



Tenable Web App Scanning User Guide

Last Revised: May 24, 2023



Table of Contents

Welcome to Tenable Web App Scanning	6
Get Started with Tenable Web App Scanning	8
Tenable Web App Scanning Requirements	21
Navigate Tenable Web App Scanning	22
Log In to Tenable Web App Scanning	23
Log Out of Tenable Web App Scanning	24
Deploy Tenable Web App Scanning as a Docker Image	25
Remove Tenable Web App Scanning as a Docker Container	27
Dashboards	28
Tenable Web App Scanning Dashboard	29
Assets	30
Discovered Domains Assets	32
Scanned Application Assets	35
View Asset Details	38
Scanned Application Asset Details	39
Explore Asset Filters	44
Remove and Prevent Duplicate Assets	50
Export Assets	51
Delete Assets	56
Tenable Web App Scanning Vulnerabilities Findings	60
Web Application Vulnerability Findings Details	63
Group Your Findings	69
View Findings Details	72



Findings Filters	73
Export Findings	77
Create Recast/Accept Rules in Findings	81
Saved Filters	84
Create a Saved Filter	85
Apply a Saved Filter	86
Edit a Saved Filter	87
Share a Saved Filter	89
Delete a Saved Filter	90
Create a Saved Filter	91
Apply a Saved Filter	92
Edit a Saved Filter	93
Share a Saved Filter	95
Delete a Saved Filter	96
Explore Tables	96
Filter an Explore Table	97
Filter By Value	103
Filter Out Value	104
Copy to Clipboard	105
Customize an Explore Table	106
Manage Tenable Web App Scanning Scans	108
Create and Launch a Scan	110
Edit Tenable Web App Scanning Scan Settings	113
Set Tenable Web App Scanning Scan Permissions	115



Launch a Tenable Web App Scanning API Scan	118
Tenable Web App Scanning Scan Filters	120
View Tenable Web App Scanning Scan Details	121
Scan Notes Severity Details in Tenable Web App Scanning	126
View Tenable Web App Scanning Scan Progress	128
Export Scan Results	129
Basic Settings in Tenable Web App Scanning Scans	132
Scope Settings in Tenable Web App Scanning Scans	137
Assessment Settings in Tenable Web App Scanning Scans	141
Report Settings in Tenable Web App Scanning Scans	146
Advanced Settings in Tenable Web App Scanning Scans	147
Credentials in Tenable Web App Scanning Scans	153
Configure Credentials Settings in a Tenable Web App Scanning Scan	155
Configure Selenium Credentials Settings Automatically	157
Tenable Web App Scanning Selenium Commands	159
HTTP Server Authentication Settings in Tenable Web App Scanning Scans	163
Web Application Authentication	164
Client Certificate Authentication	168
Plugin Settings in Tenable Web App Scanning Scans	169
Tenable-Provided Tenable Web App Scanning Templates	172
User-Defined Templates	175
Scan Settings	180
Tenable Web App Scanning Scan Settings	182
Tenable Web App Scanning Settings	184



View your License Information	186
Tenable Web App Scanning Licenses	189



Welcome to Tenable Web App Scanning

This guide includes new and updated features to the Tenable Vulnerability Management platform that are available to customers participating in the early access program. For more information about these updates—which this document collectively refers to as *Tenable Vulnerability Management Key Enhancements*—see [Tenable Vulnerability Management Key Enhancements](#).

Tenable Vulnerability Management® allows security and audit teams to share multiple Tenable Nessus, Tenable Nessus Agents, and Tenable Nessus Network Monitors, scan schedules, scan policies, and scan results among an unlimited set of users or groups.

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

Tenable One Exposure Management Platform

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

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

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

Tip: For additional information on getting started with Tenable One products, check out the [Tenable One Deployment Guide](#).

Tenable Web App Scanning

[Get Started with Tenable Web App Scanning](#)



Tenable Web App Scanning offers significant improvements over the existing **Web Application Tests** policy template provided by the Tenable Nessus scanner, which is incompatible with modern web applications that rely on Javascript and are built on HTML5. This leaves you with an incomplete understanding of your web application security posture.

Tenable Web App Scanning provides comprehensive vulnerability scanning for modern web applications. Tenable Web App Scanning's accurate vulnerability coverage minimizes false positives and false negatives, ensuring that security teams understand the true security risks in their web applications. The product offers safe external scanning that ensures production web applications are not disrupted or delayed, including those built using HTML5 and AJAX frameworks.

Tenable Vulnerability Management API

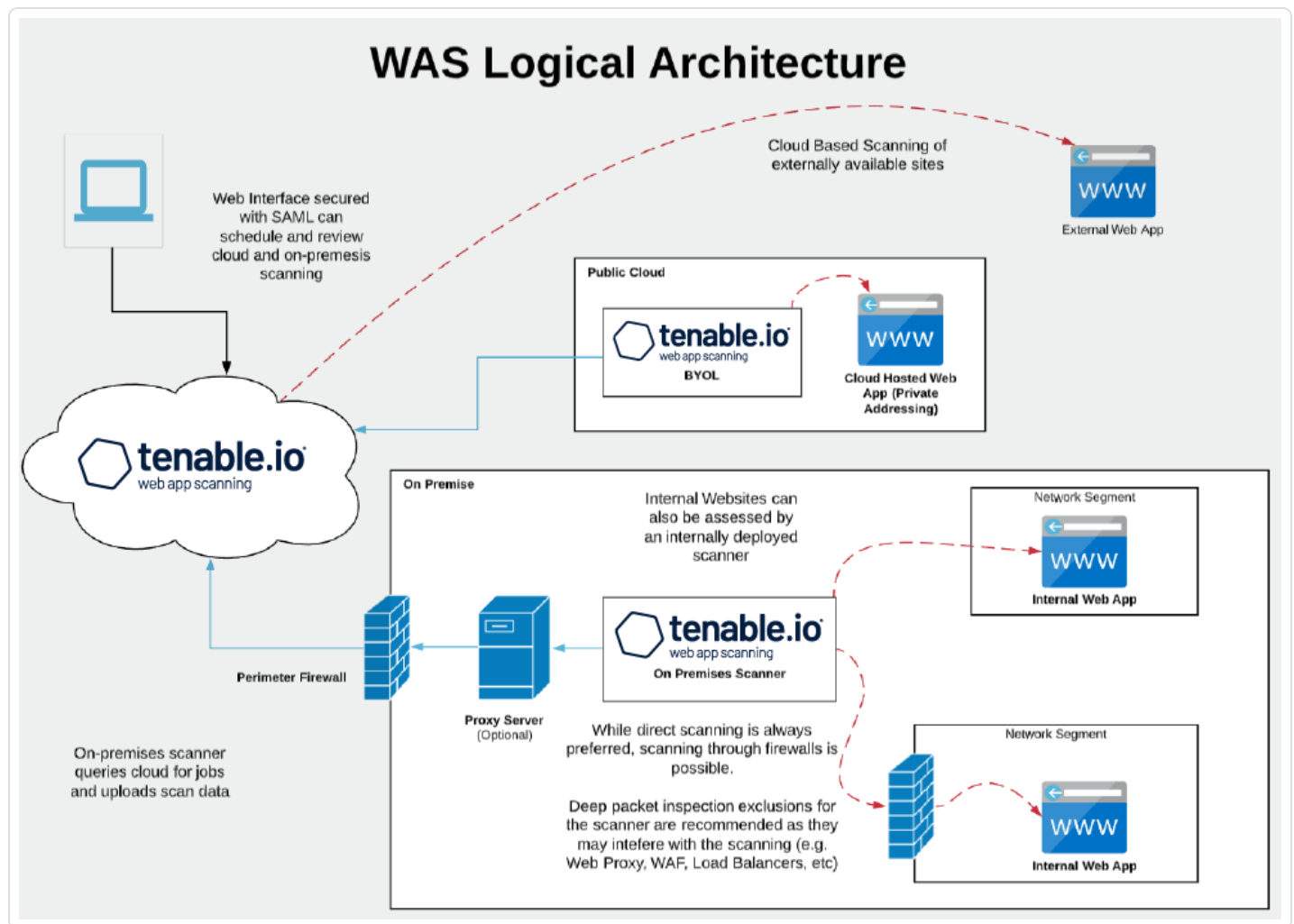
[See the API](#)

The Tenable Vulnerability Management API can be leveraged to develop your own applications using various features of the Tenable Vulnerability Management platform, including scanning, creating policies, and user management.

Get Started with Tenable Web App Scanning

There are significant differences between scanning for vulnerabilities in web applications and scanning for traditional vulnerabilities with Tenable Nessus, Tenable Nessus Agents or Tenable Nessus Network Monitor. As a result, Tenable Web App Scanning (Tenable Web App Scanning) requires a different approach to vulnerability assessment and management.

Tenable Web App Scanning Application Topology



Tenable Web App Scanning offers significant improvements over the legacy Tenable Nessus-based web application scanning policy:



- The legacy scanning template for Tenable Nessus is incompatible with modern web application frameworks such as Javascript, HTML 5, AJAX, or single page applications (SPA), among others, which can potentially leave you with an incomplete understanding of your web application security posture.
- Tenable Web App Scanning provides comprehensive vulnerability scanning for modern web applications. Its accurate vulnerability coverage minimizes false positives and false negatives to ensure that security teams understand the true security risks in their web applications. It offers safe external scanning so that production web applications do not experience disruptions or delays.
- Tenable Web App Scanning uses region-specific cloud scanners. There is no need for more scanners if your web application analysis scope includes only publicly available assets. If your web applications are not public, your installation plan depends on where your web applications run and your organization's data storage needs.

Use the following sequence to configure and manage your Tenable Web App Scanning deployment:

1. [Prepare](#)
2. [Install](#)
3. [Configure Scans](#)
4. [Configure Additional Settings](#)

Prepare

Before you begin, familiarize yourself with Tenable Web App Scanning basics to establish a deployment plan and an analysis workflow for your implementation and configurations:

Types of Tenable Web App Scanning Programs

There are several viable ways to operate a web application scanning program based on dynamic application security testing (DAST) technology. Most programs use some combination of each approach to meet different needs for each site. The following list gives Tenable supported scan templates:



- **Scan:** The complete set of available checks which includes all other pre-built templates, except for the API scan.
- **Overview:** A simplified version of the “Scan” template without several active tests to lower its impact and speed up the scan.
- **PCI:** A special template used as part of the attestation offering that Tenable provides for the payment card industry (PCI) security standard. Only submissions to attestation consume PCI licenses; otherwise, this template is a simplified version of the "Scan" template.
- **SSL/TLS:** A health check scan focused on the current state of the web server encryption settings and certificate state (for example, the remaining time on the certificate).
- **Config Audit:** A compliance audit that detects externally viewable web server settings that external audit providers commonly review to evaluate the health of a security program.
- **API Scan:** A special template requiring more configuration to describe the application programming interface (API), so that the scanner can successfully detect relevant vulnerabilities. This includes some similar tests in the “Scan” template but adds others unique to API endpoints.

Quick Surface-level Checks

You typically use the “SSL_TLS” or “Config Audit” scan templates to run a rapid test – often lasting only minutes – on a more regular basis than in-depth scans to give you an overview of surface-level checks such as any certificate-type and encryption-type issues with a given site or commonly exposed configuration parameters that are not best practice.

- **Untuned Detailed Scans:** Without requiring tuning or refinement, this approach uses the “Scan” template to optimize detection of most vulnerabilities, and simulates drive-by style attacks that sites commonly experience. These scans deploy quickly and return valuable incremental visibility from the scan target while using basic validation to avoid obvious scan errors. However, this approach may run into timeouts (such as the eight-hour default in Tenable Vulnerability Management), or miss more complex sections of a site that requires authentication or fine-tuning for correct scans. These drawbacks are common with sites that have forums, blogs, large product volume, multiple languages, or a high number of pages.
- **Authenticated Detailed Scans:** While similar to the Untuned Detailed scan, this approach uses authentication. You can do this in the scan configuration page or in the Chrome extension



from Tenable. In addition to the benefits of an untuned scan, authenticated scans log on as a user to test for potential issues. Tenable recommends that you never log on as an admin user, especially in production (see the "Key Considerations" section). Authentication requires you to create and maintain the test user account and to update any unique site configurations.

- **Tuned Detailed Scans:** In addition to authentication, you can use other methods to optimize scans for speed or complexity (see "Key Considerations"). These refinements involve an initial time investment before deployment and may require semi-regular adjustments depending on the frequency of the site updates.

