



# Tenable PCI ASV User Guide

Last Revised: July 23, 2025



## Table of Contents

<b>Welcome to Tenable PCI ASV</b>	<b>4</b>
Get Started with Tenable PCI ASV Scanning	5
Log in to Tenable PCI ASV	6
Log Out of Tenable PCI ASV	7
Navigate Tenable PCI ASV	7
Planes	15
Tenable PCI ASV Workbench Tables	16
Filter a Table	18
<b>Tenable PCI ASV Workbench</b>	<b>21</b>
<b>Create a Tenable PCI ASV Scan</b>	<b>26</b>
Tenable PCI ASV Scan Templates	28
Tenable PCI ASV Scan Settings for Vulnerability Management	29
Basic Settings in Tenable PCI ASV	30
Discovery Settings in Tenable PCI ASV	36
Discovery Settings for Custom Scan Type	37
Assessment Settings in Tenable PCI ASV	46
Assessment Settings for Custom Mode	48
Report Settings in Tenable PCI ASV Scans	57
Advanced Settings in Tenable PCI ASV	59
Custom Advanced Settings in Tenable PCI ASV Scans	61
Tenable PCI ASV Scan Settings for Tenable Web App Scanning	67
Basic Settings in Tenable Web App Scanning Scans	67
Scope Settings in Tenable Web App Scanning Scans	72



Report Settings in Tenable Web App Scanning Scans .....	74
Assessment Settings in Tenable Web App Scanning Scans .....	75
Advanced Settings in Tenable Web App Scanning Scans .....	75
<b>Launch a Tenable PCI ASV Scan .....</b>	<b>82</b>
Scan Status .....	83
<b>Submit a Scan for PCI Validation .....</b>	<b>86</b>
<b>Create an Attestation .....</b>	<b>90</b>
Mark an Asset as Out of Scope .....	93
Disputes .....	94
Create a Dispute .....	95
Edit a Dispute .....	99
Clone a Dispute to an Attestation .....	99
Delete a Dispute .....	100
Dispute Reasons .....	101
Export Attestations .....	103
<b>Submit an Attestation for ASV Review .....</b>	<b>106</b>
Attestation Status .....	113
<b>Respond to an ASV Review Information Request .....</b>	<b>114</b>
<b>Download Completed Attestation Reports .....</b>	<b>116</b>
<b>Tenable PCI ASV Settings .....</b>	<b>117</b>



## 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.

**Tip:** In addition to the Tenable PCI ASV workbench, you can use Tenable Vulnerability Management to launch PCI-related scans via Tenable Nessus scanners and Tenable Agents.

You can use the **PCI Internal Nessus Agent** (DSS 4.0) and **Internal PCI Network Scan** (DSS 11.3.1.2) templates together to achieve full internal coverage of your systems. Additionally, you can use the **PCI Quarterly External Scan** to perform the quarterly external scans that are required by PCI.

For more information, see [Scan Templates](#) in the *Tenable Vulnerability Management User Guide*.



## Get Started with Tenable PCI ASV Scanning

**Important:** Only Administrator users can perform the scanning portions of the following workflow.

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](#):
  - (Required) A Tenable PCI ASV scan with the **PCI Quarterly External Scan** template.
  - (Optional, if web apps are present) 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).

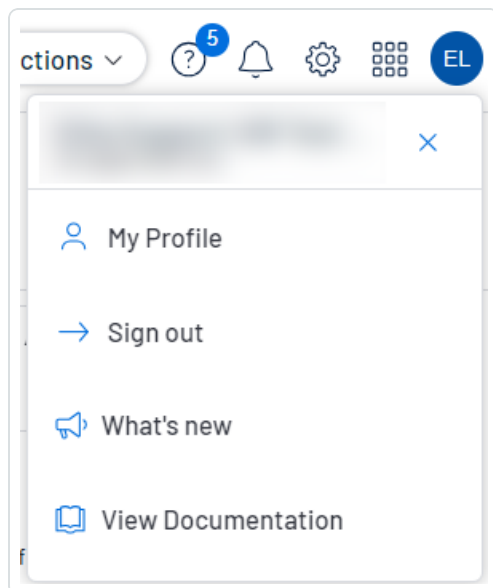
## Log Out of Tenable PCI ASV

**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

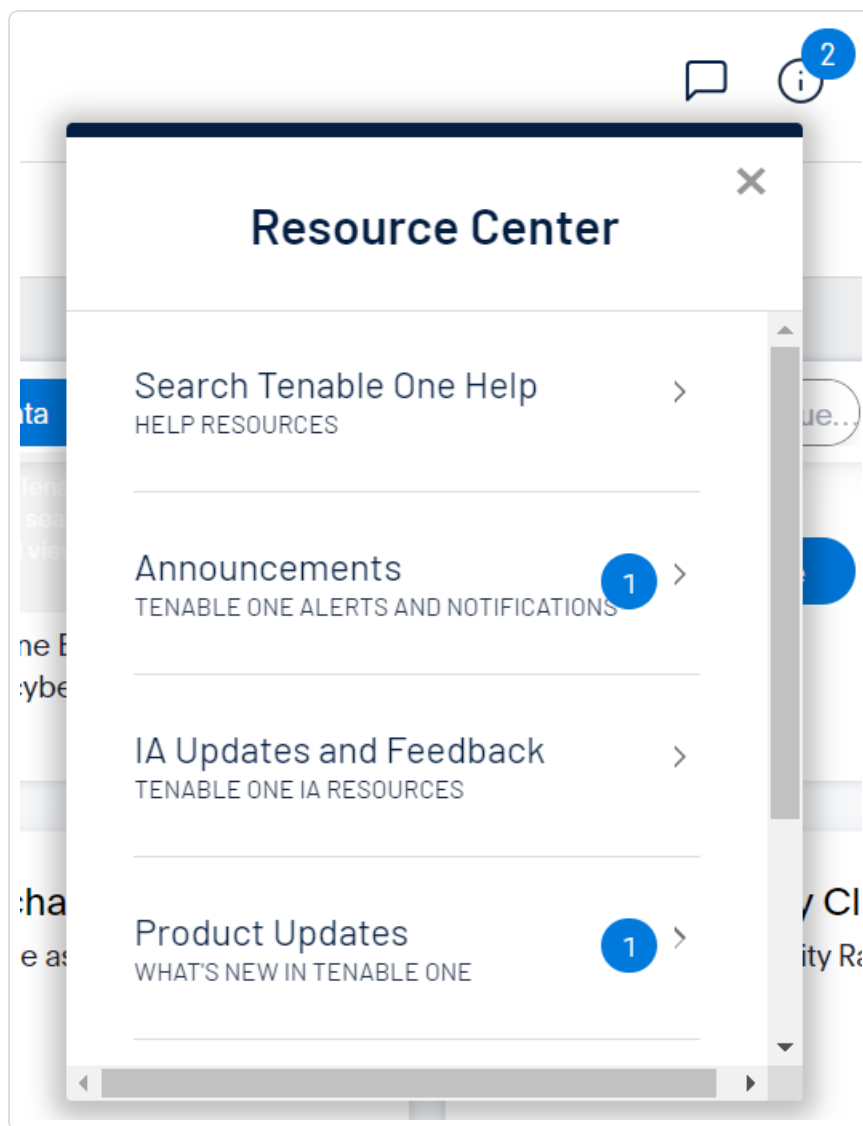
The **Resource Center** displays a list of informational resources including product announcements, Tenable blog posts, and user guide documentation.

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

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

**Note:** For more information, see [Settings](#) within the *Tenable Vulnerability Management User Guide*.

## Workspace


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

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

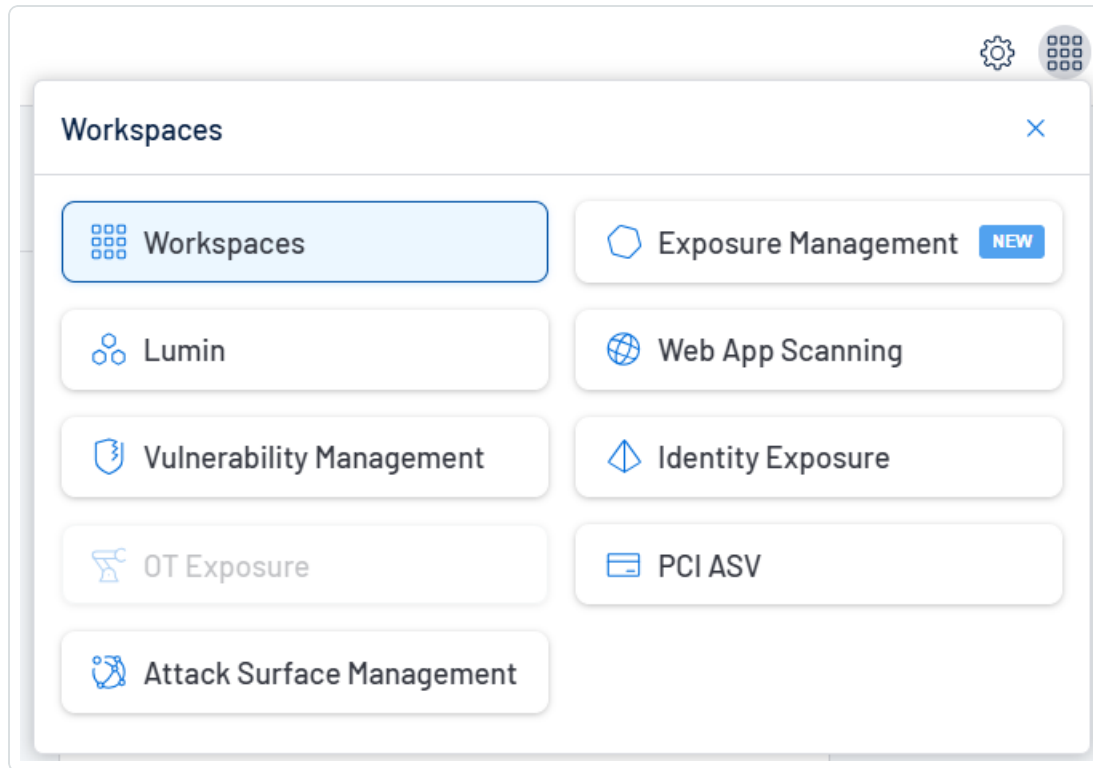
## Open the Workspace Menu

To open the **Workspace** menu:



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


The **Workspace** menu appears.



