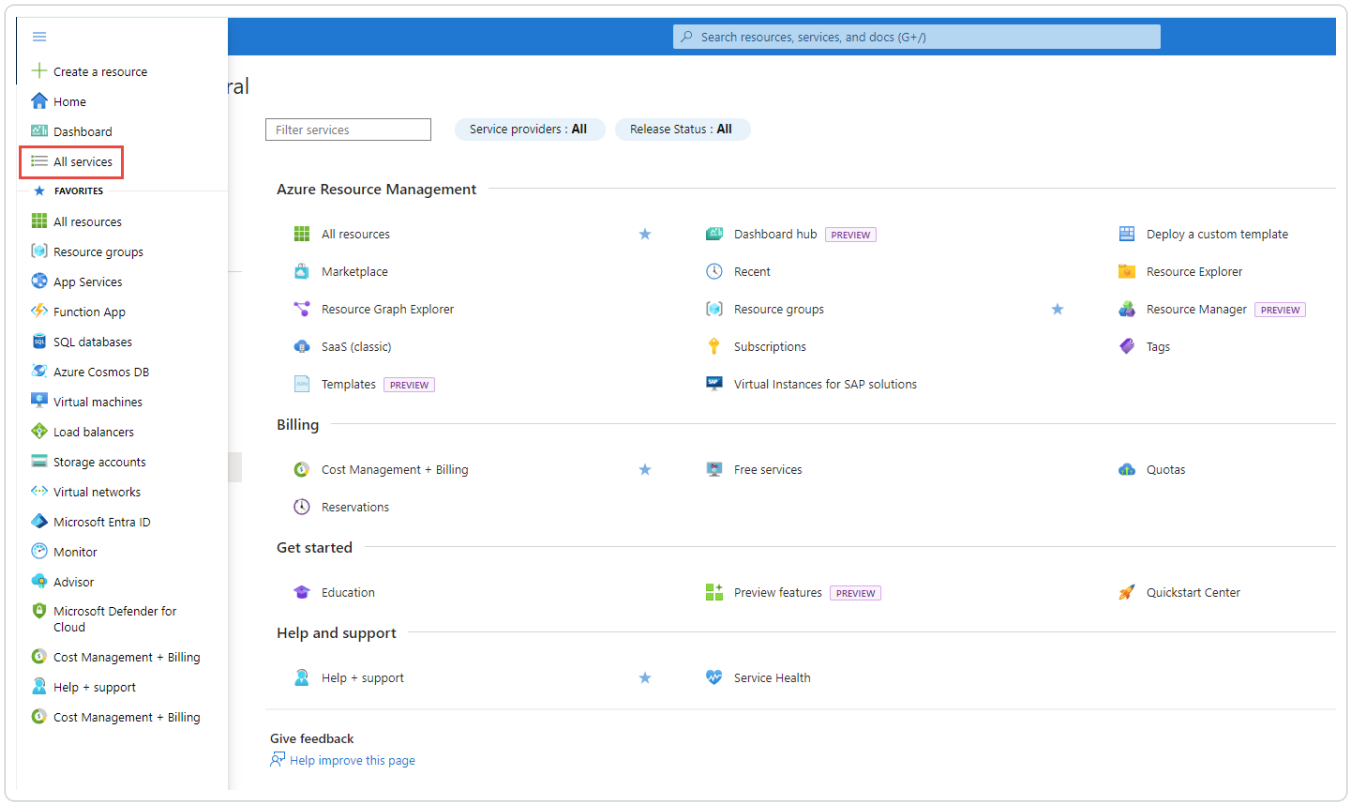
- Obtain the Azure Subscription ID.

Obtain Azure Subscription ID

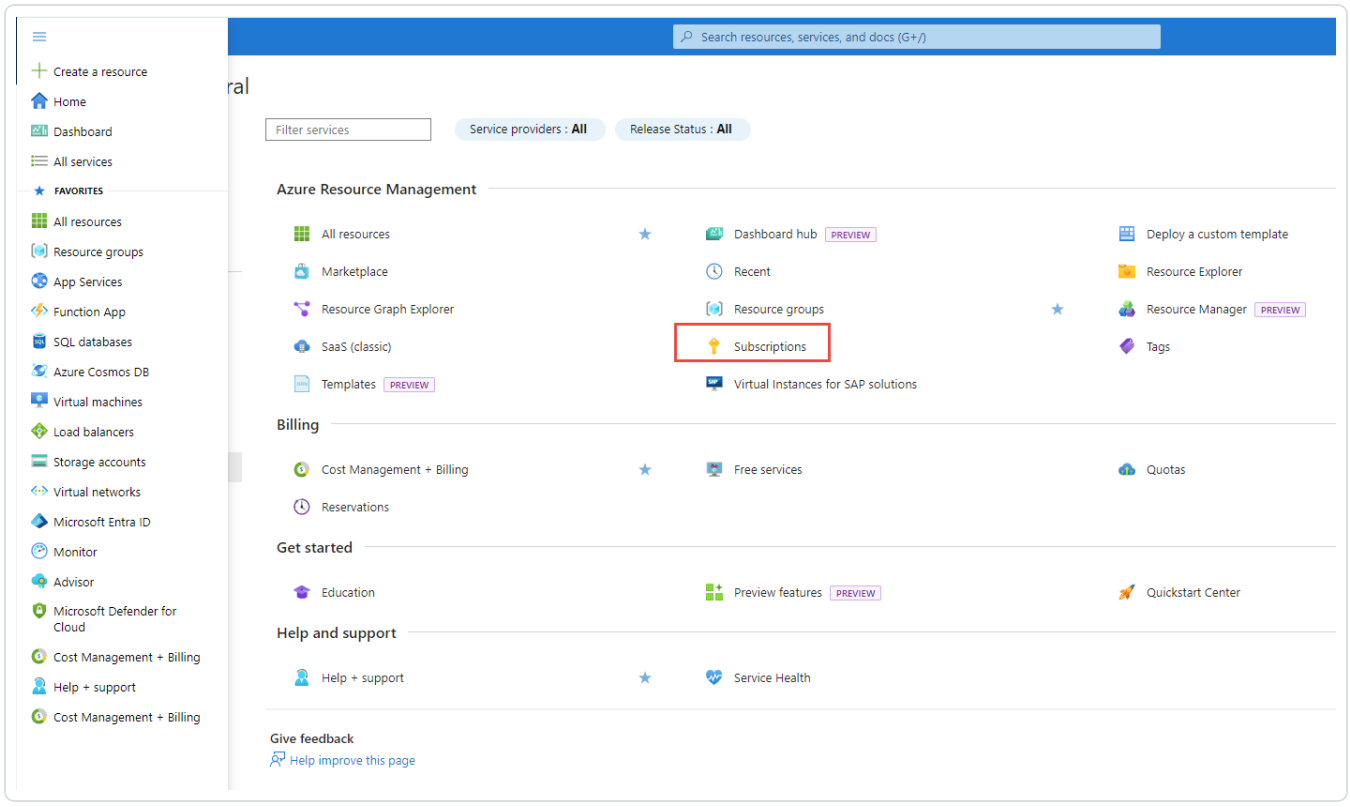
> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

To obtain your Subscription ID for an Azure Tenable Vulnerability Management connector:

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click **All Services**.



3. In the **General** section, click **Subscriptions**.



4. Copy the **Subscription ID** for the applicable subscription.

What to do next:

- Grant the Azure Application reader role permissions.

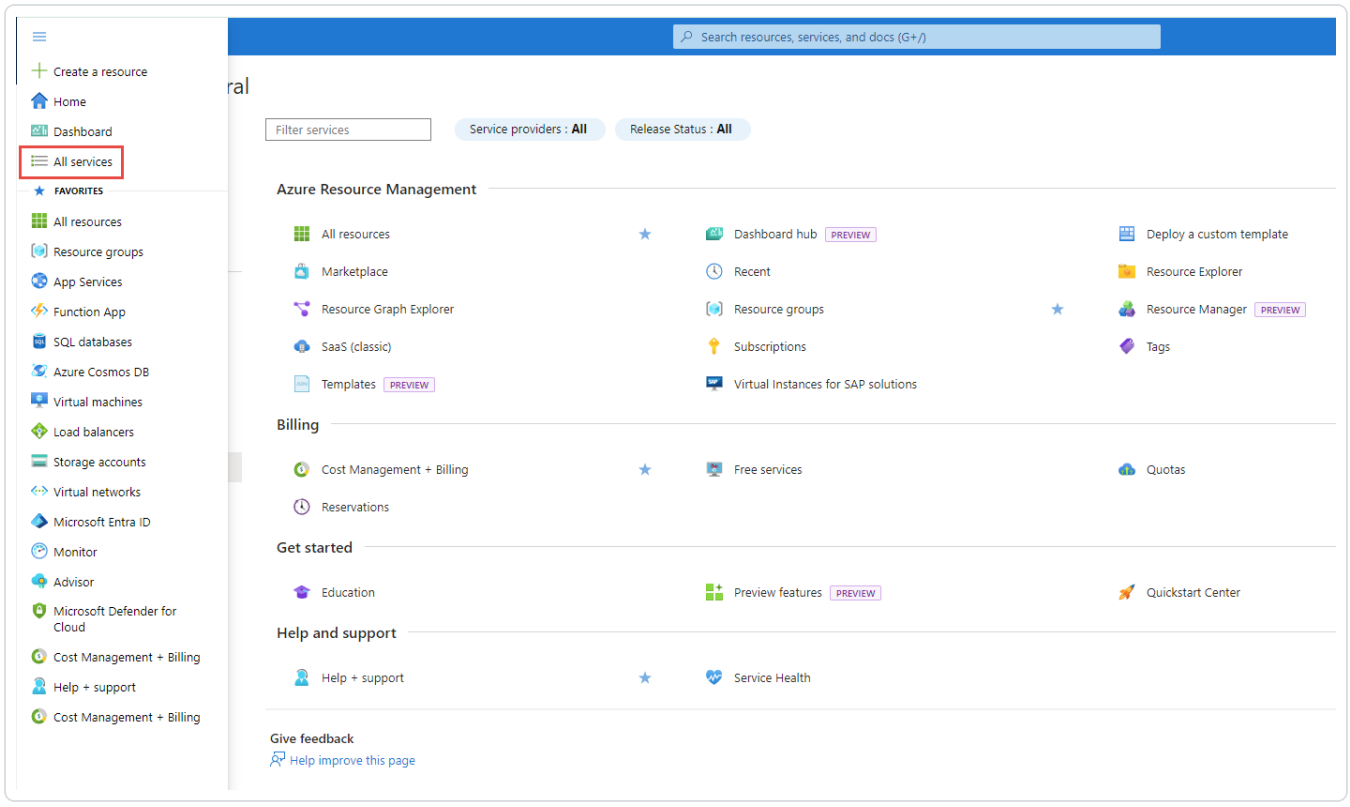
Grant the Azure Application Reader Role Permissions

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

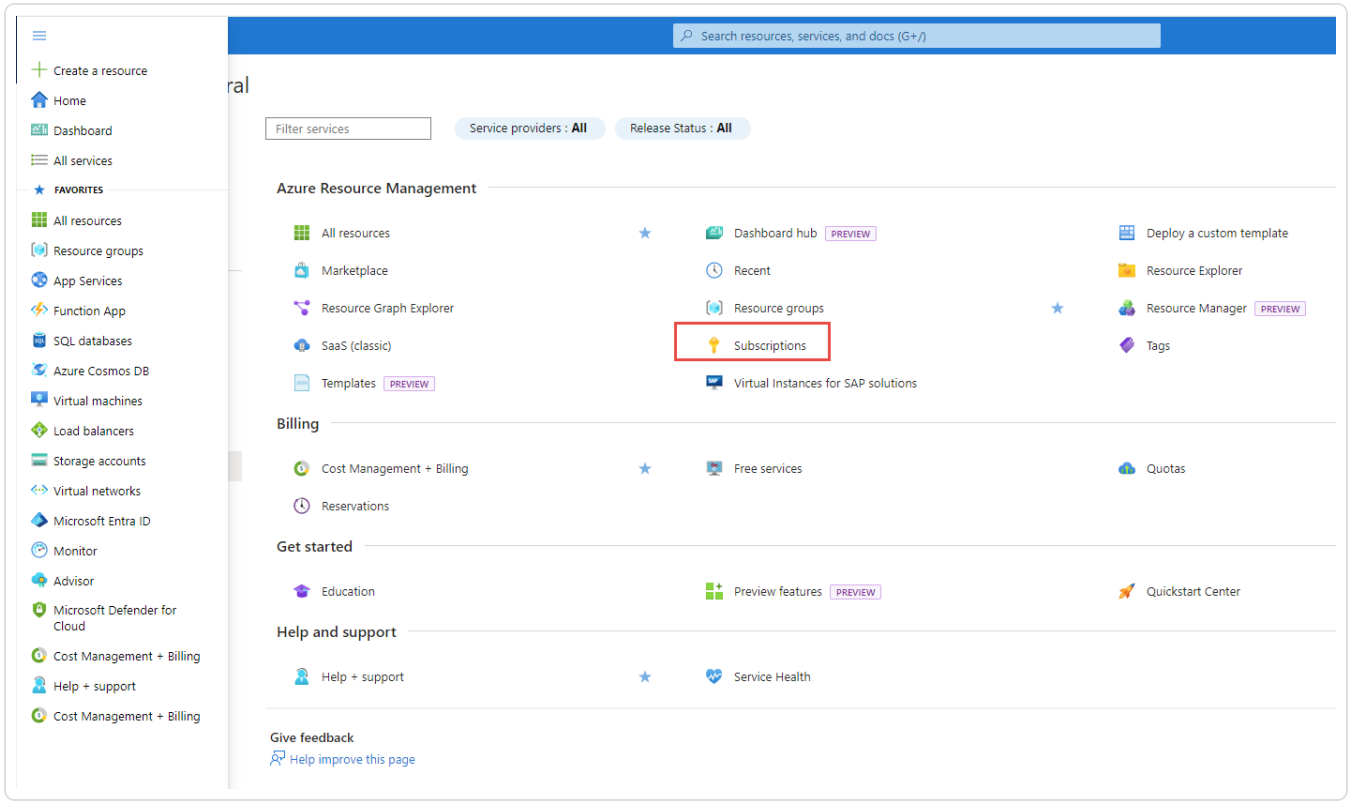
To grant an Azure application reader role permissions for an Azure Tenable Vulnerability Management connector:

> **Note:** For more information, see the Microsoft Azure documentation: Manage access to Azure resources using RBAC and the Azure portal.

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click **All Services**.



3. In the **General** section, click **Subscriptions**.



4. In the subscription table, click the applicable subscription.

   The **Overview** page for the subscription appears.

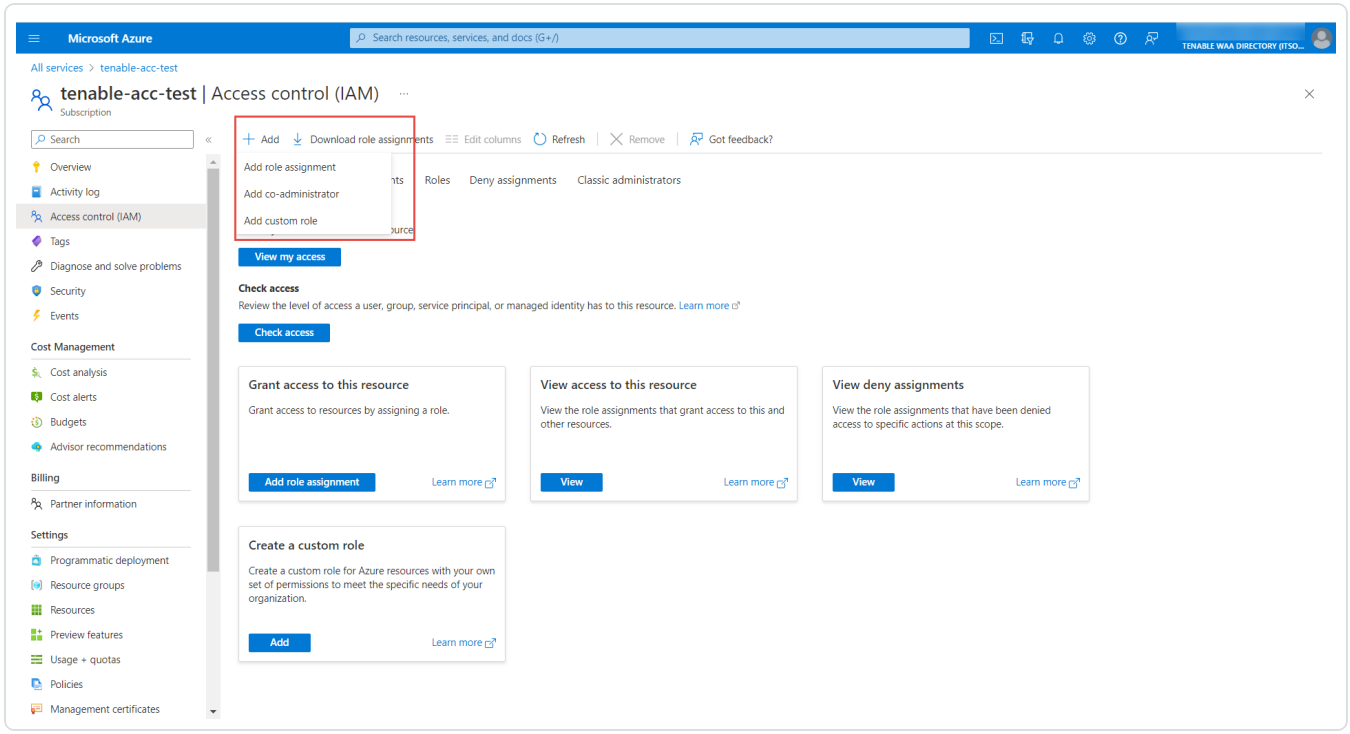
5. In the menu for the subscription, click **Access control (IAM)**.

   The **Access control (IAM)** page appears.

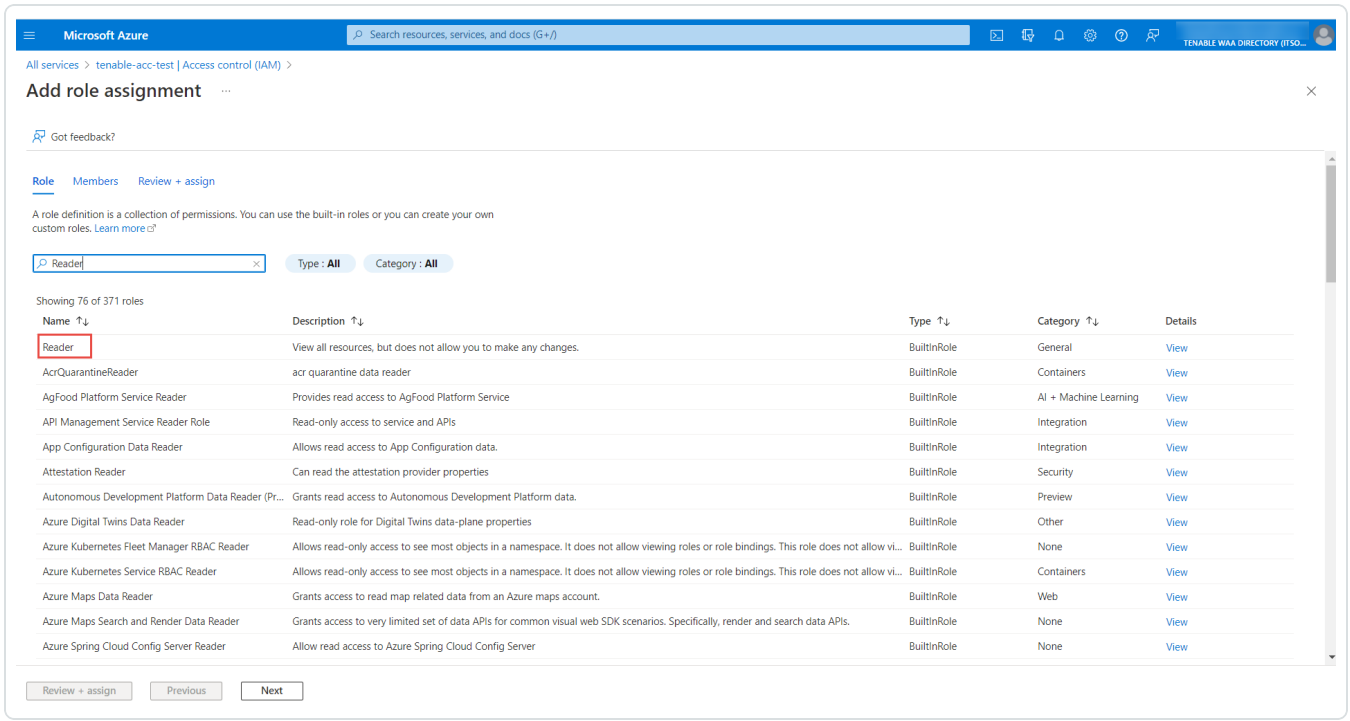
6. Click the **+Add** button.

   A pop-up menu appears.

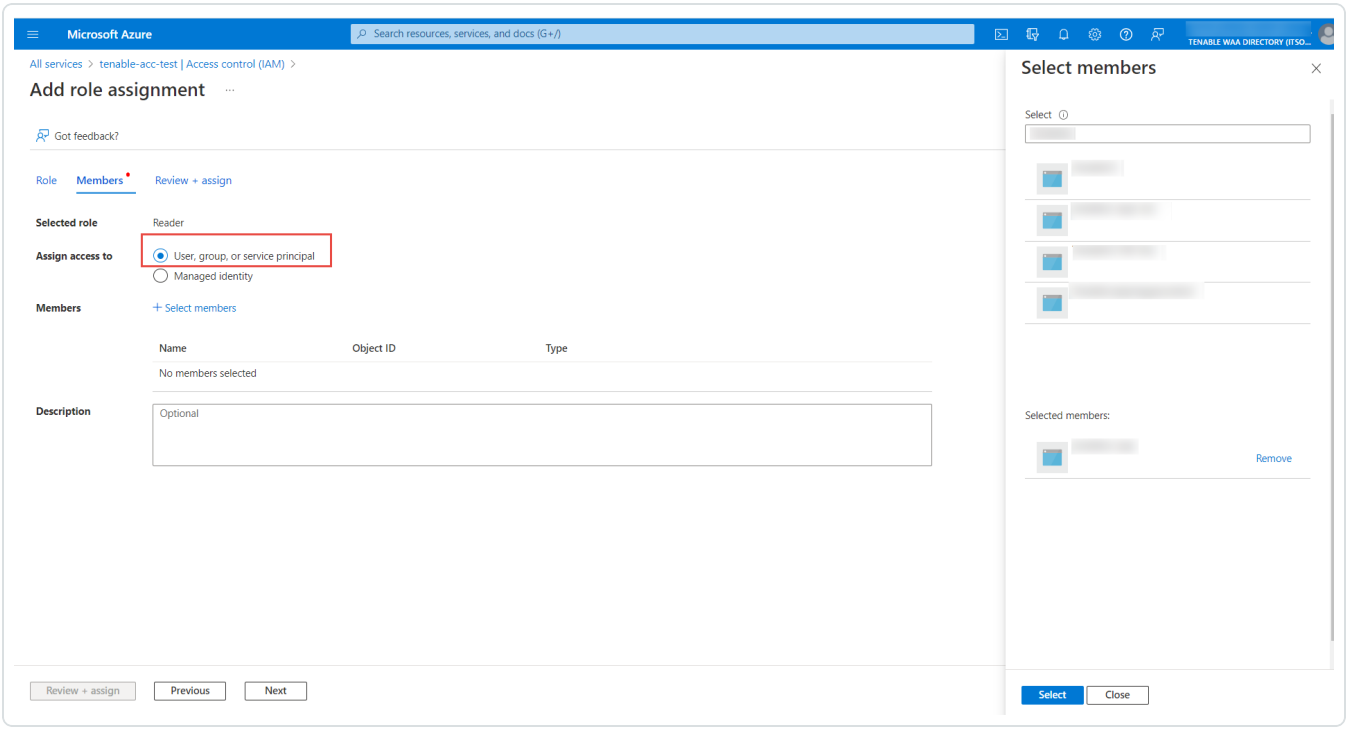
7. Click **Add role assignment**.



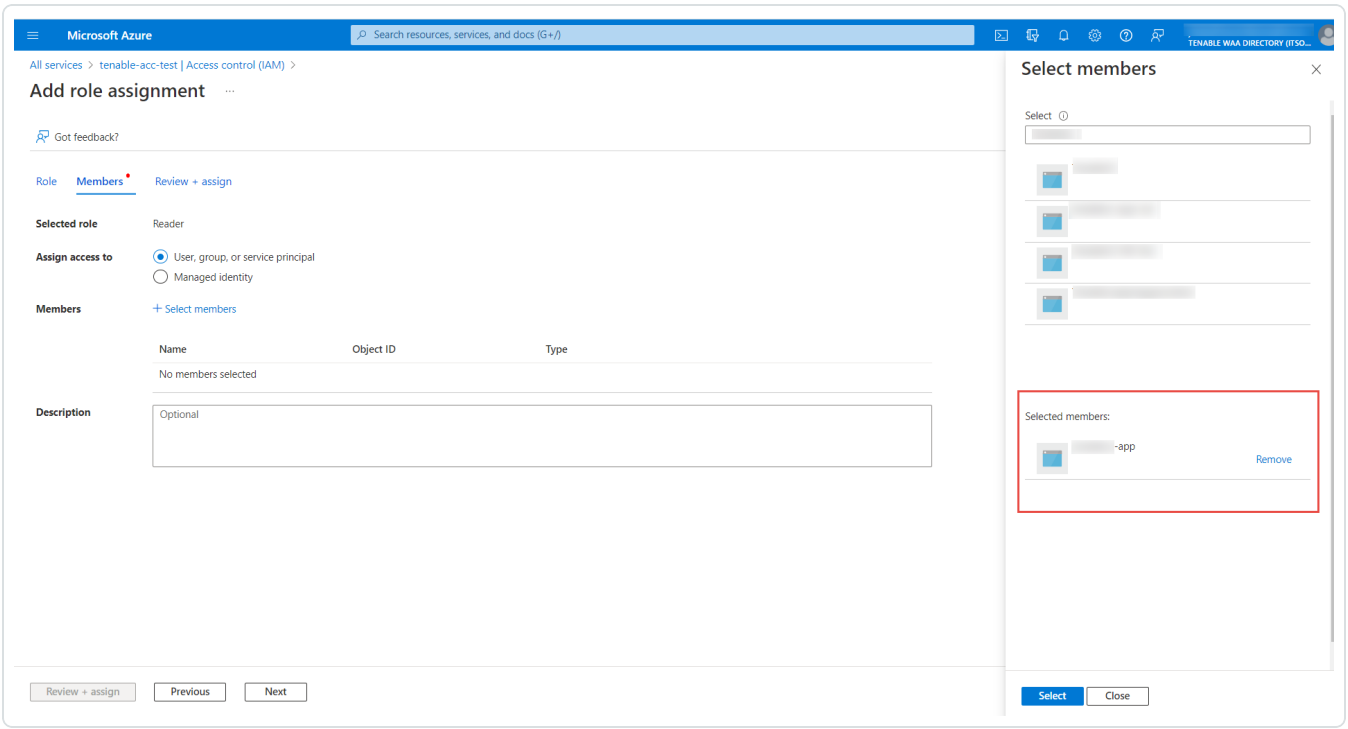
8. In the **Add role assignment** window, in the **Role** tab, search and select **Reader**.



9. In the **Members** tab, in the **Assign access to** section, select **User, group, or service principal**.

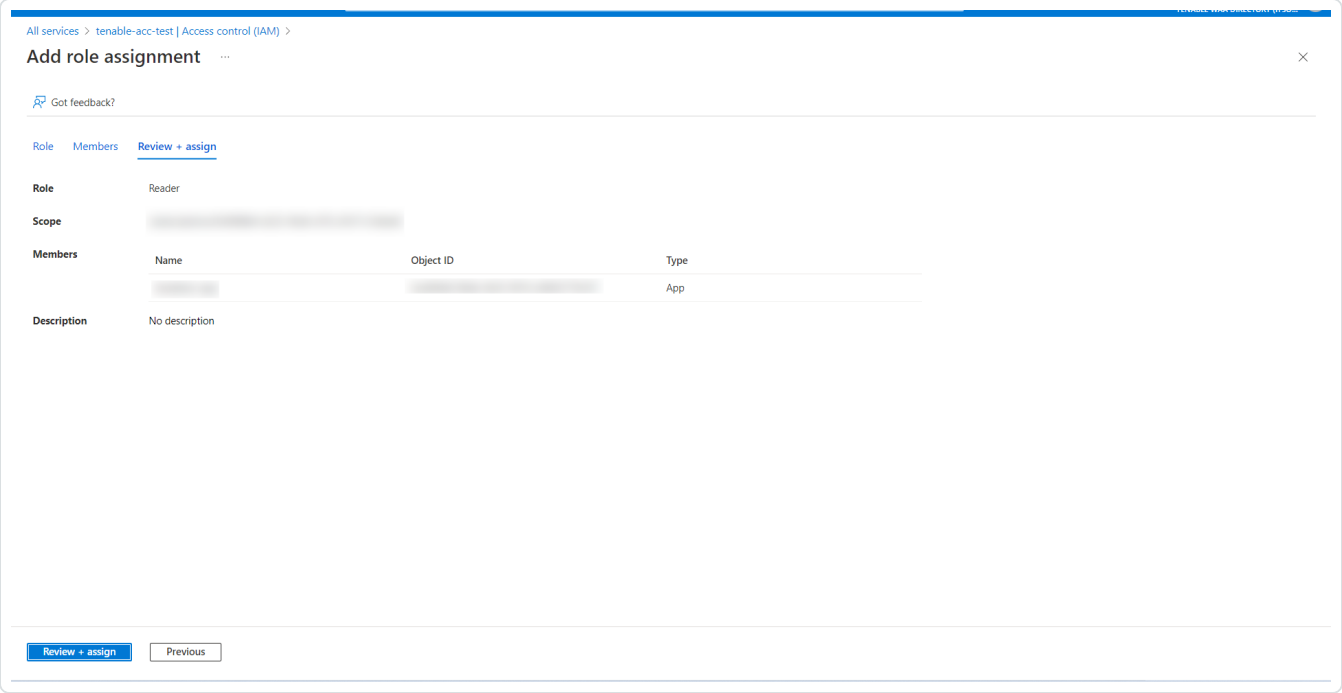


10. To select your Azure Application, click **+ Select Members**.



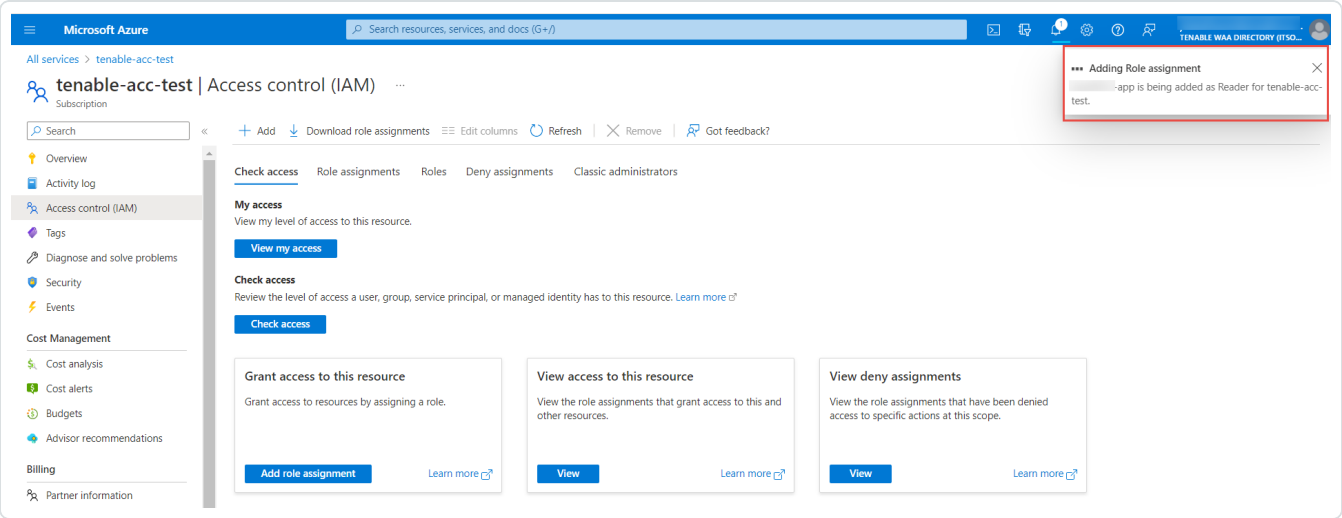
The **Select members** plane appears.

11. Search for the Azure application and select the required application from the list.
12. In the **Review + assign** tab, review the selected role and members.



13. Click **Review + assign**.

    The selected application gets added as **Reader** for the subscription.



What to do next:

Do one of the following:

- (Optional) Link Additional Azure Subscriptions to your Azure Application.
- Create an Azure connector.

Link Azure Subscriptions

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

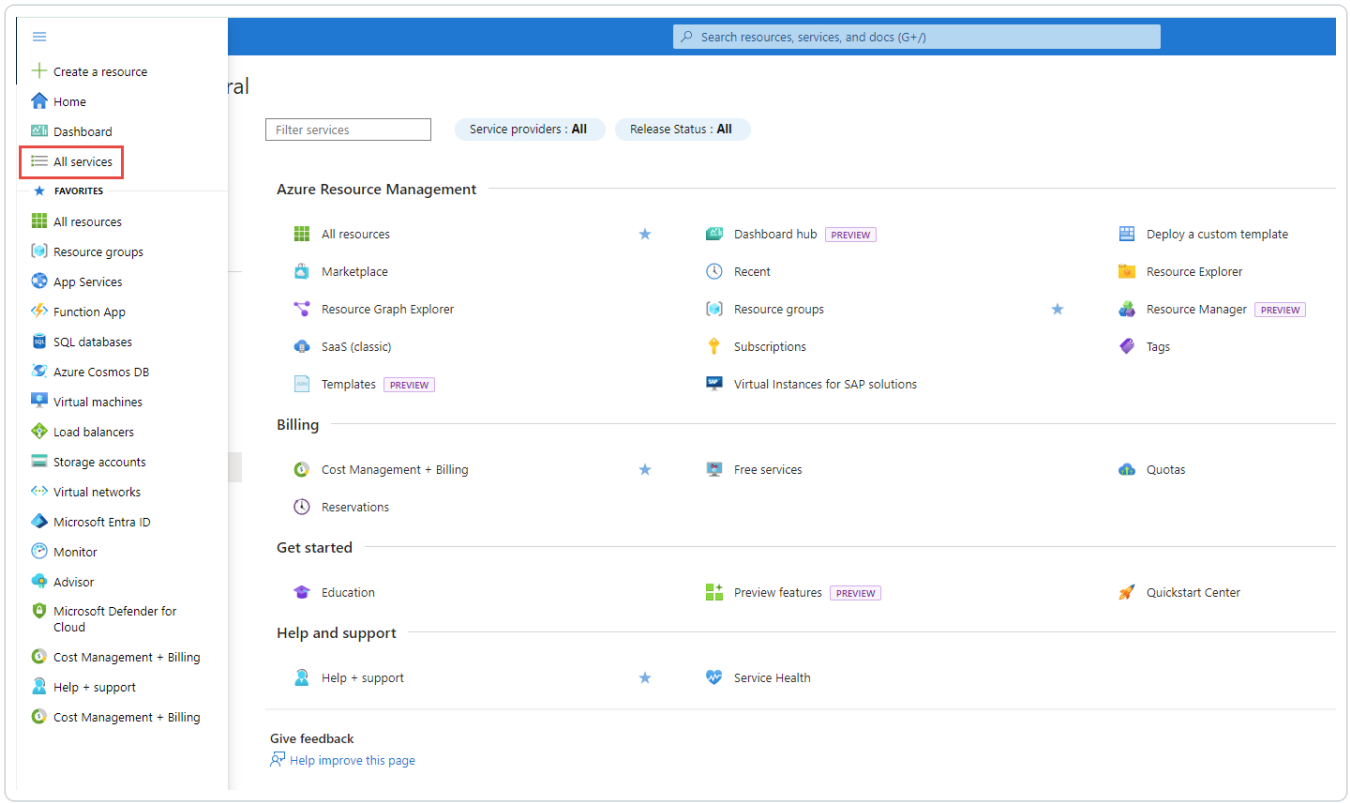
Before you begin:

- Record the name of the application you created for your primary Azure subscription.

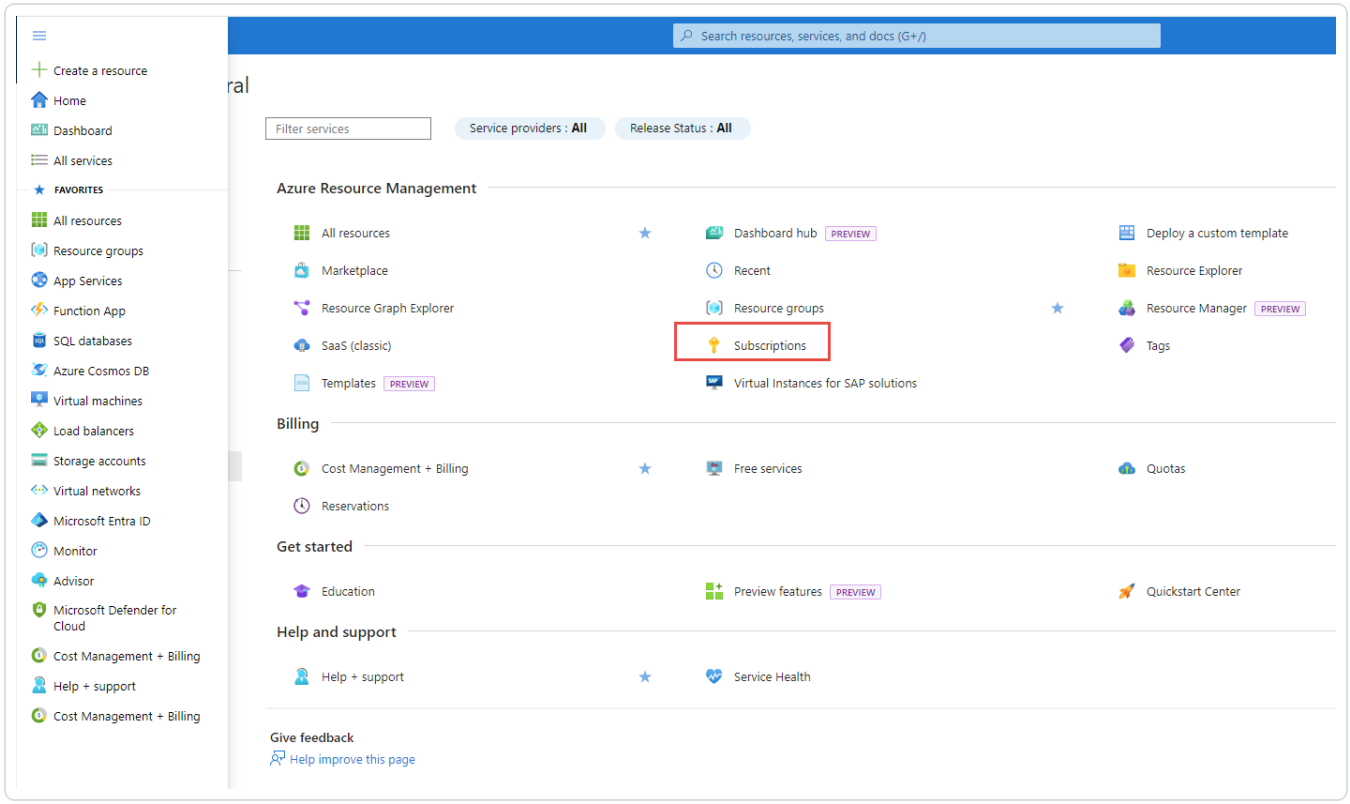
To configure linked Azure subscriptions:

Grant the secondary subscription reader role permissions for the application you created for your primary Azure subscription.

1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click **All Services**.



3. In the **General** section, click **Subscriptions**.



4. In the subscription table, click the applicable subscription.

   The **Overview** page for the subscription appears.

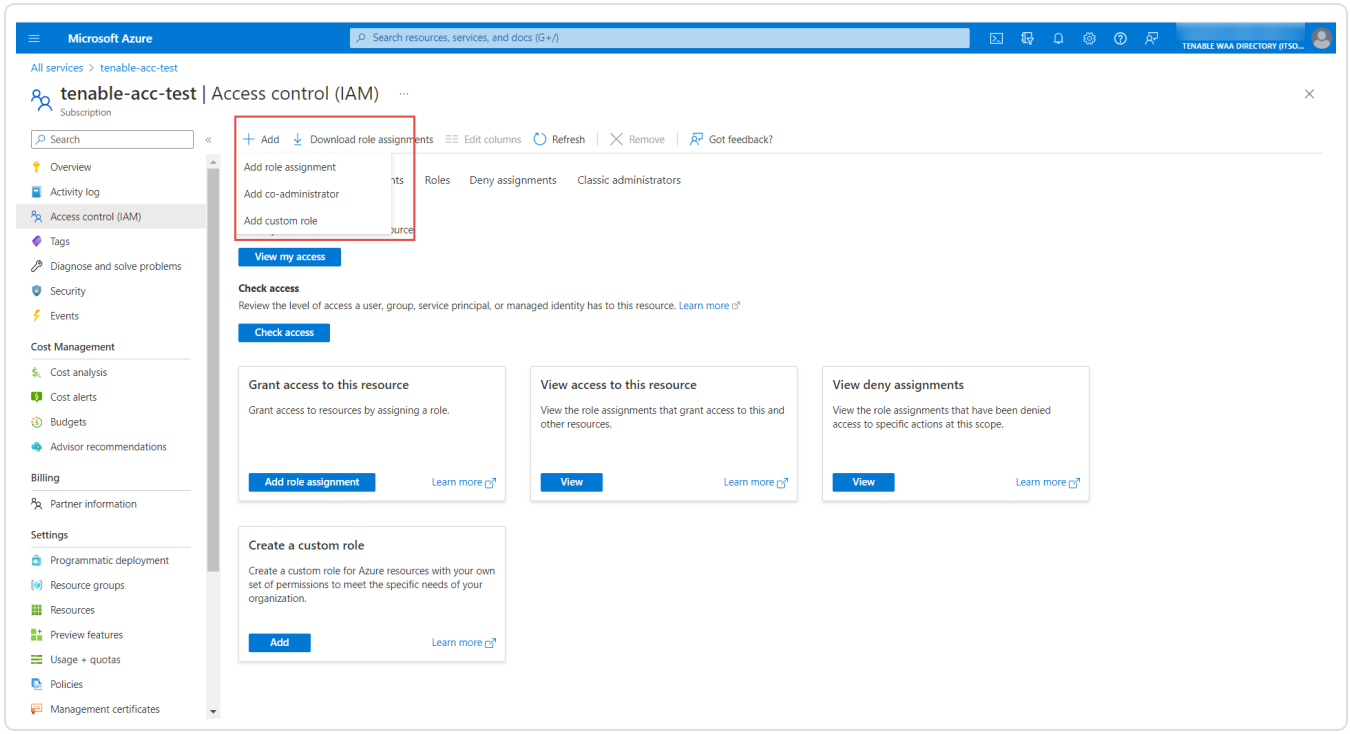
5. In the menu for the subscription, click **Access control (IAM)**.

   The **Access control (IAM)** page appears.