Pre-production Scanning

To limit scanner impact on a production site and maintain 100 percent uptime, you can consider integrating scans using the Tenable Vulnerability Management API to trigger a scan based on a weekly or monthly build, or a pre-production location on a regular schedule. This protects the more exposed production site which may differ from internal builds. This scanning approach works to varying degrees with most mature organizations and often depends on-site criticality and resource availability.

API Scanning

Organizations are increasingly adopting APIs to power web applications, B2B transactions, mobile applications, and automation scenarios. You can assess these potential exposures by using the API scanning template within Tenable Web App Scanning to provide critical visibility into more cyber risks. In general, high risk and exposure are drivers for mature programs or organizations to scan APIs more frequently. Ultimately, as the security program develops, many organizations proactively identify all vulnerable locations to ensure full coverage. This type of scan can require more input from development staff and rely on an OpenAPI file to provide the endpoint definitions for the scanner to communicate to the API itself.

Decide Which Tenable Web App Scanning Program to Use

Most programs start with a few scans based on the "SSL_TLS" or "Config Audit" templates to familiarize vulnerability managers with how to establish scans and review results. Then, they progress into running an untuned scan using the Tenable Web App Scanning scan template.

Timeouts are common when you first build out your program. The default scan completion timeout in Tenable Vulnerability Management is eight hours, and extending this may not "complete" the scan; this may only be achievable via tuning for greater speed.



It is viable to run a program based on untuned scans while accepting the timeout. As many web application vulnerabilities span multiple pages containing the same vulnerability, it is likely that a scan automatically detects a significant proportion of vulnerabilities within the first several hours. Tenable's own monitoring can confirm this. Tuned scans typically improve scan efficiency and accuracy by only a small degree and cost more time to refine the scan configuration.

Most mature organizations tune scans on their most critical sites, which involve 10-20 minutes of effort per site and improves with operator experience. An organization's level of knowledge and resource availability can determine the percentage of sites that undergo detailed tuning. It is rare to see all sites tuned, especially in organizations with many websites. This is due partly to the dynamic nature of websites; they often expand or change significantly every few years, and this requires a review of scan settings to adapt to the development pace of the test site.

- **Focus on the process first:** Start with the Tenable Web App Scanning “Scan” (a complete set of checks) or an “Overview” scan (fewer checks but lower impact) templates. Familiarize yourself with the scanner output and work with your teams to incorporate the findings into your workflows. Develop your mitigation and resolution programs.
- **Dig deeper into critical areas:** Once you have established some of the baseline procedures and identified the right owners within your organization for the output from the scanner, start investing time in more advanced-tuned scans to gain better visibility into your most important sites.
- **Take action:** The scans return a significant amount of data to drive organizational action. Consider the potential consumers of the data. Developers want details to identify necessary fixes and improve over time. Management must know which sites contribute the greatest risk to the business, and thereby allocate resources. Security leadership needs general category information such as the OWASP vulnerability categories for all sites to focus on a specific classification of vulnerabilities.

Note: Tenable Professional Services offers a highly recommended [quick-start program](#) for new users of Tenable Web App Scanning scanning to help establish the mechanics of developing a new program. Also, the ProServe team runs a [workshop](#) to establish the internal processes and initial goals of developing a broader vulnerability management program. These services help organizations get a solid foundation and understanding of effective cybersecurity programs and familiarization with the product. Contact your Tenable sales representative at sales@tenable.com.

Key Considerations to Optimize Your Scan Results



1. Identify where the location of the web application:

- **Public Websites**

You can scan external websites from Tenable Vulnerability Management using the internet-based Tenable Web App Scanning or an on-premises scanner.

- **Private Websites**

You can scan internal or intranet web applications from Tenable Vulnerability Management using an on-premises Tenable Web App Scanning Scanner.

2. Ensure that the scanner has a network route to the target:

If the scanner cannot reach the web application, or cannot deliver an input and retrieve results, scanning fails. Network constraints such as latency can affect scanning or network controls (for example, host-based firewalls, network firewalls, network segregation, etc.). Always include internal web application scanners on your "allow" list.

3. Scanner location can impact latency or server response times

If there are too many timeouts during a scan, the session terminates. Choose a scanner located as close as possible to the targets. Review the sitemap plugin attachments to check for long page load times or timeouts. This can occur with too many concurrent tests on a slower server, a scanner that's not close enough to the web application (such as scanning Australia from a US scanner), or the site setup that may lead to longer load times. Changing your scanner location can help to prevent readjustments for advanced settings that slow the scanner down. Counter-intuitively, slowing the [scan speed settings](#) can speed up results on a site that responds slowly, by lowering the rate of queries and adding less variability to the returned queries.

4. The scanner acts as a user:

The scanner can follow links, press buttons, and simulate the actions of a user based on what it can access. There can be undesired interaction on the site as a result of its site discovery phase. For example, if a user can send an email, the scanner can fill out forms and press the "send email" button potentially more than once. The scanner has no context for any specific button action, unless you teach it or exclude either the whole page or page element to prevent it from pressing a button unintentionally. (For more information, view our documentation on [Scope Settings](#).) Keep in mind that excluding page elements to prevent such actions lowers



the accuracy of the scan, so consider plans to scan sites like this in pre-production on a regular schedule.

5. The scanner acts as many users:

With its default settings, the scanner can operate as several users navigating the website at the same time. On servers with good capacity, there is typically minimal impact from this activity. However, if the state of the server is unknown, you can de-tune the speed of the scan – at least for the first test – to alert to any potential site impact from simultaneous sessions. For more details on configuring such a test, see [Advanced Settings](#).

6. Customize tuning for each site; it requires effort, but it is optional.

Customized tuning generally applies to most websites because each web application is different. There are unique structures, sitemaps, third-party libraries, components, and custom code working together. Your investment in tuned scans depends on resource availability, criticality of the site, and impact to the business.

7. When tuning for authentication, never run a Tenable Web App Scanning scan as a web site administrator in production - only in test or pre-production environments.

Running a web application scan with administrator credentials could create or delete users, or perform other undesired administrative functions.

8. When tuning for speed, a rudimentary understanding of your sites can help accelerate DAST scans.

- a. Review the sitemap plugin and associated file attachment.
- b. Configure your settings: Increase “Network Timeout,” or lower “Max Simultaneous Requests” and “Requests per Second,” if you experience significant page timeouts, or discover higher than five-second average page response times in the sitemap attachment.
- c. Consider speeding up your scan settings if you obtain sub one-second responses and only minimal impact to the web server.
- d. Deduplicate site content: The scanner does not test site text, image, and video content – only input fields and interactions. If you have redundant pages, such as a site that uses



multiple languages but has the same underlying code, you only need to test one language version of the site.

- e. Add more binary exclusions: Tenable Web App Scanning does not “test” text, images, or videos and decide which file extensions to exclude. The [scan scope](#) section provides a default set that you can adapt for a specific site.
- f. Prioritize critical URLs: Identify the critical portions of the application, such as those ones forms that can return sensitive data. Add those URLs to the scope of your testing, either via “include” in the [scan scope](#) section or through manual crawl script. You can also consider whether these sites require testing in pre-production.

9. **When tuning for complexity, use session recordings to train the scanner.**

You can do this either by using the Tenable Chrome extension or Selenium IDE, and adding within the [scope section](#) of a scan configuration. With this process, you can perform manual crawling to ensure that the scanner can test a highly complex location within a site. For example, a site can require a specific series of button presses and a specific set of correct input values to reach a page that isn’t available any other way. You can record the steps to enable the scanner to play it back.

10. **Map out whether there is a web application firewall (WAF), web proxy, or load balancer between the scanner and the target:**

Som network devices can interfere with the scanning or completely invalidate the results. You may think it’s sufficient to receive only the “remote” view of results filtered by the firewall; however, it’s possible the WAF’s built-in protections only prevent one or two methods of executing the flaw. Gaining a full picture of the true state of the site is imperative to make risk-based decisions. Configure your WAF to support bypass functionality to allow specific IPs or a combination of IP and agent header strings to prove and authorize the incoming scan. A list of Tenable scanner IP ranges is available [here](#).

11. **Some sites can require specific browser identities:**

Check whether the application is compatible with the default user agent (configured as “WAS/%v” by default). If not, it may need a specific or commonly available header from a standard browser, such as Mozilla/5.0. Some server-side protections or a web application firewall can require a specific set of results. In this case, you can copy the user agent string from a known browser that can access the site successfully.



12. Target critical sites with greater care at the outset:

Is the target site production-facing, or in any other way critical? What is the business impact if the web application scanner causes a service disruption? Always perform the first scan of a site in a controlled manner, either with staff on-hand or within a pre-production environment. Once you understand the nature of the site, you can begin full automation.

For more information and guided product walk-throughs, visit our [Tenable Product Education YouTube channel](#). These short, instructional videos explain how to make the best use of Tenable Web App Scanning, including the authentication and tuning procedures mentioned above to help you secure your vulnerable web applications.

Install

1. Preparation for Deployment

- a. **Confirm requisite access to the Tenable Vulnerability Management platform and Tenable Web App Scanning application.** Create users with appropriate access to Tenable Web App Scanning for scanning and viewing of results. You can configure Role-Based Access Control (RBAC) to allow user access. You must have Administrative credentials for configuration.
- b. **Determine whether you need a local scanner.** You can deploy local or cloud-based scanners and connect them to Tenable Vulnerability Management. You can use these scanners on internet-facing web applications and development or pre-production environments (if suitable firewall rules apply).

The [Tenable Core + Tenable Web App Scanning](#) scanner supports installation on VMware (.ova), Hyper-V (.zip), or a physical machine (.ISO). You can deploy it locally on-premises or within a cloud-based development environment to scan non-internet-facing web applications.

You can download the local scanner [here](#). Check that you have the following:

- Outbound access to <https://cloud.tenable.com> via port 443 to communicate with Tenable Vulnerability Management.



- Inbound access via HTTPS on port 8000 for browser access to the management interface.

2. Identification and Planning

- a. **Define the security objectives.** Why are we scanning, what do we hope to achieve, and what does success look like?
- b. **Determine scanning priorities.** Identify which target web applications are within the scope of quick scanning and which require more detailed scanning.
- c. **Ensure full coverage.** Determine whether there are any other (possibly unidentified) web servers, services, or applications that you need to scan, and how to find them.

3. Documentation

- a. **Track everything.** Produce and manage documentation that captures full details of the deployment requirements, deployed scanner resources (if applicable), web applications identified for scanning, and the tuning you applied to the scans with an accompanying rationale.
- b. **Communicate your findings.** Establish reporting requirements to identify: the recipients, the level of detail, and the frequency of the reports distribution. Developers may need PDFs, while ticketing systems require vulnerability details. Management often prefers a higher-level summary of overall exposure and risk reduction.

Configure Scans

After you prepare your analysis workflow and determine the scope of the web application assets, you can configure and run scans on those assets.

Tenable recommends that you first run high-level overview scans to help you determine the settings to configure for more in-depth scans.



1. Do one of the following:

- To configure and run overview scans:

1. Do one of the following:

- To perform an overview scan to determine which web application targets Tenable Web App Scanning scans by default, [create a scan](#) using the **Overview scan template**.
- To perform an overview scan to determine if your web application is compliant with common security industry standards, [create a scan](#) using the **Config Audit scan template**.

Note: The Tenable-provided scan templates for overview scans do not require authentication. However, the plugin results from these scans can help you identify the types of credentials your web applications require for more in-depth scans.

2. Review the [scan results](#), along with your scanning strategy, and determine which configuration settings you want to adjust when you run your standard web application scans.

- To configure and run standard scans:

1. [Create a scan](#) using the template that best matches your assessment needs:

- To perform a comprehensive vulnerabilities scan, select the **Scan** template.
- To perform a scan to determine if your web application appropriately implements SSL/TLS public key encryption, select the **SSL TLS** template.

2. (Optional) Configure your scan settings, including [user permissions](#), and [plugin](#) settings.

Note: You can also configure your [credentials](#) options in standard scans. However, you need to add credentials only if your web application requires them for authentication.

3. Monitor the scan status.

2. [Launch](#) the scan.



3. [View](#) and analyze your scan results:

- Analyze the findings.
- Use the sitemap crawled as an input to detailed scanning, tuning and optimization, reviewing for page timeouts, length of time to access a page, errors, or opportunities to remove repetitive content.
- Review the “Scan notes” for any higher priority concerns, which may provide suggestions for scan improvement.

4. Further tune your scans based on your business needs:

a. **Experiment with advanced settings.** Perform scan tuning in a few locations based on the data gathered in the previous step. You can then update and deploy the scan for the targeted web applications. For more information, see

- [Scope Settings](#)
- [Assessment Settings](#)
- [Advanced Settings](#)

Note: With a Tenable Web App Scanning trial license, you can run up to five scans concurrently using your cloud scanners. You can run any number of scans concurrently using on-premises scanners.