2. Click an application tile to open it.

## View the Workspace Page

To view the Workspace page:

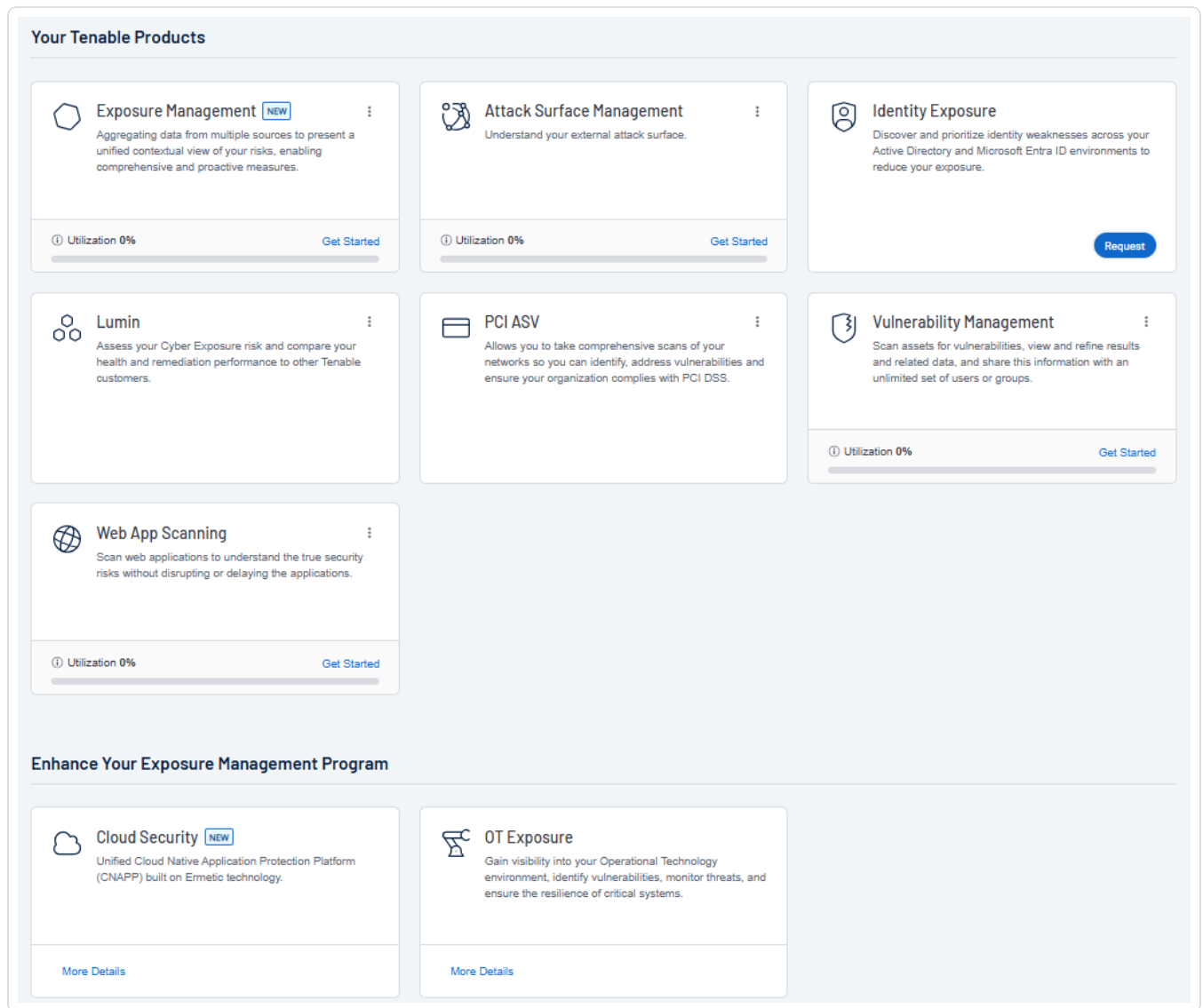
1. From any Tenable application, in the upper-right corner, click the  button.

The **Workspace** menu appears.

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



The **Workspace** page appears.



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

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

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

- Set a default application:



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

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

To set a default login application:

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

A menu appears.

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

This application now appears when you log in.

- Remove a Default Application:

To remove a default login application:

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

A menu appears.

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

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

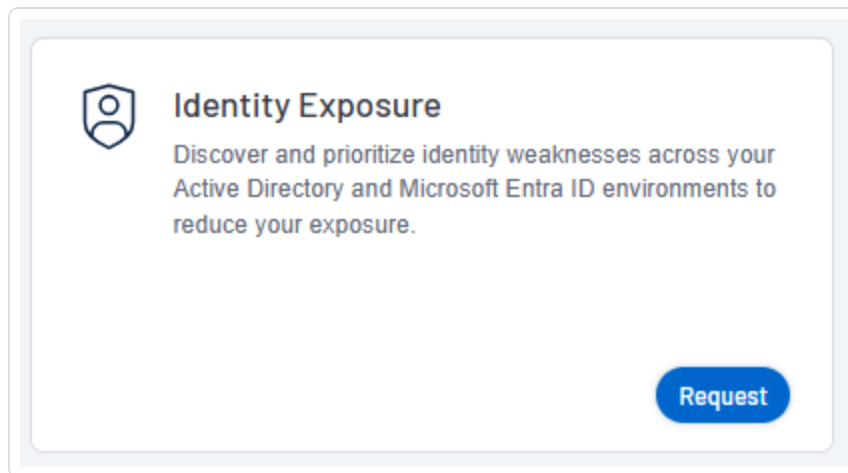
- Request Access to a Tenable application:

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

To request access to a Tenable application:



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



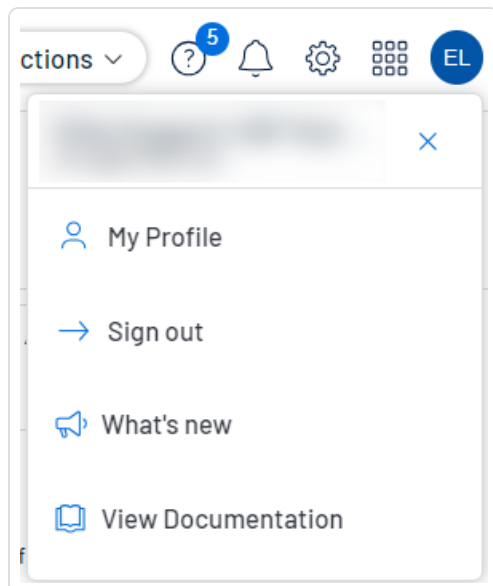
You navigate directly to the request page for the selected application.

## User Account Menu

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

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

The user account menu appears.





2. Do one of the following:

- Click **My Profile** to configure your own user account. You navigate directly to the **My Account** settings page.
- 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:

[Planes](#)


[Tenable PCI ASV Workbench Tables](#)

## 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: <ol style="list-style-type: none"><li>a. Click the box to display the drop-down list.</li></ol>



	b. Search for and select one of the listed values.
Multiple valid values	<p>To select one or more values:</p> <ol style="list-style-type: none"><li>Click the box to display the drop-down list.</li><li>Search for and select a value.  The selected value appears in the box.</li><li>Repeat until you have selected all appropriate values</li><li>Click outside the drop-down list to close it.</li></ol> <p>To deselect values:</p> <ol style="list-style-type: none"><li>Roll over the value you want to remove.  The ✕ button appears over the value.</li><li>Click the ✕ button.  The value disappears from the box.</li></ol>

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:

- 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.