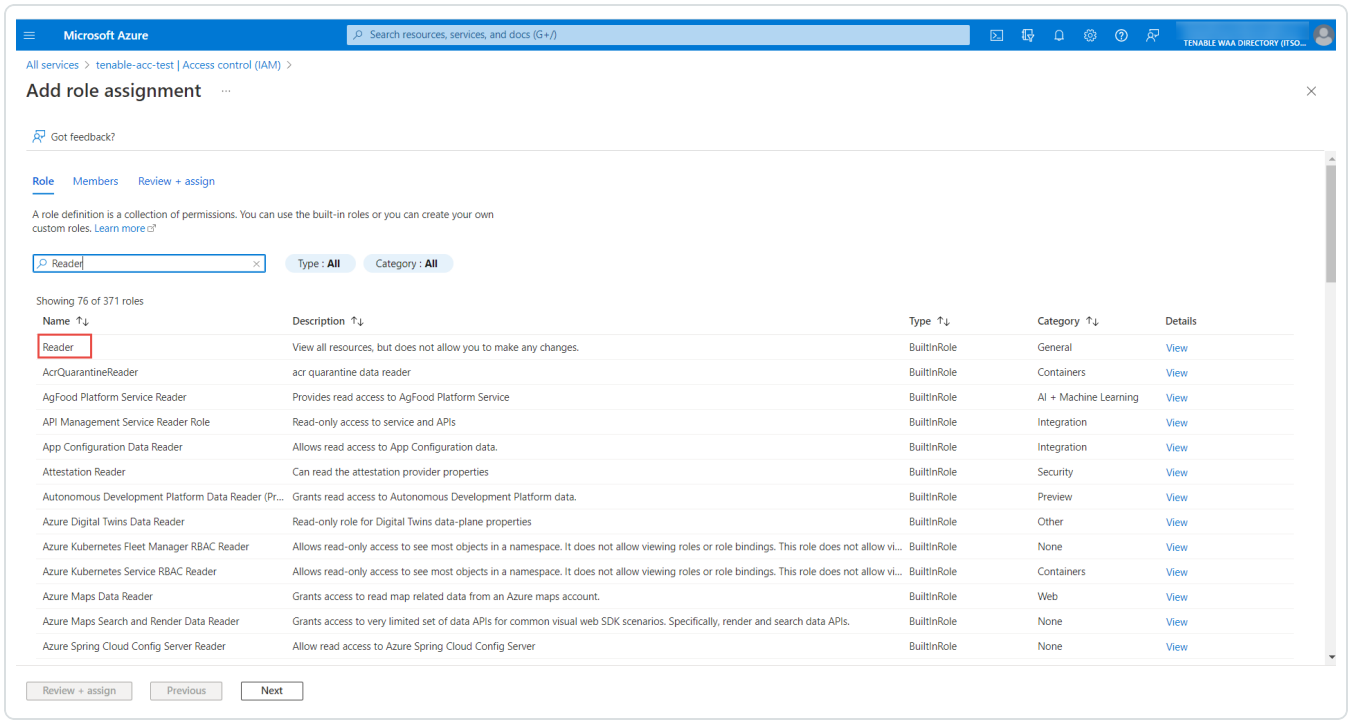
6. Click the **+Add** button.

   A pop-up menu appears.

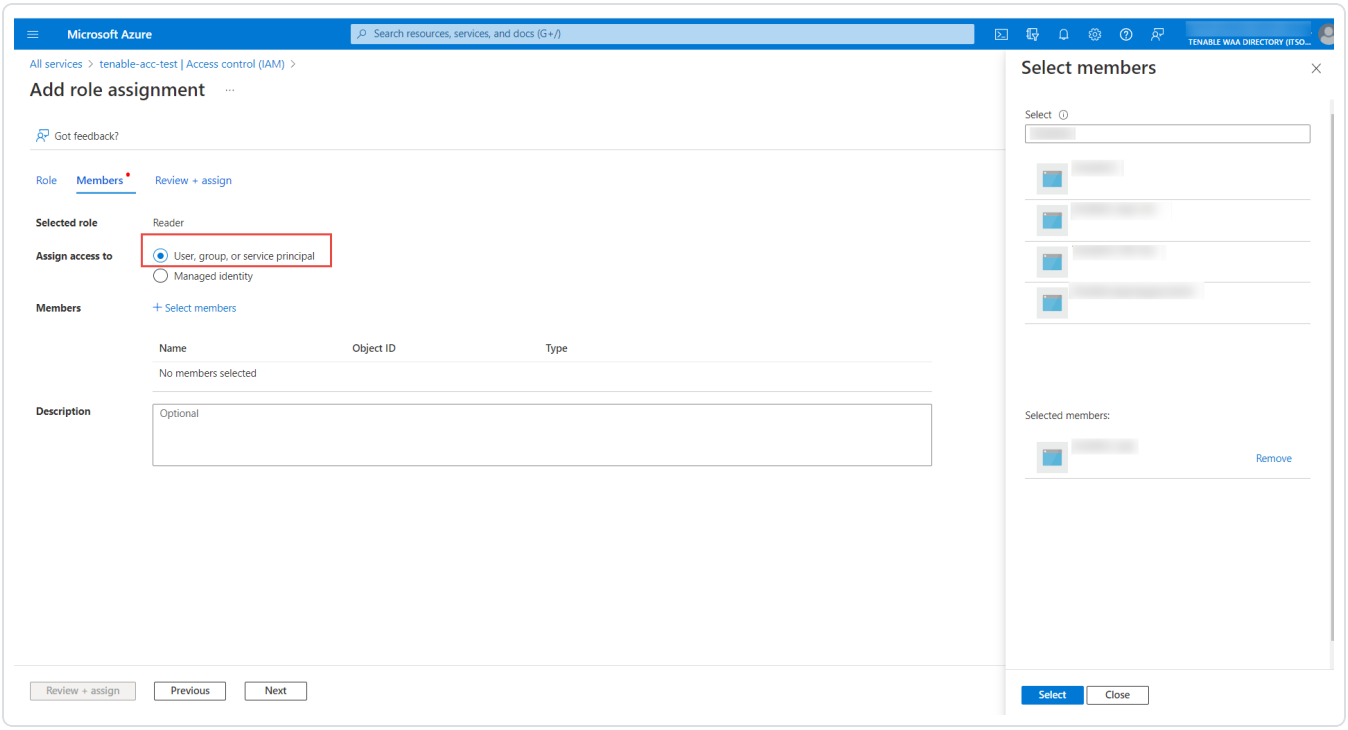
7. Click **Add role assignment**.



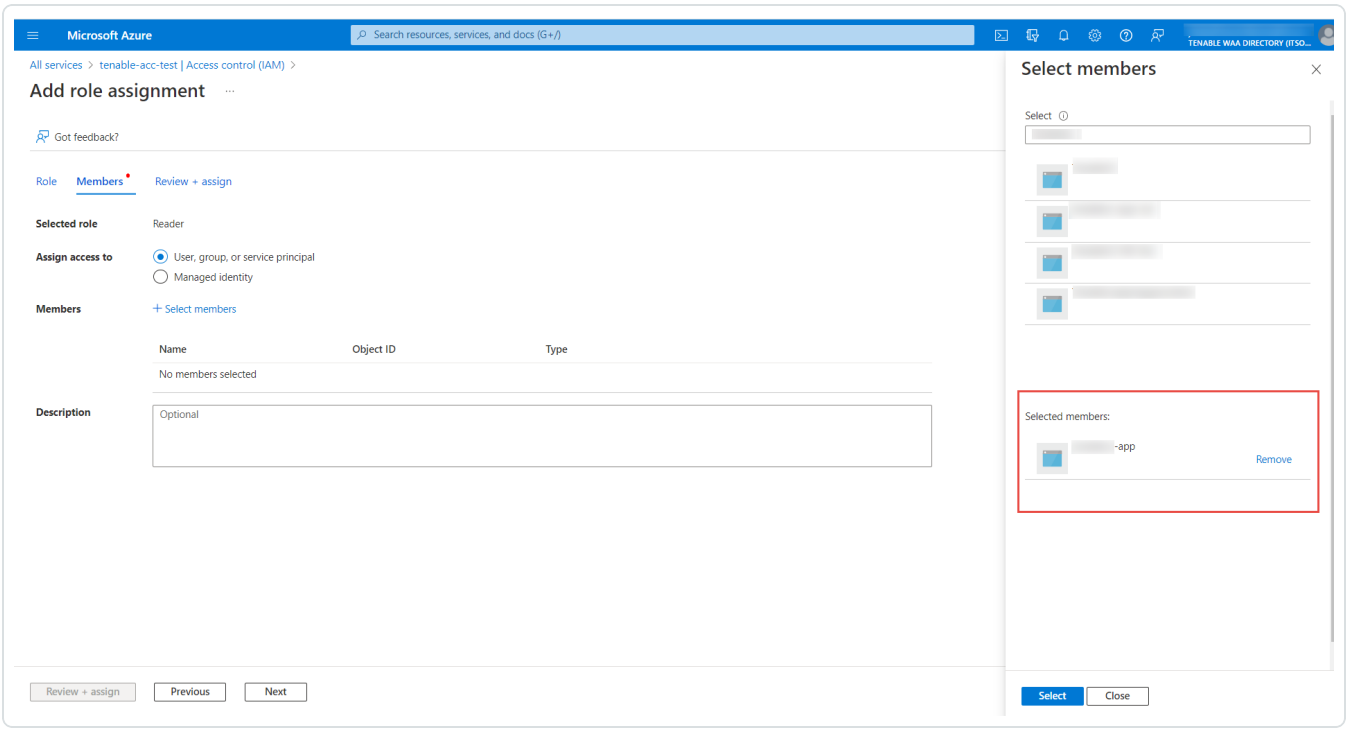
8. In the **Add role assignment** window, in the **Role** tab, search and select **Reader**.



9. In the **Members** tab, in the **Assign access to** section, select **User, group, or service principal**.

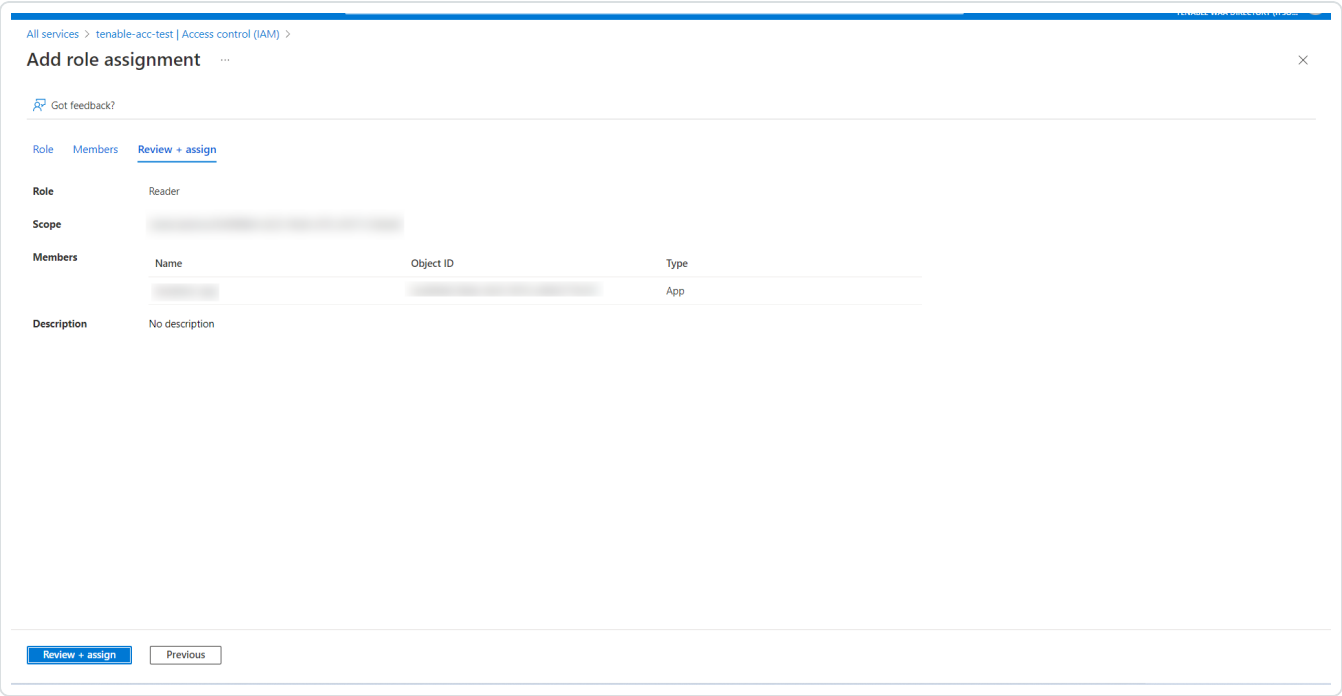


10. To select your Azure Application, click **+ Select Members**.



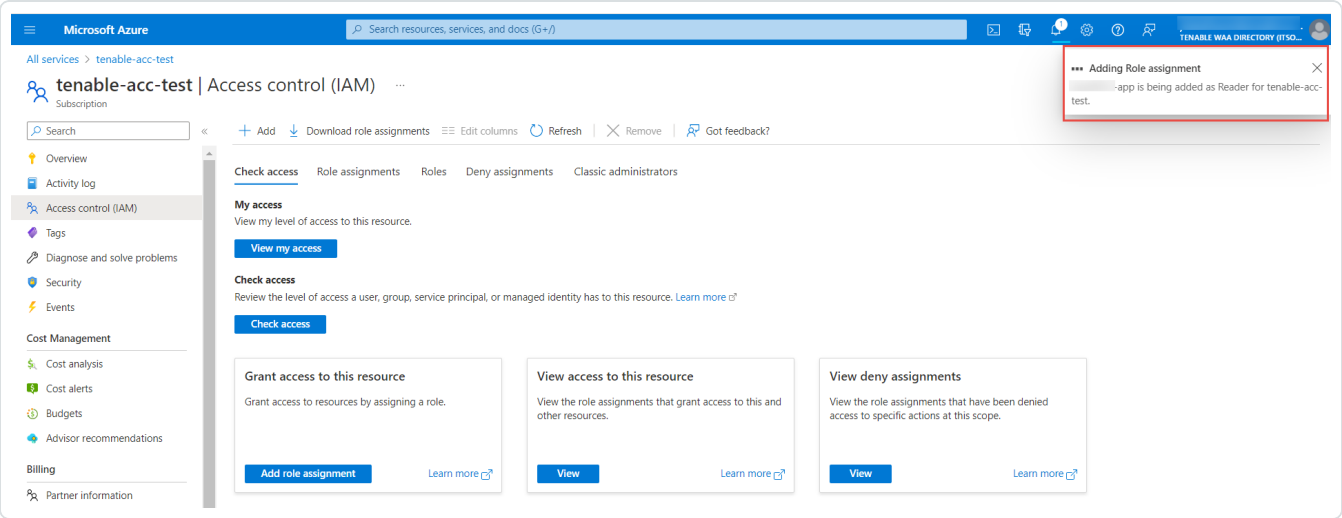
The **Select members** plane appears.

11. Search for the Azure application and select the required application from the list.
12. In the **Review + assign** tab, review the selected role and members.



13. Click **Review + assign**.

    The selected application gets added as **Reader** for the subscription.



What to do next:

- Create an Azure connector.

Create a Microsoft Azure Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

Before you begin:

- Complete the required Microsoft Azure configuration steps.
- Update your plugin set to 2018-12-19 or later.

To create a Microsoft Azure connector:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

4. In the upper-right corner of the page, click the **Create Cloud Connector** button.

   The **Cloud Connectors** plane appears.

5. In the **Cloud Connectors** section, click **Microsoft Azure**.

   The **Microsoft Azure** settings plane appears.

6. In the **Connector Name** box, type a name to identify the connector.
7. In the **Application ID** box, type the Azure application ID that you obtained when configuring Microsoft Azure.
8. In the **Tenant ID** box, type the Azure Tenant ID obtained when configuring Microsoft Azure.
9. In the **Client Secret** box, type the client secret obtained when configuring Microsoft Azure.
10. Use the **Auto Account Discovery** toggle to enable or disable automatic discovery of Azure subscription ID(s).

> **Note:** Auto account discovery is enabled by default. The Azure connector automatically discovers your subscription ID and any linked subscription ID(s).

11. (Optional) If **Auto Account Discovery** is disabled, manually add one or more subscription IDs:

    a. In the **Subscription IDs** section, click the ⊕ button next to **Subscription IDs**.

    The **Add Subscription IDs** plane appears.

    b. In the **Subscription ID** box, type the subscription ID obtained when configuring Microsoft Azure.

    c. (Optional) Click the ⊕ button next to **Add Another Subscription ID** to add additional linked Azure accounts.

    d. In the **Subscription ID** box, type the subscription ID for the Azure account that you want to link. For information about configuring linked subscriptions, see Link Azure Subscription.

    e. To add the Subscription ID(s), click **Add**.

    Tenable Vulnerability Management displays the **Microsoft Azure** settings plane, and the Subscription ID(s) you linked are listed under **Subscription IDs**.

12. In the **Select or Create Network** drop-down box, select an existing network for your connector or click the ⊕ button to create a new network.

> **Note:** Networks help to avoid IP address collisions between cloud assets and Nessus-discovered assets. Tenable recommends creating a network for each connector type in use to prevent asset records in different cloud environments from overwriting each other. For more information about the network feature, see Networks.

13. Use the **Schedule Import** toggle to enable or disable scheduled imports.

> **Note:** By default, Tenable Vulnerability Management requests new and updated asset records every (1) days.

When enabled:

- In the **Import** text box, type the frequency with which Tenable Vulnerability Management sends data requests to the Azure server.

- In the drop-down box select **Minutes**, **Hours**, or **Days**.

> **Note**: When you schedule a connector configuration to sync every 30 minutes, a discovery job is placed in a queue every 30 minutes. The results of the discovery job become available in the Tenable Vulnerability Management interface and logs depending on the workload for the connector services. So, the results of the discovery job can take more than 30 minutes depending on the queue.

14. Do one of the following:

    - To save the connector, click **Save**.
    - To save the connector and import your assets from Azure, click **Save & Import**.

> **Note:** There may be a short delay before your assets appear in Tenable Vulnerability Management.

Google Cloud Platform Connector

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

The Google Cloud Platform (GCP) Connector provides real-time visibility and inventory of assets in Google Cloud Platform. The GCP connector refreshes according to a schedule set by the user.

To import and analyze information about assets in Google Cloud Platform, you must configure GCP to support connectors and then create a GCP connector in Tenable Vulnerability Management.

This connector uses a service account to collect information on Compute Instances in the GCP account.

To analyze assets via a GCP connector:

1. Configure your GCP account to support your connectors, as described in Configure Google Cloud Platform (GCP).
2. Create your GCP connector, as described in Create a Google Cloud Platform Connector (Discovery Only).

> **Note:** To manage existing GCP connectors, see Manage Connectors.

> **Tip:** For common connector errors, see Connectors in the Tenable Developer Portal.

Configure Google Cloud Platform (GCP)

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

Before you can use Tenable Vulnerability Management GCP connectors, you must configure GCP to support your connectors.

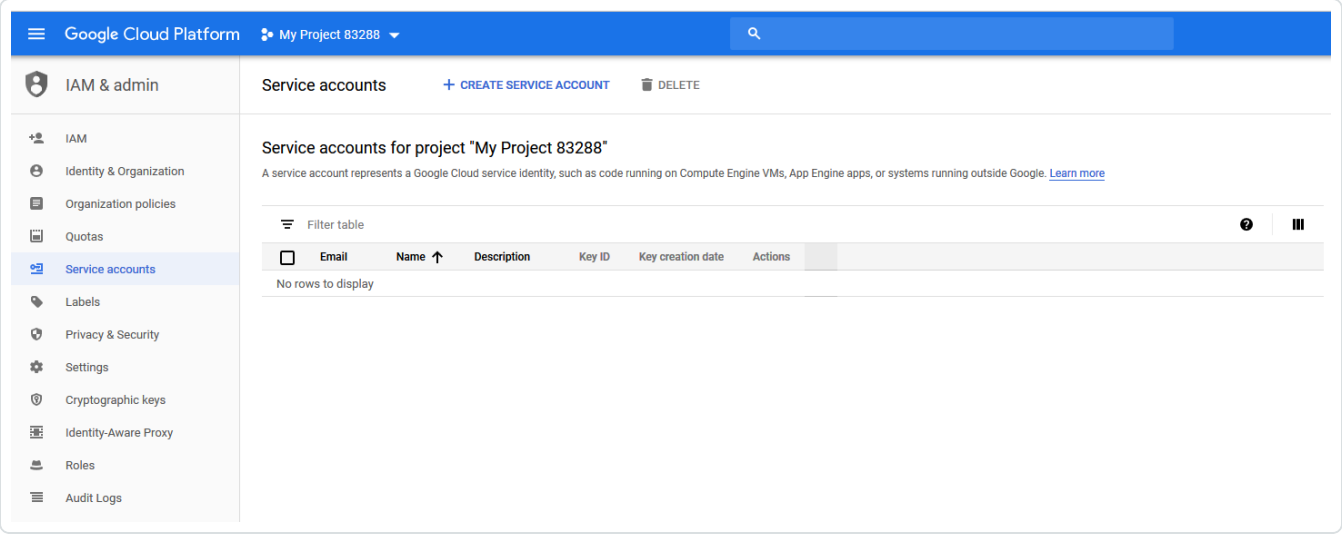
Note: Before configuring connectors, you must enable the compute engine API for each project you want scanned from within Google Cloud Platform. See the Google API documentation for more information.

To configure GCP to support Tenable Vulnerability Management connectors:

1. Log into Google Cloud Platform.
2. In the left navigation bar, select **IAM & Admin**.

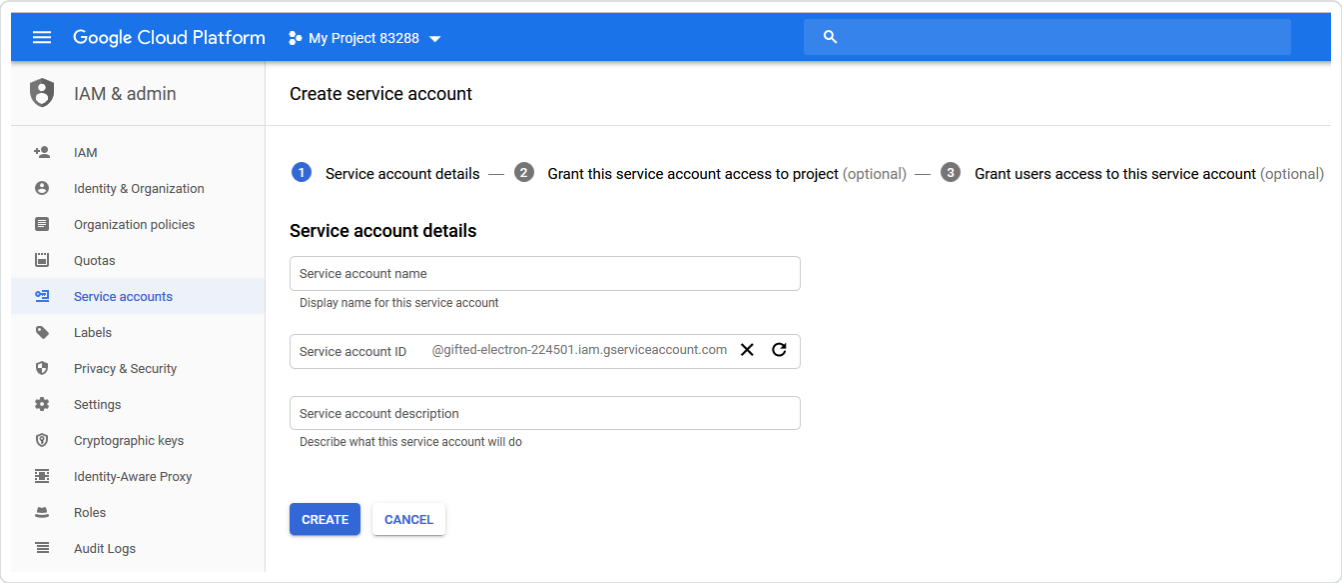
   The **IAM** page appears.
3. In the **Select a project** drop-down box in the upper-left, select the applicable GCP project.
4. In the left navigation bar, select **Service accounts**.

   The **Service accounts** page for your GCP project appears.



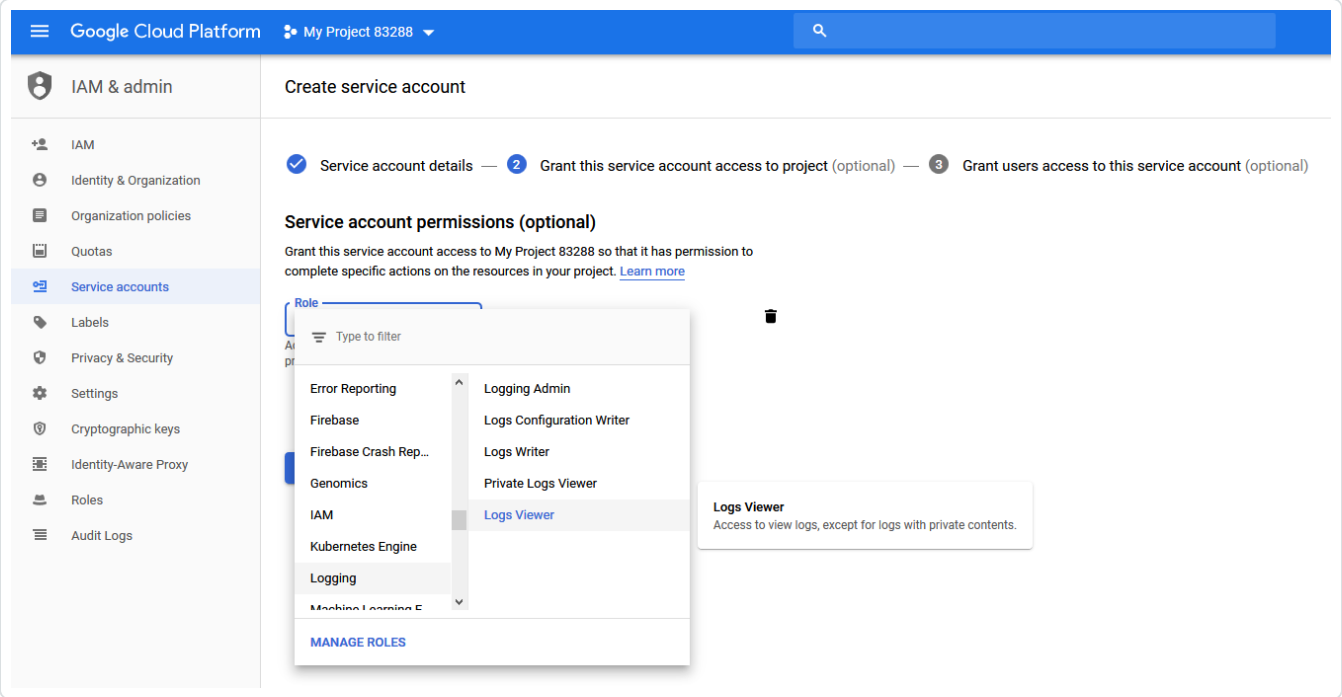
5. Click **+ CREATE SERVICE ACCOUNT**.

   The **Create service account** page appears.



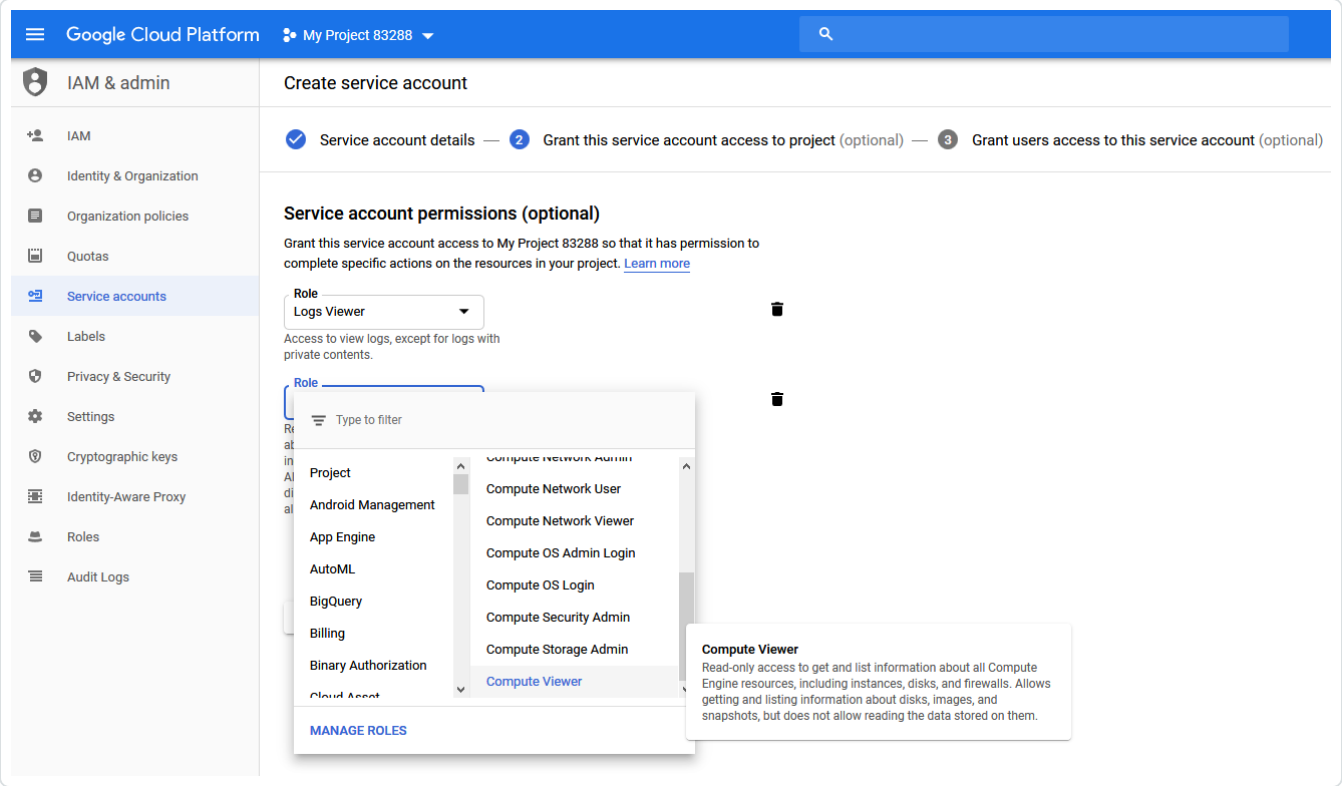
6. In the **Service account name** box, type a display name for your service account.
7. In the **Service account ID** box, type a unique service account ID.
8. In the **Service account description** box, describe what the service account will do.
9. Click **CREATE**.

   The **Grant this service account access to project** page appears.
10. In the drop-down box on the **Service account permissions (optional)** page, add the **Logging** > **Logs Viewer** role.



Note: The service accounts must have the **Logging** > **Log Viewer** role for discovery sync (incremental syncs after initial full sync).

11. Click **+ ADD ANOTHER ROLE** on the **Service account permissions (optional)** page.
12. Add the **Compute Engine** > **Compute Viewer** role.



13. Click **Continue**.

    The **Grant users access to this service account** page appears.

14. In the **Create key (optional)** section, click **+CREATE KEY**.

    The **create key (optional)** pane appears.

15. Under **Key type**, select **JSON** to create a key in JSON format.

16. Click **CREATE**.

    Your browser downloads the key in JSON format.

(Optional) To configure a GCP service account that can access multiple projects:

You may have multiple GCP accounts that you add and remove regularly. Instead of adding each GCP account as a different connector, you can configure the top-level service account to access multiple projects. The GCP connector automatically discovers all linked projects and pulls assets from those projects.

> **Note:** The top-level service account must have the Cloud Resource Manager API enabled in order to access multiple projects.

Caution: The GCP connector pulls assets from any project with configured access to the top-level service account. Only add projects from which you want the GCP connector to pull data.

1. Log into Google Cloud Platform.
2. In the left navigation bar, select **IAM & Admin**.

   The **IAM** page appears.
3. In the drop-down menu in the upper-left corner, select the second GCP project.
4. In the IAM menu bar, click **+ ADD**.

   The **Add members to project** pane appears.
5. In the **New Members** box, type the name of the top-level service account you created in step 6 of the first section.
6. In the **Select a role** drop-down box, select the **Logging** > **Logs Viewer** role.
7. Click the **+ ADD ANOTHER ROLE** button.
8. In the **Select a role** drop-down box, select the **Compute Engine** > **Compute Viewer** role.
9. Click the **+ ADD ANOTHER ROLE** button.
10. In the **Select a role** drop-down box, select the **Service Account Token Creator** role.
11. Click the **+ ADD ANOTHER ROLE** button.
12. In the **Select a role** drop-down box, select **Workload Identity User** role.
13. (Optional) Click the **+ ADD ANOTHER ROLE** button to add additional roles.

What to do next:

- Create a Google Cloud Platform Connector (Discovery Only)
- Create a GCP Connector with Workload Identity Federation Authentication (Discovery Only)
  - Create a GCP Workload Identity Pool and Download the Configuration File
  - Add Principal to Service Account in GCP

Create a Google Cloud Platform Connector (Discovery Only)

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

Before you begin:

- Complete the required GCP configuration steps.

To create a GCP connector:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

3. In the upper-right corner of the page, click the **Create Connector** button.

   The **Select a Connector** pane appears.

4. In the **Connectors** section, click **Google Cloud Platform**.

   The **Google Cloud Platform** pane appears.

5. In the **Connector Name:** box, type a name to identify the connector.

6. In the **Service Account Key** section, click **Add File** to upload your service account key that you obtained when configuring GCP.

7. The **Auto Account Discovery** toggle is always enabled and cannot be disabled. Any Project ID (s) associated with the service account you provided are auto-discovered and assets will be pulled from those projects.

8. In the **Select or Create Network** drop-down box, select an existing network for your connector or click the ⊕ button to create a new network.

   Note: Networks help to avoid IP address collisions between cloud assets and Nessus-discovered assets. Tenable recommends creating a network for each connector type in use to prevent asset records in different cloud environments from overwriting each other. For more information about the

network feature, see Networks.

9. Use the **Schedule Import:** toggle to enable or disable scheduled imports.

   Note: By default, Tenable Vulnerability Management requests new and updated asset records every 1 day.

   If enabled:

   - In the **Import** text box, type the frequency with which Tenable Vulnerability Management sends data requests to the GCP server.
   - In the drop-down box select *Minutes*, *Hours*, or *Days*.

     Note: When you schedule a connector configuration to sync every 30 minutes, a discovery job is placed in a queue every 30 minutes. The results of the discovery job become available in the Tenable Vulnerability Management interface and logs depending on the workload for the connector services. So, the results of the discovery job can take more than 30 minutes depending on the queue.

10. Do one of the following:

    - To save the connector, click **Save**.
    - To save the connector and import your assets from GCP, click **Save & Import**.

    Note: There may be a short delay before your assets appear in Tenable Vulnerability Management.

Create a GCP Connector with Workload Identity Federation Authentication (Discovery Only)

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

Create a GCP connector to discover GCP assets and import them to Tenable Vulnerability Management. Assets discovered through the connectors do not count against the license unless Tenable Vulnerability Management scans them for vulnerabilities.

Before you begin:

- Make sure your service account has the following roles:
  - **Compute Viewer**
  - **Logs Viewer**
  - **Service Account Token Creator**
  - **Workload Identity User**

  For more information about adding these roles, see Configure GCP.
- Create a Workload Identity Pool or Workload Identity Pool Provider and download the credential configuration file. See Create a GCP Workload Identity Pool and Download the Configuration File.
- Add a Principal to your Service Account.

To create a GCP connector with Workload Identity Federation authentication:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.
2. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.
3. In the upper-right corner of the page, click the **Create Cloud Connector** button.

   The cloud connector selection plane appears.
4. In the **Cloud Connectors** section, click **GCP Workload Identity Federation**.

   The **Connector Setup** window appears.
5. In the **Connector Name** box, type a name to identify the connector and click **Next**.
6. In the **Apply Choices** section, do the following:
   a. Click **Add File** and browse to your local system to add a credential configuration file.

   > **Note**: To download the GCP credential configuration file, follow the steps in Create a GCP Workload Identity Pool and Download the Configuration File

   b. Make sure the **Auto Account Discovery** option is selected.

c. In the **Network** drop-down box, select an existing network to add the connector. When the connector discovers an asset, the associated network figure in the asset's details. Click **Create New** to add a new network.

d. (Optional) Use the **Schedule Import** toggle to enable or disable scheduled imports. By default, Tenable Vulnerability Management requests new and updated asset records every 1 day.

   If enabled:

   i. In the text box, type the frequency that Tenable Vulnerability Management sends data requests to the GCP server.

   ii. In the drop-down box select **Minutes**, **Hours**, or **Days**.

   > **Note**: When you schedule a connector configuration to sync every 30 minutes, a discovery job is placed in a queue every 30 minutes. The results of the discovery job become available in the Tenable Vulnerability Management interface and logs depending on the workload for the connector services. So, the results of the discovery job can take more than 30 minutes depending on the queue.

7. Do one of the following:

   - To save the connector, click **Save**.
   - To save the connector and import your assets from GCP, click **Save & Import**.

   Tenable Vulnerability Management imports your assets from GCP. There may be a short delay before your assets appear.

Add Principal to Service Account in GCP

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

> **Required User Role:** Administrator

Add a principal to your service account and assign the **Workload Identity User** role for GCP Workload Identity Federation authentication. For more information about principals, see the Google Cloud documentation.

Before you begin:

- Make sure you have a valid GCP account.

To add a principal to your service account:

1. Log into Google Cloud Platform.
2. Select the **IAM & Admin** tile.

   The **IAM** page appears.
3. In the left navigation pane, select **Service Accounts**.

   The **Service Accounts** page appears.
4. In the row of the service account you are using for **Workload Identity Federation**, click ⋮ > **Manage Permissions**.

   The **Permissions** tab of the service account appears.
5. In the **View By Principals** tab, click **Grant Access**.

   The **Grant access to service account** panel appears with the following:

   `principalSet://iam.googleapis.com/projects/PROJECT_NUMBER/locations/global/workloadIdentityPools/POOL_ID/*`

   - Replace the `PROJECT_NUMBER` with your project number. Note that you use the project number and not the project ID here.
   - Replace the `POOL_ID` with the name of the workload pool you created. See Create a GCP Workload Identity Pool and Download the Configuration File.
6. In the **Assign Roles** section, select the **Workload Identity User** role.
7. Click **Save**.

   GCP adds the principal to your service account.

Create a GCP Workload Identity Pool and Download the Configuration File

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

To create a GCP Workload Identity Federation cloud connector, you must create a workload identity pool in GCP. Add a provider to the pool, grant access to the provider, and download the credential configuration file. You can use this configuration file when configuring the GCP Workload Identity Federation connector. For more information about pools and how they manage external identities, see the Google Cloud documentation.

Before you begin:

- Make sure you have a valid GCP account.

To create a Workload Identity Pool:

1. Log into Google Cloud Platform.
2. In the left navigation bar, select **IAM & Admin**.

   The **IAM** page appears.
3. In the left navigation pane, select **Workload Identity Federation**.

   The **Workload Identity Pools** page appears.
4. Click **Create Pool**.

   The **New workload provider and pool** page appears.
5. In the **Create an Identity pool** section, do the following:
   a. In the **Name** box, type a name for the pool.
   b. (Optional) In the **Description** box, provide a description for the pool.
   c. Click **Continue**.
6. In the **Add a provider to pool** section, do the following:
   a. From the **Select a provider** drop-down box, select AWS from the list.
   b. In the **Provider details** box, provide the Tenable AWS account name. You can choose any name.
   c. In the **AWS account ID** box, provide the Tenable AWS account ID: `012615275169`
   d. Click **Continue**.

7. In the **Configure provider attributes** section, click **Save**.

   GCP creates the pool and opens the newly created pool page.

8. Click **Grant Access**.

   The **Grant access to service account** panel appears.

9. Select the **Grant access using Service Account Impersonation** option.

   The relevant sections appear.

10. In the **Service** account drop-down box, select the service account.

11. In the **Select principals** drop-down box, select `aws_role` and provide the `aws_role arn` value as `arn:aws:iam::012615275169:role/keyless_connector_role`

12. Click **Save**.

    The **Configure your application** dialog box appears.

13. In the **Provider** drop-down box, select the workload identity pool provider, then click **Download Config**.

    GCP downloads the configuration file. Use this file in the **Add File** section when you create the GCP Workload Identity Federation connector.

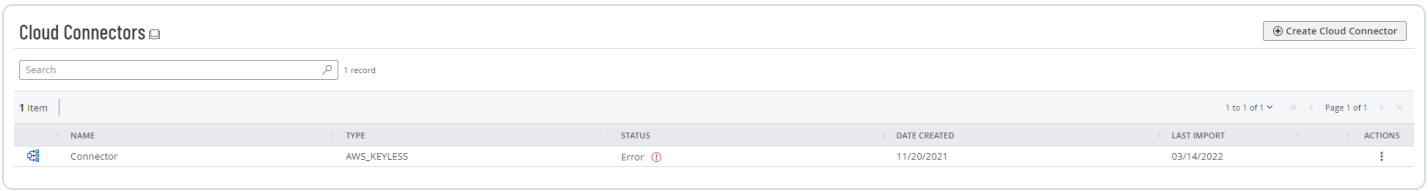
What to do next

Create a GCP Connector with Workload Identity Federation Authentication (Discovery Only)

Manage Existing Connectors

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

The **Cloud Connectors** page displays the Connectors table, which lists all your configured connectors.



Launch a Connector Import Manually

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

To launch a manual import for a connector:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

3. In the row of the connector from which you want to launch a manual import, in the **Actions** column, click ⋮ > ⇤ **Import**.

   Tenable Vulnerability Management sends a request for data to the source. During the request processing, the import button appears as a check mark. You cannot launch another manual import for that connector until the request process completes.

View Connectors Details

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

On the **Connectors** page, you can view details about your connectors and imports.

Note: You can also complete connector management tasks from the **Connectors** page, including launching an import manually, editing a connector, and deleting a connector. For more information, see Manage Existing Connectors.

Before you begin:

- Configure the platform your connector must access and create your connector, as described in Connectors.

To view connector and import details:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

3. In the **Connectors** table, you can:

   a. Search the **Connectors** table.

   b. View details about your connectors and imports.

Column	Action
Name	View the name of the connector.
Type	View the platform or registry type from which your connector pulls assets.
Status	View the status for your most recent asset import. **Note**: If your connector is a Tenable Container Security connector, you can hover over the connector row in the **STATUS** column to view error details for failed imports.
Date Created	• View the date your connector was created in MM/DD/YYYY format. • Click the column header to sort your connectors by creation date.
Last Import	View the date for the most recent asset import. **Note**: If your connector is a Tenable Container Security connector, a green ⟳ icon appears next the date after the import starts. You can hover over the icon to view details for each asset the connector imports. As the import progresses, the details update in real time.

View Connector Event History

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

For Microsoft Azure connectors and AWS connectors configured with keyless authentication, you can view connector event history to help you troubleshoot issues. You can see events such as when Tenable Vulnerability Management synced with the connector, imported assets, or checked for terminated assets.

Before you begin:

- Configure the platform your connector must access and create your connector, as described in Connectors.

To view connector event history:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

3. In the connector table, click the connector for which you want to view event history.

   Note: You can view event history for Microsoft Azure connectors and AWS connectors configured with keyless authentication.

   The connector settings plane appears.

4. Click **View Event History**.

   The connector plane expands and displays the **Connector Event History** table. The table displays events sent by the connector to Tenable Vulnerability Management, such as when Tenable Vulnerability Management synced with the connector, imported assets, or checked for terminated assets. For information on connector errors, see Connectors as documented in the Tenable Developer Portal.

Edit a Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

From the **Settings** page, you can edit your connector details, including the asset import schedule. The steps to edit a connector vary depending on the platform.

Before you begin:

- Configure and create your connector, as described in Connectors.
- Log in to Tenable Vulnerability Management.

To edit a Microsoft Azure connector:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

3. In the connector table, click the connector that you want to edit.

   The **Edit Connector** pane appears.

4. Modify any of the following connector settings:

   - In the **Select or Create Network** drop-down box, change the existing network for your connector or click the ⊕ button to create a new network.
   - In the **Connector Name** box, change the name of the connector.
   - In the **Application ID** box, change the application ID.
   - In the **Tenant ID** box, change the tenant ID.
   - In the **Client Secret** box, change the client secret.
   - Use the **Auto Account Discovery** toggle to enable or disable automatic discovery of subscription IDs.
   - If **Auto Account Discovery** is disabled, add or remove subscription IDs.
   - In the **Schedule Import** options, change the frequency of scheduled imports.

5. Click **Save**.

Tenable Vulnerability Management saves the connector. There may be a short delay before your assets appear in Tenable Vulnerability Management.

To edit an Amazon Web Service (AWS) connector:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

3. In the connector table, click the connector that you want to edit.

   The **Edit Connector** pane appears.

4. Modify the connector.

   ### If using AWS role delegation (keyless authentication):

   - In the **Select or Create Network** drop-down box, change the existing network for your connector or click the ⊕ button to create a new network.
   - In the **Connector Name** box, change the name of the connector.
   - Use the **Auto Account Discovery** toggle to enable or disable automatic discovery of linked accounts and CloudTrails.
   - In the **Schedule Import** options, change the frequency of scheduled imports.

   ### If using key-based authentication:

   - In the **Select or Create Network** drop-down box, change the existing network for your connector or click the ⊕ button to create a new network.
   - In the **Connector Name** box, change the name of the connector.
   - In the **Access Key** box, change the access key.
   - In the **Secret Key** box, change the secret key that corresponds to the access key.
   - In the **Additional Accounts** section, add or remove linked accounts.
   - In the **AWS CloudTrails** section, add or remove CloudTrails.

- Click **Refresh CloudTrails** to query the AWS regions and update the **AWS CloudTrails** table.
- In the **Schedule Import** options, change the frequency of scheduled imports.

5. (Optional) If you selected different trails, click **Find Assets**.

   The number of assets to be imported into Tenable Vulnerability Management appears next to the **Find Assets** button. This number may include assets that were previously imported. No duplicate is created if an asset was previously imported.

6. Click **Save**.

   The connector saves. If you selected different trails, your assets from AWS import. There may be a short delay before your assets appear in Tenable Vulnerability Management.

To edit a Google Cloud Platform (GCP) connector:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

3. In the connector table, click the connector that you want to edit.

   The **Edit Connector** pane appears.