Configure Additional Settings

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

1. Add [credentials](#) to your scan:

- If the scan must authenticate to the web application using methods required by your server's HTTP protocol, [add HTTP Server-Based authentication](#).
- If the scan must authenticate to the web application using methods required by the web application, [add Web App authentication](#).

2. Download the [Tenable Web App Scanning Google Chrome Extension](#) to [configure Selenium credentials automatically](#).



3. Consider further custom adjustments, such as [scan settings](#), [user permissions](#) and [plugin settings](#).

Tip: Each application is unique. Running scans and analyzing the results reveal techniques that help you run scans most efficiently and ensure coverage of all areas of the application. Depending on the size or complexity of the web application, the scan may complete and you can analyze the results for further optimization. Tenable highly recommends that you review the “scan notes” after a scan completes and the attachment to the sitemap plugin regularly.



Tenable Web App Scanning Requirements

Hardware Requirements

Scenario	Hardware Recommendations
WAS Scanning up to 4 concurrent web applications	CPU: (4) 2 GHz cores Core Ram: 16GB RAM Hard Drive: 25GB

Application Requirements

All applications you want to scan must be compatible with Google Chrome, because Tenable Web App Scanning uses Google Chrome browsers to run certain plugins.



Navigate Tenable Web App Scanning

For more information on Tenable Web App Scanning specific navigation, see the following topics:

- [Log In to Tenable Web App Scanning](#)
- [Log Out of Tenable Web App Scanning](#)

Many products within the Tenable Vulnerability Management platform can be navigated in the same manner. For more information, see the following topics in the *Tenable Vulnerability Management Platform User Guide*:

Topic	Description
Updates to the Interface	View new updates to the interface.
Access the Workspace	Access the workspace and each of its products.
Access the User Account Menu	View and manage your user account.
Access the Quick Actions Menu	View a list of common actions to take within the user interface.
Access the Resource Center	View a list of informational resources including product announcements, Tenable blog posts, and user guide documentation.
View Notifications	View and manage system notifications.
Navigate Breadcrumbs	View the path of pages you visited to reach your current page.
Navigate Planes	Learn how to navigate planes within the user interface.
Tables	Learn how to navigate tables within the user interface.
Saved Search	Save and manage frequently used filter parameters.
Error Messages	Learn what error messages mean within the user interface.



Log In to Tenable Web App Scanning

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

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

Before you begin:

- Obtain credentials for your user account.

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

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

The login page appears.

2. In the username box, type your Tenable Web App Scanning username.
3. In the password box, type the Tenable Web App Scanning 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 landing page appears.

Note: Tenable Web App Scanning logs you out after a period of inactivity (typically, 30 minutes).



Log Out of Tenable Web App Scanning

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

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

To log out of Tenable Web App Scanning:

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

The user account menu appears.

2. Click **Sign Out**.



Deploy Tenable Web App Scanning as a Docker Image

You can deploy Tenable Web App Scanning (Tenable Web App Scanning) as a Docker image to run on a container. The base image is an Oracle Linux 8 instance of Tenable Web App Scanning. You can set up your Tenable Web App Scanning instance with environment variables to deploy the Docker image with configuration settings automatically.

Note: Tenable Web App Scanning does not have a command-line interface or configuration wizard, users must use environment variables to configure Tenable Web App Scanning.

Note: Tenable Web App Scanning docker image only works on AMD 64-bit systems and does not support ARM or Windows systems.

Before you begin:

- Download and install Docker for your operating system.
- Access the Tenable Web App Scanning Docker image from <https://hub.docker.com/r/tenable/was-scanner>.

To deploy Tenable Web App Scanning as a docker image:

1. Use the operators with the appropriate options for your deployment, as described in [Operators](#).
2. Use the `-e` operator to set environment variables, as described in [Environment Variables](#).

To Stop and Remove Tenable Web App Scanning as a Docker Image:

- To stop and remove the container, see [Remove Tenable Web App Scanning as a Docker Container](#).

Operators

Operator	Description
<code>--name</code>	Sets the name of the container in Docker.
<code>-d</code>	Starts a container in detached mode.
<code>-e</code>	Precedes an environment variable.



For descriptions of environment variables you can set to configure settings in your Tenable Web App Scanning instance, see [Environment Variables](#).

Environment Variables

Deploying a Tenable Web App Scanning image that is linked to Tenable Vulnerability Management.

Variable	Required?	Description
WAS_SCANNER_NAME	Yes	The name of the Tenable Web App Scanning scanner to appear in Tenable Vulnerability Management.
WAS_LINKING_KEY	Yes	The linking key from Tenable Vulnerability Management.
WAS_SCANNER_GROUPS	No	Scanner groups the scanner must be added to (e.g., "scanner-group-1, sec-scanner-group").
WAS_AUTO_UNLINK_ON_EXIT	No	Automatically unlinks scanner when scanner stops.
WAS_PLATFORM_URL	No	Defaults to <code>https://cloud.tenable.com</code> .
WAS_PROXY_URL	No	URL to use for proxy to platform.



Remove Tenable Web App Scanning as a Docker Container

When you remove Tenable Web App Scanning running as a Docker container, you lose the container data.

To remove Tenable Web App Scanning as a docker container:

1. In your terminal, stop the container from running using the `docker stop` command.

```
$ docker stop <container name>
```

2. Remove your container using the `docker rm` command.

```
$ docker rm <container name>
```



Dashboards

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

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

- Tenable-provided dashboards.
- Dashboards you have created.
- Dashboards that other users have shared with you. Click the **Shared with Me** tab to view dashboards that others have shared with you.

For more information on the Tenable Web App Scanning dashboard, see [Tenable Web App Scanning Dashboard](#).

For more information about all dashboard types, see the following topics in the *Cloud Platform User Guide*:

Topic	Description
View the Dashboards Page	View and interact with the Dashboards page.
Create a Dashboard	Create and configure a dashboard.
Enable Explore Dashboards	Enable Explore dashboards within your user interface.
Manage Dashboards	View, manage, and delete dashboards.
Manage Widgets	View, manage, create, and delete dashboard widgets.



Tenable Web App Scanning Dashboard

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

Tip: For more information on Tenable Web App Scanning, see [Get Started with Tenable Web App Scanning](#).

Tenable Web App Scanning Statistics

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

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

OWASP Top 10

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



Assets

Note: This section describes the new interface. For information about the classic interface, see [Assets in the Classic Interface](#).

The **Assets** page provides insight into your organization's discovered domains and scanned applications.

This page contains **List** view of your asset information:

- [List](#)– A table that lists all your assets from all sources.

About Assets

Tenable Vulnerability Management includes the ability to track assets that belong to your organization. Assets are entities of value on a network that can be exploited. This includes laptops, desktops, servers, routers, mobile phones, virtual machines, software containers, and cloud instances. By providing comprehensive information about the assets that belong to your organization, Tenable Vulnerability Management helps to eliminate potential security risks, identify under-utilized resources, and support compliance efforts.

Tenable Vulnerability Management automatically creates or updates assets when a scan completes or scan results are imported. Tenable Vulnerability Management attempts to match incoming scan data to existing assets using a complex algorithm. This algorithm looks at attributes of the scanned hosts and employs a variety of heuristics to choose the best possible match. If Tenable Vulnerability Management cannot find a match, the system assumes this is the first time Tenable Vulnerability Management has encountered the asset and creates a new record for it. Otherwise, if Tenable Vulnerability Management finds a matching asset, the system updates any properties that have changed since the last time Tenable Vulnerability Management encountered the asset.

In addition to vulnerability information, Tenable Vulnerability Management also attempts to gather various other information about the asset, including:

- Interfaces (IP address and MAC address)
- DNS Names
- NetBIOS Name
- Operating System



- Installed Software
- UUIDS (Tenable, ePO, BIOS)
- Whether an agent is present



Discovered Domains Assets

Required Additional License: Tenable Web App Scanning

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

On the **Assets** page, you can drill down to view only your web application assets.

To view your discovered domain assets:

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

The left navigation plane appears.

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

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

3. In the discovered domains assets table, you can perform any or all the following actions:

- Refine the table data. For more information, see [Tenable Vulnerability Management Tables](#).
- [Filter](#) the table.
- [Export](#) your discovered domain assets.

Discovered Domains

You can view basic information about your discovered domains in the following table:

Column	Description
Asset ID	The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable Web App Scanning.
Name	The asset name. Tenable Web App Scanning assigns this identifier based on the presence of certain asset attributes in the following order: <ol style="list-style-type: none">1. Agent Name (if agent-scanned)



	<ol style="list-style-type: none">2. NetBIOS Name3. FQDN4. IPv6 address5. IPv4 address <p>For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the asset name.</p> <p>This column appears in the table by default.</p>
Host Name	The hostname for the asset.
Record Type	The type of asset.
Record Value	The value of the asset.
Domain	The domain name for the asset.
DNS (FQDN)	The fully qualified domain name of the asset host.
IP Address	The IP address for the asset, if any.
Hosting Provider	The hosting provider for the asset.
ASN	The Autonomous System Number (ASN) of the asset.
Licensed	Specifies whether the asset is included in the asset count for Tenable Web App Scanning.
Created Date	The time and date when Tenable Vulnerability Management created the asset record.
Updated Date	The time and date when a user last updated the asset.
Port	The port associated with the asset.



Actions	The actions you can perform with the asset.
----------------	---



Scanned Application Assets

Required Additional License: Tenable Web App Scanning

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

On the **Assets** page, you can drill down to view only your scanned application assets.

To view your scanned application assets:

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

The left navigation plane appears.

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

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

3. Select the **Scanned Applications** tab.

Tenable Web App Scanning shows your scanned application assets.

Name	AES	ACR	SSL/TLS	IPv4 Address	Operating System	Last Seen	Source	Tags	Actions
<input type="checkbox"/> target2.pubtarg.tenablesecurity.com	200	1	No	44.242.109.183		11/28/2022	Web Application		⋮
<input type="checkbox"/> target1.pubtarg.tenablesecurity.com	549	N/A	No	44.241.194.21		11/28/2022	Web Application		⋮
<input type="checkbox"/> target3.pubtarg.tenablesecurity.com	550	3	No	44.241.160.134		11/28/2022	Web Application		⋮
<input type="checkbox"/> target4.pubtarg.tenablesecurity.com	550	3	No	44.235.70.201		11/23/2022	Web Application		⋮
<input type="checkbox"/> win2019.target.tenablesecurity.com	0	5	No			11/23/2022	Web Application		⋮
<input type="checkbox"/> target977.pubtarg.tenablesecurity.com	0	5				11/23/2022	Web Application		⋮

4. In the scanned applications assets table, you can perform any or all the following actions:

- Refine the table data. For more information, see [Tenable Vulnerability Management Tables](#).
- [Filter](#) the table.



- [View asset details](#) for your web application assets on the [Scanned Application Asset Details](#) page.
- [Export](#) your web application assets.

Scanned Application Assets

You can view basic information about your scanned application assets in the following table:

Column	Description
Name	<p>The asset name. Tenable Web App Scanning assigns this identifier based on the presence of certain asset attributes in the following order:</p> <ol style="list-style-type: none">1. Agent Name (if agent-scanned)2. NetBIOS Name3. FQDN4. IPv6 address5. IPv4 address <p>For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the asset name.</p> <p>This column appears in the table by default.</p>
AES	(Requires Tenable Lumin license)
ACR	(Requires Tenable Lumin license) The asset's ACR .
SSL/TLS	Specifies whether the application on which the asset is hosted uses SSL/TLS public-key encryption.
IPv4 Address	<p>The IPv4 address associated with the asset record.</p> <p>This filter supports multiple asset identifiers as a comma-separated list (for example, hostname_example, example.com, 192.168.0.0). For IP addresses, you can specify individual addresses, CIDR notation (for example, 192.168.0.0/24), or a range (for example, 192.168.0.1-192.168.0.255).</p>



	<p>Note: Tenable Vulnerability Management does not support a CIDR mask of /0 for this parameter, because that value would match all IP addresses. If you submit a /0 value for this parameter, Tenable Vulnerability Management returns a 400 Bad Request error message.</p> <p>Note: Ensure the filter value does not end in a period.</p>
Operating System	<p>The operating system that a scan identified as installed on the asset.</p> <p>This column appears in the table by default.</p>
Last Seen	<p>The date when a scan last found the vulnerability on an asset.</p> <p>This column appears in the table by default.</p>
Source	<p>The source of the scan that identified the asset.</p> <p>This column appears in the table by default.</p>
Tags	<p>Tags applied to the asset.</p> <p>This column appears in the table by default.</p>
Actions	<p>The actions you can perform with the asset.</p>



View Asset Details

Required Additional License: Tenable Web App Scanning

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

To view details for a specific asset:

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

The left navigation plane appears.