PCI WAS Scans must be combined with a PCI Quarterly External Scan before submitting for ASV review. For information on combining scans, please reference our <a href="#">KB article</a> with steps.						
PCI ASV						
New Scan Results   In Remediation   In ASV Review   Attestations						
1 Item   1 to 1 of 1   Page 1 of 1						
NAME	SCAN TYPE	ASSETS	FAILURES	IMPORT STATUS	END DATE	ACTIONS
PCI Pub Target Scan Created By Hemant Barot	Nessus	3	136	Complete	March 27 at 5:36 AM	


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








<b>Actions</b>	<p>Click the  button to view available actions for the scan:</p> <ul style="list-style-type: none"><li>• <b>Start Attestation</b> — Begin an attestation for the scan. For more information, see <a href="#">Create an Attestation</a>.</li><li>• <b>Delete</b> — Delete the scan:<ol style="list-style-type: none"><li>a. Click <b>Delete</b>. A confirmation message appears.</li><li>b. Click <b>Delete</b>. Tenable PCI ASV deletes the scan from the table.</li></ol></li></ul>
----------------	---

- **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
<b>Name</b>	The name of the attestation.
<b>Owner</b>	The owner of, or person who created, the attestation.
<b>Assets</b>	The number of assets associated with the attestation.
<b>Failures</b>	The number of failures associated with the attestation.
<b>Status</b>	<p>The status of the attestation draft:</p> <ul style="list-style-type: none"><li>• <b>In-Progress</b> — You are actively working on the attestation report.</li><li>• <b>Needs Work</b> — The attestation report has been sent back to you to provide more information to the assessor before the attestation can be resubmitted for ASV review.</li></ul>



<b>ASV Message</b>	Where applicable, a message from the ASV reviewer regarding the attestation status.
<b>Last Modified</b>	The date and time at which the attestation was last modified by a user.
<b>Actions</b>	<p>Click the  button to view available actions for the attestation:</p> <ul style="list-style-type: none"><li>• <b>Send to ASV Review</b> – Submit the attestation for ASV review. For more information, see <a href="#">Submit an Attestation for ASV Review</a>.</li><li>•  <b>ASV Scan Report Summary</b> – Download the ASV Scan Report Summary as a PDF export file.</li><li>•  <b>ASV Scan Report Vulnerability Details</b> – Download the ASV Scan Report for Vulnerability Details as a PDF export file.</li><li>• <b>Delete</b> – Delete the attestation:<ol style="list-style-type: none"><li>a. Click <b>Delete</b>. A confirmation message appears.</li><li>b. Click <b>Delete</b>. Tenable PCI ASV deletes the scan from the table.</li></ol></li><li>•  <b>Feedback</b> – Download a feedback form for the attestation in PDF format.</li><li>•  <b>Export</b> – Export the attestation. For more information, see <a href="#">Export Attestations</a>.</li></ul>

- **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
<b>Name</b>	The name of the attestation.
<b>Owner</b>	The owner of, or person who created, the attestation.
<b>Assets</b>	The number of assets associated with the attestation.
<b>Failures</b>	The number of failures associated with the attestation.
<b>Disputes</b>	The number of disputes associated with the attestation.
<b>Status</b>	<p>The <a href="#">status</a> of the attestation, for example, <b>Assigned</b> or <b>In-Review</b>.</p> <div><b>Note:</b> An attestation may show a status of <b>Info Provided</b> even if there are still disputes that require additional information. In this case, the number of disputes that require additional information appears in parentheses beside the attestation status.</div>
<b>Last Modified</b>	The date and time at which the attestation was last modified by a user.
<b>Actions</b>	<p>Click the <b>:</b> button to view available actions for the attestation:</p> <ul style="list-style-type: none"><li>• <b>↓ ASV Scan Report Summary</b> – Download the ASV Scan Report Summary as a PDF export file.</li><li>• <b>↓ ASV Scan Report Vulnerability Details</b> – Download the ASV Scan Report for Vulnerability Details as a PDF export file.</li><li>• <b>↓ Feedback</b> – Download a feedback form for the attestation in PDF format.</li><li>• <b>[→ Export</b> – Export the attestation. For more information, see <a href="#">Export Attestations</a>.</li></ul>

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

This table includes the following information:





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

Column	Details
<b>Name</b>	The name of the attestation.
<b>Owner</b>	The owner of, or person who created, the attestation.
<b>Assets</b>	The number of assets associated with the attestation.
<b>Failures</b>	The number of failures associated with the attestation.
<b>Disputes</b>	The number of disputes associated with the attestation.
<b>Status</b>	The status of the attestation, for example, <b>Passed</b> or <b>Failed</b> .
<b>Last Modified</b>	The date and time at which the attestation was last modified by a user.
<b>Actions</b>	<p>Click the <b>:</b> button to view available actions for the attestation:</p> <ul style="list-style-type: none"><li>• <b>↓ ASV Scan Report Summary</b> – Download the ASV Scan Report summary as a PDF export file.</li><li>• <b>↓ ASV Scan Report Vulnerability Details</b> – Download the ASV Scan Report for Vulnerability Details as a PDF export file.</li><li>• <b>↓ Feedback</b> – Download a feedback form for the attestation in PDF format.</li><li>• <b>[→ Export</b> – Export the attestation. For more information, see <a href="#">Export Attestations</a>.</li></ul>



## 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**.

**Note:** If you re-scan an already scanned network, Tenable PCI ASV creates a new, separate scan for the network. Tenable recommends re-scanning networks after remediation is complete to confirm any failures have been fixed.

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	<p>Configure the settings available in the scan template.</p> <p><b>Vulnerability Management Scan using the Internal PCI Network Scan or PCI Quarterly External Scan templates</b></p> <ul style="list-style-type: none"><li>• <a href="#">Basic</a> – 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.</li><li>• <a href="#">Discovery</a> – Specifies how a scan performs discovery and port scanning.</li><li>• <a href="#">Assessment</a> – 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.</li></ul> <div><b>Note:</b> Assessment settings appear only on Internal PCI Network Scan templates.</div> <ul style="list-style-type: none"><li>• <a href="#">Report</a> – Specifies whether the scan generates a report.</li></ul> <div><b>Note:</b> Report settings appear only on Internal PCI Network Scan templates.</div> <ul style="list-style-type: none"><li>• <a href="#">Advanced</a> – Specifies advanced controls for scan efficiency.</li></ul>
	<p><b>Tenable Web App Scanning scan using the PCI template</b></p> <ul style="list-style-type: none"><li>• <a href="#">Basic</a> – 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.</li><li>• <a href="#">Scope</a> – Specifies the URLs and file types that you want to</li></ul>



	<p>include in or exclude from your scan.</p> <ul style="list-style-type: none"><li>• <a href="#">Assessment</a> – Specifies which web application elements you want the scanner to audit as it crawls your URLs.</li><li>• <a href="#">Report</a> – Specifies extra items to include in the scan report.</li><li>• <a href="#">Advanced</a> – Specifies advanced controls you want to implement in a web application scan.</li></ul>
<b>Credentials</b>	<p>PCI ASV scans are designed from an external threat's perspective. As such, PCI ASV scans mirror the Basic scan template, which allows for a minimal set of credentials. While <b>Credentials</b> options are available when creating a PCI ASV scan, you should NOT configure these settings as they change the intent of the scan and can ultimately lead to scan complications and PCI failures.</p>

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	<p>Performs an internal PCI DSS (11.2.1) vulnerability scan.</p> <p>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.</p> <div><b>Note:</b> 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).</div>
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	Description
---------	---------	-------------



Value		
Name	None	Specifies the name of the scan.
Description	None	(Optional) Specifies a description of the scan.
Scan Results	Keep private	<p>Specifies whether the results of the scan should appear in dashboards or be kept private.</p> <p>When set to <b>Keep private</b>, the scan results <b>Last Seen</b> dates do not update and you must access the scan directly to view the results.</p> <div><b>Important:</b> By default, PCI scan data is excluded from dashboards, reports, and workbenches. To view this data, you must set the <b>Scan Results</b> setting to <b>Show in the workbenches, dashboards, and reports</b>.</div>
Folder	My Scans	<p>Specifies the <a href="#">folder</a> where the scan appears after being saved.</p> <p>You cannot specify a folder when you launch a remediation scan. All remediation scans appear in the <b>Remediation Scans</b> folder only.</p>
Scanner Type	Internal Scanner	Specifies whether a local, internal scanner or a cloud-managed scanner performs the scan, and determines whether the <b>Scanner</b> field lists local or cloud-managed scanners to choose from.
Scanner	Auto-Select	<p>Select a scanner based on the location of the targets you want to scan. For example:</p> <ul style="list-style-type: none"><li>Select a <a href="#">linked scanner</a> to scan non-routable IP addresses.</li></ul> <div><b>Note:</b> Auto-select is not available for <a href="#">cloud scanners</a>.</div> <ul style="list-style-type: none"><li>Select a <a href="#">scanner group</a> if you want to:<ul style="list-style-type: none"><li>Improve scan speed by balancing the scan load</li></ul></li></ul>



		<p>among multiple scanners.</p> <ul style="list-style-type: none"><li>◦ Rebuild scanners and link new scanners in the future without having to update scanner designations in scan configurations.</li><li>• Select <b>Auto-Select</b> to enable <a href="#">scan routing</a> for the targets.</li></ul>
Tags	None	Select one or more <a href="#">tags</a> to scan all assets that have any of the specified tags applied. To see a list of assets identified by the specified tags, click <b>View Assets</b> .
Scan Window	Disabled	<p>(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.</p> <div><p><b>Note:</b> 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 <b>Completed</b> after the scan window is complete. Once Tenable PCI ASV indexes the scan, it shows as <b>Completed</b>.</p></div>
Network	Default	
Targets	None	<p>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.</p> <p>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.</p> <div><p><b>Tip:</b> You can force Tenable PCI ASV to use a given hostname for a server during a scan by using the <code>hostname[ip]</code> syntax</p></div>





		<p>(for example, <code>www.example.com[192.168.1.1]</code>). However, you cannot use this approach if you enable scan routing for the scan.</p> <p><b>Note:</b> You cannot apply more than 300,000 IP address targets to a scan. To learn more about scan limitations in Tenable PCI ASV, see <a href="#">Scan Limitations</a>.</p> <p><b>Note:</b> See <a href="#">Permissions</a> for more information on how permissions affect targets.</p>
Upload Targets	None	<p>Uploads a text file that specifies targets.</p> <p>The targets file must be formatted in the following manner:</p> <ul style="list-style-type: none"><li>• ASCII file format</li><li>• Only one target per line</li><li>• No extra spaces at the end of a line</li><li>• No extra lines following the last target</li></ul> <p><b>Note:</b> Unicode/UTF-8 encoding is not supported.</p>

## 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.



		<ul style="list-style-type: none"><li>• <b>Once:</b> Schedule the scan at a specific time.</li><li>• <b>Daily:</b> Schedule the scan to occur every 1-20 days, at a specific time.</li><li>• <b>Weekly:</b> Schedule the scan to occur every 1-20 weeks, by time and day or days of the week.</li><li>• <b>Monthly:</b> Schedule the scan to occur every 1-20 months, by:<ul style="list-style-type: none"><li>• <b>Day of Month:</b> 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.</li><li>• <b>Week of Month:</b> 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.</li></ul></li></ul> <div><p><b>Note:</b> 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.</p></div> <ul style="list-style-type: none"><li>• <b>Yearly:</b> Schedule the scan to occur every 1-20 years, by time and date.</li></ul>
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 <i>09/31/2018</i> and <i>09:30</i> .
Timezone	Varies	Specifies the timezone of the value set for <b>Starts</b> .