4. Modify any of the following connector settings:

   - In the **Select or Create Network** drop-down box, change the existing network for your connector or click the ⊕ button to create a new network.
   - In the **Connector Name** box, change the name of the connector.
   - Under **Service Account Key**, click **Add File** to change your service account key.
   - In the **Schedule Import** options, change the frequency of scheduled imports.

5. Click **Save**.

   Tenable Vulnerability Management saves the connector. There may be a short delay before your assets appear in Tenable Vulnerability Management.

Delete a Connector

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required User Role: Administrator

To delete a connector:

1. In the left navigation, click ⚙ **Settings**.

   The **Settings** page appears.

2. Click the **Cloud Connectors** tile.

   The **Cloud Connectors** page appears and displays the configured connectors table.

3. In the connector table, click the ✕ button next to the connector that you want to delete.

   A **Confirm Deletion** window appears.

4. Click **Delete**.

   Tenable Vulnerability Management deletes the connector.

Tenable Data Stream

With Tenable Data Stream, you connect an AWS S3 bucket to Tenable Vulnerability Management, which then continuously sends your Tenable data to the bucket in JSON format. This feature is an alternative to the Tenable export APIs.

Note: To connect to your AWS bucket, Tenable uses an AWS Identity Access Management (IAM) role with *least privilege* access.

The following topics break down how to configure Tenable Data Stream and use its manifest files to ingest vulnerability data into your application. They also describe the format of the payload files sent by Tenable Vulnerability Management.

- Configure Tenable Data Stream
- Best Practices
- Manifest Files
- Assets Payload Files

- Assets Properties
- Findings Payload Files
- Findings Properties
- Tags Payload Files
- Tags Properties

Configure Tenable Data Stream

To set up Tenable Data Stream, connect your AWS bucket to Tenable Vulnerability Management. When connecting to your AWS bucket, Tenable uses an *AWS Identity Access Management (IAM) role* with a *trust relationship* and *least privilege access*.

To configure Tenable Data Stream:

1. In the left navigation, click **Settings**.

   The **Settings** page appears.

2. Click **Tenable Data Stream**.

   The **Tenable Data Stream** page appears.

3. In the top-left corner, click **Add an Integration**.

4. In the **Add Integration** window, enter the following:

Option	Description
Integration Name	The name of the integration.
Integration Type	The type of the integration. **AWS S3** is the only selectable option.
Integration Data	Determines the type or types of data that Tenable Vulnerability Management streams to your AWS bucket. You can select any combination of the following options: • Tenable Vulnerability Management

	• **Assets**
	• **Vulnerabilities**
	• **Host Audit**
	• Tenable Web App Scanning
	  • **Assets**
	  • **Findings**
	
	Note: Selecting either asset type configures Tenable Vulnerability Management to stream tag data in addition to the asset data. For example, if you select Tenable Web App Scanning **Assets**, Tenable Vulnerability Management streams Web App Scanning asset *and* tag data.

Email Notification	(Optional) An email address where notifications will be sent if the stream state changes (for example, when a stream fails).

5. Click **Next**.

6. In **Configure an IAM Role**, enter the following:

Option	Description
AWS Account ID.	Your organization's AWS account ID, as described in AWS Account Management in the AWS documentation.
IAM Role Name	The IAM role to use, as described in IAM roles in the AWS documentation. **Tip**: Tenable recommends creating a new IAM role. To do this, copy the *Trust Policy* from the blue box and add it to your AWS settings as described in Creating a role using custom trust policies in the AWS documentation. If not creating a new role, copy the Trust Policy into the existing role instead.
External ID	A secret alphanumeric identifier that Tenable will use to assume the IAM role, as described in Access to AWS accounts owned by third parties in the AWS documentation.

7. Click **Next**.
8. In **Configure an AWS Bucket**, add the following:

Option	Description
S3 Bucket Name	The name you want to use for the S3 bucket. **Tip**: Tenable recommends creating a new AWS bucket. When doing this, copy the *Bucket Policy* from the blue box and add it to your S3 bucket permissions. Otherwise, copy the Bucket Policy to your existing bucket.
Path Prefix	The path prefix for the AWS path where your data will be saved.

9. Click **Save**.

   Tenable Vulnerability Management begins processing the AWS integration.

Tenable Data Stream Best Practices

When configuring Tenable Data Stream, Tenable recommends the following.

Configuring an IAM Role

To access your AWS bucket, the Tenable system assumes an AWS Identity and Access Management (IAM) role, for which it requires a *trust relationship*. When assuming the role, the system employs temporary session tokens which are regenerated once an hour. To learn more, see IAM roles in the AWS documentation.

> **Tip**: Tenable recommends using *least-privilege permissions* when configuring the AWS bucket and role.

Configuring the S3 Bucket

When configuring the S3 bucket, follow these guidelines:

- **IAM policy** – Apply a *policy* to define permissions for the Tenable system. To learn more, see Policies and permissions in AWS Identity and Access Management in the AWS documentation.

- **AWS region** – For the fastest speeds, use an S3 bucket in the same *AWS Region* as your Tenable container.
- **Server-side encryption** – By default, AWS uses server-side encryption with Amazon S3-managed keys. Tenable only supports the *default* encryption mode of SSE-S3, not other modes such as SSE-KMS. To learn more, see Protecting data with server-side encryption in the AWS documentation.
- **Writing to the bucket** – The Tenable system can only write to your S3 bucket when sending data.
- **Deleting files** – To delete files or free space, use *object expiration*. To learn more, see Expiring objects in the AWS documentation.
- **AWS storage** – The more Tenable scans you run, the more data will be sent. This impacts your AWS storage costs.
- **Notification events** – You must manually configure any notifications or triggers that start processes to ingest incoming data into your systems.

Troubleshooting Tenable Data Stream

Check the status of your streams in **Settings** > **Tenable Data Stream**.

> **Tip**: To get emails about stream status, when configuring new streams, enable email notifications.

Streams have three states:

State	Description
OK	Stream data is being successfully sent.
RETRY	The system has encountered configuration errors and will retry the stream for three days. If the errors are fixed, the stream resumes from the last checkpoint with no lost data.
FAILED	The stream is suspended and the system will not retry. Data has been lost. When you address any configuration errors, the system will treat the stream as a new stream.

About Stream Failures

Streams can fail for the following reasons:

- **Misconfigured IAM role** – Deleting the role from your AWS account or changing the trust relationship.
- **S3 bucket issue** – Changing the bucket policy (for example, by removing permissions), deleting the bucket, incorrect provisioning, or AWS storage issues.

Consuming Data from Tenable Data Stream

Tenable Data Stream writes data in the order that it's observed (for example, in the order of a series of scans). In AWS, you can sort files by name to put them in sequential order. You can also use the order from the manifest file sent when a stream completes successfully within 60 minutes.

Manifest Files

When the Tenable system finishes sending payload files, it sends a *manifest file* that lists the files in the order they were sent, along with metadata and file paths. The system generates a manifest file as often as every 15 minutes.

Using Manifest Files

You can reference manifest files when building logic to ingest vulnerability data into your application. To do this, apply a *handler* to the manifest file so the resulting process consumes payload files in order.

For example, let's say the Tenable system sends 100 findings payload files to your AWS bucket between 12:00 PM and 12:15 PM and they are saved in …/finding/<export-date>/. At 12:15 PM, the system sends a manifest file to …/manifest_finding/<export-date>/ in this format with a list of the files.

This process works the same way for all payload file types: assets, findings, and tags.

Manifest File Properties

The following table defines the properties that appear in Tenable Data Stream manifest files.

Property	Data Type	Description
type	string	The type of manifest file: MANIFEST_ASSET, MANIFEST_ASSET_ENRICHED_ATTRIBUTES, MANIFEST_FINDING,

		`MANIFEST_TAGS`, `MANIFEST_HOST_AUDIT_FINDING`, `MANIFEST_WAS_ASSET`, or `MANIFEST_WAS_FINDING`.
`payload_type`	string	The type of payload the manifest contains: `ASSET`, `ASSET_ENRICHED_ATTRIBUTES`, `FINDING`, `TAGS`, `HOST_AUDIT_FINDING`, `WAS_ASSET`, or `WAS_FINDING`.
`payloads[].path`	string	The path to the payload file in your AWS bucket.
`payloads[].md5`	string	The MD5 hash value of the payload file.
`payloads[].version`	integer	The version identifier for the manifest file.
`payloads[].num_updates`	integer	The number of updates in the payload file.
`payloads[].num_deletes`	integer	The number of deleted items in the payload file.
`payloads[].first_record_timestamp`	integer	The Unix timestamp of the first entry in the payload file.
`payloads[].last_record_timestamp`	integer	The Unix timestamp of the last entry in the payload file.
`payloads[].scan_id`	string	The grouping ID for assets, findings, or tags in the payload file. If there is no grouping ID, this value is empty.

Example Manifest Files

The following examples show the format of the manifest files sent by the Tenable system. In the files, each payload file is one object in an array.

Asset Manifest File


```
{
    "type": "MANIFEST_ASSET",
    "payload_type": "ASSET",
    "payloads": [
        {
            "path": "path-prefix/asset/2024-09-23/asset-1727096558876-17-5a0ffa7d-6b2c-4af6-a0f1-
f506fe769dba.json.gz",
            "md5": "c515b063ad68680fc90257444f782e94",
            "version": 1,
            "num_updates": 1,
            "num_deletes": 0,
            "first_record_timestamp": 1727096558490,
            "last_record_timestamp": 1727096558490,
            "scan_id": "5a0ffa7d-6b2c-4af6-a0f1-f506fe769dba"
        }
    ]
}
```


Asset Enriched Attributes Manifest File


```
{
    "type": "MANIFEST_ASSET_ENRICHED_ATTRIBUTES",
    "payload_type": "ASSET_ENRICHED_ATTRIBUTES",
    "payloads": [
        {
            "path": "qa-develop/asset_enriched_attributes/2025-06-18/asset_enriched_attributes-
1750252966511-1.json.gz",
            "md5": "616617a2dfe0df8e892316058cf5530c",
            "version": 1,
            "num_updates": 17,
            "num_deletes": 0,
            "first_record_timestamp": 1750172403355,
            "last_record_timestamp": 1750176033025,
            "scan_id": ""
        },
        {
            "path": "qa-develop/asset_enriched_attributes/2025-06-18/asset_enriched_attributes-
1750252984136-2.json.gz",
            "md5": "39a54218060ab9a631b474917dc6e236",
            "version": 1,
            "num_updates": 31,
            "num_deletes": 0,
            "first_record_timestamp": 1750172403475,
            "last_record_timestamp": 1750172403641,
            "scan_id": ""
        }
    ]
}
```

Findings Manifest File


```
{
  "type": "MANIFEST_FINDING",
  "payload_type": "FINDING",
  "payloads": [
    {
      "path": "path-prefix/finding/2024-09-23/finding-1727096618967-60-5a0ffa7d-6b2c-4af6-a0f1-
f506fe769dba.json.gz",
      "md5": "e6919aaffa6967e0c6de3908c9a04a78",
      "version": 1,
      "num_updates": 2,
      "num_deletes": 0,
      "first_record_timestamp": 1727096618799,
      "last_record_timestamp": 1727096618820,
      "scan_id": "5a0ffa7d-6b2c-4af6-a0f1-f506fe769dba"
    }
  ]
}
```


Host Audit Manifest File


```
{
  "type": "MANIFEST_HOST_AUDIT_FINDING",
  "payload_type": "HOST_AUDIT_FINDING",
  "payloads": [
    {
      "path": "milestone/host_audit_finding/2025-03-21/host_audit_finding-1742541936393-96-9282cea5-
39e8-cefa-d974-f2a2bd7ac70c9d992fe1d8037d1c.json.gz",
      "md5": "15b7e9ed5bdace3f0f23f1b19974f5ad",
      "version": 1,
      "num_updates": 1,
      "num_deletes": 0,
      "first_record_timestamp": 1742541936259,
      "last_record_timestamp": 1742541936259,
      "scan_id": "9282cea5-39e8-cefa-d974-f2a2bd7ac70c9d992fe1d8037d1c"
    },
    {
      "path": "milestone/host_audit_finding/2025-03-21/host_audit_finding-1742541940859-8-9282cea5-
39e8-cefa-d974-f2a2bd7ac70c9d992fe1d8037d1c.json.gz",
      "md5": "ef85f63c46c5cf48c09bfc70ffcdaa91",
      "version": 1,
      "num_updates": 1,
      "num_deletes": 0,
      "first_record_timestamp": 1742541936099,
      "last_record_timestamp": 1742541936099,
      "scan_id": "9282cea5-39e8-cefa-d974-f2a2bd7ac70c9d992fe1d8037d1c"
    }
  ]
}
```


Tags Manifest File

```
{
    "type": "MANIFEST_TAGS",
    "payload_type": "TAGS",
    "payloads": [
        {
            "path": "path-prefix/tags/2024-09-23/tags-1727096866393-5.json.gz",
            "md5": "d641c41a287911d4779d1215edb2406d",
            "version": 1,
            "num_updates": 1,
            "num_deletes": 0,
            "first_record_timestamp": 1727096866345,
            "last_record_timestamp": 1727096866345,
            "scan_id": ""
        }
    ]
}
```


Web App Scanning Asset Manifest File


```
{
  "type": "MANIFEST_WAS_ASSET",
  "payload_type": "WAS_ASSET",
  "payloads": [
    {
      "path": "milestone/was_asset/2025-03-26/was_asset-1742967665045-19-8ad3db69-f2d6-4f53-abd8-
edcfd8bcaea4.json.gz",
      "md5": "9a5ce4f4aa2dc16fb89a0865236aef4c",
      "version": 1,
      "num_updates": 1,
      "num_deletes": 0,
      "first_record_timestamp": 1742967664402,
      "last_record_timestamp": 1742967664402,
      "scan_id": "8ad3db69-f2d6-4f53-abd8-edcfd8bcaea4"
    },
    {
      "path": "milestone/was_asset/2025-03-26/was_asset-1742967785809-8-987ab9a2-13ff-4ceb-806f-
cdd85d24c1ab.json.gz",
      "md5": "dba15c9adc1db1fc8393d60c63bab70d",
      "version": 1,
      "num_updates": 1,
      "num_deletes": 0,
      "first_record_timestamp": 1742967781319,
      "last_record_timestamp": 1742967781319,
      "scan_id": "987ab9a2-13ff-4ceb-806f-cdd85d24c1ab"
    },
    {
      "path": "milestone/was_asset/2025-03-26/was_asset-1742967791501-0-9fb210fa-5481-4ac4-895a-
3d9b62450062.json.gz",
      "md5": "ed32e90f74bd456a74390a0fff849b95",
      "version": 1,
      "num_updates": 1,
      "num_deletes": 0,
      "first_record_timestamp": 1742967786554,
      "last_record_timestamp": 1742967786554,
      "scan_id": "9fb210fa-5481-4ac4-895a-3d9b62450062"
    }
  ]
}
```

Web App Scanning Finding Manifest File


```
{
  "type": "MANIFEST_WAS_FINDING",
  "payload_type": "WAS_FINDING",
  "payloads": [
    {
      "path": "milestone/was_finding/2025-03-26/was_finding-1742967776983-105-8ad3db69-f2d6-4f53-
abd8-edcfd8bcaea4.json.gz",
      "md5": "dcf5f81f73dc5b61fce615114a162a71",
      "version": 1,
      "num_updates": 2,
      "num_deletes": 0,
      "first_record_timestamp": 1742967774285,
      "last_record_timestamp": 1742967774305,
      "scan_id": "8ad3db69-f2d6-4f53-abd8-edcfd8bcaea4"
    },
    {
      "path": "milestone/was_finding/2025-03-26/was_finding-1742967790057-87-9fb210fa-5481-4ac4-895a-
3d9b62450062.json.gz",
      "md5": "aa20d588c550ad683f790bc5721452a5",
      "version": 1,
      "num_updates": 3,
      "num_deletes": 0,
      "first_record_timestamp": 1742967785559,
      "last_record_timestamp": 1742967785559,
      "scan_id": "9fb210fa-5481-4ac4-895a-3d9b62450062"
    }
  ]
}
```


Assets Payload Files

When the system updates, adds, or deletes assets, Tenable Data Stream sends a payload file to your AWS bucket. In the file, updates appear in the `updates` array and deletions appear with a timestamp in the `deletes` array.

> **Note:** Asset deletions (host assets *and* WAS assets) appear in both the `assets` and `was_assets` folders. Ignore the asset IDs that are not relevant to you.

The following example shows the format of an assets payload file. For definitions of the properties in this file, see Assets Properties.


```
{
  "payload_id": "asset-1735809383052-16-f693e786-803c-4b52-9470-2f42939e8191",
  "version": 1,
  "type": "ASSET",
  "count_updated": 1,
  "count_deleted": 0,
  "updates": [
    {
```

```
      "id": "8d84147c-7086-4707-b644-33bd6a794f3c",
      "has_agent": false,
      "has_plugin_results": true,
      "created_at": "2024-05-16T09:54:57.453Z",
      "terminated_at": null,
      "terminated_by": null,
      "updated_at": "2025-01-02T09:16:09.872Z",
      "deleted_at": null,
      "deleted_by": null,
      "first_seen": "2024-05-16T09:54:53.000Z",
      "last_seen": "2025-01-02T09:16:09.872Z",
      "first_scan_time": "2024-05-16T09:54:53.000Z",
      "last_scan_time": "2025-01-02T09:16:09.872Z",
      "last_authenticated_scan_date": "2025-01-02T09:16:09.872Z",
      "last_licensed_scan_date": "2025-01-02T09:16:09.872Z",
      "last_scan_id": "f693e786-803c-4b52-9470-2f42939e8191",
      "last_schedule_id": "template-0c0f6be8-52e7-33a8-5efe-6c56590ade7c69dc748acb78459e",
      "last_scan_target": "target2.pubtarg.tenablesecurity.com",
      "last_authentication_attempt_date": "2025-01-02T09:16:09.872Z",
      "last_authentication_success_date": "2025-01-02T09:16:09.872Z",
      "last_authentication_scan_status": "Success",
      "agent_uuid": null,
      "bios_uuid": null,
      "network_id": "00000000-0000-0000-0000-000000000000",
      "azure_vm_id": null,
      "azure_resource_id": null,
      "gcp_project_id": null,
      "gcp_zone": null,
      "gcp_instance_id": null,
      "aws_ec2_instance_ami_id": null,
      "aws_ec2_instance_id": null,
      "network_name": null,
      "aws_owner_id": null,
      "aws_availability_zone": null,
      "aws_region": null,
      "aws_vpc_id": null,
      "aws_ec2_instance_group_name": null,
      "aws_ec2_instance_state_name": null,
      "aws_ec2_instance_type": null,
      "aws_subnet_id": null,
      "aws_ec2_product_code": null,
      "aws_ec2_name": null,
      "mcafee_epo_guid": null,
      "mcafee_epo_agent_guid": null,
      "servicenow_sysid": null,
      "bigfix_asset_id": null,
      "agent_names": [],
      "installed_software": [
        "cpe:/a:apache:http_server:2.4.58",
        "cpe:/a:openbsd:openssh:9.6",
        "cpe:/a:openbsd:openssh:9.6p1"
      ],
      "ipv4s": [
        "35.93.112.36"
      ],
      "ipv6s": [],
      "fqdns": [
        "target2.pubtarg.tenablesecurity.com"
      ],
      "mac_addresses": [],
      "netbios_names": [],
```

```
      "operating_systems": [
        "Linux Kernel 2.6"
      ],
      "system_types": [
        "general-purpose"
      ],
      "hostnames": [
        "target2.pubtarg.tenablesecurity.com"
      ],
      "ssh_fingerprints": [],
      "qualys_asset_ids": [],
      "qualys_host_ids": [],
      "manufacturer_tpm_ids": [],
      "symantec_ep_hardware_keys": [],
      "sources": [
        {
          "name": "AsgardPublisher",
          "first_seen": "2024-05-16T12:33:50.393Z",
          "last_seen": "2024-09-17T12:29:26.687Z"
        },
        {
          "name": "NessusScanEnrichment",
          "first_seen": "2024-09-03T13:00:27.000Z",
          "last_seen": "2024-11-21T14:32:31.000Z"
        },
        {
          "name": "NESSUS_SCAN",
          "first_seen": "2024-05-16T09:54:53.000Z",
          "last_seen": "2025-01-02T09:16:09.872Z"
        }
      ],
      "tags": [],
      "network_interfaces": [
        {
          "name": "CATCH_ALL_INTERFACE",
          "virtual": null,
          "aliased": null,
          "fqdns": [
            "target2.pubtarg.tenablesecurity.com"
          ],
          "mac_addresses": [],
          "ipv4s": [
            "35.93.112.36"
          ],
          "ipv6s": []
        }
      ],
      "open_ports": [
        {
          "port": 22,
          "protocol": "TCP",
          "service_names": [
            "ssh"
          ],
          "first_seen": "2024-05-16T09:54:53.492Z",
          "last_seen": "2024-11-21T14:32:31.480Z"
        },
        {
          "port": 80,
          "protocol": "TCP",
          "service_names": [
```

```
            "www"
          ],
          "first_seen": "2024-09-03T13:00:27.227Z",
          "last_seen": "2024-11-21T14:32:31.480Z"
        }
      ],
      "acr_score": "8",
      "exposure_score": "661",
      "custom_attributes": []
    }
  ],
  "deletes": [],
  "first_ts": "1735809378425",
  "last_ts": "1735809378425"
}
```


Assets Properties

The following table defines the properties in a Tenable Data Stream assets payload file. To see an example file, go to Assets Payload Files.

Property	Data Type	Description
payload_id	string	The ID of the payload sent from Tenable Vulnerability Management.
version	integer	The version of the payload. This number increments when the payload structure changes.
type	string	The type of payload, for example, `TAGS`.
count_updated	integer	The number of objects updated in the payload.
count_deleted	integer	The number of objects deleted in the payload.
updates[{}]	array of objects	Contains the objects updated in the payload; for example, assets or tags.
updates[].id	string	The UUID of the asset in Tenable Vulnerability Management. Use this value as the unique key for the asset.
updates[].has_agent	boolean	Specifies whether a Tenable Agent scan identified the asset.
updates[].has_	boolea	Specifies whether the asset has plugin results associated with

Property	Data Type	Description
`plugin_results`	n	it.
`updates[].created_at`	string	An ISO timestamp indicating the date and time when the system created the asset record.
`updates[].terminated_at`	string	An ISO timestamp indicating the date and time when a user terminated the Amazon Web Service (AWS) virtual machine instance of the asset.
`updates[].terminated_by`	string	The user who terminated the AWS instance of the asset.
`updates[].updated_at`	string	An ISO timestamp indicating the date and time when the asset record was last updated.
`updates[].deleted_at`	string	An ISO timestamp indicating the date and time when a user deleted the asset record. When a user deletes an asset record, the system retains the record until the asset ages out of the license count.
`updates[].deleted_by`	string	The user who deleted the asset record.
`updates[].first_seen`	string	An ISO timestamp indicating the date and time when a scan first identified the asset.
`updates[].last_seen`	string	An ISO timestamp indicating the date and time of the scan that most recently identified the asset.
`updates[].first_scan_time`	string	An ISO timestamp indicating the date and time of the first scan run against the asset.
`updates[].last_scan_time`	string	An ISO timestamp indicating the date and time of the last scan run against the asset.

Property	Data Type	Description
updates[].last_authenticated_scan_date	string	An ISO timestamp indicating the date and time of the last credentialed scan run on the asset.
updates[].last_licensed_scan_date	string	An ISO timestamp indicating the date and time of the last scan that identified the asset as licensed. The system categorizes an asset as licensed if a scan of that asset has returned results from a non-discovery plugin within the last 90 days.
updates[].last_scan_id	string	The UUID of the scan configuration used during the last scan of the asset.
updates[].last_scan_target	string	The IP address of the last target scanned.
updates[].acr_score	integer	(Tenable Lumin-only) The Asset Criticality Rating (ACR) for the asset.
updates[].exposure_score	integer	(Tenable Lumin-only) The Asset Exposure Score (AES) for the asset.
updates[].last_schedule_id	string	The `schedule_uuid` for the last scan of the asset.
updates[].last_scan_target	string	The IP address or fully qualified domain name (FQDN) of the asset targeted in the last scan.
updates[].last_	string	An ISO timestamp indicating the date and time when Tenable Nessus last attempted to sign in, either with SSH on Unix-

Property	Data Type	Description
authentication_attempt_date		based systems or SMB on Windows systems.
updates[].last_authentication_success_date	string	An ISO timestamp indicating the date and time when Tenable Nessus last successfully authenticated. Since agents do not log in, they do not update this property.
updates[].last_authentication_scan_status	string	Indicates if the last authentication attempt by Tenable Nessus was successful. Possible values are **Success**, **Failure**, and **N/A**. Since agents do not log in, they do not update this property.
updates[].azure_vm_id	string	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see Accessing and Using Azure VM Unique ID in the Microsoft Azure documentation.
updates[].azure_resource_id	string	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager documentation.
updates[].gcp_project_id	string	The unique identifier of the virtual machine instance in Google Cloud Platform (GCP).
updates[].gcp_instance_id	string	The customized name of the project to which the virtual machine instance belongs in GCP. For more information see Creating and Managing Projects in the GCP documentation.
updates[].aws_ec2_instance_ami_id	string	The zone where the virtual machine instance runs in GCP. For more information, see Regions and Zones in the GCP documentation.
updates[].aws_ec2_instance_id	string	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.
updates	string	This property represents the `tenable_uuid`. This identifier

Property	Data Type	Description
[].agent_uuid		can originate from either an agent or a credentialed remote Tenable Nessus scan. If no agent is present on the asset, a UUID is assigned by Tenable Vulnerability Management during a credentialed scan when the Create unique identifier on hosts scanned with credentials option is enabled. Note that no UUID is set for an uncredentialed non-agent scans.
updates [].bios_uuid	string	The BIOS UUID of the asset.
updates [].network_id	string	The ID of the network associated with the scanners that identified the asset. The default network ID is `00000000-0000-0000-0000-000000000000`. For more information about network objects, see Manage Networks.
updates[].aws_owner_id	string	The canonical user identifier for the AWS account associated with the virtual machine instance. For example, `79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`. For more information, see AWS Account Identifiers in the AWS documentation.
updates[].aws_availability_zone	string	The availability zone where Amazon Web Services hosts the virtual machine instance, for example, `us-east-1a`. Availability zones are subdivisions of AWS regions. For more information, see Regions and Availability Zones in the AWS documentation.
updates[].aws_region	string	The region where AWS hosts the virtual machine instance, for example, `us-east-1`. For more information, see "Regions and Availability Zones" in the AWS documentation.
updates[].aws_vpc_id	string	The unique identifier for the virtual public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.
updates[].aws_	string	The virtual machine instance's group in AWS.

Property	Data Type	Description
`ec2_instance_group_name`		
`updates[].aws_ec2_instance_state_name`	string	The state of the virtual machine instance in AWS at the time of the scan.
`updates[].aws_ec2_instance_type`	string	The type of instance in AWS EC2.
`updates[].aws_subnet_id`	string	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.
`updates[].aws_ec2_product_code`	string	The product code associated with the AMI used to launch the virtual machine instance in AWS EC2.
`updates[].aws_ec2_name`	string	The name of the virtual machine instance in AWS EC2.
`updates[].mcafee_epo_guid`	string	The unique identifier of the asset in McAfee ePolicy Orchestrator (ePO). For more information, see the McAfee documentation.
`updates[].mcafee_epo_agent_guid`	string	The unique identifier of the McAfee ePO agent that identified the asset. For more information, see the McAfee documentation.
`updates[].servicenow_sysid`	string	The unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.
`updates[].bigfix_asset_id[]`	string	The unique identifiers of the asset in HCL BigFix. For more information, see the HCL BigFix documentation.

Property	Data Type	Description
updates[].agent_names[]	array of strings	The names of any Tenable Agents that scanned and identified the asset.
updates[].installed_software[]	array of strings	A list of Common Platform Enumeration (CPE) values that represent software applications a scan identified as present on an asset. This attribute supports the CPE 2.2 format. For more information, see the "Component Syntax" section of the CPE Specification, Version 2.2. For assets identified in Tenable scans, this attribute contains data only if a scan using Nessus Plugin ID 45590 has evaluated the asset. **Note**: If no scan detects an application within 30 days of the scan that originally detected the application, Tenable Vulnerability Management considers the detection of that application expired. As a result, the next time a scan evaluates the asset, Tenable Vulnerability Management removes the expired application from the installed_software_attribute. This activity is logged as a `remove` type of `attribute_change` update in the asset activity log.
updates[].ipv4s[]	array of strings	The IPv4 addresses that scans have associated with the asset record.
updates[].ipv6s[]	array of strings	The IPv6 addresses that scans have associated with the asset record.
updates[].fqdns[]	array of strings	The fully-qualified domain names that scans have associated with the asset record.
updates[].mac_addresses[]	array of strings	The MAC addresses that scans have associated with the asset record.
updates[].netbios_names[]	array of strings	The NetBIOS names that scans have associated with the asset record.

Property	Data Type	Description
updates[].operating_systems[]	array of strings	The operating systems that scans have associated with the asset record.
updates[].system_types[]	array of strings	The system types as reported by Plugin ID 54615. Possible values include `router`, `general-purpose`, `scan-host`, and `embedded`.
updates[].hostnames[]	array of strings	The hostnames that scans have associated with the asset record.
updates[].ssh_fingerprints[]	array of strings	The SSH key fingerprints that scans have associated with the asset record.
updates[].qualys_asset_ids[]	array of strings	The Asset ID of the asset in Qualys. For more information, see the Qualys documentation.
updates[].qualys_host_ids[]	array of strings	The Host ID of the asset in Qualys. For more information, see the Qualys documentation.
updates[].manufacturer_tpm_ids[]	array of strings	The manufacturer's unique identifiers of the Trusted Platform Module (TPM) associated with the asset.
updates[].symantec_ep_hardware_keys[]	array of strings	The hardware keys for the asset in Symantec Endpoint Protection.
updates[].sources[{}]	array of objects	The sources of the scans that identified the asset. An asset source is the entity that reported the asset details. Sources can include sensors, connectors, and API imports. If your request specifies multiple sources, Tenable Vulnerability Management returns all assets seen by any of the specified

Property	Data Type	Description
		sources. The items in the sources array must correspond to the names of the sources as defined in your organization's implementation of Tenable Vulnerability Management. Commonly used names include: • **AWS** – The asset data was obtained from an Amazon Web Services connector. • **PVS** – The asset data from a Tenable Network Monitor scan. • **NESSUS_SCAN** – The asset data was obtained from a Tenable Nessus scan. • **WAS** – The asset data was obtained from a Tenable Web App Scanning scan. • **NESSUS_AGENT** – The asset data was obtained from a Tenable Agent scan.
`updates[].sources[].name`	string	The name of the entity that reported the asset details. Sources can include sensors, connectors, and API imports. Source names can be customized by your organization (for example, you specify a name when you import asset records). If your organization does not customize source names, the system-generated names include: • **AWS** – The asset data was obtained from an Amazon Web Services connector. • **PVS** – The asset data from a Tenable Network Monitor scan. • **NESSUS_SCAN** – The asset data was obtained from a Tenable Nessus scan.

Property	Data Type	Description
		• **WAS** – The asset data was obtained from a Tenable Web App Scanning scan. • **NESSUS_AGENT** – The asset data was obtained from a Tenable Agent scan.
`updates[].sources[].first_seen`	string	An ISO timestamp indicating the date and time when the source first reported the asset.
`updates[].sources[].last_seen`	string	An ISO timestamp indicating the date and time when the source last reported the asset.
`updates[].network_interfaces[{}]`	array of objects	The network interfaces that scans identified on the asset.
`updates[].network_interfaces.name`	string	The name of the interface.
`updates[].network_interfaces[].mac_addresses`	array of strings	The MAC addresses of the interface.
`updates[].network_interfaces[].ipv6s`	array of strings	One or more IPv6 addresses belonging to the interface.
`updates[].network_`	array of strings	One or more IPv4 addresses belonging to the interface.

Property	Data Type	Description
`interfaces[].ipv4s`		
`updates[].network_interfaces[].fqdns`	array of strings	One or more FQDNs belonging to the interface.
`updates[].network_interfaces.virtual`	boolean	If a virtual name exists for the interface.
`updates[].network_interfaces.aliased`	boolean	If an alias exists for the interface.
`updates[].open ports`	array of objects	An array of open ports and their services as reported by the info-level plugins. For more information about open ports reported by info-level plugins, see Open Ports and the Assets Workbench.
`updates[].open_ports[].port`	integer	The open port number.
`updates[].open_ports[].protocol`	string	The communication protocol corresponding to the open port.
`updates[].open_ports[].service_names`	array of strings	The names of the services associated with the open port.

Property	Data Type	Description
updates[].gcp_zone	string	The customized name of the project to which the virtual machine instance belongs in GCP. For more information see "Creating and Managing Projects" in the GCP documentation.
updates[].network_name	string	The ID of the network object associated with scanners that identified the asset. The default network name is `Default`. All other network names are user-defined.
updates[].open_ports[].first_seen	string	An ISO timestamp indicating the date and time when the source first detected the open port on the asset.
updates[].open_ports[].last_seen	string	An ISO timestamp indicating the date and time when the source last detected the open port on the asset.
updates[].custom_attributes	array of objects	Custom attributes for the asset.
updates[].custom_attributes[].id	string	The custom ID for the asset.
updates[].custom_attributes[].value	string	The custom value for the asset.
updates[].tags	array of objects	Object containing the tags for the asset. **Note**: The `tags` object is always empty and appears to maintain compatibility with the Tenable API. Your tag data is sent in the tags payload file.
updates[].tags	string	The UUID of the tag.

Property	Data Type	Description
`[].uuid`		
`updates[].tags[].key`	string	The tag category.
`updates[].tags[].value`	string	The tag value.
`updates[].tags[].added_by`	string	The UUID of the user who assigned the tag to the asset.
`updates[].tags[].added`	string	An ISO timestamp indicating the date and time when the tag was assigned to the asset.
`deletes[]`	array of objects	Contains any assets deleted in the payload, along with their `_id` and a timestamp.
`deletes[].id`	string	The UUID of the deleted asset in Tenable Vulnerability Management.
`deletes[].deleted_at`	string	An ISO timestamp indicating the date and time of the data deletion.
`first_ts`	string	A Unix timestamp indicating the date and time of the first entry in the payload.
`last_ts`	string	A Unix timestamp indicating the date and time of the last entry in the payload.

.

Asset Enriched Attributes Payload Files

When the system adds, edits, or deletes asset attributes, Tenable Data Stream sends a payload file to your AWS bucket. In the file, updates appear in the `updates` array and deletes appear with a timestamp in the `deletes` array.

The following example shows the format of an ASSET_ENRICHED_ATTRIBUTES payload file. For definitions of the properties in this file, see Asset Enriched Attributes Properties.

```
{
    "payload_id": "asset_enriched_attributes-1751265865888-0",
    "version": 1,
    "type": "ASSET_ENRICHED_ATTRIBUTES",
    "count_updated": 1,
    "count_deleted": 0,
    "updates": [
        {
            "asset_id": "8be86514-cc16-42fa-b832-56bf96c66df5",
            "ratings": {
                "aes": {
                    "score": 572.0
                },
                "acr": {
                    "score": 4.0
                }
            },
            "product": "VM"
        }
    ],
    "deletes": [],
    "first_ts": "1751223659279",
    "last_ts": "1751223659300"
}
```


Asset Enriched Attributes Properties

The following table defines the properties in a Tenable Data Stream asset_enriched_attributes payload file. To see an example, go to Asset Enriched Attributes Payload Files.

Property	Data Type	Description
payload_id	string	The ID of the payload sent from Tenable Vulnerability Management.
version	integer	The version of the payload. This number increments when the payload structure changes.
type	string	The type of payload, for example, `ASSET_ENRICHED_ATTRIBUTES`.
count_updated	integer	The number of objects updated in the payload.
count_deleted	integer	The number of objects deleted in the payload.
updates[{}]	array of objects	Contains the objects updated in the payload.

Property	Data Type	Description
updates[].asset_id	string	The UUID of the asset for which the system updated an asset. Use this value as the unique key for the asset.
updates[{}].ratings	object	Contains information about asset scores.
updates[].ratings.aes.score	number	The Asset Exposure Score (AES) for the asset.
updates[].ratings.acr.score	number	The Asset Criticality Rating (ACR) for the asset.
updates[].product	string	The product the asset applies to, for example, `VM` for Tenable Vulnerability Management or `WAS` for Tenable Web App Scanning
deletes[]	array	Contains asset attributes deleted in the payload.
deletes[].id	string	Indicates the ID for the deleted asset attribute.
deletes[].deleted_at	string	An ISO timestamp indicating the date and time when the asset attribute was deleted.
first_ts	integer	A Unix timestamp indicating the date and time of the first entry in the payload.
last_ts	integer	A Unix timestamp indicating the date and time of the last entry in the payload.

Findings Payload Files

When the system adds, updates, or deletes findings associated with assets, Tenable Data Stream sends a payload file to your AWS bucket. In the file, updates appear in the `updates` array and deletes appear with a timestamp in the `deletes` array.

The following example shows the format of a findings payload file. For definitions of the properties in this file, see Findings Properties.

```
{
  "payload_id": "finding-1735809381920-24-f693e786-803c-4b52-9470-2f42939e8191",
  "version": 1,
  "type": "FINDING",
  "count_updated": 1,
  "count_deleted": 0,
  "updates": [
    {
      "finding_id": "4e4d4dd2-e8a3-5c6a-9d32-f5864e8aef52",
      "asset": {
        "agent_uuid": null,
        "bios_uuid": null,
        "device_type": "general-purpose",
        "fqdn": "target2.pubtarg.tenablesecurity.com",
        "hostname": "target2.pubtarg.tenablesecurity.com",
        "uuid": "8d84147c-7086-4707-b644-33bd6a794f3c",
        "ipv4": "35.93.112.36",
        "ipv6": null,
        "last_authenticated_results": null,
        "last_unauthenticated_results": null,
        "last_scan_target": "target2.pubtarg.tenablesecurity.com",
        "mac_address": null,
        "netbios_name": null,
        "netbios_workgroup": [],
        "operating_system": [
          "Linux Kernel 2.6"
        ],
        "network_id": "00000000-0000-0000-0000-000000000000",
        "tracked": true
      },
      "output": null,
      "plugin": {
        "bid": [70657],
        "canvas_package": null,
        "checks_for_default_account": false,
        "checks_for_malware": false,
        "cpe": [],
        "cve": null,
        "cvss4_base_score": 8.6,
        "cvss4_threat_vector": {
            "threat_score": 6.1,
            "exploit_maturity": "Unreported",
            "raw": "CVSS:4.0/E:U"
        },
        "cvss4_vector":{
           "attack_vector":"Network",
           "attack_complexity":"Low",
           "attack_requirements":"None",
           "privileges_required":"None",
           "user_interaction":"None",
           "vulnerable_system_confidentiality":"High",
           "vulnerable_system_integrity":"High",
           "vulnerable_system_availability":"High",
           "subsequent_system_confidentiality":"None",
           "subsequent_system_integrity":"None",
           "subsequent_system_availability":"None",
           "raw":"AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N"
        },
        "cvss3_base_score": null,
        "cvss3_temporal_score": null,
        "cvss3_temporal_vector": {
```

```
          "exploitability": null,
          "remediation_level": null,
          "report_confidence": null,
          "raw": null
        },
        "cvss3_vector": {
          "access_complexity": null,
          "access_vector": null,
          "privileges_required": null,
          "user_interaction": null,
          "scope": null,
          "availability_impact": null,
          "confidentiality_impact": null,
          "integrity_impact": null,
          "raw": null
        },

        "cvss_base_score": null,
        "cvss_temporal_score": null,
        "cvss_temporal_vector": {
          "exploitability": null,
          "remediation_level": null,
          "report_confidence": null,
          "raw": null
        },
        "cvss_vector": {
          "access_complexity": null,
          "access_vector": null,
          "authentication": null,
          "availability_impact": null,
          "confidentiality_impact": null,
          "integrity_impact": null,
          "raw": null
        },
        "d2_elliot_name": null,
        "description": "This script detects which algorithms and languages are supported by the
remote service for encrypting communications.",
        "epss_score": 0.00553,
        "exploit_available": false,
        "exploit_framework_canvas": false,
        "exploit_framework_core": false,
        "exploit_framework_d2_elliot": false,
        "exploit_framework_exploithub": false,
        "exploit_framework_metasploit": false,
        "exploitability_ease": null,
        "exploited_by_malware": false,
        "exploited_by_nessus": false,
        "exploithub_sku": null,
        "family": "Misc.",
        "family_id": null,
        "has_patch": false,
        "id": 70657,
        "in_the_news": false,
        "metasploit_name": null,
        "ms_bulletin": null,
        "name": "SSH Algorithms and Languages Supported",
        "patch_publication_date": "null",
        "modification_date": "2017-08-28T00:00:00Z",
        "publication_date": "2013-10-28T00:00:00Z",
        "risk_factor": "info",
        "see_also": [],
        "solution": null,
```

```
        "stig_severity": null,
        "synopsis": "An SSH server is listening on this port.",
        "type": "remote",
        "unsupported_by_vendor": false,
        "usn": null,
        "version": "null",
        "vuln_publication_date": "null",
        "xrefs": [],
        "vpr": {
          "score": null,
          "drivers": {
            "age_of_vuln": {
              "lower_bound": 0,
              "upper_bound": 0
            },
            "exploit_code_maturity": null,
            "cvss_impact_score_predicted": null,
            "cvss3_impact_score": null,
            "threat_intensity_last28": null,
            "threat_recency": {
              "lower_bound": 0,
              "upper_bound": 0
            },
            "threat_sources_last28": [],
            "product_coverage": null
          },
          "updated": "null"
        },
        "vpr_v2": {
          "score": 3,
          "vpr_percentile": "22.61",
          "vpr_severity": "LOW",
          "exploit_probability": 0,
          "cve_id": "CVE-2024-23314",
          "exploit_code_maturity": "UNPROVEN",
          "on_cisa_kev": false,
          "in_the_news_intensity_last30": "VERY LOW",
          "in_the_news_recency": "NO RECORDED EVENTS",
          "malware_observations_intensity_last30": "VERY LOW",
          "malware_observations_recency": "NO RECORDED EVENTS",
          "in_the_news_sources_last30": [
              "Blogs & Individual Researchers",
                "Cyber News & Media",
                "Security Research, Tools & Resources"
          ],
          "exploit_chain": [
              "CVE-2024-44309"
          ],
           "threat_summary": {
              "summary": "null",
              "lastUpdated": "null"
          },
          "remediation": {
              "summary": "null",
              "lastUpdated": "null"
          },
          "targeted_industries": [
              "Energy",
              "Government",
              "Government - Federal",
              "Government - State/Local",
```

```
              "Healthcare",
              "Insurance",
              "Legal Services"
           ],
           "targeted_regions": [
              "Europe",
              "Germany",
              "North America",
              "Russia",
              "Ukraine",
              "United States"
           ]
         },
         "workaround": "Workaround description",
         "workaround_type": "Configuration Change",
         "workaround_published": "2025-01-02T09:11:11.756Z",
         "has_workaround": false
       },
       "port": {
         "port": 22,
         "protocol": "TCP",
         "service": "ssh"
       },
       "recast_reason": null,
       "recast_rule_uuid": null,
       "scan": {
         "schedule_uuid": "template-0c0f6be8-52e7-33a8-5efe-6c56590ade7c69dc748acb78459e",
         "started_at": "2025-01-02T09:11:11.756Z",
         "uuid": "f693e786-803c-4b52-9470-2f42939e8191",
         "target": "target2.pubtarg.tenablesecurity.com"
       },
       "severity": "info",
       "severity_id": 0,
       "severity_default_id": 0,
       "severity_modification_type": "NONE",
       "first_found": "2024-05-16T09:54:53.492Z",
       "last_fixed": "2025-01-02T09:16:09.872Z",
       "last_found": "2024-11-21T14:32:31.480Z",
       "indexed": "2025-01-02T09:16:22.207Z",
       "state": "FIXED",
       "source": "NESSUS",
       "resurfaced_date": "2024-12-27T11:57:24.384Z",
       "time_taken_to_fix": 4045860
     }
   ],
   "deletes": [],
   "first_ts": "1735809379276",
   "last_ts": "1735809379276"
}
```


Findings Properties

The following table defines the properties in a Tenable Data Stream findings payload file. To see an example file, go to Findings Payload Files.