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

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

3. (Optional) Refine the table data. For more information, see [Tenable Vulnerability Management Tables](#).

4. In the assets table, click the row for the asset for which you want to see details.

A preview plane of partial asset details appears at the bottom of the page.

5. In the upper-right corner of the split screen, click **See All Details**.

The **Asset Details** page appears.



Scanned Application Asset Details

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

On the **Assets** page, you can click an asset to view basic details about the asset in the preview panel. You can [view](#) more details about the asset on the **Asset Details** page.

The following tables describe the information that appears in each asset details view:



- [Preview Panel](#)
- [Scanned Application Asset Details Page](#)

Preview Panel

The preview panel shows the following details about the scanned application asset.

Section	Description
Left section	
Header	<p>The asset identifier. Tenable Web App Scanning assigns this identifier based on the presence of certain asset attributes in the following order:</p> <ol style="list-style-type: none">1. Agent Name (if agent-scanned)2. NetBIOS Name3. FQDN4. IPv6 address5. IPv4 address <p>For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.</p>
Asset Exposure Score	(Requires Tenable Lumin license) A descriptive icon indicating the Asset Exposure Score (AES) calculated for the asset.
Asset Criticality Rating	(Requires Tenable Lumin license) A descriptive icon indicating the asset's ACR .



Screenshot Available	An interactive button that indicates whether a screenshot is available. To view a screenshot, click the  button.
Center section	
Asset Information	Information about the host asset, including: <ul style="list-style-type: none">• IPv4 Address – An IPv4 address for the asset.• Asset ID – The UUID of the asset.
Scan Information	Information about the asset's scan history, including: <ul style="list-style-type: none">• First Seen – The date and time when a scan first identified the asset.• Last Seen – The date and time of the scan that most recently identified the asset.• Last Licensed Scan – The time and date of the last scan that identified the asset as licensed. For more information about licensed assets, see Tenable Web App Scanning Licenses.
License Information	Specifies whether the asset is licensed.
Right section	
Tags	Tags applied to the asset. Under Tags , you can perform the following tasks: <ul style="list-style-type: none">• Add a tag to the asset by clicking the  button next to Tags• Remove a tag from the asset.
Custom Attributes	Custom attributes that one or more users on your Tenable Web App Scanning instance added to the asset. For more information, see the Tenable Developer Portal .


Scanned Application Asset Details Page

The **Asset Details** page shows the following details about the scanned application asset.



Section	Description
Header	<p>The header row, which includes:</p> <ul style="list-style-type: none">• Scanned Application Asset – The scanned application asset name. Tenable Web App Scanning assigns this identifier based on the presence of certain asset attributes in the following order:<ul style="list-style-type: none">◦ Agent Name (if agent-scanned)◦ NetBIOS Name◦ FQDN◦ IPv6 address◦ IPv4 addressFor example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the asset name.• Actions ^ – An menu button that allows you to perform the following actions:<ul style="list-style-type: none">◦ Export the asset.◦ Delete the asset.
Top section	
Asset Information	<p>Information about the asset, including:</p> <ul style="list-style-type: none">• System Type – The system types as reported by Plugin ID 54615. For more information, see Tenable Plugins.• Operating System – The operating system that a scan identified as installed on the asset.• IP Address – The first IPv4 address for the asset. If there is no IPv4 address, then the first IPv6 for the asset.• Asset ID – The UUID of the asset.



	<ul style="list-style-type: none">• DNS – The fully qualified domain name of the asset host.
Additional Information	<p>Additional information about the asset, including:</p> <ul style="list-style-type: none">• Network – The name of the network object associated with scanners that identified the asset. The default network name is Default. For more information, see Networks.• MAC Address – The static Media Access Control (MAC) address for the asset.• SSH Fingerprint – The SSH key fingerprints that scans have associated with the asset record.• Tenable UUID – The unique identifier for the Tenable account associated with the asset.
Lower section	
Findings	<p>A table that lists all the findings associated with the asset. In this section, you can perform the following actions:</p> <ul style="list-style-type: none">• Refine the table data. For more information, see Tenable Vulnerability Management Tables.• Export one or more findings.• To view the findings for the asset, click Open in Findings.
Right section	
Asset Exposure Score	(Requires Tenable Lumin license) A descriptive icon indicating The Asset Exposure Score (AES) calculated for the asset.
Asset Criticality Rating	(Requires Tenable Lumin license) A descriptive icon indicating The asset's ACR .
Tags	<p>Tags applied to the asset.</p> <p>Under Tags, you can perform the following tasks:</p> <ul style="list-style-type: none">• Add a tag to the asset by clicking the  button next to Tags



	<ul style="list-style-type: none">• Remove a tag from the asset.
Web Application Findings	A colorized list of the VPR scores for the asset's findings, along with a number that indicated the number of findings that received each score.
Scan Information	Information about the asset's scan history, including: <ul style="list-style-type: none">• First Seen – The date and time when a scan first identified the asset.• Last Seen – The date and time of the scan that most recently identified the asset.s• Last Authenticated Scan – The time and date when the scanner last ran a credentialed scan on the asset.



Explore Asset Filters

On the **Assets** page, you can [filter](#) your assets via standard filters that apply to all assets or by asset-specific filters.

You can save a set of commonly used filters as a [saved filter](#) to access later or share with other members of your team.

Note: To optimize performance, Tenable limits the number of filters that you can apply to any **Explore > Findings** or **Assets** views (including **Group By** tables) to 18.

You can select from the following filter types:

Scanned Applications Assets

The following table describes the web application asset filters:

Filter	Description
ACR	(Requires Tenable Lumin license) The asset's ACR .
ACR Severity	(Requires Tenable Lumin license) The ACR category of the ACR calculated for the asset.
AES	(Requires Tenable Lumin license) The AES category of the AES calculated for the asset.
AES Severity	(Requires Tenable Lumin license) The AES category of the AES calculated for the asset.
Asset ID	The asset's UUID.
Custom Attribute	A filter that searches for custom attributes via a category-value pair. For more information about custom attributes, see the Tenable Developer Portal .
Last Authenticated Scan	The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the Last Authenticated Scan field, but not the Last Licensed Scan field.
Last Licensed	The time and date of the last scan that identified the asset as licensed. For



Scan	more information about licensed assets, see Tenable Web App Scanning Licenses .
Last Seen	The date and time of the scan that most recently identified the asset. <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">Note: This filter is selected by default.</div>
Licensed	Specifies whether the asset is included in the asset count for the Tenable Vulnerability Management instance.
Mitigated	Specifies whether a scan has identified mitigation software on the asset.
Mitigation Last Detected	The date and time of the scan that last identified mitigation software on the asset.
Mitigation Product Name	The name of the mitigation software identified on the asset. Tenable Lumin defines mitigations as security agent software running on endpoint assets, which include antivirus software, Endpoint Protection Platforms (EPPs), or Endpoint Detection and Response (EDR) solutions.
Mitigation Version	The version of the mitigation software that a scan identified on the asset.
Name	The asset identifier; assigned based on the presence of certain attributes in the following logical order: <ol style="list-style-type: none">1. Hostname2. WebApp hostname3. Container Security Image name4. Container Runtime hostname5. Nessus Agent name6. Cloud Common Resource name7. Cloud Common Resource identifier8. Cloud Runtime name



	<p>9. Cloud IAC name</p> <p>10. Active Directory Asset name</p> <p>11. Domain Record hostname</p> <p>If none of the above attributes are present, then FQDN is selected as the name for the asset.</p> <p>Note: This filter is selected by default.</p>
Operating System	The operating system that a scan identified as installed on the asset.
Scanned vs. Discovered	<p>Specifies whether Tenable Vulnerability Management scanned the asset for vulnerabilities or if Tenable Vulnerability Management only discovered the asset via a discovery scan. Possible values are:</p> <ul style="list-style-type: none">• Scanned• Discovered
SSL/TLS	Specifies whether the application on which the asset is hosted uses SSL/TLS public-key encryption.
Tags	<p>A unique filter that searches tag (category: value) pairs. When you type a tag value, you must use the <i>category: value</i> syntax, including the space after the colon (:). You can use commas (,) to separate values. If there is a comma in the tag name, insert a backslash (\) before the comma. You can add a maximum of 100 tags.</p> <p>For more information, see tags.</p> <p>Note: If your tag name includes double quotation marks (" "), you must use the UUID instead.</p> <p>Note: This filter is selected by default.</p>

Discovered Domain Assets

The following table describes the web application asset filters:



Filter	Description
ASN	The Autonomous System Number (ASN) for the asset.
Asset ID	The asset's UUID.
Created Date	The time and date when Tenable Vulnerability Management created the asset record.
Deleted	The time and date when Tenable Vulnerability Management deleted the asset record.
DNS (FQDN)	The fully qualified domain name of the asset host.
Domain	The domain name for the asset.
Host Name	The hostname for the asset.
Hosting Provider	The hosting provider for the asset.
IPv4 Address	<p>The IPv4 address associated with the asset record.</p> <p>This filter supports multiple asset identifiers as a comma-separated list (for example, hostname_example, example.com, 192.168.0.0). For IP addresses, you can specify individual addresses, CIDR notation (for example, 192.168.0.0/24), or a range (for example, 192.168.0.1-192.168.0.255).</p> <div data-bbox="381 1318 1479 1514" style="border: 1px solid blue; padding: 5px;"><p>Note: Tenable Vulnerability Management does not support a CIDR mask of /0 for this parameter, because that value would match all IP addresses. If you submit a /0 value for this parameter, Tenable Vulnerability Management returns a 400 Bad Request error message.</p></div> <div data-bbox="381 1535 1479 1612" style="border: 1px solid blue; padding: 5px;"><p>Note: Ensure the filter value does not end in a period.</p></div>
IPv6 Address	<p>An IPv6 address that a scan has associated with the asset record.</p> <p>This filter supports multiple asset identifiers as a comma-separated list. The IPV6 address must be an exact match. (for example, 0:0:0:0:0:ffff:c0a8:0).</p>



	<p>Note: Ensure the filter value does not end in a period.</p>
Name	<p>The asset identifier; assigned based on the presence of certain attributes in the following logical order:</p> <ol style="list-style-type: none">1. Hostname2. WebApp hostname3. Container Security Image name4. Container Runtime hostname5. Nessus Agent name6. Cloud Common Resource name7. Cloud Common Resource identifier8. Cloud Runtime name9. Cloud IAC name10. Active Directory Asset name11. Domain Record hostname <p>If none of the above attributes are present, then FQDN is selected as the name for the asset.</p>
Port	<p>The port associated with the asset.</p>
Record Type	<p>The type of asset.</p>
Tags	<p>A unique filter that searches tag (category: value) pairs. When you type a tag value, you must use the <i>category: value</i> syntax, including the space after the colon (:). You can use commas (,) to separate values. If there is a comma in the tag name, insert a backslash (\) before the comma. You can add a maximum of 100 tags.</p> <p>For more information, see tags.</p>



	<p>Note: If your tag name includes double quotation marks (" "), you must use the UUID instead.</p>
Updated Date	The time and date when a user last updated the asset.



Remove and Prevent Duplicate Assets

In Tenable Vulnerability Management, assets get assigned a unique ID when scanned with credentialed or agent scans. Tenable Vulnerability Management checks this unique ID each time a scan runs, so that it can update the existing asset record with new findings, resolved findings, or resurfaced findings. When you then run an uncredentialed scan against the same asset, the scan cannot log in to the asset and retrieve the unique ID. This causes Tenable Vulnerability Management to view the asset as new, and therefore create a new record (in this case a duplicate of an asset).

Remove Duplicate Assets

To remove duplicate assets in Tenable Vulnerability Management:

1. Within the **Explore** section, [view](#) your asset list.
2. Delete any duplicate assets.

Once an asset is deleted, Tenable Vulnerability Management immediately returns the license to your available license count.

Prevent Duplicate Assets

Preventing duplicate assets from appearing in Tenable Vulnerability Management is usually as simple as avoiding the causes mentioned above. As a best practice, and to resolve duplicate issues, we never recommend scanning assets with uncredentialed and credentialed or agent scans. Instead, pick one or the other.

While there are different use cases for each scan type, generally, Tenable recommends prioritizing the types of scans you run in the following order:

1. Credentialed Scans from a Tenable Nessus Scanner
2. Tenable Nessus Agent Scans
3. Uncredentialed Scans
4. Tenable Nessus Network Monitor

For more information, see [Create a Tenable Vulnerability Management Scan](#).



