Tenable PCI ASV User Guide

Last Revised: February 29, 2024

Table of Contents

Welcome to Tenable PCI ASV

Credit card industry standards dictate that companies whose networks process payment card transactions must scan those networks for Payment Card Industry Data Security Standards (PCI DSS) compliance at regular intervals. Additionally, these companies must submit their scan results to a third-party Approved Scanning Vendor (ASV) for review.

Tenable PCI ASV allows you to take comprehensive scans of your networks so you can identify and address vulnerabilities and ensure your organization complies with PCI DSS. Tenable is also a licensed ASV reviewer, providing the external scanning and validation that PCI Security Standards require. The Tenable PCI ASV process strictly follows PCI Compliance Guidelines, ensuring that vulnerabilities do not exist for more than 90 days on any networks that involve payment card transactions. This user guide aims to help you navigate the Tenable PCI ASV process from start to finish.

The team is primarily utilized to assess the false positives and compensating controls. The team evaluates disputes via the Tenable PCI ASV Workbench in accordance to the public guide. It's the ASV assessor's responsibility to ensure that the scan customers disputes have appropriate evidence and are defensible when viewed by other stake holders in the PCI process. If needed, assessors ask for further clarification of a dispute.

In-depth consulting is currently not part of the service as the guide relegates such duties to the scan customer's trusted security professional. This ensures that the assessors are performing separate duty and not involved in the design or modification of security controls, where resolution of inconclusive scans involves ASV personnel, the personnel must be ASV Employees qualified by PCI SSC per Section 3.2, "ASV Employee – Skills and Experience" of the ASV Qualification Requirements.

Get Started with Tenable PCI ASV Scanning

To prepare for a Tenable PCI ASV review:

1. Work with your organization to determine what assets in your cardholder data environment (CDE) are in scope for Tenable PCI ASV scanning and review.
2. Create a Tenable PCI ASV Scan:
    - A Tenable PCI ASV scan with the **PCI Quarterly External Scan** template.
    - A Tenable Web App Scanning using the **PCI** template. This scan should be run on payment pages, web application pages, or any pages that can be seen as entry into the CDE or that may contain Card Holder Data (CHD).

    Important: By default, PCI scan data is excluded from dashboards, reports, and workbenches. To view this data, when creating a Tenable PCI ASV scan, you must set the **Scan Results** setting to **Show in the workbenches, dashboards, and reports**.

    Note: Because Tenable PCI ASV scans using the **PCI Quarterly External Scan** and **PCI** template have their own set of rules, any recast rules do not apply to the scan results.

    Note: PCI DSS requires organizations to complete quarterly internal network scans, so you may also need to create a scan using the **PCI Internal Network Scan** template. However, you do not need to submit the internal network scan results for ASV review and validation.
3. Launch a Tenable PCI ASV Scan.

    Note: Since a clean scan substantially increases your chances to pass the ASV certification review, Tenable recommends that you launch the Tenable PCI ASV scan as many times as is needed to get the cleanest scan possible.
4. Submit a Scan for PCI Validation.
5. Create an attestation request draft. As you create the draft, you may need to do one or both of the following:
    - If your scan results include assets that are irrelevant to the attestation, mark each irrelevant asset out of scope.

- If the scan results include any failures, create a dispute for each failure.

  > **Note**: If you leave any failures undisputed when you submit your attestation for review, the ASV reviewer must fail the attestation.

6. After you have addressed all the failures, submit the scan attestation for ASV review.

Log in to Tenable PCI ASV

Required User Role: Administrator and Custom Role

Before you begin:

- Obtain credentials for your user account.

  Note: If you are an administrator logging in to your Tenable PCI ASV 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 PCI ASV after initial setup, your username is the email address you used to register for your Tenable PCI ASV account.

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

To log in to Tenable PCI ASV:

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

   The login page appears.

2. In the username box, type your username.

3. In the password box, type the 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 landing page appears.

6. Click the Tenable PCI ASV tile.

   The Tenable PCI ASV Workbench appears.

Note: Tenable PCI ASV logs you out after a period of inactivity (typically, 30 minutes).

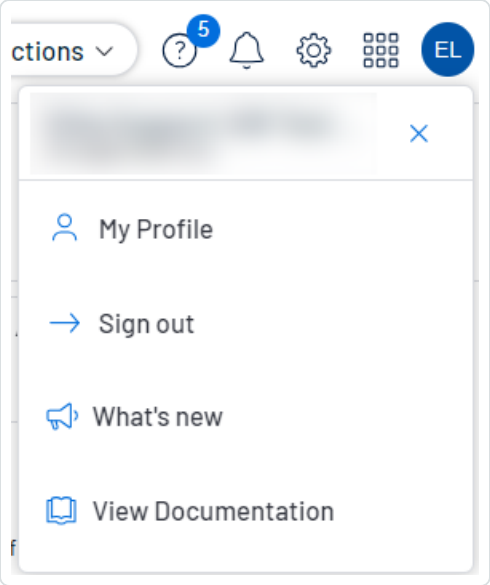
Log Out of Tenable PCI ASV

Required User Role: Administrator and Custom Role

To log out of Tenable PCI ASV:

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

   The user account menu appears.

2. Click **Sign Out**.

Navigate Tenable PCI ASV

Tenable PCI ASV, 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.

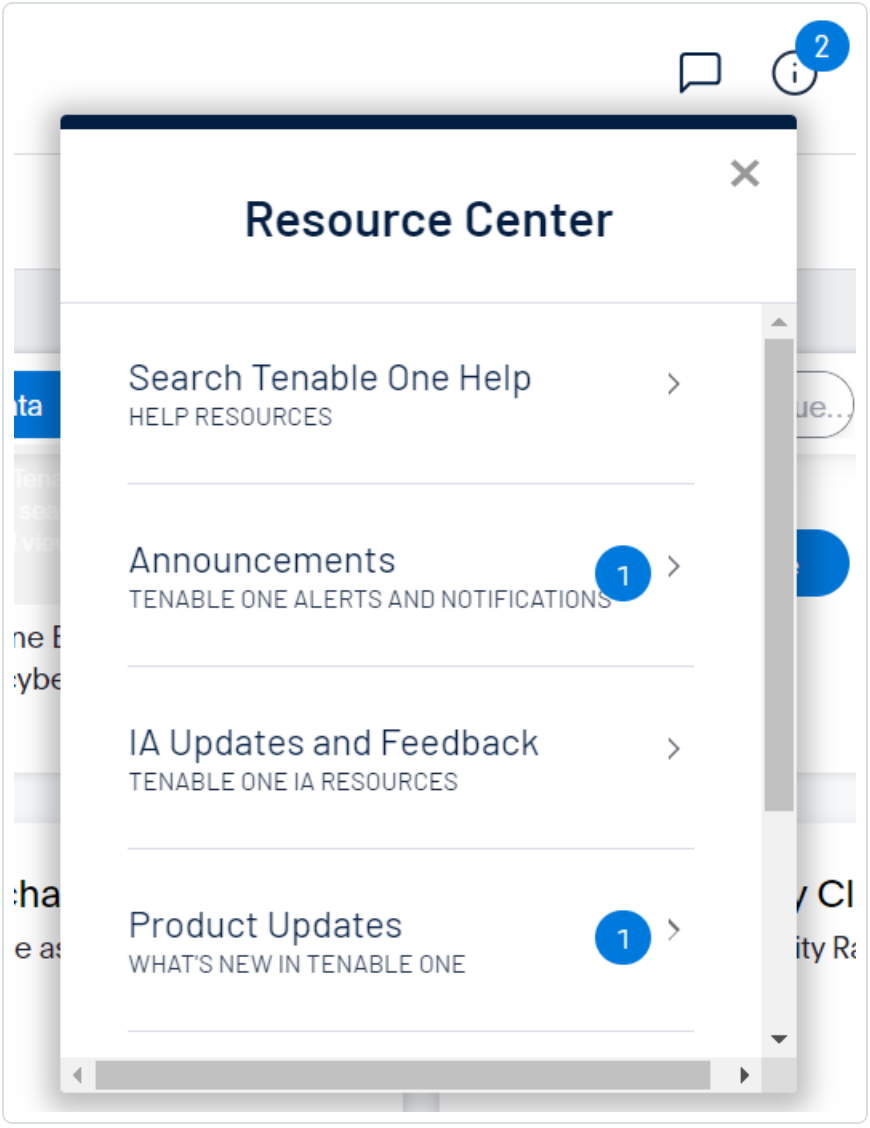
Resource Center

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 PCI ASV, 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 PCI ASV marks those notifications as seen. Once you have seen a notification, you can clear it to remove it from the **Notifications** panel.

> **Note:** Tenable PCI ASV 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 Icon

Workspace

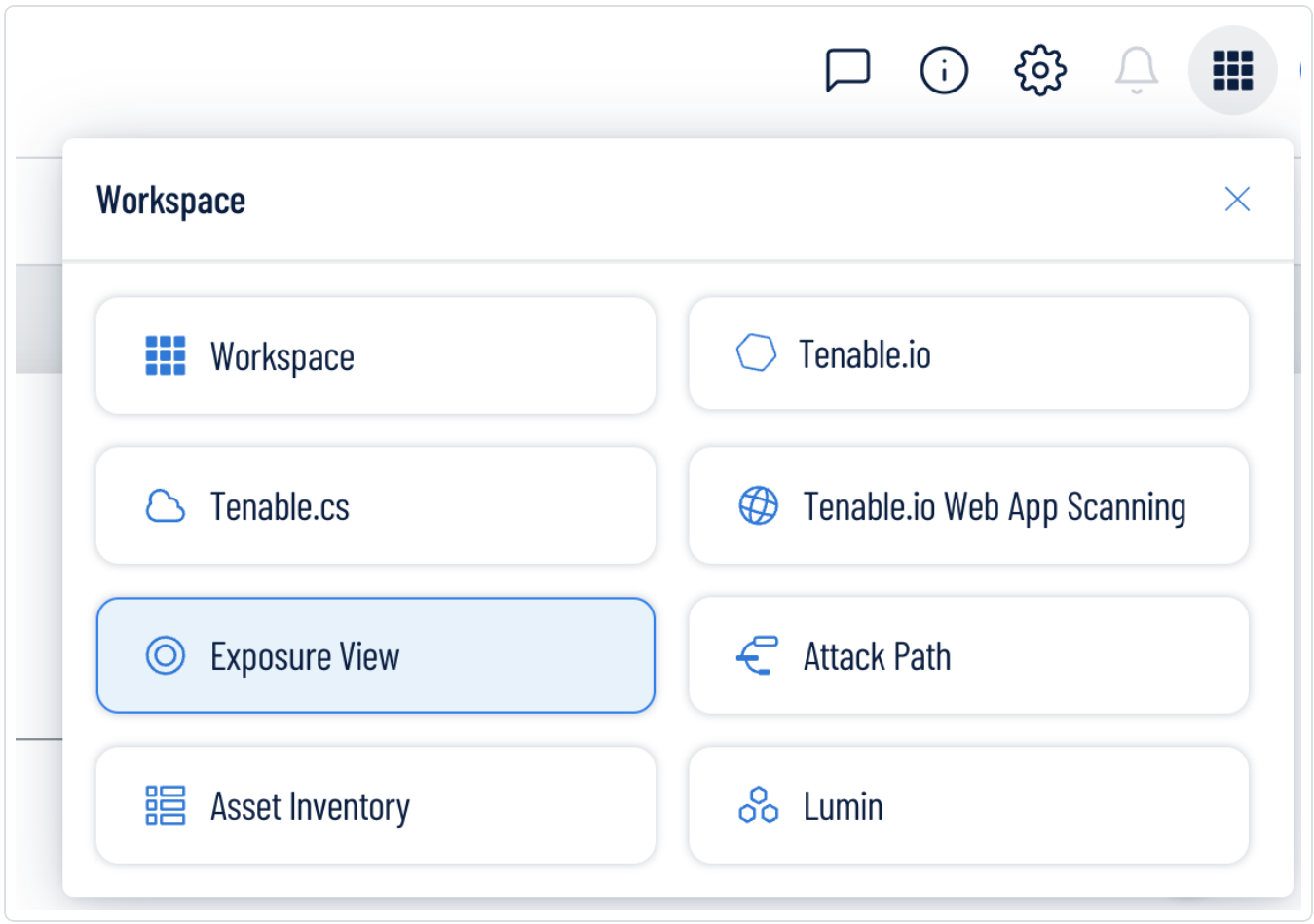
When you log in to Tenable, the **Workspace** page appears by default. On the **Workspace** page, you can switch between your Tenable applications or set a default application to skip the **Workspace** page in the future. You can also switch between your applications from the **Workspace** menu, which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

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

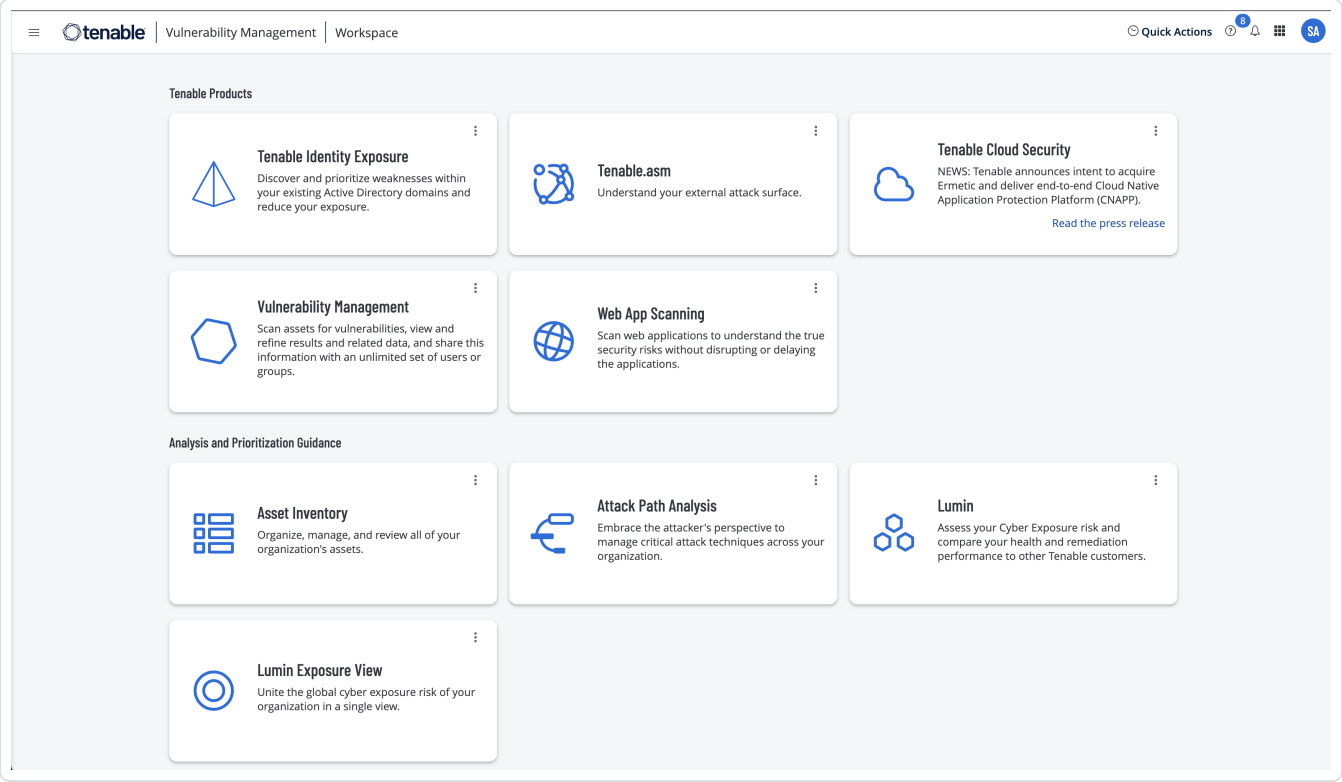
To view the Workspace page:

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

   The **Workspace** menu appears.

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

The **Workspace** page appears.



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.

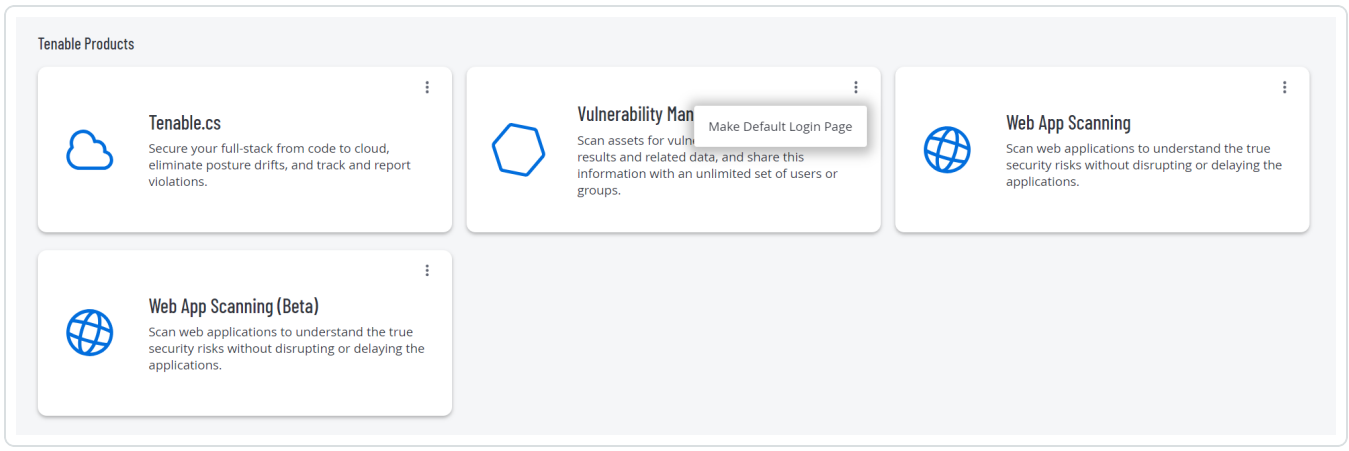
To set a default login application:

1. Log in to Tenable.

   The **Workspace** page appears.

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

   A menu appears.



3. 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. Log in to Tenable.

   The **Workspace** page appears.

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

   A menu appears.

3. Click **Remove Default Login Page**.

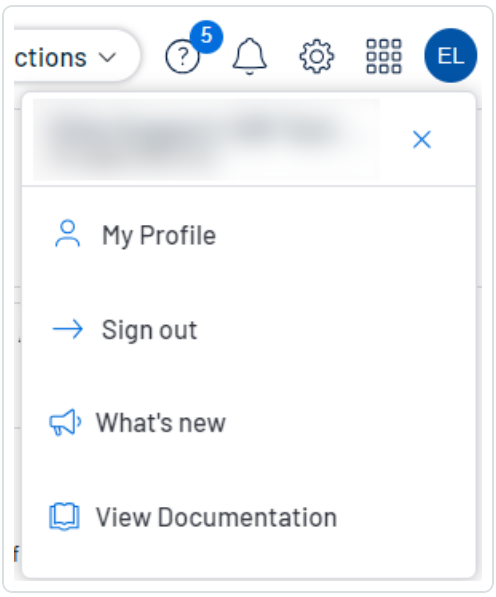
   The **Workspace** page now appears when you log in.

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.
   - Click **Sign out** to sign out of Tenable PCI ASV.
   - Click **What's new** to navigate directly to the Tenable PCI ASV Release Notes.
   - Click **View Documentation** to navigate directly to the Tenable PCI ASV User Guide documentation.

For more information on Tenable PCI ASV specific navigation, see the following topics:

Navigate Planes

Tenable PCI ASV Workbench Tables

Navigate Planes

Tenable PCI ASV 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.

Tenable PCI ASV Workbench Tables

Note: Customizable tables also include the ability to access the actions buttons by right-clicking a table row. To access your browser menu, press the Ctrl key and right-click.

Tenable PCI ASV Workbench tables are any tables in the Tenable PCI ASV interface outside of the **Explore** section.

To interact with a Tenable PCI ASV workbench table:

1. View a workbench table.
2. Do any of the following:

    - Navigate the table:

        - To adjust the sort order, click a column title.

          Tenable PCI ASV sorts all pages of the table by the data in the column you selected.

        - In Tenable PCI ASV, to increase or decrease the number of rows displayed per page, click **Results per page** and select a number.

          Tenable PCI ASV refreshes the table.

        - To view all action buttons available in a table row, click the button.

          This button appears instead of individual action buttons if 5 or more actions are possible for the row.

        - To navigate to another page of the table, click the arrows:

Button	Action
|<	Navigate to the first page of the table.
< >	Navigate to the previous or next page of the table.
>|	Navigate to the last page of the table.

> **Note:** Due to limitations, the total number of findings is not always known past the 1000 limit. In this case, the table may display a modified interface, changes in pagination labeling, and a disabled last page navigation button.

- Search the table:

  In the new interface, a search box appears above individual tables in various pages and planes. In some cases, the search box appears next to the **Filters** box.

  a. In the **Search** box, type your search criteria.

     Your search criteria depends on the type of data in the table you want to search.

  b. Click the button.

     Tenable PCI ASV filters the table by your search criteria.

- To change the column order, drag and drop a column header to another position in the table.

- Remove or add columns:

  a. Roll over any column.

     The button appears in the header.

  b. Click the button.

     A column selection box appears.

  c. Select or clear the check box for any column you want to show or hide in the table.

     > **Tip:** Use the search box to quickly find a column name.

     The table updates based on your selection.

- Adjust column width:

  a. Roll over the header between two columns until the resize cursor appears.

     Click and drag the column width to the desired width.

> **Tip:** To automatically resize a column to the width of its content, double-click the right side of the column header.

- To sort data in the table, click a column header.

  Tenable PCI ASV sorts all pages of the table by the data in the column you selected.

- To sort data in the table by multiple columns, press **Shift** and click one or more column headers.

  > **Note:** Not all tables or columns support sorting by multiple columns.

  Tenable PCI ASV sorts all pages of the table in the order in which you selected the columns.

Filter a Table

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

In Tenable PCI ASV, 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 Tenable Vulnerability Management Tables.

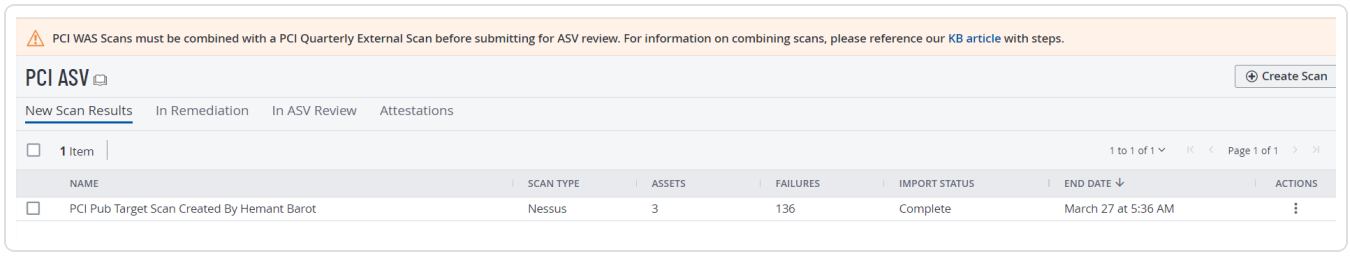
Tenable PCI ASV Workbench

The Tenable PCI ASV Workbench is the landing page for your Tenable PCI ASV product. Here, you can begin your scan review and attestation process.

To access the Tenable PCI ASV Workbench:

1. In the Workspace, click the **PCI ASV** tile.

   The **PCI ASV Workbench** page appears, showing a scans table.



2. From the **PCI ASV Workbench**, you can access the following tabs:

   - **New Scan Results — The New Scan Results tab appears by default when you log in to Tenable PCI ASV. This tab includes a table that shows your Tenable PCI ASV scans.**

     This table includes the following information:

Column	Details
Name	The name of the Tenable PCI ASV scan.
Scan Type	The type of scan, for example, **Nessus** or **WAS**.
Assets	The number of assets discovered during the scan.
Failures	The number of failures discovered during the scan.
Import Status	The status of the scan import job, for example, **In Progress** or **Complete**.
End Date	The date and time at which the scan completed.

Actions	Click the ⋮ button to view available actions for the scan: • **Start Attestation** — Begin an attestation for the scan. For more information, see Create an Attestation. • **Delete** — Delete the scan: a. Click **Delete**. A confirmation message appears. b. Click **Delete**. Tenable PCI ASV deletes the scan from the table.

- **In Remediation — This tab includes a table that shows all attestation drafts that have not yet been submitted for ASV review.**

This table includes the following information:

Column	Details
Name	The name of the attestation.
Owner	The owner of, or person who created, the attestation.
Assets	The number of assets associated with the attestation.
Failures	The number of failures associated with the attestation.
Status	The status of the scan import job, for example, **In-Progress** or **Needs Work**.
ASV Message	Where applicable, a message from the ASV reviewer regarding the attestation status.
Last Modified	The date and time at which the attestation was last modified by a user.
Actions	Click the ⋮ button to view available actions for the attestation:

	• **Send to ASV Review** — Submit the attestation for ASV review. For more information, see Submit an Attestation for ASV Review. • ↓ **ASV Scan Report Summary** — Download the ASV Scan Report Summary as a PDF export file. • ↓ **ASV Scan Report Vulnerability Details** — Download the ASV Scan Report for Vulnerability Details as a PDF export file. • **Delete** — Delete the attestation: a. Click **Delete**. A confirmation message appears. b. Click **Delete**. Tenable PCI ASV deletes the scan from the table. • ↓ **Feedback** — Download a feedback form for the attestation in PDF format. • [→ **Export** — Export the attestation. For more information, see Export Attestations.

- **In ASV Review — This tab includes a table that shows all attestations that are currently in ASV review.**

This table includes the following information:

Column	Details
Name	The name of the attestation.
Owner	The owner of, or person who created, the attestation.
Assets	The number of assets associated with the attestation.

Failures	The number of failures associated with the attestation.
Disputes	The number of disputes associated with the attestation.
Status	The status of the scan import job, for example, **Assigned** or **In-Review**.
Last Modified	The date and time at which the attestation was last modified by a user.
Actions	Click the ⋮ button to view available actions for the attestation: • ↓ **ASV Scan Report Summary** — Download the ASV Scan Report Summary as a PDF export file. • ↓ **ASV Scan Report Vulnerability Details** — Download the ASV Scan Report for Vulnerability Details as a PDF export file. • ↓ **Feedback** — Download a feedback form for the attestation in PDF format. • [→ **Export** — Export the attestation. For more information, see Export Attestations.

- **Attestations — This tab includes a table that shows all completed attestations.**

This table includes the following information:

> **Tip:** An attestation is completed when it recieves a status of **Passed**, **Failed**, or **Closed**.

Column	Details
Name	The name of the attestation.
Owner	The owner of, or person who created, the attestation.
Assets	The number of assets associated with the attestation.

Failures	The number of failures associated with the attestation.
Disputes	The number of disputes associated with the attestation.
Status	The status of the scan import job, for example, **Passed** or **Failed**.
Last Modified	The date and time at which the attestation was last modified by a user.
Actions	Click the ⋮ button to view available actions for the attestation: • ↓ **ASV Scan Report Summary** – Download the ASV Scan Report summary as a PDF export file. • ↓ **ASV Scan Report Vulnerability Details** – Download the ASV Scan Report for Vulnerability Details as a PDF export file. • ↓ **Feedback** – Download a feedback form for the attestation in PDF format. • [→ **Export** – Export the attestation. For more information, see Export Attestations.

Create a Tenable PCI ASV Scan

Required User Role: Administrator

In Tenable PCI ASV, you can create the following scans using scan templates:

- Vulnerability Management Scan using the **Internal PCI Network Scan** and **PCI Quarterly External Scan** templates
- Tenable Web App Scanning scan using the **PCI** template

When you create a scan, Tenable PCI ASV assigns you owner permissions for the scan.

Important: By default, PCI scan data is excluded from dashboards, reports, and workbenches. To view this data, you must set the **Scan Results** setting to **Show in the workbenches, dashboards, and reports**.

Before you begin:

- (Optional) View Tenable PCI ASV scan limitations.
- Create a permission configuration for any targets you want to use in the scan and assign **Can Scan** permissions to the appropriate users.

To create a Tenable PCI ASV scan:

1. Access the Tenable PCI ASV Workbench.
2. In the upper-right corner of the page, click ⊕ **Create Scan**.

   The **Select a Scan Template** page appears. By default, the **Nessus Scanner** tab is active.
3. Click the tile for the template you want to use for your scan.

   The **Create a Scan** page appears.
4. Configure the scan:

Tab	Action
Settings	Configure the settings available in the scan template. **Vulnerability Management Scan using the Internal PCI Network Scan**

	or PCI Quarterly External Scan templates • Basic — 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 — Specifies how a scan performs discovery and port scanning. • Assessment — 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. **Note**: Assessment settings appear only on Internal PCI Network Scan templates. • Report — Specifies whether the scan generates a report. **Note**: Report settings appear only on Internal PCI Network Scan templates. • Advanced — Specifies advanced controls for scan efficiency.
	Tenable Web App Scanning scan using the PCI template • Basic — 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. • Scope — Specifies the URLs and file types that you want to include in or exclude from your scan. • Assessment — Specifies which web application elements you want the scanner to audit as it crawls your URLs.

	• Report — Specifies extra items to include in the scan report. • Advanced — Specifies advanced controls you want to implement in a web application scan.
Credentials	Specify credentials you want to perform a credentialed scan. Credentials in vulnerability management scan Credentials in Tenable Web App Scanning scan

5. Do one of the following:

   - If you want to save without launching the scan, click **Save**.

     Tenable PCI ASV 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 PCI ASV saves and launches the scan.

Tenable PCI ASV Scan Templates

Scan templates contain granular configuration settings for your scans. You can use the Tenable PCI ASV scan templates to create custom scan configurations for your organization. Then, you can run scans based on scan settings configured in the templates. 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 template on which a scan is based.

Tenable PCI ASV provides the following scan templates:

Template	Description
Nessus Scanner	
Internal PCI Network Scan	Performs an internal PCI DSS (11.2.1) vulnerability scan. This template creates scans that you can use to satisfy internal (PCI DSS 11.2.1) scanning requirements for ongoing vulnerability management programs that satisfy PCI compliance requirements. You can use these scans for ongoing vulnerability management and to perform rescans until passing or clean results are achieved. You can provide credentials to enumerate missing patches and client-side vulnerabilities. **Note:** While the PCI DSS requires you to provide evidence of passing or "clean" scans on at least a quarterly basis, you must also perform scans after any significant changes to your network (PCI DSS 11.2.3).
PCI Quarterly External Scan	Performs quarterly external scans as required by PCI.
Web Application	
PCI	PCI A scan that assesses web applications for compliance with Payment Card Industry Data Security Standards (PCI DSS) for Tenable PCI ASV. (This scan also allows you to view and edit the Request Redirect Limit. The default value for this limit is 3.)

Tenable PCI ASV Scan Settings for Vulnerability Management

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 Nessus scanner PCI templates on which a scan is based.

Internal PCI Network Scan Template Settings

The Internal PCI Network Scan template settings are organized into the following categories:

- Basic Settings in Tenable PCI ASV
- Discovery Settings in Tenable PCI ASV
- Assessment Settings in Tenable PCI ASV
- Advanced Settings in Tenable PCI ASV
- Report Settings in Tenable PCI ASV Scans

PCI Quarterly External Scan Template Settings

The PCI Quarterly External Scan settings are organized into the following categories:

- Basic Settings in Tenable PCI ASV
- Discovery Settings in Tenable PCI ASV
- Advanced Settings in Tenable PCI ASV

Basic Settings in Tenable PCI ASV

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 PCI ASV, see Scan Limitations.

The **Basic** settings include the following sections:

- General
- Basic Settings in Tenable PCI ASV
- 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	Keep private	Specifies whether the results of the scan should appear in dashboards or be kept private. When set to **Keep private**, you must access the scan directly to view the results. **Important:** By default, PCI scan data is excluded from dashboards, reports, and workbenches. To view this data, you must set the **Scan Results** setting to **Show in the workbenches, dashboards, and reports**.
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.
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	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.
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**.
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 PCI ASV may still need to index the scan job for up to 24 hours. This can cause the scan not to show as **Completed** after the scan window is complete. Once Tenable PCI ASV indexes the scan, it shows as **Completed**.
Network	Default	
Targets	None	Specifies one or more targets to be scanned. If you select a target group or upload a targets file, you are not required to specify additional targets. 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 PCI ASV 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 PCI ASV, see Scan Limitations. **Note:** See Permissions for more information on how permissions affect targets.
Upload Targets	None	Uploads a text file that specifies 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.

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.

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 PCI ASV 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 09/31/2018 at 9:12 AM, the default starting date and time is set to *09/31/2018* and *09:30*.
Timezone	Varies	Specifies the timezone of the value set for **Starts**.

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.
SMS Recipient(s)	None	Specifies zero or more phone numbers, separated by commas, that are alerted when a scan completes and the results are available.

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 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.

Discovery Settings in Tenable PCI ASV

The **Discovery** settings relate to discovery and port scanning, including port ranges and methods.

Template	Scan Type	Preconfigured Settings
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
PCI Quarterly External Scan	–	Specifies whether the Nessus scanner scans hosts that do not respond to any ping methods.

Discovery Settings for Custom Scan Type

If you select the **Custom** preconfigured setting option, you can manually configure **Discovery** settings in the following categories:

- Host Discovery
- Port Scanning
- Service Discovery

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**.
General Settings		
Use Fast Network Discovery	Disabled	When disabled, if a host responds to ping, Tenable PCI ASV 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 PCI ASV 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. Supported keyword values are: • `default` instructs the scanner to scan approximately 4,790 commonly used ports. • `all` instructs the scanner to scan all 65,536 ports, including port 0. Additionally, you can indicate a custom list of ports by using a comma-separated list of ports or port ranges. For example, `21,23,25,80,110` or `1-1024,8080,9000-9200`. If you wanted to scan all ports excluding port 0, you would type `1-65535`. The custom range specified for a port scan is applied to the protocols you have selected in the **Network Port Scanners** group of settings. If scanning both TCP and UDP, you can specify a split range specific to each protocol. For example, if you want to scan a different range of ports for TCP and UDP in the same policy, you would type `T:1-1024,U:300-500`. You can also specify a set of ports to scan for both protocols, as well as individual ranges for each separate

Setting	Default Value	Description
		protocol. For example, `1-1024,T:1024-65535,U:1025`.
Local Port Enumerators		
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.
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*.
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	Enabled	If a local port enumerator runs, all network port scanners will be disabled for that asset.

Setting	Default Value	Description
Local Port Enumeration Failed		
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

Setting	Default Value	Description
		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 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.

Setting	Default Value	Description
		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 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 two options: • **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 SSL/TLS ports** • **All TCP 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

Setting	Default Value	Description
		ciphers.
Enable CRL Checking (Connects to the Internet)	False	When enabled, the scanner checks that none of the identified certificates have been revoked.

Assessment Settings in Tenable PCI ASV

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.

Note: Assessment settings appear only on Internal PCI Network Scan templates.

Template	Mode	Preconfigured Settings
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	• General Settings:

	vulnerabilities (quick)	◦ 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	Assessment Settings for Custom Mode
PCI Quarterly External Scan	–	–

Assessment Settings for Custom Mode

If you select the **Custom** preconfigured setting option, you can manually configure **Assessment** settings in the following categories:

- General
- Brute Force
- Web Applications
- Windows

General

The **General** section includes the following groups of settings:

- Accuracy

Setting	Default Value	Description
Accuracy		
Override Normal Accuracy	Disabled	In some cases, Tenable PCI ASV cannot remotely determine whether a flaw is present or not. If report 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 PCI ASV 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	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.

speed)		

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 PCI ASV 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 PCI ASV from performing these tests.
Oracle Database		
Test default accounts (slow)	Disabled	Test for known default accounts in Oracle software.

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	Disabled	By default, Tenable PCI ASV does not scan

Setting	Default Value	Description
applications		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 PCI ASV 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 **<>** log out	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(\?.*)?$). Tenable PCI ASV 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 PCI ASV follows for each start page.
Follow dynamically generated pages	Disabled	If selected, Tenable PCI ASV follows dynamic links and may exceed the parameters set above.
Application Test Settings		

Setting	Default Value	Description
Enable generic web application tests	Disabled	Enables the following settings.
Abort web application tests if HTTP login fails	Disabled	If Tenable PCI ASV 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 PCI ASV 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 data to the application. When enabled, Tenable PCI ASV 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

Setting	Default Value	Description
		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 PCI ASV would attempt `/test.php?arg1=XSS&b=1&c=1`, where b and c allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated. 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

Setting	Default Value	Description
		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 PCI ASV 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 PCI ASV would never test for `/test.php?a=XSS&b=3&c=3&d=3` 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

Setting	Default Value	Description
		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 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 PCI ASV stops and switches to another web server on a different port.

Setting	Default Value	Description
		• **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 PCI ASV 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 PCI ASV 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	Enabled	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 PCI ASV enumerates users via the Security Account Manager (SAM) registry.
ADSI Query	Enabled	Tenable PCI ASV enumerates users via Active Directory Service Interfaces (ADSI). To use ADSI, you must configure credentials under **Credentials** > **Miscellaneous** > **ADSI**.
WMI Query	Enabled	Tenable PCI ASV enumerates users via Windows Management Interface (WMI).
RID Brute Forcing	Enabled	Tenable PCI ASV 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 PCI ASV attempts to enumerate domain users.
End UID	1200	The end of a range of IDs where Tenable PCI ASV 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 PCI ASV attempts to enumerate local users.
End UID	1200	The end of a range of IDs where Tenable PCI ASV attempts to enumerate local users.

Report Settings in Tenable PCI ASV Scans

The **Report** settings include the following groups of settings:

- Processing
- Output

Setting	Default Value	Description
Processing		
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		
Designate hosts by	Disabled	Uses the host name rather than IP address for report

Setting	Default Value	Description
their DNS name		output.
Display hosts that respond to ping	Disabled	Reports hosts that successfully respond to a ping.
Display unreachable hosts	Disabled	When enabled, hosts that did not reply to the ping request are included in the security report as dead hosts. Do not enable this option for large IP blocks.
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 PCI ASV

The **Advanced** settings provide increased control over scan efficiency and the operations of a scan, as well as the ability to enable plugin debugging.

Template	Scan Type	Preconfigured Settings
Vulnerability Scans (Common)		
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
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) • Windows File Search Options

Custom Advanced Settings in Tenable PCI ASV Scans

If you select the **Custom** preconfigured setting option, you can manually configure **Advanced** settings in the following categories:

- General Settings
- Performance Options
- Unix Find Command Options
- Windows File Search Options
- Debug Settings

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 PCI ASV 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 PCI ASV scans a list of IP addresses in sequential order. When this option is enabled, Tenable PCI ASV 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.

Setting	Default Value	Description
Automatically accept detected SSH disclaimer prompts	Disabled	When enabled, if a credentialed scan tries to connect via SSH to a FortiOS host that presents a disclaimer prompt, the scanner provides the necessary text input to accept the disclaimer prompt and continue the scan. The scan initially sends a bad ssh request to the target in order to retrieve the supported authorization methods. This allows you to determine how to connect to the target, which is helpful when you configure a custom ssh banner and then try to determine how to connect to the host. 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 PCI ASV 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 PCI ASV 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	Enabled	When enabled, the scanner creates a unique identifier for

Setting	Default Value	Description
identifier on hosts scanned using credentials		credentialed scans.
Trusted CAs	None	Specifies CA certificates that the scan considers as trusted. This allows you to use self-signed certificates for SSL authentication without triggering plugin 51192 as a vulnerability in your Tenable PCI ASV environment.
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 PCI ASV uses the Linux kernel to detect when it sends too many packets and the network pipe approaches capacity. If detected, Tenable PCI ASV throttles the scan to accommodate and alleviate the congestion. Once the congestion subsides, Tenable PCI ASV automatically attempts to use the available space within the network pipe again.
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.

Setting	Default Value	Description
Max simultaneous hosts per scan	Depends on the Tenable-provided template used for the scan	Specifies the maximum number of hosts that Tenable PCI ASV 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 PCI ASV 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 PCI ASV 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 sessions per host	None	Specifies the maximum number of established TCP sessions for a single host. This TCP throttling option also controls the number of packets per second the SYN scanner sends, which is 10 times the number of TCP sessions. For example, if this option is set to 15, the SYN scanner sends 150 packets per second at most.
Max number of concurrent TCP	None	Specifies the maximum number of established TCP sessions for each scan task, regardless of the number of

Setting	Default Value	Description
sessions per scan		hosts being scanned. For scanners installed on any Windows host, you must set this value to 19 or less to get accurate results.
Unix Find Command Options		
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

Setting	Default Value	Description
		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.
Windows File Search Options		
Windows Exclude Filepath	None	A plain text file containing a list of filepaths to exclude from any search on Windows systems. In the file, enter one filepath per line. This setting overrides and removes default exclusions.
Windows Include Filepath	None	A plain text file containing a list of filepaths to include in any use of Recursive search on Windows systems. In the file, enter one filepath per line. This setting replaces any defaults entirely.
Debug Settings		
Enable plugin debugging	Disabled	Attaches available debug logs from plugins to the vulnerability output of this scan.
Audit Trail Verbosity	Default	Controls verbosity of the plugin audit trail. Options include: • **No audit trail** — (Default) Tenable PCI ASV 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.

Tenable PCI ASV Scan Settings for Tenable Web App Scanning

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.

Tenable Web App Scanning scan settings are organized into the following categories:

- 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

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.

The **Basic** settings include the following sections:

- General
- Schedule
- Notifications
- User Permissions
- Data Sharing

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 after being saved.	Yes
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
Scanner	varies	Specifies the scanner that performs the scan.	Yes

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**.

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**, you must access the scan directly

Setting	Default Value	Description
		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.

The **Scope** settings include the following sections:

- Crawl Scripts
- Scan Inclusion
- Scan Exclusion
- Miscellaneous

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.

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.

Setting	Default	Description
		Type each URL on a separate line. **Note:** All URLs should have the same domain and wildcards are not allowed.

Scan Exclusion

The attributes of URLs you want the scanner to exclude from your scan.

Setting	Default Value	Description
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	Check box option that allows you to specify whether you want the scanner to ignore pages in situations when similar pages have already been audited.

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.

The **Report** settings include the following section:

- (Tenable PCI ASV 6.1) Load Balancers Usage

(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 if applicable.	No

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.

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.

Advanced Settings in Tenable Web App Scanning Scans

Advanced settings specify additional controls you want to implement in a web application scan.

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).

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** check box. 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:** The current Tenable Web App Scanning user-agent header is: `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36` **Note:** Not all requests from 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 Width	1600	Specifies the screen width, in pixels, of the browser embedded in 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	10	Specifies the maximum number of sub-directories

Depth		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, 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	1	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.

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.
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)	5	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)	30	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.

Launch a Tenable PCI ASV Scan

Required User Role: Administrator

Required Scan Permissions: Can Control

In addition to configuring Schedule settings for a scan, you can manually start a scan run.

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.

Note: To learn more about scan limitations in Tenable PCI ASV, see Scan Limitations.

To launch a 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 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 Scan Folders.

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-delimited string of targets.

c. Click **Launch**.

Tenable PCI ASV launches the scan.

You can follow the scan's progress by checking its Scan Status on the **Scans** page.

Scan Status

In Tenable PCI ASV, depending on its state, scans can have following status values:

Note: The percentage on the Tenable PCI ASV scan progress indicator represents the percentage of completed tasks in the scan. A scan with one task shows 0% progress until the scan completes.

Tip: For Tenable PCI ASV 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.

Status	Description
Tenable PCI ASV Scans **Tip:** The typical Tenable PCI ASV scan status flow is as follows: **Initializing**, **Running**, **Publishing Results**, **Completed**.	
Aborted	Either the latest run of the scan is incomplete because Tenable PCI ASV 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 PCI ASV successfully stopped the latest run of the scan.
Completed	The latest run of the scan is complete.
Empty	The scan is either empty (the scan is new or has yet to run) or pending (Tenable PCI ASV is processing a request to run the scan).
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 PCI ASV is processing the action.
Paused	At user request, Tenable PCI ASV 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 PCI ASV does not dispatch new tasks from a paused scan job. If the scan remains in a paused state for more

Status	Description
	than 14 days, the scan times out. Tenable PCI ASV then aborts the related tasks on the scanner and categorizes the scan as aborted.
Pending	Tenable PCI ASV has the scan queued to launch and is assigning scan tasks to the assigned sensors. **Note**: Tenable PCI ASV aborts scans that remain in **Pending** status for more than four hours. If Tenable PCI ASV aborts your scan, modify your scan schedules to reduce the number of overlapping scans. If you still have issues, contact Tenable Support.
Publishing Results	Tenable PCI ASV processes and stores the scan results data for you to view and use in the Tenable PCI ASV user interface. The **Publishing Results** status begins once the **Running** status reaches 100%.
Resuming	Tenable PCI ASV is in the process of restarting tasks after the user resumed the scan. Tenable PCI ASV instructs the scanner to start the tasks from the point at which the scan was paused. If Tenable PCI ASV or the scanner encounters problems when resuming the scan, the scan fails, and Tenable PCI ASV updates the scan status to aborted.
Running	The scan is currently running. While this status is shown, the scan's sensors complete their assigned scan tasks, and Tenable PCI ASV 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, and Tenable PCI ASV is processing the action.
Tenable Web App Scanning Scans	
Aborted	The scanner did not complete the scan's latest scan job. Tenable Web App Scanning may abort a scan job because the job was queued without running for more than four hours, or because Tenable Web App Scanning, or the scanner, encountered other problems and aborted the scan. For more information about why Tenable Web App Scanning aborted a scan, view the scan notes.

Status	Description
Canceled	At the user's request, Tenable Web App Scanning successfully stopped the latest scan job.
Completed	The scanner completed the scan's latest scan job.
Never Run	The scan is either empty (the scan is new or has yet to run) or pending (Tenable Web App Scanning is processing a request to run the scan).
Pending	Tenable Web App Scanning has the scan queued to launch. **Note**: Tenable Web App Scanning aborts scans that remain in **Pending** status for more than four hours. If Tenable Web App Scanning aborts your scan, modify your scan schedules to reduce the number of overlapping scans. If you still have issues, contact Tenable Support.
Processing	The scan has completed but the results are still being processed. The scanner is processing vulnerability findings, attachments, notes, and other metadata.
Running	The scanner is currently running the scan.
Stopping	The scanner acknowledged the stop request and is in the process of stopping.

Submit a Scan for PCI Validation

Required User Role: Administrator

You can submit a completed Tenable PCI ASV scan for PCI validation from the **Scans** page.

To submit a scan for PCI validation:

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. Below **Scans**, choose to view **Vulnerability Management Scans** or **Web Application Scans**.

4. 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.

5. 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.

6. In the scan details plane, click the **See All Details** button.

   The **Scan Details** page appears.

7. In the upper-right corner, click **Submit PCI**.

   A **Submit Scan for PCI Validation** window appears.

   Note: If Tenable PCI ASV detects any failures in the scan, a message appears recommending that you submit a clean scan. You can either click **Fix Failures**, discard your scan, and create another scan or you can continue with the existing scan and address the failures after you create your attestation.

8. Click **Continue**.

   A **Scan Submitted for PCI Validation** message appears.

   The scan appears in the **New Scan Results** tab in your **PCI ASV** workbench.

What to do next:

- Create an attestation for the scan.

Create an Attestation

Required User Role: Administrator and Custom Role

After you submit a Tenable PCI ASV scan, you must create an attestation request draft.

Note: When you create an attestation request draft for a scan, you do not also submit the scan for ASV attestation. You must dispute all remaining failures and address all out of scope assets before you submit the attestation for ASV approval.