Property	Data Type	Description
payload_id	string	The ID of the payload sent from Tenable Vulnerability Management.
version	integer	The version of the payload. This number increments when the payload structure changes.
type	string	The type of data in the payload; for example, `FINDING`.
count_updated	integer	The number of updated findings in the payload.
count_deleted	integer	The number of deleted findings in the payload.
updates[{}]	array of objects	Contains the tags updated in the payload.
updates[].finding_id	string	The unique identifier for the finding.
updates[].asset.agent_uuid	string	The UUID of the agent that performed the scan where the vulnerability was found.
updates[].asset.bios_uuid	string	The BIOS UUID of the asset where the vulnerability was found.
updates[].asset.device_type	string	The type of asset where the vulnerability was found.
updates[].asset.fqdn	string	The fully-qualified domain name of the asset where a scan found the vulnerability.
updates[].asset.hostname	string	The host name of the asset where a scan found the vulnerability.
updates[].asset.uuid	string	The UUID of the asset where a

Property	Data Type	Description
		scan found the vulnerability.
`updates[].asset.ipv4`	string	The IPv4 address of the asset where a scan found the vulnerability.
`updates[].asset.ipv6`	string	The IPv6 address of the asset where a scan found the vulnerability.
`updates[].asset.last_authenticated_results`	string	An ISO timestamp indicating the date and time when credentials were last successfully used to scan the asset.
`updates[].asset.last_unauthenticated_results`	string	An ISO timestamp indicating the date and time when the asset was scanned without using credentials.
`updates[].scan_target`	string	The IP address or fully qualified domain name (FQDN) of the asset targeted in the last scan.
`updates[].asset.mac_address`	string	The MAC address of the asset where a scan found the vulnerability.
`updates[].asset.netbios_name`	string	The NETBIOS name of the asset where a scan found the vulnerability.
`updates[].asset.netbios_workgroup[]`	string array	The NETBIOS workgroup of the asset where a scan found the vulnerability.
`updates[].asset.operating_system[]`	array of strings	The operating system of the asset where a scan found the vulnerability.

Property	Data Type	Description
updates[].asset.network_id	string	The ID of the network associated with the scanners that identified the asset. The default network ID is `00000000-0000-0000-0000-000000000000`. For more information about network objects, see Networks.
updates[].asset.tracked	boolean	A value specifying whether Tenable Vulnerability Management tracks the asset in the asset management system. Tenable Vulnerability Management still assigns untracked assets identifiers in scan results, but these identifiers change with each new scan of the asset. This parameter is relevant to PCI-type scans and in certain cases where there is not enough information in a scan to identify the asset. Untracked assets appear in the scan history, but do not appear in workbenches or reports.
updates[].output	string	The text output of the Nessus scanner.
updates[].plugin	object	Information about the plugin that detected the vulnerability.
updates[].plugin.epss_score	number	The Exploit Prediction Scoring System (EPSS) score of the finding.
updates[].plugin.bid[]	array of integers	The Bugtraq ID for the plugin.

Property	Data Type	Description
`updates[].plugin.canvas_package`	string	The name of the CANVAS exploit pack that includes the vulnerability.
`updates[].plugin.checks_for_default_account`	boolean	A value specifying whether the plugin checks for default accounts.
`updates[].plugin.checks_for_malware`	boolean	A value specifying whether the plugin checks for malware.
`updates[].plugin.cpe[]`	array of strings	The Common Platform Enumeration (CPE) numbers for the plugin.
`updates[].plugin.cve[]`	array of strings	The Common Vulnerability and Exposure (CVE) IDs for the plugin.
`updates[].plugin.cvss4_base_score`	number	The CVSS v4.0 base score (intrinsic and fundamental characteristics of a finding that are constant over time and user environments).
`updates[].plugin.cvss4_vector`	object	Additional CVSS v4.0 metrics for the vulnerability.
`updates[].plugin.cvss4_vector.attack_vector`	string	The context where vulnerability exploitation is possible, such as **Network** or **Local**.
`updates[].plugin.cvss4_vector.attack_complexity`	string	The conditions beyond the attacker's control that must exist to exploit the vulnerability.
`updates[].plugin.cvss4_vector.attack_requirements`	string	The resources, access, or specialized conditions required for an attacker to exploit the vulnerability.

Property	Data Type	Description
`updates[].plugin.cvss4_vector.privileges_required`	string	The permission level attackers require to exploit the vulnerability. Options are **High**, **Low**, or **None**. For example, **None** means attackers need no permissions in your environment and can exploit the vulnerability while unauthorized.
`updates[].plugin.cvss4_vector.user_interaction`	string	The level of user involvement required for an attacker to exploit the vulnerability.
`updates[].plugin.cvss4_vector.vulnerable_system_availability`	string	The impact on the availability of the vulnerable system when successfully exploited.
`updates[].plugin.cvss4_vector.vulnerable_system_confidentiality`	string	The impact on the confidentiality of the vulnerable system when successfully exploited.
`updates[].plugin.cvss4_vector.vulnerable_system_integrity`	string	The impact on the integrity of the vulnerable system when successfully exploited.
`updates[].plugin.cvss4_vector.subsequent_system_availability`	string	The impact on the availability of systems that can be impacted after the vulnerable system is exploited.
`updates[].plugin.cvss4_vector.subsequent_system_confidentiality`	string	The impact on the confidentiality of systems that can be impacted after the vulnerable system is exploited.
`updates[].plugin.cvss4_vector.subsequent_system_integrity`	string	The impact on the integrity of systems that can be impacted after the vulnerable system is exploited.

Property	Data Type	Description
updates[].plugin.cvss4_vector.raw	string	The complete `cvss4_vector` metrics and result values for the vulnerability the plugin covers in a condensed and coded format. For example, `AV:N/AC:M/Au:N/C:C/I:C/A:C`.
updates[].plugin.cvss4_threat_vector	object	An object representing the CVSS v4.0 Threat metrics for the vulnerability. These metrics provide context on current, observed threat activity in the wild, such as evidence of exploitation or the presence of available exploit code. Threat metrics can help refine the severity and prioritization of vulnerabilities beyond their intrinsic characteristics. For more details, see the CVSS v4.0 Specification.
updates[].plugin.cvss4_threat_vector.exploit_maturity	string	The CVSS v4.0 Exploit Maturity (E) metric, indicating the current development status of exploit techniques or code for the vulnerability. For more details, see the CVSS v4.0 Specification.
updates[].plugin.cvss4_threat_vector.raw	string	The complete `cvss4_threat_vector` metrics and their result values for the vulnerability, expressed as a concise, coded string. This threat vector is typically appended to the CVSSv4 Base vector. For example, `CVSS:4.0/E:U`. For more details,

Property	Data Type	Description
		see the CVSS v4.0 Specification.
`updates[].plugin.cvss4_threat_vector.threat_score`	string	The CVSS v4.0 threat score (CVSS-T), which adjusts the base score by incorporating real-world threat intelligence, such as the presence of active exploitation, exploit code availability, or observed malware activity. This score reflects the current threat landscape for the vulnerability. For more details, see the CVSS v4.0 Specification.
`updates[].plugin.cvss3_base_score`	float	The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
`updates[].plugin.cvss3_temporal_score`	float	The CVSSv3 temporal score (characteristics of a vulnerability that change over time but not among user environments).
`updates[].plugin.cvss3_temporal_vector`	object	CVSSv3 temporal metrics for the vulnerability.
`updates[].plugin.cvss3_temporal_vector.exploitability`	string	The CVSSv3 Exploit Maturity Code (E) for the vulnerability the plugin covers. Possible values include: • **Unproven** – Corresponds to the Unproven (U) value for the E metric • **Proof-of-concept** – Corresponds to the Proof-of-

Property	Data Type	Description
		Concept (POC) value for the E metric • **Functional** – Corresponds to the Functional (F) value for the E metric • **High** – Corresponds to the High (H) value for the E metric • **Not-defined** – Corresponds to the Not Defined (ND) value for the E metric
`updates[].plugin.cvss3_temporal_vector.remediation_level`	string	The CVSSv3 Remediation Level (RL) temporal metric for the vulnerability the plugin covers. Possible values include: • **O** – Official Fix • **T** – Temporary Fix • **W** – Workaround • **U** – Unavailable • **X** – Not Defined
`updates[].plugin.cvss3_temporal_vector.report_confidence`	string	The CVSSv3 Report Confidence (RC) temporal metric for the vulnerability the plugin covers. Possible values include: • **U** – Unknown • **R** – Reasonable • **C** – Confirmed

Property	Data Type	Description
		• **X** – Not Defined
updates[].plugin.cvss3_temporal_vector.raw	string	The complete `cvss3_temporal_vector` metrics and result values for the vulnerability the plugin covers in a condensed and coded format. For example, `E:U/RL:OF/RC:C`.
updates[].plugin.cvss3_vector	object	Additional CVSSv3 metrics for the vulnerability.
updates[].plugin.cvss3_vector.access_complexity	string	The CVSSv3 Access Complexity (AC) metric for the vulnerability the plugin covers. Possible values are: • **H** – High • **M** – Medium • **L** – Low
updates[].plugin.cvss3_vector.access_vector	string	The CVSSv2 Attack Vector (AV) metric for the vulnerability the plugin covers. Possible values are: • **Network** – Corresponds to the Network (N) value for the AV metric. • **Adjacent Network** – Corresponds to the Adjacent Network (A) value for the AV metric. • **Local** – Corresponds to the Local (L) value for the AV metric

Property	Data Type	Description
updates[].plugin.cvss3_vector.privileges_required	string	Level of privilege required to exploit this vulnerability. Possible values are `L` for low, `H` for high, and `None` for no access privileges required.
updates[].plugin.cvss3_vector.user_interaction	string	The user interaction required for exploitability.
updates[].plugin.cvss3_vector.scope	string	If the vulnerability can affect other assets or only the asset it was found on. Possible values are `U` for unchanged and C for changed (meaning that the vulnerability can affect other assets).
updates[].plugin.cvss3_vector.availability_impact	string	The CVSSv2 availability impact metric for the vulnerability the plugin covers. Possible values include: • **H** – High • **L** – Low • **N** – None
updates[].plugin.cvss3_vector.confidentiality_impact	string	The CVSSv3 confidentiality impact metric of the vulnerability the plugin covers to the vulnerable component. Possible values include: • **H** – High • **L** – Low • **N** – None
updates[].plugin.cvss3_	string	The CVSSv3 integrity impact metric

Property	Data Type	Description
vector.integrity_impact		for the vulnerability the plugin covers. Possible values include: • **H** – High • **L** – Low • **N** – None
updates[].plugin.cvss3_vector.raw	string	The complete `cvss3_vector metrics` and result values for the vulnerability the plugin covers in a condensed and coded format. For example, `AV:N/AC:M/Au:N/C:C/I:C/A:C`.
updates[].plugin.cvss_base_score	float	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
updates[].plugin.cvss_temporal_score	float	The CVSSv2 temporal score (characteristics of a vulnerability that change over time but not among user environments).
updates[].plugin.cvss_temporal_vector	object	CVSSv2 temporal metrics for the vulnerability.
updates[].plugin.cvss_temporal_vector.exploitability	string	The CVSSv2 Exploitability (E) temporal metric for the vulnerability the plugin covers. Possible values include: • **U**–Unproven • **POC** – Proof-of-Concept • **F** – Functional

Property	Data Type	Description
		• **H** – High • **ND** – Not Defined
updates[].plugin.cvss_temporal_vector.remediation_level	string	The CVSSv2 Remediation Level (RL) temporal metric for the vulnerability the plugin covers. Possible values include: • **OF** – Official Fix • **TF** – Temporary Fix • **W** – Workaround • **U** – Unavailable • **ND** – Not Defined
updates[].plugin.cvss_temporal_vector.report_confidence	string	The CVSSv2 Report Confidence (RC) temporal metric for the vulnerability the plugin covers. Possible values include: • **UC** – Unconfirmed • **UR** – Uncorroborated • **C** – Confirmed • **ND** – Not Defined
updates[].plugin.cvss_temporal_vector.raw	string	The complete `cvss_temporal_vector` metrics and result values for the vulnerability the plugin covers in a condensed and coded format. For example, `E:U/RL:OF/RC:C`.
updates[].plugin.cvss_vector.access_complexity	string	The CVSSv2 Access Complexity (AC) metric for the vulnerability the

Property	Data Type	Description
		plugin covers. Possible values include: • **H** – High • **M** – Medium • **L** – Low
`updates[].plugin.cvss_vector.access_vector`	string	The CVSSv2 Access Vector (AV) metric for the vulnerability the plugin covers. Possible values include: • **L** – Local • **A** – Adjacent Network • **N** – Network
`updates[].plugin.cvss_vector.authentication`	string	The CVSSv2 Authentication (Au) metric for the vulnerability the plugin covers. Possible values include: • **N** – None • **S** – Single • **M** – Multiple
`updates[].plugin.cvss_vector.availability_impact`	string	The CVSSv2 availability impact metric for the vulnerability the plugin covers. Possible values include: • **N** – None • **P** – Partial • **C** – Complete

Property	Data Type	Description
updates[].plugin.cvss_vector.confidentiality_impact	string	The CVSSv2 confidentiality impact metric for the vulnerability the plugin covers. Possible values include: • **N** – None • **P** – Partial • **C** – Complete
updates[].plugin.cvss_vector.integrity_impact	string	The CVSSv2 integrity impact metric for the vulnerability the plugin covers. Possible values include: • **N** – None • **P** – Partial • **C** – Complete
updates[].plugin.cvss_vector.raw	string	The complete `cvss_vector` `metrics` and result values for the vulnerability the plugin covers in a condensed and coded format. For example, `AV:N/AC:M/Au:N/C:C/I:C/A:C`.
updates[].plugin.d2_elliot_name	string	The name of the exploit in the D2 Elliot Web Exploitation framework.
updates[].plugin.description	string	Full text description of the vulnerability.
updates[].plugin.exploit_available	boolean	A value specifying whether a public exploit exists for the vulnerability.
updates[].plugin.exploit_framework_canvas	boolean	A value specifying whether an exploit exists in the Immunity CANVAS framework.

Property	Data Type	Description
updates[].plugin.exploit_framework_core	boolean	A value specifying whether an exploit exists in the CORE Impact framework.
updates[].plugin.exploit_framework_d2_elliot	boolean	A value specifying whether an exploit exists in the D2 Elliot Web Exploitation framework.
updates[].plugin.exploit_framework_exploithub	boolean	A value specifying whether an exploit exists in the ExploitHub framework.
updates[].plugin.exploit_framework_metasploit	boolean	A value specifying whether an exploit exists in the Metasploit framework.
updates[].plugin.exploitability_ease	string	Description of how easy it is to exploit the issue.
updates[].plugin.exploited_by_malware	boolean	The vulnerability discovered by this plugin is known to be exploited by malware.
updates[].plugin.exploited_by_nessus	boolean	A value specifying whether Nessus exploited the vulnerability during the process of identification.
updates[].plugin.exploithub_sku	string	The SKU number of the exploit in the ExploitHub framework.
updates[].plugin.family	string	The family to which plugin belongs.
updates[].plugin.family_id	integer	The ID of the plugin family.
updates[].plugin.has_patch	boolean	A value specifying whether the vendor has published a patch for the vulnerability.
updates[].plugin.id	integer	The ID of the plugin that identified

Property	Data Type	Description
		the vulnerability.
updates[].plugin.in_the_news	boolean	A value specifying whether this plugin has received media attention (for example, ShellShock, Meltdown).
updates[].plugin.metasploit_name	string	The name of the related exploit in the Metasploit framework.
updates[].plugin.ms_bulletin	array of strings	The Microsoft security bulletin that the plugin covers.
updates[].plugin.name	string	The name of the plugin that identified the vulnerability.
updates[].plugin.patch_publication_date	string	An ISO timestamp indicating the date and time when the vendor published a patch for the vulnerability.
updates[].plugin.modification_date	string	An ISO timestamp indicating the date and time when the plugin was last modified.
updates[].plugin.publication_date	string	An ISO timestamp indicating the date and time when the plugin was published.
updates[].plugin.risk_factor	string	The risk factor associated with the plugin. Possible values are: `Low`, `Medium`, `High`, or `Critical`. See the `risk_factor` attribute in Tenable Plugin Attributes.
updates[].plugin.see_also[]	array of strings	Links to external websites that contain helpful information about the vulnerability.

Property	Data Type	Description
updates[].plugin.solution	string	Remediation information for the vulnerability.
updates[].plugin.stig_severity	string	Security Technical Implementation Guide (STIG) severity code for the vulnerability.
updates[].plugin.synopsis	string	Brief description of the plugin or vulnerability.
updates[].plugin.type	string	The general type of plugin check (for example, `local` or `remote`).
updates[].plugin.unsupported_by_vendor	boolean	Software found by this plugin is unsupported by the software's vendor (for example, Windows 95 or Firefox 3).
updates[].plugin.usn	string	Ubuntu security notice that the plugin covers.
updates[].plugin.version	string	The version of the plugin used to perform the check.
updates[].plugin.vuln_publication_date	string	An ISO timestamp indicating the date and time when the plugin was published.
updates[].plugin.xrefs[]	array of objects	References to third-party information about the vulnerability, exploit, or update associated with the plugin. Each reference includes a type and an ID. For example, 'FEDORA' and '2003-047'. This object can include `type` and `id` fields.

Property	Data Type	Description
`updates[].plugin.xrefs[].type`	string	The type of reference.
`updates[].plugin.xrefs[].id`	string	The ID for the reference.
`updates[].plugin.vpr_v2`	object	An object containing information about the Vulnerability Priority Rating (VPRv2) for the vulnerability.
`updates[].plugin.vpr_v2.score`	number	The Vulnerability Priority Rating (VPRv2) for the vulnerability. If a plugin is designed to detect multiple vulnerabilities, the VPR score represents the highest value calculated for a vulnerability associated with the plugin. For more information, see Tenable Metrics in the *Tenable Vulnerability Management User Guide*.
`updates[].plugin.vpr_v2.vpr_percentile`	string	Filter on the VPR v2 score percentile ranking of the CVE, indicating its position relative to other vulnerabilities.
`updates[].plugin.vpr_v2.vpr_severity`	string	Filter on the VPR v2 severity categorization of the CVE. Options are **Critical**, **High**, **Medium**, **Low**, **Info**.
`updates[].plugin.vpr_v2.exploit_probability`	number	Filter on the probability of exploitation produced by the VPR v2 threat model for the CVE.
`updates[].plugin.vpr_v2.cve_id`	string	Filter on a specific CVE ID for the CVE that is a primary contributor to the calculated VPRv2 score for a

Property	Data Type	Description
		vulnerability.
`updates[].plugin.vpr_v2.exploit_code_maturity`	string	Filter on current availability and maturity of exploit code. Options are **High**, **Functional**, **POC**, and **Unproven**.
`updates[].plugin.vpr_v2.on_cisa_kev`	boolean	Filter on whether the CVE is listed on the CISA Known Exploited Vulnerabilities list. Options are **Yes**, **No**.
`updates[].plugin.vpr_v2.exploit_chain[]`	array of strings	Allows filtering on CVEs that are part of an exploit chain.
`updates[].plugin.vpr_v2.in_the_news_intensity_last30`	string	Allows filtering on the volume of news reporting on the CVE within the last 30 days. Options are **Very Low**, **Low**, **Medium**, **High**, **Very High**.
`updates[].plugin.vpr_v2.in_the_news_recency`	string	Allows filtering on the recency of news sources reporting on the CVE. Options are **No Recorded Events**, **60 to 180 days**, **30 to 60 days**, **14 to 30 days**, **7 to 14 days**, **0 to 7 days**.
`updates[].plugin.vpr_v2.in_the_news_sources_last30[]`	array of strings	Filter on categories of news sources that have referenced the CVE within the last 30 days. Select from one or more of **Academic and Research Institutions**, **Blogs and Individual Researchers**, **Code Repositories**, **Cybersecurity News Media**, **Cybersecurity Vendors**,

Property	Data Type	Description
		Forums and Community Platforms, **Government and Regulatory**, **Mainstream News and Media**, **Security Research**, **Technology Companies**, **Tools and Resources**, **Other**.
`updates[].plugin.vpr_v2.malware_observations_intensity_last30`	string	Filter on the volume of observed malware exploiting the CVE within the last 30 days. Options are **Very Low**, **Low**, **Medium**, **High**, **Very High**.
`updates[].plugin.vpr_v2.malware_observations_recency`	string	Filter on the recency of observed malware exploiting the CVE. Options are **No Recorded Events**, **60 to 180 days**, **30 to 60 days**, **14 to 30 days**, **7 to 14 days**, **0 to 7 days**.
`updates[].plugin.vpr_v2.threat_summary[]`	object	The object container for information about the threat posed by the vulnerability, including relevant details that contribute to its Vulnerability Priority Rating (VPR) v2 score.
`updates[].plugin.vpr_v2.threat_summary[].summary`	string	Information about the threat posed by the vulnerability, including relevant details that contribute to its Vulnerability Priority Rating (VPR) v2 score.
`updates[].plugin.vpr_v2.threat_summary[].lastUpdated`	string	Most recent update to threat summary information.

Property	Data Type	Description
`updates[].plugin.vpr_v2.remediation[]`	object	The object container for information and recommended actions for mitigating or resolving the vulnerability. This may include patches, configuration changes, or other remediation guidance.
`updates[].plugin.vpr_v2.remediation[].summary`	string	Information and recommended actions for mitigating or resolving the vulnerability. This may include patches, configuration changes, or other remediation guidance.
`updates[].plugin.vpr_v2.remediation[].last_updated`	string	Most recent update to remediation summary information.
`updates[].plugin.vpr_v2.targeted_industries[]`	array of strings	Allows filtering on specific industries where attacks leveraging the CVE have been observed. Sample options include **Banking**, **Technology**, **Government**.
`updates[].plugin.vpr_v2.targeted_regions[]`	array of strings	Allows filtering on specific geographic regions where attacks leveraging the CVE have been observed.
`updates.plugin.vpr`	object	Information about the Vulnerability Priority Rating (VPR) for the vulnerability.
`updates[].plugin.vpr.score`	float	The Vulnerability Priority Rating (VPR) for the vulnerability. If a plugin is designed to detect multiple vulnerabilities, the VPR represents the highest value calculated for a

Property	Data Type	Description
		vulnerability associated with the plugin. For more information, see Severity vs. VPR in the Tenable Vulnerability Management User Guide.
updates[].plugin.vpr.drivers	object	The key drivers Tenable uses to calculate a vulnerability's VPR. For more information, see Vulnerability Priority Rating Drivers.
updates[].plugin.vpr.drivers.age_of_vuln	object	A range representing the number of days since the National Vulnerability Database (NVD) published the vulnerability. Ranges include 0-7 days, 7-30 days, 30-60 days, 60-180 days, 180-365 days, 365-730 days, and more than 730 days (+731)
updates[].plugin.vpr.drivers.age_of_vuln.lower_bound	integer	The lower bound of the range. For example, for the 0-7 days range, this attribute is `0`. For the highest range (more than 730 days), this value is `731`.
updates[].plugin.vpr.drivers.age_of_vuln.upper_bound	integer	The upper bound of the range. For example, for the 0-7 days range, this attribute is `7`. For the highest range (more than 730 days), this value is `0`, which signifies that there is no higher category.
updates[].plugin.vpr.drivers.exploit_code_maturity	string	The relative maturity of a possible exploit for the vulnerability based

Property	Data Type	Description
		on the existence, sophistication, and prevalence of exploit intelligence from internal and external sources (for example, Reversinglabs, Exploit-db, Metasploit, etc.). The possible values (`High`, `Functional`, `PoC`, or `Unproven`) parallel the CVSS Exploit Code Maturity categories.
updates[].plugin.vpr.drivers.cvss_impact_score_predicted	boolean	A value specifying whether Tenable predicted the CVSSv3 impact score for the vulnerability because NVD did not provide one (`true`) or used the NVD-provided CVSSv3 impact score (`false`) when calculating the VPR.
updates[].plugin.vpr.drivers.cvss3_impact_score	float	The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Vulnerability Management displays a Tenable-predicted score.
updates[].plugin.vpr.drivers.threat_intensity_last28	string	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`.
updates[].plugin.vpr.drivers.threat_recency	object	A range representing the number of days since a threat event occurred for the vulnerability. Ranges include 0-7 days, 7-30 days, 30-120 days, 120-365 days, and more than 365

Property	Data Type	Description
		days (+365).
updates[].plugin.vpr.drivers.threat_recency.lower_bound	integer	The lower bound of the range. For example, for the 0-7 days range, this attribute is `0`. For the highest range (more than 365 days), this value is `366`.
updates[].plugin.vpr.drivers.threat_recency.upper_bound	integer	The upper bound of the range. For example, for the 0-7 days range, this attribute is `7`. For the highest range (more than 730 days), this value is `0`, which signifies that there is no higher category.
updates[].plugin.vpr.drivers.threat_sources_last28[]	array of strings	A list of all sources (for example, social media channels, the dark web, etc.) where threat events related to this vulnerability occurred.
updates[].plugin.vpr.drivers.product_coverage	string	The relative number of unique products affected by the vulnerability: `Low`, `Medium`, `High`, or `Very High`.
updates[].plugin.vpr.updated	string	An ISO timestamp indicating the date and time whenthe system last imported the VPR for this vulnerability. The system imports a VPR value the first time you scan a vulnerability on your network. Then, it automatically re-imports new and updated VPR values daily.
updates[].workaround	string	Describes the workaround for

Property	Data Type	Description
		remediating the vulnerability.
`updates[].workaround_type`	string	The workaround action required to remediate the vulnerability. Possible workaround types include: • **Configuration Change** – You must alter the configuration of software on the asset. • **Disable Service** – You must disable a service on the asset.
`updates[].workaround_published`	string	An ISO timestamp indicating the date and time when the workaround was published.
`updates[].has_workaround`	boolean	Indicates if a workaround exists for the vulnerability.
`updates[].port`	object	Information about the port the scanner used to connect to the asset.
`updates[].port.port`	integer	The port the scanner used to communicate with the asset.
`updates[].port.protocol`	string	The protocol the scanner used to communicate with the asset.
`updates[].port.service`	string	The service the scanner used to communicate with the asset.
`updates[].recast_reason`	string	The text that appears in the Comment field of the recast rule in the Tenable Vulnerability Management user interface.

Property	Data Type	Description
updates[].recast_rule_uuid	string	The UUID of the recast rule that applies to the plugin.
updates[].scan	object	Information about the latest scan that detected the vulnerability.
updates[].scan.schedule_uuid	string	The schedule UUID for the scan that found the vulnerability.
updates[].scan.started_at	string	An ISO timestamp indicating the date and time when the scan started.
updates[].scan.uuid	string	The UUID of the scan that found the vulnerability.
updates[].severity	string	The severity of the vulnerability as defined using the Common Vulnerability Scoring System (CVSS) base score. Possible values include `info` (CVSS score of 0), `low` (CVSS score between 0.1 and 3.9), `medium` (CVSS score between 4.0 and 6.9), `high` (CVSS score between 7.0 and 9.9), and `critical` (CVSS score of 10.0).
updates[].severity_id	integer	The code for the severity assigned when a user recast the risk associated with the vulnerability. Possible values include: • **0** – The vulnerability has a CVSS score of 0, which corresponds to the "info" severity level.

Property	Data Type	Description
		• **1** – The vulnerability has a CVSS score between 0.1 and 3.9, which corresponds to the "low" severity level. • **2** – The vulnerability has a CVSS score between 4.0 and 6.9, which corresponds to the "medium" severity level. • **3** – The vulnerability has a CVSS score between 7.0 and 9.9, which corresponds to the "high" severity level. • **4** – The vulnerability has a CVSS score of 10.0, which corresponds to the "critical" severity level.
updates[].severity_default_id	integer	The code for the severity originally assigned to a vulnerability before a user recast the risk associated with the vulnerability. Possible values are the same as for the `severity_id` attribute.
updates[].severity_modification_type	string	The type of modification a user made to the vulnerability's severity. Possible values include: • **none** – No modification has been made. • **recasted** – A user in the Vulnerability Management user interface has recast the

Property	Data Type	Description
		risk associated with the vulnerability • **accepted** – A user in the vulnerability Management user interface has accepted the risk associated with the vulnerability.
`updates[].first_found`	string	An ISO timestamp indicating the date and time when a scan first detected the vulnerability on the asset.
`updates[].last_fixed`	string	An ISO timestamp indicating the date and time when a scan no longer detects the previously detected vulnerability on the asset.
`updates[].last_found`	string	An ISO timestamp indicating the date and time when a scan last detected the vulnerability on the asset.
`updates[].indexed`	string	An ISO timestamp indicating the date and time when the system added the finding to the Tenable Vulnerability Management database.
`updates[].state`	string	The state of the vulnerability as determined by the Tenable Vulnerability Management state service. Possible values include: • **OPEN** – The vulnerability is currently present on an asset.

Property	Data Type	Description
		• **REOPENED** – The vulnerability was previously marked as fixed on an asset, but has been detected again by a new scan. • **FIXED** – The vulnerability was present on an asset, but is no longer detected.
updates[].source	string	The source of the scans that identified the vulnerability. Sources can include sensors, connectors, and API imports. The values in the `source` field correspond to the names of the sources as defined in your organization's implementation of Tenable Vulnerability Management. Commonly used source names include: • **AGENT** – The vulnerability data was obtained from a Tenable Agent scan. • **NNM** – The vulnerability data was obtained from a Tenable Network Monitor scan. • **NESSUS** – The vulnerability data was obtained from a Tenable Nessus scan.
updates[].resurfaced_date	string	An ISO timestamp indicating the date and time the vulnerability

Property	Data Type	Description
		resurfaced. Only the most recent date appears if a vulnerability has resurfaced multiple times.
updates[].time_taken_to_fix	long	The length of time (in seconds) it took for your organization to fix the vulnerability. This property only appears for fixed vulnerabilities.
deletes[{}]	array of objects	Contains any findings deleted in the payload, along with their `_id` and a timestamp.
deletes[]._id	string	The UUID of the deleted finding in Tenable Vulnerability Management.
deletes[].deleted_at	string	An ISO timestamp indicating the date and time when the data in the payload was deleted.
first_ts	string	A Unix timestamp indicating the date and time of the first entry in the payload.
last_ts	string	A Unix timestamp indicating the date and time of the last entry in the payload.

Host Audit Payload Files

When the system updates, adds, or deletes host audits, Tenable Data Stream sends a payload file to your AWS bucket. In the file, updates appear in the `updates` array and deletions appear with a timestamp in the `deletes` array.

The following example shows the format of a host audit payload file. For definitions of the properties in this file, see Host Audit Properties.

```
{
    "payload_id": "host_audit_finding-1744708524728-24",
    "version": 1,
    "type": "HOST_AUDIT_FINDING",
    "count_updated": 1,
    "count_deleted": 0,
    "updates": [
        {
            "finding_id": "30f88ab0-8d20-59e7-9765-40dee1d518f0",
            "asset_uuid": "5ca153b5-1402-4f0e-bad3-c300b69a4261",
            "first_seen": "2025-03-17T11:42:40.162Z",
            "last_seen": "2025-04-15T09:15:17.702Z",
            "audit_file": "Tenable_Best_Practices_Cisco_ACI_v1.0.0.audit",
            "check_id": "b6aa447a3dbc58cd0598ac3db38177cb5a2aa7617dc8a5eef652ffce0ad89412",
            "check_name": "Tenable_Best_Practices_Cisco_ACI_v1.0.0.audit",
            "check_info": "Info",
            "expected_value": "PASSED",
            "actual_value": "PASSED",
            "status": "PASSED",
            "reference": [
                {
                    "framework": "framework-id",
                    "control": "control-id"
                }
            ],
            "see_also": "check reference",
            "solution": "solution",
            "check_error": "check for errors",
            "profile_name": "profile information",
            "db_type": "sqlite",
            "plugin_id": 137785,
            "state": "ACTIVE",
            "description": "\"Tenable_Best_Practices_Cisco_ACI_v1.0.0.audit: [PASSED]\"\n\nPolicy
Value:\nPASSED\n\nError:\n",
            "audit_description": "check audit description",
            "compliance_benchmark_name": "Custom",
            "compliance_benchmark_version": "2",
            "compliance_control_id": "fabiub43551ri1bf3",
            "compliance_full_id": "124c1c4124c124c124",
            "compliance_functional_id": "c1412c4c41c412c",
            "compliance_informational_id": "c1241241c555c1",
            "synopsis": "Compliance checks for Cisco ACI devices.",
            "last_fixed": "2025-04-15T09:15:17.702Z",
            "last_observed": "2025-04-15T09:15:17.702Z",
            "metadata_id": "d5fa5292952f366f922d9b4a06c3e970dcb1ef62518ac948f8e1ac01e692f053",
            "uname_output": "output value",
            "indexed_at": "2025-04-15T09:15:25.225Z",
            "plugin_name": "Cisco ACI Compliance Checks",
            "asset": {
                "id": "5ca153b5-1402-4f0e-bad3-c300b69a4261",
                "ipv4_addresses": [
                    "44.241.160.134"
                ],
                "ipv6_addresses": [
                    "2001:0db8:85a3:0000:0000:8a2e:0370:7334"
                ],
                "fqdns": [
                    "target3.pubtarg.tenablesecurity.com"
                ],
                "name": "target3.pubtarg.tenablesecurity.com",
                "agent_name": "agent-name",
                "agent_uuid": "4f0e-bad3-c300b69a4261",
```

```
                "tags": [
                    {
                        "category": "category-id-1",
                        "value": "value-id-1"
                    }
                ],
                "mac_addresses": [
                    "00:1A:2B:3C:4D:5E"
                ],
                "operating_systems": [
                    "Linux Kernel 3.13 on Ubuntu 14.04 (trusty)"
                ],
                "system_type": "general-purpose",
                "network_id": "00000000-0000-0000-0000-000000000000"
            },
            "scan": {
                "completed_at": "2025-04-15T09:15:17.702Z",
                "schedule_uuid": "9fb5426c-3190-4a4a-aeff-8b6e45b92b08",
                "started_at": "2025-04-15T09:15:17.702Z",
                "uuid": "09753677-c85e-d017-7ac9-54bde5c266d61a99ef02f5844cba",
                "target": "41.151.155.44"
            }
        }
    ],
    "deletes": [
        {
            "id": "0d8c3882-870a-5777-a9ec-25ni25275211",
            "deleted_at": "2025-04-06T04:01:40Z"
        }
    ],
    "first_ts": "1744708524606",
    "last_ts": "1744708524606"
}
```


Host Audit Properties

The following table defines the properties in a Tenable Data Stream host audit payload file. To see an example file, go to Host Audit Payload Files.

Property	Data Type	Description
payload_id	string	The ID of the payload sent from Tenable Vulnerability Management.
version	integer	The version of the payload. This number increments when the payload structure changes.
type	string	The type of payload (`HOST_AUDIT_FINDING`).
count_updated	integer	The number of objects updated in the payload.
count_deleted	integer	The number of objects deleted in the payload.

Property	Data Type	Description
updates[]	array of objects	Contains the host audit objects updated in the payload.
updates[].finding_id	string	The ID of the finding.
updates[].asset_uuid	string	The UUID of the asset on which the compliance check was executed.
updates[].first_seen	string	The ISO date when a compliance scan first assessed the asset with the compliance check.
updates[].last_seen	string	The ISO date when a compliance scan last assessed the asset with the compliance check.
updates[].audit_file	string	The name of the audit file containing the compliance check.
updates[].check_id	string	The unique identifier for the compliance finding. This identifier is generated based on the `compliance_full_id`, `compliance_functional_id`, and `compliance_informational_id`. The `check_id` is regenerated if any of the identifiers it's based on changes.
updates[].check_name	string	The descriptive name of the compliance check.
updates[].check_info	string	A full text description of the compliance check.
updates[].expected_value	string	The desired value (integer or string) for the compliance check. For example, if a password length compliance check requires passwords to be 8 characters long then 8 is the expected value. For manual checks, this field will contain the command used for the compliance check.
updates[].actual_value	string	The actual value (integer, string, or table) evaluated from the compliance check. For

Property	Data Type	Description
		example, if a password length compliance check requires passwords to be 8 characters long, but the evaluated value was 7 then 7 is the actual value. For manual checks, this field will contain the output of the command that was executed.
updates[].status	string	The result status of the audit check: • `PASSED` – Returned if the asset has passed the compliance check • `FAILED` – Returned if the asset has failed the compliance check. • `WARNING` – Returned when there is no definable passing criteria (for example, an audit verifying that members of the administrator group are appropriate for your organization). • `SKIPPED` – Returned if the plugin determined that the check is not applicable to the asset. It can also be returned in other various cases (for example, if a check requires that a direct command be run to gather data on an offline network device or if a check contains commands that will not run on the specified operating system). • `UNKNOWN` – Returned when a status cannot be determined for the OVAL check. The OVAL engine sets this status.
updates[].reference[]	array of objects	Industry references for the compliance check.
updates[].reference	string	The name of the compliance framework.

Property	Data Type	Description
[].framework		
updates[].reference[].control	string	The specific control within the compliance framework.
updates[].see_also	string	Links to external websites that contain reference information about the compliance check.
updates[].solution	string	Remediation information for the compliance check.
updates[].check_error	string	An error message if the compliance evaluation fails.
updates[].profile_name	string	The name of the profile for the benchmark standard.
updates[].db_type	string	The type of database if the compliance check assessed a database.
updates[].plugin_id	integer	The unique ID of the compliance plugin.
updates[].state	string	The state as determined by the Tenable Vulnerability Management state service. This field is `NULL` for findings last seen before December 2021. Possible values include: • `OPEN` — The compliance finding is currently present on an asset. • `REOPENED` — The compliance finding was previously marked as fixed on an asset but has been detected again by a new scan. • `FIXED` — The compliance finding was present on an asset but is no longer detected. • `ACTIVE` — The compliance finding is currently active on an asset.

Property	Data Type	Description
		Note that the API uses different terms for states than the user interface. The `new` and `active` states in the user interface map to the `OPEN` state in the API. The `resurfaced` state in the user interface maps to the `REOPENED` state in the API. The `fixed` state is the same.
`updates[].description`	string	A detailed description of the finding.
`updates[].audit_description`	string	A detailed description of the compliance check.
`updates[].compliance_benchmark_name`	string	The name of the compliance benchmark (for example, `CIS SQL Server 2019`).
`updates[].compliance_benchmark_version`	string	The version of the compliance benchmark (for example, `1.2.0`).
`updates[].compliance_control_id`	string	A unique identifier for the aggregation of multiple results to single recommendations in CIS and DISA audits. This identifier is a computed and hashed value for CIS and DISA content that enables customers to match checks that evaluate the same recommendation within a benchmark.
`updates[].compliance_full_id`	string	A unique identifier that identifies a full compliance result in the context of an audit. The identifier is a hash of fields within the compliance check (excluding external references). The identifier changes if any of the fields within the compliance check change.
`updates[].compliance_functional_id`	string	A unique identifier for aggregating or comparing compliance results that were tested the same way. The identifier is a hash of the code within the audit that actually performs the check. The identifier changes if functional evaluation of the

Property	Data Type	Description
		audit changes.
updates[].compliance_informational_id	string	A unique identifier for aggregating or comparing compliance results that have the same informational data. For example, the same solution text. The identifier is a hash of the info and solution fields within the compliance check. The identifier changes if either of these fields are updated.
updates[].synopsis	string	A short summary of the compliance audit.
updates[].last_fixed	string	The ISO date when the compliance failure was last fixed on the asset.
updates[].last_observed	string	The ISO date when the compliance issue was last observed (whether `active` or `fixed`) on the asset.
updates[].metadata_id	string	A unique identifier used in the Tenable Vulnerability Management pipeline results ingestion.
updates[].uname_output	string	The output of the `uname` command on the asset. It typically contains the operating system type and version.
updates[].indexed_at	string	The ISO date when the audit for the asset was indexed into Tenable Vulnerability Management.
updates[].plugin_name	string	The name of the compliance check.
updates[].asset	object	An object containing detailed information about the affected asset.
updates[].asset.id	string	The UUID of the asset in Tenable Vulnerability Management. Use this value as the unique key for the asset.

Property	Data Type	Description
updates[].asset.ipv4_addresses[]	array of strings	A list of IPv4 addresses that are associated with the asset.
updates[].asset.ipv6_addresses[]	array of strings	A list of IPv6 addresses that are associated with the asset.
updates[].asset.fqdns[]	array of strings	A list of fully-qualified domain names (FQDNs) that are associated with the asset.
updates[].asset.name	string	The name of the asset.
updates[].asset.agent_name	string	The name of the Tenable Agent that scanned and identified the asset.
updates[].asset.agent_uuid	string	This property represents the `tenable_uuid`. This identifier can originate from either an agent or a credentialed remote Tenable Nessus scan. If no agent is present on the asset, a UUID is assigned by Tenable Vulnerability Management during a credentialed scan when the Create unique identifier on hosts scanned with credentials option is enabled. Note that no UUID is set for an uncredentialed non-agent scans.
updates[].asset.tags[]	array of objects	The tags assigned to the asset in Tenable Vulnerability Management. **Note**: The `tags` object is always empty and appears to maintain compatibility with the Tenable API. Your tag data is sent in the tags payload file.
updates[].asset.tags[].category	string	The tag category identifier.
updates[].asset.tags[].value	string	The tag value identifier.
updates[].asset.mac_	array of	A list of MAC addresses that are associated with

Property	Data Type	Description
addresses[]	strings	the asset.
updates [].asset.operating_ systems[]	array of strings	The operating systems that scans have associated with the asset record.
updates [].asset.system_type	string	The system type as reported by Plugin ID 54615. Possible values include: • `router` • `general-purpose` • `scan-host` • `embedded`
updates [].asset.network_id	string	The ID of the network to which the asset belongs. The default network ID is `00000000-0000-0000-0000-000000000000`. For more information about network objects, see Manage Networks.
updates[].scan	object	Information about the scan that detected the finding.
updates [].scan.completed_at	string	An ISO timestamp indicating the date and time when the scan was completed.
updates [].scan.schedule_uuid	string	The unique identifier for the scan schedule.
updates [].scan.started_at	string	An ISO timestamp indicating the date and time when the scan started.
updates[].scan.uuid	string	The UUID of the scan.
updates[].scan.target	string	The target IP or hostname of the scan.
deletes[]	array of objects	Contains the host audit objects deleted in the payload.

Property	Data Type	Description
deletes[].id	string	The ID of the deleted host audit.
deletes[].deleted_at	string	An ISO timestamp indicating the date and time when the host audit was deleted.
first_ts	string	A Unix timestamp indicating the date and time of the first entry in the payload.
last_ts	string	A Unix timestamp indicating the date and time of the last entry in the payload.

Tags Payload Files

When the system adds, edits, or deletes asset tags, Tenable Data Stream sends a payload file to your AWS bucket. In the file, updates appear in the `updates` array and deletes appear with a timestamp in the `deletes` array.

> **Note**: To maintain compatibility with the Tenable API, Tenable Data Stream also sends an assets payload file with an empty tags object.

The following example shows the format of a tags payload file. For definitions of the properties in this file, see Tags Properties.


```
{
  "payload_id": "tags-1727096866393-5",
  "version": 1,
  "type": "TAGS",
  "count_updated": 1,
  "count_deleted": 0,
  "updates": [
    {
      "target": {
        "asset_uuid": "03215919-88c1-4ed9-a59e-7d530940c7f4"
      },
      "tags": [
        {
          "type": "DYNAMIC",
          "category_uuid": "bef73bb5-c35c-4a70-a1fd-3bfcf8b034bb",
          "value_uuid": "5317410c-87b0-4a96-8cca-fc2d3e56c94b",
          "category_name": "Asset Type",
          "tag_name": "sample",
          "created_by": null,
          "created_at": 1727096866286,
          "updated_by": null,
          "updated_at": 1727096866286,
          "description": null,
```

```
          "category_description": null,
          "product": "IO"
        }
      ]
    }
  ],
  "deletes": [],
  "first_ts": "1727096866345",
  "last_ts": "1727096866345"
}
```


Tags Properties

The following table defines the properties in a Tenable Data Stream tags payload file. To see an example, go to Tags Payload Files.

Property	Data Type	Description
payload_id	string	The ID of the payload sent from Tenable Vulnerability Management.
version	integer	The version of the payload. This number increments when the payload structure changes.
type	string	The type of payload, for example, `TAGS`.
count_updated	integer	The number of objects updated in the payload.
count_deleted	integer	The number of objects deleted in the payload.
updates[{}]	array of objects	Contains the objects updated in the payload.
updates[].target.asset_uuid	string	The UUID of the asset for which the system updated tags. Use this value as the unique key for the asset.
updates[{}].tags	array of objects	Contains information about the asset tags updated in the payload.
updates[].tags[].type	string	The type of tag: `STATIC` or `DYNAMIC`.
updates[].tags	string	The UUID of the tag category.

Property	Data Type	Description
`[].category_uuid`		
`updates[].tags [].value_uuid`	string	The UUID of the tag value.
`updates[].tags [].category_name`	string	The tag category (the first half of the category:value pair).
`updates[].tags [].tag_name`	string	The tag value (the second half of the category:value pair).
`updates[].tags [].created_by`	string	The UUID of the user who assigned the tag to the asset.
`updates[].tags [].created_at`	integer	A Unix timestamp indicating the date and time when the tag was created.
`updates[].tags [].updated_by`	string	The UUID of the user who last updated the tag.
`updates[].tags [].updated_at`	integer	A Unix timestamp indicating the date and time when the tag was updated.
`updates[].tags [].description`	string	The tag description.
`updates[].tags [].category_ description`	string	The tag category description.
`updates[].tags [].product`	string	The product the tag applies to, for example, `IO` for Tenable Vulnerability Management.
`deletes[{}]`	array of objects	Contains tags deleted in the payload.
`deletes[].id`	string	Indicates the ID for the deleted tag.
`deletes[].deleted_ at`	string	An ISO timestamp indicating the date and time when the tag was deleted.