Export Assets

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

On the **Assets** page, you can export assets in .csv or .json format. You can customize the asset exports that you create. You can schedule exports, send them to a particular email address, and set them to expire.

Note: You cannot export Domain Inventory assets.

Export Assets from the Assets Page

To export assets from the **Assets** page:

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

The left navigation plane appears.

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

The **Assets** page appears.

3. (Optional) Refine the data shown in the table. For more information, see [Explore Tables](#).

4. On the left side, select the checkbox next to the assets to export. You can select up to 200 assets. If you need to export more than 200 assets, select all assets.

The action bar appears at the top of the table.

5. In the action bar, click [→] **Export**.

The **Export** plane appears.

6. In the **Export** plane, configure the following settings:

- a. (Optional) In the **Name** box, type a name for your export.
- b. In the **Formats** section, click the export format to use:



Format	Description
.csv	A .csv file that contains a list of assets. Note: If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article .
.json	A .json file that contains a nested list of assets. Tenable Vulnerability Management does not include empty fields in the .json file.

- c. (Optional) In the **Configurations** section, select the checkboxes next to the fields to include. To view only selected fields, click **View Selected**.

Note: If you modify your field selections, Tenable Vulnerability Management retains them as default the next time you export from the **Assets** page.

- d. (Optional) In the **Expiration** box, type the number of days before the export file ages out.

7. (Optional) Turn on the **Schedule** toggle to set a schedule for your export:

- a. In the **Start Date and Time** section, select the date and time for the schedule to start.

Note: When you schedule an export with filters that do not specify a certain date, those filters update the export as time passes. For example, if you schedule an export for assets that were **Last Seen after** March 15, 2023, Tenable Vulnerability Management increases the export count every time it discovers more assets.

- b. In the **Time Zone** drop-down box, select a time zone.
- c. In the **Repeat** drop-down box, select how often you want the export to repeat.
- d. In the **Repeat Ends** drop-down box, select the date when you want the schedule to end. If you select **Never**, the schedule repeats until you modify or delete the export schedule.

8. (Optional) Enable the **Email Notification** toggle to send email notifications on completion of the export:

- a. In the **Add Recipients** box, type the email addresses to which you want to send a notification.



- b. In the **Password** box, type a password for the export file. Share this password with the recipients to allow them to download the file.

9. Click **Export**.

Depending on the size of the export, Tenable Vulnerability Management may take several minutes to finish processing the export. When processing completes, Tenable Vulnerability Management downloads the export file to your computer.

If you close the **Export** plane before the download completes, you can access your file in **Settings > Exports**.

Export an Asset from the Asset Details Page

To export an asset from the **Asset Details** page:

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

The left navigation plane appears.

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

The **Assets** page appears.

3. (Optional) Refine the data shown in the table. For more information, see [Explore Tables](#).

4. Click the asset to export.

5. On the right side, click **See All Details**.

The **Asset Details** page appears.

6. In the top-right corner, click **Actions**.

7. In the drop-down list, click [→] **Export**.

The **Export** plane appears.

8. In the **Export** plane, add the following information:

- a. (Optional) In the **Name** box, type a name for your export.
- b. In the **Formats** section, click the export format to use:



Format	Description
.csv	<p>A .csv file that contains a list of assets.</p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.</p></div>
.json	<p>A .json file that contains a nested list of assets. Tenable Vulnerability Management does not include empty fields in the .json file.</p>

- c. (Optional) In the **Configurations** section, select the checkboxes next to the fields to include. To view only selected fields, click **View Selected**.

Note: If you modify your field selections, Tenable Vulnerability Management retains them as default the next time you export from the **Assets** page.

- d. (Optional) In the **Expiration** box, type the number of days before the export file ages out.

- 9. (Optional) Turn on the **Schedule** toggle to set a schedule for your export:

- a. In the **Start Date and Time** section, select the date and time for the schedule to start.

Note: When you schedule an export with filters that do not specify a certain date, those filters update the export as time passes. For example, if you schedule an export for assets that were **Last Seen after** March 15, 2023, Tenable Vulnerability Management increases the export count every time it discovers more assets.

- b. In the **Time Zone** drop-down box, select a time zone.
- c. In the **Repeat** drop-down box, select how often you want the export to repeat.
- d. In the **Repeat Ends** drop-down box, select the date on which you want the schedule to end. If you select **Never**, the schedule repeats until you modify or delete the export schedule.

- 10. (Optional) Turn on the **Email Notification** toggle to send email notifications on completion of the export:



- a. In the **Add Recipients** box, type the email addresses to which you want to send a notification.
- b. In the **Password** box, type a password for the export file. Share this password with the recipients to allow them to download the file.

11. Click **Export**.

Tenable Vulnerability Management downloads the export file to your computer. If you close the **Export** plane before the download completes, you can access your file in **Settings > Exports**.

Note: You can export all findings for an asset from the **Findings** tab of the **Details** page. For more information, see [Export Findings](#).



Delete Assets

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

You can delete Host and Web Application assets from the **Assets** page, the **Asset Detail** page, or the **Vulnerability by Asset** page.

When you delete an asset, Tenable Vulnerability Management deletes the asset from the default view of the assets table, deletes vulnerability data associated with the asset, and stops matching scan results to the asset.

If the asset is an Explore asset, then Tenable Vulnerability Management removes the asset from your asset count within 24 hours. All other assets remain on your license count until 90 days after Tenable Vulnerability Management last sees the asset in a scan.

Note: If an asset is part of a network with an **Asset Age Out** setting, this setting overrides these default settings. For more information, see [View or Edit a Network](#).

To delete a single asset:




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

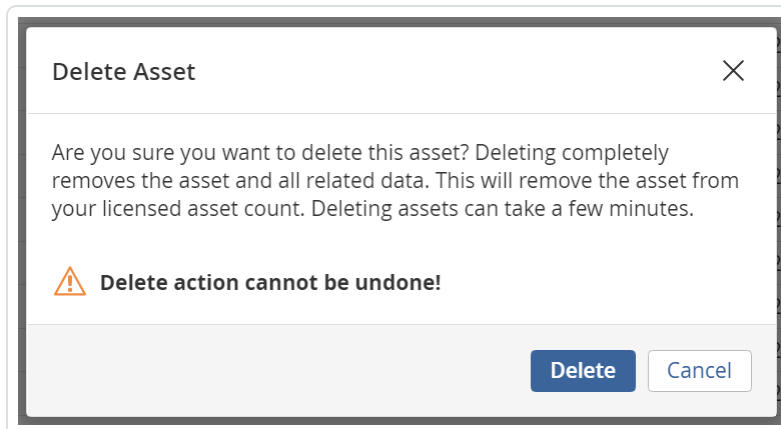
The left navigation plane appears.

2. Do one of the following:

Location	Action
Assets page	<ol style="list-style-type: none">a. View the assets table.b. In the assets table, in the row for the asset you want to delete, click the ⋮ button. A menu appears.c. Click Delete. A confirmation window appears.
Asset Details page	<ol style="list-style-type: none">a. View the asset details.



	<p>b. In the upper-right corner, click the Actions button.</p> <p>The actions menu appears.</p> <p>c. In the actions menu, click  Delete.</p> <p>A confirmation window appears.</p>
Vulnerabilities by Assets	<p>a. View vulnerabilities by asset.</p> <p>b. In the assets table, in the row for the asset you want to delete, click the  button.</p> <p>A menu appears.</p> <p>c. Click  Delete.</p> <p>A confirmation window appears.</p>



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

Tenable Vulnerability Management deletes the asset.

To delete multiple assets:

Note: Tenable Vulnerability Management limits asset deletion to 1,000 records at a time in the **Explore > Assets** table. If you select more than the 1,000 record limit (through individual selections or the **Select All Assets** function), the action button appears in the table's toolbar.



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

The left navigation plane appears.

2. Do one of the following:

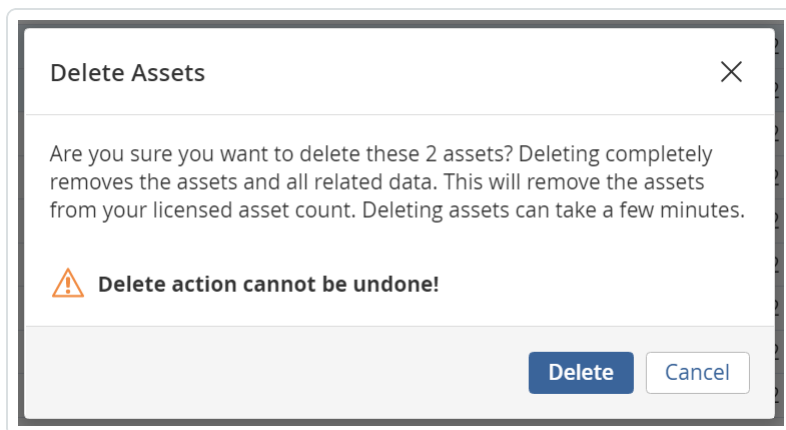
- [View](#) your assets.
- [View](#) your vulnerabilities by asset.

3. In the assets table, click the check box next to each asset you want to delete.

The action bar appears at the bottom of the pagetop of the table.

4. In the action bar, click the 🗑️ **Delete** button.

A confirmation window appears.]



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

Tenable Vulnerability Management deletes the selected assets.


To delete all assets:

Note: Tenable Vulnerability Management limits asset deletion to 5,000 records at a time in the **Explore > Assets** table. If you select more than the 5,000 record limit (through individual selections or the **Select All Assets** function), the action button does not appear in the table's toolbar.

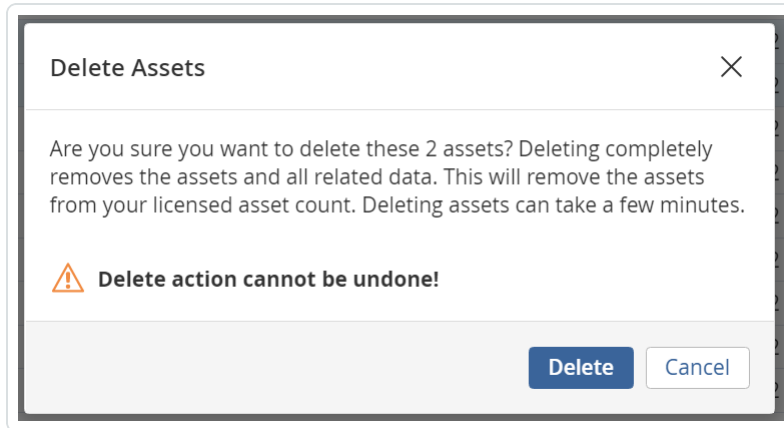
1. [View](#) your assets.
2. In the asset table header row, select the check box to select all assets on the current page.

The action bar appears at the bottom of the pagetop of the table.



3. In the action bar, click **(Select All Assets)** to select all remaining assets.
4. In the action bar, click the  button.

A confirmation window appears.



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

Tenable Vulnerability Management deletes all assets.



Tenable Web App Scanning Vulnerabilities Findings

Required Additional License: Tenable Web App Scanning

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

The **Findings** page provides insight into your organization's vulnerability findings, and the assets on which Tenable Vulnerability Management identified the finding. A finding is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

Note: Tenable Vulnerability Management retains findings data for only 15 months.

The **Findings** page contains a list view of web application findings identified, organized by findings type. You can drill down to view findings for one of the following findings types.

On the **Findings** page, you can drill down to view only vulnerability findings for your web application vulnerabilities.

To view your web application vulnerabilities findings:

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

The left navigation plane appears.

2. The left navigation plane, in the **Explore** section, click **Findings**.

The **Findings** page appears, showing a table that lists your findings. By default, **Group by None** is active.

Web Application Vulnerabilities Findings

You can view basic information about your web application vulnerability findings in the following table.

Column	Description
Asset Name	The name of the asset where the scanner detected the vulnerability. This value is unique to Tenable Vulnerability Management.



	<p>This filter appears on the filter plane by default.</p>
Severity	<p>The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.</p> <p>This column appears in the table by default.</p>
Name	<p>The name of the plugin that identified the vulnerability detected in the finding.</p> <p>This column appears in the table by default.</p>
Plugin ID	<p>The ID of the plugin that identified the vulnerability detected in the finding.</p> <p>This column appears in the table by default.</p>
Family	<p>The family of the plugin that identified the vulnerability.</p> <p>This column appears in the table by default.</p>
State	<p>The state of the vulnerability.</p> <p>This column appears in the table by default.</p>
Last Updated	<p>The date when a scan last found the vulnerability on an asset.</p> <p>This column appears in the table by default.</p>
Asset ID	<p>The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management.</p>
First Seen	<p>The date when a scan first found the vulnerability on an asset.</p>
Actions	<p>Shows an interactive button that allows you to complete certain actions with the finding.</p> <p>This column appears in the table by default and you cannot remove or configure it.</p> <p>To view and complete actions with a finding in the findings table:</p> <ol style="list-style-type: none">In the row for the finding for which you want to complete an action, in the Actions column, click the ⋮ button. <p>The action menu appears in the row.</p>



b. Click the action you want to complete.