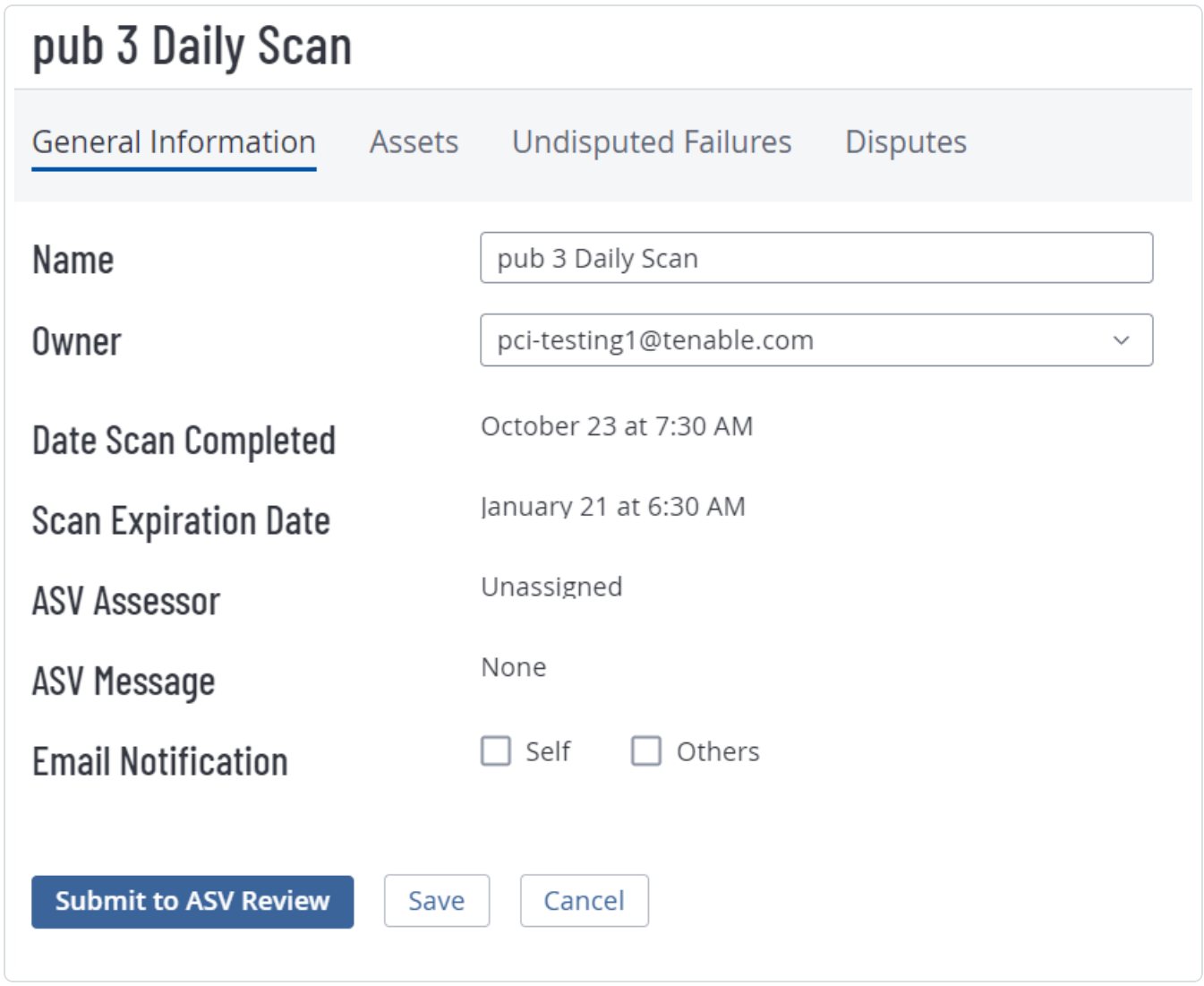
Caution: You cannot create an attestation for scans that are more than 90 days old.

To create an attestation request:

1. Access the Tenable PCI ASV Workbench.
2. In the scans table, in the **New Scan Results** tab, select the check box next to the scan or scans for which you want to create an attestation.
3. In the action bar, click **Start Attestation**.

   The **Attestation Detail** page appears.

   Note: You cannot start an attestation for Tenable Web App Scanning unless you include a PCI Quarterly External scan as well. For more information, see the KB article: How To Combine multiple PCI ASV Scans.



4. In the **Name** box, type the name of the attestation as you want it to appear on the attestation request.

   Note: Tenable recommends that you type a name you can easily identify. After you submit the attestation request, you cannot change the name on the attestation.

5. (Optional) To assign the attestation to a different user, in the **Owner** drop-down box, select the user to whom you want to assign the attestation.

6. (Optional) To enable email notifications for the attestation:

a. Select the check box(es) for the user(s) you want to notify about the attestation:

- **Self** — Notify the owner about the attestation.

  Tip: The notifications are sent to the user selected in the **Owner** drop-down box.

- **Others** — Notify other users about the attestation:

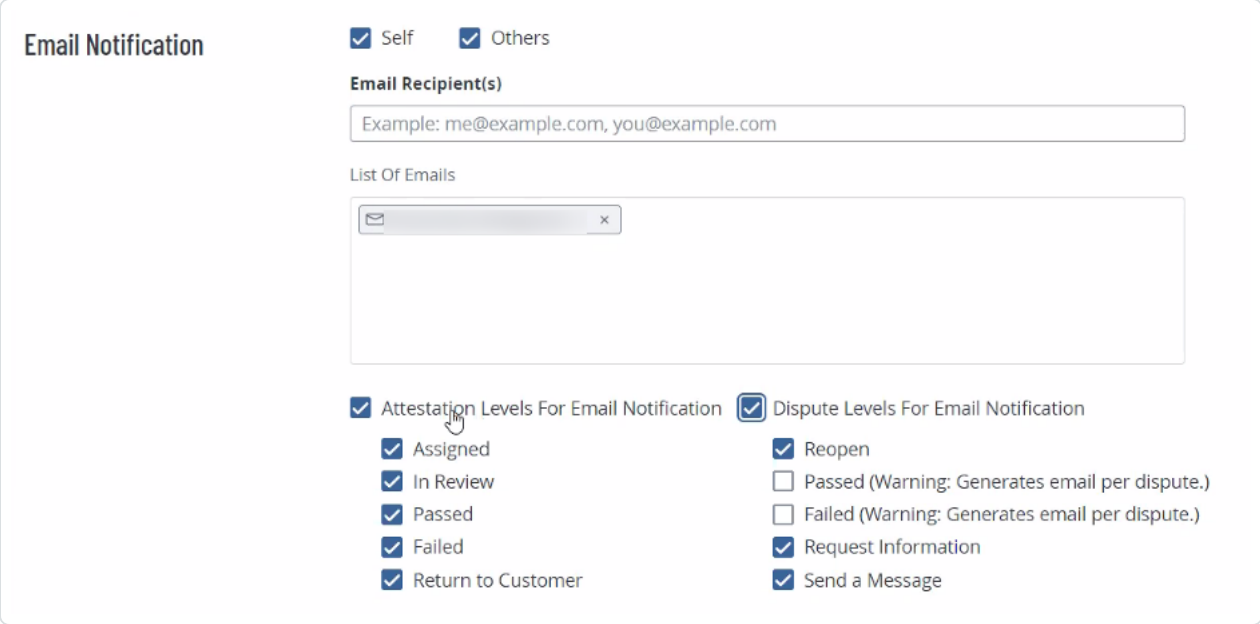
  Email recipient options appear.

  i. In the **Email Recipient(s)** box, type the email of the user you want to notify about the attestation.

  ii. On your keyboard, press **Enter**.

  Tenable PCI ASV adds the email to the **List Of Emails** box.

A list of notification types appears.



b. Select the check box next to each notification type for which you want to trigger an email notification.

Note: Because a Tenable PCI ASV generates a notification for every individual dispute, the **Passed** and **Failed** notification types are deselected by default.

7. Do one of the following:

- Click **Save**.

  Tenable PCI ASV saves the attestation draft in the **In Remediation** tab of the Tenable PCI ASV table.

  > **Note**: You can return to a saved, unsubmitted attestation and configure the options until you submit the attestation for review.

- Click **Submit to ASV Review**. For more information, see Submit an Attestation for ASV Review.

What to do next:

- If the scan includes any assets that are irrelevant to the Tenable PCI ASV review, mark each irrelevant asset out of scope.
- If the new attestation displays any failures in the **Undisputed Failures** tab, create a dispute for each failure.

Mark an Asset as Out of Scope

Required User Role: Administrator and Custom Role

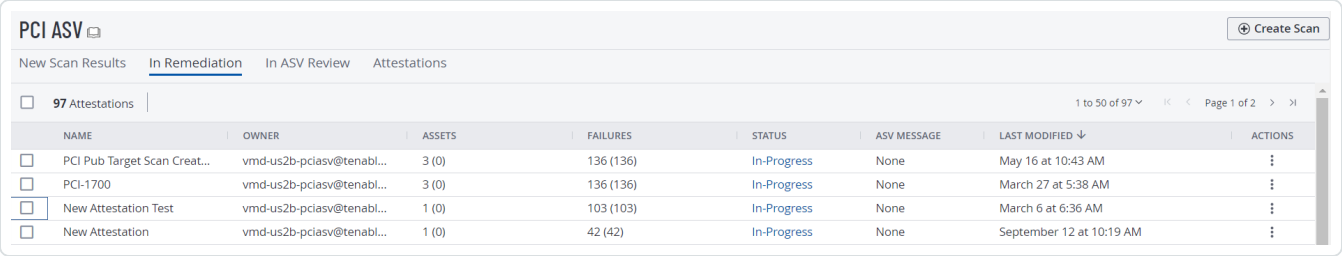
Before you begin:

- Create and launch your scan.
- Create an attestation request for your scan.

To mark an asset as out of scope:

1. Access the Tenable PCI ASV Workbench.
2. Click the **In Remediation** tab.

   A table of your attestation requests appears.



3. Click the attestation that has an asset you want to mark out of scope.

   The **Attestation Details** page appears.

4. Click the **Assets** tab.

   A table of assets associated with the attestation appears.

5. Select the check box next to the asset or assets you want to mark out of scope.

   The **Mark as Out of Scope** button appears.

6. Click the **Mark as Out of Scope** button.

   Tenable PCI ASV removes the asset or assets from Tenable PCI ASV review scope.

   The **Out Of Scope** pane appears.

7. In the **Message for Analyst** text box, provide the reason for out of scope as a message to the analyst.
8. Click **Save**.

   Tenable PCI ASV removes the asset or assets from Tenable PCI ASV review scope.

What to do next:

- If your attestation request includes any undisputed failures, create a dispute for each failure.
- If your attestation request has no undisputed failures, submit the attestation request for ASV review.

Disputes

When you create and launch a Tenable PCI ASV scan, the scan results may include findings you want to dispute before you submit the associated attestation for review. To address these finding, you can create a dispute to submit to the ASV reviewer.

After you create a dispute, you can edit, clone, or delete the dispute as needed.

- Create a Dispute
- Clone a Dispute to an Attestation
- Edit a Dispute
- Delete a Dispute

Create a Dispute

Required User Role: Administrator and Custom Role

When you run a Tenable PCI ASV scan and the scan detects failures, you must dispute the failures before you can submit the associated attestation for ASV review.

Before you begin:

- Create an Attestation for the scan.
- (Optional) To remove certain assets from the Tenable PCI ASV review, mark each asset as out of scope.

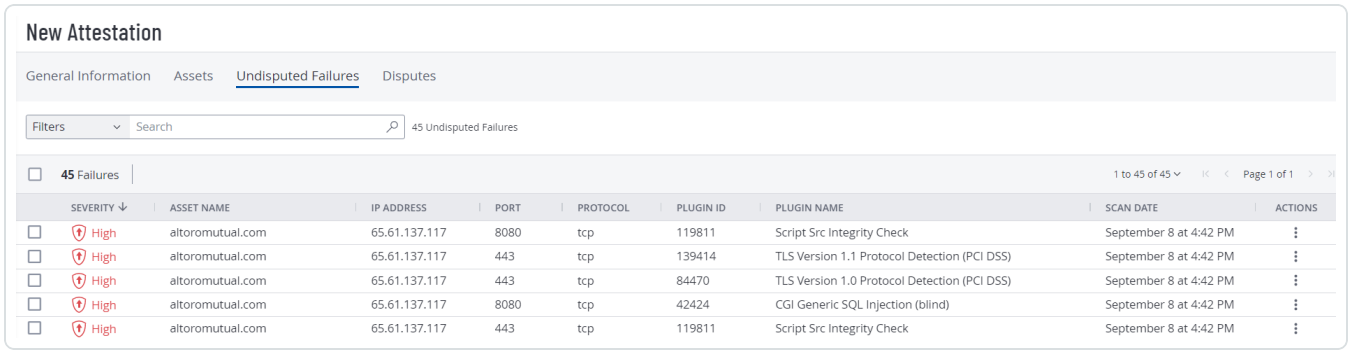
To create a dispute:

1. Access the Tenable PCI ASV Workbench.
2. Click the **In Remediation** tab.

   A table of your attestation requests appears.
3. Click the attestation that has a failure you want to dispute.

   The **Attestation Details** page appears.
4. Click the **Undisputed Failures** tab.

   A table of the undisputed failures for the attestation appears.



5. Do one of the following:

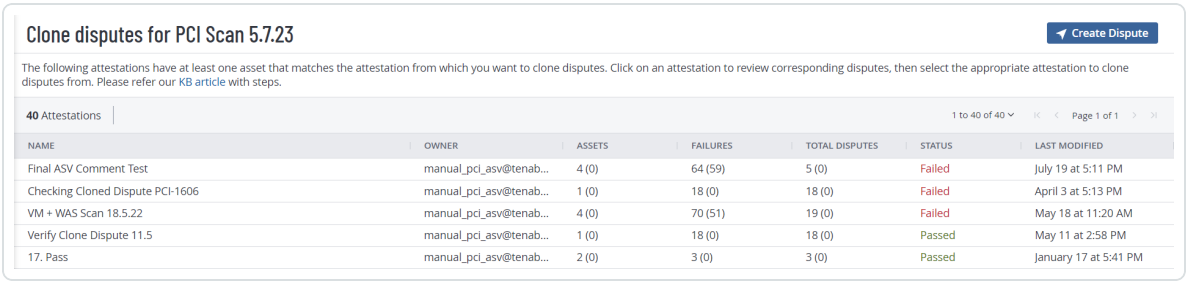
- To create a dispute for a single failure, roll over the row for the failure you want to dispute and click ⋮ > **Create Dispute**.

- To create a dispute for multiple failures, select the check box next to each failure you want to dispute and click **Create Dispute**.

  > **Note**: You can create a single dispute for multiple failures only if all the failures have the same plugin ID.

  Depending on the attestation, one of the following pages appears:

  - If the failure is associated with an asset that already has attestations with disputes, the **Clone disputes** page appears. You can either clone a dispute or create a new dispute.

    To clone a dispute:

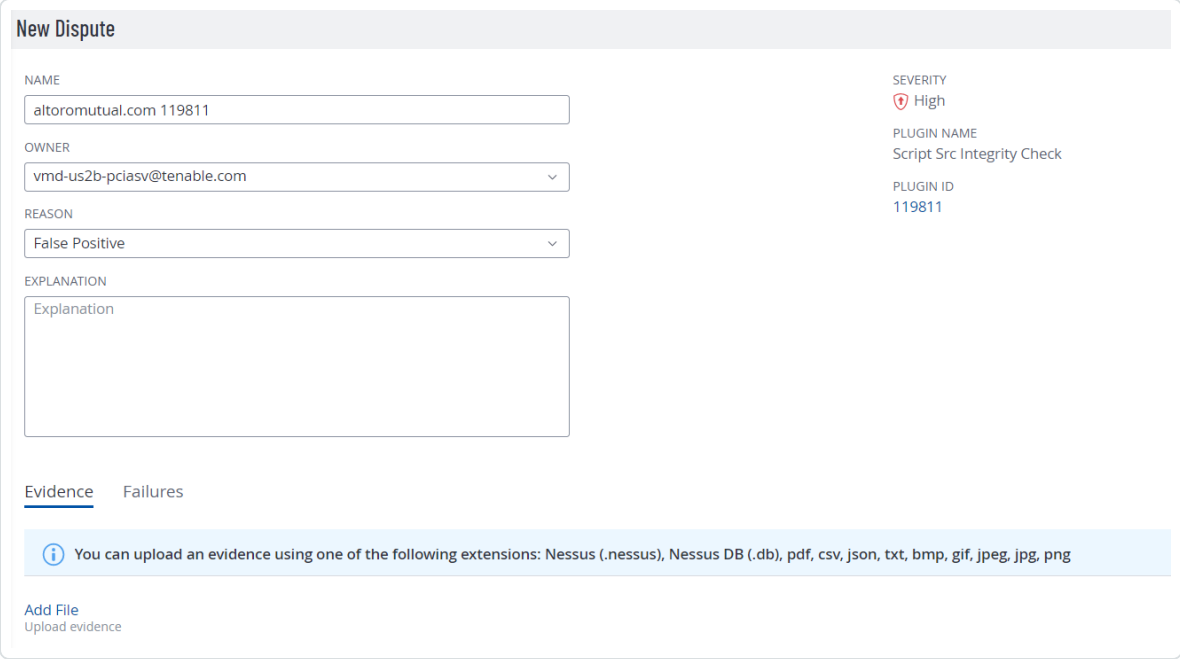
    a. Click the attestation from which you want to clone the dispute.

       The **Disputes to Clone** plane appears and displays the disputes that will be cloned from the attestation.

    b. Click **Clone**.

       A **Disputes successfully cloned** message appears and Tenable PCI ASV clones the dispute into the attestation.

- If there are no attestations to clone for a failure, the **New Dispute** page appears.



6. To create a new dispute, follow these steps on the **New Dispute** page:

   a. In the **Name** box, type a name for the dispute.

   > **Note**: By default, a concatenation of the IP address and plugin ID associated with the failure appears in the **Name** box.

   b. (Optional) To assign the dispute to a different user, in the **Owner** drop-down box, select the user you to whom you want to assign the dispute.

   c. In the **Reason** drop-down box, select the reason for the dispute. For details on each reason, see Dispute Reasons.

   d. In the **Explanation** text box, type an explanation for the dispute.

   > **Note:** You can click the plugin ID to get more information about the failure and use the information in your explanation.

   e. (Optional) To add an external file as evidence to support your dispute, do the following:

- In the **Evidence** section, click **Add File**.

  An explorer window appears.

- Select the file you want to add to your dispute.

> **Note:** Tenable PCI ASV supports the following file types for evidence attachments:
>
> - .bmp
> - .csv
> - .db
> - .gif
> - .jpeg
> - .jpg
> - .json
> - .nessus
> - .pdf
> - .png
> - .txt
>
> When you upload a file as evidence, Tenable PCI ASV automatically saves the uploaded file to the dispute before you click **Save** or **Cancel**.

f. (Optional) To add more files to the dispute, repeat the previous step.

> **Note**: You can add as many files as you want to a dispute as long as the total file size does not exceed 10 GB.

g. Click **Save**.

   Tenable PCI ASV saves your dispute to the attestation.

   A **Dispute Successfully Submitted** notification momentarily appears.

   Your dispute appears in the **Disputes** tab.

What to do next:

- (Optional) To change details of the dispute, edit the dispute.
- (Optional) To remove the dispute from your attestation, delete the dispute.

Edit a Dispute

Required User Role: Administrator and Custom Role

Note: You cannot edit a dispute after you submit the attestation for ASV review.

To edit a dispute:

1. Access the Tenable PCI ASV Workbench.
2. Click the **In Remediation** tab.

   A table of your attestation requests appears.
3. Click the attestation that has a dispute you want to edit.

   The **Attestation Details** page appears.
4. Click the **Disputes** tab.

   A table of your disputes appears.
5. Click the dispute you want to edit.

   The **Edit Dispute** page appears.
6. Configure the options you want to change. For information about the options, see Create a Dispute.
7. Click **Save**.

   Tenable PCI ASV saves your edits to the dispute.

Clone a Dispute to an Attestation

Required User Role: Administrator and Custom Role

You can clone a dispute from a previously submitted attestation for use in a new attestation.

Note: When you clone a dispute from an attestation, any other disputes attached to the same attestation are deleted.

1. Access the Tenable PCI ASV Workbench.
2. Click the **In Remediation** tab.

   A table of your attestation requests appears.
3. Click the attestation that has a dispute you want to clone into a previously submitted attestation.

   The **Attestation Detail** page appears.
4. In the upper-right corner, click **Clone Disputes**.

   The **Clone Disputes** page appears.

   Note: Only attestations that you previously submitted for ASV validation appear in the table.
5. Click the row that contains the attestation disputes you want to clone.

   The **Disputes to Clone** plane appears and displays the disputes that will be cloned from the attestation.
6. Click **Clone**.

   A **Disputes successfully cloned** message appears and Tenable PCI ASV clones the dispute.

Delete a Dispute

Required User Role: Administrator and Custom Role

Note: You cannot delete a dispute after you submit the attestation associated to the dispute for ASV review.

To delete a dispute:

1. Access the Tenable PCI ASV Workbench.
2. Click the **In Remediation** tab.

   A table of your attestation requests appears.
3. Click the attestation that includes a dispute you want to delete.

   The **Attestation Details** page appears.
4. Click the **Disputes** tab.

   A table of your disputes appears.
5. Do one of the following:
   - To delete one dispute:
     a. Roll over the row for the dispute you want to delete.

        The 🗑 button appears next to the last modified date.

     b. Click the 🗑 button.

        A confirmation window appears, prompting you to confirm you want to delete the dispute.
   - To delete multiple disputes:
     a. Select the check box next to each dispute you want to delete.

     b. In the lower-right corner, click **Delete**.

        A confirmation window appears, prompting you to confirm you want to delete the dispute.

6. Click **Delete**.

   Tenable PCI ASV deletes the dispute.

Dispute Reasons

Before you submit your Tenable PCI ASV attestation for review, you may want to dispute detected failures in the Tenable PCI ASV scan. When you dispute a failure, you must select an appropriate reason and provide an explanation.

When filing a Tenable PCI ASV dispute, you can select one of the following reasons:

1. False Positive
2. Compensating Controls
3. Exception

False Positive

It's possible that after patching or fixing all reported vulnerabilities, as defined by the PCI DSS compliance standards, you have a failure in your scan report that doesn't apply to the host. False positives can occur due to rapid changes in vendor-specific updates or backported patches that aren't easily detected by banner checks.

For example, a scan may report that a critical patch is missing from a host; however, the patch is actually installed. If a false positive occurs, you can provide proof of the false positive by uploading a screen capture, configuration file, or other supporting data as evidence. Evidence must be accompanied by a description of when, where, and how the evidence was obtained.

Compensating Controls

Compensating controls may be considered for most PCI DSS requirements if, due to legitimate technical or documented business constraints, you cannot meet a requirement as stated. You can, however, sufficiently mitigate the risk associated with the requirement through implementation of other, or compensating, controls.

Compensating controls must satisfy the following criteria:

- They must meet the intent and rigor of the original PCI DSS requirement.
- They must provide a similar level of defense as the original PCI DSS requirement, such that the compensating control sufficiently offsets the risk that the original PCI DSS requirement was designed to defend against.

> **Tip:** You can check the Guidance Column for the intent of each PCI DSS requirement in the Payment Card Industry (PCI) Data Security Standard specification document.

- They must go "above and beyond" other PCI DSS requirements. Simply being compliant with other PCI DSS requirements does not constitute a compensating control.

For example, if you are unable to render cardholder data unreadable per Requirement 3.4 (for example, by encryption), a compensating control could consist of a device or combination of devices, applications, and controls that address all of the following:

- internal network segmentation
- IP address or MAC address filtering
- one-time passwords

> **Note:** The Payment Card Industry (PCI) Data Security Standard specification document provides a compensating controls worksheet in Appendix C.

Exception

A dispute can still be filed for a failure that is not a false positive or if compensating controls are not in place. An exception must be supported by evidence that the failure does not pose a risk to the Cardholder Data Environment (CDE). Common exceptions include disputed CVSS base scores or PCI ASV scans that cannot be completed due to scan interference.

Export Attestations

Required User Role: Administrator and Custom Role

You can export your attestations at any point during the attestation process.

To export your attestations:

1. Access the Tenable PCI ASV Workbench.
2. Do one of the following:
   - Click the **In Remediation** tab.
   - Click the **In ASV Review** tab.
   - Click the **Attestations** tab.

   A table of your attestations appears.
3. In the row for the attestation for which you want to download a report, click the ⋮ button.

   A menu appears.
4. Click [→ **Export**.

   The **Export** plane appears.
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 PCI ASV 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 PCI ASV does not include empty fields in the JSON file.

7. (Optional) In the **Configurations** section, deselect any fields you do not want to appear in the export file.
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 PCI ASV 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 PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

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

Submit an Attestation for ASV Review

Required User Role: Administrator and Custom Role

Before you begin:

- Create an attestation for the scan you want to submit for ASV review.
- If your attestation includes assets that are not in scope for the Tenable PCI ASV review, mark each irrelevant asset as out of scope.
- If your attestation includes undisputed failures, create a dispute for each failure.

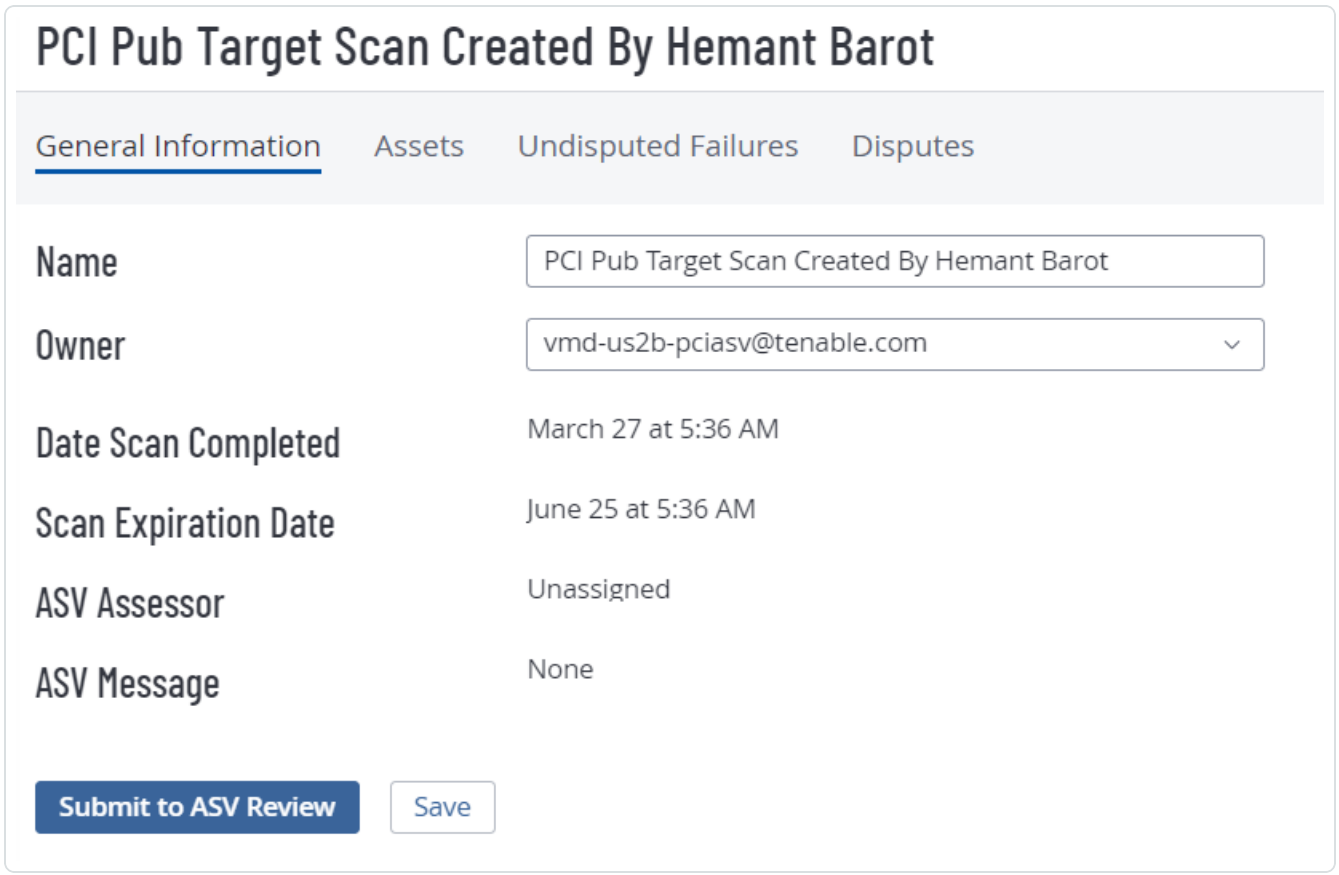
Caution: Assessors can only review submitted attestations while your subscription is active. This means that if your subscription expires during the normal review period, Tenable cannot complete your report. You must renew your Tenable PCI ASV subscription, at which time Tenable can continue reviewing your attestation.

To submit an attestation for ASV review:

1. Access the Tenable PCI ASV Workbench.
2. Click the **In Remediation** tab.

   A table of your attestation requests appears.
3. Click the attestation you want to submit for ASV review.

   The **Attestation Details** page appears.



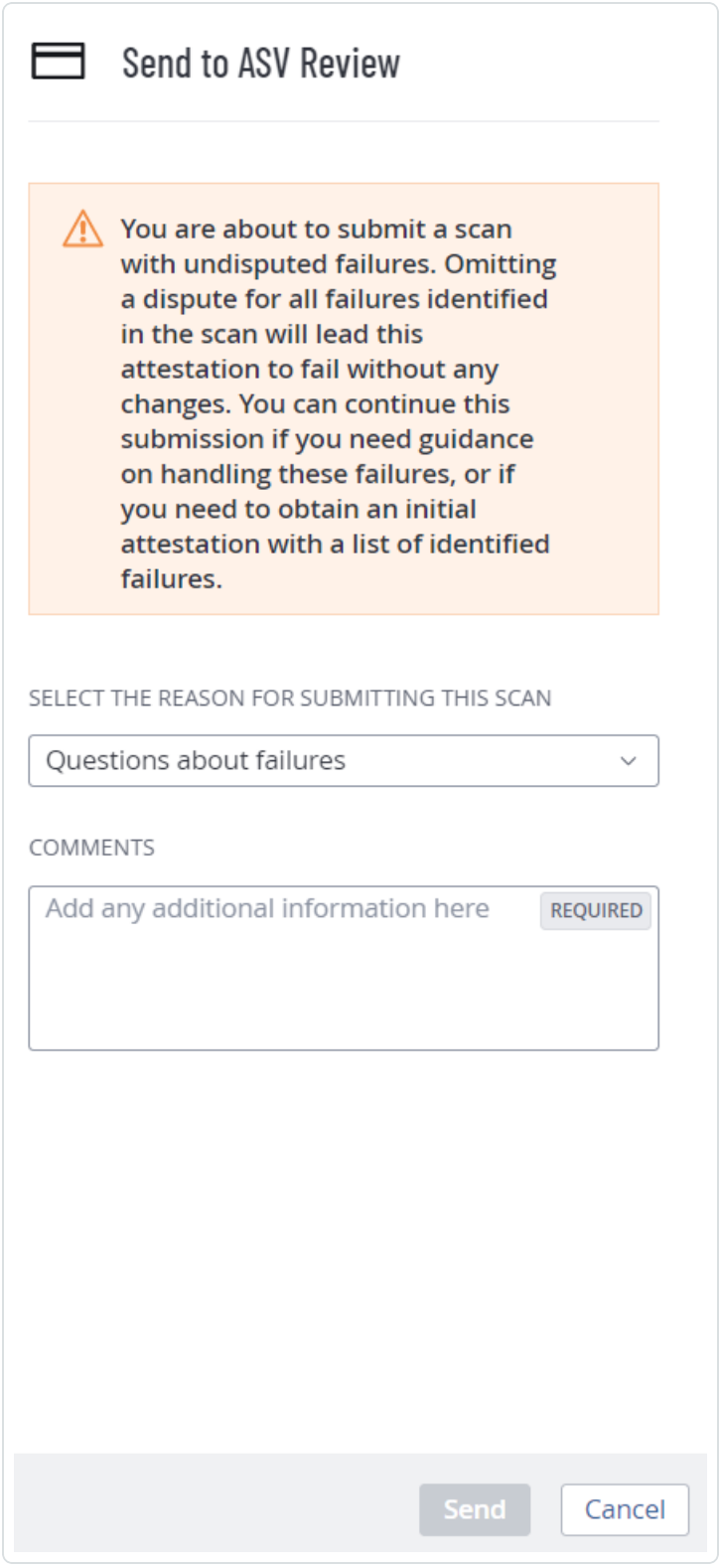
4. (Optional) To update the name of the attestation, in the **General Information** tab, in the **Name** box, type a new name.
5. (Optional) To update the owner of the attestation, in the **General Information** tab, in the **Owner** drop-down box, select the owner you want to assign to the attestation.
6. Do one of the following:
   - Fix any undisputed failures before submitting the attestation:
     a. On the **Undisputed Failures** tab, create a dispute for each failure.
     b. Click **Submit to ASV Review**.
   - Submit the attestation with known failures.

     Note: You may want to submit an attestation with undisputed failures if you need guidance on handling these failures, or if you need to obtain an initial attestation with a list of identified failures.

Caution: If you submit an attestation that has undisputed failures to ASV for review, the ASV reviewer must fail the attestation.

a. Click **Submit to ASV Review**.

   The **Submit for ASV Review** panel appears.


Send to ASV Review
You are about to submit a scan with undisputed failures. Omitting a dispute for all failures identified in the scan will lead this attestation to fail without any changes. You can continue this submission if you need guidance on handling these failures, or if you need to obtain an initial attestation with a list of identified failures.
SELECT THE REASON FOR SUBMITTING THIS SCAN
Questions about failures
COMMENTS
Add any additional information here
REQUIRED
Send
Cancel

b. In the **Select the reason for submitting this scan** drop-down, select the reason you want to submit the scan with known failures.

c. In the **Comments** box, provide any additional information on why you want to submit the scan with known failures.

d. Click **Submit Scan**.

The **Attestation Detail** page appears.

7. On the **Attestation Detail** page, configure the attestation information:

   a. In the **Contact Name** box, type a contact for the attestation.

   b. In the **Email** box, type an email for the attestation contact.

   c. In the **Phone** box, type a phone number for the attestation contact.

   d. In the **Job Title** box, type a job title for the attestation contact.

   e. In the **Company** box, type the company where the attestation contact works.

   f. In the **Web URL** box, type the URL for the company's website.

   g. In the **Address Line 1** box, type the address of the company.

   h. (Optional) In the **Address Line 2** box, type any additional address information for the company, such as a suite number or floor number.

   i. In the **City** box, type the city where the company is located.

   j. In the **State / Province / Region** box, type the state, province, or region where the company is located.

   k. In the **Zip / Postal Code** box, type the zip code for the company's address.

   l. (Optional) To add the country where the company is located, in the **Country** box, type the country.

8. In the **Attestation Agreement** section, carefully read the terms of the attestation agreement.

9. Click **Attest**.

   An **Attestation Successfully Submitted for ASV Review** success notification appears, and Tenable PCI ASV adds the attestation to the **Attestations** tab.

After the ASV review completes the review, the attestation appears under the **In ASV Review** tab. If the attestation passed, the status is set to **Passed** and if the attestation failed, the status is set to **Failed** in the row.

> **Note**: Once your attestation moves to the **In ASV Review** or **Attestations** tab, the attestation is read-only. You cannot make additional changes to the attestation unless an ASV reviewer initiates an information request.

> **Tip**: After you create your first attestation request, the **New Attestation** screen automatically populates the above fields with your previously entered information in each subsequent attestation request.

What to do next:

- The ASV assessment team aims to provide a passed or failed attestation within 45 days of the submission date.

  ### What's the process?

  Attestations get assigned within 14 business days of submission (with the exception of holidays). Once a report is assigned, it may take an additional 14 business days for the attestation to be **In-Review**. Once an attestation is **In-Review**, an assessor is actively reviewing the disputes. The completion and generation of the final reports for an **In-Review** attestation depends upon the number of disputes in the report and the responsiveness of a scan customer during this phase. If any disputes are questionable, an information request is provided by the assessor within 48 business hours. Once a scan customer has sufficiently answered all information requests, the report can be finalized and ready for export within 24 business hours.

- If the ASV reviewer requests additional information about your disputed failures, respond to the request. For more information, see Respond to an ASV Review Information Request.
- Download any completed attestation reports from the **Attestations** tab.
- Tenable advises that you submit an ASV scan 30 days before any compliance deadlines to ensure there is enough time to complete the review process.

  You can submit as many scans as needed, but ensure that you can properly dispute any risks presented as PCI failures and provide enough time to respond to requests for additional

information from the ASV reviewer. For more information, see the Tenable blog Understanding PCI DSS Scanning Requirements.

Attestation Status

After a scan has been submitted for ASV review, the attestation status on the **In ASV Review** tab changes depending on the stage of review. The following table provides the list of statuses for an attestation:

Status	Description
Unassigned	Attestation is new and not yet assigned to an ASV reviewer.
Assigned	Attestation is assigned to an ASV reviewer.
Info Requested	The ASV reviewer has requested for additional information for the disputes.
Info Provided	A response is provided for the requested information.
In-Review	The ASV reviewer is reviewing the attestation. After review, all attestations move to the **Attestations** with the **Passed**, **Failed**, or **Closed** status.

Respond to an ASV Review Information Request

Required User Role: Administrator and Custom Role

If you have any disputed failures in your attestation request when you submit the attestation for ASV review, the ASV reviewer may ask for additional information.

You can respond to the reviewer directly in the dispute.

Before you begin:

- Submit your attestation for ASV review.

To respond to an information request:

1. Access the Tenable PCI ASV Workbench.
2. Click the **In ASV Review** tab.

   A table of your attestation requests appears.
3. Locate the attestation that has an ⚠ icon next to the **Owner**.
4. Click the attestation.

   The **Attestation Details** page appears.
5. Click the **Disputes** tab.

   A table of your disputes appears.
6. Click the dispute that has an ⚠ icon next to the reason.

   The dispute details page appears.
7. In the **Explanation** section, view the question or comment the ASV reviewer submitted.
8. Do one of the following:

   - To submit a text-based response to the ASV reviewer, in the **Explanation** section, in the text box, type your response.
   - To add a file as evidence to support your dispute:

a. In the **Evidence** section, click **Add File**.

   An explorer window appears.

b. Select the file you want to add to your dispute.

   Note: Tenable PCI ASV does not restrict the file types you add to a dispute. Additionally, when you upload a file as evidence, Tenable PCI ASV automatically saves the file to the dispute before you click **Save** or **Cancel**.

c. (Optional) To add more files to the dispute, repeat the previous step.

   Note: You can add as many files as you want to a dispute as long as the total file size does not exceed 10 GB.

9. Click **Save**.

   A **Dispute Successfully Submitted** notification momentarily appears.

   Tenable PCI ASV submits your response to the ASV reviewer.

   Note: You cannot edit or delete a response after you submit it to the ASV reviewer.

10. Repeat steps 6-9 for each dispute in the **Disputes** tab that has an ⓘ icon next to the reason.

Download Completed Attestation Reports

Required User Role: Administrator and Custom Role

On the Attestation tab, you can download your completed attestation reports.

Tip: An attestation is completed when it receives a status of **Passed**, **Failed**, or **Closed**.

Note: Tenable stores completed reports for 3 years, at which time they are removed from the system completely and cannot be recovered. Tenable recommends downloading any important finalized reports to private storage to avoid losing the information permanently.

To download your completed attestation reports:

1. Access the Tenable PCI ASV Workbench.
2. Click the **Attestations** tab.

   A table of your completed attestations appears.
3. In the row for the attestation for which you want to download a report, click the ⋮ button.

   A menu appears.
4. Click one of the following options:
   - ↓ **ASV Scan Report Summary** — Download the ASV Scan Report Summary as a PDF export file.
   - ↓ **ASV Scan Report Vulnerability Details** — Download the ASV Scan Report for Vulnerability Details as a PDF export file.
   - ↓ **Feedback** — Download a feedback form for the attestation in PDF format.
   - [→ **Export** — Export the attestation.

   Tenable PCI ASV downloads the file to your computer.

Tenable PCI ASV Settings

The **Settings** page allows you to view and manage all of your Tenable PCI ASV settings configurations.

To access the Settings page:

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

   The left navigation plane appears.

2. Click **Settings**.

   The **Settings** page appears.

Click on a tile to navigate to specific settings. For more information, see the following topics in the *Cloud Platform User Guide*:

Topic	Description
General	View and manage your general settings.
My Account	View and manage your account settings.
SAML	Manage SAML credentials and self service.
License	View licensing details and statistics.
Access Control	View and manage which hosts users can scan and can view in scan results and aggregated data.
Activity Logs	View activity logs for your organization's account.
Exports	View export activity and manage scheduled exports.
Tags	View and manage tags and tagging rules.
Sensors	Manage sensors and sensor groups.
Credentials	View and manage scanning credentials.
Exclusions	View and manage scanning restrictions.
Connectors	Enable Cloud Connectors.

General Settings

Required User Role: Administrator

On the **General** page, you can configure general settings for your Tenable PCI ASV instance.

To access general settings:

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** page appears. By default, the **Severity** tab is active.

Here, you can configure the following options:

Severity

By default, Tenable PCI ASV uses CVSSv3 scores to calculate severity for individual vulnerability instances based on the move to the PCI-DSS 4.0 specification.

Service-Level Agreement (SLA)

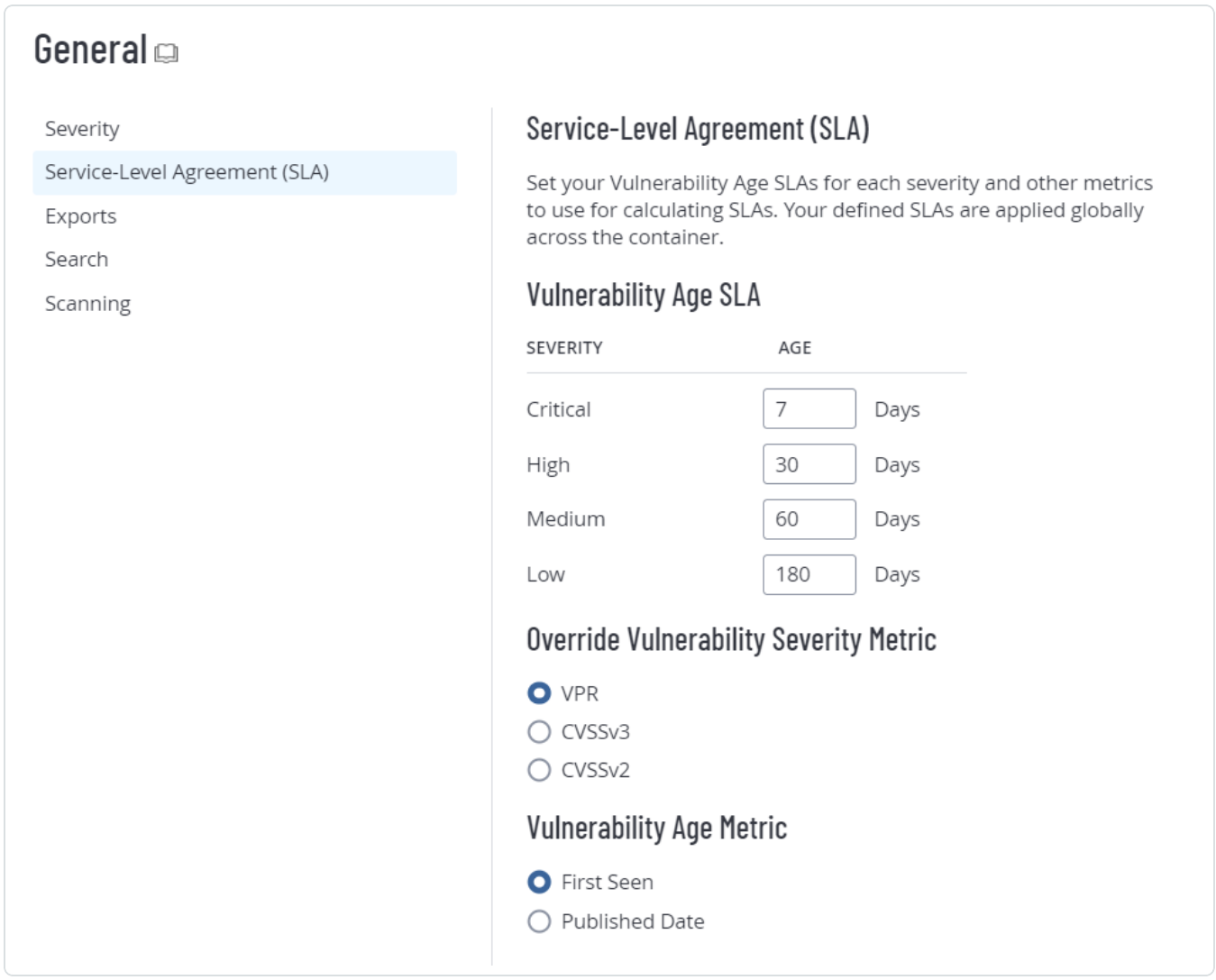
You can configure Service Level Agreement (SLA) settings to modify how Tenable calculates your SLA data.

You can view this data in the **SLA Progress: Vulnerability Age** widget on the **Vulnerability Management Overview** dashboard. For more information, see Vulnerability Management Overview.

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 PCI ASV saves your SLA settings.

Language

On the **General** page, you can change the plugin language in your Tenable PCI ASV 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 PCI ASV updates the plugin language for your container.

Exports

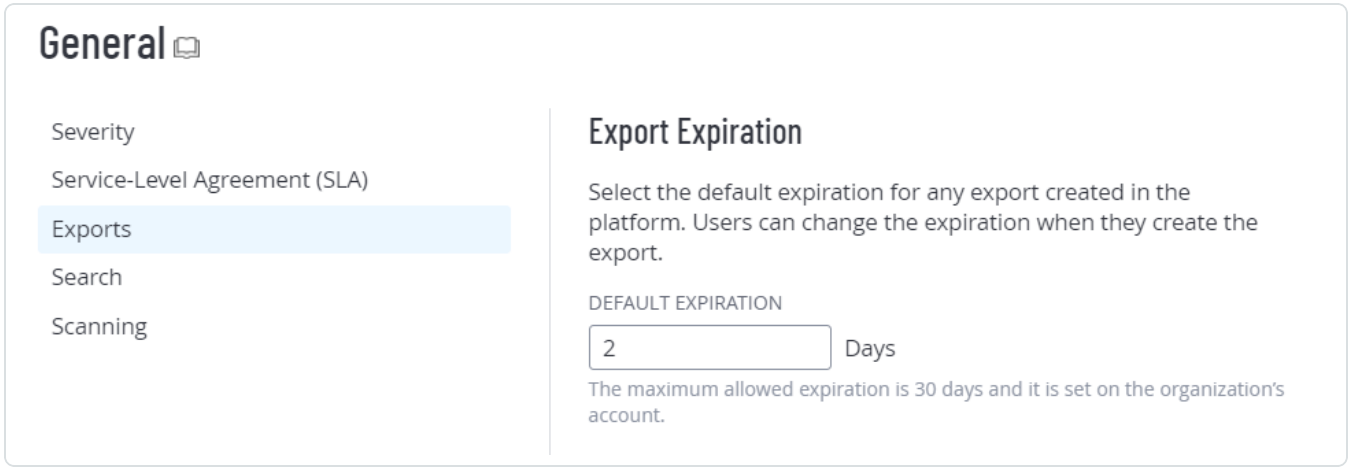
To configure your default export expiration:

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 PCI ASV allows before your export files expire.

By default, any exports you create in Tenable PCI ASV have an expiration date of 30 days. If you want to decrease the number of days that Tenable PCI ASV 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 PCI ASV to allow before your exports expire.

   Note: Tenable PCI ASV allows you to set a maximum of 30 calender days for export expiration.

> **Note**: You must type the number of days as an integer between 1 and 30.

3. Click **Save**.

   Tenable PCI ASV saves your settings and updates the number of allowable days before your exports expire.

Search

Enabling plugin output data retention allows Tenable PCI ASV to store your plugin output data each time you launch a scan. You can then filter your vulnerability findings by plugin output. For more information, see Findings Filters.

> **Note:** Tenable automatically disables this setting if it is unused for 35 days. Re-enable the setting to conduct a search on plugin output for all scans from that point onward. Only use this setting if you need to perform regular searches within the **Explore** user interface.