Property	Data Type	Description
`first_ts`	integer	A Unix timestamp indicating the date and time of the first entry in the payload.
`last_ts`	integer	A Unix timestamp indicating the date and time of the last entry in the payload.

Web App Scanning Asset Payload Files

When the system updates, adds, or deletes web app scanning assets, Tenable Data Stream sends a payload file to your AWS bucket. In the file, updates appear in the `updates` array and deletions appear with a timestamp in the `deletes` array.

> **Note:** Asset deletions (host assets *and* WAS assets) appear in both the `assets` and `was_assets` folders. Ignore the asset IDs that are not relevant to you.

The following example shows the format of a web app scanning asset payload file. For definitions of the properties in this file, see Web App Scanning Asset Properties.


```
{
    "payload_id": "was_asset-1744711190422-6",
    "version": 1,
    "type": "WAS_ASSET",
    "count_updated": 1,
    "count_deleted": 0,
    "updates": [
        {
            "id": "57d474ae-5495-471a-b663-62991764bbe2",
            "has_agent": false,
            "has_plugin_results": false,
            "is_licensed": true,
            "types": [
                "webapp"
            ],
            "terminated_by": "user",
            "deleted_by": "user",
            "agentNames": [
                "agent1",
                "agent2"
            ],
            "operating_systems": [
                "Linux Kernel 3.10 on CentOS Linux release 7"
            ],
            "system_types": [
                "general-purpose"
            ],
            "manufacturer_tpm_ids": [
                "id1",
                "id2"
```

```
        ],
        "installed_software": [
            "cpe:/a:openbsd:openssh:8.0",
            "cpe:/a:docker:docker:23.0.1",
            "cpe:/a:exiv2:exiv2:0.27.3",
            "cpe:/a:gnome:gnome-shell:3.32.2",
            "cpe:/a:gnupg:libgcrypt:1.8.5",
            "cpe:/a:haxx:curl:7.61.1",
            "cpe:/a:sqlite:sqlite:3.26.0",
            "cpe:/a:tenable:nessus_agent:10.7.2",
            "cpe:/a:vim:vim:8.0",
            "cpe:/a:tenable:sensorproxy:1.0.7"
        ],
        "is_public": true,
        "sources": [
            {
                "name": "WAS",
                "first_seen": "2025-04-15T09:07:23.467Z",
                "last_seen": "2025-04-15T12:14:51.469Z"
            }
        ],
        "tags": [
            {
                "uuid": "13e8edc5-c4fa-478e-b9e7-3564406230dc",
                "key": "operating_system_linux",
                "value": "linux",
                "added_at": "2024-12-28T16:26:50.731Z",
                "added_by": "57d474ae-5495-471a-b663"
            },
            {
                "uuid": "0ab549cf-32a4-4325-8dc9-aadf45ce00a7",
                "key": "aad",
                "value": "asdasd",
                "added_at": "2024-11-08T17:02:57.945Z",
                "added_by": "57d474ae-5495-471a-b663"
            }
        ],
        "network": {
            "network_id": "00000000-0000-0000-0000-000000000000",
            "network_name": "Default",
            "ipv4s": [
                "44.235.70.201"
            ],
            "bios_uuid": "57d474ae-5495-471a-b663-412451525f41",
            "ipv6s": [
                "2001:0db8:85a3:0000:0000:8a2e:0370:7334"
            ],
            "fqdns": [
                "target4.pubtarg.tenablesecurity.com"
            ],
            "mac_addresses": [
                "00:1A:2B:3C:4D:5E"
            ],
            "netbios_names": [
                "server1"
            ],
            "hostnames": [
                "http://target4.pubtarg.tenablesecurity.com"
            ],
            "ssh_fingerprints": [
                "ssh-fingerprint-example"
```

```
            ],
            "network_interfaces": [
                {
                    "name": "interface-1",
                    "virtual": false,
                    "aliased": false,
                    "fqdns": [
                        "target4.pubtarg.tenablesecurity.com"
                    ],
                    "mac_addresses": [
                        "00:1A:2B:3C:4D:5E"
                    ],
                    "ipv4s": [
                        "44.235.70.201"
                    ],
                    "ipv6s": [
                        "2001:0db8:85a3:0000:0000:8a2e:0370:7334"
                    ]
                }
            ],
            "open_ports": [
                {
                    "port": 313,
                    "protocol": "TCP",
                    "service_names": [
                        "service-1"
                    ],
                    "first_seen": "2025-04-15T09:07:23.467Z",
                    "last_seen": "2025-04-15T12:14:51.469Z"
                }
            ]
        },
        "scan": {
            "first_scan_time": "2025-04-15T09:07:23.467Z",
            "last_scan_time": "2025-04-15T12:14:51.469Z",
            "last_authenticated_scan_date": "2025-04-15T12:14:51.469Z",
            "last_licensed_scan_date": "2025-04-15T12:14:51.469Z",
            "last_scan_id": "6be2178e-b46f-4cc1-b5e0-e4695482edcb",
            "last_schedule_id": "template-6be2178e-b46f-4cc1-b5e0-e4695482edcb414",
            "last_authentication_attempt_date": "2025-04-15T12:14:51.469Z",
            "last_authentication_success_date": "2025-04-15T12:14:51.469Z",
            "last_authentication_scan_status": "SUCCESS",
            "last_scan_target": "44.235.70.201"
        },
        "timestamps": {
            "created_at": "2025-04-15T09:15:19.295Z",
            "updated_at": "2025-04-15T12:17:27.560Z",
            "deleted_at": "2025-04-15T12:17:27.560Z",
            "terminated_at": "2025-04-15T12:17:27.560Z",
            "first_seen": "2025-04-15T09:07:23.467Z",
            "last_seen": "2025-04-15T12:14:51.469Z"
        },
        "custom_attributes": [
            {
                "id": "attr1",
                "value": "attrVal1"
            },
            {
                "id": "attr2",
                "value": "attrVal2"
            }
```

```
            ],
            "ratings": {
                "acr": {
                    "score": 5.0
                },
                "aes": {
                    "score": 700.0
                }
            },
            "acr_score": "5",
            "exposure_score": "700"
        }
    ],
    "deletes": [
        {
            "id": "0d8c3882-870a-5777-a9ec-25ni25275211",
            "deleted_at": "2025-04-06T04:01:40Z"
        }
    ],
    "first_ts": "1744708524606",
    "last_ts": "1744708524606"
}
```


Web App Scanning Asset Properties

The following table defines the properties in a Tenable Data Stream web app scanning assets payload file. To see an example file, go to Web App Scanning Asset Payload Files.

Property	Data Type	Description
payload_id	string	The ID of the payload sent from Tenable Vulnerability Management.
version	integer	The version of the payload. This number increments when the payload structure changes.
type	string	The type of payload (`WAS_ASSET`).
count_updated	integer	The number of objects updated in the payload.
count_deleted	integer	The number of objects deleted in the payload.
updates[]	array of objects	A list of updated web app scanning asset objects.

Property	Data Type	Description
updates[].id	string	The UUID of the asset in Tenable Vulnerability Management. Use this value as the unique key for the asset.
updates[].has_agent	boolean	Specifies whether a Tenable Agent scan identified the asset.
updates[].has_plugin_results	boolean	Specifies whether the asset has plugin results associated with it.
updates[].is_licensed	boolean	Indicates whether the asset is licensed by Tenable.
updates[].types[]	array of strings	A list of asset types that apply to the asset (for example, `webapp`).
updates[].terminated_by	string	The user who terminated the AWS instance of the asset.
updates[].deleted_by	string	The user who deleted the asset record.
updates[].agentNames[]	array of strings	The names of any Tenable Agents that scanned and identified the asset.
updates[].operating_systems[]	array of strings	The operating systems that scans have associated with the asset record.
updates[].system_types[]	array of strings	The system types as reported by Plugin ID 54615. Possible values include `router`, `general-purpose`, `scan-host`, and `embedded`.
updates[].manufacturer_tpm_ids[]	array of strings	The manufacturer's unique identifiers of the Trusted Platform Module (TPM) associated with the asset.
updates[].installed_software[]	array of strings	A list of Common Platform Enumeration (CPE) values that represent software applications a scan identified as present

Property	Data Type	Description
		on an asset. This attribute supports the CPE 2.2 format. For more information, see the "Component Syntax" section of the CPE Specification, Version 2.2. For assets identified in Tenable scans, this attribute contains data only if a scan using Nessus Plugin ID 45590 has evaluated the asset. **Note**: If no scan detects an application within 30 days of the scan that originally detected the application, Tenable Vulnerability Management considers the detection of that application expired. As a result, the next time a scan evaluates the asset, Tenable Vulnerability Management removes the expired application from the installed_software_attribute. This activity is logged as a `remove` type of `attribute_change` update in the asset activity log.
`updates[].is_public`	boolean	Specifies whether if the asset is an internet-facing and accessible externally.
`updates[].sources[]`	array of objects	Objects that describe the scan sources that identified the asset. An asset source is the entity that reported the asset details. Sources can include sensors, connectors, and API imports. If your request specifies multiple sources, Tenable Vulnerability Management returns all assets seen by any of the specified sources. The items in the sources array must correspond to the names of the sources

Property	Data Type	Description
		as defined in your organization's implementation of Tenable Vulnerability Management. Commonly used names include: • **AWS** – The asset data was obtained from an Amazon Web Services connector. • **NESSUS_AGENT** – The asset data was obtained from a Tenable Agent scan. • **NESSUS_SCAN** – The asset data was obtained from a Tenable Nessus scan. • **PVS** – The asset data from a Tenable Network Monitor scan. • **WAS** – The asset data was obtained from a Tenable Web App Scanning scan.
`updates[].sources[].name`	string	The name of the entity that reported the asset details. Sources can include sensors, connectors, and API imports. Source names can be customized by your organization (for example, you specify a name when you import asset records). If your organization does not customize source names, the system-generated names include: • **AWS** – The asset data was obtained from an Amazon Web Services connector.

Property	Data Type	Description
		• **NESSUS_AGENT** – The asset data was obtained from a Tenable Agent scan. • **NESSUS_SCAN** – The asset data was obtained from a Tenable Nessus scan. • **PVS** – The asset data from a Tenable Network Monitor scan. • **WAS** – The asset data was obtained from a Tenable Web App Scanning scan.
updates[].sources[].first_seen	string	The ISO timestamp when the source first reported the asset.
updates[].sources[].last_seen	string	The ISO timestamp when the source last reported the asset.
updates[].tags	array of objects	Object containing the tags for the asset. **Note**: The `tags` object is always empty and appears to maintain compatibility with the Tenable API. Your tag data is sent in the tags payload file.
updates[].tags[].uuid	string	The UUID of the tag.
updates[].tags[].key	string	The tag category (the first half of the category:value pair).
updates[].tags[].value	string	The tag value (the second half of the category:value pair).
updates[].tags[].added_at	string	The ISO timestamp when the tag was assigned to the asset.
updates[].tags[].added_by	string	The UUID of the user who assigned the

Property	Data Type	Description
		tag to the asset.
updates[].network	object	An object containing network-related information for the asset.
updates[].network.network_id	string	The ID of the network associated with the scanners that identified the asset. The default network ID is `00000000-0000-0000-0000-000000000000`. For more information about network objects, see Manage Networks.
updates[].network.network_name	string	The ID of the network object associated with scanners that identified the asset. The default network name is `Default`. All other network names are user-defined. For more information about network objects, see Manage Networks.
updates[].network.ipv4s[]	array of strings	The IPv4 addresses that scans have associated with the asset record.
updates[].network.bios_uuid	string	The BIOS UUID of the asset.
updates[].network.ipv6s[]	array of strings	The IPv6 addresses that scans have associated with the asset record.
updates[].network.fqdns[]	array of strings	The fully-qualified domain names that scans have associated with the asset record.
updates[].network.mac_addresses[]	array of strings	The MAC addresses that scans have associated with the asset record.
updates[].network.netbios_names[]	array of strings	The NetBIOS names that scans have associated with the asset record.
updates[].network.hostnames	array of	The hostnames that scans have

Property	Data Type	Description
`[]`	strings	associated with the asset record.
`updates[].network.ssh_fingerprints[]`	array of strings	The SSH key fingerprints that scans have associated with the asset record.
`updates[].network.network_interfaces[]`	array of objects	The network interfaces that scans identified on the asset.
`updates[].network.network_interfaces[].name`	string	The name of the network interface.
`updates[].network.network_interfaces[].virtual`	boolean	Indicates whether the network interface is virtual.
`updates[].network.network_interfaces[].aliased`	boolean	Indicates whether the network interface is aliased.
`updates[].network.network_interfaces[].fqdns[]`	array of strings	A list of FQDNs for the network interface.
`updates[].network.network_interfaces[].mac_addresses[]`	array of strings	The MAC addresses of the network interface.
`updates[].network.network_interfaces[].ipv4s[]`	array of strings	A list of IPv4 addresses belonging to the interface.
`updates[].network.network_interfaces[].ipv6s[]`	array of strings	A list of IPv6 addresses belonging to the interface.
`updates[].network.open_ports[]`	array of objects	An array of open ports and their services as reported by the info-level plugins.
`updates[].network.open_ports[].port`	integer	The open port number.
`updates[].network.open_ports[].protocol`	string	The communication protocol corresponding to the open port.
`updates[].network.open_ports[].service_names[]`	array of strings	The names of the services associated with the open port.

Property	Data Type	Description
updates[].network.open_ports[].first_seen	string	The ISO timestamp when the source first detected the open port on the asset.
updates[].network.open_ports[].last_seen	string	The ISO timestamp when the source last detected the open port on the asset.
updates[].scan	object	An object containing scan-related information for the asset.
updates[].scan.first_scan_time	string	The time and date of the first scan run against the asset.
updates[].scan.last_scan_time	string	The time and date of the last scan run against the asset.
updates[].scan.last_authenticated_scan_date	string	The time and date of the last credentialed scan run on the asset.
updates[].scan.last_licensed_scan_date	string	The time and date of the last scan that identified the asset as licensed. Tenable Vulnerability Management categorizes an asset as licensed if a scan of that asset has returned results from a non-discovery plugin within the last 90 days.
updates[].scan.last_scan_id	string	The UUID of the scan configuration used during the last scan of the asset.
updates[].scan.last_schedule_id	string	The `schedule_uuid` for the last scan of the asset.
updates[].scan.last_authentication_attempt_date	string	The date when last authentication scan attempt was made.
updates[].scan.last_authentication_success_date	string	The date when last authentication scan attempt was successful.
updates[].scan.last_authentication_scan_status	string	The status of the last scan authentication (for example, `SUCCESS`).

Property	Data Type	Description
updates[].scan.last_scan_target	string	The last scan target that was scanned.
updates[].timestamps	object	An object containing various timestamps related to the asset.
updates[].timestamps.created_at	string	The time and date when Tenable Vulnerability Management created the asset record.
updates[].timestamps.updated_at	string	The time and date when the asset record was last updated.
updates[].timestamps.deleted_at	string	The time and date when a user deleted the asset record. When a user deletes an asset record, Tenable Vulnerability Management retains the record until the asset ages out of the license count.
updates[].timestamps.terminated_at	string	The time and date when a user terminated the Amazon Web Service (AWS) virtual machine instance of the asset.
updates[].timestamps.first_seen	string	The time and date when a scan first identified the asset.
updates[].timestamps.last_seen	string	The time and date of the scan that most recently identified the asset.
updates[].custom_attributes[]	array of objects	A list of custom attributes for the asset.
updates[].custom_attributes[].id	string	The identifier for the custom attribute.
updates[].custom_attributes[].value	string	The value of the custom attribute.

Property	Data Type	Description
`updates[].ratings`	object	A list of vulnerability ratings and score calculations. These ratings provide a comprehensive view of exposure. Currently, only the Asset Criticality Rating (ACR) and Asset Exposure Score (AES) are provided.
`updates[].ratings.acr`	object	The Tenable-defined Asset Criticality Rating (ACR) for the asset. Tenable uses an algorithm based on the asset profile to assign a metric rating the importance of an asset to your organization from 1 to 10, with higher numbers for more critical assets.
`updates[].ratings.acr.score`	number	The Asset Criticality Rating (ACR) value.
`updates[].ratings.aes`	object	The Tenable-defined Asset Exposure Score (AES) for the asset. This metric weighs an asset's Vulnerability Priority Rating (VPR) and Asset Criticality Rating (AES) and then assigns a number from 1 to 1000, with higher numbers for more exposed assets.
`updates[].ratings.aes.score`	number	The Asset Exposure Score (AES) value.
`updates[].acr_score`	string	(Tenable Lumin-only) The Asset Criticality Rating (ACR) for the asset.
`updates[].exposure_score`	string	(Tenable Lumin-only) The Asset Exposure Score (AES) for the asset.
`deletes[]`	array of objects	Contains the web app scanning asset objects deleted in the payload.
`deletes[].id`	string	The ID of the deleted web app scanning

Property	Data Type	Description
		asset.
deletes[].deleted_at	string	An ISO timestamp indicating the date and time when the asset was deleted.
first_ts	string	A Unix timestamp indicating the date and time of the first entry in the payload.
last_ts	string	A Unix timestamp indicating the date and time of the last entry in the payload.

Web App Scanning Findings Payload Files

When the system updates, adds, or deletes web app scanning findings, Tenable Data Stream sends a payload file to your AWS bucket. In the file, updates appear in the `updates` array and deletions appear with a timestamp in the `deletes` array.

The following example shows the format of a web app scanning finding payload file. For definitions of the properties in this file, see Web App Scanning Findings Properties.


```
{
  "payload_id": "was_finding-1744708521126-68",
  "version": 1,
  "type": "WAS_FINDING",
  "count_updated": 1,
  "count_deleted": 0,
  "updates": [
    {
      "finding_id": "0d8c3882-870a-5777-a9ec-666879a9bdb8",
      "url": "http://target2.pubtarg.tenablesecurity.com/",
      "input_type": "type",
      "input_name": "name",
      "http_method": "SSL",
      "output": "The scanner detected the lack of a correct X-Content-Type-Options header
configuration in the target application response",
      "proof": "sample-proof-value",
      "payload": "sample-payload-value",
      "state": "OPEN",
      "severity": "INFO",
      "severity_id": 0,
      "severity_default_id": 0,
      "severity_modification_type": "NONE",
      "recast_reason": "NONE",
      "recast_rule_uuid": "870a-5777-a9ec-666879a9bdb8",
      "first_found": "2025-04-06T04:01:40Z",
      "last_found": "2025-04-06T04:01:40Z",
      "last_fixed": "2025-04-06T04:01:40Z",
      "last_observed": "2025-04-06T04:01:40Z",
```

```
      "indexed_at": "2025-04-06T04:01:47.098Z",
      "plugin": {
        "id": 112529,
        "risk_factor": "LOW",
        "original_risk_factor_num": 1,
        "locale": "en",
        "type": "REMOTE",
        "intel_type": "SENSOR",
        "name": "Missing 'X-Content-Type-Options' Header",
        "version": "1",
        "publication_date": "2018-11-28T00:00:00Z",
        "modification_date": "2024-03-25T00:00:00Z",
        "solution": "Configure your web server to include an 'X-Content-Type-Options' header with a
value of 'nosniff'.",
        "synopsis": "Missing 'X-Content-Type-Options' Header",
        "description": "The HTTP 'X-Content-Type-Options' response header prevents the browser from
MIME-sniffing a response away from the declared content-type.\n\nThe server did not return a correct
'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site
Scripting (XSS) attack.",
        "patch_publication_date": "2018-11-28T00:00:00Z",
        "exploitability_ease": "NONE",
        "stig_severity": "NONE",
        "public_display": 112529,
        "in_the_news": false,
        "exploited_by_malware": false,
        "epss_score": 0.00553,
        "cvss2_base_score": 2.6,
        "cvss2_temporal_score": 1.9,
        "cvss3_base_score": 3.1,
        "cvss3_temporal_score": 6.2,
        "see_also": [
          "https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options",
          "https://www.owasp.org/index.php/OWASP_Secure_Headers_Project#xcto"
        ],
        "bid": [
          "112529"
        ],
        "policy": [
          "policy 1"
        ],
        "xrefs": [
          {
            "type": "capec",
            "id": [
              "1",
              "107",
              "127",
              "17",
              "20",
              "22",
              "237",
              "36",
              "477",
              "480",
              "51",
              "57",
              "59",
              "65",
              "74",
              "87"
            ]
```

```
        },
        {
          "type": "hipaa",
          "id": [
            "164.306(a)(1)",
            "164.306(a)(2)"
          ]
        },
        {
          "type": "iso",
          "id": [
            "27001-A.14.2.5"
          ]
        },
        {
          "type": "nist",
          "id": [
            "sp800_53-CM-6b"
          ]
        },
        {
          "type": "pci_dss",
          "id": [
            "3.2-2.2"
          ]
        }
      ],
      "cpe": [
        "cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:*"
      ],
      "cve": [
        "CVE-2015-9251"
      ],
      "cwe": [
        "693"
      ],
      "wasc": [
        "Application Misconfiguration"
      ],
      "owasp_2010": [
        "A6"
      ],
      "owasp_2013": [
        "A5"
      ],
      "owasp_2017": [
        "A6"
      ],
      "owasp_2021": [],
      "owasp_api_2019": [
        "API7"
      ],
      "vpr": {
        "score": 2.15,
        "drivers": {
          "age_of_vuln": {
            "lower_bound": 730,
            "upper_bound": 897
          },
          "exploit_code_maturity": "UNPROVEN",
          "cvss_impact_score_predicted": true,
```

```
            "cvss3_impact_score": 1.4,
            "threat_intensity_last28": "LOW",
            "threat_recency": {
              "lower_bound": 730,
              "upper_bound": 897
            },
            "threat_sources_last28": [
              "source1",
              "source2"
            ],
            "product_coverage": "LOW"
          },
          "updated": "2024-06-12T06:06:31.000Z",
          "updated_reason": "Update"
        },
        "vpr_v2": {
          "score": 3,
          "vpr_percentile": "22.61",
          "vpr_severity": "LOW",
          "exploit_probability": 0,
          "cve_id": "CVE-2024-23314",
          "exploit_code_maturity": "UNPROVEN",
          "on_cisa_kev": false,
          "in_the_news_intensity_last30": "VERY LOW",
          "in_the_news_recency": "NO RECORDED EVENTS",
          "malware_observations_intensity_last30": "VERY LOW",
          "malware_observations_recency": "NO RECORDED EVENTS",
          "threat_summary": {
              "summary": "null",
              "lastUpdated": "null"
          },
          "remediation": {
              "summary": "null",
              "lastUpdated": "null"
          },
          "targeted_industries": [
              "Energy",
              "Government",
              "Government - Federal",
              "Government - State/Local",
              "Healthcare",
              "Insurance",
              "Legal Services"
           ],
           "targeted_regions": [
              "Europe",
              "Germany",
              "North America",
              "Russia",
              "Ukraine",
              "United States"
           ]
        },
        "cvss2_temporal_vector": {
          "exploitability": "Unproven",
          "remediation_level": "Official Fix",
          "report_confidence": "Confirmed",
          "raw": "E:U/RL:OF/RC:C"
        },
        "cvss2_vector": {
          "access_complexity": "High",
```

```
        "access_vector": "Network",
        "authentication": "None required",
        "availability_impact": "None",
        "confidentiality_impact": "Partial",
        "integrity_impact": "None",
        "raw": "CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N"
      },
      "cvss3_temporal_vector": {
        "exploitability": "Unproven",
        "remediation_level": "Official Fix",
        "report_confidence": "Confirmed",
        "raw": "E:U/RL:O/RC:C"
      },
      "cvss3_vector": {
        "access_complexity": "High",
        "access_vector": "Network",
        "authentication": "None required",
        "availability_impact": "None",
        "confidentiality_impact": "Low",
        "integrity_impact": "None",
        "raw": "CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N"
      },
      "cvss4_base_score": 8.6,
      "cvss4_threat_vector": {
          "threat_score": 6.1,
          "exploit_maturity": "Unreported",
          "raw": "CVSS:4.0/E:U"
      },
      "cvss4_vector":{
         "attack_vector":"Network",
         "attack_complexity":"Low",
         "attack_requirements":"None",
         "privileges_required":"None",
         "user_interaction":"None",
         "vulnerable_system_confidentiality":"High",
         "vulnerable_system_integrity":"High",
         "vulnerable_system_availability":"High",
         "subsequent_system_confidentiality":"None",
         "subsequent_system_integrity":"None",
         "subsequent_system_availability":"None",
         "raw":"AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N"
      }
    },
    "asset": {
      "uuid": "c8dc1a55-98d3-4eef-a779-8a5978630219",
      "fqdn": "target2.pubtarg.tenablesecurity.com",
      "ipv4s": [],
      "ipv4": null
    },
    "scan": {
      "completed_at": "2025-04-06T04:01:40Z",
      "schedule_uuid": "template-id",
      "started_at": "2025-04-06T04:01:40Z",
      "uuid": "3b500e25-f392-4d37-a0e5-5baacf6a1c3e",
      "target": null
    }
  }
],
"deletes": [
  {
    "id": "0d8c3882-870a-5777-a9ec-25ni25275211",
```

```
      "deleted_at": "2025-04-06T04:01:40Z"
    }
  ],
  "first_ts": "1744708520487",
  "last_ts": "1744708520761"
}
```


Web App Scanning Findings Properties

The following table defines the properties in a Tenable Data Stream web app scanning findings payload file. To see an example file, go to Web App Scanning Findings Payload Files.

Property	Data Type	Description
payload_id	string	The ID of the payload sent from Tenable Vulnerability Management.
version	integer	The version of the payload. This number increments when the payload structure changes.
type	string	The type of payload (`WAS_FINDING`).
count_updated	integer	The number of objects updated in the payload.
count_deleted	integer	The number of objects deleted in the payload.
updates[]	array of objects	Contains the web app scanning findings objects updated in the payload.
updates[].finding_id	string	The unique identifier of the finding (vulnerability).
updates[].url	string	The fully-qualified domain name or URL associated with the finding.
updates[].input_type	string	The type of HTML Form input associated with the finding.

Property	Data Type	Description
updates[].input_name	string	The type of page element that's vulnerable (for example, an HTML form).
updates[].http_method	string	The HTTP method associated with the finding. .
updates[].output	string	The text output from the plugin that detected the finding.
updates[].proof	string	The output from the web application corroborating that the finding is present.
updates[].payload	string	The attack payload used to detect the finding.
updates[].state	string	The state as determined by the Tenable Web App Scanning state service. Possible values include: • `OPEN` — The compliance finding is currently present on an asset. • `REOPENED` — The compliance finding was previously marked as fixed on an asset but has been detected again by a new scan. • `FIXED` — The compliance finding was present on an asset but is no longer detected. • `ACTIVE` — The compliance finding is currently active on

Property	Data Type	Description
		an asset. Note that the API uses different terms for states than the user interface. The `new` and `active` states in the user interface map to the `OPEN` state in the API. The `resurfaced` state in the user interface maps to the `REOPENED` state in the API. The `fixed` state is the same.
`updates[].severity`	string	The severity of the finding as defined using the Common Vulnerability Scoring System (CVSS) base score. Possible values include `info` (CVSS score of 0), `low` (CVSS score between 0.1 and 3.9), `medium` (CVSS score between 4.0 and 6.9), `high` (CVSS score between 7.0 and 9.9), and `critical` (CVSS score of 10.0).
`updates[].severity_id`	integer	The code for the severity assigned when a user recast the risk associated with the finding. Possible values include: • 0 – The vulnerability has a CVSS score of 0, which corresponds to the `info` severity level. • 1 – The vulnerability has a CVSS score between 0.1 and 3.9, which corresponds to the

Property	Data Type	Description
		`low` severity level. • 2 – The vulnerability has a CVSS score between 4.0 and 6.9, which corresponds to the `medium` severity level. • 3 – The vulnerability has a CVSS score between 7.0 and 9.9, which corresponds to the `high` severity level. • 4 – The vulnerability has a CVSS score of 10.0, which corresponds to the `critical` severity level.
`updates[].severity_default_id`	integer	The code for the severity originally assigned to a finding before a user recast the risk associated with the finding. Possible values are the same as for the `severity_id` attribute.
`updates[].severity_modification_type`	string	The type of modification a user made to the finding's severity. Possible values include: • `NONE` – No modification has been made. • `RECASTED` – A user in the Tenable Web App Scanning user interface has recast the risk associated with the finding.

Property	Data Type	Description
		• `ACCEPTED` — A user in the Tenable Web App Scanning user interface has accepted the risk associated with the finding. For more information about recast and accept rules, see Recast/Accept Rules in the *Tenable Vulnerability Management User Guide*.
`updates[].recast_reason`	string	The text that appears in the **Comment** field of the recast rule in the Tenable Web App Scanning user interface.
`updates[].recast_rule_uuid`	string	The UUID of the recast rule that applies to the plugin.
`updates[].first_found`	string	An ISO timestamp indicating the date and time when a scan first detected the finding on the asset.
`updates[].last_found`	string	An ISO timestamp indicating the date and time when a scan last detected the finding on the asset.
`updates[].last_fixed`	string	An ISO timestamp indicating the date and time when a scan no longer detects the previously detected finding on the asset.
`updates[].last_observed`	string	An ISO timestamp indicating the date and time when the finding was previously detected/observed on the asset.

Property	Data Type	Description
updates[].indexed_at	string	An ISO timestamp indicating the date and time when the vulnerability was indexed into Tenable Web App Scanning.
updates[].plugin	object	An object containing plugin details for the finding.
updates[].plugin.epss_score	number	The Exploit Prediction Scoring System (EPSS) score of the finding.
updates[].plugin.id	integer	The ID of the plugin that identified the finding.
updates[].plugin.risk_factor	string	The risk factor of the finding associated with the plugin. The risk factor is determined based on the calculation of the CVSS score. The possible values are: • `LOW` — The vulnerability has a CVSS score between 0.1 and 3.9. • `MEDIUM` — The vulnerability has a CVSS score between 4.0 and 6.9. • `HIGH` — The vulnerability has a CVSS score between 7.0 and 9.9. • `CRITICAL` — The vulnerability has a CVSS score of 10.0.
updates[].plugin.original_risk_factor_num	integer	The code for the severity originally assigned to a plugin.

Property	Data Type	Description
updates[].plugin.locale	string	The plugin language used.
updates[].plugin.type	string	The general type of plugin check (for example, `LOCAL` or `REMOTE`).
updates[].plugin.intel_type	string	The intelligence type/source for the plugin.
updates[].plugin.name	string	The name of the plugin that identified the vulnerability.
updates[].plugin.version	string	The version of the plugin used to perform the check.
updates[].plugin.publication_date	string	An ISO timestamp indicating the date and time the publication date of the plugin.
updates[].plugin.modification_date	string	An ISO timestamp indicating the date and time the last modification date of the plugin.
updates[].plugin.solution	string	Remediation information for the vulnerability.
updates[].plugin.synopsis	string	Brief description of the plugin or vulnerability.
updates[].plugin.description	string	The full text description of the plugin.
updates[].plugin.patch_publication_date	string	An ISO timestamp indicating the date and time the vendor's patch publication date for the plugin.
updates[].plugin.exploitability_ease	string	The vulnerability's ease of exploitability.
updates[].plugin.stig_severity	string	The Security Technical

Property	Data Type	Description
		Implementation Guide (STIG) severity code for the vulnerability.
`updates[].plugin.public_display`	integer	The public display details for the plugin.
`updates[].plugin.in_the_news`	boolean	A value specifying whether this plugin has received media attention (for example, ShellShock, Meltdown).
`updates[].plugin.exploited_by_malware`	boolean	The finding discovered by this plugin is known to be exploited by malware.
`updates[].plugin.cvss2_base_score`	number	The CVSSv2 base score (intrinsic and fundamental characteristics of a finding that are constant over time and user environments).
`updates[].plugin.cvss2_temporal_score`	number	The CVSSv2 temporal score (characteristics of a finding that change over time but not among user environments).
`updates[].plugin.cvss3_base_score`	number	The CVSSv3 base score (intrinsic and fundamental characteristics of a finding that are constant over time and user environments).
`updates[].plugin.cvss3_temporal_score`	number	The CVSSv3 temporal score (characteristics of a finding that change over time but not among user environments).
`updates[].plugin.see_also[]`	array of strings	Links to external websites that contain helpful information about

Property	Data Type	Description
		the vulnerability.
updates[].plugin.bid[]	array of integers	A list of Bugtraq IDs associated with the finding.
updates[].plugin.policy[]	array of strings	A list of policy names associated with the finding.
updates[].plugin.xrefs[]	array of objects	References to third-party information about the finding, exploit, or update associated with the plugin. Each reference includes a type and an ID (for example, `capec` and `2003-047`).
updates[].plugin.xrefs[].type	string	The type of cross-reference (for example, `capec`, `hipaa`, or `iso`).
updates[].plugin.xrefs[].id[]	array of strings	A list of IDs for the cross-reference type.
updates[].plugin.cpe[]	array of strings	The Common Platform Enumeration (CPE) number for the plugin.
updates[].plugin.cve[]	array of strings	The Common Vulnerability and Exposure (CVE) ID for the plugin.
updates[].plugin.cwe[]	array of strings	The Common Weakness Enumeration (CWE) ID for the plugin.
updates[].plugin.wasc[]	array of strings	The Web Application Security Consortium (WASC) ID for the plugin.
updates[].plugin.owasp_2010[]	array of strings	A list of chapters in OWASP Categories 2010 report for the

Property	Data Type	Description
		plugin.
updates[].plugin.owasp_2013[]	array of strings	A list of chapters in OWASP Categories 2013 report for the plugin.
updates[].plugin.owasp_2017[]	array of strings	A list of chapters in OWASP Categories 2017 report for the plugin.
updates[].plugin.owasp_2021[]	array of strings	A list of chapters in OWASP Categories 2021 report for the plugin.
updates[].plugin.owasp_api_2019[]	array of strings	A list of chapters in OWASP Categories API 2019 report for the plugin.
updates[].plugin.vpr_v2	object	An object containing information about the Vulnerability Priority Rating (VPRv2) for the vulnerability.
updates[].plugin.vpr_v2.score	number	The Vulnerability Priority Rating (VPRv2) for the vulnerability. If a plugin is designed to detect multiple vulnerabilities, the VPR score represents the highest value calculated for a vulnerability associated with the plugin. For more information, see Tenable Metrics in the *Tenable Vulnerability Management User Guide*.
updates[].plugin.vpr_v2.vpr_percentile	string	Filter on the VPR v2 score percentile ranking of the CVE, indicating its position relative to

Property	Data Type	Description
		other vulnerabilities.
`updates[].plugin.vpr_v2.vpr_severity`	string	Filter on the VPR v2 severity categorization of the CVE. Options are **Critical**, **High**, **Medium**, **Low**, **Info**.
`updates[].plugin.vpr_v2.exploit_probability`	number	Filter on the probability of exploitation produced by the VPR v2 threat model for the CVE.
`updates[].plugin.vpr_v2.cve_id`	string	Filter on a specific CVE ID for the CVE that is a primary contributor to the calculated VPRv2 score for a vulnerability.
`updates[].plugin.vpr_v2.exploit_code_maturity`	string	Filter on current availability and maturity of exploit code. Options are **High**, **Functional**, **POC**, and **Unproven**.
`updates[].plugin.vpr_v2.on_cisa_kev`	boolean	Filter on whether the CVE is listed on the CISA Known Exploited Vulnerabilities list. Options are **Yes**, **No**.
`updates[].plugin.vpr_v2.exploit_chain[]`	array of strings	Allows filtering on CVEs that are part of an exploit chain.
`updates[].plugin.vpr_v2.in_the_news_intensity_last30`	string	Allows filtering on the volume of news reporting on the CVE within the last 30 days. Options are **Very Low**, **Low**, **Medium**, **High**, **Very High**.
`updates[].plugin.vpr_v2.in_the_news_recency`	string	Allows filtering on the recency of news sources reporting on the

Property	Data Type	Description
		CVE. Options are **No Recorded Events**, **60 to 180 days**, **30 to 60 days**, **14 to 30 days**, **7 to 14 days**, **0 to 7 days**.
`updates[].plugin.vpr_v2.in_the_news_sources_last30[]`	array of strings	Filter on categories of news sources that have referenced the CVE within the last 30 days. Select from one or more of **Academic and Research Institutions**, **Blogs and Individual Researchers**, **Code Repositories**, **Cybersecurity News Media**, **Cybersecurity Vendors**, **Forums and Community Platforms**, **Government and Regulatory**, **Mainstream News and Media**, **Security Research**, **Technology Companies**, **Tools and Resources**, **Other**.
`updates[].plugin.vpr_v2.malware_observations_intensity_last30`	string	Filter on the volume of observed malware exploiting the CVE within the last 30 days. Options are **Very Low**, **Low**, **Medium**, **High**, **Very High**.
`updates[].plugin.vpr_v2.malware_observations_recency`	string	Filter on the recency of observed malware exploiting the CVE. Options are **No Recorded Events**, **60 to 180 days**, **30 to 60 days**, **14 to 30 days**, **7 to 14 days**, **0 to 7 days**.
`updates[].plugin.vpr_v2.threat_summary[]`	object	The object container for information about the threat posed by the

Property	Data Type	Description
		vulnerability, including relevant details that contribute to its Vulnerability Priority Rating (VPR) v2 score.
`updates[].plugin.vpr_v2.threat_summary[].summary`	string	Information about the threat posed by the vulnerability, including relevant details that contribute to its Vulnerability Priority Rating (VPR) v2 score.
`updates[].plugin.vpr_v2.threat_summary[].lastUpdated`	string	Most recent update to threat summary information.
`updates[].plugin.vpr_v2.remediation[]`	object	The object container for information and recommended actions for mitigating or resolving the vulnerability. This may include patches, configuration changes, or other remediation guidance.
`updates[].plugin.vpr_v2.remediation[].summary`	string	Information and recommended actions for mitigating or resolving the vulnerability. This may include patches, configuration changes, or other remediation guidance.
`updates[].plugin.vpr_v2.remediation[].last_updated`	string	Most recent update to remediation summary information.
`updates[].plugin.vpr_v2.targeted_industries[]`	array of strings	Allows filtering on specific industries where attacks leveraging the CVE have been observed. Sample options include **Banking**, **Technology**, **Government**.
`updates[].plugin.vpr_`	array of	Allows filtering on specific

Property	Data Type	Description
v2.targeted_regions[]	strings	geographic regions where attacks leveraging the CVE have been observed.
updates[].plugin.vpr	object	An object containing information about the Vulnerability Priority Rating (VPR) for the vulnerability.
updates[].plugin.vpr.score	number	The Vulnerability Priority Rating (VPR) for the vulnerability. If a plugin is designed to detect multiple vulnerabilities, the VPR represents the highest value calculated for a vulnerability associated with the plugin. For more information, see Severity vs. VPR in the *Tenable Vulnerability Management User Guide*.
updates[].plugin.vpr.drivers	object	The key drivers Tenable uses to calculate a vulnerability's VPR. For more information, see Vulnerability Priority Rating Drivers.
updates[].plugin.vpr.drivers.age_of_vuln	object	A range representing the number of days since the National Vulnerability Database (NVD) published the vulnerability. The valid ranges are: • `0-7 days` • `7-30 days` • `30-60 days` • `60-180 days`

Property	Data Type	Description
		• `180-365 days` • `365-730 days` • `More than 730 days (+731)`
updates[].plugin.vpr.drivers.age_of_vuln.lower_bound	integer	The lower bound of the range. For example, for the 0-7 days range, this attribute is `0`. For the highest range (more than 730 days), this value is `731`.
updates[].plugin.vpr.drivers.age_of_vuln.upper_bound	integer	The upper bound of the range. For example, for the 0-7 days range, this attribute is `7`. For the highest range (more than 730 days), this value is `0`, which signifies that there is no higher category.
updates[].plugin.vpr.drivers.exploit_code_maturity	string	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 (for example, Reversinglabs, Exploit-db, Metasploit). The possible values (`HIGH`, `FUNCTIONAL`, `POC`, or `UNPROVEN`) parallel the CVSS Exploit Code Maturity categories.
updates[].plugin.vpr.drivers.cvss_impact_score_predicted	boolean	A value specifying whether Tenable predicted the CVSSv3 impact score for the vulnerability because NVD

Property	Data Type	Description
		did not provide one (`true`) or used the NVD-provided CVSSv3 impact score (`false`) when calculating the VPR.
updates [].plugin.vpr.drivers.cvss3_impact_score	number	The NVD-provided CVSSv3 impact score for the vulnerability. If the NVD did not provide a score, Tenable Vulnerability Management shows a Tenable-predicted score.
updates [].plugin.vpr.drivers.threat_intensity_last28	string	The relative intensity based on the number and frequency of recently observed threat events related to this vulnerability. The possible values are: • `VERY LOW` • `LOW` • `MEDIUM` • `HIGH` • `VERY HIGH`
updates [].plugin.vpr.drivers.threat_recency	object	A range representing the number of days since a threat event occurred for the vulnerability. The possible ranges are: • `0-7 days` • `7-30 days` • `30-120 days` • `120-365 days`

Property	Data Type	Description
		• `More than 365 days (+365)`
updates[].plugin.vpr.drivers.threat_recency.lower_bound	integer	The lower bound of the range. For example, for the 0-7 days range, this attribute is `0`. For the highest range (more than 365 days), this value is `366`.
updates[].plugin.vpr.drivers.threat_recency.upper_bound	integer	The upper bound of the range. For example, for the 0-7 days range, this attribute is `7`. For the highest range (more than 730 days), this value is `0`, which signifies that there is no higher category.
updates[].plugin.vpr.drivers.threat_sources_last28[]	array of strings	A list of all sources (for example, social media channels, the dark web, etc.) where threat events related to this vulnerability occurred.
updates[].plugin.vpr.drivers.product_coverage	string	The relative number of unique products affected by the vulnerability. The possible values are: • `LOW` • `MEDIUM` • `HIGH` • `VERY HIGH`
updates[].plugin.vpr.updated	string	The ISO timestamp when v last imported the VPR for this vulnerability. v imports a VPR value

Property	Data Type	Description
		the first time you scan a vulnerability on your network. Then, Tenable Web App Scanning automatically re-imports new and updated VPR values daily.
updates[].plugin.vpr.updated_reason	string	The reason for the VPR update.
updates[].plugin.cvss2_temporal_vector	object	CVSSv2 temporal metrics for the vulnerability.
updates[].plugin.cvss2_temporal_vector.exploitability	string	The CVSSv2 Exploitability (E) temporal metric for the vulnerability the plugin covers. The possible values are: • `U` – Unproven • `POC` – Proof-of-Concept • `F` – Functional • `H` – High • `ND` – Not Defined
updates[].plugin.cvss2_temporal_vector.remediation_level	string	The CVSSv2 Remediation Level (RL) temporal metric for the vulnerability the plugin covers. The valid values are: • `O` – Official Fix • `T` – Temporary Fix • `W` – Workaround • `U` – Unavailable • `X` – Not Defined

Property	Data Type	Description
updates[].plugin.cvss2_temporal_vector.report_confidence	string	The CVSSv2 Report Confidence (RC) temporal metric for the vulnerability the plugin covers. The possible values are: • `UC` – Unconfirmed • `UR` – Uncorroborated • `C` – Confirmed • `ND` – Not Defined
updates[].plugin.cvss2_temporal_vector.raw	string	The complete `cvss_temporal_vector` metrics and result values for the vulnerability the plugin covers in a condensed and coded format. For example, `E:U/RL:OF/RC:C`.
updates[].plugin.cvss2_vector	object	Additional CVSSv2 metrics for the vulnerability.
updates[].plugin.cvss2_vector.access_complexity	string	The CVSSv2 Access Complexity (AC) metric for the vulnerability the plugin covers. The possible values are: • `H` – High • `M` – Medium • `L` – Low
updates[].plugin.cvss2_vector.access_vector	string	The CVSSv2 Access Vector (AV) metric for the vulnerability the plugin covers. The possible values are: • `L` – Local

Property	Data Type	Description
		• `A` – Adjacent Network • `N` – Network
`updates[].plugin.cvss2_vector.authentication`	string	The CVSSv2 Authentication (Au) metric for the vulnerability the plugin covers. The possible values are: • `N` – None Required • `S` – Single • `M` – Multiple
`updates[].plugin.cvss2_vector.availability_impact`	string	The CVSSv2 availability impact metric for the vulnerability the plugin covers. The possible values are: • `N` – None • `P` – Partial • `C` – Complete
`updates[].plugin.cvss2_vector.confidentiality_impact`	string	The CVSSv2 confidentiality impact metric for the vulnerability the plugin covers.The possible values are: • `N` – None • `P` – Partial • `C` – Complete
`updates[].plugin.cvss2_vector.integrity_impact`	string	The CVSSv2 integrity impact metric for the vulnerability the plugin covers. The possible values are:

Property	Data Type	Description
		• `N` – None • `P` – Partial • `C` – Complete
`updates[].plugin.cvss2_vector.raw`	string	The complete `cvss_vector` metrics and result values for the vulnerability the plugin covers in a condensed and coded format. For example, `AV:N/AC:M/Au:N/C:C/I:C/A:C`.
`updates[].plugin.cvss3_temporal_vector`	object	An object containing the CVSS v3 temporal vector details.
`updates[].plugin.cvss3_temporal_vector.exploitability`	string	The CVSSv3 Exploit Maturity Code (E) for the vulnerability the plugin covers. The possible values are: • `Unproven` – Corresponds to the Unproven (U) value for the E metric. • `Proof-of-concept` – Corresponds to the Proof-of-Concept (POC) value for the E metric. • `Functional` – Corresponds to the Functional (F) value for the E metric. • `High` – Corresponds to the High (H) value for the E metric. • `Not-defined` – Corresponds to the Not Defined (ND) value

Property	Data Type	Description
		for the E metric.
updates[].plugin.cvss3_temporal_vector.remediation_level	string	The CVSSv3 Remediation Level (RL) temporal metric for the vulnerability the plugin covers. The valid values are: • `O` – Official Fix • `T` – Temporary Fix • `W` – Workaround • `U` – Unavailable • `X` – Not Defined
updates[].plugin.cvss3_temporal_vector.report_confidence	string	The CVSSv3 Report Confidence (RC) temporal metric for the vulnerability the plugin covers. The possible values are: • `U` – Unknown • `R` – Reasonable • `C` – Confirmed • `X` – Not Defined
updates[].plugin.cvss3_temporal_vector.raw	string	The complete `cvss3_temporal_vector` metrics and result values for the vulnerability the plugin covers in a condensed and coded format. For example, `E:U/RL:OF/RC:C`.
updates[].plugin.cvss3_vector	object	Additional CVSSv3 metrics for the vulnerability.
updates[].plugin.cvss3_	string	The CVSSv3 Access Complexity

Property	Data Type	Description
vector.access_complexity		(AC) metric for the vulnerability the plugin covers. The possible values are: • `H` – High • `M` – Medium • `L` – Low
updates[].plugin.cvss3_vector.access_vector	string	The CVSSv3 Attack Vector (AV) metric for the vulnerability the plugin covers. The possible values are: • `Network` – Corresponds to the Network (N) value for the AV metric. • `Adjacent Network` – Corresponds to the Adjacent Network (A) value for the AV metric. • `Local` – Corresponds to the Local (L) value for the AV metric.
updates[].plugin.cvss3_vector.authentication	string	The CVSSv3 Authentication (Au) metric for the vulnerability the plugin covers. The possible values are: • `None required` – Corresponds to the None (N) value for the Au metric. • `Requires-single-instance` – Corresponds to the Single

Property	Data Type	Description
		(S) value for the Au metric. • `Requires-multiple-instances` – Corresponds to the Multiple (M) value for the Au metric.
`updates[].plugin.cvss3_vector.availability_impact`	string	The CVSSv3 availability impact metric for the vulnerability the plugin covers. The possible values are: • `H` – High • `L` – Low • `N` – None
`updates[].plugin.cvss3_vector.confidentiality_impact`	string	The CVSSv3 confidentiality impact metric for the vulnerability the plugin covers.The possible values are: • `H` – High • `L` – Low • `N` – None
`updates[].plugin.cvss3_vector.integrity_impact`	string	The CVSSv3 integrity impact metric for the vulnerability the plugin covers. The possible values are: • `H` – High • `L` – Low • `N` – None
`updates[].plugin.cvss3_vector.raw`	string	The complete `cvss3_vector` metrics and result values for the

Property	Data Type	Description
		vulnerability the plugin covers in a condensed and coded format. For example, `AV:N/AC:M/Au:N/C:C/I:C/A:C`.
`updates[].plugin.cvss4_base_score`	number	The CVSS v4.0 base score (intrinsic and fundamental characteristics of a finding that are constant over time and user environments).
`updates[].plugin.cvss4_threat_vector`	object	An object representing the CVSS v4.0 Threat metrics for the vulnerability. These metrics provide context on current, observed threat activity in the wild, such as evidence of exploitation or the presence of available exploit code. Threat metrics can help refine the severity and prioritization of vulnerabilities beyond their intrinsic characteristics. For more details, see the CVSS v4.0 Specification.
`updates[].plugin.cvss4_threat_vector.exploit_maturity`	string	The CVSS v4.0 Exploit Maturity (E) metric, indicating the current development status of exploit techniques or code for the vulnerability. For more details, see the CVSS v4.0 Specification.
`updates[].plugin.cvss4_threat_vector.raw`	string	The complete `cvss4_threat_vector` metrics and their result values for the vulnerability, expressed as a concise, coded

Property	Data Type	Description
		string. This threat vector is typically appended to the CVSSv4 Base vector. For example, `CVSS:4.0/E:U`. For more details, see the CVSS v4.0 Specification.
updates[].plugin.cvss4_threat_vector.threat_score	string	The CVSS v4.0 threat score (CVSS-T), which adjusts the base score by incorporating real-world threat intelligence, such as the presence of active exploitation, exploit code availability, or observed malware activity. This score reflects the current threat landscape for the vulnerability. For more details, see the CVSS v4.0 Specification.
updates[].plugin.cvss4_vector	object	Additional CVSS v4.0 metrics for the vulnerability.
updates[].plugin.cvss4_vector.attack_vector	string	The context where vulnerability exploitation is possible, such as **Network** or **Local**.
updates[].plugin.cvss4_vector.attack_complexity	string	The conditions beyond the attacker's control that must exist to exploit the vulnerability.
updates[].plugin.cvss4_vector.attack_requirements	string	The resources, access, or specialized conditions required for an attacker to exploit the vulnerability.
updates[].plugin.cvss4_vector.privileges_required	string	The permission level attackers require to exploit the vulnerability.