## 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 <b>Trash</b> folder. They cannot view the scan configuration or permanently delete the scan.
Can Execute	<p>In addition to the tasks allowed by <b>Can View</b>, groups and users with this permission can launch, pause, and stop a scan. They cannot view the scan configuration or permanently delete the scan.</p> <div><b>Note:</b> In addition to <b>Can Execute</b> permissions for the scan, users running a scan must have <b>Can Scan</b> permissions in an access group for the specified target, or the scanner does not scan the target.</div>
Can Edit	<p>In addition to the tasks allowed by <b>Can Execute</b>, 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.</p> <div><b>Note:</b> Only the scan owner can change scan ownership.</div> <div><b>Note:</b> User roles override scan permissions in the following cases:<ul style="list-style-type: none"><li>• A basic user cannot run a scan or configure a scan, regardless of the permissions assigned to that user in the individual scan.</li><li>• An administrator always has the equivalent of <b>Can Edit</b> permissions, regardless of the permissions set for the administrator account in the individual scan.</li></ul></div>

## 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)	<ul style="list-style-type: none"><li>• General Settings:<ul style="list-style-type: none"><li>◦ Always test the local Nessus host</li><li>◦ Use fast network discovery</li></ul></li><li>• Port Scanner Settings:</li></ul>



		<ul style="list-style-type: none"><li>◦ Scan common ports</li><li>◦ Use netstat if credentials are provided</li><li>◦ Use SYN scanner if necessary</li><li>• Ping hosts using:<ul style="list-style-type: none"><li>◦ TCP</li><li>◦ ARP</li><li>◦ ICMP (2 retries)</li></ul></li></ul>
	<b>Port scan (all ports)</b>	<ul style="list-style-type: none"><li>• General Settings:<ul style="list-style-type: none"><li>◦ Always test the local Nessus host</li><li>◦ Use fast network discovery</li></ul></li><li>• Port Scanner Settings:<ul style="list-style-type: none"><li>◦ Scan all ports (1-65535)</li><li>◦ Use netstat if credentials are provided</li><li>◦ Use SYN scanner if necessary</li></ul></li><li>• Ping hosts using:<ul style="list-style-type: none"><li>◦ TCP</li><li>◦ ARP</li><li>◦ ICMP (2 retries)</li></ul></li></ul>
	<b>Custom</b>	<a href="#">All defaults</a>
<b>PCI Quarterly External Scan</b>	–	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	<p>If set to <b>On</b>, the scanner pings remote hosts on multiple ports to determine if they are alive. Additional options <b>General Settings</b> and <b>Ping Methods</b> appear.</p> <p>If set to <b>Off</b>, the scanner does not ping remote hosts on multiple ports during the scan.</p> <div><b>Note:</b> To scan VMware guest systems, <b>Ping the remote host</b> must be set to <b>Off</b>.</div>
General Settings		
Use Fast Network Discovery	Disabled	<p>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.</p> <p>When enabled, Tenable PCI ASV does not perform these checks.</p>
Ping Methods		
ARP	Enabled	<p>Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.</p>



TCP	Enabled	Ping a host using TCP.
Destination Ports (TCP)	Built-In	<p>Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that are checked via TCP ping.</p> <p>Type one of the following: <b>built-in</b>, a single port, or a comma-separated list of ports.</p> <p>For more information about which ports <b>built-in</b> specifies, see the <a href="#">knowledge base article</a>.</p>
ICMP	Enabled	Ping a host using the Internet Control Message Protocol (ICMP).
Assume ICMP Unreachable From the Gateway Means the Host is Down	Disabled	<p>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.</p> <div><b>Note:</b> 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.</div>
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	<p>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.</p> <p>When disabled, the scanner uses ICS/SCADA Smart Scanning to cautiously identify OT devices and stops scanning them once they are discovered.</p>
Wake-on-LAN		
List of MAC Addresses	None	<p>The Wake-on-LAN (WOL) menu controls which hosts to send WOL magic packets to before performing a scan.</p> <p>Hosts that you want to start prior to scanning are provided by uploading a text file that lists one MAC address per line.</p> <p>For example:</p> <div><pre>33:24:4C:03:CC:C7 FF:5C:2C:71:57:79</pre></div>
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	<p>Specifies the range of ports to be scanned.</p> <p>The supported ranges are:</p> <ul style="list-style-type: none"><li>• <code>default</code> – Instructs the scanner to scan approximately 4,790 commonly used ports specified in the <code>nessus-services</code> file. You can also combine the <code>default</code> keyword with other ports and port ranges.</li></ul> <div><p><b>Note:</b> You can convert the <code>nessus-services</code> file to a custom list of ports by performing four consecutive regular expression (regex) replace-all operations in a text editor that supports such operations:</p><ul style="list-style-type: none"><li>• <code>.*\s+(\d+)\s*/(tcp udp)(\r\n \r \n)</code> to <code>\$1/\$2,</code></li><li>• <code>(\d+)\s*/(tcp udp)</code> to <code>\$2:\$1</code></li><li>• <code>tcp</code> to <code>T</code></li><li>• <code>udp</code> to <code>U</code></li></ul><p>You can find the <code>nessus-services</code> file in the following directories, depending on your operating system:</p><ul style="list-style-type: none"><li>• Linux – <code>/opt/nessus/var/nessus/nessus-services</code></li><li>• Windows – <code>C:\ProgramData\Tenable\Nessus\nessus\ness</code></li></ul></div>



Setting	Default Value	Description
		<div><div>us-services</div><ul style="list-style-type: none"><li>macOS — /Library/Nessus/run/var/nessus/nessus-services</li></ul></div> <ul style="list-style-type: none"><li><b>all</b> — Instructs the scanner to scan all 65,536 ports, including port 0. You cannot combine the <b>all</b> keyword with other ranges.</li><li>A comma-separated list of ports (for example, <b>21,23,25,80,110</b>), port ranges (for example, <b>1-1024,9000-9200</b> or <b>1-65535</b> to scan all ports but 0 and <b>T:1-1024,U:300-500</b> or <b>1-1024,T:1024-65535,U:1025</b> to scan separate or overlapping TCP and UDP port ranges), or combinations thereof.</li></ul> <p>If you disable the UDP, SYN, or TCP port scanner settings in the scan policy <b>Discovery</b> settings, those ports are not scanned despite what range of ports you specify. The UDP and TCP port scanner settings are disabled by default; the SYN port scanner setting is enabled by default.</p>
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. To use this setting, you must first configure SSH Credentials.
WMI (netstat)	Enabled	When enabled, the scanner uses netstat to determine open ports while performing a WMI-based scan.  In addition, the scanner:



Setting	Default Value	Description
		<ul style="list-style-type: none"><li>• Ignores any custom range specified in the <b>Port Scan Range</b> setting.</li><li>• Continues to treat unscanned ports as closed if the <b>Consider unscanned ports as closed</b> setting is enabled.</li></ul> <p>If any port enumerator (netstat or SNMP) is successful, the port range becomes <i>all</i>. To use this setting, you must first configure Windows Credentials.</p>
SNMP	Enabled	When enabled, if the appropriate credentials are provided by the user, the scanner can better test the remote host and produce more detailed audit results. For example, there are many Cisco router checks that determine the vulnerabilities present by examining the version of the returned SNMP string. This information is necessary for these audits.
Only Run Network Port Scanners if Local Port Enumeration Failed	Enabled	<p>When this setting is enabled, the scanner relies on local port enumeration before relying on network port scans. If a local port enumerator runs, all network port scanners are disabled for the asset.</p> <p>When this setting is disabled, the scanner performs network port scans regardless of the local port enumeration status.</p>
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



Setting	Default Value	Description
		<b>Override Automatic Firewall Detection</b> option.
SYN	Enabled	<p>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.</p> <p>If you enable this option, you can also set the <b>Override Automatic Firewall Detection</b> option.</p>
Override Automatic Firewall Detection	Disabled	<p>This setting can be enabled if you enable either the <b>TCP</b> or <b>SYN</b> option.</p> <p>When enabled, this setting overrides automatic firewall detection.</p> <p>This setting has three options:</p> <ul style="list-style-type: none"><li>• <b>Use aggressive detection</b> attempts to run plugins even if the port appears to be closed. It is recommended that this option not be used on a production network.</li><li>• <b>Use soft detection</b> disables the ability to monitor how often resets are set and to determine if there is a limitation configured by a downstream network device.</li><li>• <b>Disable detection</b> disables the firewall detection feature.</li></ul>
UDP	Disabled	<p>This option engages the built-in Tenable Nessus UDP scanner to identify open UDP ports on the targets.</p> <p>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</p>