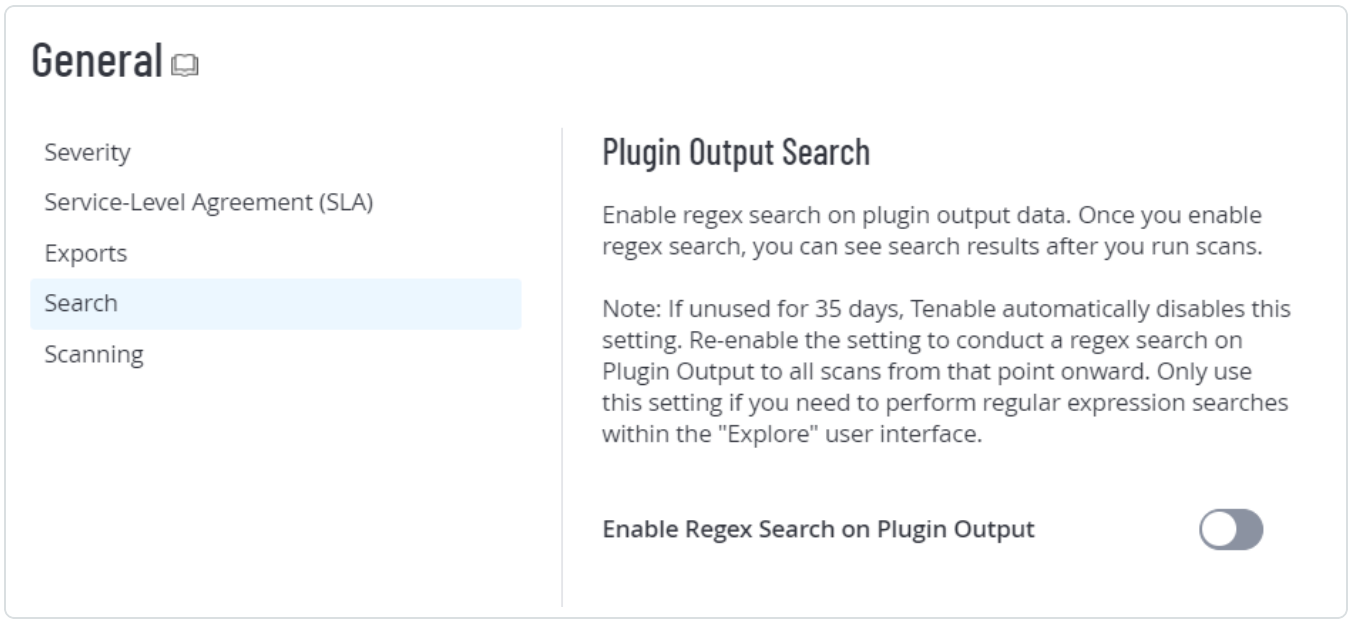
Once you have enabled plugin output data retention, you must launch a scan so that Tenable PCI ASV can identify and store your plugin output data.

> **Caution**: You cannot disable plugin output data retention once you have enabled it.

To enable plugin output data retention:

1. In the left navigation plane, click the **Search** tab.

   The search options appear.



2. Click the **Enable Regex Search on Plugin Output** toggle.
3. Click **Save**.

   Tenable PCI ASV enables plugin output data retention on your account.

What to do next:

- Launch a scan for your host assets.

Scanning

In the **Scanning** section, you can change how Tenable PCI ASV handles info-level plugins with two settings.

Process High-Traffic Info Plugins

Caution: Tenable plans to deprecate this setting and replace it with **Relocate Open Port Findings**.

Disable this setting to stop Tenable PCI ASV from generating an individual finding for every open port on every scanned host. Disabling this setting reduces scan time and scan result export time, while enabling it may significantly increase these times. For more information, see Platform Performance Improvement FAQ - Info Plugins.

The following plugin IDs are impacted

- 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)
- 10736 - DCE Services Enumeration
- 99265 - macOS Remote Listeners Enumeration
- 10335 - Nessus TCP scanner
- 14274 - Nessus SNMP Scanner
- 34277 - Nessus UDP Scanner

Tip: For more information about these plugins, see the Tenable Plugins site.

Relocate Open Port Findings

Enable this setting to change how Tenable PCI ASV handles open port findings by displaying them on the **Asset Details** page instead of the **Findings** workbench. To learn about the impact this change may have on your organization, see Tenable Vulnerability Management New Data Format: Relocate Open Port Findings.

Note: If you use third-party integrations such as ServiceNow, Jira, or Splunk with Tenable Vulnerability Management, your open ports data is now sent as an asset property.

This setting does the following:

- *Moves* open port findings from the **Findings** workbench to the **Asset Details** page. The **Asset Details** page appears when you click a host asset on the **Assets** workbench.

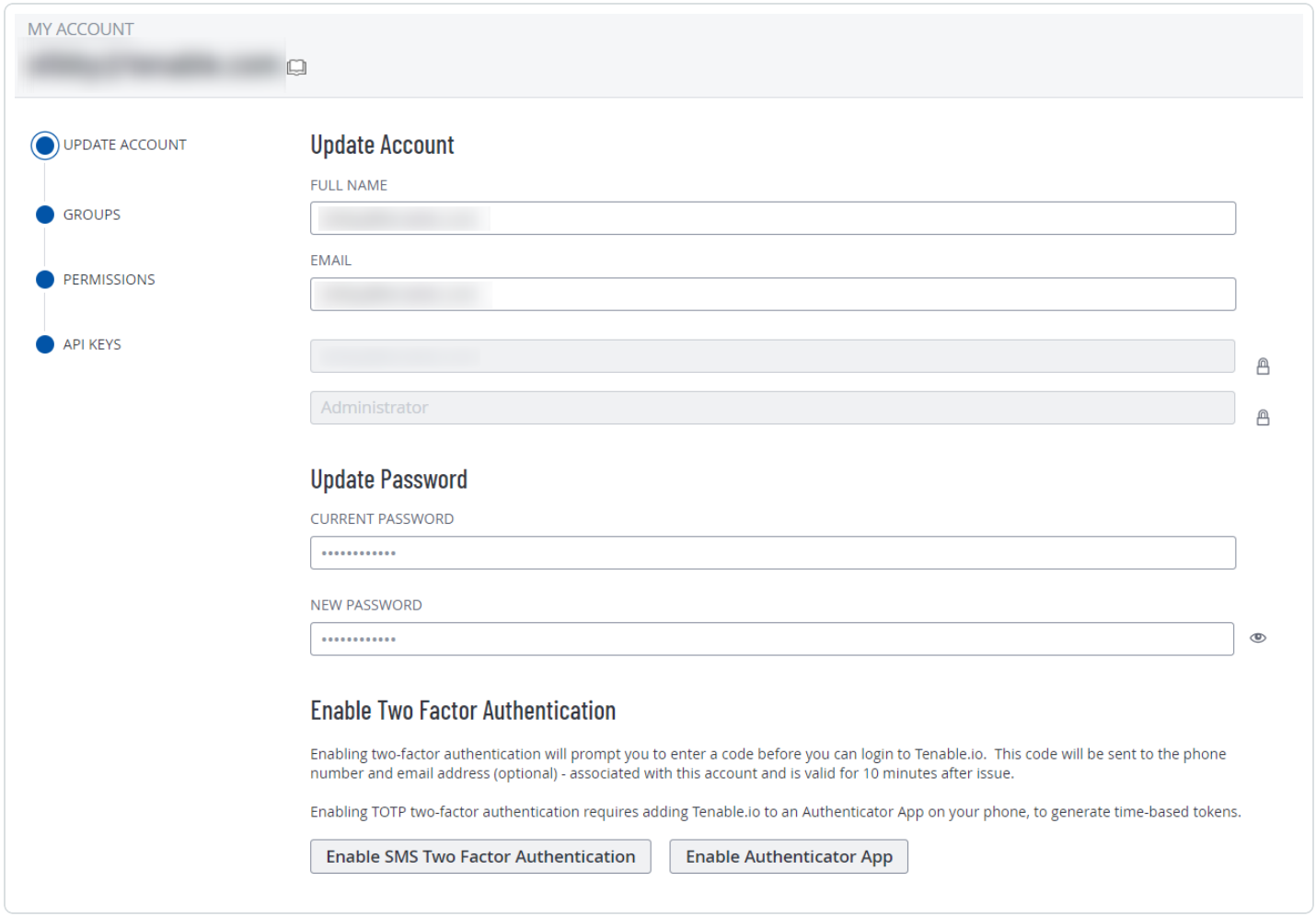
  Open port findings from the following high-traffic plugins move to the Asset Details page

  - 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)
    - 10736 - DCE Services Enumeration
    - 99265 - macOS Remote Listeners Enumeration
    - 10335 - Nessus TCP scanner
    - 14274 - Nessus SNMP Scanner
    - 34277 - Nessus UDP Scanner
- Enables the **Open Ports** tab on the **Asset Details** page, which now contains open port findings.
- Enables the **Open Ports** filter on the **Assets** workbench, where you can search for open ports on host assets.
- Enables the **Open Ports** rule on the **Tags** page, so you can tag open ports.
- Adds an Open Ports field to the **Assets** workbench, so you can export open port data.
- (Optional) Adds open port findings to the bulk asset export API. To learn more, see the API changelog in the *Tenable Developer Portal*. To request this feature, contact your Tenable Customer Success Manager.

My Account

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



You can navigate to the My Account page via one of the following methods:

- To access the **My Account** page from the **Settings** page:

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

  The left navigation plane appears.

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

  The **Settings** page appears.

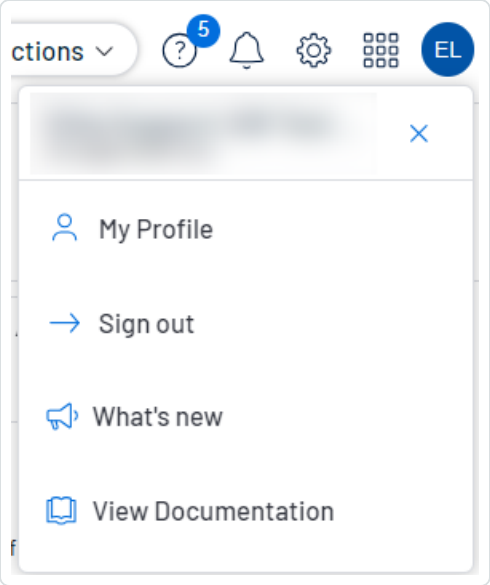
c. Click the **My Account** tile.

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

- To access the **My Account** page from the top navigation menu of any page:

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

     The user account menu appears.



  b. 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. 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**.

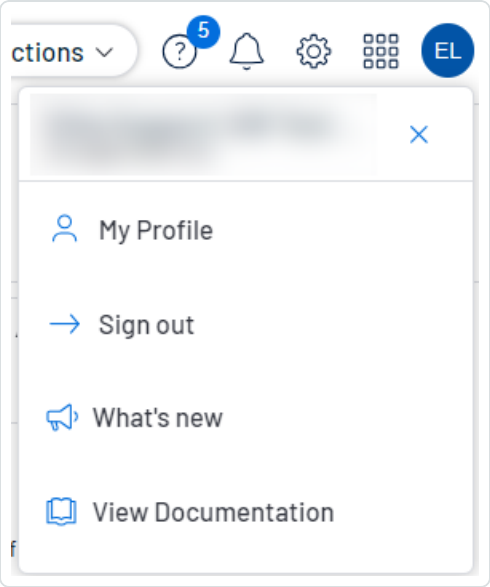
           The **Settings** page appears.

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

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

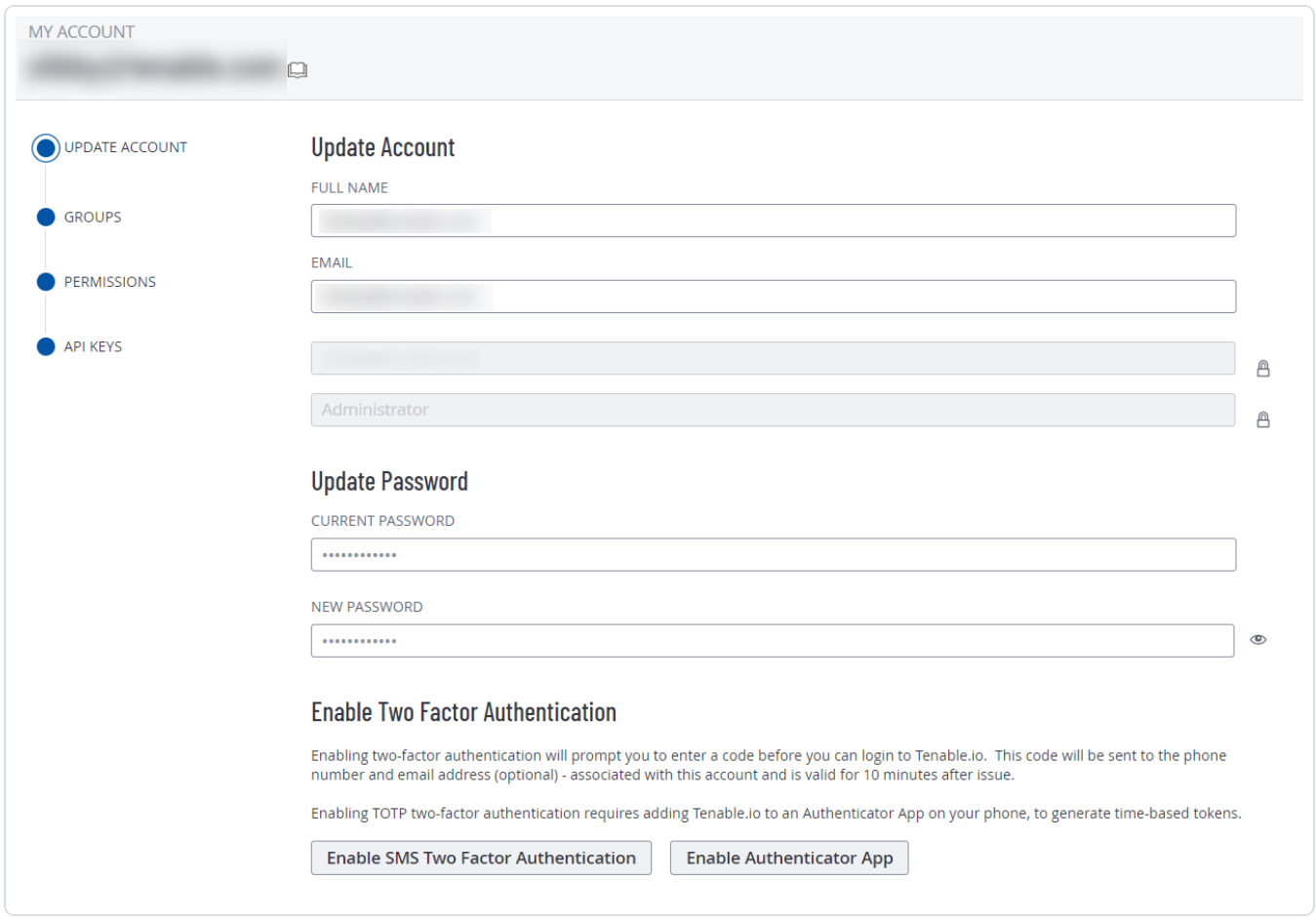
    - In the upper-right corner, click the blue user circle.

      The user account menu appears.



a. Click **My Profile**.

   The **My Account** page appears.



2. 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 PCI ASV.

Note: User accounts expire according to when the Tenable PCI ASV 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. 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**.

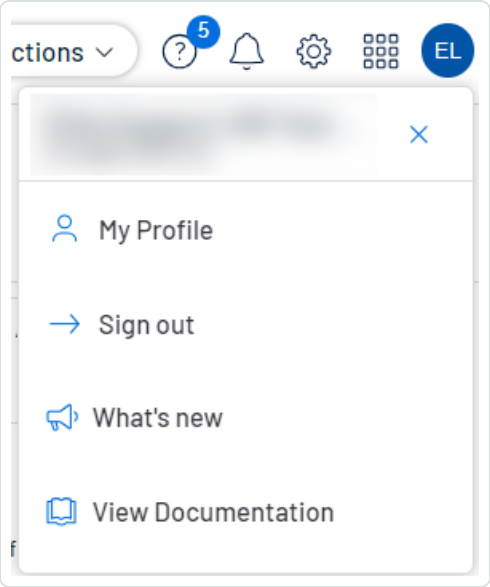
        The **Settings** page appears.

     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. (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 PCI ASV instance.

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

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

4. Click **Save**.

Tenable PCI ASV 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. 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**.

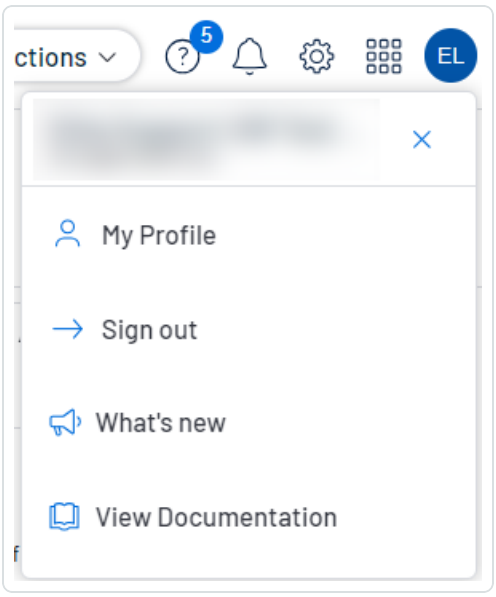
           The **Settings** page appears.

        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 **Current Password** box, type your current password.
3. In the **New Password** box, type a new password. See Tenable PCI ASV Password Requirements for more information.
4. Click the **Save** button.

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

5. Log in to Tenable PCI ASV using your new password.

Configure Two-Factor Authentication

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 PCI ASV.

To add or modify two-factor authentication:

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**.

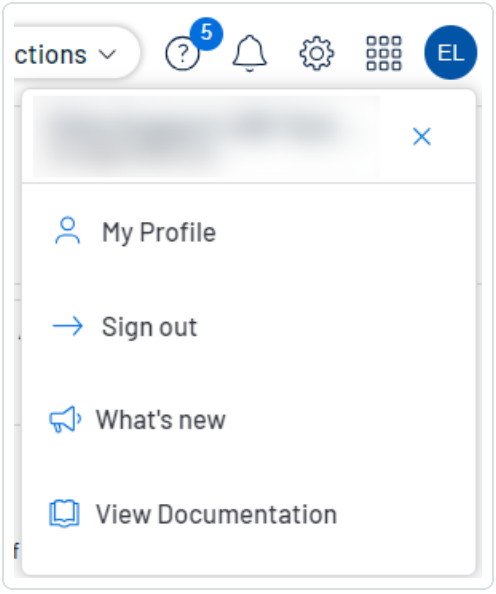
        The **Settings** page appears.

     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 **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 PCI ASV password.

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

     > **Note:** By default, Tenable PCI ASV 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 PCI ASV 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 PCI ASV applies your settings to your Tenable PCI ASV account.

g. (Optional) To configure whether Tenable PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV applies your settings to your Tenable PCI ASV 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**.

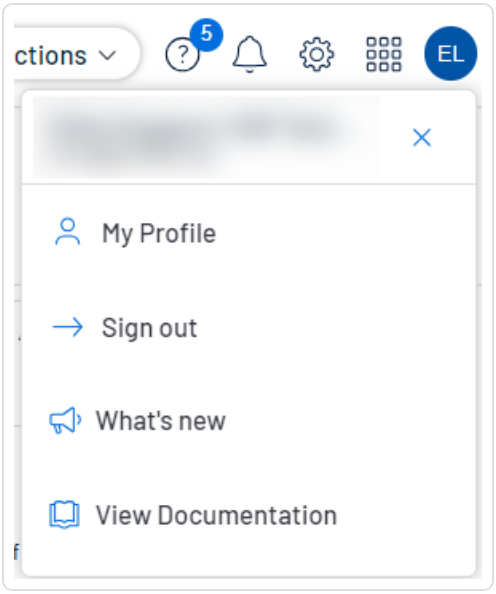
           The **Settings** page appears.

        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 PCI ASV 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 PCI ASV products for which your organization is licensed.

Note: Tenable PCI ASV API access and secret keys are required to authenticate with the Tenable PCI ASV 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 PCI ASV 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. 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**.

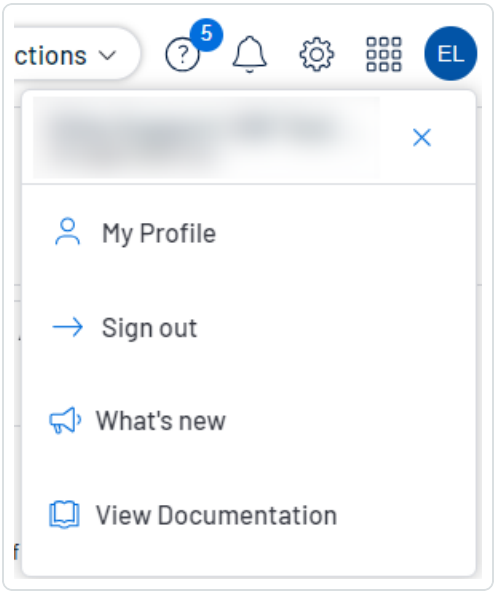
   The **Settings** page appears.

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. 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 PCI ASV 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 PCI ASV.

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 PCI ASV locks you out if you attempt to log in and fail 5 consecutive times.

Note: If you no longer no longer have access to the email address specified in your account, an administrator for your Tenable PCI ASV instance can reset your password instead.

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 PCI ASV login page, click the **Forgot your password?** link.

   The password reset page appears.

2. In the **Username** box, enter your Tenable PCI ASV username.

3. In the CAPTCHA box, type your answer to the question.

4. Click **Send**.

   Tenable PCI ASV 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.

SAML

You can configure Tenable PCI ASV 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 PCI ASV. Once you enable SAML for a user, they can log in to Tenable PCI ASV directly through their identity provider, which automatically signs them in and redirects them to the Tenable PCI ASV 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 PCI ASV 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 PCI ASV.

Note: Tenable PCI ASV 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 the **Sign in via SSO** link on the Tenable PCI ASV login page.

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 PCI ASV 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 PCI ASV has login data for the SAML identity provider.
Last	The date and time on which a user on your instance last attempted to log in

Attempted Login	via the SAML configuration. **Note**: The **Last Attempted Login** column shows a value only if Tenable PCI ASV 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 PCI ASV 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 PCI ASV.

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 PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV login page.

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 PCI ASV. This includes the following high-level steps:

- Follow the steps described in your IdP's documentation to set up a SAML application for Tenable PCI ASV on your IdP account. Your IdP requires an entity ID and a reply URL for Tenable PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV 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.
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**.

6. Click **Save**.

   Tenable PCI ASV saves your SAML configuration.

What to do next:

- Download the metadata.xml from Tenable PCI ASV using the **Download SP Metadata** option in the SAML Configurations table.
- Upload this file to the SAML application you created for Tenable PCI ASV 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.

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 PCI ASV 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 **Enable** setting is set to **Enabled**. In the upper-right corner, click the toggle to disable SAML configuration.
Type	**Manual Entry** , **Import XML**	Specifies the type of identity provider you are using. Tenable PCI ASV supports SAML 2.0 (e.g., Okta, OneLogin, etc.).
UUID	**Entry**, **Import XML**	A unique identifier for your identity provider that Tenable PCI ASV automatically generates when you create a new SAML configuration. This box is read-only.
URL	**Manual Entry** , **Import XML**	The login URL that Tenable PCI ASV generates when you create a configuration. This box is read-only.
Entity ID	**Manual Entry** , **Import XML**	A unique identifier that Tenable PCI ASV 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** ,	The time and date on which an administrator user last updated the configuration.

	Import XML	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.
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	**Manual**	To assign a role each time a user logs in,

at Each Login	**Entry**	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**.
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 PCI ASV 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 PCI ASV. 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 PCI ASV using their SAML credentials. Make sure all users on your instance have an alternative method to log in to Tenable PCI ASV 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 PCI ASV disables the SAML configuration. On the **SAML** page, the disabled configuration appears in light gray.

Enable a SAML Configuration

Required User Role: Administrator

You can enable a disabled a SAML configuration. For more information about SAML authentication in Tenable PCI ASV, 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 PCI ASV.

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 PCI ASV login page.

Before you Begin:

Configure your IdP to authenticate with Tenable PCI ASV. 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 PCI ASV 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 PCI ASV 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 PCI ASV.

Tenable PCI ASV creates automatically provisioned accounts with the following defaults:

- **Full name** — NameID
- **Username** — NameID
- **Email** — NameID
- **User role** — Basic

Tenable PCI ASV does not currently support any other claim types.

Before you Begin:

Configure your IdP to authenticate with Tenable PCI ASV. 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV, 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 PCI ASV 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.

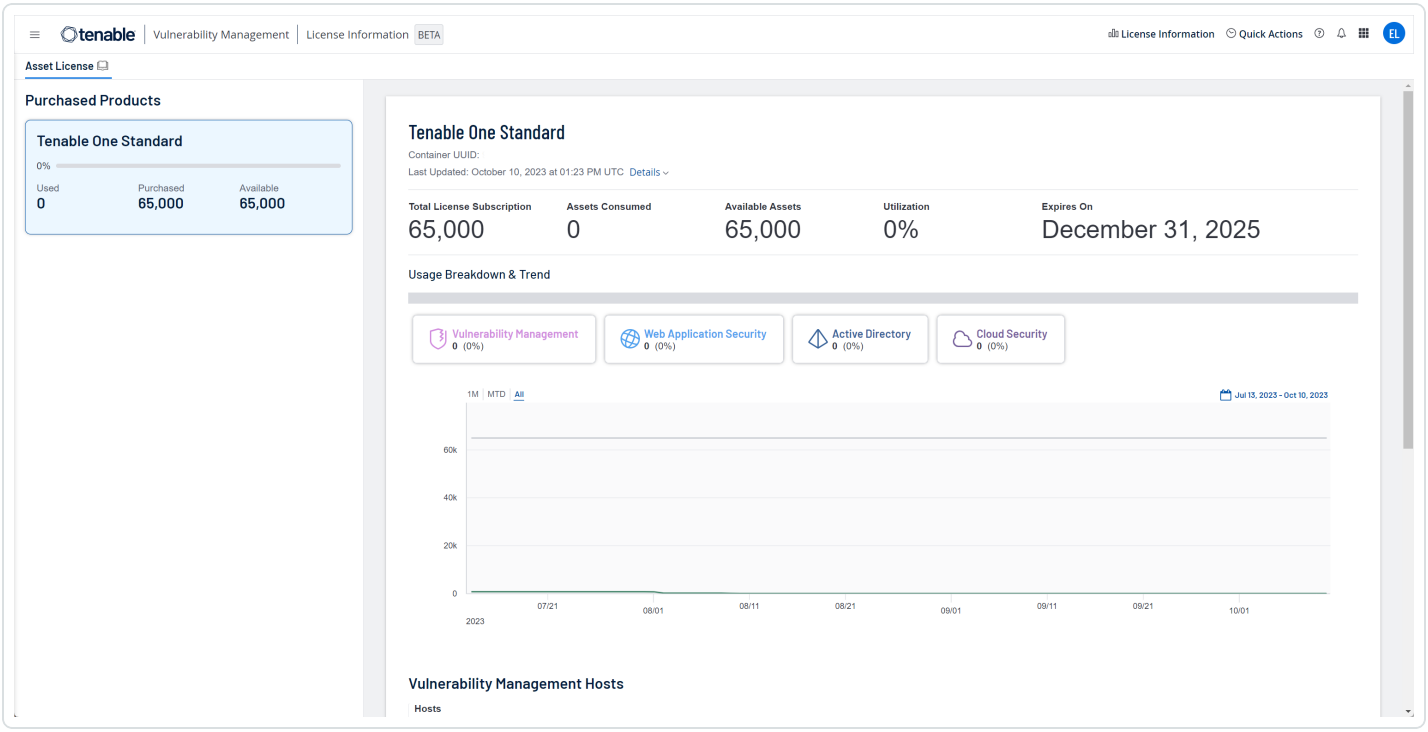
License Information

On the **License Information** page, you can view a complete breakdown of your Tenable products and their license usage. 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.

Tip: For more information about how Tenable counts and reclaims licenses, see Tenable Vulnerability Management Licenses and Tenable Web App Scanning Licenses. For information about license overages, see Tenable Cloud Overage Process.

View the License Information Page

To view the **License Information** page, in the top navigation bar, click **License Information**.



The **License Information** page shows license usage for all products in your current Tenable container and has the following sections.

Section	Description

Purchased Products	On the left, click a product tile to view details. If a product is still being evaluated or has expired, a label appears. • **Used** — The total number of licenses used or assessed from your product subscription. • **Purchased** — The number of licenses you have purchased for that product. • **Available** — The remaining available licenses from your subscription that have not yet been assessed.
Product Summary	At the top of the page, view a summary of the selected product: • **Product Name** — The name of the product. • **Container UUID** — The unique ID for the container. • **Last Updated** — The date and time the product was last updated. • **Site Name** — The cluster containing your installed products in Tenable's cloud. • **Region** — The geographic region in which your cluster is located. • **Plugin Set** — The version for the product's Nessus plugin set. • **Plugin Updated** — The date and time the Nessus plugin set was last updated. • **Total License Subscription** — The total number of licenses purchased as part of your product subscription. • **Assets Consumed** — The total number of licenses used or assessed from your product subscription. • **Available Assets** — The remaining available licenses from your subscription that have not yet been assessed. • **Utilization** — The percentage of your licenses that have been used. This value is calculated as the number of licenses consumed divided by the total license subscription.

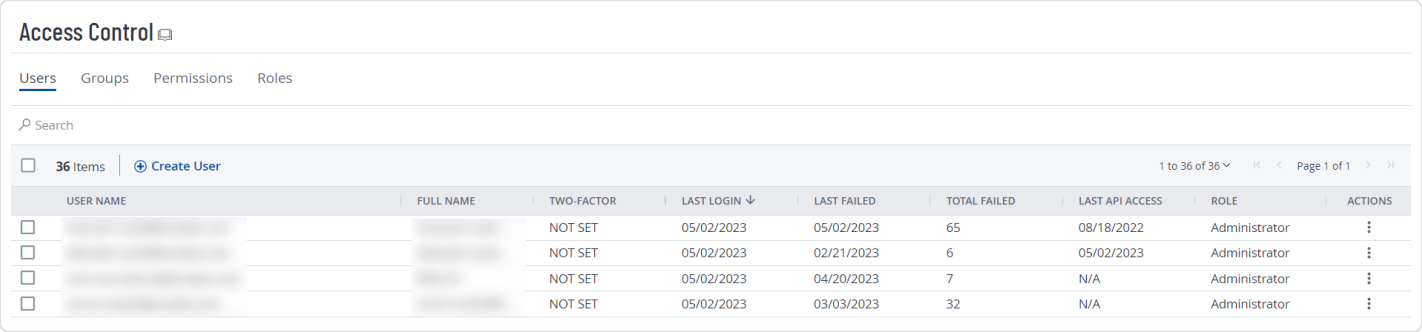
	• **Expires On** — The date your Tenable subscription expires.
Usage Breakdown & Trend	See visual breakdowns of your asset usage: • **Bar Chart** — (Tenable One only) View your total license use by Tenable One component in a bar chart. • **Usage Over Time** – View your license use over time in a line chart where the X-axis is the time period and the Y-axis is the number of assets used. With the filters at the top of the chart, switch between time periods on the left, or specify a custom date range on the right. **Tip**: (Tenable One-only) Click the tiles above the chart to select or deselect products.
Vulnerability Management Hosts	View the number of Tenable Vulnerability Management assets that count towards your license: • **Hosts** — The number of hosts that count towards your license.
Cloud Security Resources	View the number of cloud resources in your environment identified by Tenable Cloud Security. • **License Ratio** — (New version only) Any ratio applied to your **Compute**, **Serverless**, and **Container Repositories** resources. For example, if your organization has a ratio of 3, 10 Compute resources equals 30 *licensed* Tenable assets. To learn more about the ratio Tenable may apply to cloud resources, contact your Tenable representative. • **Compute** — (New version only) Cloud computing resources such as AWS EC2 instances or Azure virtual machines. Hover on this field to view your *billable* resources, or the total number of resources before any ratio is applied. • **Serverless** — (New version only) Cloud serverless resources such as AWS Lambda or Azure Functions. Hover on this field to view your *billable* resources, or the total number of resources before any ratio is applied.

	• **Container Repositories** — (New version only) Cloud container repositories scanned by Tenable Cloud Security. Hover on this field to view your *billable* resources, or the total number of resources before any ratio is applied. • **Container Images (Legacy Container Security)** — The number of packaged applications that count towards your license. Only used if you have Tenable Container Security. • **Billable** — (Legacy only) A subset of cloud assets that are considered licensed, typically cloud compute, storage, or network resources scanned in the past 90 days. • **Non-Billable** — (Legacy only) Infrastructure as code (IaC) assets scanned locally, in a repository or a pipeline. These are not considered licensed.
Web App Scanning FQDNs	View the number of Tenable Web App Scanning resources that count towards your license: • **FQDNs** — The number of fully qualified domain names that count towards your license. **Note**: Tenable Web App Scanning determines asset count by the number of *fully qualified domain names* (FQDNs) that are scanned for your user account. An asset does not count against your license limit until it has been successfully scanned for vulnerabilities.
Attack Surface Management Assets	View your Tenable Attack Surface Management resources: • **Observable Objects** — The number of assets discovered and added to your inventory in Tenable Attack Surface Management. **Note**: If you are a Tenable One Standard customer, these resources do not count towards your asset license.
Active Directory Users	View the number of Tenable Identity Exposure resources that count towards your license: • **Users** — The number of enabled active users.

Access Control

Required User Role: Administrator

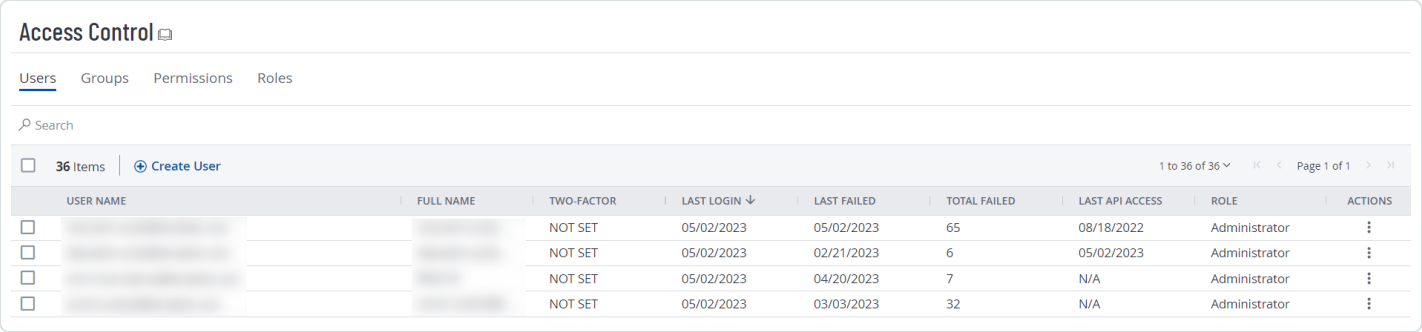
From the **Access Control** page, you can view and configure the list of users and groups on your account and the permissions assigned to them.



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 PCI ASV.



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 PCI ASV interface.
Last Failed	The date on which the user failed to log in to the Tenable PCI ASV 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).

On the **Users** page, you can perform the following actions:

- Create a User Account
- View Your List of Users
- Edit a User Account
- Change Another User's Password
- Assist a User with Their Account
- Generate Another User's API Keys
- Unlock a User Account
- Disable a User Account
- Enable a User Account
- Manage User Access Authorizations
- Audit User Activity
- Export Users
- Delete a User Account

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 PCI ASV 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 upper-left corner, click the ☰ button.

   The left navigation plane appears.

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

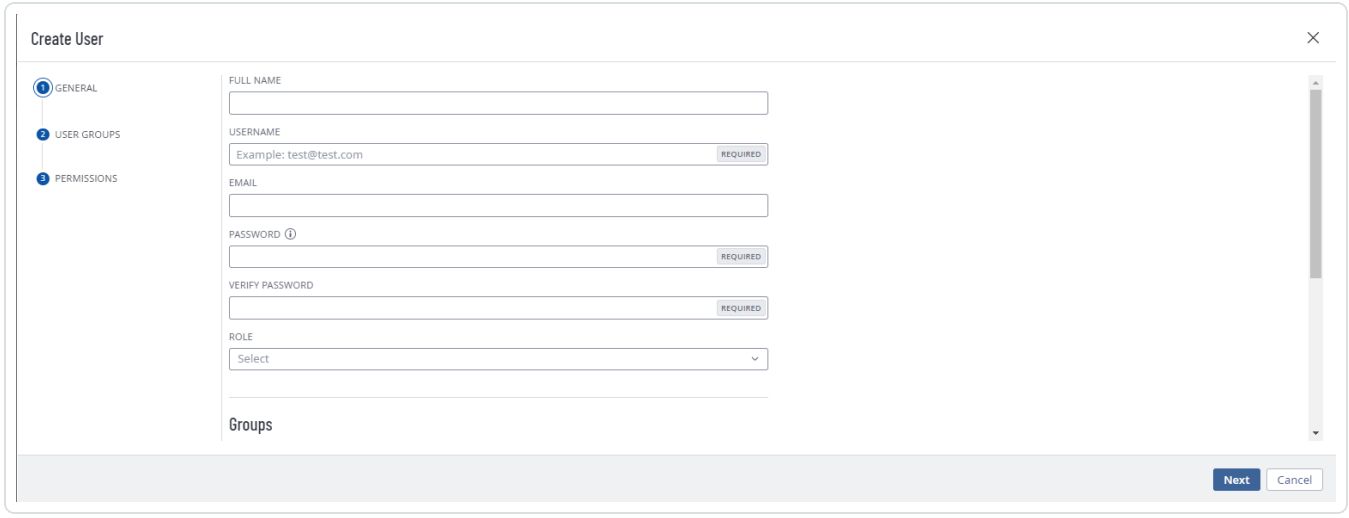
   The **Settings** page appears.

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 PCI ASV account.

4. Click the ⊕ **Create User** button.

   The **Create User** page appears.



5. 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 PCI ASV instance. **Note:** During initial setup, Tenable configures approved domains for your Tenable PCI ASV 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 PCI ASV instance. This email address overrides the email address set in the **Username** box. If you leave this option empty, Tenable PCI ASV 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 PCI ASV 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.

6. Click **Save**.

> **Note**: If you assign permissions to the user, the button appears as **Add & Save**.

Tenable PCI ASV 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 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 PCI ASV account.

4. In the users table, click the name of the user that you want to edit.

   The **Edit User** page appears.

5. 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 PCI ASV instance. This email address overrides the email address set in the **Username** box. If you leave this option empty, Tenable PCI ASV 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.

6. (Optional) Generate API keys for the user.
7. Click **Save**.

   Tenable PCI ASV 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 PCI ASV instance.

To view users and user data for your Tenable PCI ASV instance:

1. In the left navigation plane, 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 PCI ASV account.

3. Click the **Users** tab.

   The **Users** tab appears, containing a table of all Tenable PCI ASV user accounts on your Tenable PCI ASV 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 PCI ASV instance.

Column	Description
Name	The username for the account.
Last Login	The date on which the user last successfully logged in to the Tenable PCI ASV interface.
Last Failed	The date on which the user failed to log in to the Tenable PCI ASV 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).

Tenable PCI ASV Password Requirements

Tenable PCI ASV 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 PCI ASV passwords do not expire.

Account Lockout

By default, after 5 failed login attempts, Tenable PCI ASV 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 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 PCI ASV account.

4. In the users table, click the name of the user that you want to edit.

   The **Edit User** page appears.

5. In the **New Password** box, type a new password. See Password Requirements for more information.

6. Click **Save**.

   Tenable PCI ASV saves the new password for the user account.

Configure SSO/SAML Authentication in FedRAMP Containers

You can configure single sign-on (SSO)/Security Assertion Markup Language (SAML) authentication in FedRAMP containers so users can use provider-initiated SSO when logging in to Tenable PCI ASV. By default, SSO is not enabled.

Tip: These instructions are only for FedRAMP environments. If you are using a commercial Tenable PCI ASV environment, you can configure self-service SAML.

Note: Using SAML for your account does not disable traditional login.

Tenable PCI ASV supports:

- SAML 2.0-based authentication (for example, Okta or OneLogin)
- Shibboleth 1.3 authentication

Note: If you configure SSO authentication, Tenable PCI ASV does not log user actions to the audit log. This information may be available from the identity services provider you use.

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://fedcloud.tenable.com does not allow SSO. Additionally, all users must have an account configured in Tenable PCI ASV that matches their SSO login.

Step 1: Configure SSO on the Tenable PCI ASV Side

To configure SSO authentication:

1. Get the Identity Provider (IdP) .xml metadata file from your SAML provider.

   Note: Follow your SAML providers instructions to generate the IdP .xml file.

2. Contact your sales team and provide the IdP .xml file and a valid Tenable Vulnerability Management email address.

   Note: The estimated turnaround time for this request is approximately 15 days.

Note: If you are using ADFS or Microsoft Entra ID as your IdP, the metadata may contain two (or more) signing certificates. Instead, follow the instructions in Configure Tenable PCI ASV with ADFS SAML.

Step 2: Configure SSO on the SAML Side

Note: These terms may vary between SSO providers.

To manually configure SSO on the SAML side:

On the SAML side, configure the following parameters:

- **ACS/Single Sign On URL**: https://fedcloud.tenable.com/saml/login/<SAML_UUID>;
- **NameID Format**: Unspecified
- **NameID Value**: The username of the existing user account in Tenable PCI ASV. Typically this is the user's email address, but can be any unique identifier in *user@domain* format.
- **Audience**: A UUID-based value that matches the Tenable Container Security Entity ID. You can find this value on the **Settings** > **SAML** > **Edit** page within the Tenable PCI ASV user interface.

Note: The following are the most common reasons that SAML configuration fails:

- The IDP metadata was generated incorrectly
- The IDP metadata included the incorrect certificate
- The SSO login does not match the Tenable PCI ASV login

For more information on troubleshooting configuration failures, see the FedRAMP SAML/SSO Configuration Guidance Quick Reference Guide.

Assist a User with Their Account

Required User Role: Administrator

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 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 PCI ASV account.

4. 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.

5. 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 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 PCI ASV account.

4. In the users table, click the name of the user that you want to edit.

   The **Edit User** page appears.

5. 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.

6. 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.

7. (Optional) Click **Re-generate API Keys**.

8. 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 PCI ASV.

Unlock a User Account

Tenable PCI ASV 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

Disabling a user account prevents the user from logging in and prevents their scans from running. You can enable a disabled user account as described in Enable a User Account.

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 Reports.

To disable 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 PCI ASV account.

4. 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.

5. In the confirmation window, click **Disable**.

   A success message appears.

   Tenable PCI ASV 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 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 PCI ASV account.

4. 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.

5. In the confirmation window, click **Enable**.

   A success message appears.

   Tenable PCI ASV enables the selected user or users. In the users table, an enabled user appears in black.

Manage User Access Authorizations

Users can access Tenable PCI ASV using the following methods:

- Username and password login.
- Single sign-on (SSO). For more information, see SAML.
- Tenable PCI ASV 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 PCI ASV 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.

Audit User Activity

Required User Role: Administrator

In Tenable PCI ASV, the audit log records user events that take place in your organization's Tenable PCI ASV 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 audit log provides visibility into the actions that users in your organization take in Tenable PCI ASV, and can be helpful for identifying security issues and other potential problems.

To view the audit log for your organization's Tenable PCI ASV account:

- Use the **Audit Log** endpoint as documented in the Tenable Developer Portal.

Logged Events

Audit 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.

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 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 PCI ASV account.

4. Click the **Users** tab.

   The **Users** page appears. This page contains a table that lists all users for your Tenable PCI ASV instance.

5. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

6. 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.

7. In the **Name** box, type a name for the export file.
8. 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 PCI ASV 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.

9. (Optional) Deselect any fields you do not want to appear in the export file.
10. In the **Expiration** box, type the number of days before the export file expires.

    Note: Tenable PCI ASV allows you to set a maximum of 30 calender days for export expiration.

11. (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.

12. (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 PCI ASV sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

13. Click **Export**.

    Tenable PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

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

14. 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	Permanently deleted
Managed Credentials	No	Retained (**Created By** value displays as **null**)

Object Type	Deleted	Notes
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
Sensors	No	Retained

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 PCI ASV 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 PCI ASV deletes the user and transfers any user objects to the user you designated.

User Groups

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.

User groups allow you to manage user permissions for various resources in Tenable PCI ASV. 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.

Note: For an example of how user groups interact with user accounts and access groups, see Example: Access Groups.

To view your user groups:

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

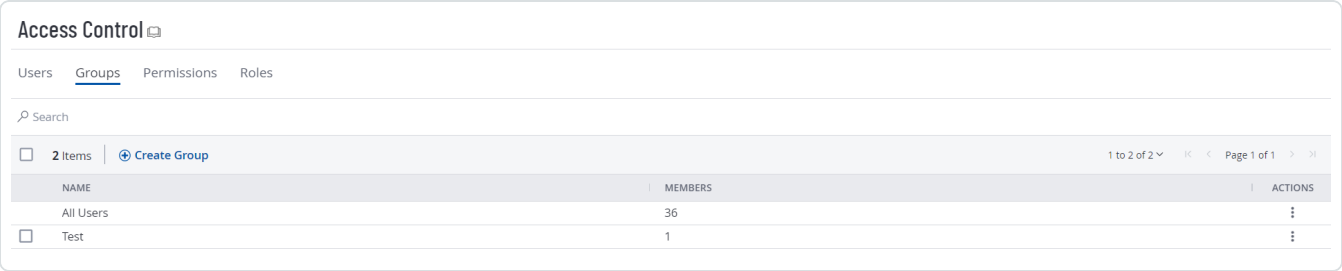
   The **Settings** page appears.

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 PCI ASV account.

3. Click the **Groups** tab.

   The **Groups** page appears.



The **User Groups** page displays a table of all user groups in your Tenable PCI ASV 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 upper-left corner, click the ☰ button.

   The left navigation plane appears.

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

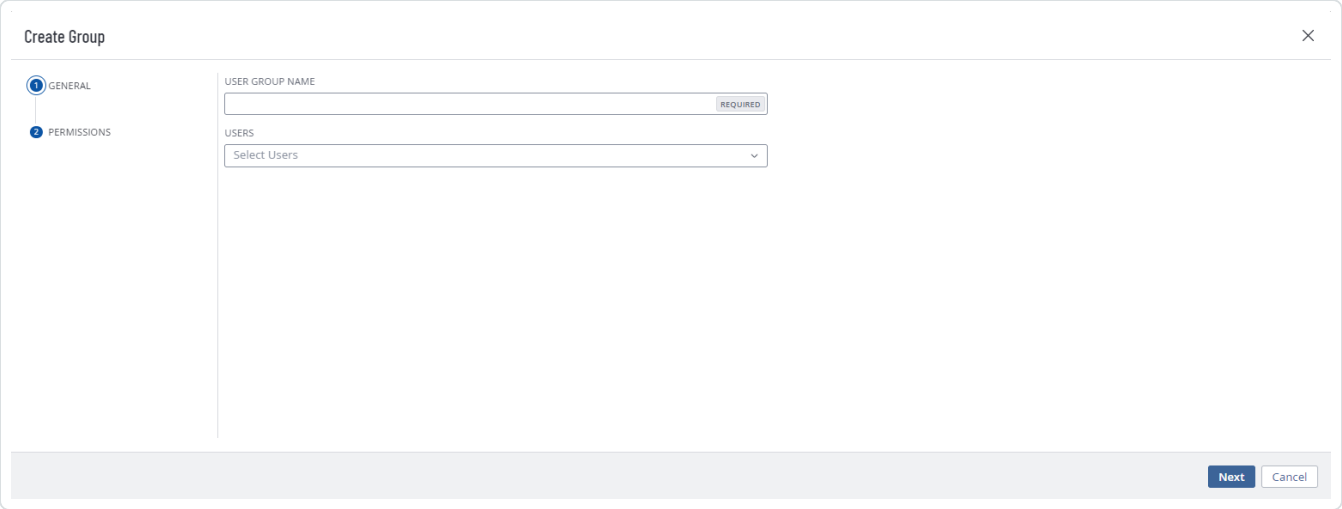
   The **Settings** page appears.

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 PCI ASV account.

4. At the top of the user group table, click the ⊕ **Create User Group** button.

   The **Create Group** page appears.



5. In the **User Group Name** box, type a name for the new 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 user name.

   As you type, Tenable PCI ASV filters the list of users in the drop-down box to match your search.

b. Select a user from the drop-down box.

   Tenable PCI ASV 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 PCI ASV 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 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 PCI ASV account.

4. In the user groups table, click the user group that you want to edit.

   The **Edit User Group** page appears.

5. 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 user name.

        As you type, Tenable PCI ASV filters the list of users in the drop-down box to match your search.

     b. Select a user from the drop-down box.

        Tenable PCI ASV 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 the user account you want to remove.

   Tenable Vulnerability Management removes the user from the **Users** list.

- Add or remove permissions from the group.

6. Click **Save**.

   Tenable PCI ASV saves the user group with any changes you made.

   The **Groups** page appears, where you can view the new group listed in the user groups table.

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 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 PCI ASV account.

4. Click the **Groups** tab.

   The **Groups** tab appears, containing a table that lists all user groups in your Tenable PCI ASV instance.

5. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

6. 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 PCI ASV 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.

7. In the **Name** box, type a name for the export file.
8. 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 PCI ASV 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.

9. (Optional) Deselect any fields you do not want to appear in the export file.
10. In the **Expiration** box, type the number of days before the export file expires.

    Note: Tenable PCI ASV allows you to set a maximum of 30 calender days for export expiration.

11. (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.

12. (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 PCI ASV sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

13. Click **Export**.

    Tenable PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

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

14. 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 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 PCI ASV account.