Property	Data Type	Description
		Options are **High**, **Low**, or **None**. For example, **None** means attackers need no permissions in your environment and can exploit the vulnerability while unauthorized.
updates[].plugin.cvss4_vector.user_interaction	string	The level of user involvement required for an attacker to exploit the vulnerability.
updates[].plugin.cvss4_vector.vulnerable_system_availability	string	The impact on the availability of the vulnerable system when successfully exploited.
updates[].plugin.cvss4_vector.vulnerable_system_confidentiality	string	The impact on the confidentiality of the vulnerable system when successfully exploited.
updates[].plugin.cvss4_vector.vulnerable_system_integrity	string	The impact on the integrity of the vulnerable system when successfully exploited.
updates[].plugin.cvss4_vector.subsequent_system_availability	string	The impact on the availability of systems that can be impacted after the vulnerable system is exploited.
updates[].plugin.cvss4_vector.subsequent_system_confidentiality	string	The impact on the confidentiality of systems that can be impacted after the vulnerable system is exploited.
updates[].plugin.cvss4_vector.subsequent_system_integrity	string	The impact on the integrity of systems that can be impacted after the vulnerable system is exploited.
updates[].plugin.cvss4_vector.raw	string	The complete `cvss4_vector` metrics and result values for the

Property	Data Type	Description
		vulnerability the plugin covers in a condensed and coded format. For example, `AV:N/AC:M/Au:N/C:C/I:C/A:C`.
updates[].asset	object	Information about the asset where the scan detected the vulnerability.
updates[].asset.uuid	string	The UUID of the asset where a scan found the vulnerability.
updates[].asset.fqdn	string	The fully qualified domain name for the asset.
updates[].asset.ipv4s[]	array of strings	This value always returns as null.
updates[].asset.ipv4	string	This value always returns as null.
updates[].scan	object	Information about the latest scan that detected the vulnerability.
updates[].scan.completed_at	string	The ISO timestamp when the scan completed.
updates[].scan.schedule_uuid	string	The schedule UUID for the scan that found the vulnerability.
updates[].scan.started_at	string	The ISO timestamp when the scan started.
updates[].scan.uuid	string	The UUID of the scan that found the vulnerability.
updates[].scan.target	string or null	The target IP or hostname of the scan.
deletes[]	array of objects	Contains the host audit objects deleted in the payload.

Property	Data Type	Description
`deletes[].id`	string	The ID of the deleted host audit.
`deletes[].deleted_at`	string	An ISO timestamp indicating the date and time when the host audit was deleted.
`first_ts`	string	A Unix timestamp indicating the date and time of the first entry in the payload.
`last_ts`	string	A Unix timestamp indicating the date and time of the last entry in the payload.

Welcome to Tenable Lumin

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

> 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.

You can use Tenable Lumin to quickly and accurately assess your 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.

Tenable-provided metrics help you quantify your risk to make informed remediation and strategic security decisions. For more information about the metrics used in Tenable Lumin analysis, see Tenable Lumin Metrics.

For information on how to prepare, install, and configure Tenable Lumin, see Get Started with Tenable Lumin.

Get Started with Tenable Lumin

> 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.

You can use Tenable Lumin to quickly and accurately assess your 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.

Tenable recommends the following to get started with Tenable Lumin data and functionality.

License and Enable

Acquire a Tenable Lumin license and enable Tenable Lumin in Tenable Vulnerability Management.

1. To add Tenable Lumin to your Tenable Vulnerability Management license, contact your Tenable representative.
2. In your browser, disable features that may prevent you from enabling Tenable Lumin:
   - Ad blocker extensions
   - Do Not Track (Mozilla Firefox, Google Chrome, Apple Safari, or Microsoft Internet Explorer)
   - Protected Mode (Microsoft Internet Explorer)

   Tip: You can re-enable these features after you fully enable Tenable Lumin.
3. Log in to Tenable Vulnerability Management.

   The Tenable Lumin welcome window appears.
4. Follow the wizard to enable Tenable Lumin.

   The **Lumin** dashboard appears.

Prepare

Generate data and learn about Tenable Lumin terminology.

Tenable Vulnerability Management Only	Tenable Security Center + Tenable Vulnerability Management Tenable Lumin
1. Run an authenticated assessment scan in Tenable Vulnerability Management to generate vulnerability data. **Note:** You must run scans to start seeing data in Tenable Lumin views; Tenable Lumin shows scan result data generated after you licensed Tenable Lumin. For more information, see Tenable Lumin Data Timing. **Note:** Tenable Lumin does not support	1. Sync repositories to Tenable Lumin from Tenable Security Center. All vulnerability data is synced immediately. **Note:** Tenable Lumin does not support third-party integration data. 2. Create assets in Tenable Security Center to add business context to your assets. 3. Configure Tenable Security Center to

third-party integration data.

2. Create tags in Tenable Vulnerability Management to add business context to your assets.
3. Review the metrics terminology to understand Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) values and how they impact your Asset Exposure Score (AES), Assessment Maturity grade, and Cyber Exposure Score (CES).
4. Allow sufficient time for your metrics to calculate. For more information, see Tenable Lumin Data Timing.

Tenable Lumin synchronization.

Allow sufficient time for the synchronization to complete. For more information, see Tenable Lumin Data Timing.

4. View your assets as business context *tags* in Tenable Vulnerability Management. For more information, see Add a Tag to an Asset.
5. Review the metrics terminology to understand Vulnerability Priority Rating (VPR) and Asset Criticality Rating (ACR) values and how they impact your Asset Exposure Score (AES), Assessment Maturity grade, and Cyber Exposure Score (CES).
6. Allow sufficient time for your metrics to calculate. For more information, see Tenable Lumin Data Timing.

Assess Your Exposure

Note: All Tenable Lumin data reflects all assets within the organization's Tenable Vulnerability Management instance.

Review your CES and perform vulnerability management analysis.

1. Use the Tenable Lumin dashboard to understand your CES and access details pages.
    - **Cyber Exposure Score** widget – How does your overall risk compare to other Tenable customers in your Salesforce industry and the larger population?
    - **Cyber Exposure Score Trend** widget – How has the overall risk for your entire organization changed over time?

- **Assessment Maturity** widget – How frequently and thoroughly are you scanning your assets?
- **Remediation Maturity** widget – How quickly and thoroughly are you remediating vulnerabilities on your assets?
- **Reduce Cyber Exposure Score** widget – What would the impact be if you addressed all of your top 20 recommended actions?
- **Asset Criticality Rating Breakdown** widget – How critical are your assets?
- **Asset Scan Distribution widget** – What types of scans have run on your assets?
- **Mitigations** widget – What endpoint protection agents are running on your assets?
- **Cyber Exposure Score by Business Context/Tag** widget – How do assets with different tags (unique business context) compare?

2. To browse the most critical vulnerabilities on your network, sort your vulnerabilities by VPR.
3. To browse the most critical assets on your network, sort your assets by ACR.

Customize Your ACR Values

Review the Tenable-provided ACR values and customize them to reflect the unique infrastructure or concerns of your organization.

1. Use the Assets page to review the Tenable-provided ACR values for your assets.
    - Do any of your assets have ACR values that seem too high for the relative criticality of that asset?
    - Do any of your assets have ACR values that seem too low for the relative criticality of that asset?
2. If necessary, manually customize your asset ACR values.

Lower Your CES and AES

You must address vulnerabilities on your network to lower your CES and AES.

Important: Private findings are excluded from all scores in Tenable Lumin. For more information see Findings.

1. View lists of Tenable-recommended action items:

    - Top recommended actions for all assets on your network.

      Export your top recommended actions, as necessary.

    - All solutions on your network.

      Export your solutions, as necessary.

2. Follow the recommendations and take steps to address the vulnerabilities on your network.

Mature

Mature your vulnerability management strategy.

- Continue monitoring and addressing vulnerabilities to lower your CES and AES.
- Continue exporting and sharing recommended actions (solutions) data with others in your organization to refine your vulnerability management strategy.

Tenable Lumin Metrics

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

> 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 Tenable Lumin uses several metrics to help you assess your risk.

- Cyber Exposure Score (CES)
- Vulnerability Priority Rating (VPR)
- Asset Criticality Rating (ACR)
- Asset Exposure Score (AES)
- Assessment Maturity Grade
- Remediation Maturity Grade

For information about improving the accuracy of your Tenable Lumin metrics and increasing your overall vulnerability management health, see Improve Your Tenable Lumin Metrics.

Important: Private findings are excluded from all scores in Tenable Lumin. For more information see Findings.

Cyber Exposure Score (CES)

Tenable calculates a dynamic CES that represents exposure risk as an integer between 0 and 1000, based on the Asset Exposure Score (AES) values for licensed assets scanned in the last 90 days. Higher CES values indicate higher risk.

You can view CES for different groups of licensed assets, including:

- the overall CES for your entire organization (for example, the CES displayed in the **Cyber Exposure Score** widget)
- the tag-level CES for assets in a specific business context (for example, the CES displayed in the **Cyber Exposure Score by Business Context/Tag** widget).

CES Category	CES Range
High	650 to 1000
Medium	350 to 649
Low	0 to 349

To view the CES for your entire organization or for a group of assets, view the widgets on the View the Tenable Lumin Dashboard.

For more information about how long Tenable Vulnerability Management takes to calculate or recalculate your CES, see Tenable Lumin Data Timing.

Vulnerability Priority Rating (VPR)

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 Vulnerability Management provides a VPR value the first time you scan a vulnerability on your network. Then, Tenable Vulnerability Management automatically provides new and updated VPR values daily.

Tenable recommends prioritizing vulnerabilities with the highest VPRs that are present on your assets with the highest ACRs.

To view the VPR for a specific vulnerability, view vulnerabilities as described in Findings.

VPR Key Drivers

Tenable uses the following key drivers to calculate a vulnerability's VPR.

Note: Tenable does not customize these values for your organization; VPR key drivers reflect a vulnerability's global threat landscape.

Key Driver	Description
Age of Vuln	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 Vulnerability Management 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

Asset Criticality Rating (ACR)

Tenable assigns an ACR to each asset on your network to represent the asset's relative criticality as an integer from 1 to 10. A higher ACR indicates higher criticality.

ACR Category	ACR Range
Critical	9 to 10
High	7 to 8
Medium	4 to 6
Low	1 to 3

Because Tenable Vulnerability Management calculates ACR values every 24 hours, you may need to wait up to 24 hours to view the ACR after scanning the asset on your network.

Note: Tenable recommends reviewing your Tenable-provided ACR values and overriding them, if necessary. You can customize ACR values to reflect the unique infrastructure or needs of your organization, as described in Edit an ACR.

If an asset receives multiple ACR values, Tenable Vulnerability Management prioritizes the values in the following order:

1. If set, the manually overridden ACR value.
2. The Tenable-provided ACR value.

To view the ACR for a specific asset, view the asset details as described in View Asset Details.

ACR Key Drivers

Tenable uses the following key drivers to calculate an asset's Tenable-provided ACR.

Note: Tenable does not customize these values for your organization; ACR key drivers reflect the global threat landscape associated with the asset's characteristics.

Note: Running unauthenticated scans may result in limited or incomplete ACR key drivers.

Key Driver Types:

Key Driver	Description
device_type	The device type. For example:

	• **hypervisor** – The device is a Type-1 hypervisor that hosts a virtual machine (e.g., Microsoft Hyper-V, VMware ESX/ESXi, or Xen). • **printer** – The device is a networked printer or a printing server.
device_capability	The device's business purpose. For example: • **file_server** – The device is a server that provides file sharing services (e.g., an FTP, SMB, NFS, or NAS server). • **mail_server** – The device is a server designated for sending and receiving emails.
internet_exposure	The device's location on your network and proximity to the internet. For example: • **internal** – The device is located within your local area network (LAN), possibly behind a firewall. • **external** – The device is located outside your LAN and not behind a firewall.

ACR Device Capabilities:

Part of ACR device capabilities are defined by which software is installed on the target host.

Capability	Description	Software or Services
accounting_system	An accounting solution is installed on the target asset.	Intuit Quickbooks
backup_agent	A backup solution agent is installed on the target asset.	Amanda backup (agent)

analytics_system	A software solution for data analytics and reporting is installed on the target host.	QlikView
		TIBCO Spotfire
		IBM SPSS
		SharePoint 2013
		SOLR
		Elasticsearch
		Enterprise Search
		Google Search Appliance
		Lucene
		SQL Server Reporting Services
		Oracle BI publisher
		SAP Business Object
backup_server	An enterprise backup solution is installed or running on the target host.	Acronis Backup
		Quest NetVault
		Unitrends Enterprise Backup
		Veritas Backup Exec
		Spectrum Protect (formerly Tivoli Storage Manager)

crm_system	A Customer Relation Management (CRM) solution is installed or running on the target host	SugarCRM
		Bitrix24 CRM
		Siebel CRM

database_server	A database system is installed on the target host or a database server is running on the target host.	PostgreSQL
		Microsoft SQL Server
		MongoDB
		Oracle Database
		Db2 Hosted
		Percona XtraDB Cluster
		IBM Informix
		PostgreSQL
		Percona Server
		MariaDB Cluster
		MySQL
		Microsoft SQL Server
		SAP Adaptive Server Enterprise (ASE)
		MariaDB Server
		SQLite
		Apache Derby Network Server
		SAP DB
		Cogent Datahub Server

directory_server	The target asset is an authentication server.	McAfee Stonegate Authentication Server
		Kerberos Ticketing Server
		LDAP protocol
		IBM Tivoli
		Stonegate Auth Server
dns_server	A DNS server is running on the target asset.	DNS Service on Port 53
erp_system	An Enterprise Resource Planning Suite server is running or is installed on the target asset.	Microsoft Dynamics AX
		Oracle E-Business Suite
		SAP ERP
		Microsoft Dynamics GP
		SAP DB
		SAPControl
		SAP RMI-P4 Protocol Service
		SAP Host Control
		Apache OFBiz
erp_system_client	The target asset has installed a client software for accessing ERP systems.	SAP GUI

file_server	The target asset is used for file sharing purposes. The file sharing here is a narrow sense. SMB server is not considered as a file server in this classification.	WebCenter
		ownCloud
		Sharepoint
		Oracle WebCenter Content
		Sharepoint
		FTP service
		Apple File Protocol (AFP) service
		Network File System (NFS) Server Detection
helpdesk_system	A help desk ticketing server is installed or running on the target asset.	SugarCRM
		Track-It!
		ServiceDesk Plus
		OTRS
		ManageEngine Service Desk

it_management_system	The target asset performs some types of IT management function. It can be IT infrastructure management, including managing a single or a group of devices or services, or IT service management such as software provisioning, device, or software repository management.	Application Insight

		Solarwinds Server & Application Monitor
		ManageEngine Application Performance Monitoring
		System Center Operations Manager
		Applications Manager- ManageEngine
		ManageEngine Desktop Central
		Ghost Solution Suite
		ZENworks - Configuration Management
		IBM BigFix
		System Center Configuration Manager
		CA Unified Infrastructure Management
		Centreon
		VMware vRealize

		Operations

		OpManager

		Nagios XI

		SCOM

		PRTG Network Monitor
		Zabbix
		SolarWinds Storage Resource Monitor
		GroundWork Monitor
		Pandora FMS
		Tivoli Monitoring
		OP5 Monitor
		NetFlow Traffic Analyzer
		PRTG Network Monitor
		Cisco Prime Infrastructure
		H3C Intelligent Management Center
		ZENworks Asset Management
		ManageEngine Desktop Central
		Unified Endpoint Manager
		Google Analytics

		Cisco Prime Infrastructure
		H3C Intelligent Management Center
		HP 3PAR Management Server
		Ghost Solution Suite
		Fortigate Firewall Management Console
		Barracuda Spam & Virus Firewall Management Web Console
mail_server	The target asset is a mail server.	IBM Domino
		IMAP Service Detection
		CCProxy SMTP Server Detection
		SMTP Service Detection
		POP Service Detection
pci	The target asset has PCI sensitive information.	PCI Plugin Fired
pci-target	The target asset is a PCI scan target.	"pci" Keyword

		Found in Scan Name
proxy_server	The target asset is a proxy server.	Oracle iPlanet Web Proxy Server
		HTTP proxy Detected in Service Banner
		McAfee Email Gateway
reverse_proxy_server	The target asset is a reverse proxy that directs external client requests to internal servers. A reverse proxy can be an ADC or a load-balancer.	NetApp SANtricity Web Services Proxy
		Foreman Smart-Proxy TFTP
rnd_software	The target asset is for development purposes because product development software is installed on it.	Red Hat Mobile Application Platform
		Application Testing Suite
		Windows Visual Studio
		AutoCAD
		MAC OS Xcode IDE
		Autodesk DWG TrueView Detection
scada	Software systems used for managing industrial	AVEVA InduSoft

	processes are installed or running on the target asset.	Web Studio / InTouch Edge HMI TCP/IP Server
		Trihedral VTScada Detection
upnp	The target asset supports UPnP. It is likely to be an appliance.	UPnP service detection

web_application_server	There is a web application server running or installed on the target asset. Having a web application server running on the target asset does not necessarily indicate its criticality. But it can hint criticality when used in together with some properties, e.g. web application server + external + server device type = high criticality.	Geronimo
		Resin
		Tuxedo
		Tomcat
		Jetty
		Red Hat OpenShift
		Microsoft .NET Platform
		Red Hat Jboss EAP
		WebLogic Server
		Magento
		WebSphere Commerce
		Cobalt
		DNN Platform
		Umbraco
		Oracle WebCenter Sites
		Glassfish
		nginx
		Microsoft IIS

Asset Exposure Score (AES)

Tenable calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.

Tenable calculates AES based on the current ACR (Tenable-provided or custom) and the VPRs associated with the asset.

AES Category	AES Range
High	650 to 1000
Medium	350 to 649
Low	0 to 349

To view the AES for a specific asset, see Assets.

Assessment Maturity Grade

Important: Your Assessment Maturity and Remediation Maturity scores may have recently changed due to data migration and algorithm changes within Tenable Lumin. This is expected behavior. For more information, contact your Tenable representative.

Assessment Maturity provides a high-level summary of how effectively you are scanning for vulnerabilities on your licensed assets. Tenable calculates a dynamic Assessment Maturity grade that represents your assessment scanning health as a letter grade between **A** and **F**. An **A** grade indicates you are assessing your assets frequently and thoroughly.

Tenable provides an Assessment Maturity grade the first time you scan. Then, Tenable Vulnerability Management automatically provides an updated Assessment Maturity grade daily.

Assessment Maturity Letter Grade	Numerical Range
A	75 to 100
B	55 to 74
C	30 to 54
D	15 to 29
F	0 to 14

How is my Assessment Maturity calculated?

- For asset scores:
  - **Scan Frequency** score — How often the asset was scanned within the last 90 days
  - **Scan Depth** score — Whether or not the asset was in an authenticated scan within the last 90 days
  - **Assessment Maturity** score — A calculation of (Scan Frequency score + Scan Depth score) / 2
- For a container/business context score:
  - **Scan Frequency** score — the average of the asset Scan Frequency scores
  - **Scan Depth** score — the average of the asset Scan Depth scores
  - **Assessment Maturity** score — the average of the asset Assessment Maturity scores

Scan Depth Score

A high depth grade indicates you are running authenticated scans on these assets.

Depth Grade Letter Grade	Numerical Range
A	75 to 100
B	55 to 74
C	30 to 54
D	15 to 29
F	0 to 14

Scan Frequency Score

Tenable calculates your frequency grade based on how often you scan assets on your network. A high frequency grade indicates you are scanning your assets often.

Frequency Grade Letter Grade	Numerical Range
A	75 to 100
B	55 to 74
C	30 to 54

D	15 to 29
F	0 to 14

To view your Assessment Maturity grade, depth grade, and frequency grade, see View Assessment Maturity Details.

For more information about how long Tenable Vulnerability Management takes to calculate or recalculate your Assessment Maturity grade, see Tenable Lumin Data Timing.

Remediation Maturity Grade

> **Important**: Your Assessment Maturity and Remediation Maturity scores may have recently changed due to data migration and algorithm changes within Tenable Lumin. This is expected behavior. For more information, contact your Tenable representative.

Remediation Maturity provides a high-level summary of how effectively you are remediating vulnerabilities on your licensed assets. Tenable calculates a dynamic Remediation Maturity grade that represents your remediation health as a letter grade between **A** and **F**. An **A** grade indicates you are remediating the vulnerabilities on your assets quickly and thoroughly.

Remediation Maturity Letter Grade	Numerical Range
A	75 to 100
B	55 to 74
C	30 to 54
D	15 to 29
F	0 to 14

Your Remediation Maturity grade is the combination of your Remediation Maturity *remediation responsiveness grade* and your Remediation Maturity *remediation coverage grade*.

Tenable provides a Remediation Maturity grade the first time you remediate a vulnerability. Then, Tenable Lumin automatically provides an updated Remediation Maturity grade daily.

Remediation Responsiveness Grade

Tenable calculates your remediation responsiveness grade based on how long it takes you to remediate a vulnerability after it is first discovered (the **First Seen** date).

A high remediation responsiveness grade indicates you are quickly remediating the vulnerabilities on your assets.

Remediation Responsiveness Letter Grade	Numerical Range
A	75 to 100
B	55 to 74
C	30 to 54
D	15 to 29
F	0 to 14

Remediation Coverage Grade

Tenable calculates your remediation coverage grade based on the percentage of remediated vulnerabilities on your assets.

A high remediation coverage grade indicates you are remediating a high percentage of the vulnerabilities on your assets.

Remediation Coverage Letter Grade	Numerical Range
A	75 to 100
B	55 to 74
C	30 to 54
D	15 to 29
F	0 to 14

To view your Remediation Maturity grade, remediation responsiveness grade, and remediation coverage grade, see View Remediation Maturity Details.

For more information about how long Tenable Lumin takes to calculate or recalculate your Remediation Maturity grade, see Tenable Lumin Data Timing.

Improve Your Tenable Lumin Metrics

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

If you want to improve the accuracy of your Tenable Lumin metrics and increase your overall vulnerability management health, evaluate your Tenable-provided values and your scanning strategy.

Important: Private findings are excluded from all scores in Tenable Lumin. For more information see Findings.

To improve the accuracy of your Tenable Lumin metrics:

1. On the Assessment Maturity Details page, review your Assessment Maturity grade to evaluate your overall scanning health.

   Do any of the following, depending on what your data shows:

   - Perform any actions described in the **Recommended Actions** widget.
   - View details about your Assessment Maturity depth grade in the **Depth Grade** widget. If necessary, improve your depth grade by increasing the number of plugins enabled in your user-defined templates or scans, or by increasing the number of authenticated or agent scans. For more information, see Configure Plugins in Tenable Vulnerability Management Scans, Credentials in Tenable Vulnerability Management Scans, or Scan Templates.

   Better overall scanning health results in a higher Assessment Maturity score.

   If you improve your Assessment Maturity score, you improve the accuracy of your Tenable-provided ACR and VPR values. Then, more accurate ACR and VPR values improve the accuracy of your AES and CES values.

2. In the Assets table, review your Tenable-provided ACR values to evaluate the characterizations of the assets on your network. If the ACR values do not reflect the unique infrastructure or needs of your organization, you can override them. For more information, see Edit an ACR Manually.

   More accurate ACR values improve the accuracy of your AES and CES values.

3. On the Remediation Maturity Details page, review your Remediation Maturity grade to evaluate your overall vulnerability remediation health.

Do any of the following, depending on what your data shows:

- Perform any actions described in the **Recommended Actions** widget.
- View details about your Remediation Maturity remediation responsiveness grade in the **Remediation Responsiveness Grade** widget. If necessary, improve your remediation responsiveness grade by quickly remediating your most critical (highest VPR) vulnerabilities. For more information, see View Recommended Actions.
- View details about your Remediation Maturity remediation coverage grade in the **Remediation Coverage Grade** widget. If necessary, improve your remediation coverage grade by increasing the number of vulnerabilities you remediate. For more information on the assets with the most critical vulnerabilities, see the **Vulnerability Priority Rating (VPR)** widget described in Vulnerability Management Dashboard.

Better overall remediation health results in a higher Remediation Maturity score.

Edit an ACR Manually

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required Additional License: Tenable Lumin

Required User Role: Administrator

You can customize an asset's Asset Criticality Rating (ACR) value to reflect the unique infrastructure or needs of your organization. You can edit the ACR for a single asset independently or multiple assets simultaneously.

Tip: Changes to an ACR value (and recalculations for your AES and CES values) take effect within 24 hours.

Tip: For information about how Tenable Vulnerability Management prioritizes manually overridden ACR values, see Asset Criticality Rating (ACR).

Important: Edits to your Tenable Lumin ACR do not sync to any connected Tenable Security Center consoles.

Note: All Tenable Lumin data reflects all assets within the organization's Tenable Vulnerability Management instance.

To edit the ACR for a single asset:

1. In the Tenable Vulnerability Management interface, do one of the following:

Location	Action
Asset Details page	a. Access the Asset Details page. b. Click an asset row. The **Asset Details** page appears. c. In the **Asset Criticality Rating** section, click the ✎ button. The Tenable Lumin **Edit Asset Criticality Rating** plane appears.
Assets page	a. Access the Assets page. b. In the assets table, roll over the asset you want to edit. c. Click the ⋮ button. d. Click the ✎ **Edit ACR** button. The **Edit Asset Criticality Rating** plane appears.

2. Do one of the following:
   - To modify the ACR value, click or drag 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**.
3. (Optional) If you want to include a justification for your ACR change, in the **Overwrite Reasoning** section, select one or more reasons.

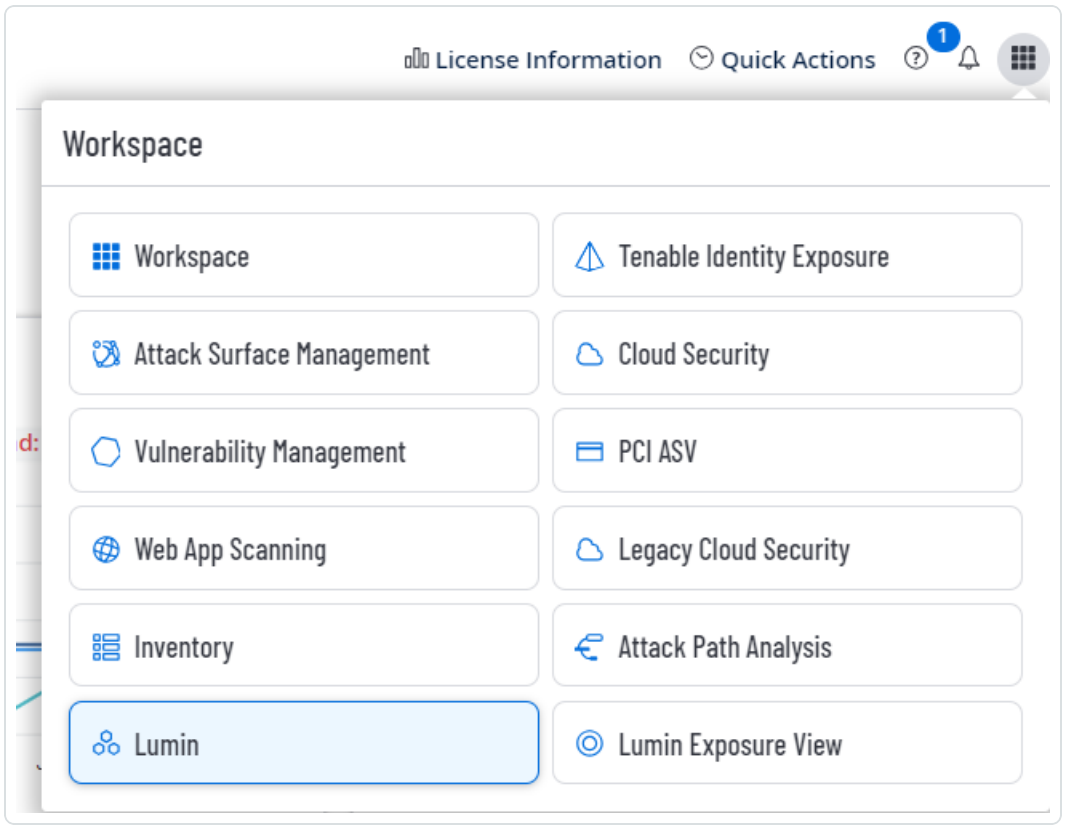
For example, if an asset in your development lab environment received a Tenable-assigned ACR appropriate for a more public asset, you could select **Dev Only** as the overwrite reasoning.

4. (Optional) If you want to include a note about your ACR change, in the **Notes** section, type a note.
5. Click **Save**.

   Tenable Vulnerability Management saves the custom ACR.

To edit the ACR for multiple assets:

1. In the Workspace menu, click **Lumin**.



   The **Lumin** dashboard appears.

2. In the **Cyber Exposure Score by Business Context/Tag** widget, click the tag for which you want to view asset details.

   The Tenable Lumin **Business Context/Tag Asset Details** page appears, filtered by the tag you selected.

3. Access the **Assets** page through the **Asset Criticality Rating Breakdown** widget, the **Asset Scan Distribution** widget, or the **Asset Scan Frequency** widget, as described in View Business Context/Tag Asset Details.

   The **Assets** page appears, filtered by your widget selection.

4. In the table, select the check boxes next to the assets that you want to edit.

   The action bar appears at the bottom of the page.

5. In the action bar, click the ✎ button.

   The Tenable Lumin **Edit Asset Criticality Rating** plane appears.

6. Click and drag the **Asset Criticality Rating** slider to set the ACR.

7. (Optional) If you want to include a justification for your ACR change, in the **Overwrite Reasoning** section, select one or more reasons.

8. (Optional) If you want to include a note about your ACR change, in the **Notes** section, type a note.

9. Click **Save**.

   Tenable Vulnerability Management saves the custom ACR for all selected assets.

Tenable Lumin Data Timing

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Run scans to generate vulnerability data for use in Tenable Lumin views.

- Time to Show Tenable Vulnerability Management Scan Result Data
- Time to Synchronize Data from Tenable Security Center
- Time to Calculate or Recalculate Your CES, Assessment Maturity, or Remediation Maturity Grade

Time to Show Tenable Vulnerability Management Scan Result Data

Vulnerability data generated by Tenable Vulnerability Management scans appears in Tenable Lumin views immediately upon scan completion.

Newly generated data does not immediately impact your Tenable Lumin metrics (for example, your CES). Tenable requires more time to recalculate your metrics. For more information, see Time to Calculate or Recalculate Your CES, Assessment Maturity, or Remediation Maturity Grade.

Time to Synchronize Data from Tenable Security Center

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 repositories.	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 metrics (for example, your CES). Tenable requires up to 48 hours to recalculate your metrics.
Asset data (*tags* in Tenable Vulnerability Management)	Manual (on-demand) synchronizations only.	All data and recalculated Tenable Lumin metrics appear in Tenable Vulnerability Management within 48 hours.

For more information about Tenable Security Center synchronization, see Tenable One Synchronization in the *Tenable Security Center User Guide*.

Time to Calculate or Recalculate Your CES, Assessment Maturity, or Remediation Maturity Grade

Tenable Lumin can take up to 24 hours to calculate or recalculate your metrics after any of the following events:

- You run your first Tenable Vulnerability Management-configured scans after licensing Tenable Lumin.

- You initiate your first Tenable Security Center synchronization after licensing Tenable Lumin.
- Tenable Vulnerability Management runs a scan.
- Tenable Security Center runs a scan that imports new data to a synchronized repository.

Tip: Tenable Vulnerability Management calculates Tenable Lumin metrics based on your licensed assets seen in the last 90 days. If you change your scanning configuration (for example, you perform a recommended action to increase your Assessment Maturity grade), your changes influence the next scheduled recalculation, but take more time over the next 90 days to impact significantly and overhaul your metrics.

View the Tenable Lumin Dashboard

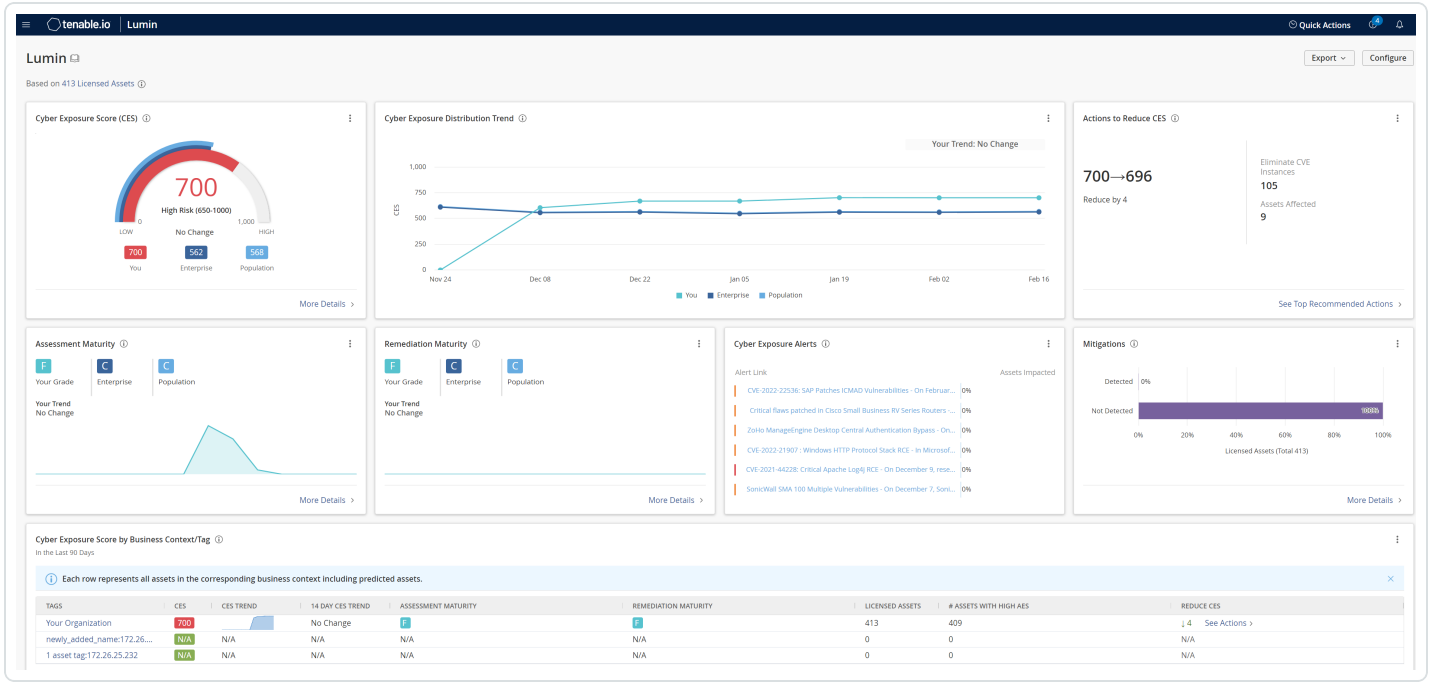
The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

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.

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

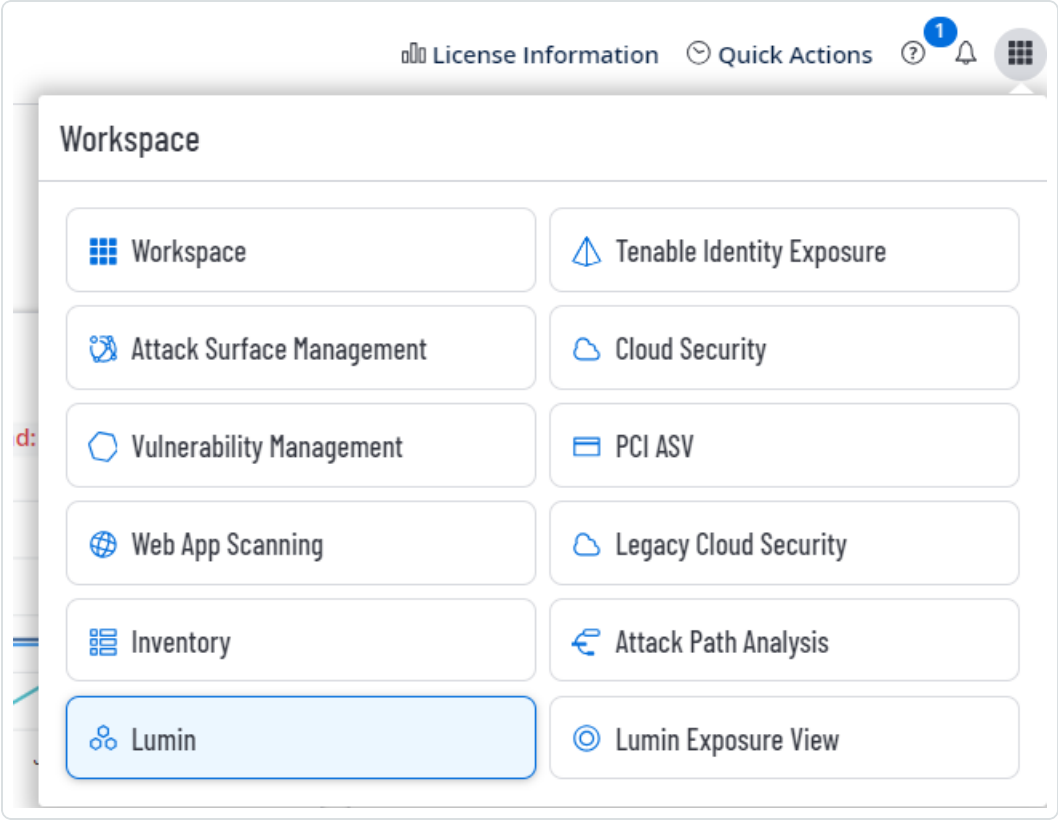
The Tenable-provided Tenable Lumin dashboard visualizes exposure data for your organization. You cannot customize the widgets on this Tenable-provided dashboard.



Important! Tenable One customers can access Tenable Lumin directly from the Workspace page.

To view summary data in the Tenable Lumin dashboard:

1. In the Workspace menu, click **Lumin**.



The **Lumin** dashboard appears.

Note: All Tenable Lumin data reflects all assets within the organization's Tenable Vulnerability Management instance.