Setting	Default Value	Description
		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	<p>When enabled, the scanner attempts to map each open port with the service that is running on that port, as defined by the <b>Port scan range</b> option.</p> <div><b>Caution:</b> In some rare cases, probing might disrupt some services and cause unforeseen side effects.</div>
Search for SSL/TLS Based Services	On	<p>Controls how the scanner tests SSL-based services.</p> <div><b>Caution:</b> Testing for SSL capability on all ports may be disruptive for the tested host.</div>
Search for SSL/TLS/DTLS Services (enabled)		
Search for SSL/TLS On	Known SSL/TLS ports	<p>Specifies which ports on target hosts the scanner searches for SSL/TLS services.</p> <p>This setting has two options:</p> <ul style="list-style-type: none"><li>• <b>Known SSL/TLS ports</b></li><li>• <b>All TCP ports</b></li></ul>
Search for DTLS On	None	<p>Specifies which ports on target hosts the scanner searches for DTLS services.</p>



Setting	Default Value	Description
		This setting has the following options: <ul style="list-style-type: none"><li>• <b>None</b></li><li>• <b>Known SSL/TLS ports</b></li><li>• <b>All TCP ports</b></li></ul>
Identify Certificates Expiring Within x Days	60	When enabled, the scanner identifies SSL and TLS certificates that are within the specified number of days of expiring.
Enumerate All SSL/TLS Ciphers	True	When enabled, the scanner ignores the list of ciphers advertised by SSL/TLS services and enumerates them by attempting to establish connections using all possible ciphers.
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	<ul style="list-style-type: none"><li>• General Settings:<ul style="list-style-type: none"><li>◦ Avoid false alarms</li><li>◦ Disable CGI scanning</li></ul></li></ul>



		<ul style="list-style-type: none"><li>• Web Applications:<ul style="list-style-type: none"><li>◦ Disable web application scanning</li></ul></li></ul>
	<b>Scan for known web vulnerabilities</b>	<ul style="list-style-type: none"><li>• General Settings:<ul style="list-style-type: none"><li>◦ Avoid potential false alarms</li><li>◦ Enable CGI scanning</li></ul></li><li>• Web Applications:<ul style="list-style-type: none"><li>◦ Start crawling from "/"</li><li>◦ Crawl 1000 pages (max)</li><li>◦ Traverse 6 directories (max)</li><li>◦ Test for known vulnerabilities in commonly used web applications</li><li>◦ Generic web application tests disabled</li></ul></li></ul>
	<b>Scan for all web vulnerabilities (quick)</b>	<ul style="list-style-type: none"><li>• General Settings:<ul style="list-style-type: none"><li>◦ Avoid potential false alarms</li><li>◦ Enable CGI scanning</li></ul></li><li>• Web Applications:<ul style="list-style-type: none"><li>◦ Start crawling from "/"</li><li>◦ Crawl 1000 pages (max)</li><li>◦ Traverse 6 directories (max)</li><li>◦ Test for known vulnerabilities in commonly used web applications</li><li>◦ Perform each generic web app</li></ul></li></ul>



		test for 5 minutes (max)
	<b>Scan for all web vulnerabilities (complex)</b>	<ul style="list-style-type: none"><li>• General Settings:<ul style="list-style-type: none"><li>◦ Avoid potential false alarms</li><li>◦ Enable CGI scanning</li><li>◦ Perform thorough tests</li></ul></li><li>• Web Applications:<ul style="list-style-type: none"><li>◦ Start crawling from "/"</li><li>◦ Crawl 1000 pages (max)</li><li>◦ Traverse 6 directories (max)</li><li>◦ Test for known vulnerabilities in commonly used web applications</li><li>◦ Perform each generic web app test for 10 minutes (max)</li><li>◦ Try all HTTP methods</li><li>◦ Attempt HTTP Parameter Pollution</li></ul></li></ul>
	<b>Custom</b>	<a href="#">Assessment Settings for Custom Mode</a>
<b>PCI Quarterly External Scan</b>	–	–

## 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 <b>Show potential false alarms</b> , a flaw is reported every time, even when there is a doubt about the remote host being affected. Conversely, a paranoia setting of <b>Avoid potential false alarms</b> 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 speed)	Disabled	Causes various plugins to work harder. For example, when looking through SMB file shares, a plugin analyzes 3 directory levels deep instead of 1. This could cause much more network traffic and analysis in some cases. By being more thorough, the scan is more intrusive and is more likely to disrupt the network, while potentially providing better audit results.

## 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 applications	Disabled	By default, Tenable PCI ASV does not scan web applications. To edit the following settings, enable this setting.
Use a custom User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)	Specifies which type of web browser Tenable PCI ASV impersonates while scanning.
Web Crawler		
Start crawling	/	The URL of the first page that is tested. If



Setting	Default Value	Description
from		multiple pages are required, use a colon delimiter to separate them (e.g., <code>/:/php4:/base</code> ).
Excluded pages (regex)	<code>/server_privileges\.php &lt;&gt; log out</code>	<p>Specifies portions of the web site to exclude from being crawled. For example, to exclude the <code>/manual</code> directory and all Perl CGI, set this field to: <code>(^/manual) &lt;&gt; (\.pl(?:\?.*)?)\$</code>.</p> <p>Tenable PCI ASV supports POSIX regular expressions for string matching and handling, as well as Perl-compatible regular expressions (PCRE).</p>
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		
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.



Setting	Default Value	Description
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 injection test may look like <code>/target.cgi?a='&amp;b=2</code> . With HTTP Parameter Pollution (HPP) enabled, the request may look like <code>/target.cgi?a='&amp;a=1&amp;b=2</code> .
Test embedded web servers	Disabled	Embedded web servers are often static and contain no customizable CGI scripts. In addition, embedded web servers may be prone to crash or become non-responsive when scanned. Tenable recommends scanning embedded web servers separately from other web servers using this option.
Test more than one parameter	Disabled	This setting manages the combination of argument values used in the HTTP



Setting	Default Value	Description
at a time per form		<p>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 <code>/test.php?arg1=XSS&amp;b=1&amp;c=1</code>, where b and c allow other values, without testing each combination. This is the quickest method of testing with the smallest result set generated.</p> <p>This setting has four options:</p> <ul style="list-style-type: none"><li>• <b>Test random pairs of parameters:</b> This form of testing randomly checks a combination of random pairs of parameters. This is the fastest way to test multiple parameters.</li><li>• <b>Test all pairs of parameters (slow):</b> This form of testing is slightly slower but more efficient than the one value test. While testing multiple parameters, it tests an attack string, variations for a single variable and then use the first value for all other variables. For example, Tenable PCI ASV would attempt <code>/test.php?a=XSS&amp;b=1&amp;c=1&amp;d=1</code> and then cycle through the variables so that one is given the attack string, one is cycled through all</li></ul>



Setting	Default Value	Description
		<p>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 <code>/test.php?a=XSS&amp;b=3&amp;c=3&amp;d=3</code> when the first value of each variable is 1.</p> <ul style="list-style-type: none"><li>• <b>Test random combinations of three or more parameters (slower):</b> 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.</li><li>• <b>Test all combinations of parameters (slowest):</b> This method of testing checks all possible combinations of attack strings with valid input to variables. Where all pairs testing seeks to create a smaller data set as a tradeoff for speed, all combinations makes no compromise on time and uses a complete data set of tests. This testing method may take a long time to complete.</li></ul>
Do not stop	Stop after one flaw is found	This setting determines when a new flaw



Setting	Default Value	Description
after first flaw is found per web page	per web server (fastest)	<p>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.</p> <p>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.</p> <p>If you enable this option, select one of the following options:</p> <ul style="list-style-type: none"><li>• <b>Stop after one flaw is found per web server (fastest)</b> – (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.</li><li>• <b>Stop after one flaw is found per parameter (slow)</b> – 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.</li><li>• <b>Look for all flaws (slowest)</b> – Perform extensive tests regardless</li></ul>



Setting	Default Value	Description
		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	Enabled	If enabled, domain users are queried instead of local users.





information about the SMB Domain		
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 <b>Credentials &gt; Miscellaneous &gt; ADSI</b> .
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 <b>Enumerate Domain Users</b> and <b>Enumerate Local User</b> 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	<p>When disabled, provides the standard level of plugin activity in the report. The output does not include the informational plugins 56310, 64582, and 58651.</p> <p>When enabled, this setting has two options:</p> <ul style="list-style-type: none"><li>• <b>I have limited disk space. Report as little information as possible</b> – Provides less information about plugin activity in the report to minimize impact on disk space.</li><li>• <b>Report as much information as possible</b> – Provides more information about plugin activity in the report. When this option is selected, the output includes the informational plugins 56310, 64582, and 58651.</li></ul>
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 their DNS name	Disabled	Uses the host name rather than IP address for report output.
Display hosts that respond to ping	Disabled	Reports hosts that successfully respond to a ping.