4. Click the **Groups** tab.

   The **Groups** page appears. This page displays a table with all the user groups on your Tenable PCI ASV account.

5. 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.

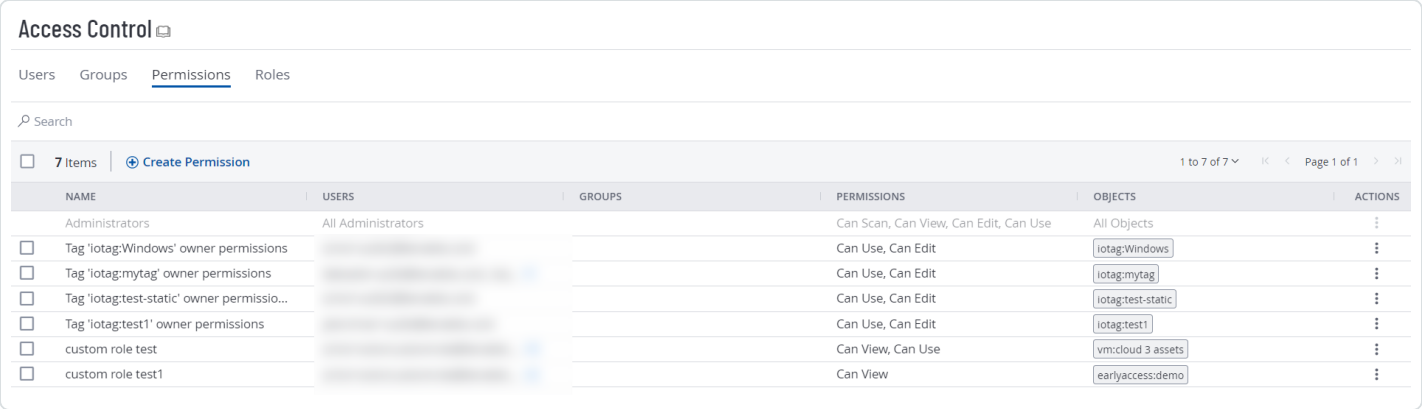
6. In the confirmation window, click **Delete**.

Tenable PCI ASV deletes the selected user group or groups. The deleted group or groups no longer appear in the user groups table.

Permissions

Tenable PCI ASV 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*.

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 Role 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 PCI ASV, these assets and the tags that define them are called *objects*.

Roles vs. Permissions: What's the difference?

- Roles — Roles allow you to manage privileges for major functions in Tenable PCI ASV and control which Tenable PCI ASV 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 the user or group to view the assets defined by the object.
Can Scan	Allows the user or group 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 PCI ASV 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 PCI ASV system, then it must be tagged by an object for which the user has **CanScan** permissions.
Can Edit	Allows the user or group to edit the tag that defines the object.
Can Use	Allows the user or group to use the tag that defines the object.

To view your permission configurations in Tenable PCI ASV:

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

   The left navigation plane appears.

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

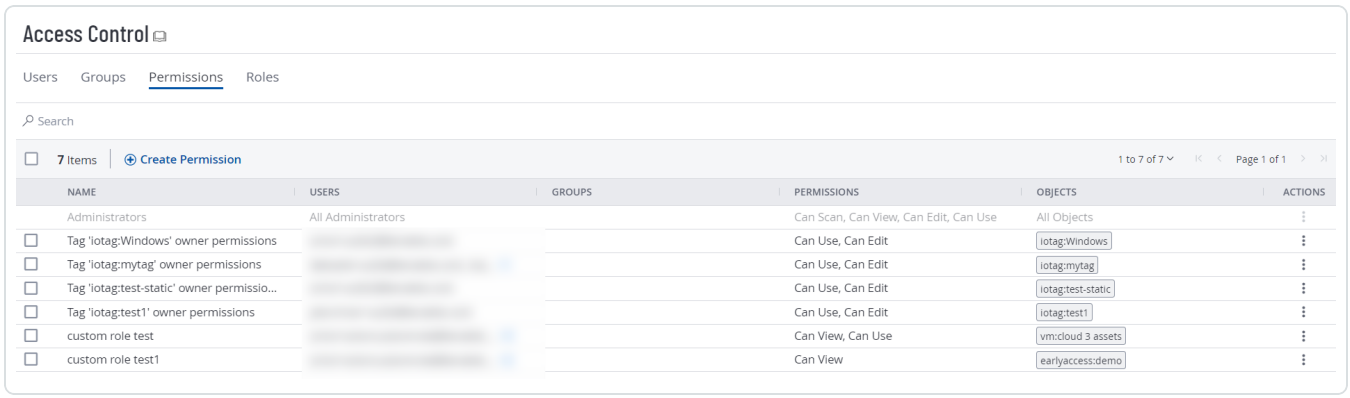
   The **Settings** page appears.

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 PCI ASV account.

4. Click the **Permissions** tab.

   The **Permissions** tab appears. This tab contains a table that lists all of the permission configurations on your Tenable PCI ASV 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 PCI ASV, you can apply that configuration to one or more users or groups.

Before you begin:

- Create a user or group for your Tenable PCI ASV 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 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.

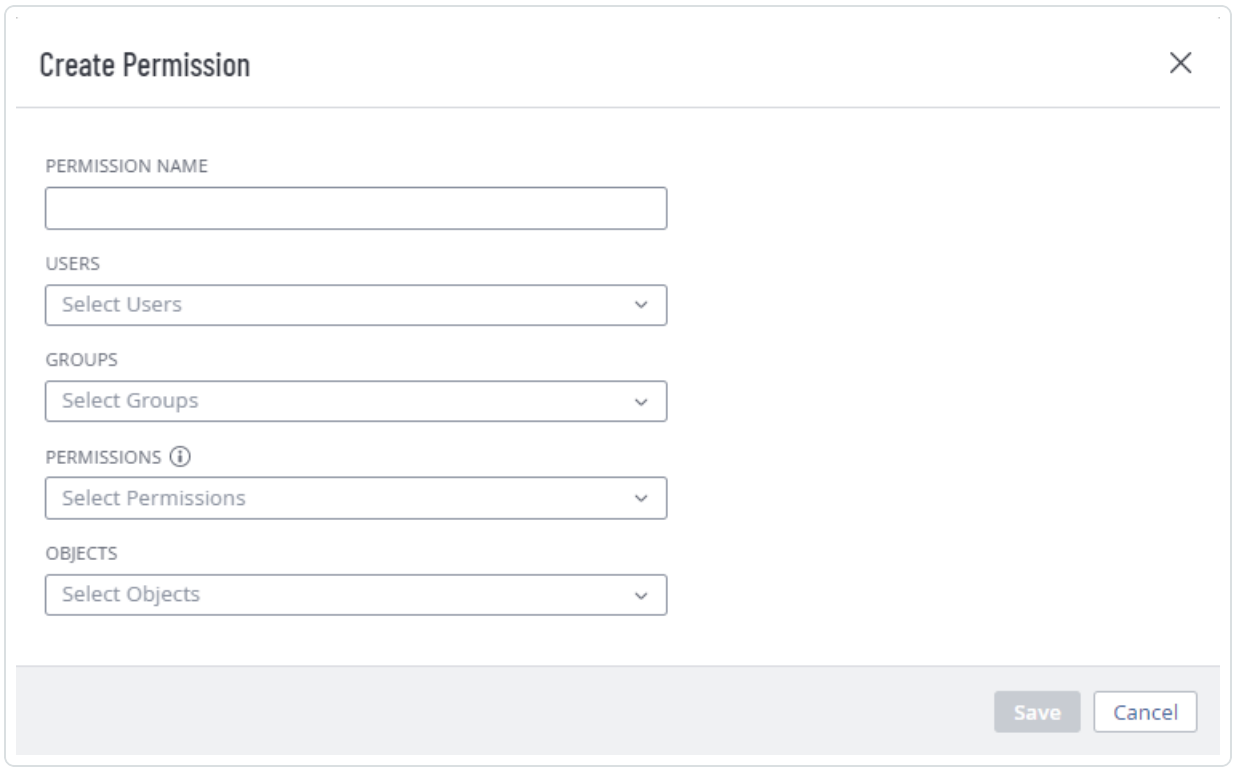
   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable PCI ASV account.

4. Click the **Permissions** tab.

   The **Permissions** tab appears. This tab contains a table that lists all of the permission configurations on your Tenable PCI ASV instance.

5. At the top of the table, click **Create Permission**.

   The **Create Permission** window appears.



6. In the **Permission Name** box, type a name for the permission configuration.
7. (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.

8. (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 PCI ASV instance. However, Tenable recommends that you use caution when assigning the permission configuration to all users because doing so goes against security best practices.

9. 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 PCI ASV automatically adds the **Can Use** permission.

10. 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.

11. Click **Save**.

    A confirmation message appears.

    Tenable PCI ASV 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 PCI ASV account.
- Create a permission configuration.

To add a permission configuration to a user or 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 **Access Control** tile.

   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable PCI ASV account.

4. 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 PCI ASV 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 PCI ASV 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.

5. Click **Save**.

Tenable PCI ASV 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 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 PCI ASV account.

4. Click the **Permissions** tab.

   The **Permissions** tab appears. This tab contains a list of all the permission configurations on your Tenable PCI ASV instance.

5. In the table, click the permission configuration you want to edit.

   The **Permission Details** page appears.

6. (Optional) In the **Permission Name** box, type a new name for the permission configuration.

7. (Optional) Add or remove users or user groups.

8. (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 PCI ASV 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 PCI ASV 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.

9. (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.

10. Click **Save**.

    Tenable PCI ASV 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 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 PCI ASV account.

4. Click the **Permissions** tab.

   The **Permissions** tab appears. This tab contains a table that lists all of the permission configurations on your Tenable PCI ASV 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.

5. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

6. 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 PCI ASV 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.

7. In the **Name** box, type a name for the export file.

8. 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 PCI ASV 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.

9. (Optional) Deselect any fields you do not want to appear in the export file.
10. In the **Expiration** box, type the number of days before the export file expires.

    Note: Tenable PCI ASV allows you to set a maximum of 30 calender days for export expiration.

11. (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.

12. (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 PCI ASV sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

13. Click **Export**.

    Tenable PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

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

14. 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 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 PCI ASV account.

4. 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 PCI ASV 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 PCI ASV 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 PCI ASV 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.

5. 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.

6. 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 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 PCI ASV account.

4. Click the **Permissions** tab.

   The **Permissions** tab appears. This tab contains a table that lists all of the permission configurations on your Tenable PCI ASV instance.

5. In the table, in the **Actions** column, click the ⋮ button next to the permission configuration you want to delete.

6. Click the **Delete** 🗑 button.

   Tenable PCI ASV deletes the permission configuration.

Tenable PCI ASV Roles

Roles allow you to manage privileges for major functions in Tenable PCI ASV and control which resources users can access in Tenable PCI ASV.

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 PCI ASV and control which Tenable PCI ASV modules and functions users can access.
- Permissions — Permissions allow you to manage access to your own data, such as Tags and Assets.

You can assign one of the following role types to users in Tenable PCI ASV:

Role Type	Description
Administrator	Administrators have the most privileges. They can view, import, export, create, modify, delete objects.
Custom Role	Contains a custom set of privileges that allow you to tailor user privileges and access to resources on your Tenable PCI ASV instance.

To view your user roles:

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 account.

4. Click the **Roles** tab.

   The **Roles** page appears. This page contains a table that lists all the user roles available on your Tenable PCI ASV 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

Create a Custom Role

Required User Role: Administrator

Note: A user assigned with the custom role cannot create or view PCI scans.

To create a custom role:

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 account.

4. Click the **Roles** tab.

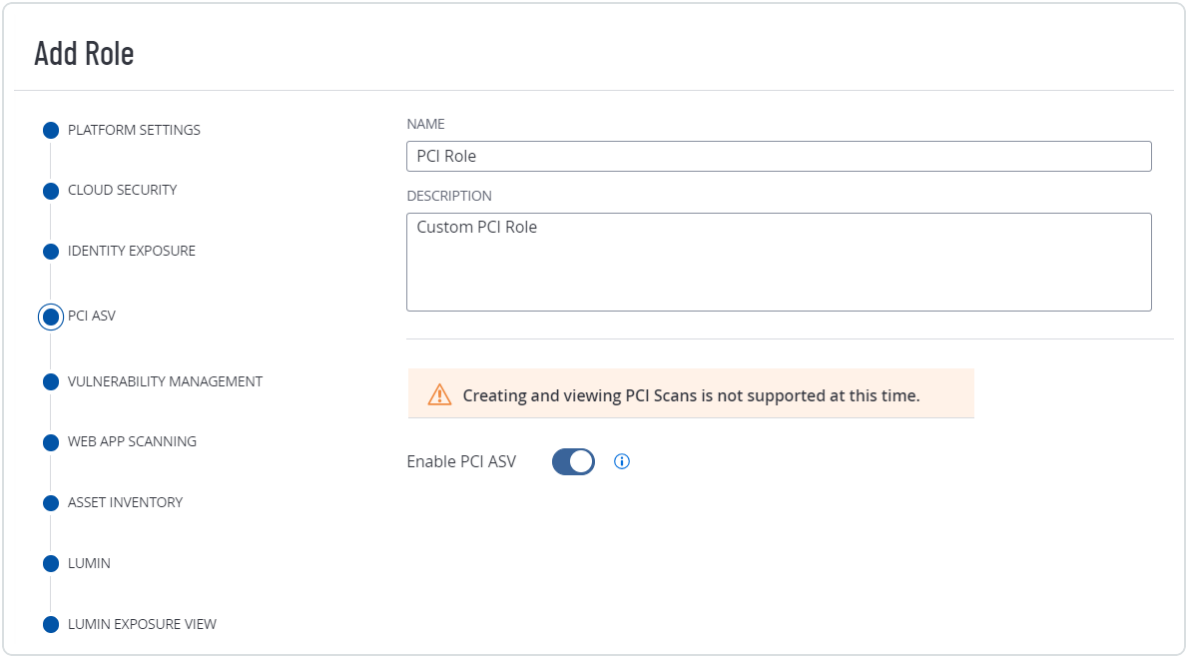
   The **Roles** page appears. This page contains a table that lists all the user roles available on your Tenable PCI ASV instance.

5. 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. On the left panel, click **PCI ASV**.

c. In the **Name** box, type a name for your custom role.

d. (Optional) In the **Description** box, type a description for your custom role.

e. Click the **Enable** toggle to enable or disable access to Tenable PCI ASV for the custom role you are creating.

f. Click **Save**.

   Tenable PCI ASV 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 the **Administrator** Role.

To create a custom role via duplication:

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 account.

4. Click the **Roles** tab.

   The **Roles** page appears. This page contains a table that lists all the user roles available on your Tenable PCI ASV instance.

5. 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.

6. In the action bar, click ⋮ **More**.

   A menu appears.

7. Click **Duplicate**.

   A copy of the role appears in the table, with the prefix *Copy of* [role name].

8. 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.

9. 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 PCI ASV area, select or deselect the check box next to each privilege you want to add to or remove from the role.

10. Click **Save**.

    Tenable PCI ASV saves your changes to the duplicate role.

Edit a Custom Role

Required User Role: Administrator

Note: You can edit only custom roles. You cannot edit the Administrator role.

To edit a custom role:

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 account.

4. Click the **Roles** tab.

   The **Roles** page appears. This page contains a table that lists all the user roles available on your Tenable PCI ASV instance.

5. In the roles table, click the role you want to edit.

   The **Roles Details** page appears.

6. 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 PCI ASV area, select or deselect the check box next to each privilege you want to add to or remove from the role.

7. Click **Save**.

   Tenable PCI ASV 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 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 account.

4. Click the **Roles** tab.

   The **Roles** page appears. This page contains a table that lists all the user roles available on your Tenable PCI ASV instance.

5. In the table, in the **Actions** column, click the ⋮ button next to the role you want to delete.

6. Click the **Delete** 🗑 button.

   Tenable PCI ASV 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 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 PCI ASV account.

4. 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 PCI ASV instance.

5. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

6. 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 PCI ASV 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.

7. In the **Name** box, type a name for the export file.
8. 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 PCI ASV 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.

9. (Optional) Deselect any fields you do not want to appear in the export file.
10. In the **Expiration** box, type the number of days before the export file expires.

    Note: Tenable PCI ASV allows you to set a maximum of 30 calender days for export expiration.

11. (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.

12. (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 PCI ASV sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

13. Click **Export**.

    Tenable PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

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

14. 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**.

Activity Logs

Required User Role: Administrator

On the **Activity Logs** page, you can view a list of events for all users in your organization's Tenable PCI ASV account. You can see when each activity took place, the action, the actor, and other relevant information about the activity.

Important: Tenable currently retains activity log data for 3 years, after which it is deleted from the Tenable database.

To view your activity logs:

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

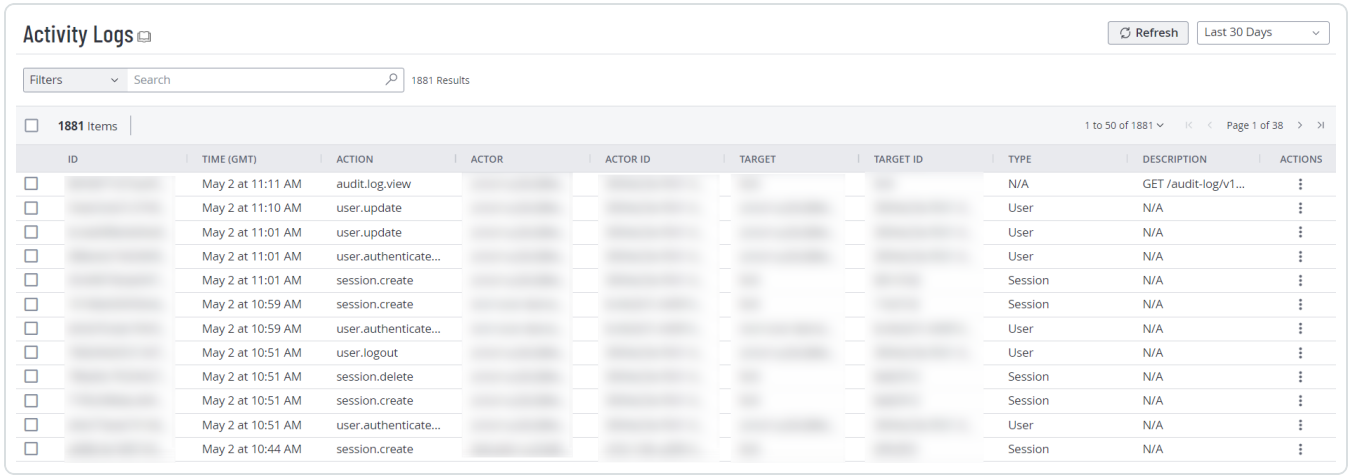
   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Activity Logs** tile.

   The **Activity Logs** page appears. This page shows a list of activities associated with your organization's Tenable PCI ASV account.



4. (Optional) Refine the table data. For more information, see Tenable Vulnerability Management Tables.

5. (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.

6. (Optional) To refresh the activity logs table, in the upper-right corner, click the **Refresh** button.
7. (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 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 **Activity Logs** tile.

   The **Activity Logs** page appears. This page shows a list of activities associated with your organization's Tenable PCI ASV account.

4. (Optional) Refine the table data. For more information, see Filter a Table.

5. 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.

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 activity logs. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable PCI ASV 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.

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 ages out.

   Note: Tenable PCI ASV allows you to set a maximum of 30 calender 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 PCI ASV 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 PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

    When processing completes, Tenable PCI ASV 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 from the Exports page.

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 to English, French, or Japanese. This setting only affects your own user account.

To change the user interface 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 **Language** tile.

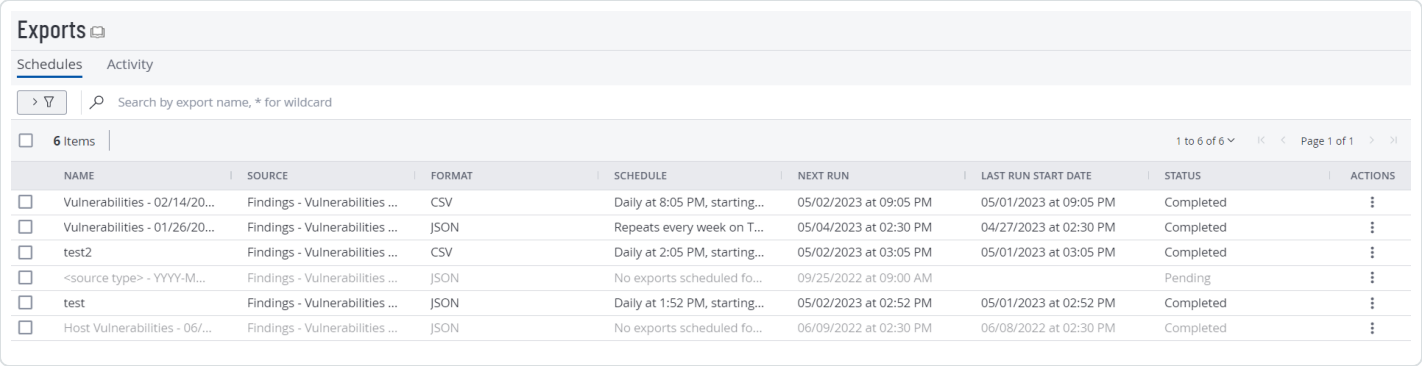
   The **Language** tile appears.

4. 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.



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 from Explore Tables.
- **Assets Host** —Information about assets Tenable Vulnerability Management identified on your host during a scan. For more information, see Host Assets and Export from Explore Tables.
- **Findings - Vulnerabilities - Host** — Information about the vulnerability findings Tenable Vulnerability Management identified on your host during a scan. For more information, see Export from Explore Tables.
- **Users** — Information about the users assigned to your account. For more information, see Export Users.

For more information, see the following topics:

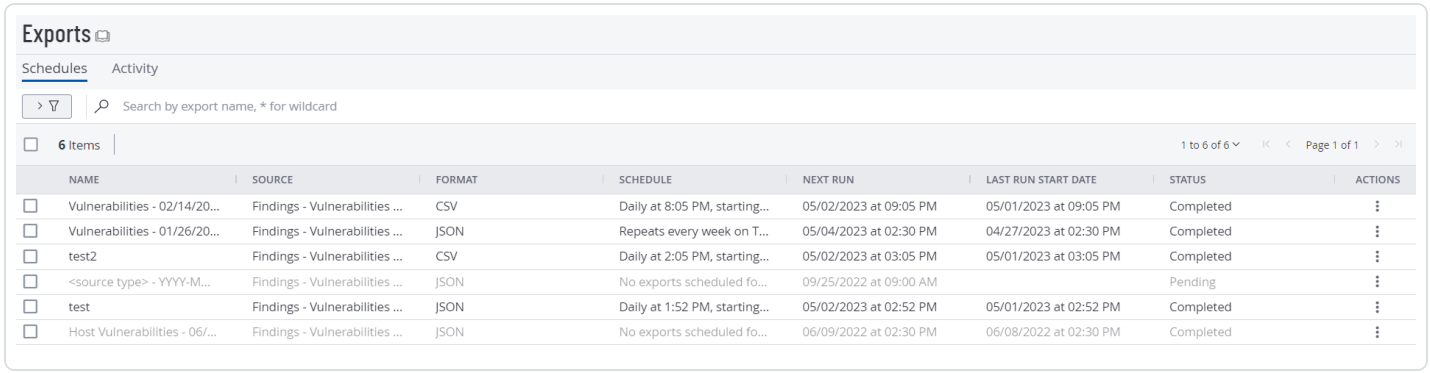
Scheduled Exports

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.

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 from Explore Tables.
- **Assets Host** —Information about assets Tenable Vulnerability Management identified on your host during a scan. For more information, see Host Assets and Export from Explore Tables.
- **Findings - Vulnerabilities - Host** — Information about the vulnerability findings Tenable Vulnerability Management identified on your host during a scan. For more information, see Export from Explore Tables.
- **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
- 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 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 **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

4. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

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 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 **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

4. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

5. 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 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 **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

4. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

5. 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.

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 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 **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

4. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

5. 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:

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

   The left navigation plane appears.

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

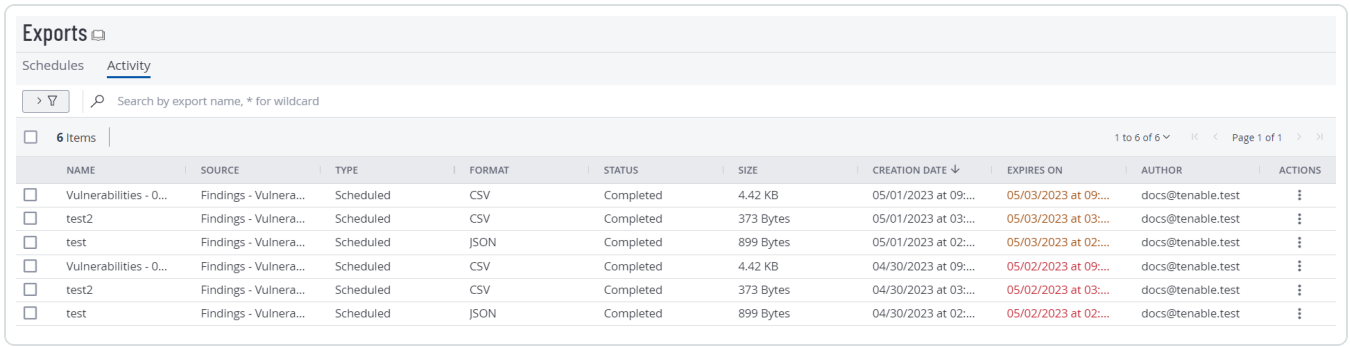
   The **Settings** page appears.

3. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

4. 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 Interact with a Customizable Table. 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:** Export expiration is set via the **Settings** section. For more information, see .
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 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 **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

4. (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.

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

   The filters plane expands. The plane displays a list of default filter options.

6. Click **Edit Filters**.

   A drop-down box appears listing all the filter options.

7. Select or deselect the filters you want to add or remove. For detailed list of available filters, see Export Filters.

8. Click outside the filter drop-down box.

   The drop-down box closes.

9. For each selected filter, in the first text box, select an operator.

10. 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**.

11. (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.

12. (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.

13. 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 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 **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

4. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

5. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

6. 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.

7. Click **Renew**.

   Tenable Vulnerability Management resets the export expiration date for 30 days from today's date.

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 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 **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

4. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

5. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

6. 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 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 **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

4. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

5. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

6. 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.

7. 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 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 **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.

4. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.

5. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

6. 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.

7. In the **Name** box, type a name for the export file.
8. 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 PCI ASV 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.

9. 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**.

10. 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 calender days for export expiration.

11. (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.

12. (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 PCI ASV sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

13. 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.

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

   The left navigation plane appears.

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

   The **Settings** page appears.
2. For more information, see Tenable PCI ASV Workbench Tables.
3. Click the **Exports** tile.

   The **Exports** page appears. By default, the **Schedules** tab is active.
4. Click the **Activity** tab.

   The **Activity** page appears. This page displays a table with all the exports on your Tenable Vulnerability Management account.
5. (Optional) Refine the table data.

6. 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.

Tags

You can add your own business context to assets by tagging them with descriptive metadata in Tenable PCI ASV. 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*.

For more information about tag structure, see Tag Format and Application.

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.

Adding your own business context to assets using tags allows you to filter analysis views by tag.

To view your tags:

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

   The left navigation plane appears.

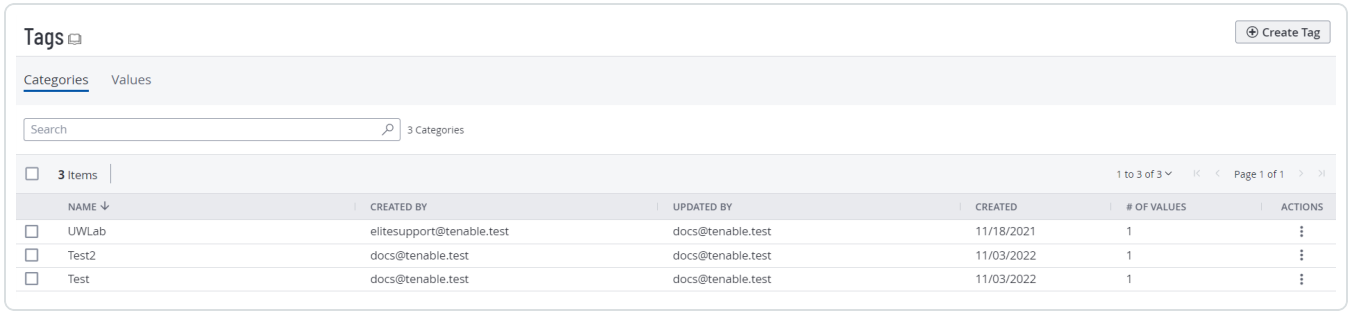
2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.



4. Do one of the following:

   To view the categories to which your all the tags on your Tenable PCI ASV 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 on your Tenable PCI ASV instance:

a. Click the **Values** tab.

The **Values** page appears, containing a table of all the tags on your Tenable PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV imports data
- Every 12 hours

Manual Tags vs. Automatic Tags

When you create a tag, Tenable PCI ASV 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 PCI ASV applies that tag to all your current assets and any new assets added to your organization's account. Tenable PCI ASV 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 PCI ASV 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	Manual	

add the tag to assets located at your headquarters.		
You create a tag with *Location*:*Headquarters* as the *Category*:*Value* pair, and you specify an IP address range in the tag rules. Tenable PCI ASV then automatically applies the tag to all existing or new assets within that IP address range.	Automatic	

Create a Manual or Automatic Tag

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

If your tags fail to apply, the tag rules may return too many assets for Tenable PCI ASV 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.

On the **Create Tag** page, you can create a manual tag to apply to assets individually. You can also create an automatic tag by creating tag rules that Tenable PCI ASV uses to identify and tag matching assets.

Note: You can create up to 100 tag categories, and each category can have up to 100,000 tags.

To create an automatic tag from the **Tags** page:

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.

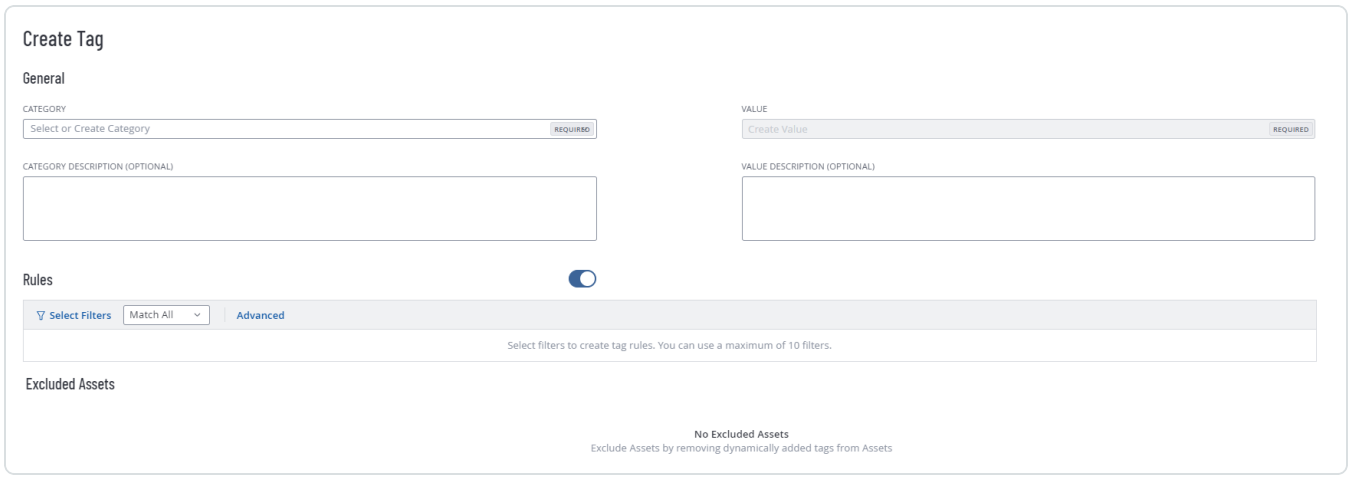
3. Click the **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

4. In the upper-right corner of the page, click the ⊕ **Create Tag** button.

   The **Create Tag** page appears.



5. Click the **Category** drop-down box.
6. In the **Add New Category** box, type a category.

   As you type, the list filters for matches.
7. 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 PCI ASV instance.
8. (Optional) In the **Category Description** box, type a description of the tag category.
9. 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.
10. (Optional) In the **Value Description** box, type a description for the new tag.
11. Do one of the following:

    To save the tag as a manual tag:

    a. Click **Save**.

       Tenable PCI ASV 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 PCI ASV 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 PCI ASV may take a few minutes to apply the tag and update any Excluded Assets, depending on the system load and the number of assets.

Considerations for Tags with Rules

Automatic Application

Tenable PCI ASV evaluates assets against tag rules in the following situations:

- When you add a new asset (via scan, connector import, or leveraging the Tenable PCI ASV API), Tenable PCI ASV evaluates the asset against your tag rules.
- When you create or update a tag rule, Tenable PCI ASV evaluates your assets against the tag rule.

  > **Note:** When you create or edit a tag rule, Tenable PCI ASV 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 PCI ASV 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 PCI ASV excludes that asset from any further evaluation against the rules.

Tag Rules

Tag rules allow Tenable PCI ASV 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 PCI ASV applies the tag to all assets on your instance that match the tag rule.

> **Note:** Tenable PCI ASV supports a maximum of 1,000 rules per tag. This limit means that you can specify a maximum of 1,000 **and** or **or** conditions for a single tag value. Additionally, Tenable PCI ASV supports a maximum of 1,024 values per individual tag rule.

For more information about automatic tags, see Tag Format and Application.

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 via 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 PCI ASV 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.

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 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 **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

4. Click the **Values** tab.

The **Values** page appears, containing a table of all the tags on your Tenable PCI ASV instance.

5. Click the **Rules** toggle to enable the rule settings.

   The **Rules** section appears.

6. 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. (Optional) To create another rule, repeat the steps to create a tag in **Basic** mode.

   h. (Optional) To create another rule:

      i. Repeat the steps to create a tag rule in **Basic** mode.

      ii. In **Rules** section, in the **Match Any** drop-down box, do one of the following:

- To apply the tag to assets that match any of the rules, select **Match Any**.

  An **OR** operator appears between each rule, and Tenable PCI ASV applies the tag to assets that meet any of the rules specified in the tag.

- To apply the tag to only assets that match all of the rules, select **Match All**.

  An **AND** operator appears between each rule.

  Tenable PCI ASV applies the tag to only assets that meet all of the rules specified in the tag.

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 will appear 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, which are contextual based on the selected filter:

   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.
is on	Filters for items with a specified date.
between	Filters for items with a date between two specified dates.

Operator	Description
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*.

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**.

e. (Optional) To create more rules for the tag:

i. Press the **Space** key.

A modifier drop-down box appears, with **AND And** and **OR Or** as options.

ii. Select a modifier.

iii. Press the **Space** key.

A drop-down box appears listing the tag rule filter options.

iv. Repeat the steps to create a tag rule in **Advanced** mode.

7. Click **Save**.

Tenable PCI ASV creates the rule and applies it to the tag.

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 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 **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

4. Click the **Values** tab.

   The **Values** page appears, containing a table of all the tags on your Tenable PCI ASV instance.

5. 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.

6. Click the **Rules** toggle to enable the rule settings.

   The **Rules** section appears.

7. 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.

8. (Optional) In the first drop-down box, select a new operator.

9. (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.

10. Click outside the rules drop-down box.

    The drop-down box closes.

11. Click **Save**.

    Tenable PCI ASV save your changes, evaluates existing assets, and automatically applies the tag to assets that match the updated tag rules.

    > **Note:** Tenable PCI ASV 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 PCI ASV 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 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 **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

4. On the **Tags** page, click the **Values** tab.

   The **Values** page appears, containing a table with all the tags on your Tenable PCI ASV instance.

5. 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.

6. In the **Rules** section, in the rule you want to delete, click the ✕ button.

   The rule disappears from the **Rules** section.

7. Click **Save**.

   Tenable PCI ASV 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 PCI ASV supports a maximum of 1,000 rules per tag. This limit means that you can specify a maximum of 1,000 **and** or **or** conditions for a single tag value. Additionally, Tenable PCI ASV 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) 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) 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 PCI ASV scanned the asset for vulnerabilities or if Tenable PCI ASV only discovered the asset via a discovery scan. Possible values are: • **Assessed** • **Discovered Only**

Asset ID	The asset's UUID.
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.
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 API Instance State 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. For more information, see AWS Account Identifiers in the AWS documentation. This attribute contains a value for Amazon EC2 instances only. For other asset types, this attribute is empty.
AWS Region	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.
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 User Guide.
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 Accessing and Using Azure VM Unique ID in the Microsoft Azure 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 PCI ASV 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 PCI ASV 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 software applications a scan identified as present on an asset. This field supports the CPE 2.2 format. For more information, see the Component Syntax section of the CPE Specification documentation, Version 2.2. For assets identified in Tenable scans, this field contains data only if a scan using Tenable 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 PCI ASV considers the detection of that application expired. As a result, the next time a scan evaluates the asset, Tenable PCI ASV removes the expired application from the **Installed Software** attribute. This activity is logged as a remove type of attribute change in the asset activity log.
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 PCI ASV 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 PCI ASV.
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.

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 licensed assets, 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 PCI ASV 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 PCI ASV 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	The operating system that a scan identified as installed 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	A unique filter that searches tag (category: value) pairs. When you type a tag value, you must use the *category: value* syntax, including the space after the colon (:). You can use commas (,) to separate values. If there is a comma in the tag name, insert a backslash (\) before the comma. You can add a maximum of 100 tags. For more information, see tags. **Note:** If your tag name includes double quotation marks (" "), you must use the UUID instead.
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 PCI ASV 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 upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Explore** section, click **Assets**.

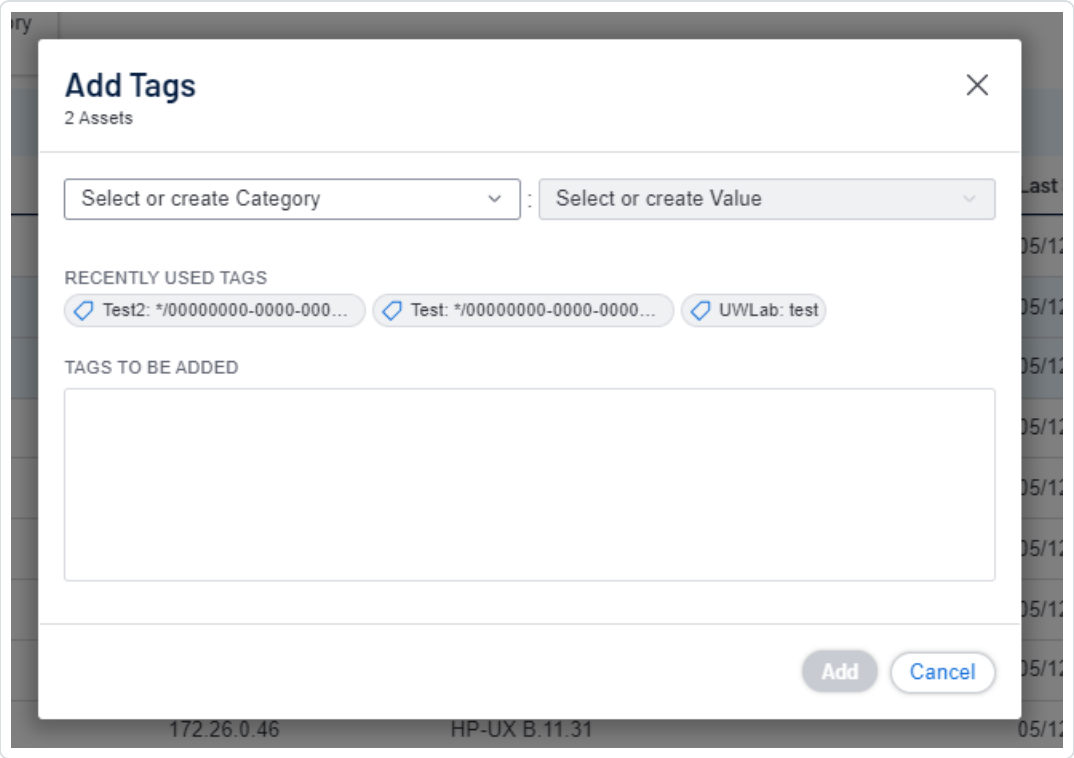
   The **Assets** page appears.

3. 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.

4. In the header, to the left of the first filter, click **Add Tags**.

   The **Add Tags** window appears.



5. Under **Create/Select Tag**, in the first drop-down box, type a category.

   As you type, the list filters for matches.

6. 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.

7. Under **Create/Select Tag**, in the second drop-down box, type a value for your new tag.

8. In the drop-down box, click **Create "***value* **"**.

9. Click **Save**.

   Tenable PCI ASV saves the tag and applies it to applicable assets on your account.

   Note: It can take up to several minutes for Tenable PCI ASV 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 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 **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

4. 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 PCI ASV 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.

5. To edit the tag category:

   Note: When you edit a tag category, Tenable PCI ASV 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.

6. Click **Save**.

   Tenable PCI ASV 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 upper-left corner, click the ☰ button.

   The left navigation plane appears.

2. In the left navigation plane, in the **Explore** section, click **Assets**.

   The **Assets** page appears. By default, the **Hosts** tab is visible.

3. 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.

4. In the header, to the left of the first filter, click the 🏷 button.

   The **Tag Matching Assets** window appears.

5. 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.

6. (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.

7. (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.

8. (Optional) In the **Chosen Search Filters for Tag** box, click the ✕ inside any filters you want to remove from the tag.

9. Click **Save**.

   Tenable PCI ASV saves your edits.

Add a Tag to an Asset

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

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 **Assets**.

   The **Assets** page appears. By default, the **Hosts** tab is visible.

3. View your assets list.

4. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

5. 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 PCI ASV 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 PCI ASV adds the tags specified in **Tags to be Added** to the assets.

6. 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.

7. Click **Add**.

The assets table appears. A confirmation message also appears. Tenable PCI ASV adds the tags specified in **Tags to be Added** to the assets.

Remove a Tag from an Asset via the Asset View

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

Required Access Group Permissions: Can View, Can Edit

This procedure describes how to remove tags from assets from the **Assets** page. You can also remove asset tags from the **Vulnerabilities by Assets** page.

If an asset matches a dynamic tag's rules but you do not want the tag applied, you can manually remove the tag from the asset. If you later want to re-apply the tag to the asset, you can remove the asset from the excluded assets list, as described in Edit Tag Rules.

To remove a tag from a single asset:

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. In the left navigation plane, in the **Explore** section, click **Assets**.

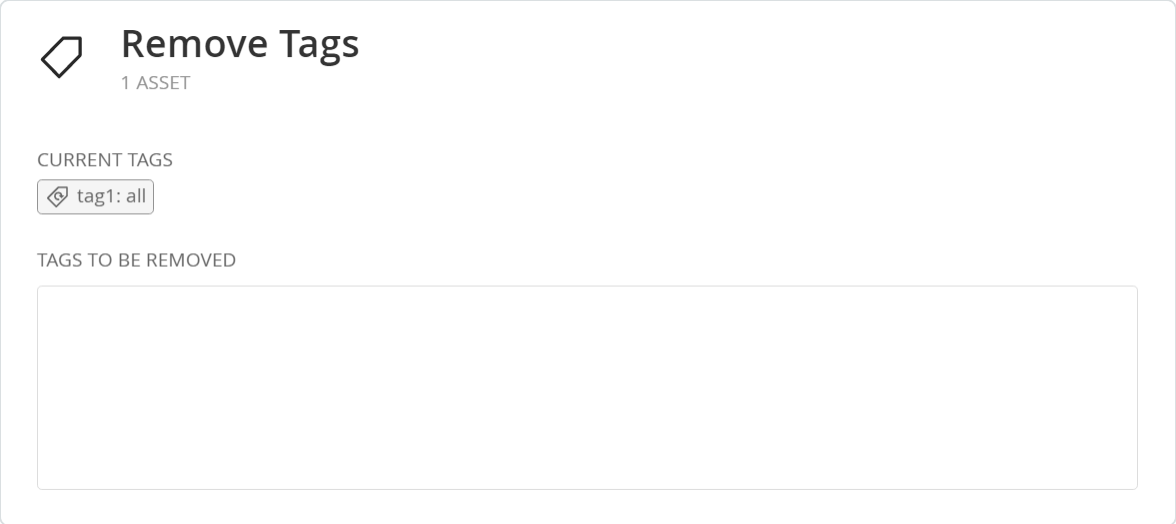
   The **Assets** page appears. By default, the **Hosts** tab is visible.

4. Do one of the following:

Location	Action
Assets page	a. Click **Remove Tag**.
Assets page	a. In the assets table, select the check box for each asset from which you want to remove a tag. The action bar appears at the bottom of the page. b. On the action bar, click **Remove Tag**.
Asset	a. In the assets table, click the asset where you want to remove the

Details page	tag. The **Asset Details** page appears. b. In the right panel, in the **Tags** section, click the name of the tag you want to remove from the asset. A menu appears. c. Click **Remove Tag**.

The **Remove Tags** plane appears.



5. Under **Current Tags**, click each tag you want to remove.

   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.

6. Click **Remove**.

   Tenable Vulnerability Management removes the tags specified in **Tags to be Removed** from the asset.

To remove tags from multiple assets:

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**.

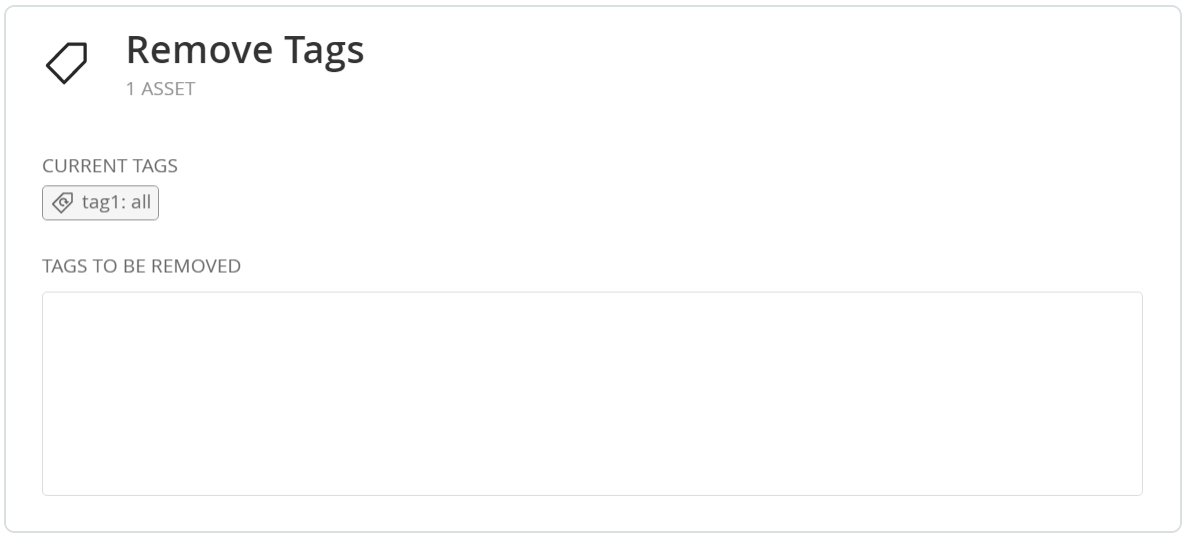
   The **Assets** page appears.

3. In the assets table, click the check box next to each asset for which you want to remove the tag.

   The action bar appears at the bottom of the page.

4. In the action bar, click **Remove Tag**.

   The **Remove Tags** plane appears.



5. Under **Current Tags**, click each tag you want to remove.

   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.

6. Click **Remove**.

   Tenable PCI ASV removes the tags specified in **Tags to be Removed** from the selected 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 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 **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

4. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

   Note: You cannot filter the tables on the **Tags** page.

5. 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.

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 tag categories or values. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable PCI ASV 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.

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 calender 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 PCI ASV 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 PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

    When processing completes, Tenable PCI ASV 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 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 PCI ASV 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 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 **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

4. Click the **Categories** tab.

   The tag categories table appears.

5. 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..

6. Click **Delete**.

Tenable PCI ASV 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

When you delete a tag, Tenable PCI ASV removes that specific tag from all assets where you applied the tag.

To delete one or more tags:

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 **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

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 PCI ASV 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 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 **Tagging** tile.

   The **Tags** page appears. On this page, you can view your asset tag categories and values.

   The **Categories** tab is active.

4. Click the **Values** tab.

5. In the table, click the ⋮ button.

   The actions menu appears.

6. Click 🔍 **Search by Tag**.

   The **Assets** page appears and displays the assets table filtered by the tag you selected.