Export the Tenable Lumin Dashboard Landing Page

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

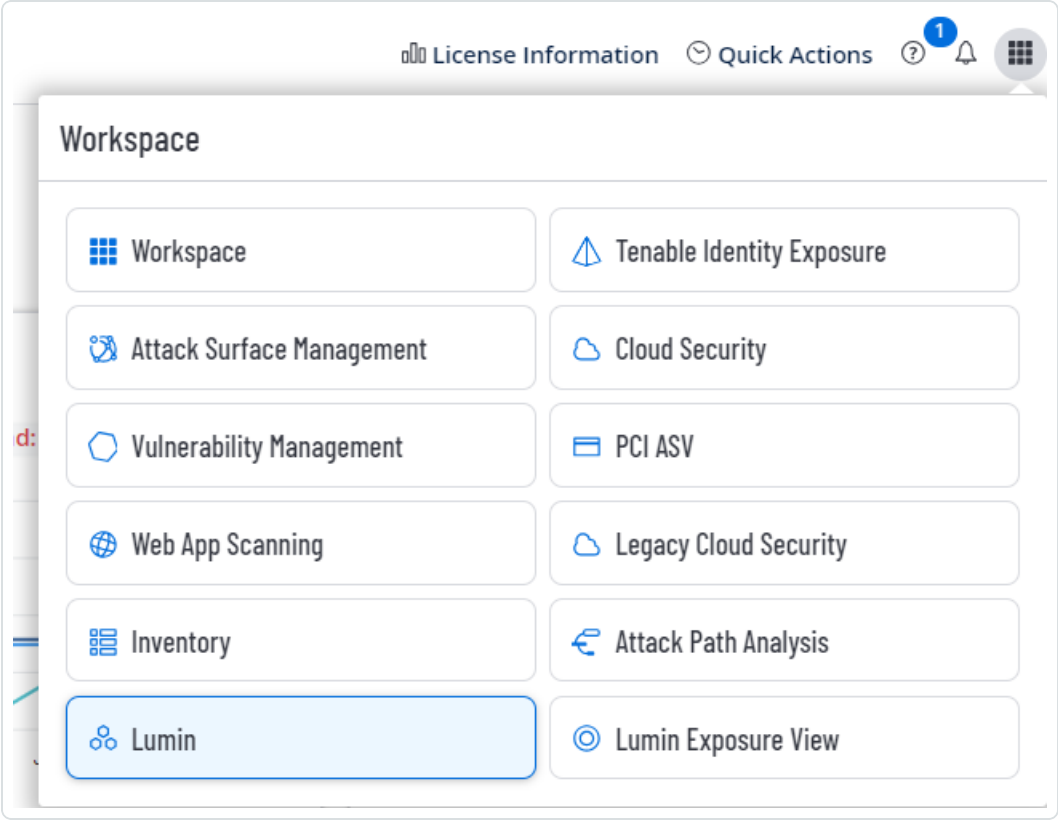
Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

In Tenable Vulnerability Management, you can export the Tenable Lumin dashboard landing page.

To export the Tenable Lumin dashboard landing page:

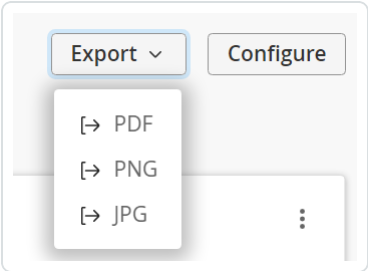
1. In the Workspace menu, click **Lumin**.



   The **Lumin** dashboard appears.

2. In the upper-right corner, click **Export**.

   A drop-down menu appears.



3. From the drop-down menu, select one of the following options:

   - Click **PDF** to export the dashboard in PDF format.
   - Click **PNG** to export the dashboard in PNG format.
   - Click **JPG** to export the dashboard in JPG format.

An **In Progress** message appears.

Once the export completes, a **Success** message appears and Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

Export a Widget from the Tenable Lumin Dashboard

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required Additional License: Tenable Lumin

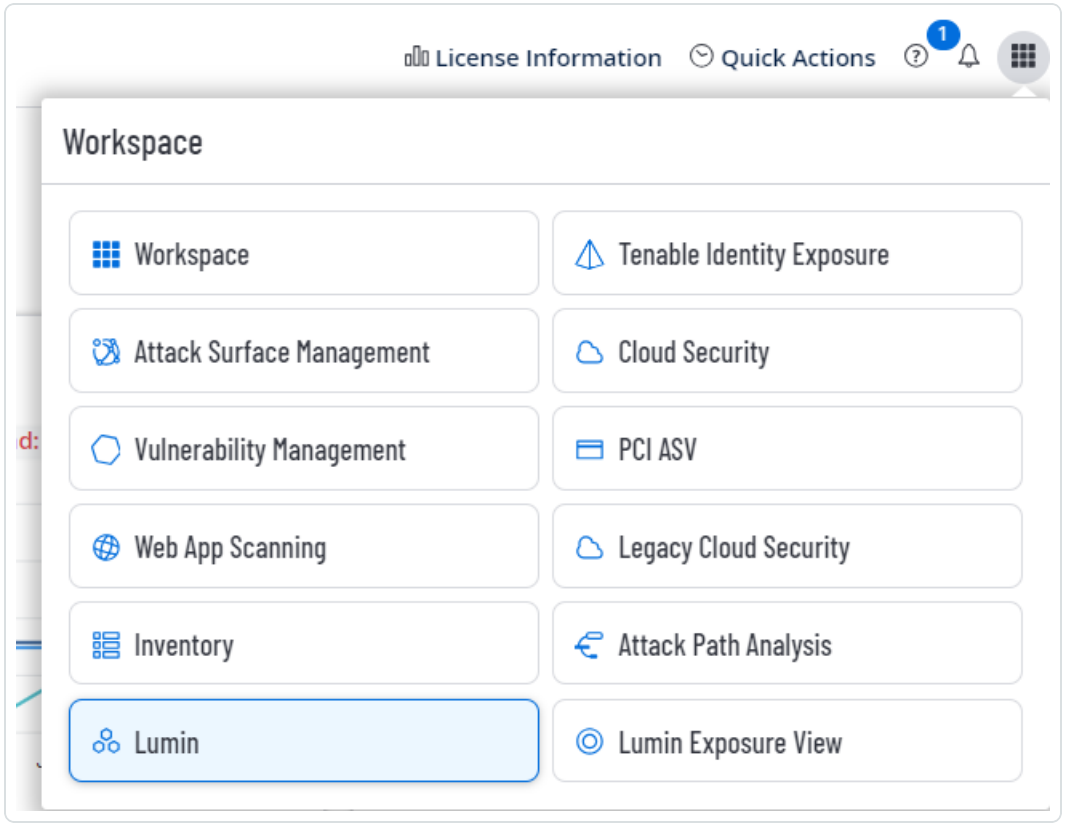
Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

In Tenable Vulnerability Management, you can export individual widgets from the Tenable Lumin dashboard.

Note: You cannot export the **Cyber Exposure Score by Business Context** widget.

To export a widget from the Tenable Lumin dashboard:

1. In the Workspace menu, click **Lumin**.



   The **Lumin** dashboard appears.

2. In the header of the widget you want to export, click the ⋮ button.

   A drop-down menu appears.

3. From the drop-down menu, select one of the following options:

   - Click **PDF** to export the dashboard in PDF format.
   - Click **PNG** to export the dashboard in PNG format.
   - Click **JPG** to export the dashboard in JPG format.

An **In Progress** message appears.

Once the export completes, a **Success** message appears and Tenable Vulnerability Management downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

Update the Tenable Lumin Industry Benchmark

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

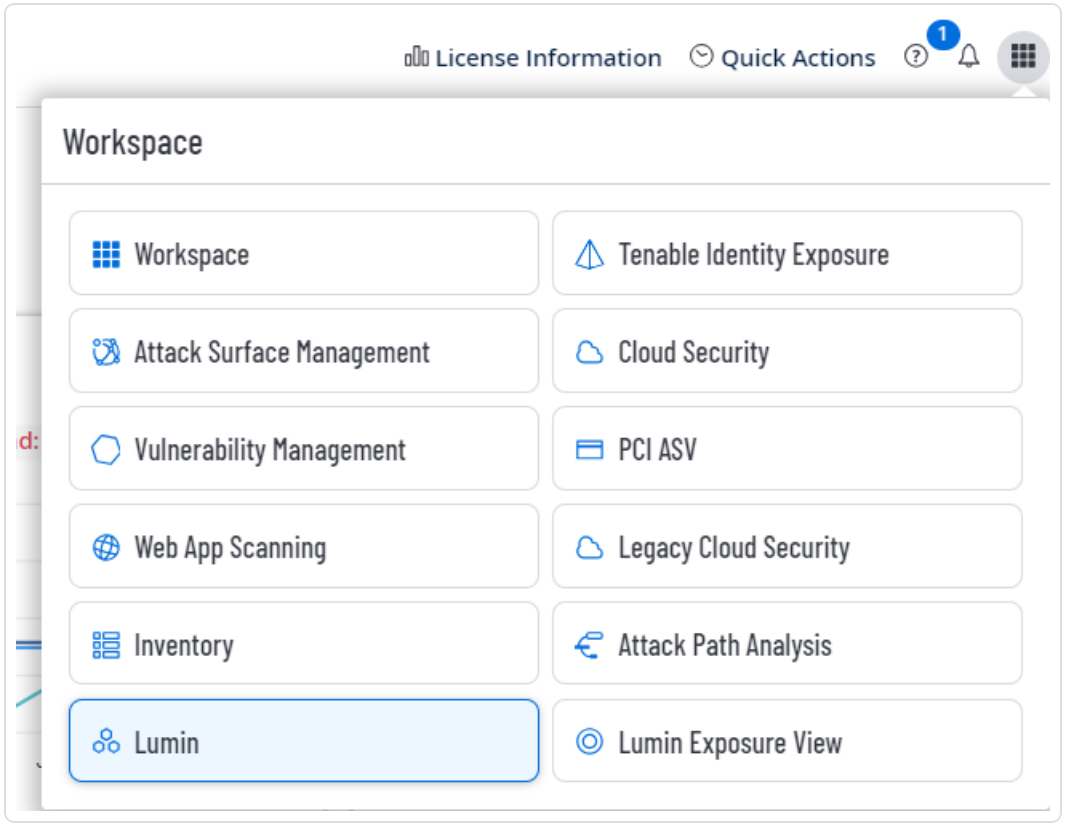
Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Larger organizations may have business units that span multiple industries, or that don't fit neatly into one industry categorization. By selecting the most applicable industry benchmark in Tenable Lumin, users can maximize the relevancy of their data and more accurately track how their Tenable Lumin metrics compare with others across similar industries.

To update the Tenable Lumin industry benchmark:

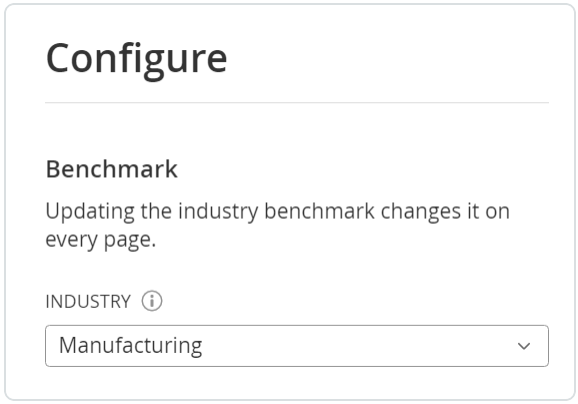
1. In the Workspace menu, click **Lumin**.



   The **Lumin** dashboard appears.

2. In the upper-right corner, click **Configure**.

   The **Configure** plane appears.



3. In the **Benchmark** section, from the **Industry** drop-down, select the industry benchmark you want to use across the Tenable Lumin dashboard.
4. Click **Save**.

An **Industry Updated** confirmation message appears, and Tenable Vulnerability Management applies the new industry across the Tenable Lumin dashboard.

(Optional) To reset the Tenable Lumin industry benchmark:

1. On the **Configure Industry** plane, click **Reset to Default**.

   A confirmation message appears.

2. Click **Confirm**.

   An **Industry Updated** confirmation message appears, and Tenable Vulnerability Management resets the industry back to the industry selected upon account creation.

Tenable Lumin Dashboard Widgets

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

The Tenable Lumin dashboard consists of the following widgets:

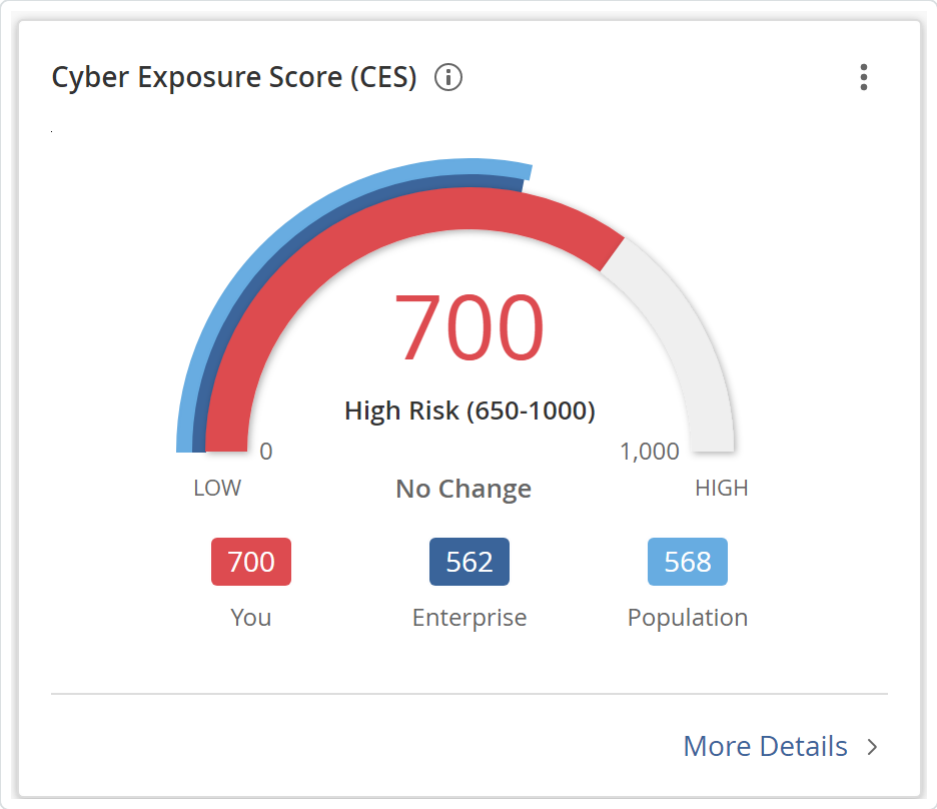
- Cyber Exposure Score
- Cyber Exposure Score Trend
- Actions to Reduce CES
- Assessment Maturity
- Remediation Maturity
- Cyber Exposure Alerts
- Mitigations
- Cyber Exposure Score by Business Context/Tag

> **Note:** All Tenable Lumin data reflects all assets within the organization's Tenable Vulnerability Management instance.

Cyber Exposure Score

How does your overall risk compare to other Tenable customers in your Salesforce industry and the larger population?

Time Frame	Assets
Past 90 days	Licensed assets for your entire organization



This widget summarizes the CES for your entire organization compared to Tenable customers in your Salesforce industry and the larger population.

In this widget, you can perform the following actions:

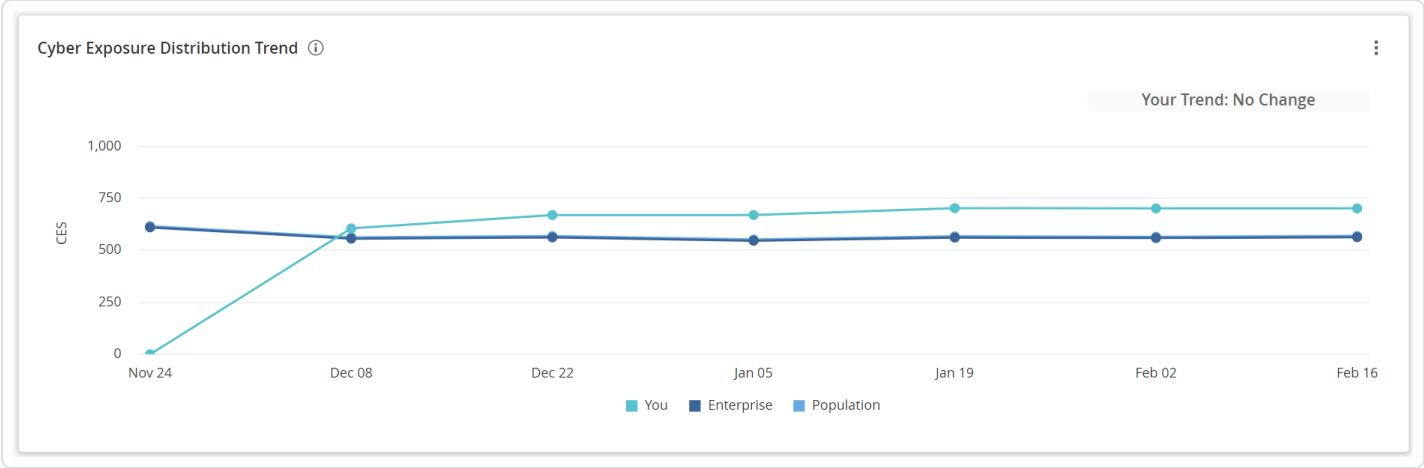
- View a visual representation of your CES compared to the average CES for Tenable customers in your Salesforce industry and the larger population.
- View a summary statement about whether your CES recently increased or decreased.
- To view details about your CES, click your CES value.

  The Tenable Lumin **Cyber Exposure Score** details panel appears. For more information, see CES Details.
- Export the dashboard widget.

Cyber Exposure Score Trend

How has the overall risk for your entire organization changed over time?

Time Frame	Assets
Past 90 days at each point on the graph, recalculated daily	Licensed assets for your entire organization



This widget graphs the increases and decreases to your CES and to the average CES for Tenable customers in your Salesforce industry and the larger population.

In this widget, you can perform the following actions:

- To view details about an industry or population CES value on a specific date, hover over a point on the graph.

  The hover text provides historical data about the CES.

- To view details about your CES value on a specific date, click a point on the **You** line.

  The Tenable Lumin **Cyber Exposure Score** details plane appears. For more information, see CES Details.

- To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend.

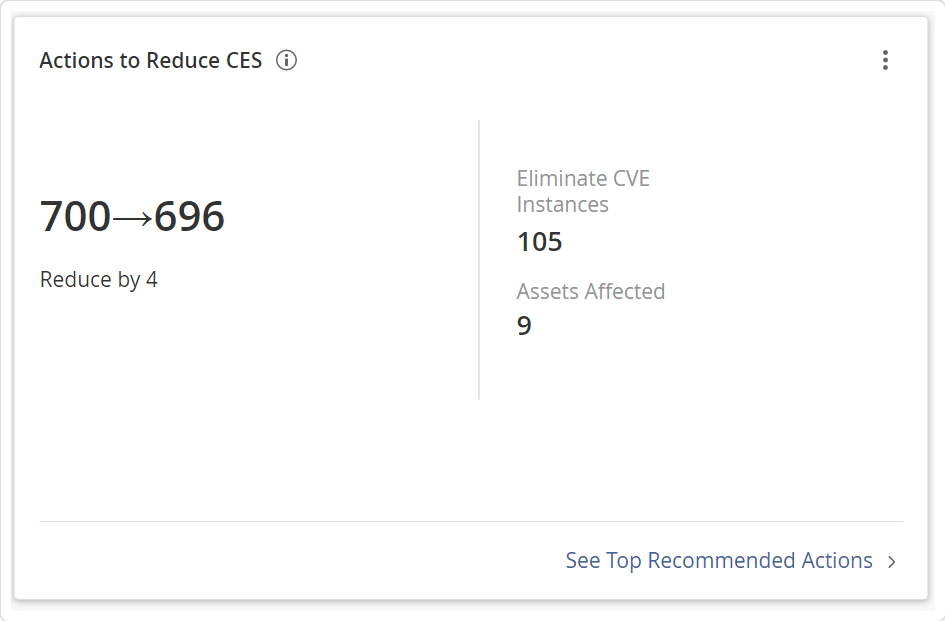
  The system updates the widget to show or hide the data you selected.

- Export the dashboard widget.

Actions to Reduce CES

What would the impact be if you addressed all of your top 20 recommended actions?

Time Frame	Assets
Past 90 days	Licensed assets for your entire organization



This widget summarizes the impact of your top 20 recommended actions.

In this widget, you can perform the following actions:

- View the expected CES reduction if you address all top 20 recommended actions.
- View the number of vulnerability instances you would eliminate if you addressed all top 20 recommended actions.

  Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

- View the number of assets affected by your top 20 recommended actions.
- To view details about your top 20 recommended actions, click **See Top Recommended Actions**.

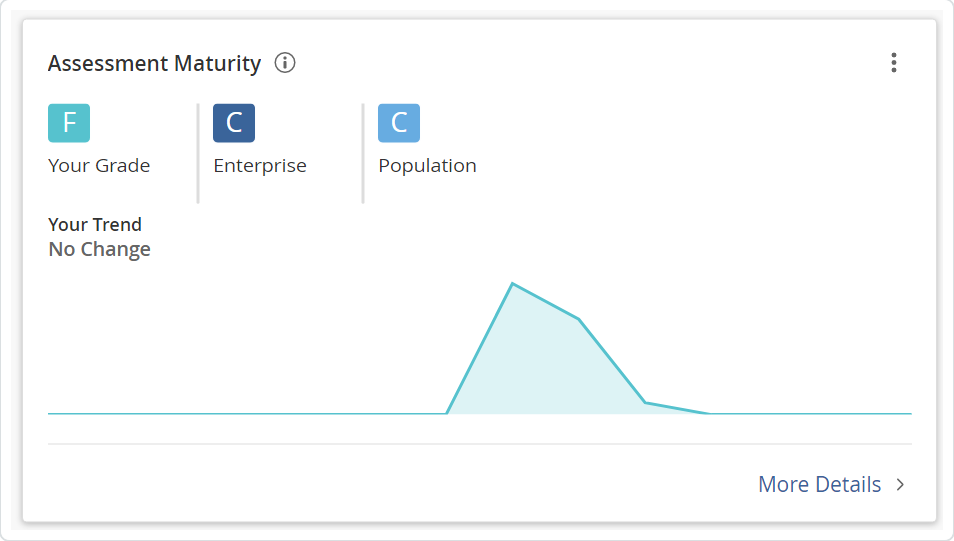
  The Tenable Lumin **Recommended Actions** page appears. For more information, see View Recommended Actions.

- Export the dashboard widget.

Assessment Maturity

How frequently and thoroughly are you scanning your assets?

Time Frame	Assets
Past 90 days	Licensed assets for your entire organization



This widget summarizes the Assessment Maturity grade for your entire organization compared to Tenable customers in your Salesforce industry and the larger population.

Important: Your Assessment Maturity and Remediation Maturity scores may have recently changed due to data migration and algorithm changes within Tenable Lumin. This is expected behavior. For more information, contact your Tenable representative.

In this widget, you can perform the following actions:

- View your Assessment Maturity grade compared to the average Assessment Maturity grade for Tenable customers in your Salesforce industry and the larger population.
- View a summary statement about whether your Assessment Maturity grade recently increased or decreased.
- To view historical details about your Assessment Maturity grade, hover over a point on the graph.

  The hover text provides historical data about the Assessment Maturity grade.

- To view more details about your Assessment Maturity grade, click **More Details**.

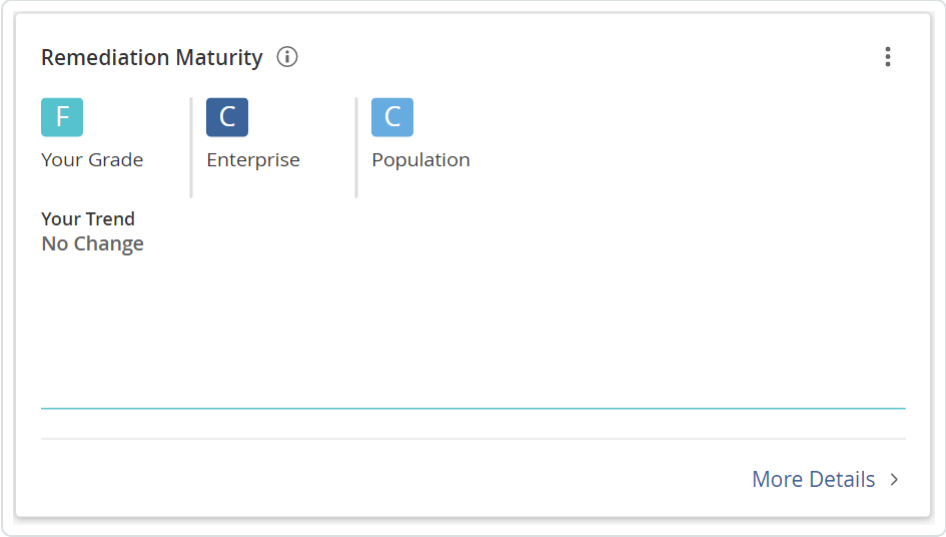
  The Tenable Lumin **Assessment Maturity** page appears. For more information, see View Assessment Maturity Details.

- Export the dashboard widget.

Remediation Maturity

How quickly and thoroughly are you remediating vulnerabilities on your assets?

Time Frame	Assets
Past 90 days	Licensed assets for your entire organization



Important: Your Assessment Maturity and Remediation Maturity scores may have recently changed due to data migration and algorithm changes within Tenable Lumin. This is expected behavior. For more information, contact your Tenable representative.

This widget summarizes the Remediation Maturity grade for your entire organization compared to Tenable customers in your Salesforce industry and the larger population.

In this widget, you can perform the following actions:

- View your Remediation Maturity grade compared to the average Remediation Maturity grade for Tenable customers in your Salesforce industry and the larger population.

- View a summary statement about whether your Remediation Maturity grade recently increased or decreased.
- To view historical details about your Remediation Maturity grade, hover over a point on the graph.

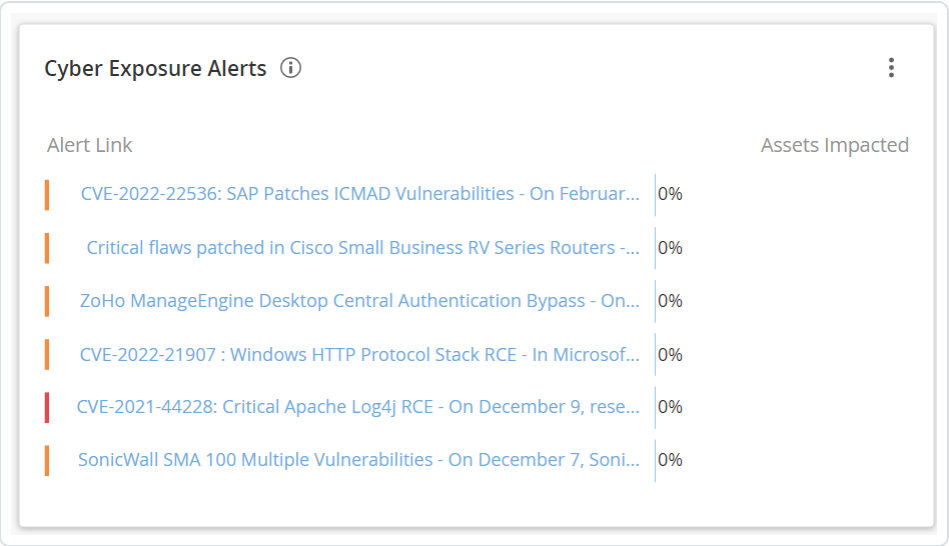
  The hover text provides historical data about the Remediation Maturity grade.
- To view more details about your Remediation Maturity grade, click **More Details**.

  The Tenable Lumin **Remediation Maturity** page appears. For more information, see View Remediation Maturity Details.
- Export the dashboard widget.

Cyber Exposure Alerts

What Tenable Research cyber security alerts should you be aware of?

Time Frame	Assets
6 most recent alerts	Licensed assets for your entire organization



This widget shows the 6 most recent cyber security alerts provided by the Tenable research team. Tenable Lumin provides further details about how many assets are potentially impacted and a link to the Tenable blog post for the alert, where you can view further information and any required responses.

Note: To maintain an accurate CVE count, Tenable Lumin does not include entries from patch Tuesdays, Oracle CPU, etc. as alerts within the **Cyber Exposure Alerts** widget.

To reduce noise within the **Cyber Exposure Alerts** widget, Tenable Lumin does not target specific CVEs (i.e., from Patch Tuesday/Oracle CPU)

In this widget, you can perform the following actions:

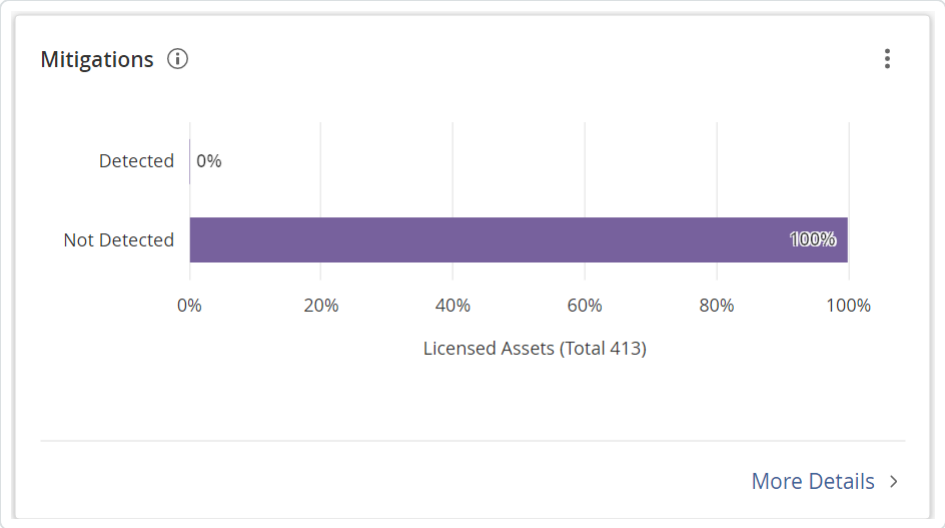
- View cyber exposure alerts with one of the following severities:
    - **Information** (Low) – The alert contains information that may be of interest, but does not require an immediate response.
    - **Advisory** (Medium) – The alert contains warning information and may require a response.
    - **Response** (Critical) – The alert requires an immediate response.
- To view the severity of the alert, a brief description, and the date on which the alert was published, roll over one of the alerts in the widget.
- To view the percentage of your assets affected by the alert (assets where one of the CVEs associated with the alert is present as a vulnerability on the asset), roll over one of the rows in the **Assets Affected** column.

  If an alert has a CVE but no assets are affected, or you have not yet scanned your assets for the vulnerability, then the **Assets Affected** column shows a value of 0%. If no CVE is currently assigned to the alert, then the **Assets Affected** column shows a value of **Pending**. Once Tenable Vulnerability Management calculates the CVE for the alert, Tenable Lumin updates the column with the appropriate value.
- To view your vulnerabilities by asset automatically filtered by the CVE associated with the alert, click one of the percentages in the widget.
- To view the Tenable blog post about the exposure alert, click one of the alerts in the widget.
- To view the **Trending Threats** page for an alert, click one of the alerts in the widget.
- Export the dashboard widget.

Mitigations

How are endpoint protection agents distributed on your assets?

Time Frame	Assets
Past 90 days	Licensed assets for your entire organization



This widget summarizes the distribution of endpoint protection agents on your assets.

If you run an authenticated scan based on the **Basic Network Scan** template or **Advanced Network Scan** template or an agent scan based on the **Basic Agent Scan** or **Advanced Agent Scan** template, Tenable automatically enables the plugins required to detect mitigations present on your assets. Tenable Lumin defines mitigations as endpoint protection agents, which include antivirus software, Endpoint Protection Platforms (EPPs), or Endpoint Detection and Response (EDR) solutions.

In this widget, you can perform the following actions:

- To view a list of assets in a Mitigations category, click one of the percentages in the widget.

  The **Assets** page appears, filtered by licensed assets, the mitigations category you selected, and the past 90 days. For more information, see Assets.

  > **Note**: When accessing the **Assets** page from the **Mitigations** widget, you may see an asset count notification at the top of the page. This notification indicates the number of assets you have permission to view based on the access group to which you belong.

- To view details about the endpoint protection agents detected on your assets, click **More Details**.

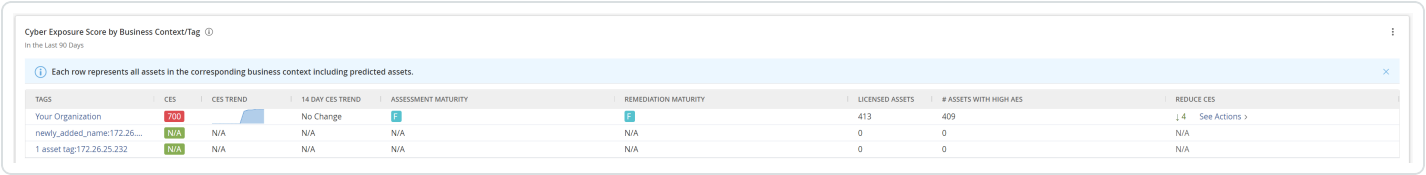
The Tenable Lumin **Mitigations** page appears. For more information, see View Mitigations Details in Tenable Lumin.

- Export the dashboard widget.

Cyber Exposure Score by Business Context/Tag

How do assets with different tags (unique business context) compare?

Time Frame	Assets
Past 90 days	All licensed assets to which the selected tags apply



This widget summarizes data about the CES calculated for your entire organization and for assets with specific business context tags.

In this widget, you can perform the following actions:

- View data for the assets with each tag.
    - **CES** – The average CES for assets with the tag. A value of **N/A** indicates Tenable is calculating your CES.
    - **CES Trend** – A visual representation of your CES change over the past 180 days. A value of **N/A** indicates Tenable is processing your CES data or that there are 0 assets with this tag.
    - **14 Day Trend** – A summary of how the CES increased (↑) or decreased (↓) in the past 14 days. A value of **N/A** indicates Tenable is processing your CES data or that there are 0 assets with this tag.
    - **Assessment Maturity** – The Assessment Maturity grade for assets with the tag. A value of **N/A** indicates there are 0 licensed assets with the tag.

      To view details about your Assessment Maturity grade for assets with a specific tag, in the **Assessment Maturity** column, click the grade.

The Tenable Lumin **Assessment Maturity** page appears, filtered by the tag you selected.

- **Remediation Maturity** – The Remediation Maturity grade for assets with the tag.

  To view details about your Remediation Maturity grade for assets with a specific tag, in the **Remediation Maturity** column, click the grade.

  The Tenable Lumin **Remediation Maturity** page appears, filtered by the tag you selected. For more information, see View Remediation Maturity Details.

- **Licensed Assets** – The number of licensed assets with the tag.
- **# Assets with High AES** – The number of assets with the tag and a high AES.
- **Reduce Tag CES** – Your expected tag-level CES reduction if you resolve all the solutions for assets with this specific tag. A value of **N/A** indicates your expected reduction is 5 or fewer. Typically, you cannot significantly reduce your CES if many assets were scanned without authentication or if your assets are healthy and your risk is already low.

  To view the recommended actions for assets with a specific tag, in the **Reduce Tag CES** column, click **See Actions**.

  The Tenable Lumin **Recommended Actions** page appears, filtered by licensed assets and the tag you selected.

- To view details about the assets with a specific tag, click a row of the table.

  The Tenable Lumin **Business Context/Tag Asset Details** page appears. For more information, see View Business Context/Tag Asset Details.

- To modify the tags that appear in the widget:

  1. Click the ⋮ button.
  2. Click the ⚙ **Configure** button.

     The widget editor plane appears.

  3. Do one of the following:

- To reorder the tags in the widget:
    a. Click and hold the ⠿ button next to the tag you want to move.
    b. Drag the tag to the new location.
    c. Release the mouse button to drop the tag in the new location.
- To delete a tag from the widget, click the 🗑 button.
- To add a tag to the widget, click the ⊕ **Add Tag** button and specify the tag you want to add.

  This widget can show data for up to 25 tags.

4. Click **Save**.

   Tenable Vulnerability Management refreshes the widget.

- To sort the table, see Tables.

View the CES Details Panel

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

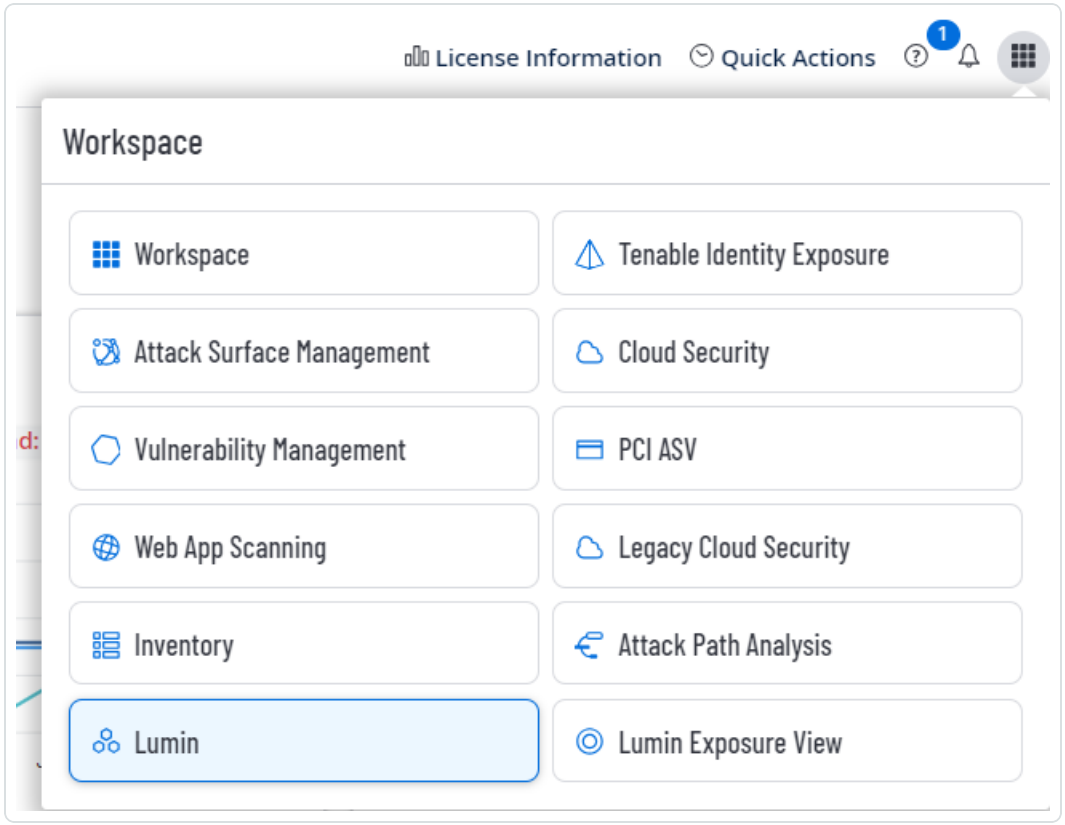
Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Use this page to browse CES details for your organization, or for assets with a specific business context tag.

To view CES details:

1. In the Workspace menu, click **Lumin**.



   The **Lumin** dashboard appears.

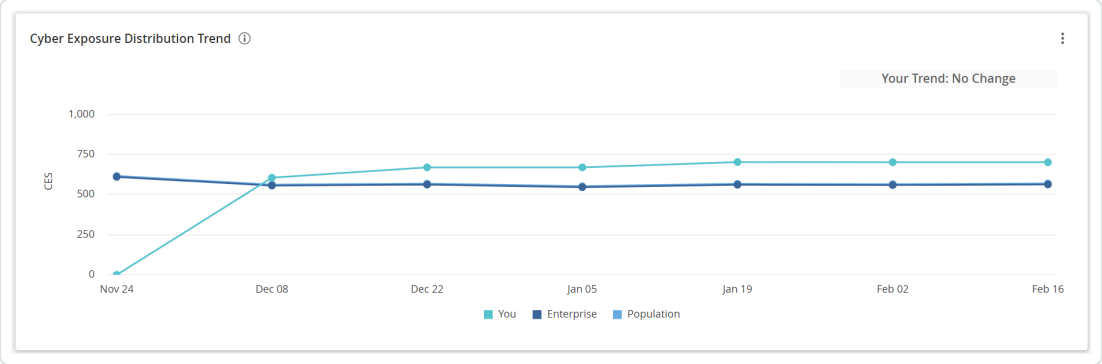
2. Do one of the following:

   - To view CES details for your entire organization:

     a. Do one of the following:

        - To view current CES details, in the **Cyber Exposure Score** widget, click the CES value.

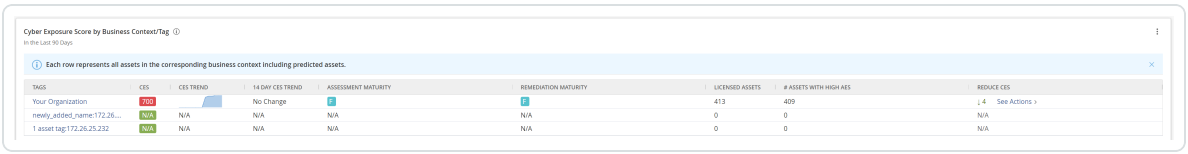
- To view historical CES details, in the **Cyber Exposure Score Trend** widget, click a past point on the graph.



- To view CES details for assets with a specific business context tag:

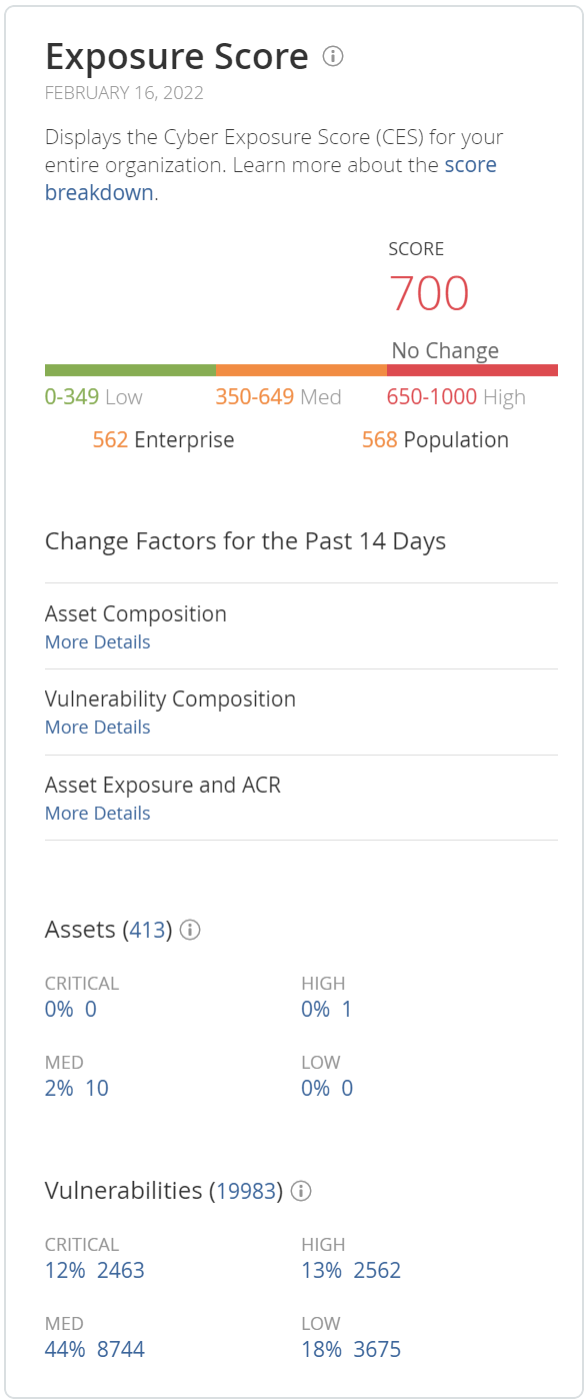
  a. In the **Cyber Exposure Score by Business Context/Tag** widget, click the tag for which you want to view asset details.

  The Tenable Lumin **Business Context/Tag Asset Details** page appears, filtered by the tag you selected.



b. In the **Cyber Exposure Score Trend** widget, click a CES value.

The Tenable Lumin **Cyber Exposure Score** details plane appears.



Note: All Tenable Lumin data reflects all assets within the organization's Tenable Vulnerability Management instance.

Section	Timeframe	Assets	Action
Score	Past 90 days	Licensed assets	• View the CES for your entire organization and the average CES for other Tenable customers in your Salesforce industry and the larger population. • View the amount by which the score for your entire organization increased (↑) or decreased (↓) in the past 14 days.
Change Factors for the Past 14 Days	Past 14 days	Licensed assets	• View the major events that contributed to your score change. Tenable Vulnerability Management groups the factors by the change type: ◦ **CES Algorithm** – Any changes related to the CES Algorithm Update. For more information, see the Lumin FAQ.

			Note: This section only appears if the algorithm update affected your CES score. ◦ **Asset Composition Change** – Asset license changes, assets depth changes, etc. ◦ **Vulnerability Composition Change** – Remediation of vulnerabilities, the discovery of new vulnerabilities, etc. ◦ **Asset Exposure and ACR Change** – Any changes to your AES or ACR • To view specific details about what changed, under any change factor group, click **More Details**. Tenable Lumin shows the amount by which specific drivers increased (↑) or

			decreased (↓) in the past 14 days.
Assets (#) (Visible only when viewing current CES details)	All time	Licensed and unlicensed assets	• View the total number of assets. • For each ACR category, view the following information: ◦ The percentage of assets with critical, high, medium, and low ACR values. **Tip:** The percentages do not total to 100% if any of your assets are unscored. ◦ The total number of assets with critical, high, medium, and low ACR values. ◦ If the number of assets with critical, high, medium, and low ACR values has increased or decreased in the past 14 days, the amount by which the percentage of

			assets and the total number of assets increased (↑) or decreased (↓) during that time. • To view a list of assets in an ACR category, click a percentage. The **Assets** page appears, filtered by licensed assets and the ACR category you selected. For more information, see Assets.
Vulnerabilities (#) (Visible only when viewing current CES details)	All time	Licensed and unlicensed assets	• View the total number of vulnerabilities present on the assets. • For each VPR category, view the following information: ◦ The percentage of vulnerabilities with critical, high, medium, and low VPR values. **Tip:** The percentages do not total to 100% if any of your assets are

			unscored. ◦ The total number of vulnerabilities with critical, high, medium, and low VPR values. ◦ If the number of vulnerabilities with critical, high, medium, and low VPR values increased or decreased in the past 14 days, the amount by which the percentage of vulnerabilities and the total number of vulnerabilities has increased (↑) or decreased (↓) during that time. • To view a list of vulnerabilities in a VPR category, click a percentage. The **Vulnerabilities** page appears, filtered by licensed assets and the VPR category you selected. For more

			information, see Findings.