Setting	Default Value	Description
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.  <b>Note:</b> 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)	<ul style="list-style-type: none"><li>Performance options:<ul style="list-style-type: none"><li>30 simultaneous hosts (max)</li><li>4 simultaneous checks per host (max)</li><li>5 second network read timeout</li></ul></li><li>Asset identification options:<ul style="list-style-type: none"><li>Create unique identifier on hosts scanned using credentials</li></ul></li></ul>
	Scan low bandwidth links	<ul style="list-style-type: none"><li>Performance options:<ul style="list-style-type: none"><li>2 simultaneous hosts (max)</li></ul></li></ul>



		<ul style="list-style-type: none"><li>◦ 2 simultaneous checks per host (max)</li><li>◦ 15 second network read timeout</li><li>◦ Slow down the scan when network congestion is detected</li><li>• Asset identification options:<ul style="list-style-type: none"><li>◦ Create unique identifier on hosts scanned using credentials</li></ul></li></ul>
	<b>Custom</b>	<a href="#">All defaults</a>
<b>PCI Quarterly External Scan</b>	<b>Default</b> (default)	<ul style="list-style-type: none"><li>• Performance options:<ul style="list-style-type: none"><li>◦ 20 simultaneous hosts (max)</li><li>◦ 4 simultaneous checks per host (max)</li><li>◦ 15 second network read timeout</li><li>◦ Slow down the scan when network congestion is detected</li></ul></li></ul>
	<b>Scan low bandwidth links</b>	<ul style="list-style-type: none"><li>• Performance options:<ul style="list-style-type: none"><li>◦ 2 simultaneous hosts (max)</li><li>◦ 2 simultaneous checks per host (max)</li><li>◦ 15 second network read timeout</li><li>◦ Slow down the scan when network congestion is detected</li></ul></li><li>• Asset identification options:<ul style="list-style-type: none"><li>◦ Create unique identifier on hosts scanned using credentials</li></ul></li></ul>



	<b>Custom</b>	<ul style="list-style-type: none"><li>• <a href="#">Performance Options</a> (default options)</li><li>• <a href="#">Unix Find Command Exclusions</a> (default options)</li><li>• <a href="#">Windows File Search Options</a></li></ul>
--	---------------	--

## 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.



Setting	Default Value	Description
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.
Automatically accept detected SSH disclaimer prompts	Disabled	<p>When enabled, if a credentialed scan tries to connect via SSH to a host that presents a disclaimer prompt, the scanner provides the necessary text input to accept the disclaimer prompt and continue the scan.</p> <p>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.</p>
Scan targets with multiple domain names in parallel	Disabled	<p>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.</p> <p>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.</p>
Create unique identifier on	Enabled	When enabled, the scanner creates a unique identifier for credentialed scans.



Setting	Default Value	Description
hosts scanned using credentials		
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	<p>Specifies the maximum number of hosts that Tenable PCI ASV submits for scanning at the same time in an <a href="#">individual scan task</a>.</p> <p>To further refine scan performance using host limits, Tenable recommends adjusting <b>Advanced</b> settings for your individual scanners (for example, <b>max_hosts</b>, <b>global.max_hosts</b>, and <b>global.max_scans</b>). For more information, see <a href="#">Advanced Settings</a> in the <i>Tenable Nessus User Guide</i>.</p> <p>If you set <b>Max simultaneous hosts per scan</b> to more than scanner's <a href="#">max_hosts</a> setting, Tenable PCI ASV caps <b>Max simultaneous hosts per scan</b> at the <b>max_hosts</b> value. For example, if you set the <b>Max simultaneous hosts per scan</b> to 150 and scanner's <b>max_hosts</b> is set to 100, with more than 100 targets, Tenable PCI ASV scans 100 hosts simultaneously.</p> <div><b>Note:</b> You can only adjust individual scanner settings for your organization's managed scanners. You cannot modify the settings of Tenable-hosted scanners.</div>
Max number of concurrent TCP sessions per host	None	<p>Specifies the maximum number of established TCP sessions for a single host.</p> <p>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.</p>
Max number of concurrent TCP	None	Specifies the maximum number of established TCP sessions for each <a href="#">scan task</a> , regardless of the number of





Setting	Default Value	Description
sessions per scan		<p>hosts being scanned.</p> <div><b>Note:</b> The MAX NUMBER OF CONCURRENT TCP SESSIONS PER SCAN setting is not enforceable in a Discovery scan. The <code>global.max_simult_tcp_sessions</code> Nessus Engine setting (that you set on each scanner) is an absolute cap that applies across all running scans on a scanner. (For example, if you have four scanners and do not want them to generate more than 10000 simultaneous TCP sessions in total at any point in time, you can set that global setting to 2500 for each individual scanner.)</div> <p>For scanners installed on any Windows host, you must set this value to 19 or less to get accurate results.</p>
Unix Find Command Options		
Exclude Filepath	None	<p>A plain text file containing a list of filepaths to exclude from all plugins that search using the <code>find</code> command on Unix systems.</p> <p>In the file, enter one filepath per line, formatted per patterns allowed by the Unix <code>find</code> command <code>-path</code> argument. For more information, see the <code>find</code> command <a href="#">man page</a>.</p>
Exclude Filesystem	None	<p>A plain text file containing a list of filesystems to exclude from all plugins that search using the <code>find</code> command on Unix systems.</p> <p>In the file, enter one filesystem per line, using filesystem types supported by the Unix <code>find</code> command <code>-fstype</code> argument. For more information, see the <code>find</code> command <a href="#">man page</a>.</p>
Include Filepath	None	<p>A plain text file containing a list of filepaths to include from all plugins that search using the <code>find</code> command on</p>



Setting	Default Value	Description
		<p>Unix systems.</p> <p>In the file, enter one filepath per line, formatted per patterns allowed by the Unix <code>find</code> command <code>-path</code> argument. For more information, see the <code>find</code> command <a href="#">man page</a>.</p> <p>Including filepaths increases the locations that are searched by plugins, which extends the duration of the scan. Make your inclusions as specific as possible.</p> <div><b>Tip:</b> Avoid having the same filepaths in <b>Include Filepath</b> and <b>Exclude Filepath</b>. This conflict may result in the filepath being excluded from the search, though results may vary by operating system.</div>
Windows File Search Options		
Windows Exclude Filepath	None	<p>A plain text file containing a list of filepaths to exclude from any search on Windows systems.</p> <p>In the file, enter one filepath per line. This setting overrides and removes default exclusions.</p>
Windows Include Filepath	None	<p>A plain text file containing a list of filepaths to include in any use of Recursive search on Windows systems.</p> <p>In the file, enter one filepath per line. This setting replaces any defaults entirely.</p>
Debug Settings		
Enable plugin debugging	Disabled	Attaches available debug logs from plugins to the vulnerability output of this scan.
Audit Trail Verbosity	Default	<p>Controls verbosity of the plugin audit trail.</p> <p>Options include:</p>



Setting	Default Value	Description
		<ul style="list-style-type: none"><li>• <b>No audit trail</b> – (Default) Tenable PCI ASV does not generate a plugin audit trail.</li><li>• <b>All audit trail data</b> – The audit trail includes the reason why plugins were not included in the scan.</li><li>• <b>Only scan errors</b> – The audit trail includes only errors encountered during the scan.</li></ul>

## 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 <a href="#">folder</a> 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 <b>Scanner</b> field lists local or cloud-managed scanners to choose from.	Yes
Scanner	varies	Specifies the scanner that performs the scan.	Yes
Target	none	<p>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.</p> <p>The <b>Import from file</b> 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.</p>	Yes



Setting	Default Value	Description	Required
		<p>After you add targets, you can search and delete targets from the list. You cannot modify targets inline.</p> <div><b>Tip:</b> 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.</div> <p>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.</p> <div><b>Note:</b> If the URL you type in the <b>Target</b> 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.</div> <div><b>Note:</b> If you create a user-defined scan template, the target setting is not saved to the template. Type a target each time you create a new scan.</div>	

## 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



Setting	Default	Description
		<p>default, scans are not scheduled.</p> <p>When the <b>Schedule</b> toggle is disabled, the other schedule settings remain hidden.</p> <p>Click the toggle to enable the schedule and view the remaining <b>Schedule</b> settings.</p>
Frequency	Once	<p>Specifies how often the scan is launched.</p> <div><p><b>Note:</b> 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.</p></div> <ul style="list-style-type: none"><li>• <b>Once:</b> Schedule the scan at a specific time.</li><li>• <b>Daily:</b> Schedule the scan to occur on a daily basis, at a specific time, up to 20 days.</li><li>• <b>Weekly:</b> Schedule the scan to occur on a recurring basis, by time and day of week, up to 20 weeks.</li><li>• <b>Monthly:</b> Schedule the scan to occur every 1-20 months, by:<ul style="list-style-type: none"><li>• <b>Day of Month:</b> The scan repeats on a specific day of the month at the selected time.</li><li>• <b>Week of Month:</b> 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.</li></ul></li></ul> <div><p><b>Note:</b> If you schedule your scan to recur monthly and by</p></div>



Setting	Default	Description
		<div>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.</div> <ul style="list-style-type: none"><li>• <b>Yearly:</b> Schedule the scan to occur every year, by time and day, up to 20 years.</li></ul>
Starts	varies	<p>Specifies the exact date and time at which a scan launches.</p> <div><b>Note:</b> 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.</div> <p>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.</p>
Timezone	varies	The time zone of the value set for <b>Starts</b> .
Repeat	Daily	The frequency of the value set for <b>Schedule</b> .

## 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 <a href="#">view the results</a> of the scan.
Can Control	In addition to the tasks allowed by <b>Can View</b> , users with this permission can <a href="#">launch</a> and <a href="#">stop</a> a scan. They cannot view or edit the scan configuration or <a href="#">delete</a> the scan.
Can Configure	In addition to the tasks allowed by <b>Can Control</b> , users with this permission can view the scan configuration and <a href="#">modify any setting</a> for the scan except scan ownership. They can also <a href="#">delete</a> 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 <b>Dashboard</b> and <b>Findings</b> pages. When set to <b>Keep private</b> , the scan results <b>Last Seen</b> dates do not update and you must access the scan directly to view the results.