Sensors

Tenable PCI ASV supports the following sensor types:

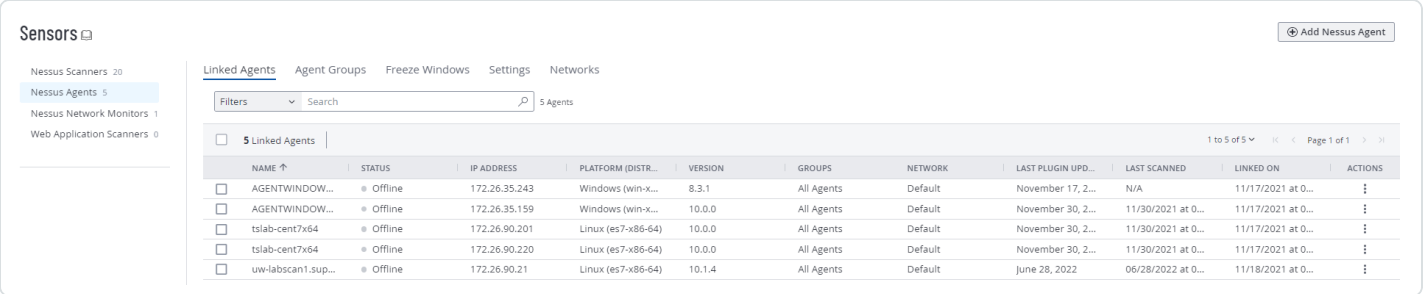
- Tenable-provided *regional cloud sensors*. For more information, see Cloud Sensors.
- Manually configured *linked sensors* (Tenable Nessus scanners, Tenable Nessus Network Monitor instances, Tenable Web App Scanning sensors, and Tenable Nessus Agents). For more information, see Linked Sensors.

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 Nessus Agent on a host and link the agent to Tenable PCI ASV, the agent appears on the Tenable PCI ASV **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 PCI ASV:

- 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 Nessus Agent Advanced Settings for more information)
- (Agents 10.0.x and later) AWS EC2 instance metadata, if available:

Note: Tenable Nessus Agent connect to 169.254.169.254 to provide AWS metadata to Tenable PCI ASV; traffic between Tenable Nessus 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: For agents versions 8.3.1 and older, agents check in on start and after a restart.

For agents version 10.0.0 and later, agents check in on start, after a restart, and whenever the metadata is updated (no more than every 10 minutes).

Tip: For information on other ways to ingest data into Tenable PCI ASV, see the Data Ingestion in Tenable Tenable Vulnerability Management quick reference guide.

Retrieve the Tenable Nessus Agent Linking Key

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Before you begin the Tenable Nessus Agents installation process, you must retrieve the agent linking key from Tenable PCI ASV.

To retrieve the agent linking key:

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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. Click ⊕ **Add Nessus Agent**.

   The **Add Agent** plane appears.

6. Click the **Copy** button to copy the **Linking Key**.

   A **Linking key copied to clipboard** confirmation message appears.

What to do next:

- Install Tenable Nessus Agent

Download Linked Agent Logs

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

In Tenable PCI ASV, 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 PCI ASV retains the log file for seven days.

To download logs from a linked agent in Tenable PCI ASV:

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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the agents table, click the agent for which you want to download logs.

   The details page for that agent appears.

6. Click the **Logs** tab.

   A table shows any previously downloaded logs.

7. 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 PCI ASV 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 PCI ASV retains the logs for seven days.

8. 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 PCI ASV 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 PCI ASV 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 PCI ASV, you can restart linked agents (versions 7.6 and later) on the **Linked Agents** tab.

To restart an agent:

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. 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 PCI ASV 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 PCI ASV 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 PCI ASV:

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. 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. For filter descriptions, see Agent Filters.

6. 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 PCI ASV 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 PCI ASV enables **More** > **Unlink Selected**. b. Click **Unlink Selected**.

Tenable PCI ASV 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 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. Click the row of the agent you want to rename.

   The agent **Details** page appears.

6. Click the ✎ button next to the agent name.

7. Edit the agent name.

8. Click the ✓ button next to the agent name.

   Tenable PCI ASV saves the new agent name and updates any related tables with the new name.

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 PCI ASV, 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 Nessus 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 Nessus Agent User Guide*.

To modify remote agent settings in Tenable PCI ASV:

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. 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 Nessus 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. 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*.	`normal`	• `normal` - Changes the backend.log logging level to `normal` and sets log tags to `"log", "info", "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 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 Nessus Agent Deployment and User Guide*.	`high`	`low`, `medium`, or `high`
Scan Performance	Sets scan	`high`	`low`, `medium`, or `high`

	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 Nessus 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	`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`

	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 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	Specifies the number of days an agent can be offline before rule-	14	Integers 1-48

Threshold	based scans stop executing.		
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 PCI ASV 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	`normal`	• `normal` - Sets log tags to `"log", "info", "warn",`

	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. For more information, see log.json Format in the *Tenable Nessus User Guide*.		`"error", "trace"` • `debug` - Sets log tags to `"log", "info", "warn", "error", "trace", "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	`high`	`low`, `medium`, or `high`

	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 Nessus 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 Nessus 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. This feature is disabled by default to prevent custom agent names from being overridden.	`no`	`yes` or `no`
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.		
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 PCI ASV 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 PCI ASV.

To modify global agent settings in Tenable PCI ASV:

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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. Select **Settings** in the drop-down box.

   The **Settings** page appears.

6. 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 PCI ASV automatically tracks unlinked agents and related data for the number of days specified in this option. You cannot turn off this

Option	Description
	tracking. **Note:** Inactive agents that were automatically unlinked by Tenable PCI ASV 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.

7. Click **Save**.

   Tenable PCI ASV saves your changes.

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.

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 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. 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 Nessus Agent version.

To create an agent profile:

1. On the **Profiles** page, click ⊕ **Add Agent Profile**.

   The **Create Agent Profile** page appears.

2. Enter a **Name** for the agent profile.

3. (Optional) Enter a **Description** for the agent profile.

4. Select the agent profile's **Sensor Version**. This is 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, 10.4.x), or you can set the agent profile to a specific patch release (for example, 10.4.1).

5. Under **Assign Agents**, select the checkboxes next to the agents you want to assign.

6. Click **Create**.

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:

   - To edit the agent profile name, click next to the agent name.
   - In the **Details** tab, you can edit the profile description and the agent version that the profile sets linked agents to.
   - In the **Agents** tab, you can add or remove linked agents from the agent profile.

3. Click **Save**.

   Tenable PCI ASV saves your changes. If you added or removed agents from the profile, the agents' versions update within 24 hours of your edit.

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 PCI ASV 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 PCI ASV 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 PCI ASV. 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 PCI ASV 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 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. 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 PCI ASV 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 PCI ASV 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 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. 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 PCI ASV 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 PCI ASV 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

Agent Status

Tenable Nessus Agents can be in one of the following statuses:

Status	Description
Online	The host that contains the Tenable Nessus Agent is currently connected and in communication with Tenable Vulnerability Management.
Offline	The host that contains the Tenable Nessus Agent is currently powered down or not connected to a network.
Initializing	The Tenable Nessus Agent is in the process of checking in with Tenable Vulnerability Management.

Export Agents

To export agents data in Tenable PCI ASV:

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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. Select the agents that you want to export by clicking each agent's checkbox.

6. At the top of the agent table, click the **Export** button.

   The **Export** plane appears and shows the number of agents that will be exported.

7. In the **Formats** section, select the **CSV** format.

   Note: If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable PCI ASV automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.

8. To export agents data in `.csv` format, click **Export**.

   Your browser's download manager appears.

9. Click **OK** to save the `agents.csv` file.

The `agents.csv` file exported from Tenable PCI ASV 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 PCI ASV.
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.

Export Linked Agents

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

On the **Sensor Management** page, you can export one or more linked agents in CSV or JSON format.

To export your linked agents:

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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Freeze Windows**.

6. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

7. 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 export schedule.
- A toggle to configure the email notification.

8. In the **Name** box, type a name for the export file.
9. 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.

10. (Optional) Deselect any fields you do not want to appear in the export file.
11. In the **Expiration** box, type the number of days before the export file expires.

> **Note**: Tenable PCI ASV allows you to set a maximum of 30 calender days for export expiration.

12. (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.

13. (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 PCI ASV sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

14. Click **Export**.

    Tenable PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

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

15. 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 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

6. In the linked agents table, click the linked agent for which you want to export details.

   The **Details** page appears.

7. 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.

8. In the **Name** box, type a name for the export file.
9. 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.
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.

10. (Optional) Deselect any fields you do not want to appear in the export file.
11. In the **Expiration** box, type the number of days before the export file expires.

Note: Tenable PCI ASV allows you to set a maximum of 30 calender days for export expiration.

12. (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.

13. (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 PCI ASV sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

14. Click **Export**.

    Tenable PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

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

15. 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**.

Filter Agents

To filter agents in the agents table in Tenable PCI ASV

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. In the left navigation menu, click **Nessus Agents**.

   The **Linked Agents** page appears.

5. Above the agents table, click the **Filters** button.

   The **Filters** pane appears.

6. 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	In the text box, type the IPv4 or IPv6 addresses on which you want to filter.

Category	Operator	Value
	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.
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	In the text box, type the version you want to filter.

Category	Operator	Value
	contains does not contain	

7. Click **Apply**.

   The manager filters the list of agents to include only those that match your configured options.

Agent Filters

Tenable PCI ASV 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 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 does not contain	In the text box, type the agent name on which you want to filter.

Category	Operator	Value
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.
UUID	is equal to is not equal to	In the text box, type the agent UUID that you want to filter. Use the following agent UUID format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx. You can find the agent's UUID by viewing the agent's details in the Tenable PCI ASV user interface, or by running the `# nessuscli agent status` 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 Groups

You can use agent groups to organize and manage the agents linked to Tenable PCI ASV. 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 PCI ASV.

To create a new agent 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Agent Groups**.

   The list of agent groups appears.

6. Click ⊕ **Add Agent Group**.

   The agent group settings plane appears.

7. In the **Group Name** box, type a name for the new agent group.

8. Configure user permissions for the agent group.

9. 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 PCI ASV. You can also add agents to a group when you modify an agent group.

To add an agent to agent groups:

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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Agent Groups**.

   The list of agent groups appears.

6. (Optional) Search for a specific agent or filter the agents in the table. For filter descriptions, see Agent Filters.

7. 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.

8. 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.
9. Click **Save** to save your changes.

   Tenable PCI ASV 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 PCI ASV

To modify an agent 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Agent Groups**.

   The list of agent groups appears.

6. (Optional) Search for a specific agent group or filter the agent groups in the table. For filter descriptions, see Agent Group Filters.

7. 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 PCI ASV saves your changes.

8. 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 PCI ASV 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 PCI ASV.

To delete an agent 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Agent Groups**.

   The list of agent groups appears.

6. (Optional) Search for a specific agent group or filter the agent groups in the table. For filter descriptions, see Agent Group Filters.

7. 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.

8. Click **Delete**.

   A confirmation window appears.

9. Click **Delete**.

   Tenable PCI ASV 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 PCI ASV.

To remove an agent from an agent 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Agent Groups**.

   The list of agent groups appears.

6. (Optional) Search for a specific agent group or filter the agent groups in the table. For filter descriptions, see Agent Group Filters.

7. In the agent groups table, click the agent group you want to modify.

   The **Group Details** page appears.

8. 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 PCI ASV 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 PCI ASV enables **More** > **Remove Selected from Group**. b. Click **Remove Selected from Group**.

Tenable PCI ASV 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 PCI ASV.

To view agents in an agent group in the new interface:

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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Agent Groups**.

   The list of agent groups appears.

6. (Optional) Search for a specific agent or filter the agents in the table. For filter descriptions, see Agent Filters.

7. 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.

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 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Freeze Windows**.

6. Click ⊕ **New Freeze Window**.

   The **New Freeze Window** plane appears.

7. Configure the options as necessary.

8. 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 PCI ASV.

To edit a freeze window:

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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Freeze Windows**.

   The list of freeze windows appears.

6. In the freeze window table, click the freeze window you want to modify.

   The **Update a Freeze Window** page appears.

7. Edit the options as necessary.

8. Click **Save** to save your changes.

   Tenable PCI ASV 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 PCI ASV.

To enable or disable a freeze window for linked agents in the new interface:

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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Freeze Windows**.

6. Search for the freeze window you want to enable or disable.

7. 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 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Freeze Windows**.

   The list of freeze windows appears.

6. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

7. 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 PCI ASV 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 export schedule.
- A toggle to configure the email notification.

8. In the **Name** box, type a name for the export file.
9. 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 PCI ASV 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.

10. (Optional) Deselect any fields you do not want to appear in the export file.
11. In the **Expiration** box, type the number of days before the export file expires.

    Note: Tenable PCI ASV allows you to set a maximum of 30 calender days for export expiration.

12. (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.

13. (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 PCI ASV sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

14. Click **Export**.

    Tenable PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

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

15. 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 PCI ASV.

To delete a freeze window for agent scanning:

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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. In the drop-down box, select **Freeze Windows**.

   The list of freeze windows appears.

6. 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.

7. Click **Delete** to confirm the deletion.

   Tenable PCI ASV deletes the selected freeze window or windows.

Plugin Updates

The following table describes the behavior of differential plugin updates for agents linked to Tenable PCI ASV:

Linked	Differential Update	Full Update
Tenable PCI ASV	The agent requests differential updates from Tenable PCI ASV 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.

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 PCI ASV. 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.

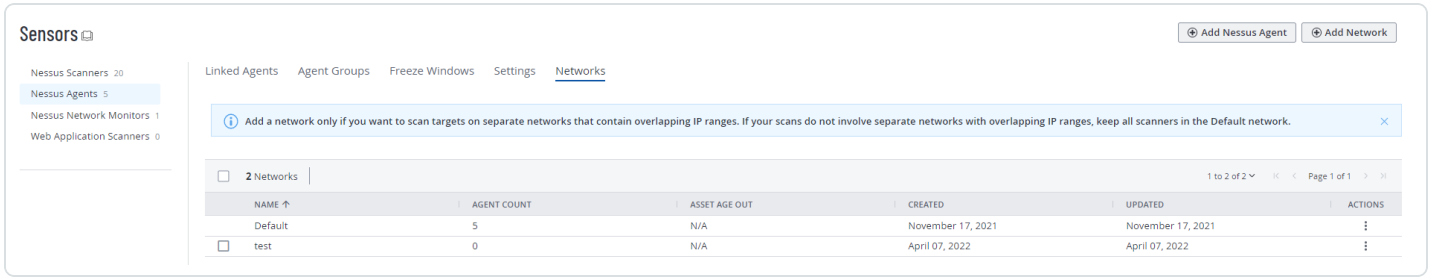
  You can view scanners in the default network, but you cannot add or remove scanners from the default network. If you remove a scanner or scanner group from a custom network, or if you delete a custom network, Tenable PCI ASV returns the scanner or scanner groups to the default network. Imported scans always belong to the default network.

  > **Note:** Assets from AWS pre-authorized scanners can only appear in the *Default* network.

  > **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: Any scanner that scans an asset that is not in the same network as the scanner will create a duplicate asset record. Therefore, you need to ensure that any new scanner or scanner group is part of the correct network before you begin scanning.



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 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. Click the **Networks** tab.

   The list of networks appears.

5. Click ⊕ **Add Network**.

   The **Settings** page appears.

6. Type a name for the network.

7. (Optional) Type a description for the network.

8. (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 PCI ASV 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 PCI ASV 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.

9. In the lower-right corner, click **Create**.

   Tenable PCI ASV 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 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. Click the **Networks** tab.

   The list of networks appears.

5. In the **Networks** table, click the network to edit.

   The **Network Details** page appears with the **Settings** tab active.

6. Make changes to your network details:

   a. Edit the network **Name** or **Description**. The name can contain any alphanumeric and special characters except < and >.

   b. Turn on **Asset Age Out** to permanently delete network assets that have not been seen on a scan for a specific number of days.

   c. In the text box that appears, type the number of days. The minimum value is 14 and the maximum value is 365.

      Caution: When you enable and save this option, Tenable PCI ASV 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.

7. Click **Save**.

   Tenable PCI ASV 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 PCI ASV 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 PCI ASV 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 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. Click the **Networks** tab.

   The list of networks appears.

5. In the networks table, click the network you want to add a scanner or scanner group to.

   The **Settings** page appears.

6. In the left navigation list, click **Manage Scanners**.

   A list of **Available Scanners to Add** and **Member Scanners in Network** appear.

7. In the row of the scanner or scanner group you want to add to the network, click the ⊕ button.

   Tenable PCI ASV determines whether there are any scanner group conflicts:

   If no conflicts are present, Tenable PCI ASV adds the scanner or scanner group to the network and moves it to the Member Scanners table.

   If any conflicts are present, Tenable PCI ASV 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 PCI ASV 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 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. Click the **Networks** tab.

   The list of networks appears.

5. In the networks table, click the network where you want to remove a scanner or scanner group.

   The **Settings** page appears.

6. In the left navigation plane, click **Manage Scanners**.

   A list of **Available Scanners to Add** and **Member Scanners in Network** appear.

7. In the row of the scanner or scanner group you want to remove from the network, click the ✕ button.

   Tenable PCI ASV 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 PCI ASV 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 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. 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 PCI ASV 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 PCI ASV 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 PCI ASV 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. 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. Click the **Nessus Agents** tab.

   The list of agents appears and **Linked Agents** is selected in the drop-down box.

5. 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**.

6. In the agent table header, select the check box to select the entire page.

   The action bar appears at the bottom of the page.

7. In the action bar, click the **Add selected to network**.

   The **Add to Network** plane appears.

8. In the drop-down, select the network to which you want to add the agent or agents.

9. Click **Assign**.

   Tenable PCI ASV 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 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. 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 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. Click the **Networks** tab.

   The list of networks appears.

5. 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.

6. Click **Move assets**.

   The **Move Assets** page appears.

7. In the **Source Network** drop-down box, select the network you want to move an asset or assets to.

8. 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 PCI ASV shows the asset or assets that match your search criteria.

9. 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV selects all assets in the source network.

  c. In the action bar, click the button.

     Tenable PCI ASV 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 Tenable Vulnerability Management 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 PCI ASV 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 view manually deleted assets, see View Deleted Assets.

To delete assets manually:

- Delete an individual asset. For more information, see Delete Assets.
- Delete multiple assets in a network in the classic interface. For more information, see Delete Assets from a Network (Classic Interface).
- Delete multiple assets using the Tenable PCI ASV API. For more information, see the Tenable Developer Portal.

Delete Assets Automatically

If you automatically delete assets in a network, Tenable PCI ASV 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 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. Click the **Networks** tab.

   The list of networks appears.

5. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

6. 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.

7. In the **Name** box, type a name for the export file.

8. 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 PCI ASV 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.

9. (Optional) Deselect any fields you do not want to appear in the export file.
10. In the **Expiration** box, type the number of days before the export file expires.

    Note: Tenable PCI ASV allows you to set a maximum of 30 calender days for export expiration.

11. (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.

12. (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 PCI ASV sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

13. Click **Export**.

    Tenable PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

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

14. 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 PCI ASV 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 PCI ASV API.
- Tenable PCI ASV 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 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. Click the **Networks** tab.

   The list of networks appears.

5. 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 PCI ASV deletes the network.

Linked Scanners

After you install a Tenable Nessus scanner, Tenable Nessus Network Monitor instance, Tenable Web App Scanning sensor, or Tenable Nessus Agent sensor, you can link it to Tenable Vulnerability Management.

Before you can use linked scanners in Tenable PCI ASV scans, you must:

1. Install the appropriate Tenable product on the sensor or the host you want to scan.

Sensor Type	More Information
Tenable Nessus Agent	• Environments • Install Tenable Nessus Agent in the *Tenable Nessus Agent Deployment and User Guide*
Tenable Nessus Network Monitor	• Environments • Install Tenable Nessus Network Monitor in the *Tenable Nessus Network Monitor User Guide* • Deploy or Install Tenable Container Security + Tenable Nessus 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 PCI ASV.

View Linked Scanners

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

To view your linked scanners:

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

   The left navigation plane appears.

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

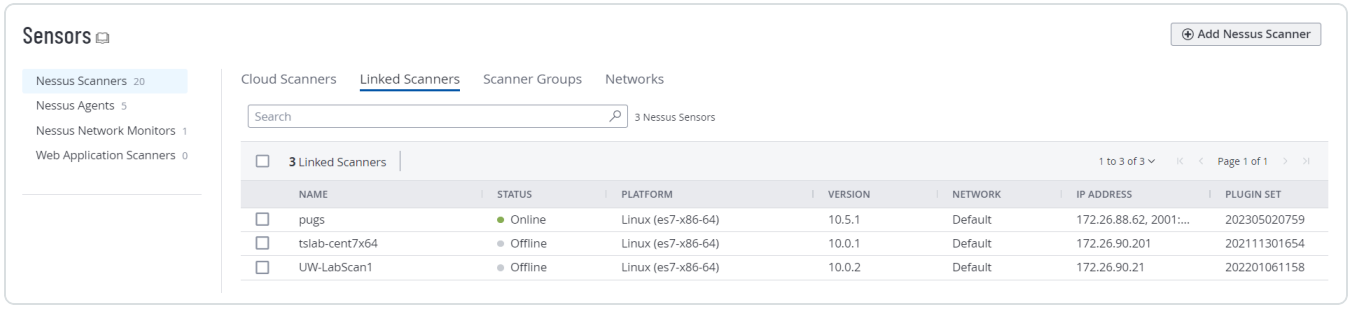
   The **Settings** page appears.

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. To view a different type of linked scanners, in the top navigation bar, click the type of linked scanners you want to view.

   Tenable PCI ASV 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 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. Click the row of the scanner you want to rename.

   The scanner **Details** page appears.

5. Click the ✎ button next to the scanner name.

6. Edit the scanner name.

7. Click the ✓ button next to the scanner name.

   Tenable PCI ASV 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 PCI ASV, 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.

To download logs from a linked scanner in Tenable PCI ASV:

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. In the linked scanners table, click the scanner for which you want to download logs.

   The details page for that scanner appears.

5. Click the **Logs** tab.

   A table shows any previously downloaded logs.

6. 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 PCI ASV requests the logs from the scanner the next time it checks in, which may take several minutes.

7. 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 PCI ASV 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 PCI ASV 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 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. 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 Nessus Network Monitor linked scanners, click the **Nessus Network Monitors** tab.

     A table with all your Tenable Nessus 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.

5. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

6. 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.

7. In the **Name** box, type a name for the export file.
8. 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 PCI ASV 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.

9. In the **Expiration** box, type the number of days before the export file expires.

   Note: Tenable PCI ASV allows you to set a maximum of 30 calender 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 PCI ASV 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 PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

    When processing completes, Tenable PCI ASV 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**.

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 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) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

5. In the linked scanners table, click the linked scanner for which you want to export details.

   The **Details** page appears.

6. 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.

7. In the **Name** box, type a name for the export file.
8. 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 PCI ASV 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.

9. (Optional) Deselect any fields you do not want to appear in the export file.
10. 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 calender days for export expiration.

11. (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.

12. (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 PCI ASV sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

13. 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.

14. 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 PCI ASV	The scanner requests differential updates from Tenable PCI ASV 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 PCI ASV).

Scanner Groups

You can use scanner groups to organize and manage the scanners linked to your Tenable PCI ASV 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.

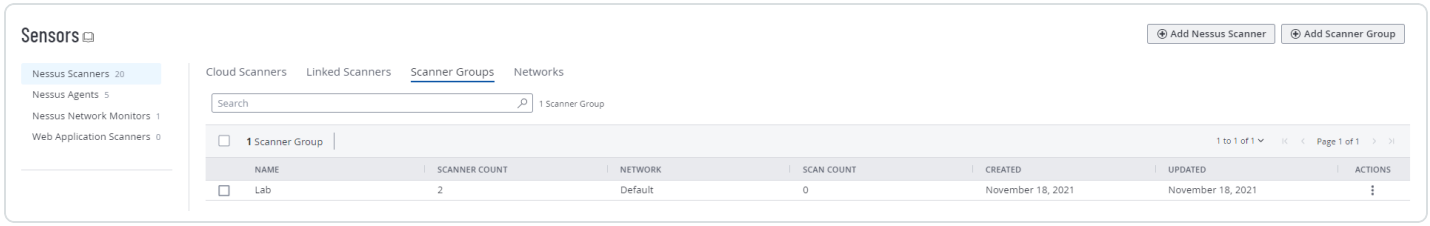
When you create a scan, you can select the scanner group to use to launch the scan. Alternatively, you can select **Auto-Select** to enable scan routing for the scan, which assigns scans to scanners based on the targets configured in scanner groups.

Tenable PCI ASV determines which scanner in a scanner group to use based on the following criteria:

- The scanner is active and has communicated to Tenable PCI ASV 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 PCI ASV 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 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. In the drop-down box, select **Scanner Groups**.

   The list of existing scanner groups you have permission to use or manage appears.

5. Click ⊕ **Add Scanner Group**.

   The **Add Scanner Group** plane appears.

6. In the **Group Name** field, type a name for the 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. (Optional) Configure user permissions for a scanner group.

   By default, in any new scanner group, Tenable PCI ASV assigns the system-generated **All Users** group **Can Use** permissions.

9. 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 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. In the drop-down box, select **Scanner Groups**.

   The list of existing scanner groups you have permission to use or manage appears.

5. (Optional) Search the table for the group you want to modify. For more information, see Tenable Vulnerability Management Tables.

6. 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.

7. Click **Edit**.

   The **Edit Scanner Group** plane appears.

8. Modify any of the following settings:

Setting	Action

Name	Type a new name.
User and Group Permissions	Configure user permissions for the scanner group.

9. (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.

10. 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 PCI ASV 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 Tenable Vulnerability Management 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 PCI ASV adds the scanner to the scanner group, and the **Group Details** page appears.
    If Tenable PCI ASV 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.

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 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 can view and edit the scanner group configuration.

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 PCI ASV 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 PCI ASV 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 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. In the drop-down box, select **Scanner Groups**.

   The list of existing scanner groups you have permission to use or manage appears.

5. 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.

6. In the confirmation window, click the **Delete** button.

   Tenable PCI ASV 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 PCI ASV cloud	no
Tenable Nessus sensor for Amazon Web Services (AWS)	no
Tenable Nessus Network Monitor (NNM)	no
Tenable Nessus Agent	no (see Agent Groups)

To add sensor to one or more scanner groups in the new interface:

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) Search for the scanner you want to add to a scanner group.

5. 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	a. In the scanner group table, do one of the following:

group or groups	• 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 PCI ASV 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.

6. Click **Save** to save your changes.

   Tenable PCI ASV 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 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. In the drop-down box, select **Scanner Groups**.

   The list of existing scanner groups you have permission to use or manage appears.

5. (Optional) Search the table for the group you want to modify. For more information, see Tenable Vulnerability Management Tables.

6. 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.

7. (Optional) Search for the sensor you want to remove. For more information, see Tenable Vulnerability Management Tables.

8. Select the sensor or sensors you want to remove:

9. 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.

10. In the confirmation window, click **Remove**.

    Tenable PCI ASV 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

To view sensors assigned to a scanner group in the new interface:

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. In the drop-down box, select **Scanner Groups**.

   The list of existing scanner groups you have permission to use or manage appears.

5. (Optional) Search the table for the group you want to view. For more information, see Tenable Vulnerability Management Tables.

6. 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.

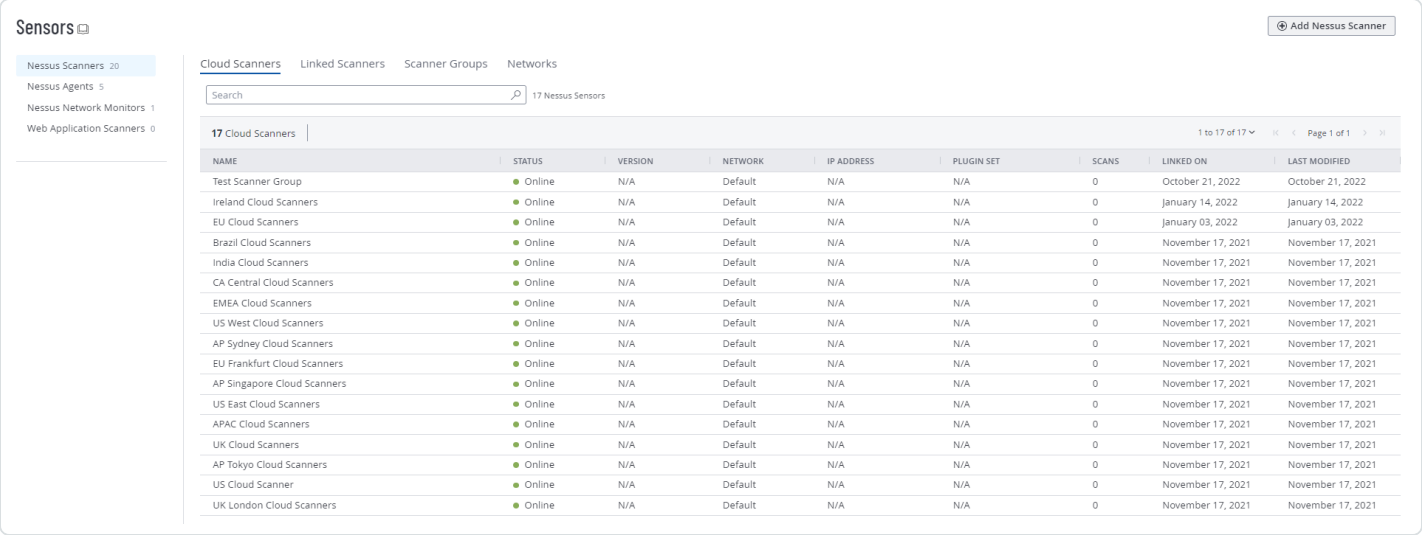
   Tenable PCI ASV shows a list of all scans the sensor is currently running.

Cloud Sensors

By default, Tenable provides regional cloud sensors for use in Tenable PCI ASV. 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.

Tenable PCI ASV



NAME	STATUS	VERSION	NETWORK	IP ADDRESS	PLUGIN SET	SCANS	LINKED ON	LAST MODIFIED
Test Scanner Group	Online	N/A	Default	N/A	N/A	0	October 21, 2022	October 21, 2022
Ireland Cloud Scanners	Online	N/A	Default	N/A	N/A	0	January 14, 2022	January 14, 2022
EU Cloud Scanners	Online	N/A	Default	N/A	N/A	0	January 03, 2022	January 03, 2022
Brazil Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
India Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
CA Central Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
EMEA Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
US West Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
AP Sydney Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
EU Frankfurt Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
AP Singapore Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
US East Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
APAC Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
UK Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
AP Tokyo Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
US Cloud Scanner	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021
UK London Cloud Scanners	Online	N/A	Default	N/A	N/A	0	November 17, 2021	November 17, 2021

Note: If you use cloud connectors, Tenable recommends allowlisting the IP addresses for the region in which the site resides.

Note: While these IP addresses are for outbound requests, they are also 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*.

Beginning on **March 16, 2024** the following **me-central-1** ranges will be available for use:

- 51.112.93.0/24
- 2406:da17:524:dd00::/56

Beginning on **March 20, 2024** the following **us-west-2** ranges will be available for use:

- 35.93.174.0/24

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
us-east-1	34.201.223.128/25 44.192.244.0/24 54.175.125.192/26	2600:1f18:614c:8000::/56
us-east-2	13.59.252.0/25 18.116.198.0/24	2600:1f16:8ca:e900::/56

Sensor Region	IPv4 Range	IPv6 Range
	3.132.217.0/25	
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	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

Tip: Add the following for internal scanner or agent communications:

- 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

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)

Note: If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Nessus Agents, Tenable Web App Scanning scanners, or Tenable Nessus Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.

Sensor Security

See the following sections to learn more about sensor security and encryption when using the Tenable PCI ASV platform:

- Sensor Overview
- Linking Keys
- Data Encryption

Sensor Overview

Sensors access Tenable PCI ASV through the following site: `<port> - sensor.cloud.tenable.com:443`. All sensors (Tenable Nessus scanners, Tenable Nessus Agents, Tenable Nessus Network Monitor) need access to `cloud.tenable.com:443`.

> **Note:** If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Nessus Agents, Tenable Web App Scanning scanners, or Tenable Nessus 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 Nessus Network Monitor - you need to access their respective user interfaces for initial setup:

- Tenable Nessus — `<IP>:8834`
- Tenable Nessus Network Monitor — `<IP>:8835`

  > **Note:** If you are deploying Tenable Nessus or Tenable Nessus 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 PCI ASV.

Nessus sensors connect to the Tenable PCI ASV platform after securely authenticating and linking to Tenable PCI ASV (see Linking Keys in the following section to learn more). Once linked, Tenable PCI ASV manages all updates to ensure the sensors are always up to date.

Sensors always initial the traffic between sensors and Tenable PCI ASV, 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 Nessus Agent for NIAP Compliance
- Configure Tenable Nessus Network Monitor for NIAP Compliance

Linking Keys

Tenable PCI ASV 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 Nessus Network Monitor) and Tenable PCI ASV.

When the Tenable PCI ASV 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 PCI ASV allows the sensor to link.

Upon linking, Tenable PCI ASV 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 PCI ASV, such as scan results or sensor health data.

- **Sensor-to-platform job communication**

  Sensors check in to Tenable PCI ASV every so often (different sensor types have different check-in frequencies). When a scan job is launched, Tenable PCI ASV 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 PCI ASV encrypts all data in all states with at least one level, using no less than AES-256:

- Data at rest — Tenable PCI ASV 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 PCI ASV uses TLS version 1.2+ with a 4096-bit key to encrypt data during transportation (including internal transports).
- Backed up or replicated data — Tenable PCI ASV 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 PCI ASV 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 PCI ASV.

Linking a sensor to Tenable PCI ASV represents a one-time event in managing a sensor, unless you remove the sensor. After you link the sensor, the sensor connects to Tenable PCI ASV using unique credentials.

Once you copy the linking key in Tenable PCI ASV, you must paste the linking key in the appropriate location of the sensor user interface (for example, the Tenable Nessus Agent CLI or the Tenable Nessus Network Monitor **Cloud Settings** section). Expand the following sections for specific details.

Note: If you use domain allowlists for firewalls, Tenable recommends adding *.cloud.tenable.com (with the wildcard character) to the allowlist. This ensures communication with sensor.cloud.tenable.com, which the scanner uses to communicate with Tenable PCI ASV. If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Nessus Agents, Tenable Web App Scanning scanners, or Tenable Nessus 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 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. Then:

   To link a Tenable Nessus Agent sensor, click the **Nessus Agents** tab.

   a. Click ⊕ **Add Agent**.

      The **Add Agent** plane appears.

   b. Do one of the following:

      - To install and link Tenable Nessus Agent manually:

        a. In the **Linking Key** section, click **Copy**.

           A **Linking key copied to clipboard** confirmation message appears.

        b. Access the Tenable Nessus Agent instance that you want to link to Tenable PCI ASV.

        c. Use the copied linking key in the Tenable Nessus Agent CLI to link the sensor. For more information, see Install Tenable Nessus Agent in the *Tenable Nessus Agent Deployment and User Guide*.

      - (Windows only) To use a single command to install and link Tenable Nessus 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 PCI ASV, 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-
           installscript.
           ps1"; & “./ms-install-script.ps1” -key “{linkingKey}” -type
           “{sensorType}” -name “<agent name>” -groups “<list of groups>“;
           Remove-Item -Path “./ms-install-script.ps1”
           ```

        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 Nessus Agent installs on your Windows machine, links to your instance of Tenable PCI ASV, and updates the agent name and agent group if necessary.

- (Linux only) To use a single command to install and link Tenable Nessus 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 PCI ASV, 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
```

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 Nessus Agent installs on your Linux machine, links to your instance of Tenable PCI ASV, and updates the agent name and agent group if necessary.

To link an Tenable Nessus 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 Nessus Network Monitor instance that you want to link to Tenable Vulnerability Management.

d. Use the copied linking key in the Tenable Nessus 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 PCI ASV.

     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 PCI ASV, 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"
        ```

     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 PCI ASV, 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 PCI ASV, 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
```

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 PCI ASV, 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 PCI ASV.

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 PCI ASV (including disabling or re-enabling the sensor link).
- Select the sensor when configuring Tenable PCI ASV scans.

Regenerate a Linking Key

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

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

Under certain circumstances, you may need to regenerate the linking key for your Tenable PCI ASV 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 PCI ASV, because the linking key is only used to establish the initial link. After you link a sensor, the sensor connects to Tenable PCI ASV 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 PCI ASV instance uses a single linking key for all sensor types. If you regenerate the linking key while working with one type of sensors (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 implementation for scripts involving all types of sensors.

Note: To learn more about Tenable PCI ASV linking keys, see Sensor Security.

To regenerate a linking key for your Tenable PCI ASV instance:

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. Click any sensor type tab (for example, **NNM**).

   The appropriate sensor page appears.

5. Click the ⊕ **Add [Sensor Type]** button (for example, **Add NNM**).

   The appropriate sensor plane appears (for example, **Add NNM**).

6. In the **Add [Sensor Type]** plane, click the **Regenerate** button.

   A confirmation window appears.

7. 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: 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 **Sensors** page, you can view your linked sensors: Tenable PCI ASV cloud sensors, your Tenable Nessus Scanners, Tenable Nessus Agents, Tenable Nessus 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 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.

   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
   - **Nessus Network Monitors**
   - **Web Application Scanners** — Linked Tenable Web App Scanning Scanners, Tenable Web App Scanning 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.

Column	Description
Name	The name of the sensor.
Created	The date on which the sensor group was created.
IP Address	The IP address of the sensor.
Last Modified	The date on which the sensor was last modified.
Linked On	The date on which the sensor was linked to Tenable Vulnerability Management.
Network	The network associated with the sensor or sensor group.
Platform	The platform associated with the sensor.
Plugin Set	The plugin set of the sensor.
Scan Count	The number of scans that the sensor or sensor group is currently running.
Scanner Count	The number of scanners in the group.
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.
Actions	The actions that you can perform for each 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 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. Click the sensor type tab you want to view.

   A table of sensors appears.

5. 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 PCI ASV. For more information, see Cloud Sensors.
   - In the drop-down box, click the **Linked Scanners** tab to view on-premises scanners linked to Tenable PCI ASV. For more information, see Linked Scanners.

6. 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 Nessus Network Monitor
- Tenable Nessus for Amazon Web Service (AWS)

To edit sensor settings in the new interface:

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. Click the appropriate sensor type tab.

   The sensor table appears.

5. 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 PCI ASV. For more information, see Cloud Sensors.
   - In the drop-down box, select the **Linked Scanners** tab to view scanners linked to Tenable PCI ASV. For more information, see Linked Scanners

6. 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.

7. Click the **Settings** tab.

   The sensor settings appear.

8. 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 PCI ASV.
Software Update Type	NNM (5.6.1 and later only)	Specifies which components, if any, you want Tenable Nessus Network Monitor to automatically update. **All components** includes web server, HTML client, plugins, and engine.
Updates instances every (minutes)	AWS	Specifies the frequency, in minutes, that you want the AWS sensor to report information to Tenable PCI ASV about the instances it has access to.

9. 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 PCI ASV 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 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. Click the appropriate sensor type tab.

   A sensors table appears.

5. If the sensor is a **Nessus Scanner**, click the **Linked Scanners** tab to view on-premises scanners linked to Tenable PCI ASV. For more information, see Linked Scanners.

6. 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.

7. Click the **Permissions** tab.

   Note: By default, any user in your Tenable PCI ASV instance can use the scanner.

8. 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 PCI ASV 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.

9. 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 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. Click the appropriate sensor type tab.

   The sensors table appears.

5. (Optional) If the sensor is a **Nessus Scanner**, select **Linked Scanners** in the drop-down box to view on-premises scanners linked to Tenable PCI ASV. For more information, see Linked Scanners.

6. 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.

7. Do one of the following:

   - To enable a sensor, click the **Enable** button.
   - To disable a sensor, click the **Disable** button.

   Tenable PCI ASV 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 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. Click the appropriate sensor type tab.

   The sensor table appears.

5. For **Nessus Scanners**, select **Linked Scanners** in the drop-down box to view on-premises scanners linked to Tenable PCI ASV. For more information, see Linked Scanners.

6. 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.

7. Click **Delete** to confirm the removal.

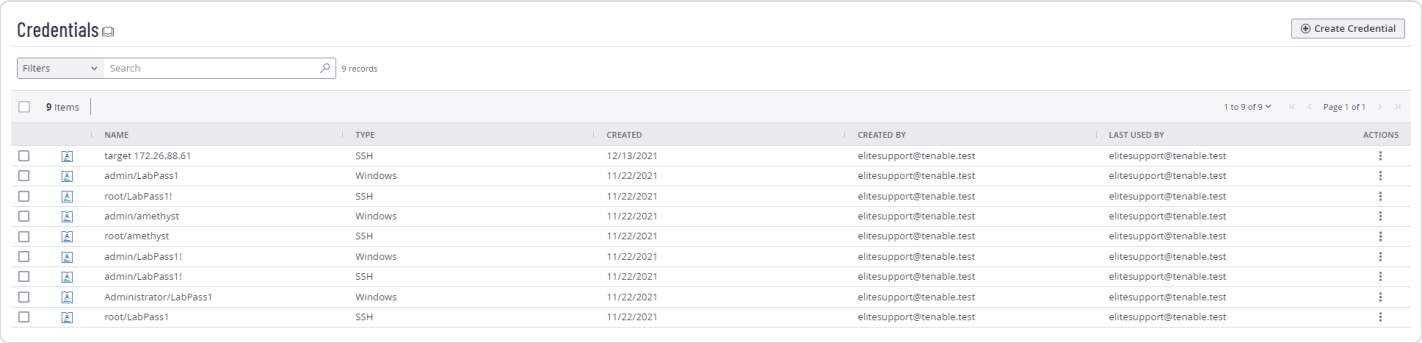
   Tenable PCI ASV removes the sensor from the list.

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 PCI ASV 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 (Tenable Vulnerability Management) or Configure Credentials Settings in Tenable Web App Scanning.

To create a managed credential:

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

   The left navigation plane appears.

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

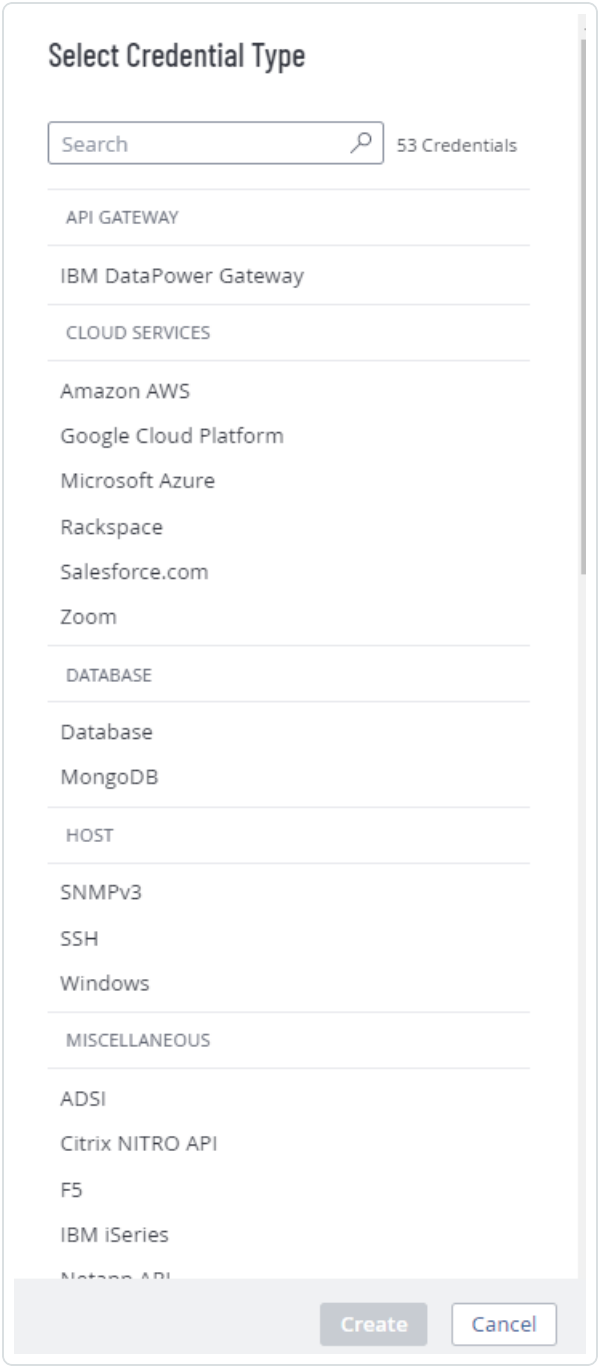
   The **Settings** page appears.

3. Click the **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

4. In the upper-right corner of the page, click the ⊕ **Create Credential** button.

   The **Select Credential Type** plane appears.



5. 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.
6. In the **Title** box, type a name for the credential.

7. (Optional) In the **Description** box, type a description for the credential.
8. 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).
9. Add user permissions.
10. Click **Save**.

    Tenable PCI ASV 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 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 **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

4. Filter or search the credentials table for the credential you want to edit. For more information, see Tenable Vulnerability Management Tables.

5. In the credentials table, click the name of the credential you want to edit.

   The credential settings plane appears.

6. 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.

7. 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 PCI ASV 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 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 **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

4. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

5. 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.

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 credentials.

	Note: If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable PCI ASV 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.

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 PCI ASV allows you to set a maximum of 30 calender 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 PCI ASV 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 PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

    When processing completes, Tenable PCI ASV 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 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 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 **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

4. Filter or search the credentials table for the credential you want to delete. For more information, see Tenable Vulnerability Management Tables.

5. In the table, roll over the credential you want to delete.

   The action buttons appear in the row.

6. Click the 🗑 button.

   The **Confirm Deletion** window appears.

7. 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.

For more information on exclusions, see the following topics:

- Create an Exclusion
- Edit an Exclusion
- Import an Exclusion
- Export an Exclusion
- Delete an Exclusion
- Exclusion Settings

Create an Exclusion

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

Note: Exclusions do not apply to Agent scans.

To create an exclusion:

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

   The left navigation plane appears.

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

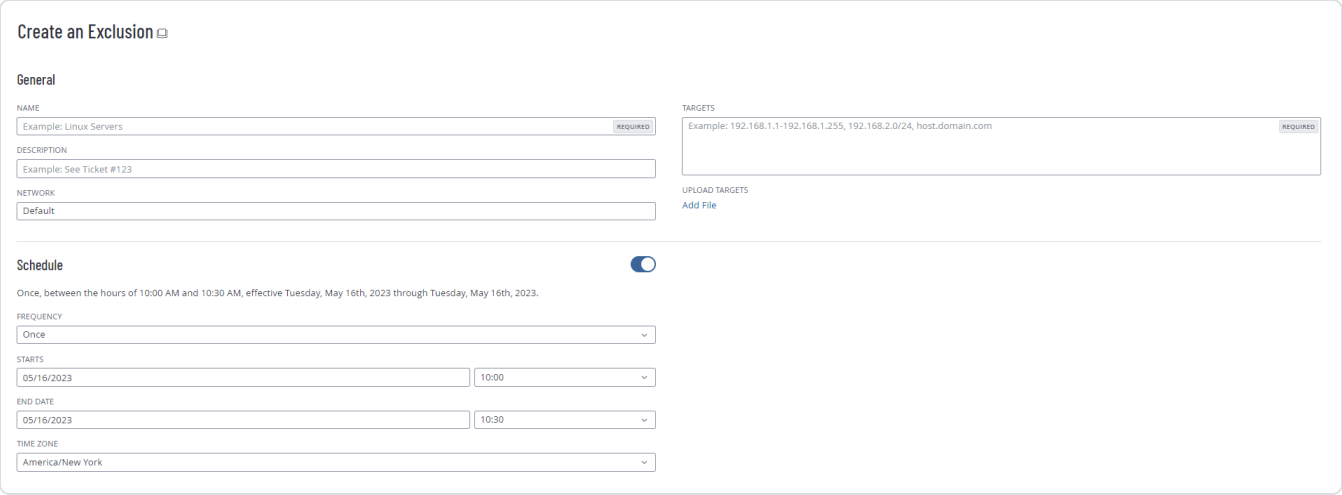
   The **Settings** page appears.

3. Click the **Exclusions** tile.

   The **Exclusions** page appears.

4. In the upper-right corner of the page, click the ⊕ **Create Exclusion** button.

   The **Create an Exclusion** page appears.



5. Set the exclusion settings.

6. Click **Save**.

   Tenable PCI ASV 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 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 **Exclusions** tile.

   The **Exclusions** page appears.

4. In the exclusions table, click the exclusion you want to edit.

   The **Update an Exclusion** page appears.