View Assessment Maturity Details

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable calculates a dynamic Assessment Maturity grade that represents your overall scanning depth and frequency. For more information, see Assessment Maturity.

Important: Your Assessment Maturity and Remediation Maturity scores may have recently changed due to data migration and algorithm changes within Tenable Lumin. This is expected behavior. For more information, contact your Tenable representative.

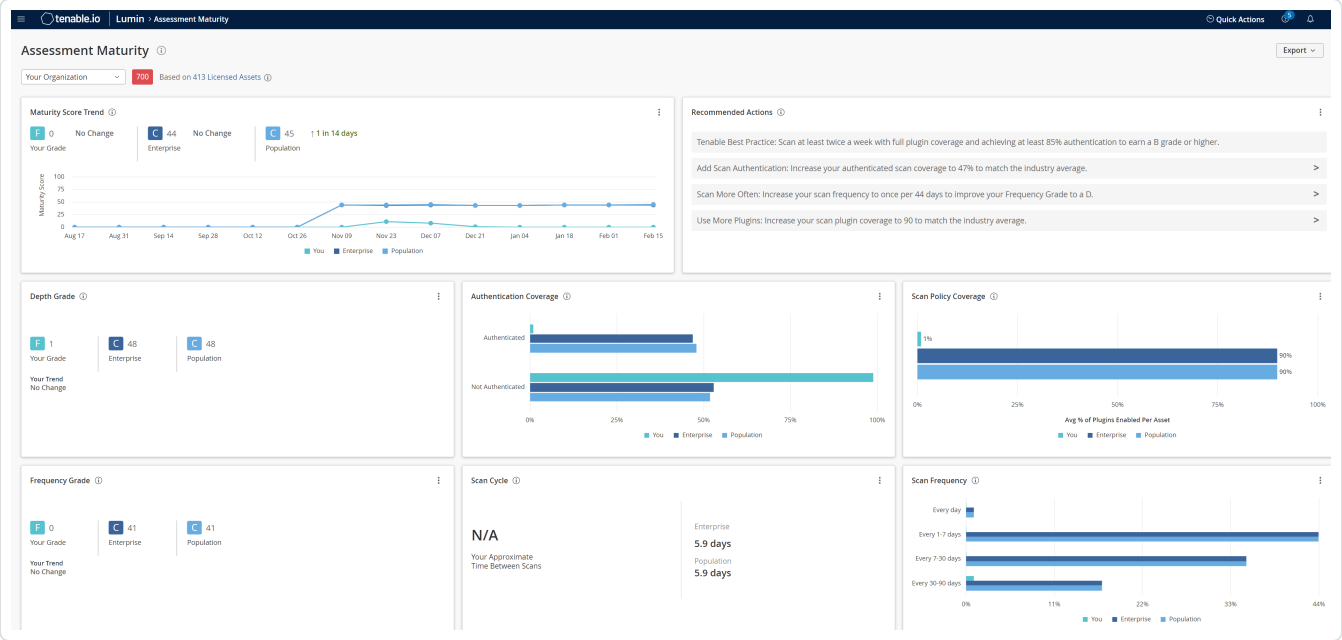
To view Assessment Maturity details for all assets:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Assessment Maturity**.

   The **Assessment Maturity** page appears and, by default, shows details for your entire organization.



3. (Optional) To change the tag filter applied to the page, in the upper left corner, select a tag from the drop-down list.

   Tenable Lumin filters the page by the tag you selected.

Note: All Tenable Lumin data reflects all assets within the organization's Tenable Vulnerability Management instance.

Section or Widget	Timeframe	Assets	Action
Summary	Past 90 days	Licensed assets	This section summarizes your Assessment Maturity grade, compared to Tenable customers in your Salesforce industry and the larger population. • View a visual representation of your Assessment Maturity compared to the average Assessment Maturity for Tenable customers in your Salesforce industry and the larger population.

			• To view a list of your licensed assets impacting your Assessment Maturity, click ***<count>* Licensed Assets**. The **Assets** page appears, filtered by licensed assets and the past 90 days. For more information, see Assets. • To view a list of your unlicensed assets that do not impact your Assessment Maturity, click ***<count>* Not Licensed**. The **Assets** page appears, filtered by unlicensed assets and the past 90 days. For more information, see Assets.
Maturity Score Trend How is your Assessment Maturity grade changing over time?	Past 90 days at each point on the graph, recalculated daily	Licensed assets	This widget graphs the increases and decreases to your Assessment Maturity grade and to the average Assessment Maturity grade for Tenable customers in your Salesforce industry and the larger population. • To view details about an Assessment Maturity grade on a specific date, hover over a point on the graph. The hover text provides historical data about the Assessment Maturity grade.

			• To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend. The system updates the widget to show or hide the data you selected.
Recommended Actions What general actions can you take to improve your scanning health?	Past 90 days	Licensed assets	This widget provides Tenable-recommended best practices to improve your scanning health. • Review your recommended best practices. • To take action, click the link next to the description.
Depth Grade Are you scanning your assets thoroughly enough?	Past 90 days	Licensed assets	This widget summarizes the Assessment Maturity depth grade for your entire organization, compared to Tenable customers in your Salesforce industry and the larger population. • View a visual representation of your depth grade compared to the average depth grade for Tenable customers in your Salesforce industry and the larger population. • View a summary statement about whether your depth grade recently increased or decreased.

Authentication Coverage How often are you performing authenticated scans?	Past 90 days	Licensed assets	This widget graphs your percentage of assets scanned with authentication and without authentication, compared to Tenable customers in your Salesforce industry and the larger population. You can optimize your authentication coverage by ensuring you scan with successful authentication so that all plugins run on your assets. • View a visual representation of your authentication coverage compared to the average depth grade for Tenable customers in your Salesforce industry and the larger population. • To view details, hover over a scan type cluster on the graph. The hover text provides data about the scan type. • To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend. The system updates the widget to show or hide the data you selected.
Frequency Grade	Past 90 days	Licensed	This widget summarizes the

Are you scanning your assets frequently enough?		assets	Assessment Maturity frequency grade for your entire organization, compared to Tenable customers in your Salesforce industry and the larger population. **Tip:** Tenable calculates your frequency grade based on how often you scan assets on your network. • View a visual representation of your frequency grade compared to the average frequency grade for Tenable customers in your Salesforce industry and the larger population. • View a summary statement about whether your frequency grade recently increased or decreased.
Scan Cycle How much time passes between your scans?	Past 90 days	Licensed assets	This widget summarizes your average scan frequency, in days, compared to Tenable customers in your Salesforce industry and the larger population. Your scan cycle is the average number of days between scans for your assets.
Asset Scan Frequency How often are you scanning your	Past 90 days	Licensed assets	This widget graphs the percentage of your assets that Tenable Vulnerability Management scans daily, weekly, monthly, and quarterly, compared to Tenable

assets?			customers in your Salesforce industry and the larger population. • To view details about a scan frequency for a specific date range, hover over a point on the graph. The hover text provides data about the scan frequency. • To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend. The system updates the widget to show or hide the data you selected.

View Remediation Maturity Details

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

Tenable calculates a dynamic Remediation Maturity grade that represents your overall vulnerability remediation responsiveness and coverage. For more information, see Remediation Maturity.

Important: Your Assessment Maturity and Remediation Maturity scores may have recently changed due to data migration and algorithm changes within Tenable Lumin. This is expected behavior. For more information, contact your Tenable representative.

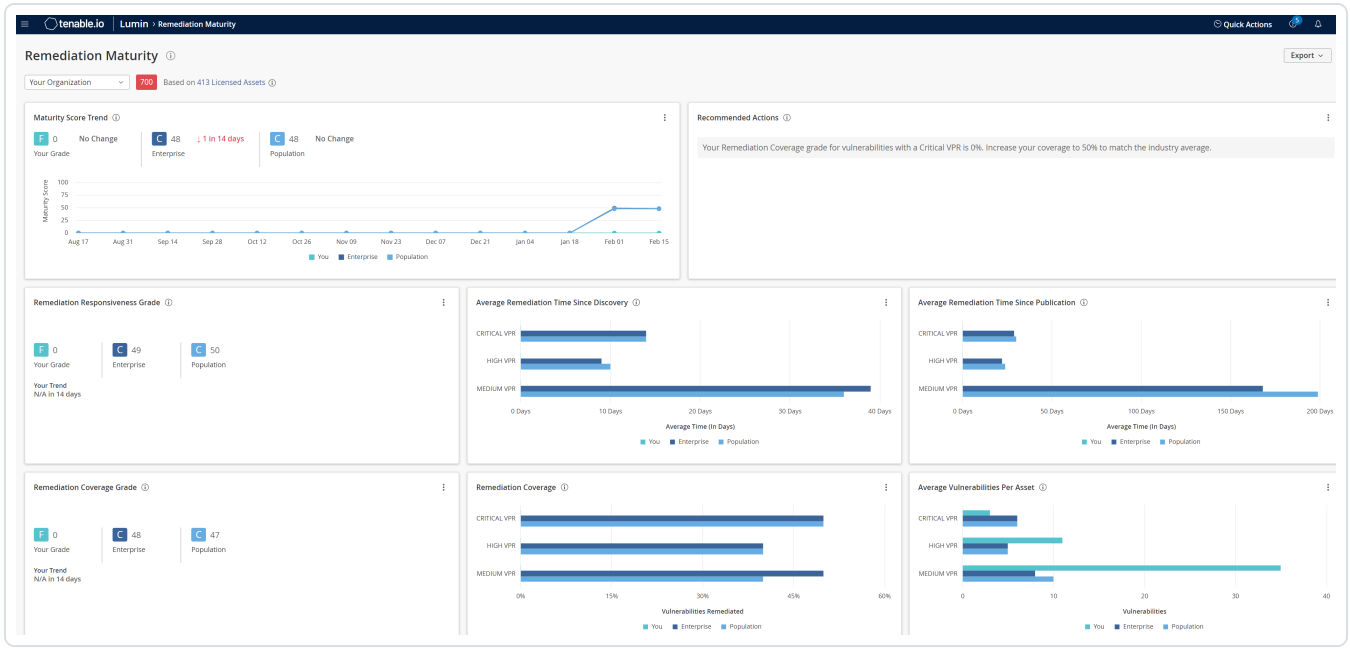
To view Remediation Maturity details for all assets:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Remediation Maturity**.

   The **Remediation Maturity** page appears.



3. (Optional) To change the tag filter applied to the page, in the upper left corner, select a tag from the drop-down list.

   Tenable Lumin filters the page by the tag you selected.

Note: All Tenable Lumin data reflects all assets within the organization's Tenable Vulnerability Management instance.

Section or Widget	Timeframe	Assets	Action
Summary	Past 90 days	Licensed assets	This section summarizes your Remediation Maturity grade, compared to Tenable customers in your Salesforce industry and the larger population. • View a visual

			representation of your Remediation Maturity compared to the average Remediation Maturity for Tenable customers in your Salesforce industry and the larger population. • To view a list of your licensed assets impacting your Remediation Maturity grade, click ***<count>*** **Licensed Assets**. The **Assets** page appears, filtered by licensed assets and the past 90 days. For more information, see Assets. • To view a list of your unlicensed assets that do not impact your Remediation Maturity grade, click ***<count>*** **Not Licensed**. The **Assets** page appears, filtered by unlicensed assets and the past 90 days. For more information, see Assets.
Maturity Score Trend How is your	Past 90 days at each point on the graph, recalculated	Licensed assets	This widget graphs the increases and decreases to your Remediation Maturity grade and to the average Remediation

Remediation Maturity grade changing over time?	daily		Maturity grade for Tenable customers in your Salesforce industry and the larger population. • To view details about a Remediation Maturity grade on a specific date, hover over a point on the graph. • To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend. The system updates the widget to show or hide the data you selected.
Recommended Actions What general actions can you take to improve your remediation health?	Past 90 days	Licensed assets	This widget provides Tenable-recommended best practices to improve your remediation health. • Review your recommended best practices. • To take action, click the link in the description.
Remediation Responsiveness Grade How quickly are you remediating vulnerabilities?	Past 90 days	Licensed assets	This widget summarizes the Remediation Maturity remediation responsiveness grade for your entire organization, compared to Tenable customers in your Salesforce industry and the larger population.

			• View a visual representation of your remediation responsiveness grade compared to the average remediation responsiveness grade for Tenable customers in your Salesforce industry and the larger population. • View a summary statement about whether your remediation responsiveness grade recently increased or decreased.
Average Remediation Time Since Discovery How long does it take you to remediate a vulnerability after it is first discovered (the **First Seen** date)?	Past 90 days	Licensed assets	This widget graphs the average time, in days, you took to remediate vulnerabilities in each VPR category after the vulnerability was first discovered, compared to Tenable customers in your Salesforce industry and the larger population. • To view details about the average time for a specific VPR category, hover over a point on the graph. • To show or hide data for your organization, the industry, or the population, click the boxes in the graph

			legend. The system updates the widget to show or hide the data you selected.
Average Remediation Time Since Publication How long does it take you to remediate a vulnerability after a plugin is first made available (the **Plugin Publication** date)?	Past 90 days	Licensed assets	This widget graphs the average time, in days, you took to remediate vulnerabilities in each VPR category after a plugin was first made available, compared to Tenable customers in your Salesforce industry and the larger population. • To view details about the average time for a specific VPR category, hover over a point on the graph. • To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend. The system updates the widget to show or hide the data you selected.
Remediation Coverage Grade How thoroughly are you remediating vulnerabilities?	Past 90 days	Licensed assets	This widget summarizes the Remediation Maturity remediation coverage grade for your entire organization, compared to Tenable customers in your Salesforce industry and the larger population.

			• View a visual representation of your remediation coverage grade compared to the average remediation coverage grade for Tenable customers in your Salesforce industry and the larger population. • View a summary statement about whether your remediation coverage grade recently increased or decreased.
Remediation Coverage What percentage of your vulnerabilities are remediated?	Past 90 days	Licensed assets	This widget graphs the percentage of your vulnerabilities that are remediated (fixed) in each VPR category, compared to Tenable customers in your Salesforce industry and the larger population. • To view details about the percentage for a specific VPR category, hover over a point on the graph. • To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend. The system updates the widget to show or hide the

			data you selected.
Average Vulnerabilities Per Asset How many vulnerabilities, on average, are present on an asset?	Past 90 days	Licensed assets	This widget graphs the average number of vulnerabilities (active, fixed, or resurfaced) in each VPR category present on your assets, compared to Tenable customers in your Salesforce industry and the larger population. • To view details about the count for a specific VPR category, hover over a point on the graph. • To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend. The system updates the widget to show or hide the data you selected.

View Business Context/Tag Asset Details

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can use this page to view details about assets with a specific business context tag.

Before you begin:

- Add tags to assets, as described in Add a Tag to an Asset.

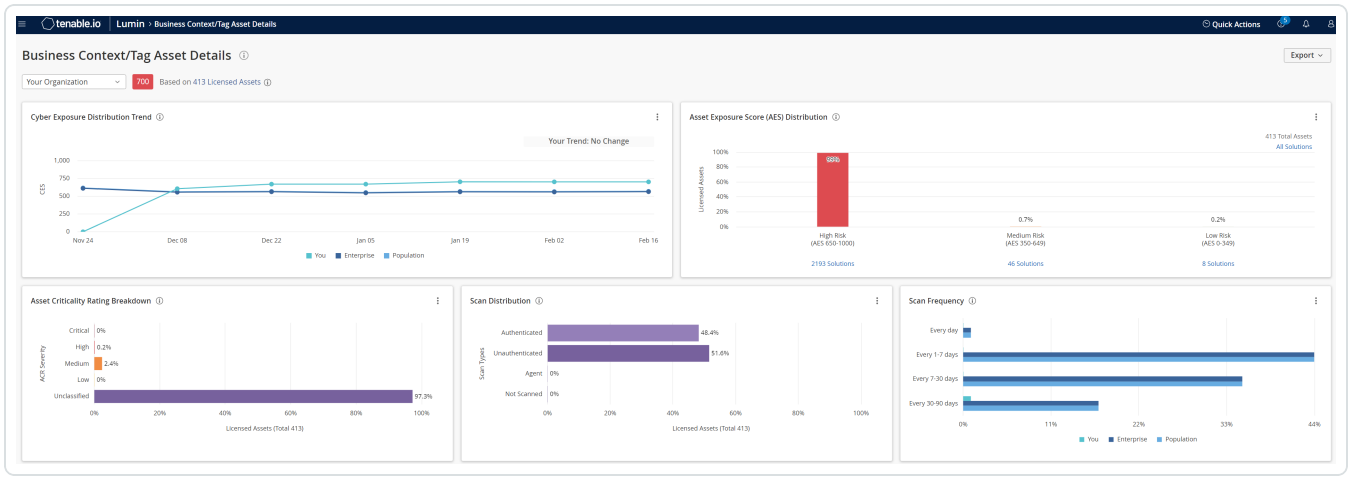
To view business context tag asset details:

1. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, click **Business Context**.

   The **Business Context/Tag Asset Details** page appears.



3. (Optional) To change the tag filter applied to the page, in the upper left corner, select a tag from the drop-down list.

   Tenable Lumin filters the page by the tag you selected.

Note: All Tenable Lumin data reflects all assets within the organization's Tenable Vulnerability Management instance.

Section or Widget	Timeframe	Assets	Action
Tag summary	All time	Licensed and unlicensed assets with the tag applied	• View the name of the tag. • View the CES calculated for assets with the tag.
Cyber Exposure Score Trend	Past 90 days at	Licensed assets	This widget graphs the

How has the overall risk for this business context changed over time?	each point on the graph, recalculated daily	with the tag applied	increases and decreases to your tag-specific CES compared to the average organization-wide CES for Tenable customers in your Salesforce industry and the larger population. **Note:** Newly added tags may take up to 14 days before displaying CES trending information. • To view details about an organization-wide industry or population CES value on a specific date, hover over a point on the graph. The hover text provides historical data about the CES. • To view details about your tag-specific CES value on a specific date, click a point on the **You** line. The Tenable Lumin **Cyber Exposure Score** details plane appears. For more information, see CES Details. • To show or hide data for your organization, the industry, or the

			population, click the boxes in the graph legend. The system updates the widget to show or hide the data you selected.
Asset Distribution by Asset Exposure Score (AES) How exposed are my assets?	Past 90 days	Licensed assets with the tag applied and shared with your user account via access groups	This widget summarizes the number of vulnerabilities in each AES category. • To view the recommended solutions for an AES category, click one of the ***<Category>* AES Solutions** links. The **Solutions** page appears, filtered by the tag, licensed assets, and the AES category you selected. For more information, see View Solutions. • To view the recommended solutions for all assets, click the **All Solutions** link. The **Solutions** page appears, filtered by the tag and licensed assets. For more information, see View Solutions.
Asset Criticality	Past 90 days	Licensed and	This widget visualizes the

Rating Breakdown How critical are my assets?		unlicensed assets with the tag applied	percentage of your assets in each ACR category. • View the total number of scanned assets on your network. • View the percentage of assets in each category: **Critical**, **High**, **Medium**, **Low**, and **Unclassified**. • To view a list of assets, click a category on the graph. The **Assets** page appears, filtered by the tag, licensed assets seen in the past 90 days, and the ACR category you selected. For more information, see Assets.
Asset Scan Distribution What percentage of your assets are scanned with different methods?	Past 90 days	Licensed and unlicensed assets with the tag applied	This widget summarizes your asset scan distribution during the past 90 days. **Authenticated Scans** are run by a non-agent scanner with credentialed scanning configured. **Agent Scans** are run by agent scanners. All other scans are **Unauthenticated Scans**. • View the total number of assets scanned on your

			network in the past 90 days. • View the percentage of assets where the system performed authenticated, unauthenticated, or agent scans in the past 90 days. • View the percentage of assets the system has not scanned in the past 90 days. • To filter the data displayed in the widget, roll over the widget and click the ▽ button. Click the desired filter. Tenable Vulnerability Management refreshes the widget. • To view the assets list, click a scan category. The **Assets** page appears, filtered by the tag, licensed assets seen in the past 90 days, the scan type you selected, and the ACR category filter applied to the widget. For more information, see Assets.
Asset Scan	Past 90 days	Licensed and	This widget visualizes the

Frequency How often are you scanning your assets?		unlicensed assets with the tag applied	percentage of assets scanned on your network during periods in the past 90 days, compared to others in your Salesforce industry and the population. • View the percentage of assets scanned on your network at **Daily**, **Weekly**, **Monthly**, or **Quarterly** intervals. • To show or hide data for your organization, the industry, or the population, click the boxes in the graph legend. The system updates the widget to show or hide the data you selected. • To filter the data displayed in the widget, roll over the widget and click the ▽ button. Click the desired filter. Tenable Vulnerability Management refreshes the widget. • To view the assets list, click a bar on the graph. The **Assets** page appears, filtered by the

			tag, licensed assets, the time period you selected, and the ACR category filter applied to the widget. For more information, see Assets.

View Mitigations Details in Tenable Lumin

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

If you run an authenticated scan based on the **Basic Network Scan** template or **Advanced Network Scan** template or an agent scan based on the **Basic Agent Scan** or **Advanced Agent Scan** template, Tenable automatically enables the plugins required to detect mitigations present on your assets. Tenable Lumin defines mitigations as endpoint protection agents, which include antivirus software, Endpoint Protection Platforms (EPPs), or Endpoint Detection and Response (EDR) solutions.

Then, you can use Tenable Lumin Mitigations data to assess whether your assets are covered properly with the endpoint protection agent software.

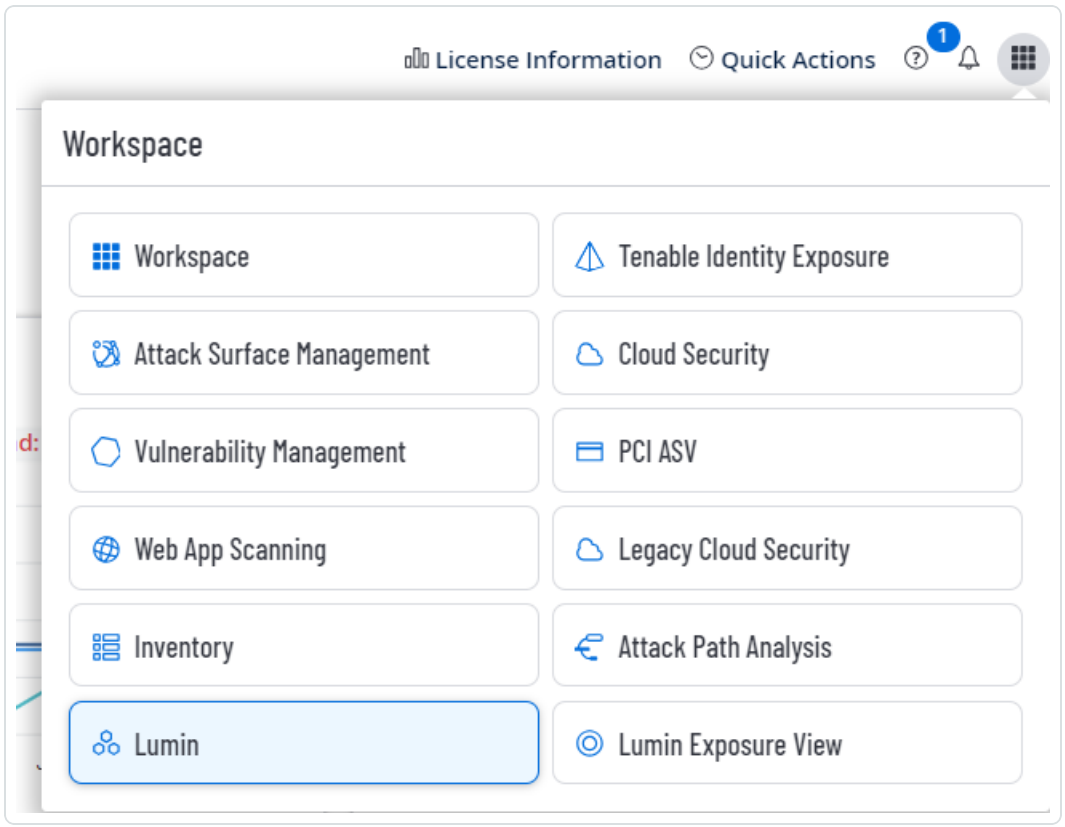
You must enable certain plugins in your authenticated and agent scans to detect endpoint protection agents on your assets. For more information, see Plugins for Mitigation Detection.

Before you begin:

- Enable the required plugins in your scans.
- Run your scans before checking the **Mitigations** page.

To view a list of endpoint protection agents on your assets:

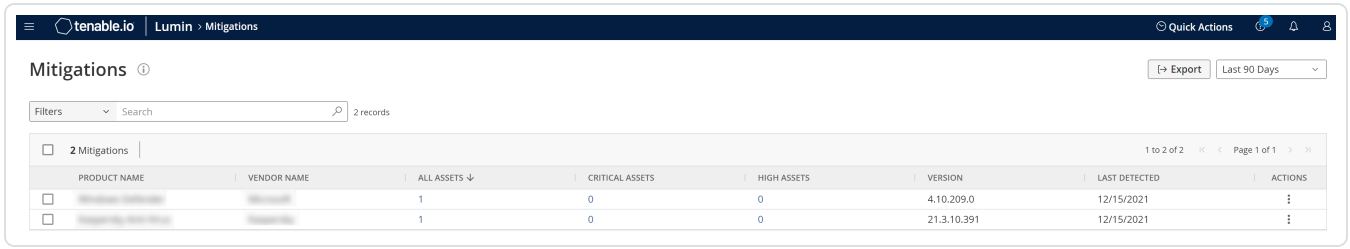
1. In the Workspace menu, click **Lumin**.



   The **Lumin** dashboard appears.

2. In the **Mitigations** widget, click **More Details**.

   The Tenable Lumin **Mitigations** page appears.



Note: All Tenable Lumin data reflects all assets within the organization's Tenable Vulnerability Management instance.

Section	Action
Exports button	Download previously generated export files.

Date range selector	Change the date range for the mitigations table. For more information, see Tables.
Filters box	Filter the data displayed in the mitigations table.
Search box	Search the mitigations table by product name. For more information, see Tables.
Mitigations table	In this table, you can: • View information about each endpoint protection agent. ◦ **Product Name** – The name of the endpoint protection agent. ◦ **Vendor Name** – The name of the vendor that maintains the endpoint protection agent. ◦ **All Assets** – The total number of assets with the endpoint protection agent present. ◦ **Critical Assets** – The total number of **Critical** ACR assets with the endpoint protection agent present. ◦ **High Assets** – The total number of **High** ACR assets with the endpoint protection agent present. ◦ **Version** – The version of the endpoint protection agent. ◦ **Last Detected** – The date that a scan last detected the endpoint protection agent on an asset. • Sort, increase or decrease the number of rows per page, or navigate to another page of the table. For more information, see Tables. • Export mitigations. • To view a list of assets with a specific endpoint protection agent present, click the asset count in the appropriate column: • **All Assets** to view all assets regardless of the asset ACR • **Critical Assets** to view **Critical** ACR assets

	• **High Assets** to view **High** ACR assets The **Assets** page appears, filtered by licensed assets, ACR severity, the mitigation product name, the mitigation vendor name, the mitigation version, and the past 90 days. For more information, see Assets.

Plugins for Mitigation Detection

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

To detect mitigations, you must enable the following plugins in your scan.

Tip: Tenable Vulnerability Management enables these plugins automatically in the following Tenable-provided scan templates: **Advanced Network Scan**, **Basic Network Scan**, **Advanced Agent Scan**, **Basic Agent Scan**.

ID	Name
12107	McAfee Antivirus Detection and Status
16192	Trend Micro Antivirus Detection and Status
20283	Panda Antivirus Detection and Status
20284	Kaspersky Anti-Virus Detection and Status
21162	Spybot Search & Destroy Detection
21608	NOD32 Antivirus Detection and Status
21725	Symantec Antivirus Software Detection and Status
21726	Webroot SpySweeper Enterprise Detection
24232	BitDefender Antivirus Detection and Status
52668	F-Secure Anti-Virus Detection and Status
54845	Sophos Anti-Virus for Mac OS X Detection
54846	Sophos Anti-Virus Detection and Status (Mac OS X)

56567	Mac OS X XProtect Detection
56568	Mac OS X XProtect Installed
58580	Trend Micro ServerProtect Detection and Status (credentialed check)
67119	McAfee ePolicy Orchestrator Installed (credentialed check)
68997	Check Point ZoneAlarm Detection and Status
74038	McAfee VirusScan Enterprise for Linux Detection and Status
84432	AVG Internet Security Detection
87777	Avast Antivirus Detection and Status
87923	McAfee Application Control / Change Control Installed
87955	McAfee Agent Detection
87989	McAfee Agent Detection (Linux/MacOS)
88598	Symantec Endpoint Protection Installed (Unix Credentialed Check)
95470	McAfee Host Intrusion Prevention Installed
100131	McAfee Security Scan Plus Detection
106757	CylancePROTECT Detection
106758	CylancePROTECT Detection (Mac OS X)
112279	Windows Defender Advanced Threat Protection Installed (Windows)
124366	McAfee Endpoint Security and Module Detection
131023	Windows Defender Installed
131725	Sophos Anti-Virus Installed (Windows)
133843	VMware Carbon Black Cloud Endpoint Standard Installed (Windows)
133962	Sophos Anti-Virus Installed (Linux)
134216	VMware Carbon Black Cloud Endpoint Standard Installed (macOS)

134871	Trend Micro Apex One Server Installed (Windows)
135408	Trend Micro Deep Security Agent Installed (Linux)
135409	Trend Micro Deep Security Agent Installed (Windows)
136760	BitDefender Endpoint Security Tools Status (Windows)
136761	BitDefender Endpoint Security Tools Detection (Windows)
138209	Symantec Critical System Protection/Data Center Security Agent (Windows)
138853	F-Secure PSB Computer Protection (Windows)
139913	Check Point Endpoint Security SandBlast Agent Installed (Windows)
139918	ClamAV Installed (Linux)
140633	CrowdStrike Falcon Sensor Installed (Windows)
152356	Cybereason Endpoint Agent Installed (Windows)

Export Mitigations

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required Additional License: Tenable Lumin

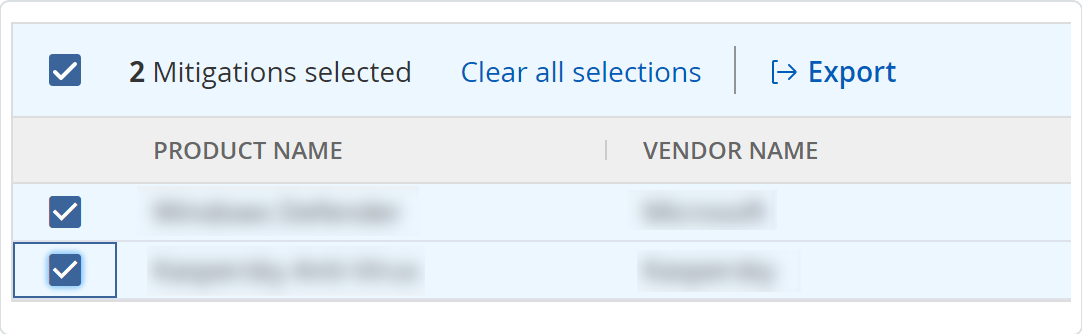
Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can export a list of mitigations and affected assets, if needed, to share the data with others in your organization.

To export mitigations and affected assets:

1. View mitigation details for your organization.
2. In the mitigations table, select the check boxes next to the mitigation or mitigations that you want to include in the export file.

   The action bar appears at the top of the table.



3. In the action bar, click **Export**.

   The Tenable Lumin mitigations **Export** plane appears.

4. In the **Type** section, click the type of export you want to perform.

   - **CSV - Mitigations** – A single `.csv` file that includes the mitigations you selected.
   - **CSV - Mitigations & Assets Affected** – Two `.csv` files that include the mitigations you selected and the assets affected where those mitigations are present.

   The export begins and Tenable Vulnerability Management downloads the export as a `tar.gz` package. For more information about the data in the export files, see Mitigations Export File Contents.

What to do next:

- To download previously exported mitigation data, see View and Download Exported Mitigations.

Mitigations Export File Contents

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

You can export mitigations from the **Mitigations** page. Your export files contain the following data.

Export Field	Description
`mitigations_summary.csv` – the **Mitigations** file	
product_name	The name of the endpoint protection agent.
vendor_name	The name of the vendor that maintains the endpoint protection agent.

all_assets	The total number of assets with the endpoint protection agent present.
critical_assets	The total number of **Critical** ACR assets with the endpoint protection agent present.
high_assets	The total number of **High** ACR assets with the endpoint protection agent present.
version	The version of the endpoint protection agent.
last_detected	The date that a scan last detected the endpoint protection agent on an asset.
`mitigations_detail.csv` – the **Affected Assets** file	
product_name	The name of the endpoint protection agent.
vendor_name	The name of the vendor that maintains the endpoint protection agent.
version	The version of the endpoint protection agent.
last_detected	The date that a scan last detected the endpoint protection agent on an asset.
asset_uuid	The asset's unique identifier.
hostname	The asset's hostname.
ipv4	The asset's IPv4 address.
operating_system	The asset's operating system.
acr_score	The asset's ACR.
acr_severity	(Requires Tenable One or Tenable Lumin license) The ACR category of the ACR calculated for the asset.
aes_score	The AES for the asset.
aes_severity	(Requires Tenable Lumin license) The AES category of the AES calculated for the asset.

View and Download Exported Mitigations

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

After you export mitigation or affected assets files, you can view and download them. You cannot view or download export files generated by other users.

Before you begin:

- Export a mitigation or affected assets file.

To view and download mitigation and affected asset exports files:

1. View mitigation details for your organization.
2. In the upper-right corner of the page, click [→ **Export**.

   The Tenable Lumin mitigations **Export** plane appears.
3. In the exports table, click the row for the export you want to download.

   Tenable Vulnerability Management downloads the export file as a `tar.gz` package. For information about the data in the export files, see Mitigations Export File Contents.

View Recommended Actions

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

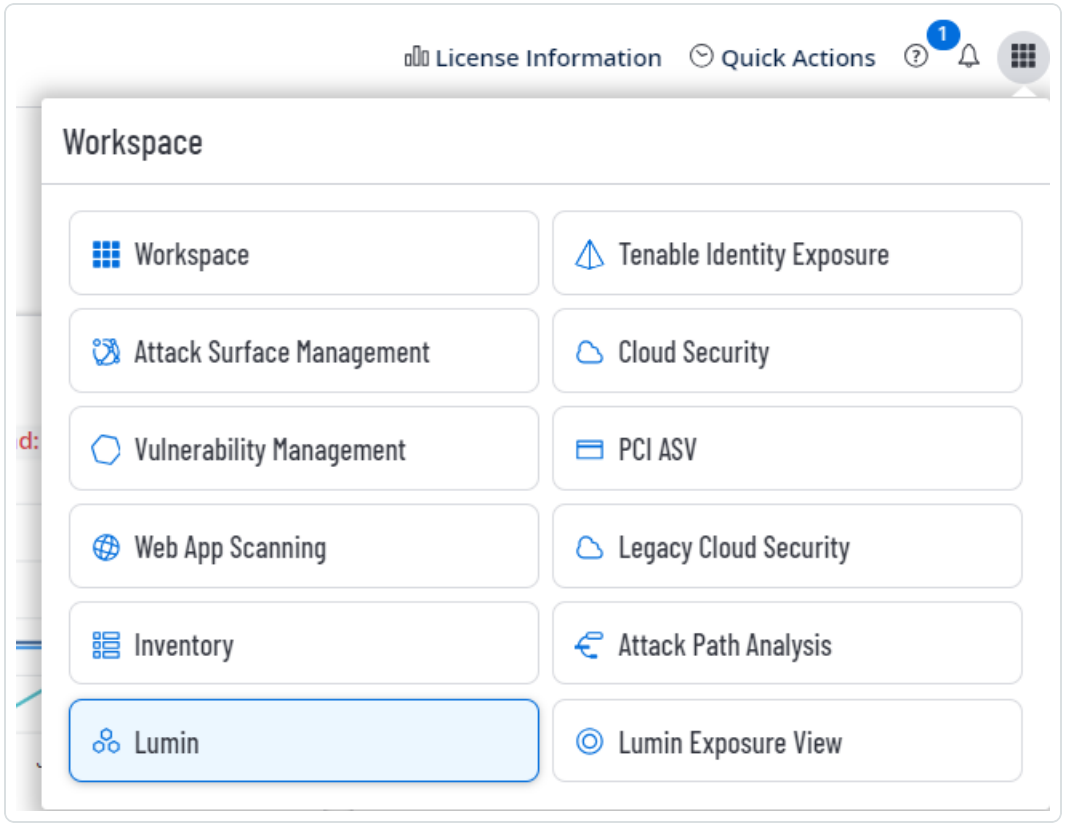
Tenable provides a list of top recommended actions (solutions) for assets on your network, regardless of your access group permissions. You can identify solutions, then drill into the solution details to understand the steps to address the vulnerability on your network.

To generate the top recommended actions, Tenable Lumin looks for the plugins that, if remediated for all licensed assets, have the biggest effect on your CES. If plugins are related, remediating one may affect other plugins.

Addressing vulnerabilities on your network lowers your CES and AES metrics.

To view the top recommended solutions for all assets on your network:

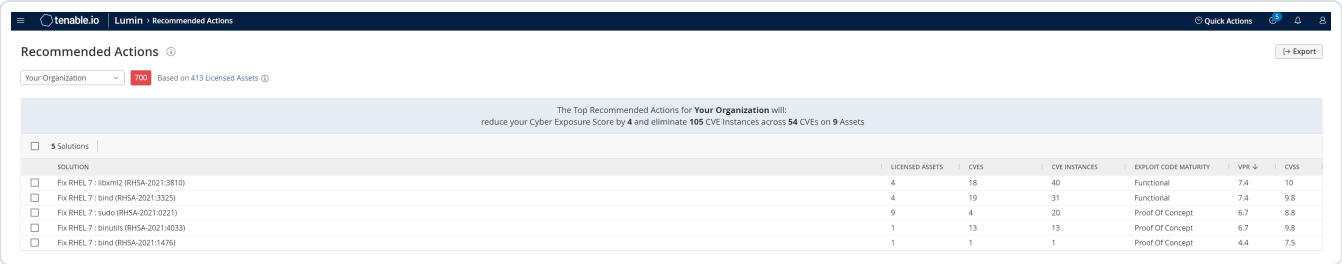
1. In the Workspace menu, click **Lumin**.



   The **Lumin** dashboard appears.

2. In the **Actions to Reduce CES** widget, click **See Top Recommended Actions**.

   The Tenable Lumin **Recommended Actions** page appears. The table sorts your top solutions (up to 20) by VPR category (**Critical** to **Low**) and then by decreasing **Assets Affected**.



3. (Optional) To change the tag filter applied to the page, in the upper left corner, select a tag from the drop-down list.

   Tenable Lumin filters the page by the tag you selected.

Section	Action
Summary bar	View summary statistics about the expected impact if you address all the solutions in the **Recommended Actions** table. • Expected CES reduction if you resolve all the top solutions. • Number of vulnerability instances eliminated by the top solutions. **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol. • Number of assets affected by the top solutions.
Recommended Actions table	• View information about each solution. • **Solution** – A description for the solution. • **Licensed Assets** – The total number of assets affected by the vulnerabilities addressed by the solution. • **CVEs** – The number of individual Common Vulnerabilities and Exposures (CVEs) addressed by the solution. • **CVE Instances** – The total number of Common Vulnerabilities and Exposures (CVEs), including duplicates, addressed by the solution. • **Exploit Code Maturity** – The key driver value for the highest VPR for the vulnerabilities addressed by the solution.

	• **VPR** – The highest VPR for the vulnerabilities addressed by the solution. • **CVSS** – The highest CVSSv2 score (or CVSSv3 score, when available) for the vulnerabilities addressed by the solution. • To view details for a solution, click a solution row. The **Solution Details** page appears. For more information, see View Solution Details. • To export solution data, see Export Recommended Actions.

Export Recommended Actions

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

Required Additional License: Tenable Lumin

Required Tenable Vulnerability Management User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

You can export a list of recommended actions (solutions) and affected assets, if needed, to share the data with others in your organization.

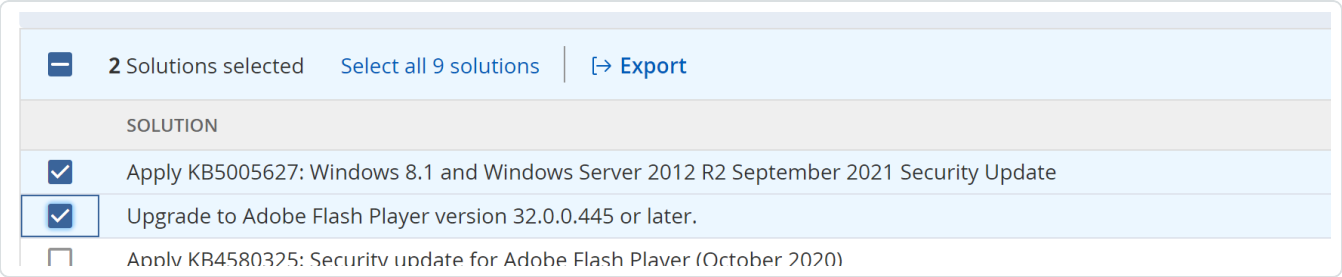
To export recommended actions and affected assets:

1. Navigate to one the Tenable Lumin **Recommended Actions** page, as described in View Recommended Actions.

   The Tenable Lumin **Recommended Actions** page appears.

2. In the table, select the check boxes next to the recommended actions that you want to include in the export file.

   The action bar appears at the top of the table.



3. In the action bar, click [→ **Export**.

   The **Exports** plane appears.

4. In the **CSV** section, select the check box for the recommended action data you want to export:

   - **Solutions** – A `.csv` file that includes the recommended actions you selected. This check box is selected by default.
   - **Details** – A `.csv` file that includes the recommended actions you selected as well as additional details about those solutions.

   The export begins and Tenable Vulnerability Management downloads the export as a `tar.gz` package. For information about the data in the export files, see Recommended Actions Export File Contents.

Recommended Actions Export File Contents

> The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the Tenable FedRAMP Product Offering.

You can export recommended actions (solutions) from two recommended action pages. The export contents from each page are unique to that page.

Recommended Actions Export for a Group of Assets

If you export recommended actions and assets affected files from the **Recommended Actions** page for a group of assets, your export files contain the following data.

Export Field	Description
`detail.csv` – the **Assets Affected** file	
solution_id	The solution's UUID.

solution_title	A description for the solution.
asset_uuid	The asset's unique identifier.
hostname	The asset's hostname.
ipv4	The asset's IPv4 address.
operating_system	The asset's operating system.
cve_count	The number of vulnerabilities on this asset addressed by the solution.
cve_instance_count	The total number of vulnerability instances on this asset 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.
`solution.csv` – the **Selected Actions** file	
solution_id	The solution's UUID.
solution_title	A description for the solution.
assets_affected	The total number of assets affected by the vulnerabilities addressed by the solution.
cve_count	The total number of vulnerabilities addressed by the solution.
vpr	The highest VPR for the vulnerabilities addressed by the solution.
cvss	The highest CVSSv2 score (or CVSSv3 score, when available) for the vulnerabilities addressed by the solution.

Recommended Actions Export for All Assets

If you export recommended actions and assets affected files from the **Recommended Actions** page for all assets, your export files contain the following data.

Export Field	Description
`detail.csv` – the **Assets Affected** file	

solution_id	The solution's UUID.
solution_title	A description for the solution.
asset_uuid	The asset's unique identifier.
hostname	The asset's hostname.
ipv4	The asset's IPv4 address.
operating_system	The asset's operating system.
acr_score	The asset's ACR.
acr_severity	(Requires Tenable One or Tenable Lumin license) The ACR category of the ACR calculated for the asset.
aes_score	The AES for the asset.
aes_severity	(Requires Tenable Lumin license) The AES category of the AES calculated for the asset.
vuln_count	The number of vulnerabilities on this asset addressed by the solution.
vuln_instance_count	The total number of vulnerability instances on this asset 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.
`summary.csv` – the **Selected Actions** file	
solution	The solution's UUID.
summary	A description for the solution.
assets_affected	The total number of assets affected by the vulnerabilities addressed by the solution.
vulnerabilities	The total number of vulnerabilities addressed by the solution.
exploit_code_maturity	The key driver value for the highest VPR for the vulnerabilities addressed by the solution.

vpr	The highest VPR for the vulnerabilities addressed by the solution.
cvss	The highest CVSSv2 score (or CVSSv3 score, when available) for the vulnerabilities addressed by the solution.