## Scope Settings in Tenable Web App Scanning Scans

Configure **Scope** settings to specify the URLs and file types that you want to include in or exclude from your scan.

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 <code>.side</code> 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 <a href="#">Basic</a> settings.  Type each URL as an absolute URL.  Type each URL on a separate line. <div><b>Note:</b> All URLs should have the same domain and wildcards are not allowed.</div>

## Scan Exclusion



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

Setting	Default Value	Description
Exclude Binaries	selected	<p>Check box option that allows you to specify whether you want the scanner to audit URLs with responses in binary format.</p> <p>Select this option to increase the surface coverage of your web application scan.</p> <div><b>Note:</b> Scans that include binaries can take longer to complete, because the scanner cannot read the binary responses.</div>

## 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	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



Setting	Default Value	Description	Required
Balancers Usage			

## 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 <code>id="logout"</code> , type <code>id</code> for the key and <code>logout</code> 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.  <b>Note:</b> 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.  <b>Note:</b> 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	<p>Specifies the name of the user-agent header you want the scanner to use when sending an HTTP request.</p> <p>You can configure this option only after you select the <b>Use a different User Agent to identify scanner</b> check box.</p> <p>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 <i>Google Chrome Documentation</i>.</p> <div><b>Note:</b> 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</div> <div><b>Note:</b> Not all requests from scanner are guaranteed to have the User Agent sent.</div>
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	none	Specifies the custom headers you want to inject into each



Headers		<p>HTTP request, in request and response format.</p> <p>You can add additional custom headers by clicking the  button and typing the values for each additional header.</p> <div><b>Note:</b> If you enter a custom User-Agent header, that value overrides the value entered in the <b>User Agent</b> setting box.</div>
---------	--	--

## 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 Depth	10	<p>Specifies the maximum number of sub-directories the scanner crawls.</p> <p>For example, if your target is <code>www.example.com</code>,</p>



		and you want the scanner to crawl <code>www.example.com/users/myname</code> , 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	5000	Specifies the time, in milliseconds, the scanner waits for all commands to render new content to finish processing.



Delay

## 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	<p>Specifies the time, in seconds, the scanner waits for a response from a host before aborting the scan, unless otherwise specified in a plugin.</p> <p>If your internet connection is slow, Tenable recommends that you specify a longer wait time.</p>
Browser Timeout (In Seconds)	30	<p>Specifies the time, in seconds, the scanner waits for a response from a browser before aborting the scan, unless otherwise specified in a plugin.</p> <p>If your internet connection is slow, Tenable recommends that you specify a longer wait time.</p>
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	
<b>Tip:</b> The typical Tenable PCI ASV scan status flow is as follows: <b>Initializing, Running, Publishing Results, Completed</b> .	
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, <a href="#">view</a> the scan warnings.
Canceled	At user request, Tenable PCI ASV successfully <a href="#">stopped</a> 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).



Status	Description
Imported	A user <a href="#">imported</a> the scan. You cannot run imported scans. Scan history is unavailable for imported scans.
Pausing	A user <a href="#">paused</a> 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 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	<p>Tenable PCI ASV has the scan queued to launch and is assigning scan tasks to the assigned sensors.</p> <div><b>Note:</b> Tenable PCI ASV aborts scans that remain in <b>Pending</b> 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.</div>
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 <b>Publishing Results</b> status begins once the <b>Running</b> status reaches 100%.
Resuming	Tenable PCI ASV is in the process of restarting tasks after the user <a href="#">resumed</a> 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 <a href="#">stopped</a> the scan, and Tenable PCI ASV is processing the action.



Status	Description
Tenable Web App Scanning Scans	
Aborted	<p>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.</p> <p>For more information about why Tenable Web App Scanning aborted a scan, <a href="#">view the scan notes</a>.</p>
Canceled	<p>At the user's request, Tenable Web App Scanning successfully <a href="#">stopped</a> the latest scan job.</p>
Completed	<p>The scanner completed the scan's latest scan job.</p>
Never Run	<p>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).</p>
Pending	<p>Tenable Web App Scanning has the scan queued to launch.</p> <div><p><b>Note:</b> Tenable Web App Scanning aborts scans that remain in <b>Pending</b> 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.</p></div>
Processing	<p>The scan has completed but the results are still being processed. The scanner is processing vulnerability findings, attachments, notes, and other metadata.</p>
Running	<p>The scanner is currently running the scan.</p>
Stopping	<p>The scanner acknowledged the <a href="#">stop</a> request and is in the process of stopping.</p>



## 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. Do one of the following:

- To submit a Tenable Vulnerability Management scan for validation, below **Scans**, click **Vulnerability Management Scans**.

- a. 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.

- b. 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.

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

The **Scan Details** page appears.

The screenshot shows the Tenable Scans interface. The main table displays a list of scans with columns for Start Time, End Time, Duration, Status, and Actions. The first scan is highlighted as 'Current'. The right-hand panel shows the 'Scan Details' for the selected scan, including a summary of vulnerabilities (8 Critical, 20 High, 120 Medium, 41 Low), scan status (Completed), start time, template, scanner, and targets.

	START TIME	END TIME	DURATION	STATUS	ACTIONS
<input type="checkbox"/>	02/12/2025 at 12:30 PM	02/11/2025 at 1:25 PM	7min	Running	
<input type="checkbox"/>	02/11/2025 at 12:30 PM	02/10/2025 at 1:06 PM	55min	Completed	
<input type="checkbox"/>	02/09/2025 at 12:30 PM	02/09/2025 at 1:11 PM	41min	Completed	
<input type="checkbox"/>	02/08/2025 at 12:30 PM	02/08/2025 at 1:12 PM	42min	Completed	
<input type="checkbox"/>	02/07/2025 at 12:30 PM	02/07/2025 at 1:52 PM	1hr 22min	Completed	
<input type="checkbox"/>	02/06/2025 at 12:30 PM	02/06/2025 at 1:32 PM	1hr 2min	Completed	
<input type="checkbox"/>	02/05/2025 at 12:30 PM	02/05/2025 at 1:13 PM	43min	Completed	
<input type="checkbox"/>	02/04/2025 at 12:30 PM	02/04/2025 at 1:37 PM	1hr 6min	Completed	
<input type="checkbox"/>	02/03/2025 at 12:30 PM	02/03/2025 at 3:24 PM	2hr 54min	Completed	
<input type="checkbox"/>	02/02/2025 at 12:30 PM	02/02/2025 at 1:10 PM	40min	Completed	

**Scan Details**

**Summary:** 8 CRITICAL VULNERABILITIES, 20 HIGH VULNERABILITIES, 120 MEDIUM VULNERABILITIES, 41 LOW VULNERABILITIES

**Status:** Completed

**START TIME:** 02/11/2025 at 12:30 PM

**TEMPLATE:** PCI Quarterly External Scan

**SCANNER:** US Cloud Scanner

**TARGETS:** target1.pubtarg.tenabledemo.com target2.pubtarg

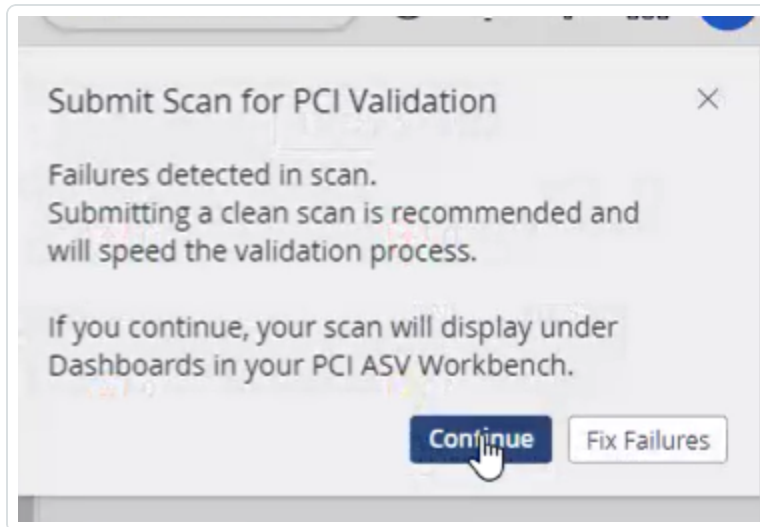
**SCANNER GROUPS:** US Cloud Scanner



- d. 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.



- e. Click **Continue**.

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

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

- To submit a Tenable Web App Scanning scan for validation, below **Scans**, click **Web Application Scans**.
  - a. 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.
  - b. 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.
  - c. In the scan details plane, click the **See All Details** button.

The **Scan Details** page appears.

The screenshot shows the 'PCI ASV test scan' page with a table of scan results. The table has columns for TARGET, VULNERABILITIES, LAUNCHED, STATUS, and ACTIONS. Three targets are listed: https://nunaya.business, https://brokencrystals.com, and https://altoromutual.com. All three are marked as 'Completed'.

TARGET	VULNERABILITIES	LAUNCHED	STATUS	ACTIONS
<input type="checkbox"/> https://nunaya.business	<div><div></div></div>	12/13/2024	Completed	<a href="#">⋮</a>
<input type="checkbox"/> https://brokencrystals.com	<div><div></div></div>	12/13/2024	Completed	<a href="#">⋮</a>
<input type="checkbox"/> https://altoromutual.com	<div><div></div></div>	12/13/2024	Completed	<a href="#">⋮</a>

d. For each target that you want to submit for validation:

i. In the **Scans** table, click the target you want to submit for validation.