5. Edit the exclusion settings.

6. Click **Save**.

   Tenable PCI ASV 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 PCI ASV 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 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 **Exclusions** tile.

   The **Exclusions** page appears.

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 PCI ASV 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 PCI ASV cannot recognize.

This file is composed of a header and at least one line of data. Each line in the file must be separated by 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 table below.

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 alpha-numeric characters or symbols.	Yes
description	A description for the exclusion.	Yes
members	The target or targets where you want the scan exclusion to apply.	Yes

	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) • 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 PCI ASV uses as the creation date for the imported exclusion.	No
last_ modification_ date	The Unix timestamp that Tenable PCI ASV 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,Exclusion Rule
2,workstations,192.0.257-192.0.267,,
```

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 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 **Exclusions** tile.

   The **Exclusions** page appears. This page displays a list of exclusions configured on your Tenable PCI ASV account.

4. (Optional) Refine the table data. For more information, see Tenable PCI ASV Workbench Tables.

5. 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.

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 exclusions. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable PCI ASV 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.

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 PCI ASV allows you to set a maximum of 30 calender 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 PCI ASV 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 PCI ASV begins processing the export. Depending on the size of the exported data, Tenable PCI ASV may take several minutes to process the export.

    When processing completes, Tenable PCI ASV 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 from the Exports page.

Delete an Exclusion

Required Tenable Vulnerability Management User Role: Scan Manager or Administrator

To delete an exclusion:

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 **Exclusions** tile.

   The **Exclusions** page appears.

4. 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.

5. In the confirmation window, click **Delete**.

   Tenable PCI ASV 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.
Targets	Specifies targets that you want excluded from scans. Add targets as host names or IP ranges, separated by commas. You cannot use the **Targets** setting if you already specified targets with the **Upload Targets** setting. **Tip:** The **Targets** setting supports excluding specific ports per IP address by typing IP:Port entries.
Network	Specifies the network that the targets belong to: either **Default** or a custom 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.
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**.

Setting	Description
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 PCI ASV 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 PCI ASV 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

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.

Container Security Connectors

For information about Tenable Container Security connectors, see Configure Connectors to Import and Scan Images.

Supported Plugins

To view the supported plugins for AWS and Azure, see the Tenable Plugins page. Use the filter **Supported Sensors** to view the Frictionless Assessment plugins.

Amazon Web Services Connector

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

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.

To assess AWS assets for vulnerabilities, Tenable recommends that you use Frictionless Assessment to assess for vulnerabilities in the cloud. 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 and assess for vulnerabilities using Frictionless Assessment The cloud connector discovers AWS assets and collects an	• Keyless authentication with Frictionless Assessment

inventory of data points on your AWS EC2 instances, then assesses the hosts for vulnerabilities in the cloud, rather than running plugins locally on the host. For more information, see Frictionless Assessment for AWS .	enabled
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.

Frictionless Assessment for AWS

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

With Frictionless Assessment, Tenable Vulnerability Management discovers and collects an inventory of data points on your Amazon Web Services (AWS) EC2 instances. Then, for EC2 instances with an AWS tag that you specify for Frictionless Assessment, Tenable Vulnerability Management assesses the hosts for vulnerabilities in the cloud, rather than running plugins locally on the hosts.

Note: Frictionless Assessment reports on Asset information even if it is in a "stopped" state. The AWS Systems Manager Agent (SSM Agent), which Frictionless Assessment leverages to collect data from a host and create an inventory of data points on your AWS EC2 instances, also collects data even in "stopped" state.

Frictionless Assessment uses the AWS Systems Manager Inventory and AWS Systems Manager Agent (SSM Agent) to collect the required data. For more information on AWS configuration requirements, see Configure AWS for Frictionless Assessment.

You do not need to configure scanners, Tenable Nessus Agents, scans, or scan schedules to assess hosts with Frictionless Assessment.

Operating System Coverage

Frictionless Assessment has vulnerability coverage for EC2 instances created from the following Amazon Machine Images:

- Amazon Linux 1 / 2
- CentOS 6 / 7 / 8
- Red Hat 6 / 7 / 8
- SUSE Linux Enterprise Server (SLES) 11.4-15.2
- SUSE Linux Enterprise Desktop (SLED) 12-15.2
- Ubuntu 16.04 / 18.04 / 20.04
- Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022
- Windows 7, Windows 8, Windows 10, Windows 11

Licensing Considerations

In general in Tenable Vulnerability Management, assets count towards your license when they are assessed for vulnerabilities. Therefore, EC2 hosts that are assessed by Frictionless Assessment count against your license. For more information, see Licenses.

When you select AWS tags for hosts to be assessed by Frictionless Assessment, note that all hosts with any of those tags count towards your license. Hosts that are only discovered by the connector, and not assessed by Frictionless Assessment (for example, hosts that do not have a tag you selected for Frictionless Assessment), do not count towards your license.

Supported Regions

The following regions are supported for AWS Frictionless Assessment:

- `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)
- `eu-central-1`, EU (Frankfurt)
- `eu-west-1`, EU (Ireland)
- `eu-west-2`, EU (London)
- `eu-west-3`, EU (Paris)
- `sa-east-1`, South America (Sao Paulo)

Limitations

- Frictionless Assessment does not run informational plugins, run remote vulnerability plugins, or gather compliance data.
- A connector configured with Frictionless Assessment only supports one AWS account. If you want to assess hosts across multiple AWS accounts, you must configure a separate connector for each AWS account.
- You must use a single AWS tag key to identify the assets you want Frictionless Assessment to access.
- Tenable Vulnerability Management creates an AWS Systems Manager inventory association on your instance to collect inventory for Frictionless Assessment. However, AWS Systems Manager has a restriction that only one inventory association can be applied to an instance at a time, as described in the AWS Documentation. If you have an existing inventory association applied to your instance, remove it before configuring Frictionless Assessment. For more information, see the AWS Documentation.
- The limit for Frictionless Assessment scans is one per day, whereas existing Frictionless Assessment connectors created before May 1, 2023 transmit inventory data more frequently. Frictionless Assessment drops data exceeding the frequency limit and does not scan it.

  > **Note**: The limitation does not apply to Tenable Container Security, Agentless Assessment, or Tenable Nessus Agent-based inventory scans.

Get Started

1. Determine who in your organization has the appropriate AWS credentials to access the AWS console.
2. Depending on who has the AWS credentials, do one of the following:
    - If you are setting up the Tenable Vulnerability Management cloud connector *and* also have the appropriate AWS credentials for your organization:
        a. Ensure your AWS configuration meets the requirements for Frictionless Assessment, as described in Configure AWS for Frictionless Assessment.
        b. Create your AWS connector, as described in Create an AWS Connector for Frictionless Assessment.
    - If you are setting up the Tenable Vulnerability Management cloud connector, but someone *other than you* in your organization has the necessary AWS credentials:
        a. The person with AWS credentials must ensure the AWS configuration meets the requirements for Frictionless Assessment, as described in Configure AWS for Frictionless Assessment.
        b. The person with AWS credentials must manually configure AWS roles and policies for use with Frictionless Assessment.
        c. Create your AWS connector, as described in Create an AWS Connector with Keyless Authentication for Frictionless Assessment.
3. To delete an AWS cloud connector, see Delete a Connector.
4. If you delete a connector, manually delete the CloudFormation stack in AWS, as described in Manually Delete Connector Artifacts in AWS.

Configure AWS for Frictionless Assessment

> Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

Frictionless Assessment leverages the AWS Systems Manager Inventory and AWS Systems Manager Agent (SSM Agent) to collect data from a host and create an inventory of data points on your AWS EC2 instances. You do not need to configure scanners, Tenable Nessus Agents, scans, or scan schedules to assess hosts with Frictionless Assessment.

If you have access to your organization's AWS console, ensure your AWS configuration meets the following requirements before creating the Tenable Vulnerability Management cloud connector.

If someone other than you has access to your organization's AWS console, ensure they configure AWS to meet the following requirements before you create the Tenable Vulnerability Management cloud connector.

To configure your AWS environment for use with Frictionless Assessment:

1. Set up AWS Systems Manager for your account, as described in the AWS Systems Manager documentation.
2. Ensure that you have access to AWS Systems Manager Inventory. For more information, see *AWS Systems Manager Inventory* in the AWS Systems Manager documentation.
3. Ensure your EC2 instances have the SSM Agent installed.
    - Most EC2 instance distributions come with SSM Agent preinstalled. For more information, see *About SSM Agent* in the AWS Systems Manager documentation.
    - If your distribution does not have SSM installed, manually install the SSM Agent as described in the AWS Systems Manager documentation.
4. Ensure the target EC2 instances you want to assess with Frictionless Assessment are tagged with a single AWS tag key. For example, you can use the tag key *Tenable*.

Later, you will select this AWS tag key to identify instances you want to assess with Frictionless Assessment.

5. Tenable Vulnerability Management creates an AWS Systems Manager inventory association on your instance to collect inventory for Frictionless Assessment. However, AWS Systems Manager has a restriction that only one inventory association can be applied to an instance at a time, as described in the AWS Documentation. If you have an existing inventory association applied to your instance, remove it before configuring Frictionless Assessment. For more information, see the AWS Documentation.

What to do next:

- Depending on who has the AWS credentials for your organization, do the following:
    - If you are setting up the Tenable Vulnerability Management cloud connector *and* also have the appropriate AWS credentials for your organization:
        - Create your AWS connector, as described in Create an AWS Connector for Frictionless Assessment.

Create an AWS Connector for Frictionless Assessment

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

Required User Role: Administrator

When you configure an Amazon Web Services (AWS) cloud connector with keyless authentication for Frictionless Assessment, Tenable Vulnerability Management uses a Cloud Formation template (CFT) to configure the required roles and policies for your AWS account automatically. This configuration sets up the regular cloud connector and Frictionless Assessment.

To use Frictionless Assessment with your AWS connector, you must enter an AWS tag key to identify hosts to be assessed by Frictionless Assessment. If you do not enter a tag key, the connector functions as discovery-only and assets are not assessed for vulnerabilities.

Note: Create a separate cloud connector for each AWS account that owns hosts you want to evaluate for Frictionless Assessment.

Before you begin:

- Ensure that your AWS configuration meets the requirements for Frictionless Assessment, as described in Configure AWS for Frictionless Assessment.
- For best results, ensure that this is a new AWS cloud connector setup. If you have existing AWS cloud connectors configured, delete the existing *tenableio-connector* IAM role before creating the new AWS cloud connector.

  Note: To use Tenable Cloud Security Preview or Tenable Cloud Security, you must update or create new roles that support Tenable Cloud Security. Tenable Vulnerability Management cloud connector roles do not support Agentless Assessment.

- In another window or tab of the same browser with which you are accessing Tenable Vulnerability Management, log in to the AWS console with the AWS account that you want to target with Frictionless Assessment.

Create the AWS Frictionless Assessment connector and CFT:

1. Log in to your Tenable Vulnerability Management user interface and go to **Settings > Cloud Connectors**.
2. Click **Create Cloud Connector**.

   The **Select a Cloud Connector** panel appears.
3. In the **Cloud Connectors** list, select **Frictionless Assessment**.

   The **Connector Setup** pop-up appears.
4. In the **Cloud Provider** step, select **AWS** and enter a **Connector Name**.

   Click **Next**.
5. In the **Enable Features** step, ensure the check box to **Identify vulnerabilities using frictionless assessment** is selected.

   Click **Next**.
6. In the **Configuration** step, select the target parameters:
   a. Enter the **Account ID** to target.
   b. Select a tag by providing the **Tag** key and value:
      i. In the **Tag Key** box, type the AWS tag key.

         For example, in the AWS tag *Tenable:FA*, the tag key is *Tenable*.
      ii. In the **Tag Value** box, do one of the following:

         For example, in the AWS tag *Tenable:FA*, the tag value is *FA*.

> **Tip:** You can only specify one tag for AWSFrictionless Assessment.

> **Note:** The tag key and value are case sensitive and must match what is in AWS exactly.

> **Note:** To use Frictionless Assessment with your AWS connector, you must enter an AWS tag key to identify hosts to be assessed by Frictionless Assessment. If you do not enter a tag key, the connector functions as discovery-only and assets are not assessed for vulnerabilities.

c. Select the **Network** to target. You can select an existing network or create a new network using the **Network** drop-down menu. If you do not specify a network, your default network is selected.

Click **Next**.

7. In the **Apply Choices** step, click **Download and Finish**.

   The CFT downloads in .yml format, and the new connector shows on the **Cloud Connectors** page.

Deploy the connector using the CFT:

Deploy the CFT you downloaded in the previous section to your AWS accounts (for more information, see the AWS documentation).

If you need to deploy to more than one region, Tenable recommends deploying the template as a stack set (for more information, see the AWS stack set documentation).

What to do next:

- Create an AWS Connector with Keyless Authentication (Discovery Only) for your AWS account if you do not already have one. Your AWS account needs a keyless connector for Tenable Vulnerability Management to track asset states and asset terminations.

  > **Note:** The keyless connector needs to be set up for the same account that AWS Frictionless Assessment is set up for.

- Edit the AWS Frictionless Assessment connector's tags when needed. For more information, see Edit an AWS Frictionless Assessment Connector.
- View assets to see hosts discovered by the connector. Hosts found by an AWS connector using Frictionless Assessment appear with the source **SSM**.
- View vulnerabilities to see vulnerabilities identified by Frictionless Assessment.

Edit an AWS Frictionless Assessment Connector

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

You can edit the name, tags, and network of an Amazon Web Services (AWS) Frictionless Assessment connector.

Note: If you edit an AWS Frictionless Assessment connector's tags, you have to redeploy the connector to your AWS accounts to update the tag information in AWS.

To edit your AWS Frictionless Assessment connector:

1. Log in to your Tenable Vulnerability Management user interface and go to **Settings > Cloud Connectors**.
2. From the Cloud Connectors table, click the **AWS_FA** connector that you want to edit tags for.

   The **Edit** connector page appears.
3. Edit the connector:
   - To edit the connector name, click the **Connect Name** field and enter a new name.
   - To edit the connector tags, do the following:
     a. In the **Tag Key** box, type the AWS tag key.

        For example, in the AWS tag *Tenable:FA*, the tag key is *Tenable*.

     b. In the **Tag Value** box, do one of the following:

        For example, in the AWS tag *Tenable:FA*, the tag value is *FA*.

   Tip: You can only specify one tag for AWS Frictionless Assessment.

   Note: The tag key and value are case sensitive and must match what is in AWS exactly.

> **Note:** To use Frictionless Assessment with your AWS connector, you must enter an AWS tag key to identify hosts to be assessed by Frictionless Assessment. If you do not enter a tag key, the connector functions as discovery-only and assets are not assessed for vulnerabilities.

- To edit the change the network the connector is linked to, select an existing network or create a new network using the **Network** drop-down menu. If you do not specify a network, Tenable Vulnerability Management selects your default network.

4. Click the **Download CFT** button.

   > **Note**: If you edited the connector tags, the button shows as **Download CFT & Save**.

   The CFT downloads in .yml format and the **Cloud Connectors** page appears with the updated connector information.

5. If you edited the connector tags, redeploy the CFT to your AWS accounts (for more information, see the AWS documentation).

   If you need to deploy to more than one region, Tenable recommends deploying the template as a stack set (for more information, see the AWS stack set documentation).

Manually Delete Connector Artifacts in AWS

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

Required User Role: Administrator

After you delete your last AWS connector, Tenable Vulnerability Management triggers an automatic deletion of most AWS artifacts associated with the connector and the Frictionless Assessment configuration.

However, the CloudFormation stack or stack set is not automatically deleted. You must manually delete the CloudFormation stack or stack set in the AWS CloudFormation console.

Before you begin:

- Delete the AWS connector, as described in Delete a Connector.

To manually delete artifacts from the AWS connector:

- Delete the Tenable-created CloudFormation stack or stack set, as described in *Deleting a stack on the AWS CloudFormation console* in the AWS CloudFormation User Guide. The stack is a `.yml` file and has the same name as its associated connector.

Update AWS Frictionless Assessment Connectors to Detect Log4j

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

To ensure that your AWS Frictionless Assessment connectors can detect the Log4j vulnerability, update the **TenableInventoryCollection** script in each AWS region where the script is installed.

Note: If you have multiple AWS accounts, you need to complete the steps below for all the relevant regions within each account.

To update the AWS Frictionless Assessment connectors to detect Log4j:

1. Go to the Tenable Frictionless Downloads page and download the `TenableInventoryCollection-document-v2.json` file.
2. Log in to the AWS console.
3. Open the **Systems Manager**.
4. Click **Documents** > **Owned by me**.
5. Open the **TenableInventoryCollection** document.

   The `TenableInventoryCollection` **Description** page opens.
6. In the upper-right corner, click **Actions**.
7. Click **Create new version**.

   The new version's **Content** pane appears.
8. Select the **JSON** radio button.
9. Delete the contents in the box under **JSON**.
10. Copy and paste the contents of `TenableInventoryCollection-document-v2.json` in the box under **JSON**.

11. Below the content box, click **Create new version**.

    The **Documents** > **Owned by Amazon** page opens.

12. Go to the **Documents** > **Owned by me** page.
13. Open the **TenableInventoryCollection** document.
14. In the upper-right corner, click **Actions**.
15. Click **Set default version**.

    The **Set default version** page appears.

16. Set the **Version** value to **2** using the drop-down list.
17. Click **Set default version**.

> **Note:** To verify that the AWS region is updated to detect Log4j, open the **TenableInventoryCollection** document, go to the **Contents** tab, and search (**Ctrl + F**) for "log4j". If the code contains "log4j", it is updated.

AWS Cloud Connector (Discovery Only)

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.

> **Tip:** To configure an AWS connector with Frictionless Assessment, which allows you to assess EC2 instances for vulnerabilities without configuring agents or scans, see Frictionless Assessment for AWS.

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 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.

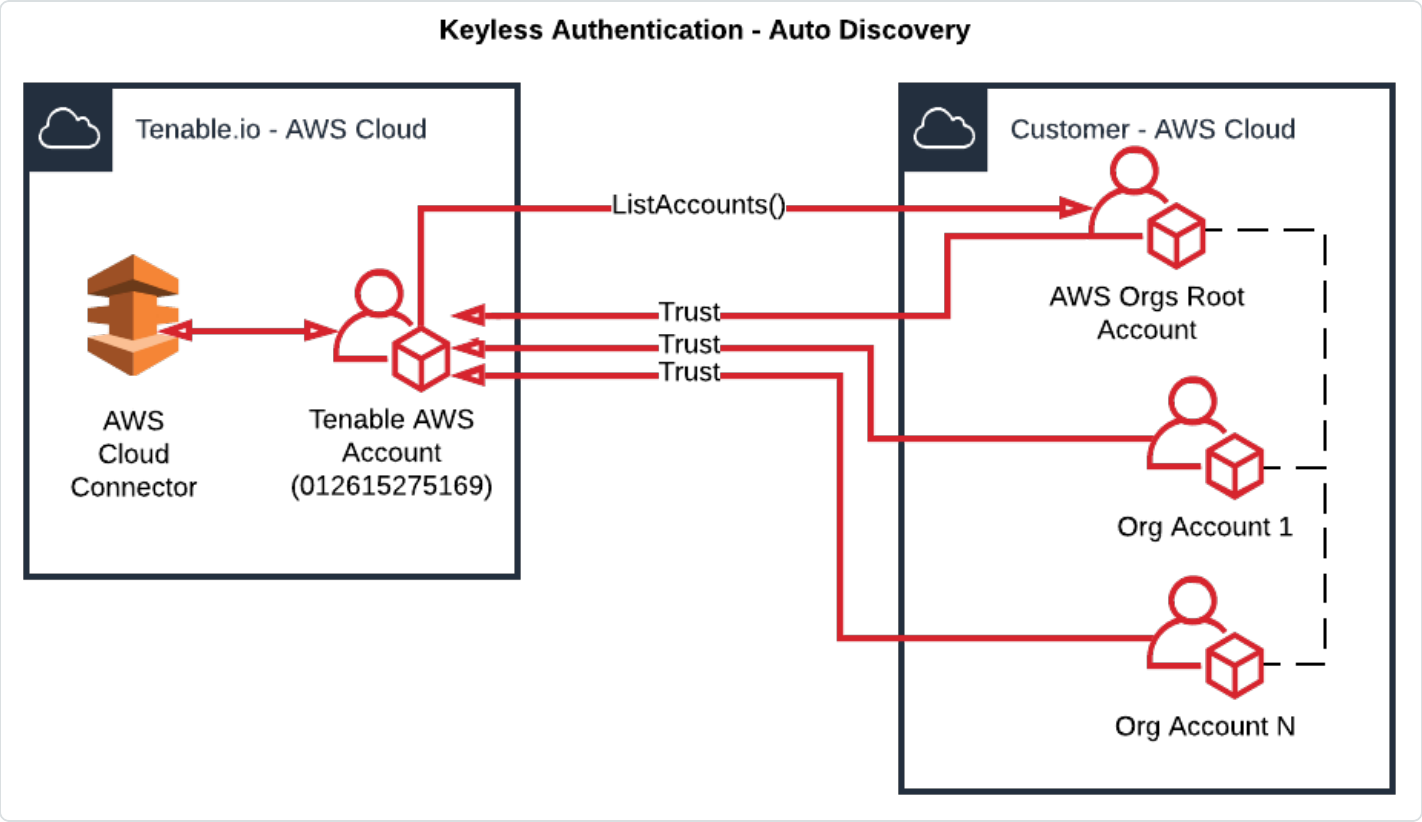
> **Tip:** To configure an AWS connector with Frictionless Assessment, which allows you to assess EC2 instances for vulnerabilities without configuring agents or scans, see Frictionless Assessment for AWS.

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

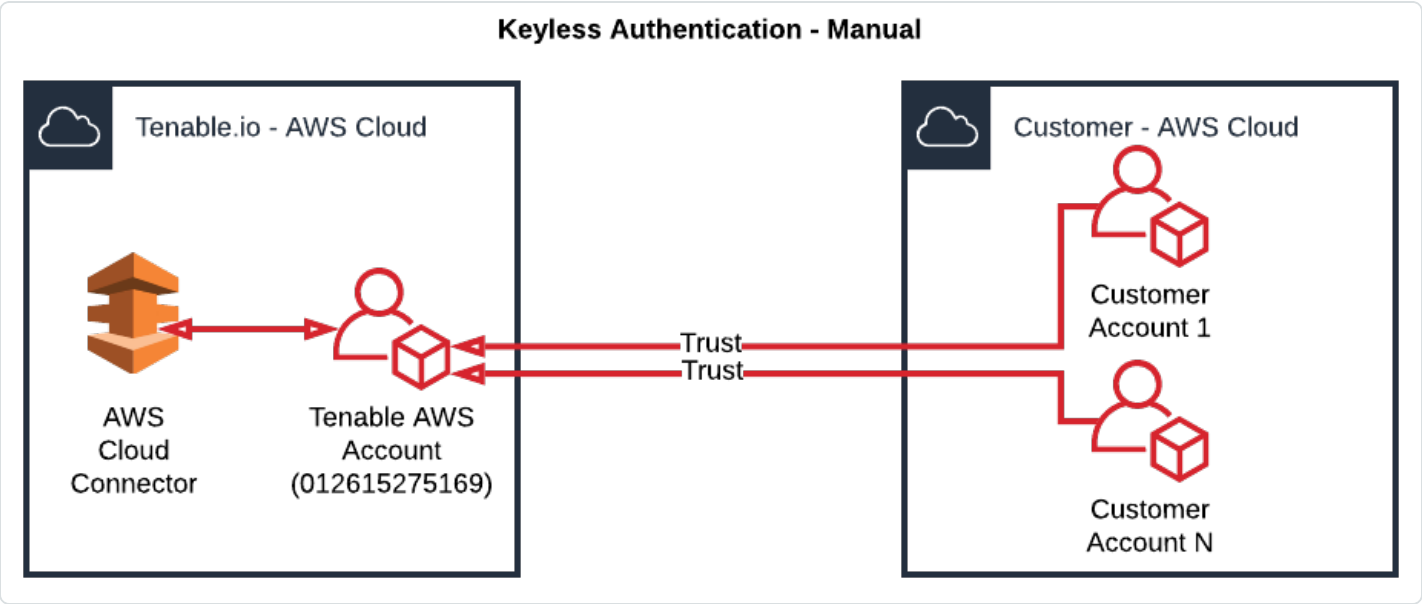
If you want to allow the Tenable AWS Account to automatically find other AWS accounts in your organization, use keyless authentication with auto account discovery. You must enable AWS Organizations and assign a `ListAccounts` policy, which then discovers other AWS accounts and establishes trust relationships 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)

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)

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)

Note: To use Tenable Cloud Security Preview or Tenable Cloud Security, you must update or create new roles that support Tenable Cloud Security. Tenable Vulnerability Management cloud connector roles do not support Agentless Assessment.

To create an AWS connector with keyless authentication for discovery only:

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 connector selection plane appears.

5. In the **Cloud Connectors** section, click **Amazon Web Services**.

   The connector creation plane appears.

6. In the **Connector Name** box, type a name to identify the connector.

7. In the **Account ID** box, type your primary AWS account ID.

8. (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.

9. (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.

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**.

    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 Amazon Web Services (AWS) Connector provides real-time visibility and inventory of EC2 assets in AWS accounts.

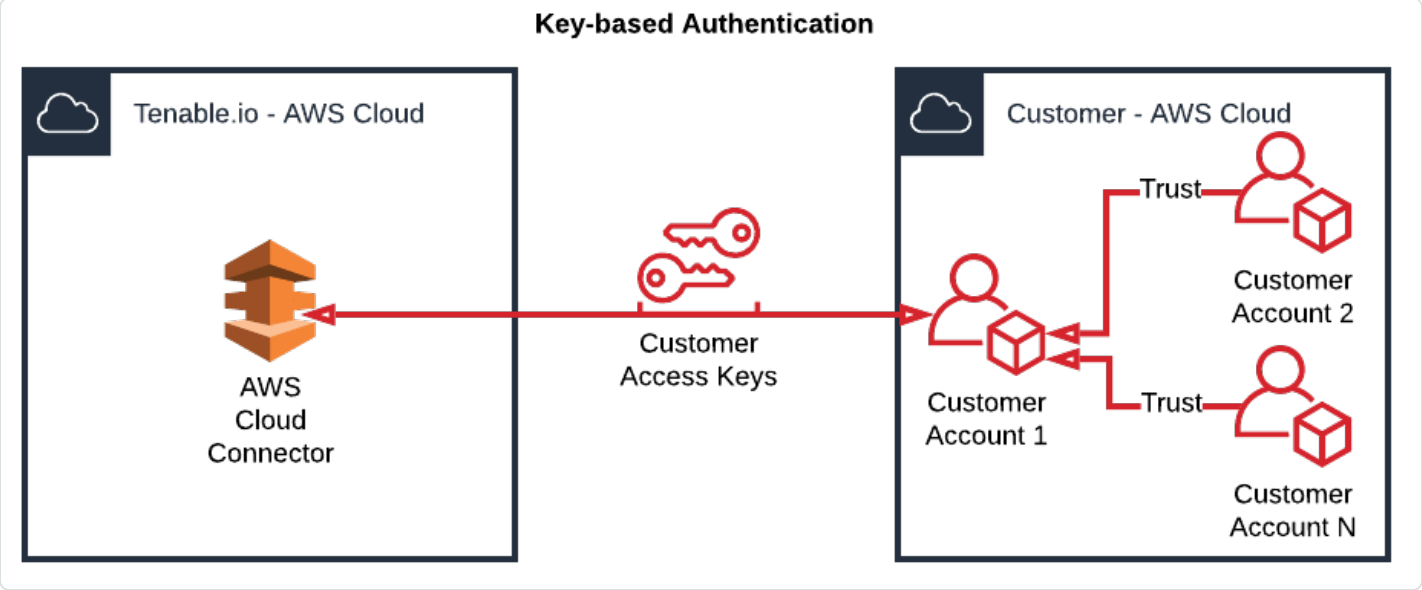
You can create an AWS connector to discover AWS assets and import them to Tenable Vulnerability Management. Assets discovered through the connectors do not count against the license until and unless the asset is scanned for vulnerabilities.

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

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

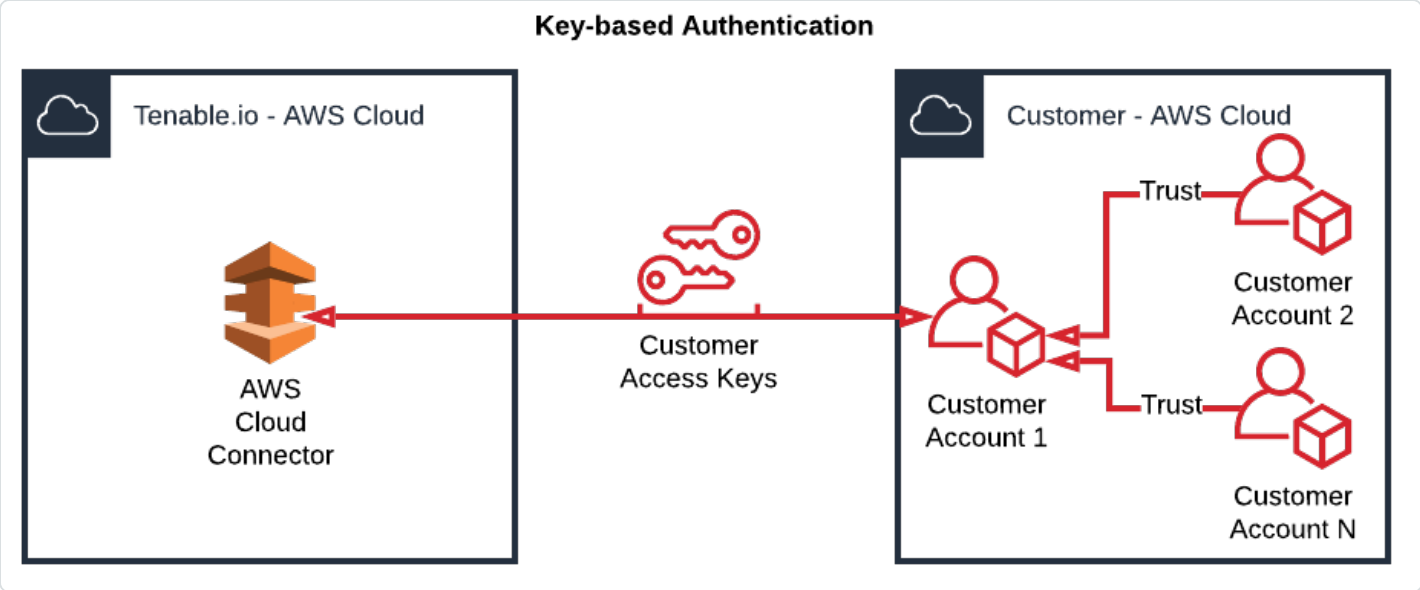
What to do next:

- 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

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 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 connector selection plane appears.

5. In the **Cloud Connectors** section, click **AWS - Keyed setup**.

   The cloud connector creation plane appears.

6. In the **Connector Name** box, type a name to identify the connector.

7. In the **Access Key** box, type the access key that you obtained when configuring AWS.

8. In the **Secret Key** box, type the secret key that corresponds to the access key you used.

9. 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.

10. 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.

11. 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

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

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.

To assess Azure assets for vulnerabilities, Tenable recommends that you use Frictionless Assessment to assess for vulnerabilities in the cloud. Alternatively, you can run a Nessus scanner or agent scan, both of which run plugins locally on the host.

Goal	Connector Type
Discover Microsoft Azure assets and assess for vulnerabilities using Frictionless Assessment The cloud connector discovers Azure assets, then assesses the hosts for vulnerabilities in the cloud, rather than running plugins locally on the host. For more information, see Frictionless Assessment for Azure.	Frictionless Assessment
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. To analyze assets via a Microsoft Azure connector:	Discovery 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.

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.

Frictionless Assessment for Azure

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

With Frictionless Assessment, Tenable Vulnerability Management discovers and collects an inventory of data points on your Azure virtual machine (VM) instances and VM scale set instances. Then, for instances that you specify for Frictionless Assessment, Tenable Vulnerability Management assesses the hosts for vulnerabilities in the cloud, rather than running plugins locally on the hosts.

Frictionless Assessment uses a custom automation runbook to collect the required data from VMs and VM scale sets in your selected resource groups. You do not need to configure a Microsoft Azure discovery connector, scanners, Tenable Nessus Agents, scans, or scan schedules to assess hosts with Frictionless Assessment.

The Azure Frictionless Assessment runbook collects data from each VM with basic commands to gather information such as installed packages and the existence of specific files. This information is then securely sent to Tenable using Azure's Public Blob Resource API. This connection is made using a customer-specific, regularly rotating shared access signature (SAS) token. For more information about the data that the runbook collects from VMs, see Azure Runbook Information .

Note: Virtual machines scanned by Azure Frictionless Assessment need outbound network access to push information to Azure's Public Blob Resource API. This can be accomplished by adding an outbound security rule using the "Storage" service tag. Without this access, the result of Runbook collection will not be received by Tenable and no assets or vulnerabilities will be assessed.

Operating System Coverage

Frictionless Assessment has vulnerability coverage for the following:

- Amazon Linux 1 / 2
- CentOS 6 / 7 / 8
- Red Hat 6 / 7 / 8

- SUSE Linux Enterprise Server (SLES) 11.4-15.2
- SUSE Linux Enterprise Desktop (SLED) 12-15.2
- Ubuntu 16.04. / 18.04 / 20.04 / 20.10
- Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022
- Windows 7, Windows 8, Windows 10, Windows 11

Licensing Considerations

In general in Tenable Vulnerability Management, assets count towards your license when they are assessed for vulnerabilities. Therefore, hosts that are assessed by Frictionless Assessment count against your license. For more information, see Licenses.

When you select Azure tags for hosts to be assessed by Frictionless Assessment, note that all hosts with any of those tags count towards your license. Hosts that are only discovered by the connector, and not assessed by Frictionless Assessment (for example, hosts that do not have a tag you selected for Frictionless Assessment), do not count towards your license.

Limitations

- Frictionless Assessment does not run informational plugins, run remote vulnerability plugins, or gather compliance data.
- Frictionless Assessment in Azure does not support custom encrypted disks.
- A connector configured with Frictionless Assessment only supports one Azure subscription. If you want to assess hosts across multiple Azure subscriptions, you must configure a separate connector for each subscription.
- You must have the **Microsoft.ContainerInstance** resource provider registered for each Azure subscription you plan to deploy the ARM template to.
- The limit for Frictionless Assessment scans is one per day, whereas existing Frictionless Assessment connectors created before May 1, 2023 transmit inventory data more frequently. Frictionless Assessment drops data exceeding the frequency limit and does not scan it.

  > **Note**: The limitation does not apply to Tenable Container Security, Agentless Assessment, or Tenable NessusAgent-based inventory scans.

Get Started

1. Create an Azure Connector for Frictionless Assessment.

   > **Note:** If you delete a Frictionless Assessment Azure connector, manually delete the remaining Azure artifacts as described in Manually Delete Connector Artifacts from Azure Frictionless Assessment.

2. Verify that the Runbook in the automation account used for Frictionless Assessment Azure completes successfully. If it does not, contact your Azure administrator or support representative to resolve the issue.

   You can find the Runbook in Microsoft Azure > **Automation Accounts** > **Tenable FA Automation Account** > **Process Automation** > **Runbooks/Job**.

Create an Azure Connector for Frictionless Assessment

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

Required User Role: Administrator

When you configure an Azure cloud connector for Frictionless Assessment, Tenable Vulnerability Management uses an Azure Resource Manager (ARM) template. ARM is Azure's method for organizing, updating, provisioning resources in an Azure resource group or subscription. It allows users to define resources, dependencies, and networking for their application or use cases.

Follow the steps below to create a Microsoft Azure Frictionless Assessment connector in Tenable Vulnerability Management. This process also creates the ARM template that you will need to deploy to each of your Azure subscriptions that you want to evaluate for Frictionless Assessment.

Before you begin:

- In another window or tab of the same browser with which you are accessing Tenable Vulnerability Management, log in to the Azure console with the Azure account that you want to target with Frictionless Assessment.

Note: To use Tenable Cloud Security Preview or Tenable Cloud Security, you must update or create new roles that support Tenable Cloud Security. Tenable Vulnerability Management cloud connector roles do not support Agentless Assessment.

Create the Microsoft Azure Frictionless Assessment connector and ARM template:

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. Click **Create Cloud Connector**.

   The **Select a Cloud Connector** panel appears.

Select a Cloud Connector

Import data from various sources to further enrich Tenable.io

Search

CLOUD CONNECTORS

AWS - Keyed setup

AWS - Keyless setup

Microsoft Azure

Microsoft Azure Frictionless Assessment

Google Cloud Platform

CONTAINER SECURITY

Container Security Scanner

Docker

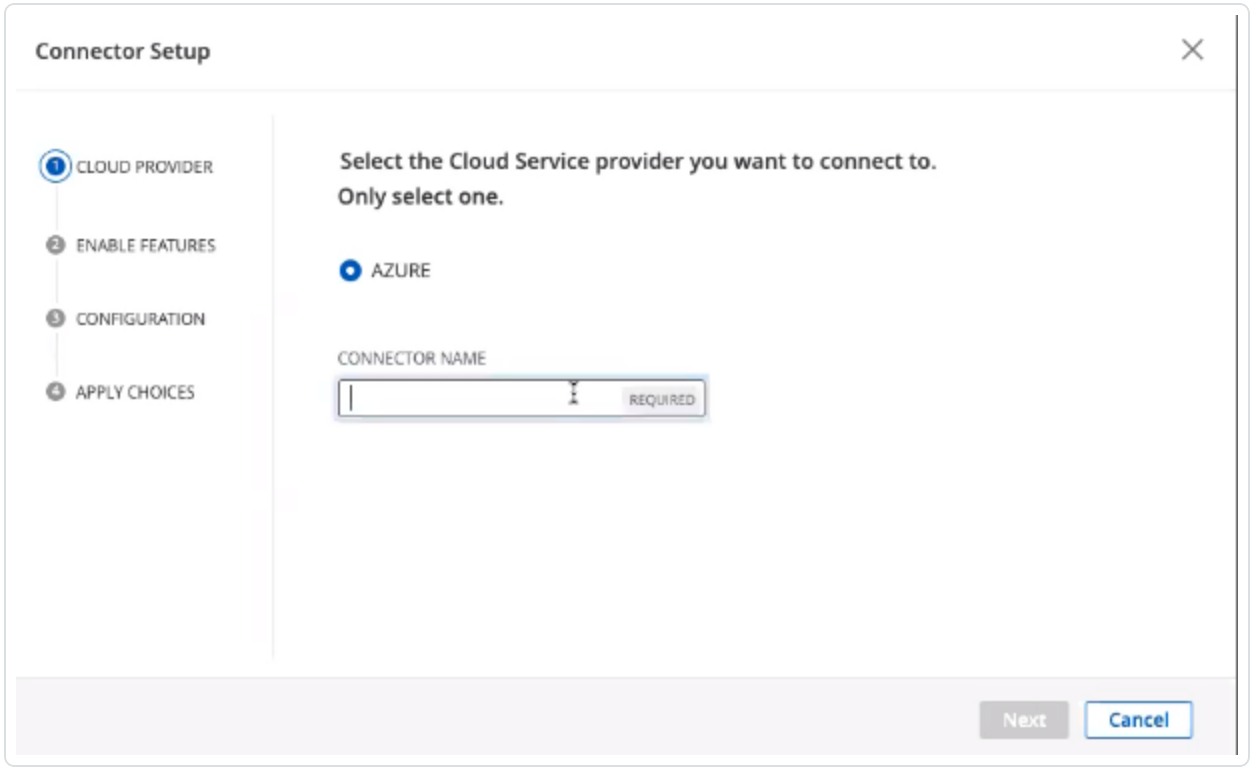
Docker EE

AWS Elastic Container Registry

JFrog Artifactory

5. In the **Cloud Connectors** list, select **Microsoft Azure Frictionless Assessment**.

   The **Connector Setup** pop-up appears.



6. In the **Cloud Provider** step, enter a **Connector Name**.

   Click **Next**.

7. In the **Enable Features** step, ensure the check box to **Identify vulnerabilities using frictionless assessment** is selected.

   Click **Next**.

8. In the **Configuration** step, either select the **Scan all** check box, or select specific target parameters.

> **Note:** To target a more specific subset of resources, you can target your connector on a specific resource group, a specific tag key, a specific tag value, or a combination of all three.

> **Note:** Use the **ANY** input from the drop-down as a wild card to target all values for a resource group, tag key, or tag value.

> **Note:** Multiple targets with specific parameters can be selected.

Click **Next**.

9. In the **Apply Choices** step, click **Download and Finish**.

   The new ARM template downloads in .json format, and the new connector shows on the **Cloud Connectors** page.

Deploy the connector using the ARM template:

Deploy the ARM template you downloaded in the previous section to your Azure subscription(s).

For deployment guidance, refer to Microsoft Azure documentation.

> **Note:** You must have the **Microsoft.ContainerInstance** resource provider registered for each Azure subscription you are deploying the ARM template.

> **Note:** When deploying Azure Frictionless Assessment through the Azure CLI, use subscription deployment with the ARM template produced by the steps above.
>
> Example:
>
> ```
> az deployment sub create --location eastus --template-file /path/to/arm-template.json
> ```
>
> You can add `--debug` to the command generate verbose logging during deployment.
>
> ```
> az deployment sub create --location eastus --template-file /path/to/arm-template.json --debug
> ```

Manually Delete Connector Artifacts from Azure Frictionless Assessment

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

Required User Role: Administrator

Before you begin:

- Delete the Azure Frictionless Assessment connector, as described in Delete a Connector.

Delete the following Azure Frictionless Assessment artifacts in the Azure portal:

- The Automation account role assignment related to the custom role definition (e.g. **Tenable-FA-Automation-Account**)
- The custom role definition (e.g. **Tenable FA Role (Subscription: [UUID] | Connector: [UUID])**)
- The Frictionless Assessment resource group (e.g. **TenableFA-Connector-{UUID}**)

  Note: The resource group can also be deleted from the Azure CLI with the following command, given that the Azure client has **Contributor** permissions or greater:

  ```
  az group list --tag Tenable=AzureFa --query "[].name" -o tsv | xargs -ot az group delete --no-wait -n
  ```

For more information on the listed Azure artifacts, see the Microsoft Azure documentation.

Azure Runbook Information

> Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

Frictionless Assessment uses a custom automation runbook and collects the following data from VMs and VM scale sets in your selected resource groups.

Some intermediary resources show up after the first few minutes of deploying an arm template. These resources are deployment scripts that Tenable Vulnerability Management uses to deploy the following resources. Tenable Vulnerability Management removes the scripts once the deployments are complete.

- Resource group:
    - Name: Starts with `Tenable-FA-Connector`
    - Contains Azure Frictionless Assessment resources.
- Automation Account:
    - Name: Starts with `Tenable-FA-Automation-Account`
- Runbooks:
    - Name: `TenableFATerminatedInstances`
    - Description: Tenable Frictionless Assessment runbook for terminated instances.
    - Name: `TenableFACollector`
    - Description: The Tenable Frictionless Assessment collection runbook.
- Storage Account:
    - Name: Starts with scripts.
    - Description: Contains shell/powershell scripted checks to run against assets.

- Role Definitions:
    - Name: Starts with `Tenable FA Role` or `Tenable-FA-Custom-Role-Def`.
    - Description: The role required for runbook to allow it to scan assets.
    - Actions:

```
"Microsoft.ClassicCompute/operatingSystems/read",
"Microsoft.ClassicCompute/operatingSystemFamilies/read",
"Microsoft.ClassicCompute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachines/runCommand/action",
"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/read",
"Microsoft.Compute/virtualMachineScaleSets/virtualMachines/runCommand/action"
```

Configure Microsoft Azure (Discovery Only)

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.

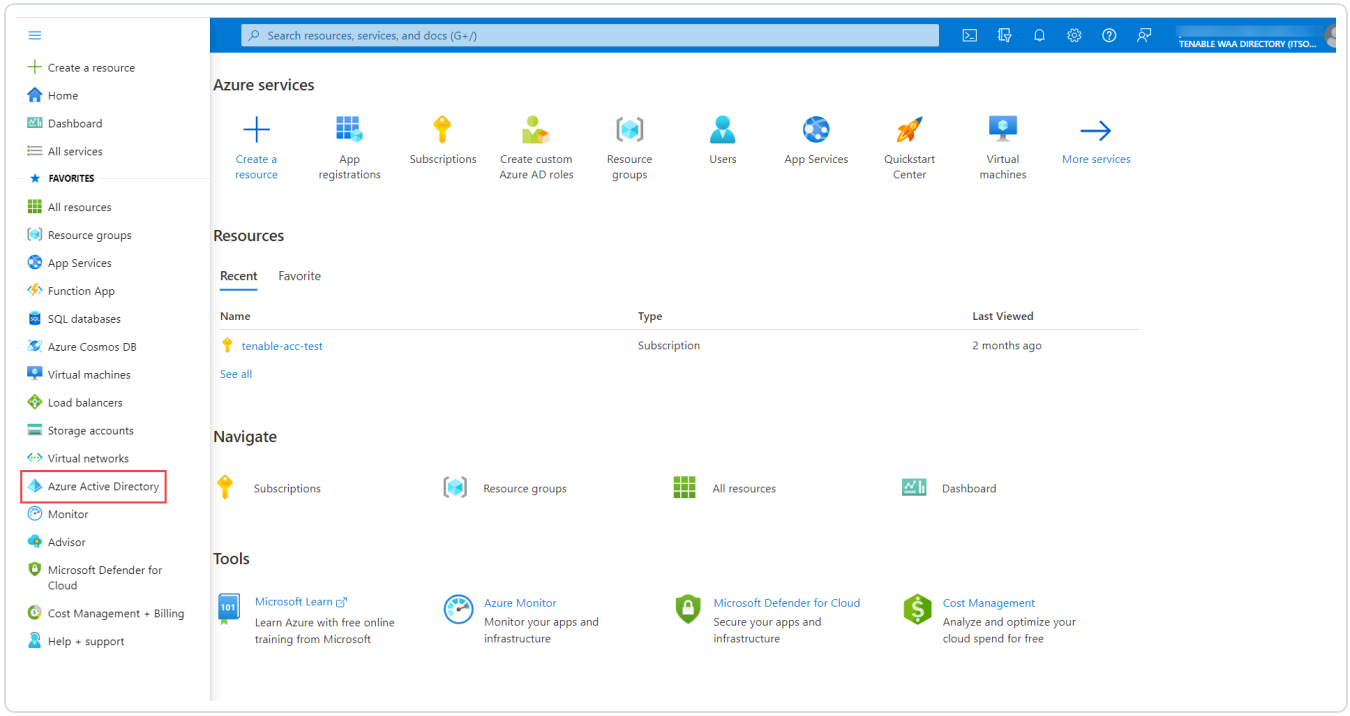
What to do next:

- Create an Azure connector.

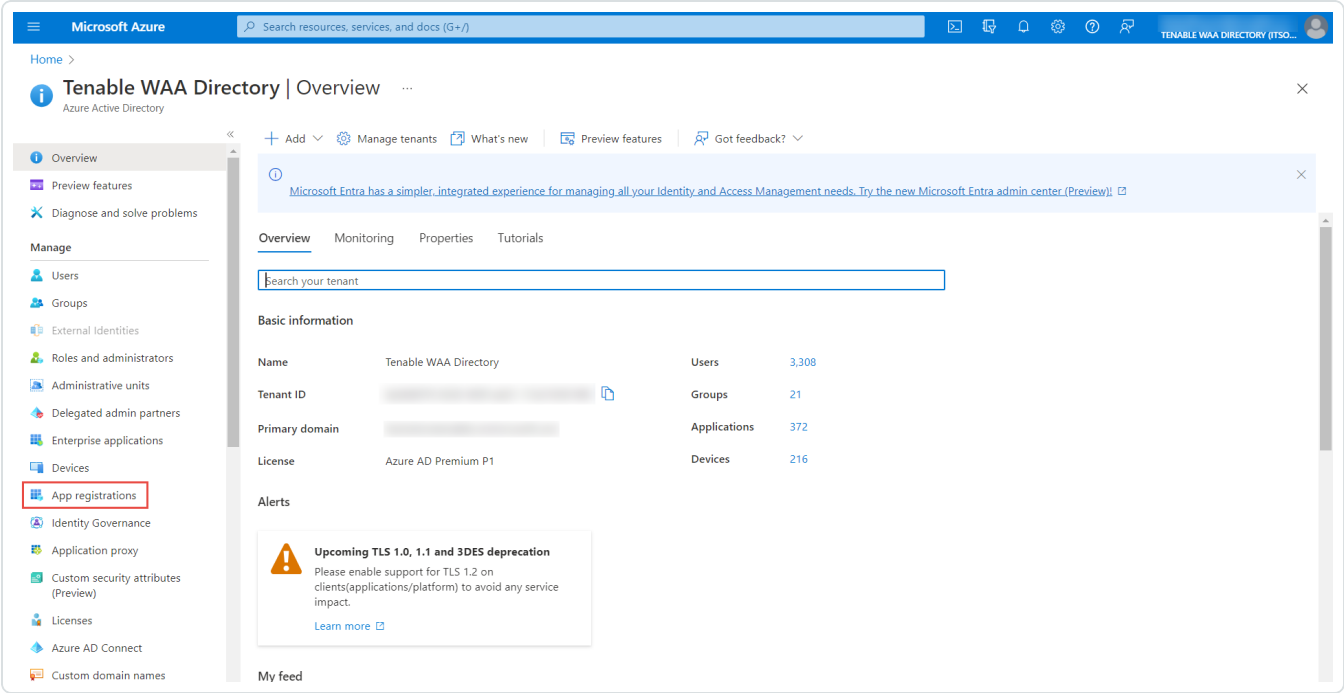
Create Azure Application

To create an Azure Application for an Azure Tenable Vulnerability Management connector:

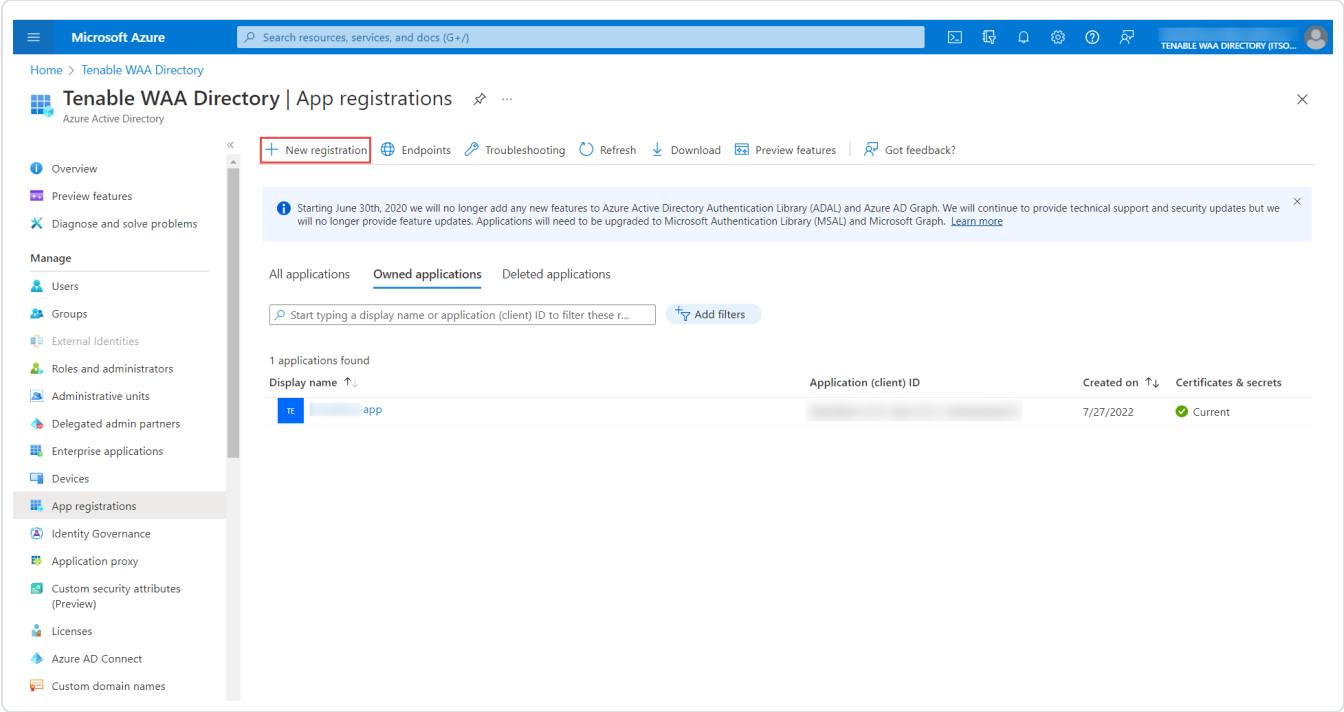
1. Log in to the Microsoft Azure portal.
2. In the left-hand menu, click **Microsoft Entra ID**.



3. Click **App registrations**.



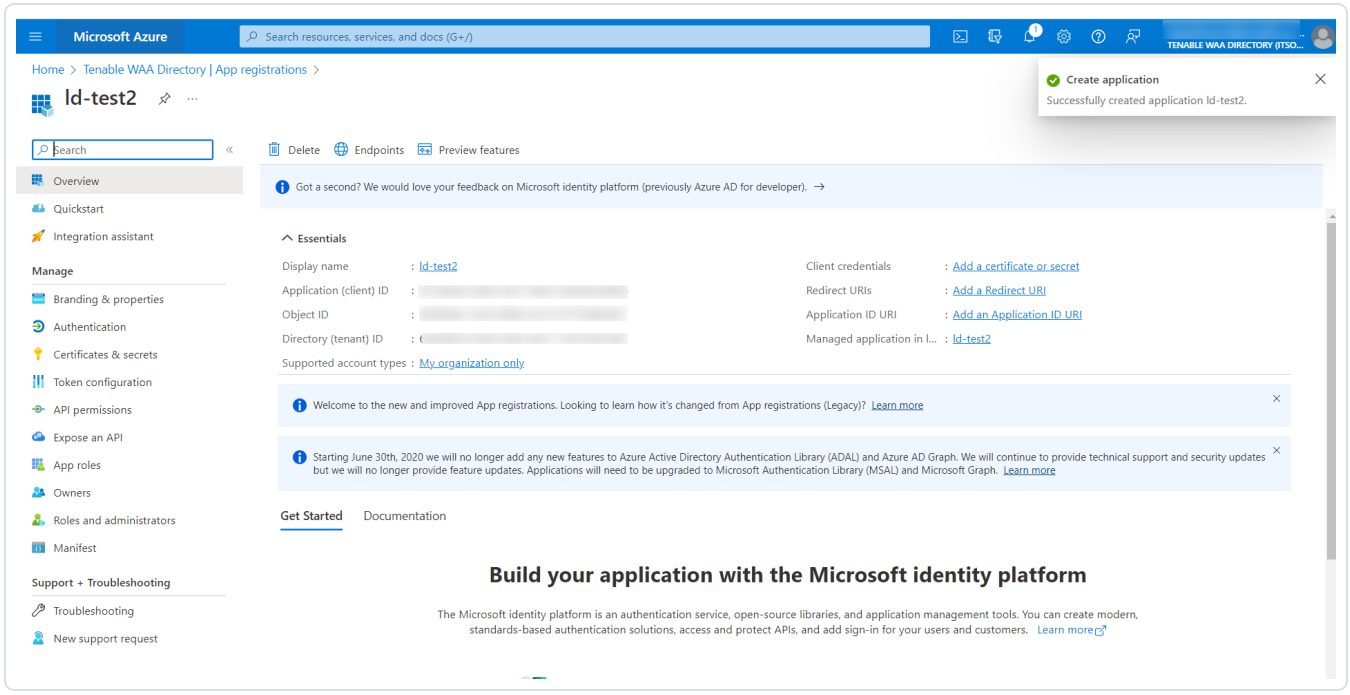
4. To add a new application, click **New registration**.



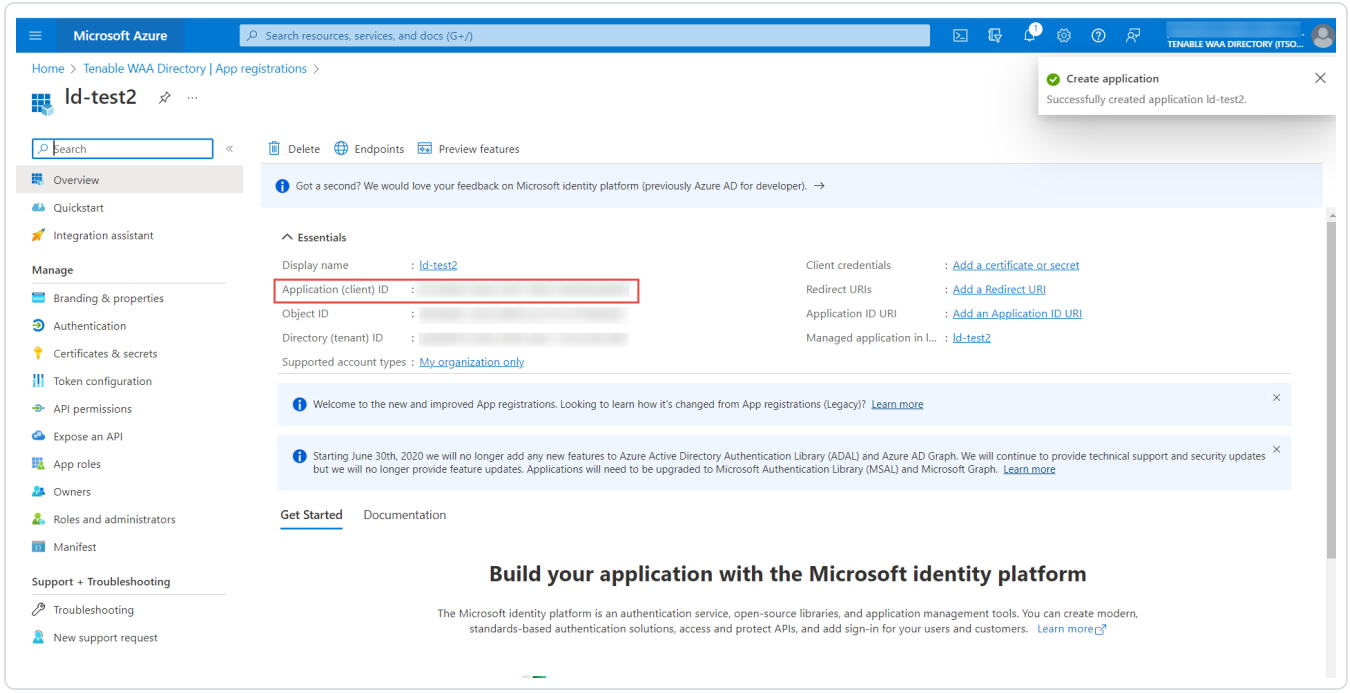
5. In the **Name** box, enter a descriptive name for the application.

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.

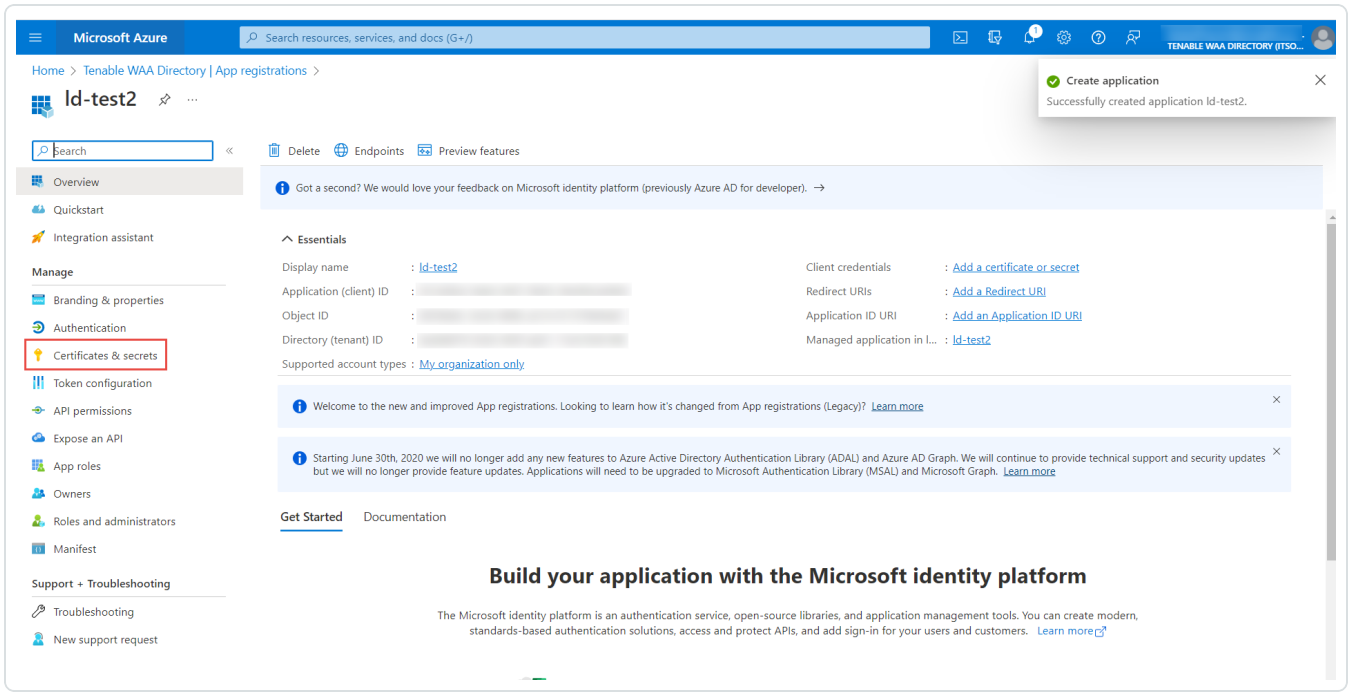
   A success message appears at the top of the page stating that the new application has been created, and the page is redirected to the **Overview page** for the application.



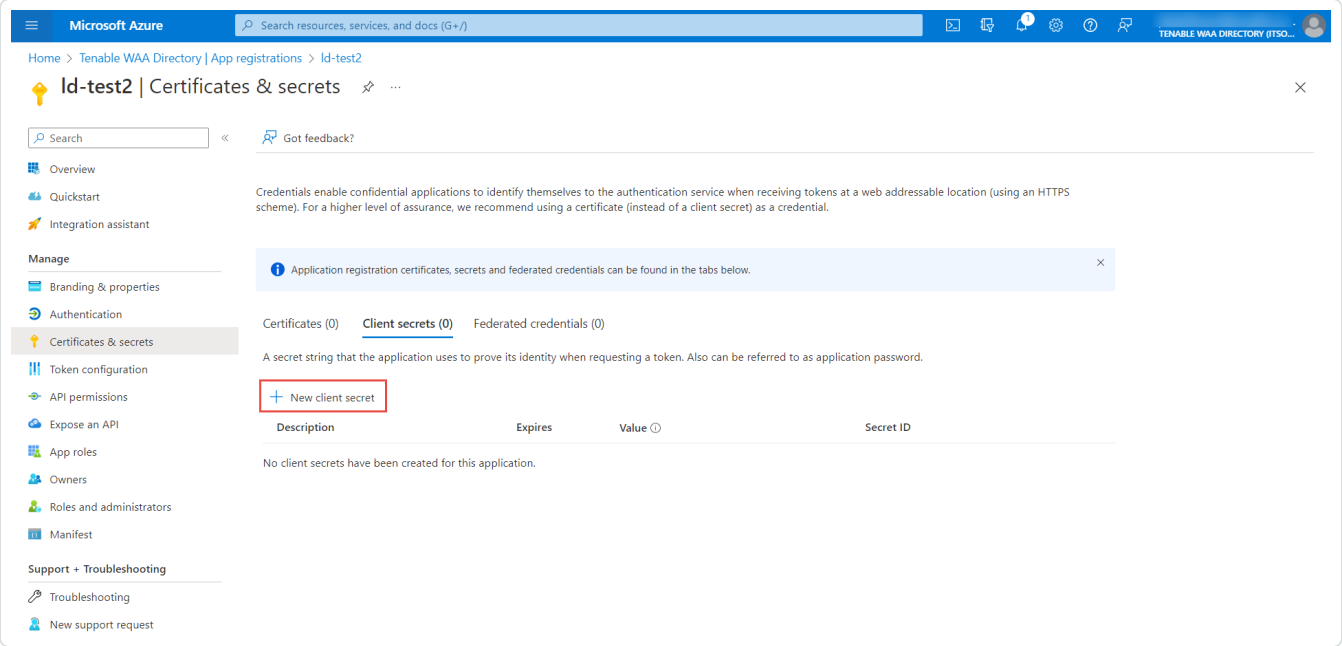
9. Copy the **Application (client) ID**. This information is used to configure a connector with Tenable Vulnerability Management.



10. In the **Manage** section for the application, click **Certificates & secrets**.

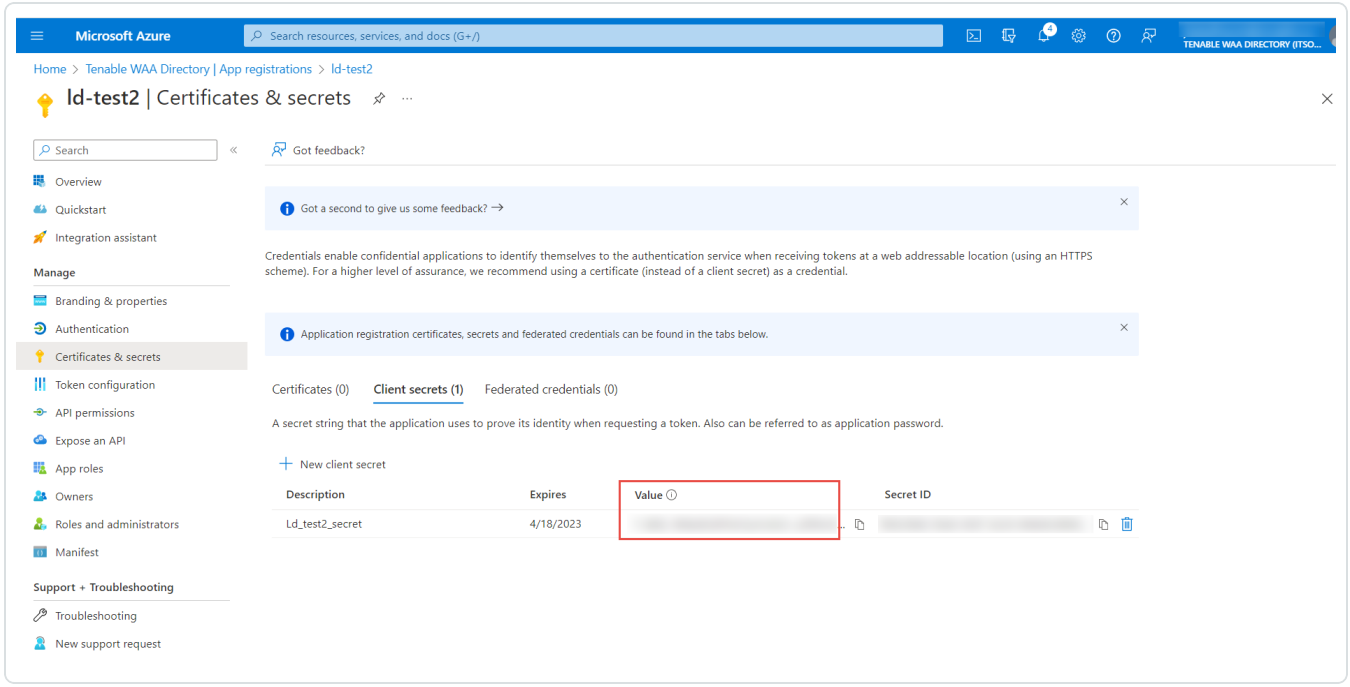


11. In the **Client Secrets** section, click **+ New client secret**.



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)

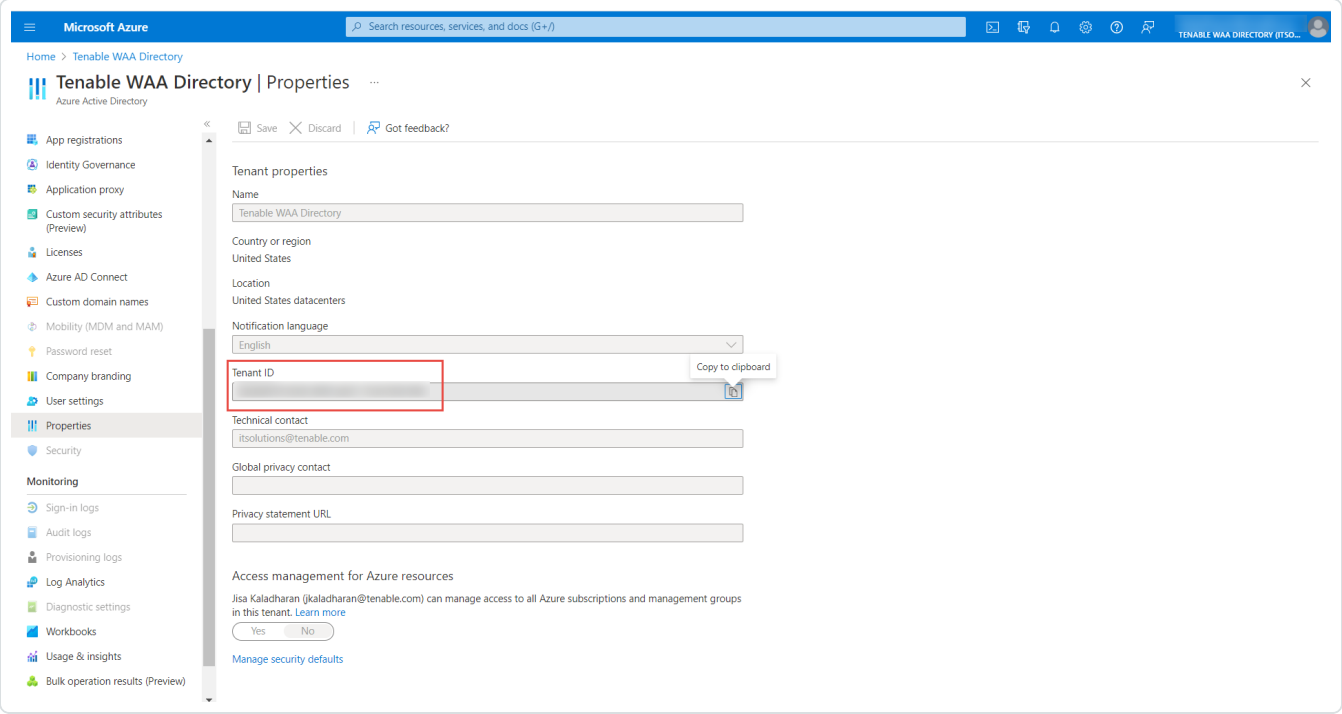
To obtain your Tenant ID for an Azure Tenable Vulnerability Management connector:

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.



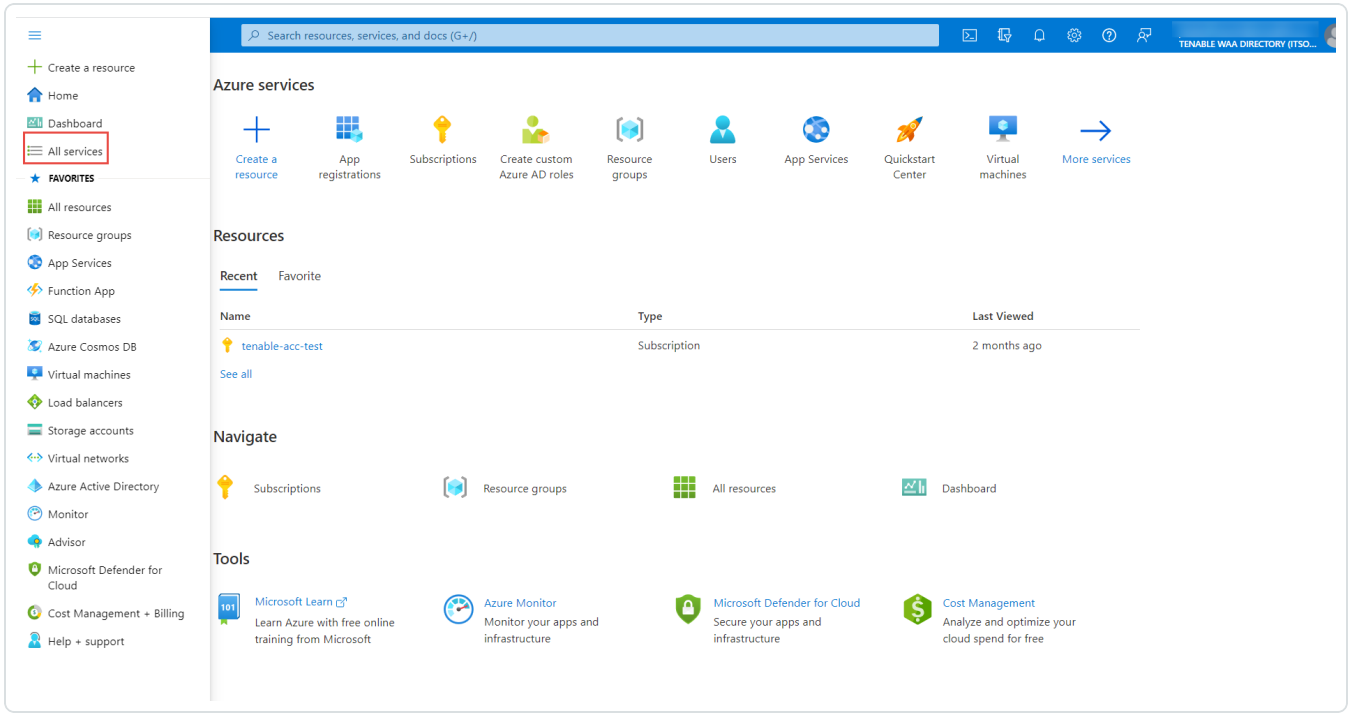
What to do next:

- Obtain the Azure Subscription ID.

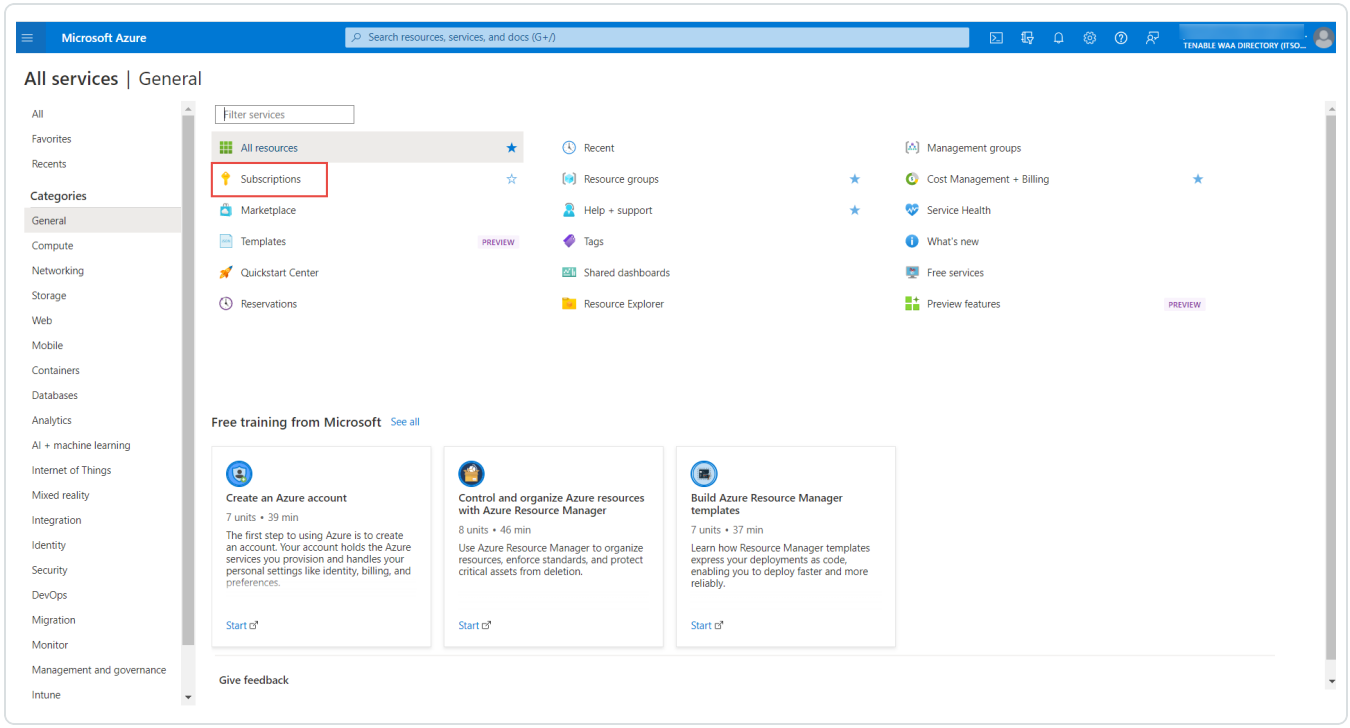
Obtain Azure Subscription ID

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:

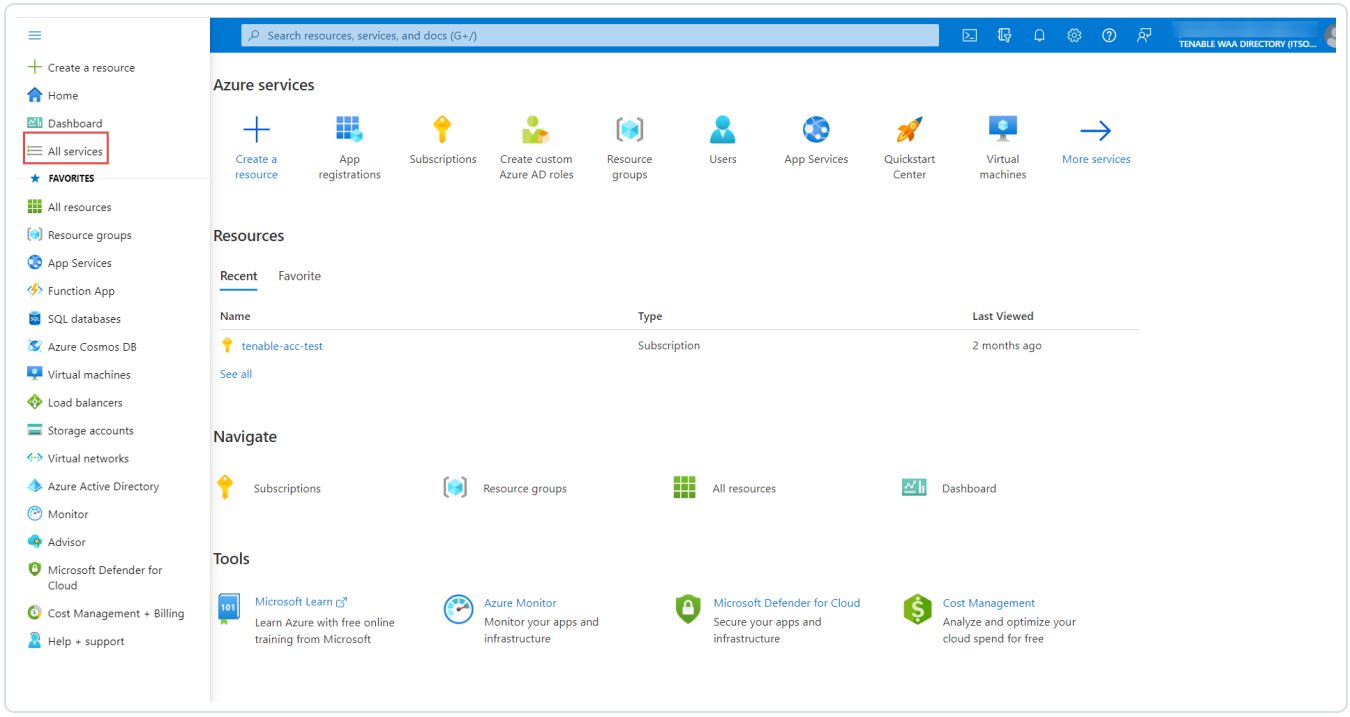
- Grant the Azure Application reader role permissions.

Grant the Azure Application Reader Role Permissions

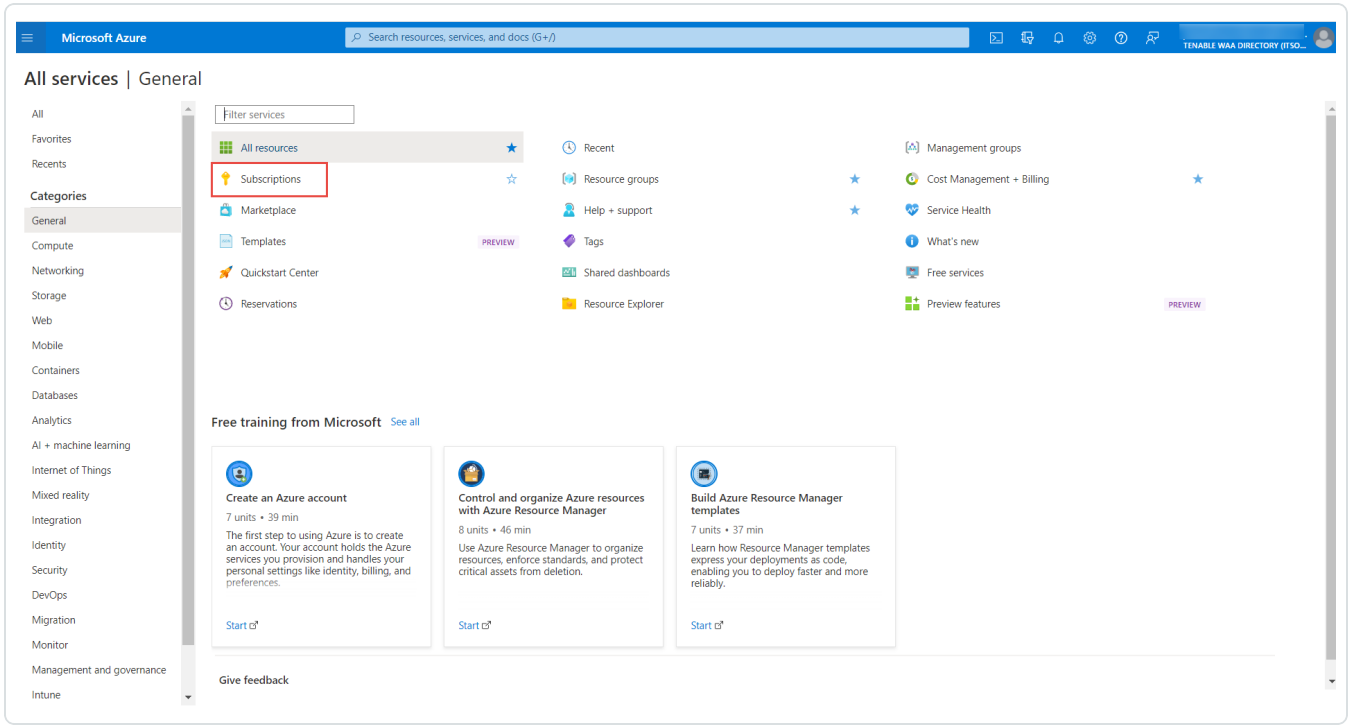
To grant an Azure application reader role permissions for an Azure Tenable Vulnerability Management connector:

> **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.

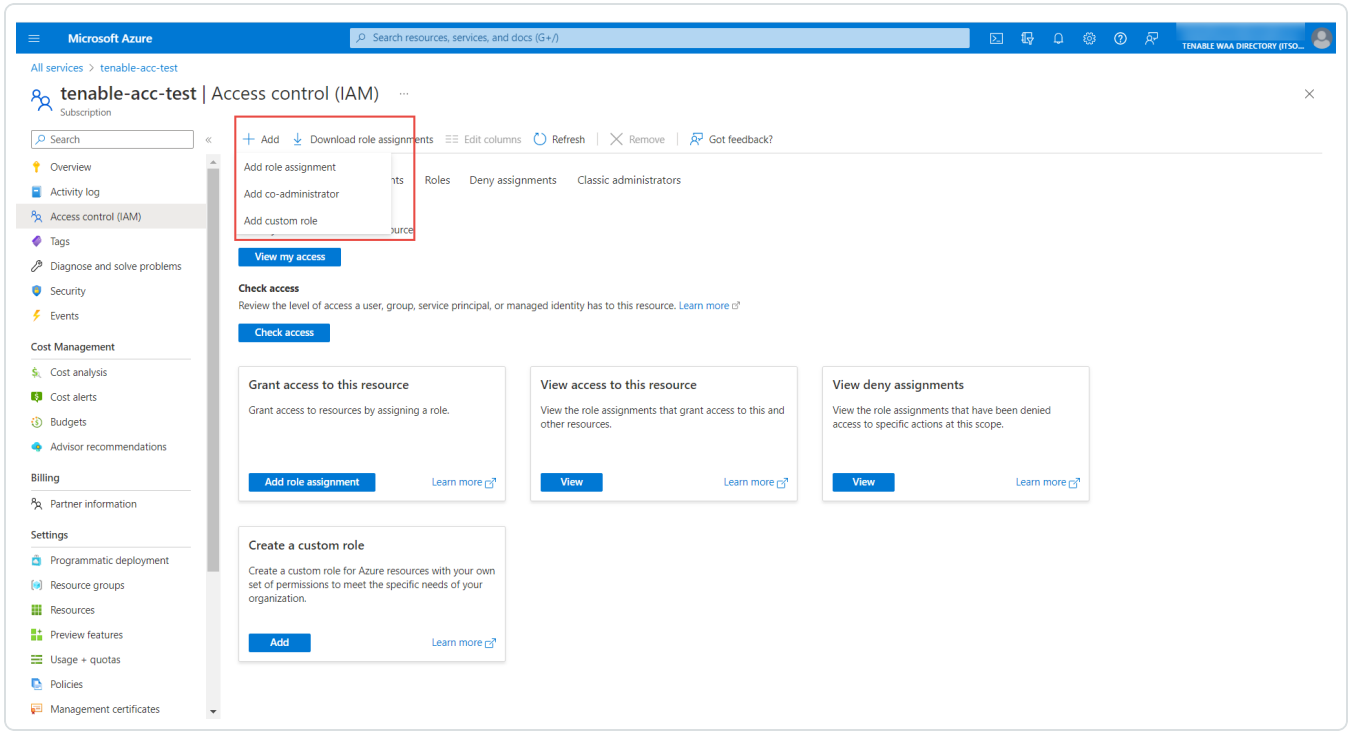
5. In the menu for the subscription, click **Access control (IAM)**.

   The **Access control (IAM)** page appears.

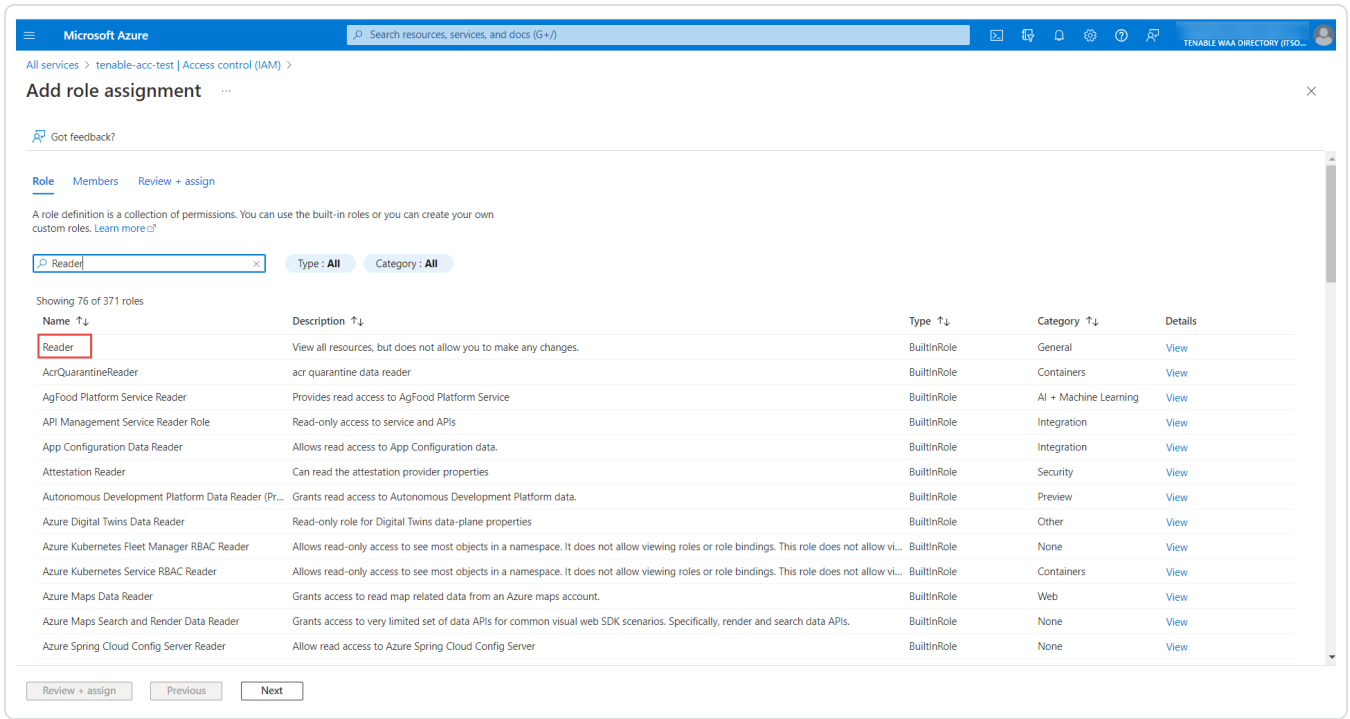
6. Click the **+Add** button.

   A pop-up menu appears.

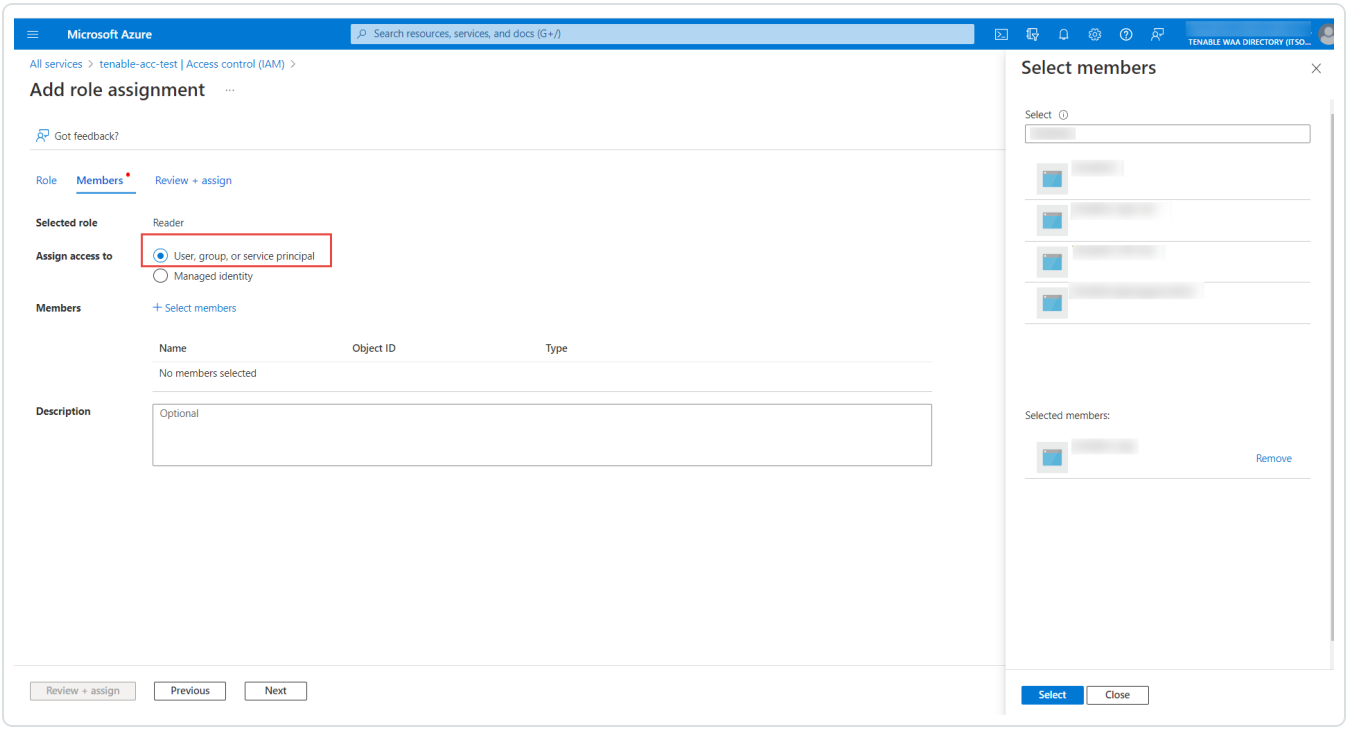
7. Click **Add role assignment**.



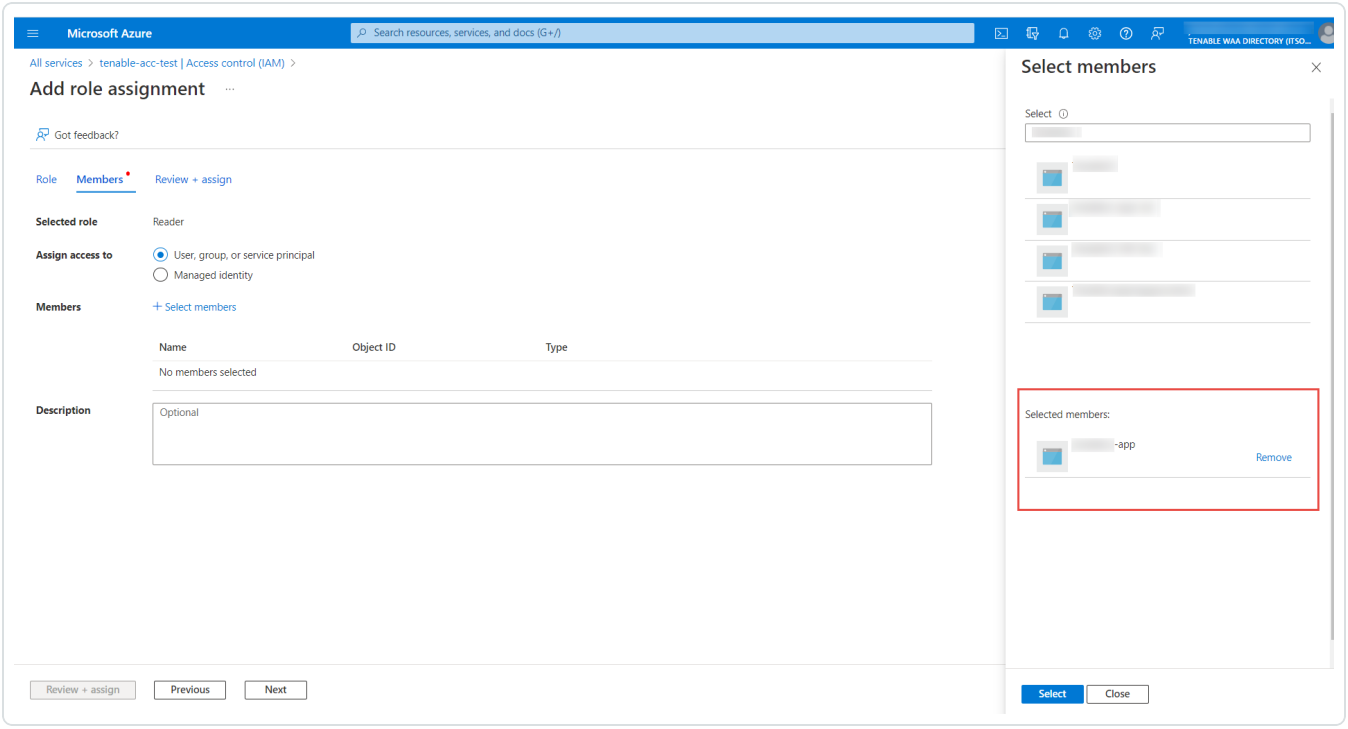
8. In the **Add role assignment** window, in the **Role** tab, search and select **Reader**.



9. In the **Members** tab, in the **Assign access to** section, select **User, group, or service principal**.

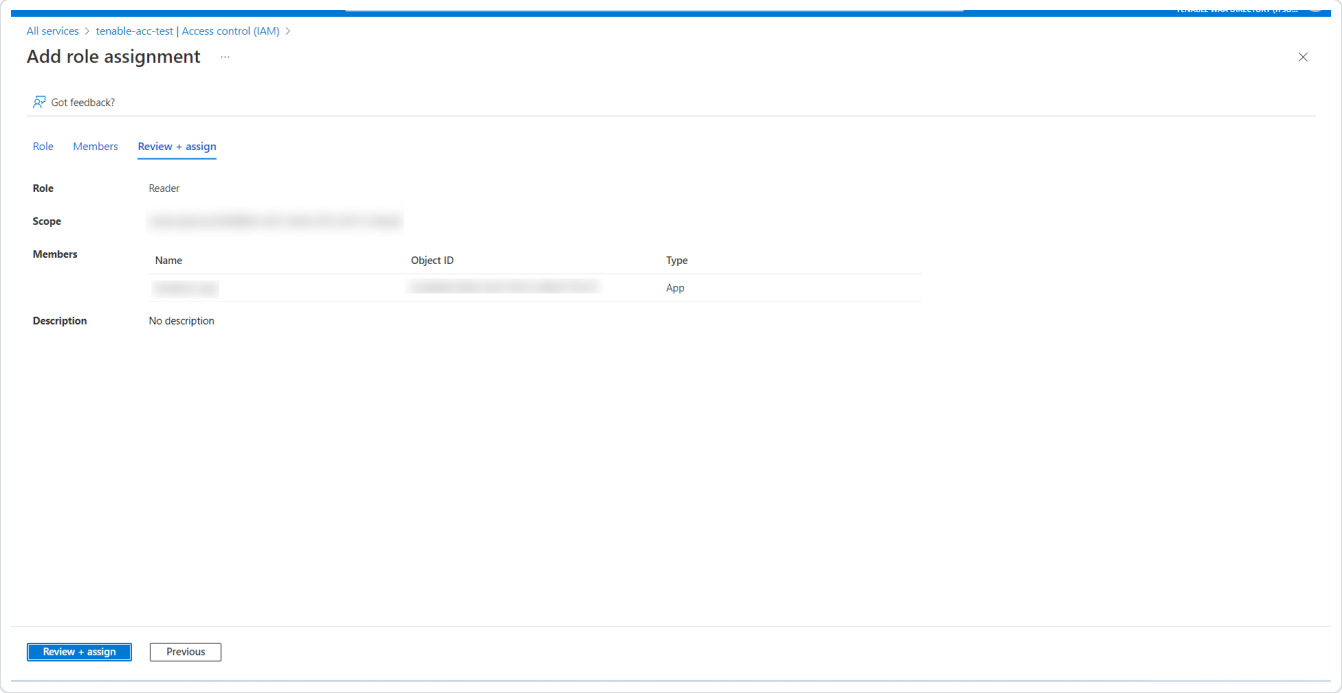


10. To select your Azure Application, click **+ Select Members**.



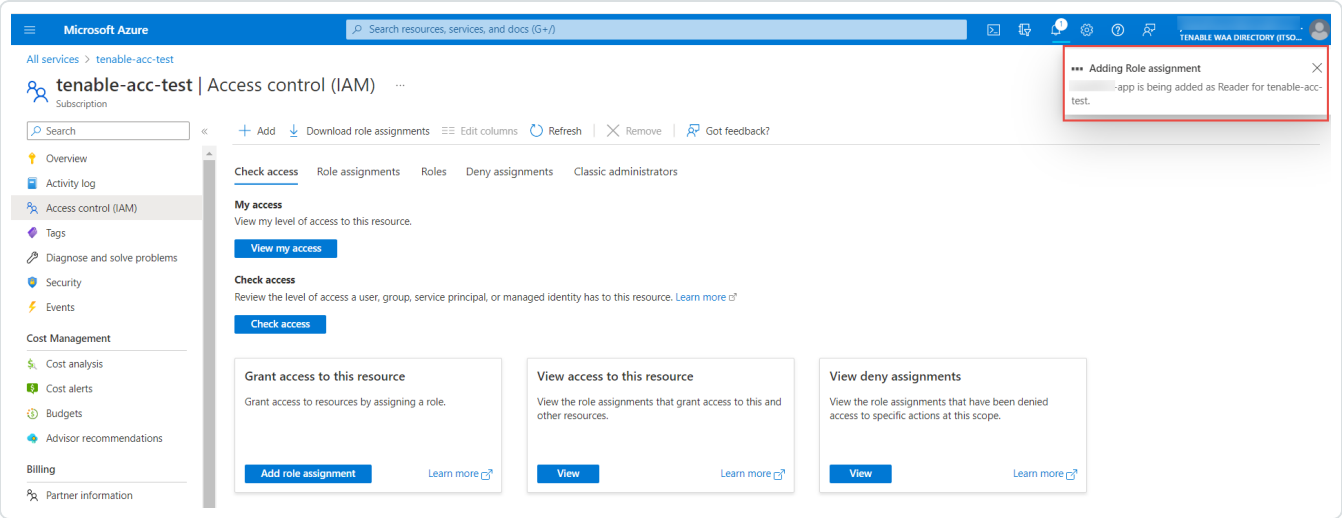
The **Select members** plane appears.

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

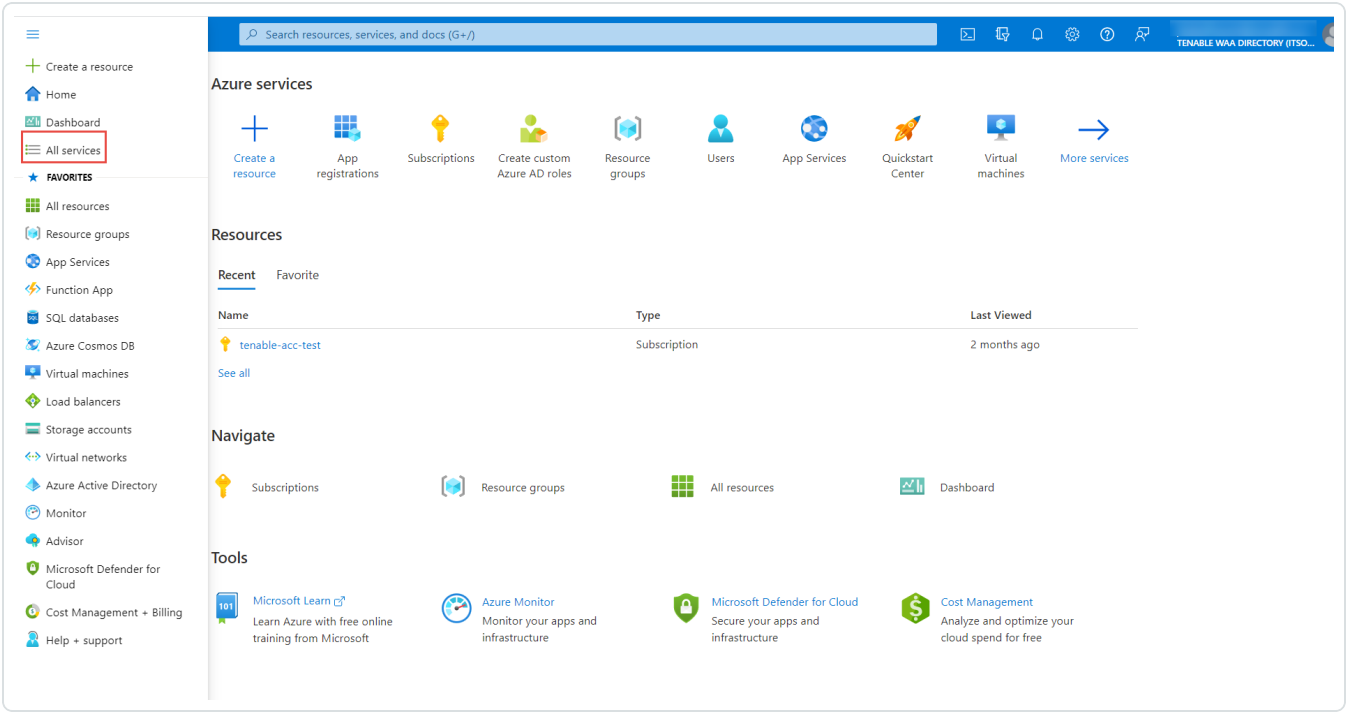
Before you begin:

- Record the name of the application you created for your primary Azure subscription.

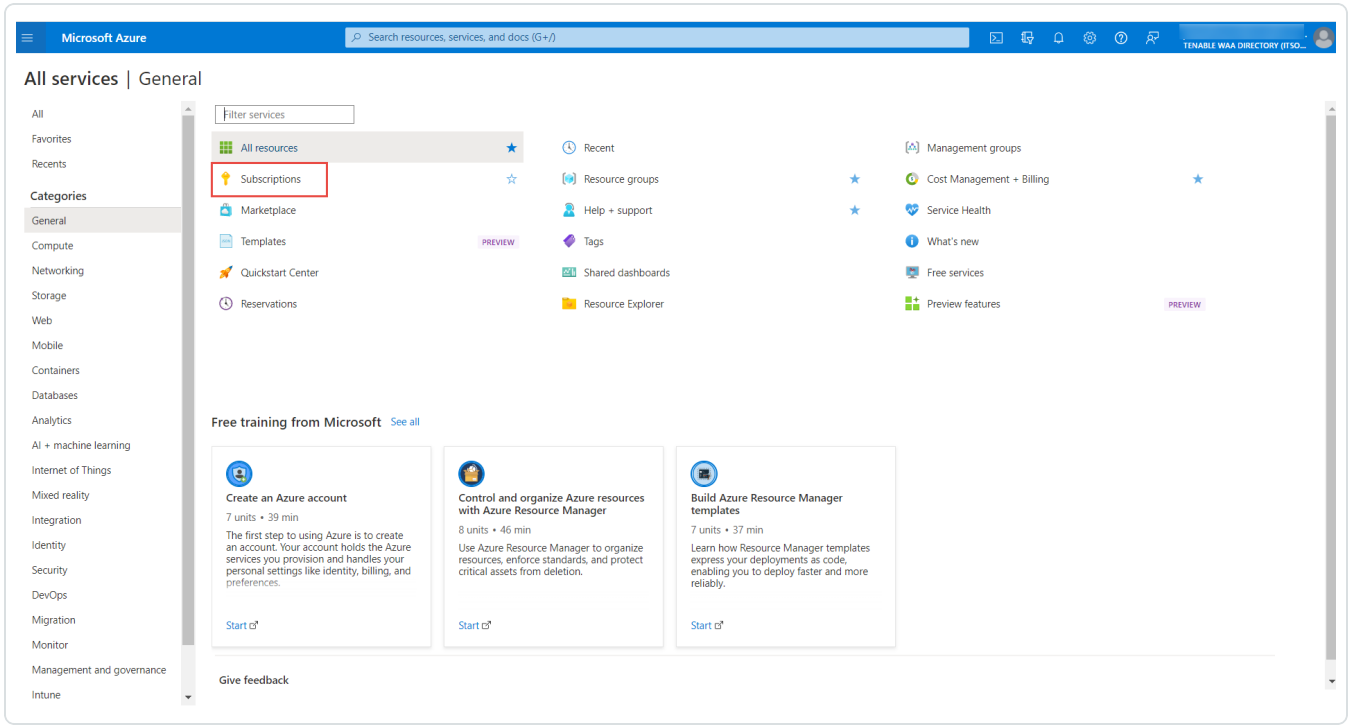
To configure linked Azure subscriptions:

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.

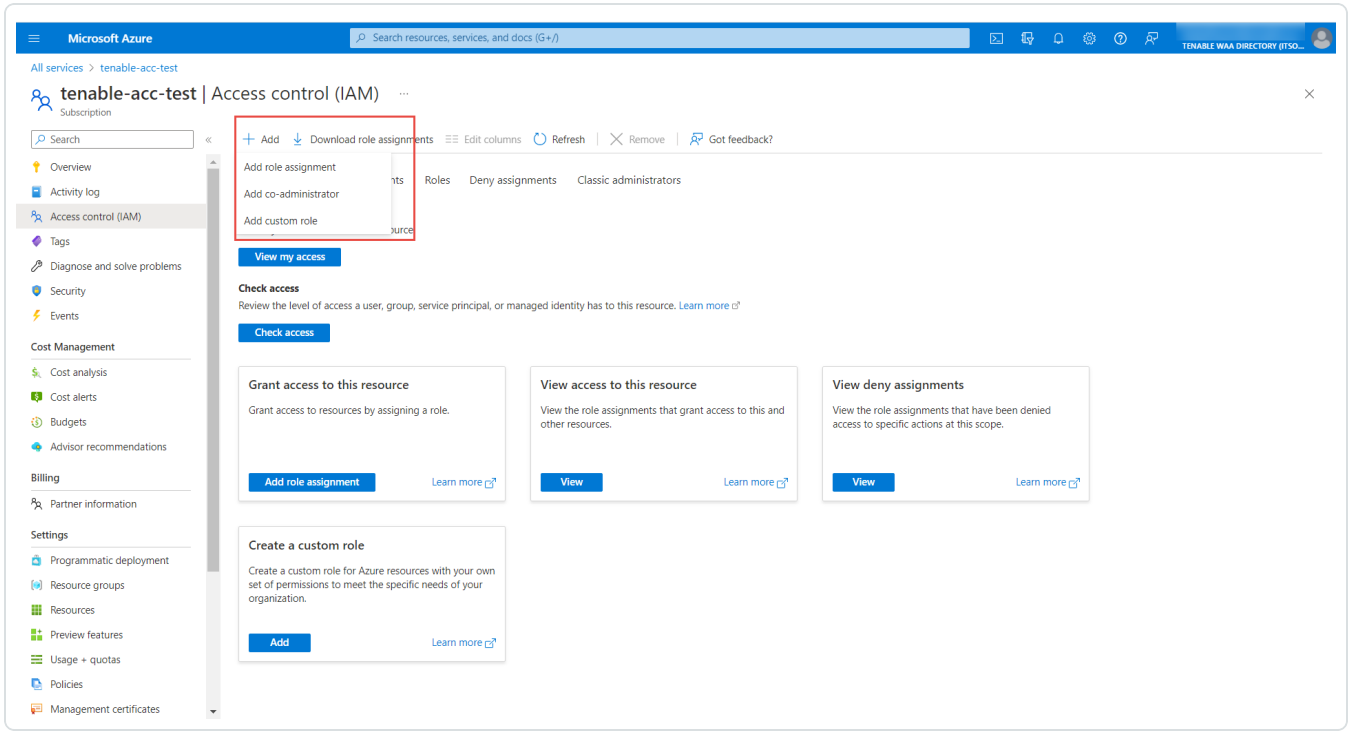
5. In the menu for the subscription, click **Access control (IAM)**.

   The **Access control (IAM)** page appears.

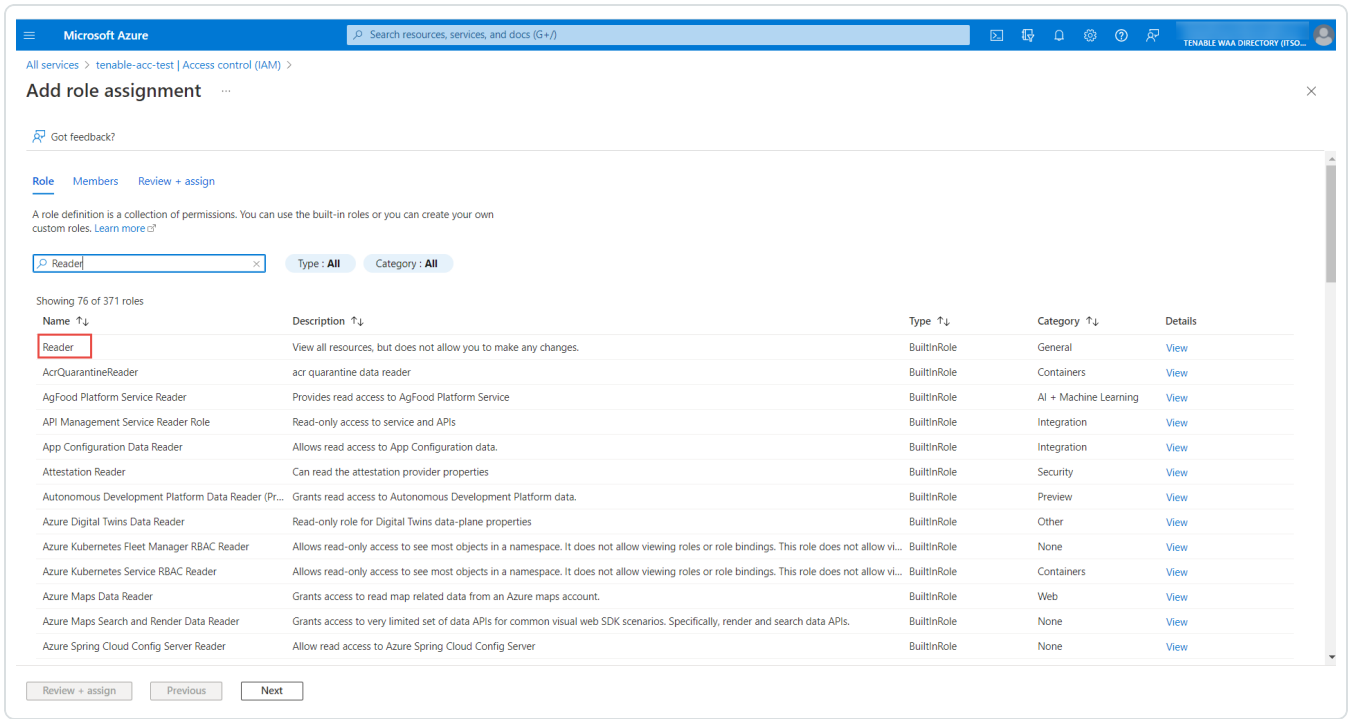
6. Click the **+Add** button.

   A pop-up menu appears.

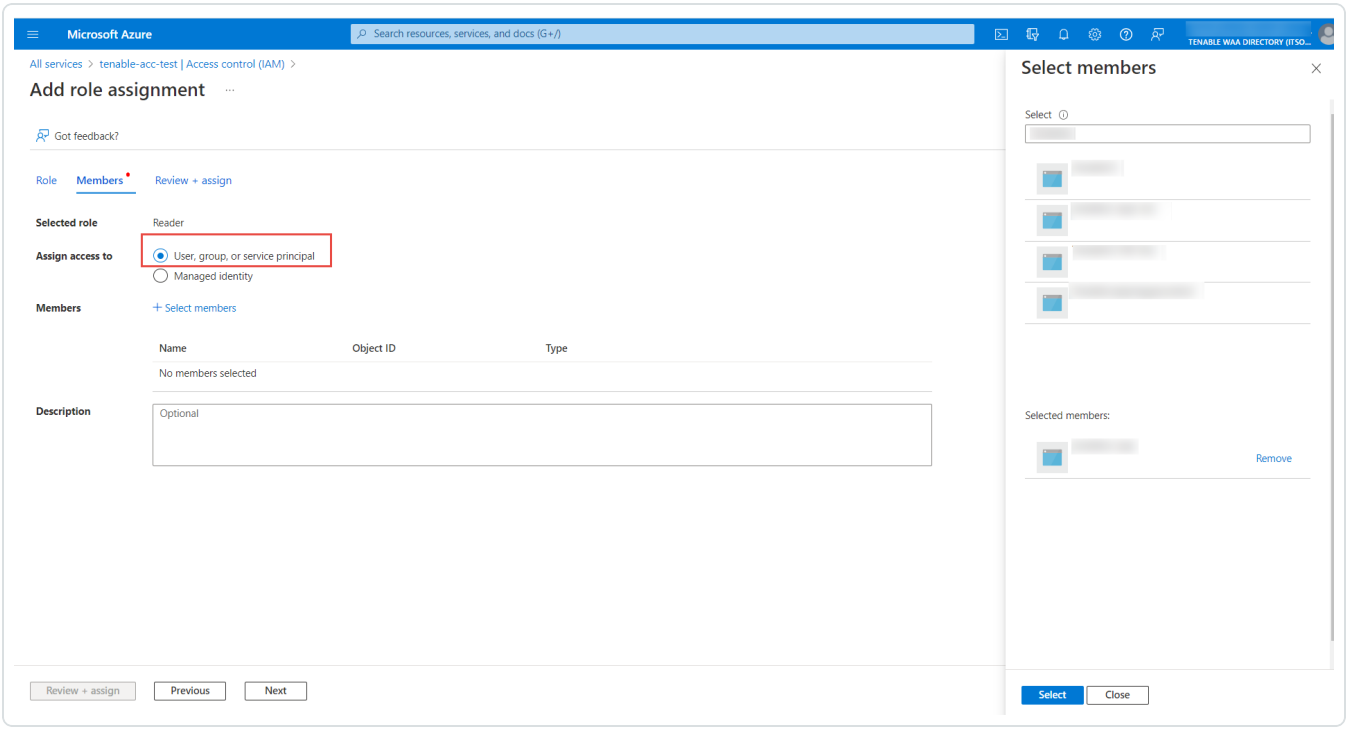
7. Click **Add role assignment**.



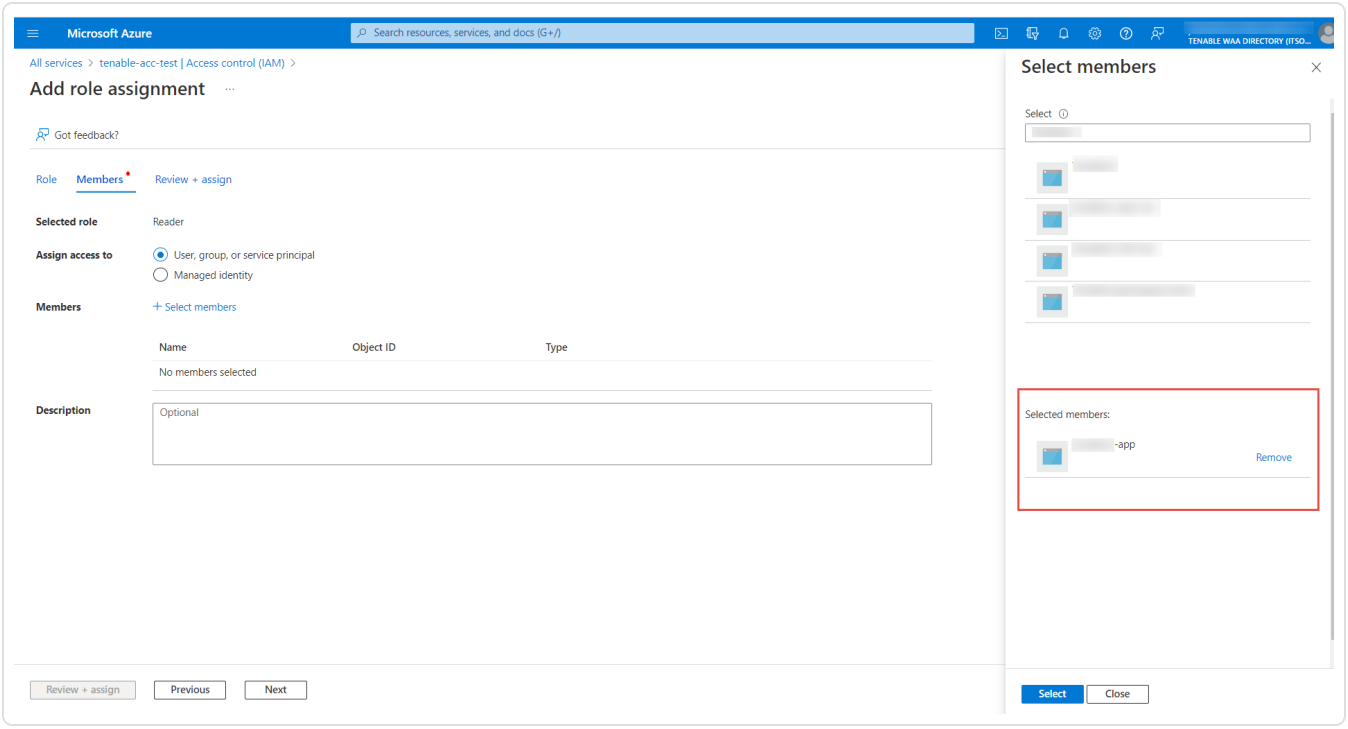
8. In the **Add role assignment** window, in the **Role** tab, search and select **Reader**.



9. In the **Members** tab, in the **Assign access to** section, select **User, group, or service principal**.

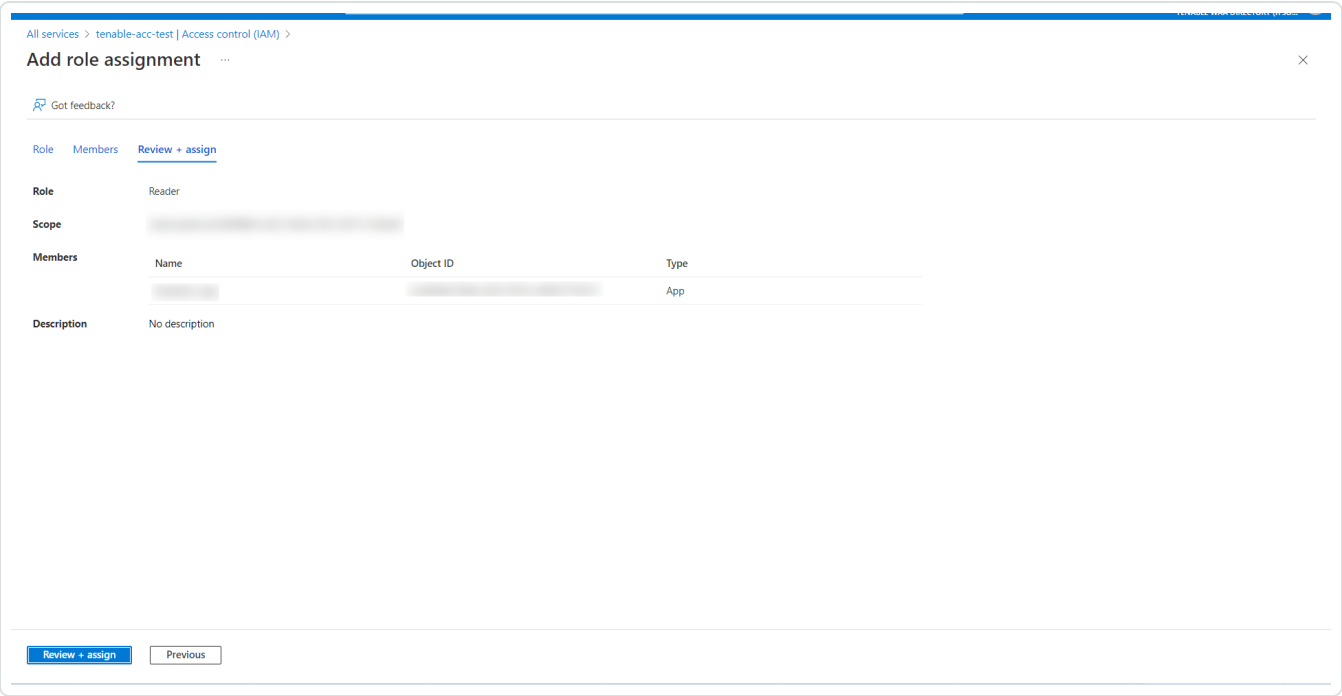


10. To select your Azure Application, click **+ Select Members**.



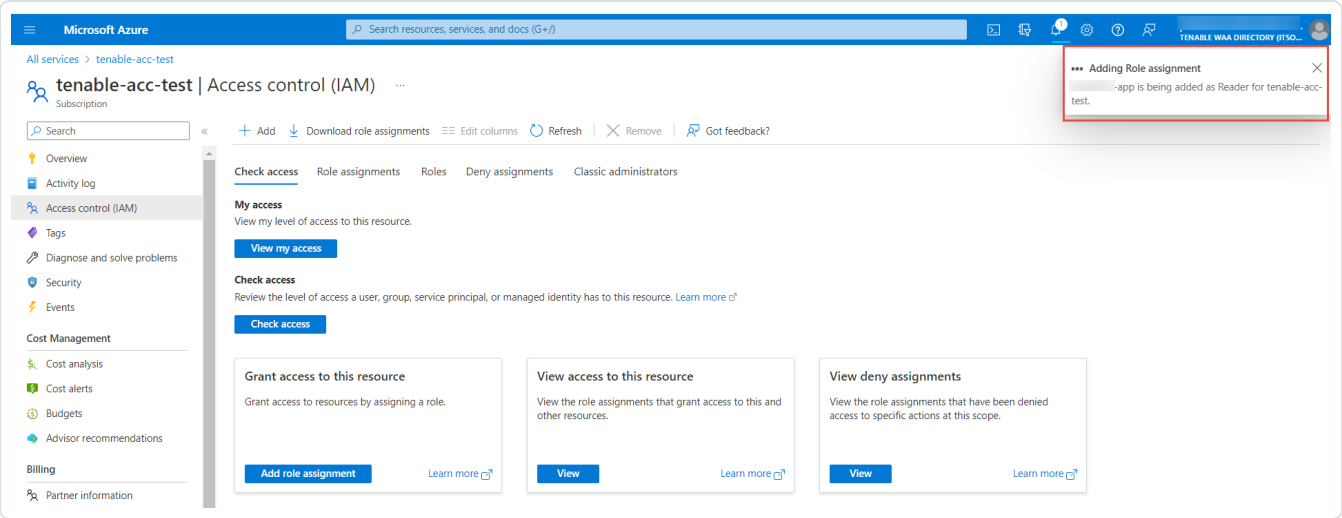
The **Select members** plane appears.

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

> **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 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.

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)

Required User Role: Administrator

Before you can use Tenable Vulnerability Management GCP connectors, you must configure GCP to support your connectors.

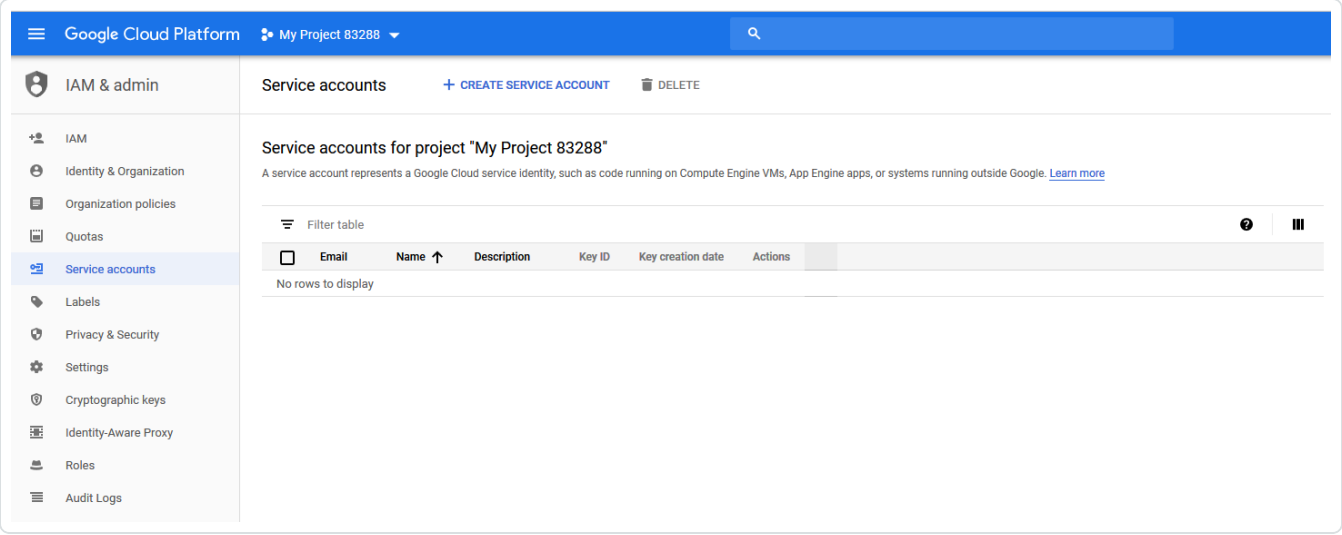
Note: Before configuring, you must enable the compute engine API for each project you want scanned from within Google Cloud Platform. See the Google API documentation for more information.

To configure GCP to support Tenable Vulnerability Management connectors:

1. Log into Google Cloud Platform.
2. In the left navigation bar, select **IAM & admin**.

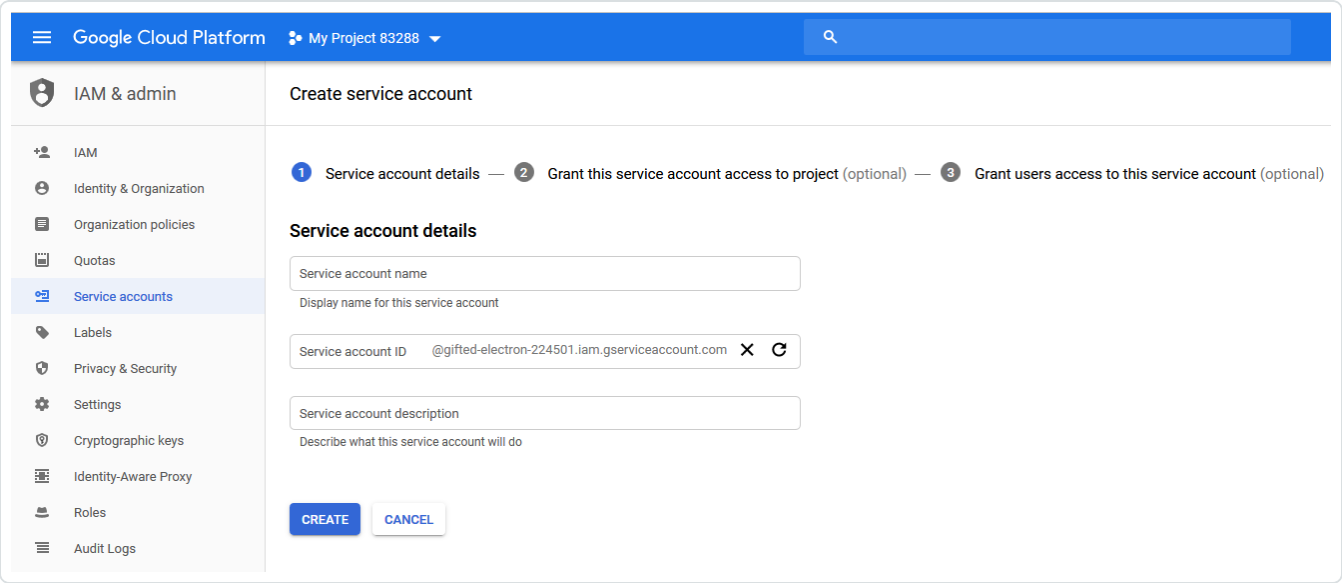
   The **IAM & admin** page appears.
3. In the **Select a project** drop-down box in the upper-left, select the applicable GCP project.
4. In the left navigation bar, select **Service accounts**.

   The **Service accounts** page for your GCP project appears.



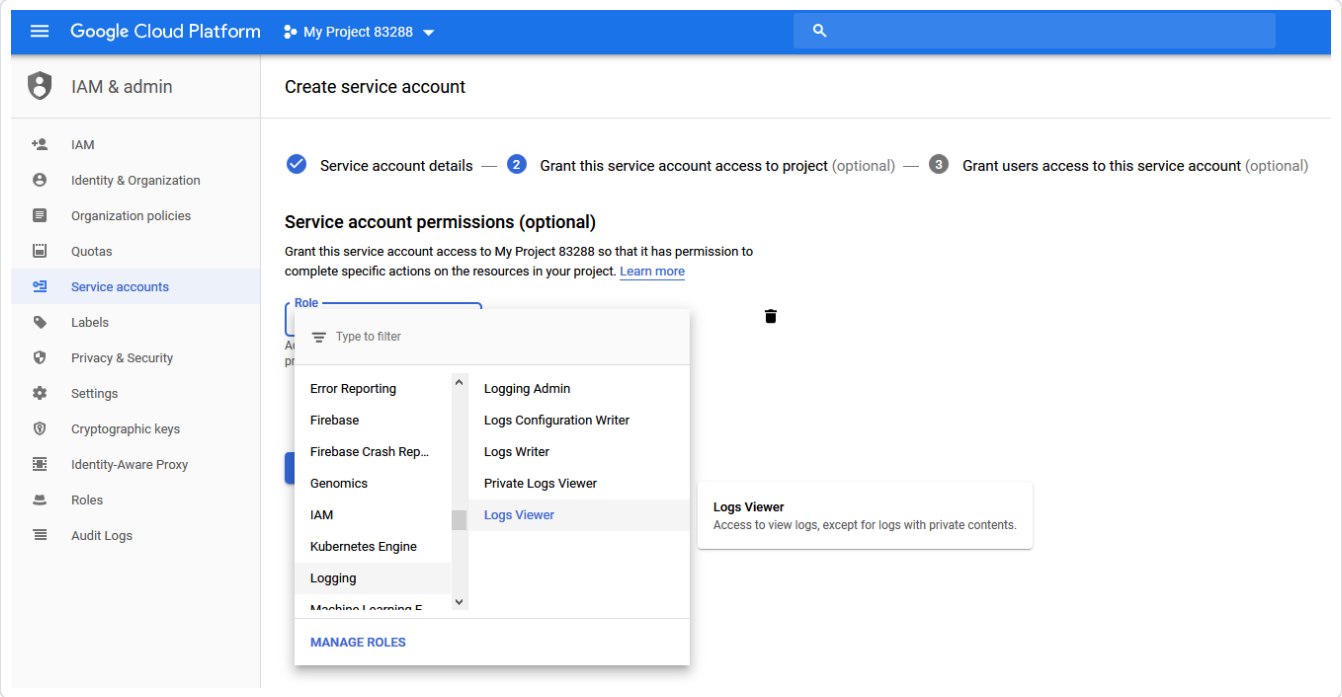
5. Click **+ CREATE SERVICE ACCOUNT**.

   The **Create service account** page appears.



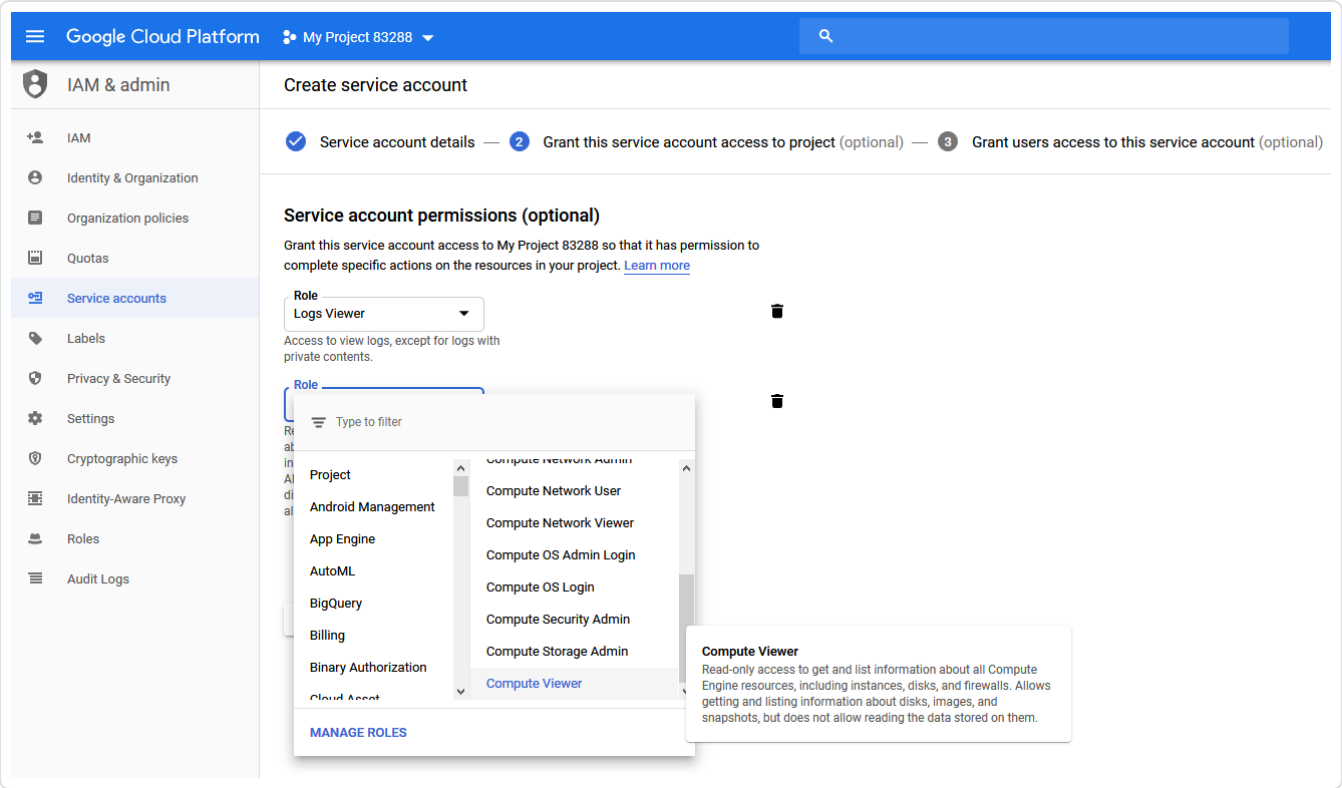
6. In the **Service account name** box, type a display name for your service account.
7. In the **Service account ID** box, type a unique service account ID.
8. In the **Service account description** box, describe what the service account will do.
9. Click the **CREATE** button.

   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 the **Continue** button.

    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 the **CREATE** button.

17. Your browser downloads the key in JSON format.

(Optional) To configure a GCP service account that can access multiple projects:

You may have dozens of GCP accounts that are added and removed 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 that is configured with access to the top-level service account. Only add projects that you want the GCP connector to pull data from.

1. Log into Google Cloud Platform.
2. In the left navigation bar, select **IAM & admin**.

   The **IAM & admin** 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 that 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. (Optional) Click the **+ ADD ANOTHER ROLE** button to add additional roles.
10. To add additional projects, repeat steps 3 through 9.

What to do next:

- Create a GCP Connector, as described in Create a Google Cloud Platform Connector (Discovery Only).

Create a Google Cloud Platform Connector (Discovery Only)

Required User Role: Administrator

Before you begin:

- Complete the required GCP configuration steps.

To create a GCP 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 Connector** button.

   The **Select a Connector** pane appears.

5. In the **Connectors** section, click **Google Cloud Platform**.

   The **Google Cloud Platform** pane appears.

6. In the **Connector Name:** box, type a name to identify the connector.

7. In the **Service Account Key** section, click **Add File** to upload your service account key that you obtained when configuring GCP.

8. 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.

9. 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.

10. 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.

11. Do one of the following:

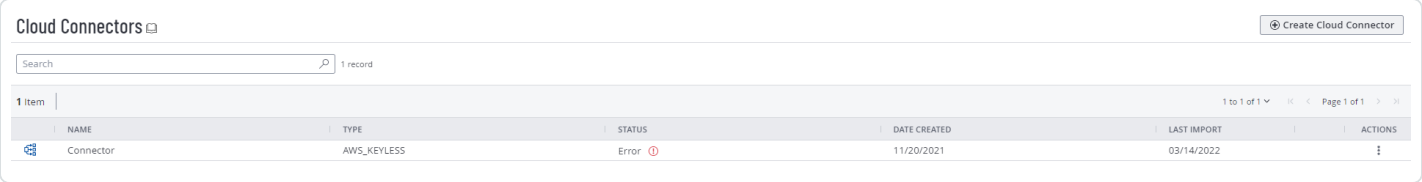
    - To save the connector, click **Save**.
    - To save the connector and import your assets from GCP, click **Save & Import**.

> **Note:** There may be a short delay before your assets appear in Tenable Vulnerability Management.

Manage Existing Connectors