A page, plane, or window appears with steps to complete the action.



Web Application Vulnerability Findings Details

Required Additional License: Tenable Web App Scanning

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

On the **Findings** page, you can click a Tenable Web App Scanning vulnerability finding to view basic details about the finding in the preview panel. You can [view](#) more details about the vulnerability on the **Web Application Vulnerabilities Details** page.

The following tables describe the information that appears in each option:

- [Preview Panel](#)
- [Web Application Vulnerabilities Details](#)

Preview Panel

The preview panel shows the following details about the Tenable Web App Scanning vulnerability

Section	Description
Left section	
Header	The name of the plugin that identified the vulnerability that Tenable Vulnerability Management detected in the finding.
Asset Information	Information about the affected asset, including: <ul style="list-style-type: none">• Asset ID – The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management.• Name – The name of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management.• ACR – The Asset Criticality Rating (ACR) for the vulnerability. For more information, see Tenable Lumin Metrics.• IP Address – The IPv4 or IPv6 address for the affected asset.• Type – The type of asset affected.



Center section	
Vulnerability Information	<p>Information about the vulnerability detected in the finding, including:</p> <ul style="list-style-type: none">• Plugin ID – The ID of the plugin that identified the vulnerability.• CVSSV3 Base Score – The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).• CVSSV3 Vector – More CVSSv3 metrics for the vulnerability.
Reference Information	<p>Industry resources that provide additional information about the vulnerability that Tenable Vulnerability Management detected in the finding, including:</p> <ul style="list-style-type: none">• OWASP – A link or links to each Open Web Application Security Project (OWASP) Top 10 list on which the vulnerability appears.• OWASP API – A link or links to each OWASP API Top 10 list on which the vulnerability appears.• WASC – A link to the Web Application Security Consortium (WASC) description for the vulnerability's threat classification.• CWE – A link to the Common Weakness Enumeration (CWE) description for the vulnerability's CWE score.
Right section	
Overview	<p>A tab containing high-level information about the vulnerability detected in the finding, including:</p> <ul style="list-style-type: none">• Description – The description of the Tenable plugin that identified the vulnerability detected in the finding.• Solution – A brief summary of how you can remediate the vulnerability detected in the finding. <div style="border: 1px solid blue; padding: 5px;"><p>Note: A solution appears only if an official vendor solution is published.</p></div>



Plugin Output	A tab containing information from the plugin about the vulnerability detected in the finding.
Attachments	A tab containing plugin attachments that include more details about the vulnerability detected in the finding. This section appears only if attachments are available.

Web Application Vulnerabilities Details

The **Web Application Vulnerabilities Details** page shows the following details about the vulnerability detected in the finding.

Section	Description
Top section	
Description	A description of the Tenable plugin that identified the vulnerability detected in the finding.
Solution	A brief summary of how you can remediate the vulnerability detected in the finding. This section appears only if an official solution is available.
See Also	Links to external websites that contain helpful information about the vulnerability detected in the finding.
Lower section	
Asset Information	Information about the affected asset, including: <ul style="list-style-type: none">• Asset ID – The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management.• Name – The name of the affected asset. You can click the link in the name to view details about the affected asset on the Web Application Asset Details page.• IPV4 Address – The IPv4 address for your asset.• Type – The type of asset affected.
Identification	Information about how the plugin identified the vulnerability detected in the



	<p>finding, including:</p> <ul style="list-style-type: none">• URL – The target URL where the scanner detected the vulnerability.• Proof – Output from the scanner's attempt to verify the vulnerability that proves the vulnerability is exploitable on the affected asset.• Input Type – The component of the asset where an attacker could inject malicious code (for example, a form or session cookie). This section appears only if the asset is vulnerable to injection attacks.• Input Name – The name of the asset component where an attacker could inject malicious code. This section appears only if the asset is vulnerable to injection attacks.• Output – More detailed information from the plugin about the vulnerability detected during the scan.
Http Info	<p>Information about the HTTP messages between the scanner and the web application, including:</p> <ul style="list-style-type: none">• HTTP Request – The HTTP request of the scanner that identified the vulnerability made to the web application.• HTTP Response – The HTTP response that the web application sent to the scanner that identified the vulnerability.
Attachments	<p>Plugin attachments that include more details about the vulnerability detected in the finding. This section appears only if attachments are available.</p>
Right section	
Finding State	<p>A descriptive icon indicating the state of the vulnerability detected in the finding. For more information, see Vulnerability States.</p>
Vulnerability Information	<p>Information about the vulnerability that the plugin identified, including:</p> <ul style="list-style-type: none">• Vuln Published – The date when the vulnerability definition was first published (for example, the date that the CVE was published).• Patch Published – The date on which the vendor published a patch for the vulnerability.



	<ul style="list-style-type: none">• Exploitability – Characteristics of the vulnerability that factor into its potential exploitability.
Discovery	<p>Information about when Tenable Vulnerability Management first discovered the vulnerability detected in the finding, including:</p> <ul style="list-style-type: none">• First Seen – The date when a scan first found the vulnerability on an asset.• Last Seen – The date when a scan last found the vulnerability on an asset.• Age – The number of days since a scan first found the vulnerability on an asset in your network.
Scan Information	<p>Information about the scan that detected the vulnerability detected in the finding, including:</p> <ul style="list-style-type: none">• First Seen – The date on which a scan first found the vulnerability on the affected asset.• Last Seen – The date on which a scan last found the vulnerability on the affected asset.• Auth Configured – Specifies whether the scan that found the vulnerability was authenticated.• Last Auth Scan – The date on which the last authenticated scan that detected the vulnerability occurred.• Last Scan Status – The status of the last scan that detected the vulnerability.• Last Scan Duration – The duration of the last scan that detected the vulnerability.• Licensed – Specifies whether the asset on which the vulnerability was detected is included in the asset count for the Tenable Vulnerability Management instance.
Plugin Details	<p>Information about the plugin that detected the vulnerability detected in the</p>



	<p>finding, including:</p> <ul style="list-style-type: none">• Publication Date – The date on which the plugin that identified the vulnerability was published.• Modification Date – The date on which the plugin was last modified.• Family – The family of the plugin that identified the vulnerability.• Risk Factor – The CVSS-based risk factor associated with the plugin.• Plugin ID – The ID of the plugin that identified the vulnerability detected in the finding.
Risk Information	<p>Information about the relative risk that the vulnerability presents to the affected asset, including:</p> <ul style="list-style-type: none">• CVSS3 Base Score – The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).• CVSS3 Vector – More CVSSv3 metrics for the vulnerability.• CVSS2 Base Score – The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).• CVSS2 Vector – More CVSSv2 metrics for the vulnerability.
Reference Information	<p>A list of references to third-party information about the vulnerability, exploit, or update associated with the plugin.</p>



Group Your Findings

Required Additional License: Tenable Web App Scanning

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

On the [Findings](#) page, you can group your vulnerability findings by specific attributes.

Note: When using the **Group By** feature, you can only [export](#) up to five findings at one time.

To group your vulnerability findings:

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

The left navigation plane appears.

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

The **Findings** page appears, showing a table that lists your findings. By default, **Group by None** is active

3. (Optional) To analyze web application vulnerability findings, click the **Web Application Findings** tab.
4. Do one of the following:

To group your web application findings:

Note: To optimize performance, Tenable limits the number of filters you can apply to any **Explore > Findings** or **Assets** views (including **Group By** tables) to seven.

- a. At the top of the **Web Application Findings** table, next to **Group By**, click one of the following attributes by which to group your findings.

Note: By default, the **None** group by setting is active, so your findings display ungrouped.

- **Asset** – The unique name for the web application associated with the affected asset.



- **Plugin** – The ID of the web application resource type (for example, a resource group or virtual machine).

The web application findings table appears with your findings grouped by the selected attribute.

- b. (Optional) View the following details about your grouped findings.

Note: The details that appear in the table vary based on the attribute you select to group your findings.

Column	Description
Asset	
Asset Name	The name of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management.
Vulnerabilities	A descriptive image that indicates vulnerability percentages by CVSS-based severity for each set of grouped findings. For more information, see CVSS vs. VPR .
Critical	The number of vulnerabilities with a critical CVSS-based severity rating on each set of grouped findings. For more information, see CVSS vs. VPR .
High	The number of vulnerabilities with a high CVSS-based severity rating on each set of grouped findings. For more information, see CVSS vs. VPR .
Vuln Count	The number of vulnerabilities that Tenable Vulnerability Management identified on each set of grouped findings.
Last Seen	The date and time when a scan last found the vulnerability on the asset.
Actions	The actions you can perform with each set of grouped find-



	ings.
Plugin	
Severity	The CVSS-based severity score identified on each set of grouped findings. For more information, see CVSS vs. VPR .
Name	The name of the plugin that identified the vulnerability.
Family	The family of the plugin that identified the vulnerability.
CVSSv2 Base Score	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;">Note: Based on your severity metric settings, this parameter may display CVSSv3 base scores. For more information, see General Settings.</div>
Plugin ID	The ID of the plugin that identified the vulnerability.
Asset Count	The number of assets that Tenable Vulnerability Management identified on each set of grouped findings.
Vuln Count	The number of vulnerabilities that Tenable Vulnerability Management identified on each set of grouped findings.
Actions	The actions you can perform with each set of grouped findings.

5. (Optional) Refine the table data. For more information, see [Tenable Vulnerability Management Tables](#).

6. (Optional) To group by another attribute, next to **Group By**, click another attribute.

The table shows your findings grouped by the new attribute.

7. (Optional) To remove grouping, next to **Group By**, click **None**.

The table shows your findings without grouping.



View Findings Details

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

To view details for a specific finding:

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

The left navigation plane appears.

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

The **Findings** page appears, showing a table that lists your findings. By default, **Group by None** is active.

3. (Optional) Refine the table data. For more information, see [Tenable Vulnerability Management Tables](#).

4. In the findings table, click the row for the finding for which you want to see details.

A preview plane of partial finding details appears at the bottom of the page.

5. In the upper-right corner of the split screen, click **See All Details**.

The **Findings Details** page appears.



Findings Filters

On the **Findings** page, you can [filter](#) and view analytics for the following findings types:

- [Web Application Vulnerabilities](#)

You can save a set of commonly used filters as a [saved filter](#) to access later or share with other members of your team.

Note: To optimize performance, Tenable limits the number of filters that you can apply to any **Explore > Findings** or **Assets** views (including **Group By** tables) to 18.

Web Application Findings Filters

Option	Description
Asset ID	The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable Vulnerability Management.
Asset Name	The name of the asset where the scanner detected the vulnerability. This value is unique to Tenable Vulnerability Management. This filter appears on the filter plane by default.
Bugtraq ID	The Bugtraq ID for the plugin that identified the vulnerability.
CPE	The Common Platform Enumeration (CPE) numbers for vulnerabilities that the plugin identifies.
CVE	The Common Vulnerability and Exposure (CVE) IDs for the vulnerabilities that the plugin identifies.
CVSSv2 Base Score	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
CVSSv2 Vector	The raw CVSSv2 metrics for the vulnerability. For more information, see CVSSv2 documentation.
CVSSv3 Base Score	The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).