The target results page appears.

The screenshot shows the target results page for https://nunaya.business. It displays a table of vulnerabilities with columns for SEVERITY, NAME, FAMILY, and INSTANCES. There are 25 results. On the right, there is a summary of vulnerabilities by severity: 0 Critical, 0 High, 2 Medium, and 4 Low. Below this is a 'Scan Details' section with information about the scan, status, create time, start time, end time, scan template, scanner, and description. At the bottom right, there is a 'Targets' section.

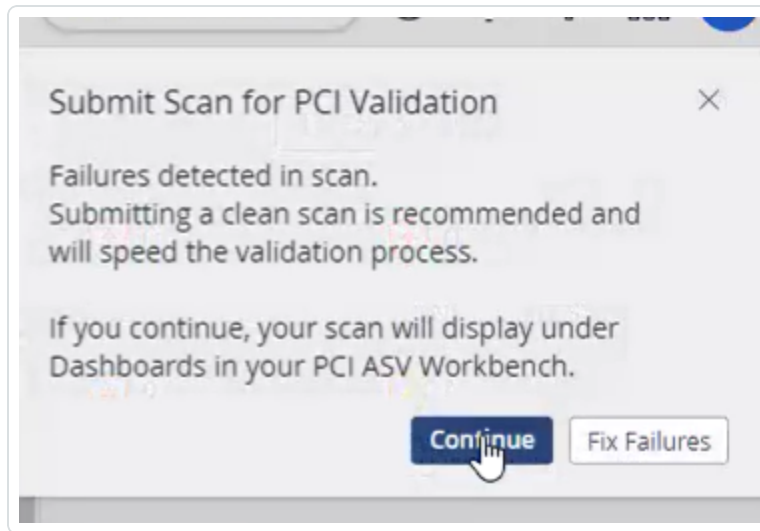
SEVERITY	NAME	FAMILY	INSTANCES
Medium	HTTP to HTTPS Redirect Not Enabled	SSL/TLS	1
Medium	Missing HTTP Strict Transport Security Policy	HTTP Security Header	1
Low	HTTP Header Information Disclosure	HTTP Security Header	1
Low	SSL/TLS Weak Cipher Suites Supported	SSL/TLS	1
Low	Cookie Without HttpOnly Flag Detected	HTTP Security Header	1
Low	Cookie Without SameSite Flag Detected	HTTP Security Header	1
Info	Target Information	General	1
Info	Screenshot	General	1
Info	External URLs	General	1

ii. 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.





iii. Click **Continue**.

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

The scan target(s) appears in the **New Scan Results** tab in your **PCI ASV** workbench.

**Note:** When you view the submission on your PCI ASV workbench, each URL scanned displays the associated scan name.

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](#).



## pub 3 Daily Scan

General Information

Assets

Undisputed Failures

Disputes

Name

pub 3 Daily Scan

Owner

pci-testing1@tenable.com

Date Scan Completed

October 23 at 7:30 AM

Scan Expiration Date

January 21 at 6:30 AM

ASV Assessor

Unassigned

ASV Message

None

Email Notification

☐ Self ☐ Others

Submit to ASV Review

Save

Cancel

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.

**Email Notification**

☒ Self ☒ Others

**Email Recipient(s)**

Example: me@example.com, you@example.com

List Of Emails

☒ Attestation Levels For Email Notification

- ☒ Assigned
- ☒ In Review
- ☒ Passed
- ☒ Failed
- ☒ Return to Customer

☒ Dispute Levels For Email Notification

- ☒ Reopen
- ☐ Passed (Warning: Generates email per dispute.)
- ☐ Failed (Warning: Generates email per dispute.)
- ☒ Request Information
- ☒ Send a Message
- ☒ Send Reminder (Info Requested Disputes)

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.



PCI ASV								Create Scan
New Scan Results In Remediation In ASV Review Attestations								
97 Attestations								1 to 50 of 97 Page 1 of 2
	NAME	OWNER	ASSETS	FAILURES	STATUS	ASV MESSAGE	LAST MODIFIED	ACTIONS
<input type="checkbox"/>	PCI Pub Target Scan Creat...	vmd-us2b-pciasv@tenabl...	3 (0)	136 (136)	In-Progress	None	May 16 at 10:43 AM	
<input type="checkbox"/>	PCI-1700	vmd-us2b-pciasv@tenabl...	3 (0)	136 (136)	In-Progress	None	March 27 at 5:38 AM	
<input type="checkbox"/>	New Attestation Test	vmd-us2b-pciasv@tenabl...	1 (0)	103 (103)	In-Progress	None	March 6 at 6:36 AM	
<input type="checkbox"/>	New Attestation	vmd-us2b-pciasv@tenabl...	1 (0)	42 (42)	In-Progress	None	September 12 at 10:19 AM	

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

The **Attestation Details** page appears.

- Click the **Assets** tab.

A table of assets associated with the attestation appears.

- 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.

- 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.

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

- 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.



## New Attestation

General Information Assets **Undisputed Failures** Disputes

Filters Search 45 Undisputed Failures

45 Failures									1 to 45 of 45	Page 1 of 1
SEVERITY	ASSET NAME	IP ADDRESS	PORT	PROTOCOL	PLUGIN ID	PLUGIN NAME	SCAN DATE	ACTIONS		
<input type="checkbox"/> High	altoromutual.com	65.61.137.117	8080	tcp	119811	Script Src Integrity Check	September 8 at 4:42 PM			
<input type="checkbox"/> High	altoromutual.com	65.61.137.117	443	tcp	139414	TLS Version 1.1 Protocol Detection (PCI DSS)	September 8 at 4:42 PM			
<input type="checkbox"/> High	altoromutual.com	65.61.137.117	443	tcp	84470	TLS Version 1.0 Protocol Detection (PCI DSS)	September 8 at 4:42 PM			
<input type="checkbox"/> High	altoromutual.com	65.61.137.117	8080	tcp	42424	CGI Generic SQL Injection (blind)	September 8 at 4:42 PM			
<input type="checkbox"/> High	altoromutual.com	65.61.137.117	443	tcp	119811	Script Src Integrity Check	September 8 at 4:42 PM			

### 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.

Clone disputes for PCI Scan 5.7.23							Create Dispute
The following attestations have at least one asset that matches the attestation from which you want to clone disputes. Click on an attestation to review corresponding disputes, then select the appropriate attestation to clone disputes from. Please refer our KB article with steps.							
40 Attestations							1 to 40 of 40
NAME	OWNER	ASSETS	FAILURES	TOTAL DISPUTES	STATUS	LAST MODIFIED	
Final ASV Comment Test	manual_pci_asv@tenab...	4 (0)	64 (59)	5 (0)	Failed	July 19 at 5:11 PM	
Checking Cloned Dispute PCI-1606	manual_pci_asv@tenab...	1 (0)	18 (0)	18 (0)	Failed	April 3 at 5:13 PM	
VM + WAS Scan 18.5.22	manual_pci_asv@tenab...	4 (0)	70 (51)	19 (0)	Failed	May 18 at 11:20 AM	
Verify Clone Dispute 11.5	manual_pci_asv@tenab...	1 (0)	18 (0)	18 (0)	Passed	May 11 at 2:58 PM	
17. Pass	manual_pci_asv@tenab...	2 (0)	3 (0)	3 (0)	Passed	January 17 at 5:41 PM	

To clone a dispute:

- 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.

### New Dispute

NAME

OWNER

REASON

EXPLANATION

SEVERITY  
High

PLUGIN NAME  
Script Src Integrity Check

PLUGIN ID  
119811

Evidence

Failures

You can upload an evidence using one of the following extensions: Nessus (.nessus), Nessus DB (.db), pdf, csv, json, txt, bmp, gif, jpeg, jpg, png

Add File

Upload evidence

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	<p>A CSV text file that contains a list of tag categories or values.</p> <div><b>Note:</b> 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 <a href="#">knowledge base article</a>.</div>
JSON	<p>A JSON file that contains a nested list of tag categories or values.</p> <p>Tenable PCI ASV does not include empty fields in the JSON file.</p>

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.



## PCI Pub Target Scan Created By Hemant Barot

General Information

Assets

Undisputed Failures

Disputes

Name

PCI Pub Target Scan Created By Hemant Barot

Owner

vmd-us2b-pciasv@tenable.com

Date Scan Completed

March 27 at 5:36 AM

Scan Expiration Date

June 25 at 5:36 AM

ASV Assessor

Unassigned

ASV Message

None

Submit to ASV Review

Save

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
<b>Unassigned</b>	Attestation is new and not yet assigned to an ASV reviewer.
<b>Assigned</b>	Attestation is assigned to an ASV reviewer.
<b>Info Requested</b>	The ASV reviewer has requested for additional information for the disputes.
<b>Info Provided</b>	<div>A response is provided for the requested information. <b>Note:</b> An attestation may show a status of <b>Info Provided</b> even if there are still disputes that require additional information. In this case, the number of disputes that require additional information appears in parentheses beside the attestation status.</div>
<b>In-Review</b>	<div>The ASV reviewer is reviewing the attestation.</div> <div>After review, all attestations move to the <b>Attestations</b> tab with a status of <b>Passed</b>, <b>Failed</b>, or <b>Closed</b>.</div>



## 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

---

In Tenable PCI ASV, you can navigate directly to Tenable Vulnerability Management to manage your system settings.

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, where you can configure your system settings.

For more information, see [Settings](#) in the *Tenable Vulnerability Management User Guide*.