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

The **Cloud Connectors** page displays the Connecotrs table, which lists all your configured connectors.



Launch a Connector Import Manually

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

Required User Role: Administrator

To launch a manual import for a 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 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

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

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 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 **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

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

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 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 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.

5. 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

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

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 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 connector table, click the connector that you want to edit.

   The **Edit Connector** pane appears.

5. 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.

6. 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 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 connector table, click the connector that you want to edit.

   The **Edit Connector** pane appears.

5. 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.

6. (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.

7. 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 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 connector table, click the connector that you want to edit.

   The **Edit Connector** pane appears.

5. 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.

6. Click **Save**.

   Tenable Vulnerability Management saves the connector. There may be a short delay before your assets appear in Tenable Vulnerability Management.

To edit a Tenable Container Security connector:

1. Log in to Tenable Container Security. For information about how to log in, see Log In to Tenable Container Security in the *Tenable Container Security User Guide*.
2. In the **Connectors** section of the Container Security dashboard, click **View Connectors**.

   The **Connectors** page appears.

3. In the connector table, click the connector you want to edit.

   The **Enter Connector Details** pane appears.

4. Modify one or more of the following connector details:

   - In the **URL** box, change the URL.
   - In the **PORT** box, change the port ID.
   - In the **USER NAME** box, change your username.
   - In the **PASSWORD** box, change your password.

5. Click **Save**.

   The connector saves. There may be a short delay before your assets appear in Tenable Vulnerability Management.

Note: For more information about Tenable Container Security connectors, see Configure Connectors to Import Images in the *Tenable Vulnerability Management Container Security User Guide*.

Delete a Connector

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

Required User Role: Administrator

To delete a 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 connector table, click the ✕ button next to the connector that you want to delete.

   A **Confirm Deletion** window appears.

5. Click **Delete**.

   Tenable Vulnerability Management deletes the connector.

What to do next:

- If you deleted an AWS connector with keyless authentication, see Manually Delete Connector Artifacts in AWS.

Remove Frictionless Assessment

Frictionless Assessment is now End of Provisioning (starting May 15, 2023), and new users will not be able to deploy Frictionless Assessment connectors. Frictionless Assessment will reach End-of-Support on December 31, 2023, and will no longer receive support or updates. However, existing Frictionless Assessment connectors will continue to function until the feature is End-of-Life on December 31, 2024. Tenable recommends that you transition to Tenable Cloud Security with Agentless Assessment for scanning your cloud resources. For more information, see the Tenable Vulnerability Management Release Notes.

Required User Role: Administrator

You can remove or offboard your existing AWS and Azure connectors from your Tenable container when you upgrade to Agentless Assessment.

- Remove AWS Frictionless Assessment
- Remove Azure Frictionless Assessment

Remove AWS Frictionless Assessment

There are two types of connectors:

- AWS Frictionless Assessment connector with keyless authentication
- AWS Frictionless Assessment connector

AWS Frictionless Assessment Connector with Keyless Authentication

Considerations before removing the AWS Frictionless Assessment connector with keyless authentication:

- This connector includes both discovery and Frictionless Assessment functionality.
- After deletion, you must create another discovery connector to continue the discovery functionality.
- Check if the connector deployed one of the following CloudFormation templates during the creation process.
  - AWS Keyless Frictionless Assessment single tag CloudFormation template
  - AWS Keyless Frictionless Assessment CloudFormation template

To remove the AWS Frictionless Assessment connector with keyless authentication:

1. Delete the AWS connector. For more information, see Delete a Connector.

   Tenable removes the following AWS Systems Manager resources from your account:

   - `TenableInventoryAssociation` — AWS Systems Manager association name.
   - `TenableInventoryCollection` — AWS Systems Manager document name.
   - `tenb-inv-upload-<customerRegionName>-<clusterName>-sync` — ResourceDataSync.
2. In AWS, verify if the AWS Systems Manager resources are removed from your account.
3. In AWS, remove the Stack instance with the name `tenableio-connector-aws-keyless-fa-single-tag-cft` or `tenableio-connector-aws-keyless-fa-cft`.

This removes the permissions that Tenable required to perform the Frictionless Assessment inventory scanning and discovery.

4. (Optional) Remove the tags for AWS EC2 instances used for Frictionless Assessment.

AWS Frictionless Assessment Connector

Considerations before removing AWS Frictionless Assessment connector:

- This connector includes only the Frictionless Assessment functionality.
- The CloudFormation StackSet deployed the AWS Systems Manager resources for this connector. Therefore, when you delete the stack instances and the StackSet from your AWS Account, the AWS Systems Manager resources are removed.
- Check if you have set up a separate discovery connector for the same account as the one for the Frictionless Assessment connector. This discovery connector detects terminated assets. There is no need to remove this discovery connector as it continues to discover and import assets from your AWS account.

To remove the AWS Frictionless Assessment connector:

1. In Tenable Vulnerability Management, delete the AWS Frictionless Assessment connector. For more information, see Delete a Connector.

   Tenable removes the backend configuration for the connector so that the inventory for your account is no longer processed.

2. In AWS, remove the StackSet that you deployed with this CloudFormation template from your AWS account.

   This removes the AWS Systems Manager association, AWS Systems Manager document, and ResourceDataSync from your account. When this step is complete, Tenable no longer receives your inventory for scanning.

3. (Optional) Remove the tags for EC2 instances scanned by Frictionless Assessment.

Remove Azure Frictionless Assessment

The Azure Frictionless Assessment is similar to AWS Frictionless Assessment connector.

To remove Azure Frictionless Assessment connector:

1. In Tenable Vulnerability Management, delete the Azure Frictionless Assessment connector. For more information, see Delete a Connector.
2. In the Azure portal, locate and delete the `Tenable-FA-Connector-*` resource group.

   This is the resource group deployed by the ARM template when you created the Azure Frictionless Assessment connector.
3. (Optional) Remove the tags used for Frictionless Assessment.