CVSSv3 Vector	More CVSSv3 metrics for the vulnerability.
CWE	The Common Weakness Enumeration (CWE) for the vulnerability.
First Seen	The date when a scan first found the vulnerability on an asset.
Input Name	The name of the specific web application component that the vulnerability exploits.
Input Type	The web application component type (for example, form, cookie, header) that the vulnerability exploits.
Last Observed	The date when a scan last observed the finding.
Original Severity	The vulnerability's CVSS-based severity when a scan first detected the finding. For more information, see CVSS vs. VPR .
OWASP 2010	The Open Web Application Security Project (OWASP) 2010 category for the vulnerability targeted by the plugin.
OWASP 2013	The Open Web Application Security Project (OWASP) 2013 category for the vulnerability targeted by the plugin.
OWASP 2017	The Open Web Application Security Project (OWASP) 2017 category for the vulnerability targeted by the plugin.
OWASP 2021	The Open Web Application Security Project (OWASP) 2021 category for the vulnerability targeted by the plugin.
OWASP API 2019	The Open Web Application Security Project (OWASP) 2019 category for the API vulnerability targeted by the plugin. Possible options are: <ul style="list-style-type: none">• API1:2019 Broken Object Level Authorization• API2:2019 Broken User Authentication• API3:2019 Excessive Data Exposure• API4:2019 Lack of Resources & Rate Limiting• API5:2019 Broken Function Level Authorization• API6:2019 Mass Assignment



	<ul style="list-style-type: none">• API7:2019 Security Misconfiguration• API8:2019 Injection• API9:2019 Improper Assets Management• API10:2019 Insufficient Logging & Monitoring
Plugin Description	The description of the Tenable plugin that identified the vulnerability detected in the finding.
Plugin Family	The family of the plugin that identified the vulnerability.
Plugin ID	The ID of the plugin that identified the vulnerability detected in the finding. This filter appears in the filters plane by default.
Plugin Modification Date	The date on which the plugin was last modified.
Plugin Name	The name of the plugin that identified the audit finding. This filter appears in the filters plane by default.
Plugin Published	The date on which the plugin that identified the vulnerability was published.
Risk Modified	The risk modification applied to the vulnerability's severity. Possible options are: <ul style="list-style-type: none">• Recast• Accepted• None For more information, see Recast/Accept Rules .
Severity	The CVSS score-based severity. For more information, see CVSS Scores vs. VPR in the Tenable Vulnerability Management User Guide. This filter appears in the filters plane by default, with Critical , High , Medium , and Low selected.



Solution	A brief summary of how you can remediate the vulnerability detected in the finding.
State	<p>The state of the vulnerability detected in the finding. For more information, see Vulnerability States.</p> <p>This filter appears in the filters plane by default, with Active and Resurfaced selected.</p>
Url	<p>The complete URL on which the scanner detected the vulnerability.</p> <p>This filter appears in the filters plane by default.</p>
WASC	The Web Application Security Consortium (WASC) category associated with the vulnerability targeted by the plugin.



Export Findings

On the **Findings** page, you can export findings in .csv or .json format. You can customize the exports that you create. You can schedule exports, send them to a particular email address, and set them to age out.

Export Findings from the Findings Page

To export findings from the **Findings** page:

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

The left navigation plane appears.

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

The **Findings** page appears.

3. (Optional) Refine the data shown in the table. For more information, see [Explore Tables](#).

Note: When using the **Group By** filter, you can only export five grouped findings at a time. After the fifth selection, the **Export** option disappears.

4. On the left side, select the checkbox next to the findings to export. You can select up to 200 findings. If you need to export more than 200 findings, select all findings.

The action bar appears at the top of the table.

5. In the action bar, click [→] **Export**.

The **Export** plane appears.

6. In the **Export** plane, configure the following settings:

- a. (Optional) In the **Name** box, type a name for your export.
- b. In the **Formats** section, click the export format to use:

Format	Description
.csv	A .csv file that contains a list of findings.



	Note: If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article .
.json	A .json file that contains a nested list of findings. Tenable Vulnerability Management does not include empty fields in the .json file.

- c. (Optional) In the **Configurations** section, select the checkboxes next to the fields to include in the export. To view only selected fields, click **View Selected**.

Note: If you modify your field selections, Tenable Vulnerability Management retains them as the default and applies them the next time you export from the **Findings** page.

- d. (Optional) In the **Expiration** box, type the number of days before the export file ages out.
7. (Optional) Turn on the **Schedule** toggle to set a schedule for your export:
 - a. In the **Start Date and Time** section, select the date and time for the schedule to start.
 - b. In the **Time Zone** drop-down box, select a time zone.
 - c. In the **Repeat** drop-down box, select how often you want the export to repeat.
 - d. In the **Repeat Ends** drop-down box, select the date when you want the schedule to end. If you select **Never**, the schedule repeats until you modify or delete the export schedule.
 8. (Optional) Enable the **Email Notification** toggle to send email notifications on completion of the export:
 - a. In the **Add Recipients** box, type the email addresses to which you want to send a notification.
 - b. In the **Password** box, type a password for the export file. Share this password with the recipients to allow them to download the file.
 9. Click **Export**.



Depending on the size of the export, Tenable Vulnerability Management may take several minutes to finish processing the export. When processing completes, Tenable Vulnerability Management downloads the export file to your computer.

If you close the **Export** plane before the download completes, you can access your file in **Settings > Exports**.

Export a Finding from the Finding Details Page

To export a finding from the **Finding Details** page:

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

The left navigation plane appears.

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

The **Findings** page appears.

3. (Optional) Refine the data shown in the table. For more information, see [Explore Tables](#).

4. Click the finding to export.

5. On the right side, click **See All Details**.

The **Finding Details** page appears.

6. In the top-right corner, click **Actions**.

7. In the drop-down list, click [→] **Export**.

The **Export** plane appears.

8. In the **Export** plane, add the following information:

- a. (Optional) In the **Name** box, type a name for your export.
- b. In the **Formats** section, click the export format to use:

Format	Description
.csv	A .csv file that contains a list of findings.



	Note: If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Vulnerability Management automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article .
.json	A .json file that contains a nested list of findings. Tenable Vulnerability Management does not include empty fields in the .json file.

- c. (Optional) In the **Configurations** section, select the checkboxes next to the fields to include. To view only selected fields, click **View Selected**.

Note: If you modify your field selections, Tenable Vulnerability Management retains them as default the next time you export from the **Findings** page.

- d. (Optional) In the **Expiration** box, type the number of days before the export file ages out.
9. (Optional) Turn on the **Schedule** toggle to set a schedule for your export:
 - a. In the **Start Date and Time** section, select the date and time for the schedule to start.
 - b. In the **Time Zone** drop-down box, select a time zone.
 - c. In the **Repeat** drop-down box, select how often you want the export to repeat.
 - d. In the **Repeat Ends** drop-down box, select the date on which you want the schedule to end. If you select **Never**, the schedule repeats until you modify or delete the export schedule
 10. (Optional) Turn on the **Email Notification** toggle to send email notifications on completion of the export:
 - a. In the **Add Recipients** box, type the email addresses to which you want to send a notification.
 - b. In the **Password** box, type a password for the export file. Share this password with the recipients to allow them to download the file.
 11. Click **Export**.

Tenable Vulnerability Management downloads the export file to your computer. If you close the **Export** plane before the download completes, you can access your file in **Settings > Exports**.



Create Recast/Accept Rules in Findings

In Tenable Tenable Vulnerability Management, you can create rules that affect your vulnerability findings. Recast rules change the [severity](#) of host vulnerabilities or web application findings, while Accept rules accept the risk of these findings without modifying their severity. This topic describes how to create rules from the [Findings workbench](#). For information about how to create or manage rules from the Tenable Vulnerability Management **Settings** section, see [Recast/Accept Rules](#).

Note: If a rule is targeted by IP address, that rule applies to the specified IP in each network in which it is found. For more information, see [Networks](#).

Create a Recast Rule in Findings

To create a Recast rule from the **Findings** workbench:

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

The left navigation plane appears.

2. In the left navigation plane and the **Explore** section, click **Findings**.

The **Findings** page appears with the **Vulnerabilities** tab active and your findings shown in a table view.

3. (Optional) Click **Web Application Findings**.

The **Web Application Findings** tab appears.

4. In the row for the finding to create a rule for, click the ⋮ button.

A drop-down menu appears.

5. Click **Recast**.

The **Add Rule** plane appears.

6. In the **Rule Information** section, complete the following options:

- a. **Vulnerability Plugin ID** - Type the ID of the plugin to recast, if different than the one preselected. For example, 51192.



Note: If the plugin ID corresponds to a Tenable Nessus plugin, the **Original Severity** indicator changes to match the default severity of the vulnerability.

- b. **New Severity** - Select the desired severity level for the vulnerability.
- c. **Targets** - Select **All** to target all assets or **Custom** to specify targets that you want the rule to run against.

Note: If you set the **Targets** drop-down to **All**, a warning appears indicating that this option may override existing rules.

- d. **Target Hosts** - Type one or more custom targets for the rule, if necessary. You can type a comma-separated list that includes any combination of IP addresses, IP ranges, CIDR, and hostnames.

Caution: For performance reasons, you can only specify 1000 comma-separated custom entries. If you need to target a larger number of custom entries, create multiple rules.

- e. (Optional) **Expires** - Select when you want the rule to expire.
- f. (Optional) **Comments** - Type a description of the rule. This option is only visible when the rule is modified.

7. Click **Save**.

Tenable Vulnerability Management starts applying the rule to existing findings. This process may take some time, depending on the system load and the number of matching findings. Tenable Vulnerability Management updates your dashboards, where a label appears to indicate how many instances of affected findings were recast.

Note: A recast rule does not affect the historical results of a scan.

Create an Accept Rule in Findings

To create an Accept rule from the **Findings** workbench:

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

The left navigation plane appears.



2. In the left navigation plane and the **Explore** section, click **Findings**.

The **Findings** page appears with the **Vulnerabilities** tab active and your findings shown in a table view.

3. (Optional) Click **Web Application Findings**.

The **Web Application Findings** tab appears.

4. In the row for the finding to create a rule for, click the **:** button.

A drop-down menu appears.

5. Click **Recast**.

The **Add Recast Rule** plane appears.

6. On the **Add Recast Rule** plane, in the **Action** section, click **Accept**.

7. In the **Rule Information** section, complete the following options:

- a. **Vulnerability Plugin ID** - Type the ID of the plugin to accept, if different than the one preselected. For example, 51192.

Note: If the plugin ID corresponds to a Tenable Nessus plugin, the **Original Severity** indicator changes to match the default severity of the vulnerability.

- b. **Targets** - Select **All** to target all assets or **Custom** to specify targets that you want the rule to run against.
- c. **Target Hosts** - Type one or more custom targets for the rule, if necessary. You can type a comma-separated list that includes any combination of IP addresses, IP ranges, CIDR, and hostnames.

Caution: For performance reasons, you can only specify 1000 comma-separated custom entries. If you need to target a larger number of custom entries, create multiple rules.

- d. (Optional) **Expires** - Select when you want the rule to expire.
- e. (Optional) **Comments** - Type a description of the rule. This option is only visible when the rule is modified.



8. (Optional) To report the vulnerability as a false positive:

- a. Enable the **Report as false positive** toggle.

A **Message To Tenable** box appears.

- b. In the **Message to Tenable** box, type a description of the false positive.

9. Click **Save**.

Tenable Vulnerability Management starts applying the rule to existing findings. This process may take some time, depending on the system load and the number of matching findings.

Saved Filters

Note: This topic is about saved filters in the **Explore** section. If you want to save filters in a legacy workbench, see [Saved Search](#).

Tables in the **Explore** section feature the ability to [filter your findings and assets](#). You can save a set of frequently used filters as a **Saved Filter**. You can then easily access the saved filter for future use, or share the saved filter with other members of your team.


Saved filters are specific to a finding or asset type. For example, you cannot use a saved filter created for Host Vulnerability findings on Host Audit findings types.

Note: When sharing saved filters, users with low-level, or restricted, access may not be able to see all the data that normally appears for a higher-level access user. For information on configuring your permissions, see [Add a Permission Configuration to a User or Group](#).



Create a Saved Filter

To create a saved filter:

1. [Add one or more filters](#) to create the search parameters that you want to save.
2. To the left of the search bar, click the **Saved Filters** drop-down.
3. In the drop-down box, click  **Save**.

A text box appears.

4. Type a name for the saved filter.

Caution: Do not use the same name as an existing [saved search](#) in a legacy workbench. In the future, your saved searches migrate to the [Findings](#) and [Assets](#) pages.

5. Click the  button to save the filters.

The text box closes. The new saved filter appears in the **Saved Filters** drop-down box.

What to do next:

- [Apply the saved filter](#) at any time.
- [Share the saved filter](#) with other users in your organization.



Apply a Saved Filter

To apply a saved filter:

1. View the table where you want to apply the saved filter.


For example, view the **Host Vulnerabilities** tab on the **Findings** page.

2. To the left of the search bar, click the **Saved Filters** drop-down.
3. In the drop-down list, select the saved filter that you want to apply. You can use the search bar in the drop-down menu to find a saved filter.
4. (Optional) To clear a saved filter, in the **Saved Filters** drop-down, click **X** next to the name of the saved filter.



Edit a Saved Filter

To edit the name of a saved filter:

1. To the left of the search bar, click the **Saved Filters** drop-down.
2. Hover over the saved filter you want to rename. You can use the search bar in the drop-down menu to find a saved filter.
3. To the right of the saved filter, click the **⋮** button.
4. Click  **Edit Name**.

A text box appears where you can edit the name of the saved filter.

Caution: Do not use the same name as an existing [saved search](#) in a legacy workbench. In the future, your saved searches migrate to the [Findings](#) and [Assets](#) pages.

5. Modify the filter name and click the **✓** button.



The text box closes. Tenable Vulnerability Management updates the saved filter.

To edit the parameters of a saved filter:

1. To the left of the search bar, click the **Saved Filters** drop-down.
2. Click the saved filter you want to modify. You can use the search bar in the drop-down menu to find a saved filter.
3. [Add, edit, or remove filters](#) at the top of the **Findings** or **Assets** table.

Tenable Vulnerability Management detects the changed filters and shows an *Edited* badge in the **Saved Filters** drop-down menu.

4. In the **Saved Filters** drop-down menu, select an option:

Option	Result
 Save as New	Creates a new saved filter that includes the applied changes.
 Update	Applies the changes to the existing saved filter.






5. (Optional) To discard your changes, in the **Saved Filters** drop-down, click **X** to the right of **EDITED**.



Share a Saved Filter

To get a shareable link for a saved filter:

Note: When sharing saved filters, users with low-level, or restricted, access may not be able to see all the data that normally appears for a higher-level access user. For information on configuring your permissions, see [Add a Permission Configuration to a User or Group](#).

1. To the left of the search bar, click the **Saved Filters** drop-down.
If you have already [applied the filter](#), then the  **Copy Link** option appears in the **Shared Filters** drop-down menu. Otherwise, continue to step 2.
2. Hover over the saved filter you want to share. You can use the search bar in the drop-down menu to find a saved filter.
3. To the right of the saved filter, click the  button.
4. Click  **Copy Link**.


A confirmation message appears, and Tenable Vulnerability Management copies a shareable link for the saved filter to your clipboard.



Delete a Saved Filter

Note: If you delete a saved filter that is currently applied to your findings or assets, Tenable Vulnerability Management clears the applied filters from the current view.

To delete a saved filter permanently:

1. On the [Findings](#) or [Assets](#) page, to the left of the search bar, click the **Saved Filters** drop-down.
2. Hover over the saved filter you want to delete. You can use the search bar in the drop-down menu to find a saved filter.
3. To the right of the saved filter, click the **⋮** button.
4. Click  **Delete**.

The **Delete** button appears.


5. To confirm you want to delete the saved filter permanently, click the **Delete** button.

Tenable Vulnerability Management deletes the saved filter.



Create a Saved Filter

To create a saved filter:

1. [Add one or more filters](#) to create the search parameters that you want to save.
2. To the left of the search bar, click the **Saved Filters** drop-down.
3. In the drop-down box, click  **Save**.

A text box appears.

4. Type a name for the saved filter.

Caution: Do not use the same name as an existing [saved search](#) in a legacy workbench. In the future, your saved searches migrate to the [Findings](#) and [Assets](#) pages.

5. Click the  button to save the filters.

The text box closes. The new saved filter appears in the **Saved Filters** drop-down box.

What to do next:

- [Apply the saved filter](#) at any time.
- [Share the saved filter](#) with other users in your organization.



Apply a Saved Filter

To apply a saved filter:

1. View the table where you want to apply the saved filter.


For example, view the **Host Vulnerabilities** tab on the **Findings** page.

2. To the left of the search bar, click the **Saved Filters** drop-down.
3. In the drop-down list, select the saved filter that you want to apply. You can use the search bar in the drop-down menu to find a saved filter.
4. (Optional) To clear a saved filter, in the **Saved Filters** drop-down, click **X** next to the name of the saved filter.



Edit a Saved Filter

To edit the name of a saved filter:

1. To the left of the search bar, click the **Saved Filters** drop-down.
2. Hover over the saved filter you want to rename. You can use the search bar in the drop-down menu to find a saved filter.
3. To the right of the saved filter, click the **:** button.
4. Click  **Edit Name**.

A text box appears where you can edit the name of the saved filter.

Caution: Do not use the same name as an existing [saved search](#) in a legacy workbench. In the future, your saved searches migrate to the [Findings](#) and [Assets](#) pages.

5. Modify the filter name and click the  button.



The text box closes. Tenable Vulnerability Management updates the saved filter.

To edit the parameters of a saved filter:

1. To the left of the search bar, click the **Saved Filters** drop-down.
2. Click the saved filter you want to modify. You can use the search bar in the drop-down menu to find a saved filter.
3. [Add, edit, or remove filters](#) at the top of the **Findings** or **Assets** table.

Tenable Vulnerability Management detects the changed filters and shows an *Edited* badge in the **Saved Filters** drop-down menu.

4. In the **Saved Filters** drop-down menu, select an option:

Option	Result
 Save as New	Creates a new saved filter that includes the applied changes.
 Update	Applies the changes to the existing saved filter.






5. (Optional) To discard your changes, in the **Saved Filters** drop-down, click ✕ to the right of **EDITED**.



Share a Saved Filter

To get a shareable link for a saved filter:

Note: When sharing saved filters, users with low-level, or restricted, access may not be able to see all the data that normally appears for a higher-level access user. For information on configuring your permissions, see [Add a Permission Configuration to a User or Group](#).

1. To the left of the search bar, click the **Saved Filters** drop-down.
If you have already [applied the filter](#), then the  **Copy Link** option appears in the **Shared Filters** drop-down menu. Otherwise, continue to step 2.
2. Hover over the saved filter you want to share. You can use the search bar in the drop-down menu to find a saved filter.
3. To the right of the saved filter, click the  button.
4. Click  **Copy Link**.

A confirmation message appears, and Tenable Vulnerability Management copies a shareable link for the saved filter to your clipboard.



Delete a Saved Filter

Note: If you delete a saved filter that is currently applied to your findings or assets, Tenable Vulnerability Management clears the applied filters from the current view.

To delete a saved filter permanently:

1. On the [Findings](#) or [Assets](#) page, to the left of the search bar, click the **Saved Filters** drop-down.
2. Hover over the saved filter you want to delete. You can use the search bar in the drop-down menu to find a saved filter.
3. To the right of the saved filter, click the **⋮** button.

4. Click  **Delete**.

The **Delete** button appears.

5. To confirm you want to delete the saved filter permanently, click the **Delete** button.

Tenable Vulnerability Management deletes the saved filter.

Explore Tables

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

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

You can access Explore tables in the **Explore** section of Tenable Vulnerability Management. Explore tables present your organization's data in a single pair of workbenches: the **Findings** workbench and the **Assets** workbench. Each workbench contains tables of findings or asset data. This topic describes how to apply filters to Explore tables and how to customize them.



Filter an Explore Table

In the **Explore** section, you can filter your organization's assets and findings on the **Assets** and **Findings** pages. For a list of available filters, see [Asset Filters](#) or [Findings Filters](#).

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

To filter a table in the **Explore** section:

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

The left navigation plane appears.

2. Do one of the following:

- In the left navigation plane, under **Explore**, click **Findings**.

The **Findings** page appears.

- In the left navigation plane, under **Explore**, click **Assets**.

The **Assets** page appears.

3. Do one of the following:

To filter the table in **Basic** mode:

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

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

- b. Click **Select Filters**.

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

- c. Select the filters you want to apply.

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

The **Select Filters** box closes.



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

The image shows a filter configuration interface for 'Severity'. At the top, there is a dropdown menu labeled 'Severity' with a downward arrow. Below it is a search operator dropdown menu showing 'is equal to' with a downward arrow. Underneath the operator menu is a list of radio button options: 'Critical' (checked), 'High', 'Medium', 'Low', and 'Info'.

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

Operator	Description
exists	Filters for items for which the selected filter exists.
does not exist	Filters for items for which the selected filter does not exist.
is equal to	Filters for items that match the filter value.
is not equal to	Filters for items that do not include the filter value.
is greater than is greater	Filters for items with a value greater than the specified filter value. If you want to include the value you specify in the filter, then use the is greater than or equal to operator.



Operator	Description
than or equal to	
is less than is less than or equal to	Filters for items with a value less than the specified filter value. If you want to include the value you specify in the filter, then use the is less than or equal to operator.
within last	Filters for items with a date within a number of hours, days, months, or years before today. Type a number, then select a unit of time.
after	Filters for items with a date after the specified filter value.
before	Filters for items with a date before the specified filter value.
older than	Filters for items with a date more than a number of hours, days, months, or years before today. Type a number, then select a unit of time.
is on	Filters for items with a specified date.
between	Filters for items with a date between two specified dates.

Tip: If you select a filter with a specific value, you must type the value. You can use a wildcard operator to do a *contains* search. For example, if you want a filter to include all values that end in 1, type **1*. If you want a filter to include all values that begin with 1, type *1**. If you want a filter to include all values with a 1 somewhere between the first and last characters, type **1**.

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

- To clear the values for a filter, hover on the right side of the filter and click **Clear**.
- To remove a single filter, hover on the right side of the filter and click **Remove**.
- To remove all filters, at the top of the filters plane, click **Clear All**.

g. Click **Apply**.

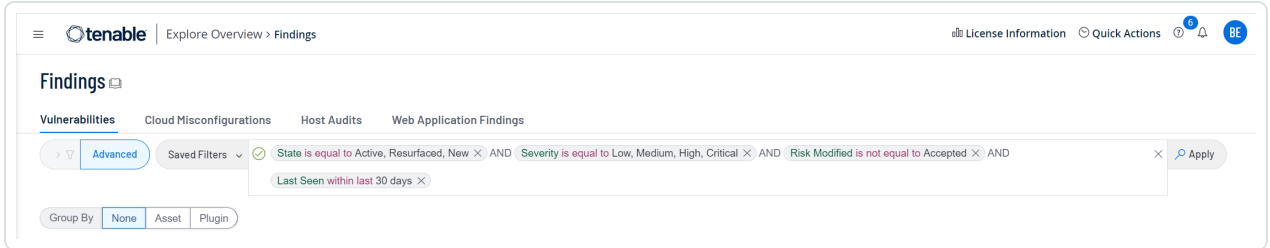
Tenable Vulnerability Management filters your data.



To filter the table in **Advanced** mode:

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

A text box appears with the current filters displayed as shown in the following image.



- b. Click inside the text box.

A drop-down box appears.

Tip: You can use the arrow keys to navigate the filter drop-down box and press the **Enter** key to select an option.

- c. In the drop-down box, select the **AND** or **OR** conditions or type them in the text box.
- d. In the drop-down box, select a filter or type its name in the text box.
- e. In the drop-down box, select one of the following operators or type it in the text box.

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

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



Operator	Description
is greater than is greater than or equal to	Filters for items with a value greater than the specified filter value. If you want to include the value you specify in the filter, then use the is greater than or equal to operator.
is less than is less than or equal to	Filters for items with a value less than the specified filter value. If you want to include the value you specify in the filter, then use the is less than or equal to operator.
within last	Filters for items with a date within a number of hours, days, months, or years before today. Type a number, then select a unit of time.
after	Filters for items with a date after the specified filter value.
before	Filters for items with a date before the specified filter value.
older than	Filters for items with a date more than a number of hours, days, months, or years before today. Type a number, then select a unit of time.
is on	Filters for items with a specified date.
between	Filters for items with a date between two specified dates.

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

Tip: Some text filters support the character (*) as a wildcard to stand in for a section of text in the filter value. For example, if you want the filter to include all values that end in 1, type **1*. If you want the filter to include all values that begin with 1, type *1**.

You can also use the wildcard operator to filter for values that contain certain text. For example, if you want the filter to include all values with a 1 somewhere between the first and last characters, type **1**.

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



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

h. Click **Apply**.

Tenable Vulnerability Management filters your data.

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

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



Filter By Value

With **Filter By Value**, you can filter your data by any value in an Explore table. For example, in the **Findings** table, you can view all findings with a certain IPv4 address through a single action.

To filter by value:

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

The left navigation plane appears.

2. Do one of the following:

- In the left navigation plane, under **Explore**, click **Assets**.

The **Assets** page appears.

- In the left navigation plane, under **Explore**, click **Findings**.

The **Findings** page appears.

3. Right-click the table cell whose value you want to filter by.

A menu appears.

4. In the menu, click  **Filter By Value**.

Tenable Vulnerability Management filters your data.



Filter Out Value

With **Filter Out Value**, you can customize an Explore table to remove all entries with certain value. For example, in the **Assets** table, you can remove assets with a certain operating system through a single action.

To filter out a value:

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

The left navigation plane appears.

2. Do one of the following:

- In the left navigation plane, under **Explore**, click **Assets**.

The **Assets** page appears.

- In the left navigation plane, under **Explore**, click **Findings**.

The **Findings** page appears.

3. Right-click the table cell whose value you want to filter out.

A menu appears.


4. In the menu, click  **Filter Out Value**.

Tenable Vulnerability Management removes the selected data from the table.



Copy to Clipboard

With **Copy to Clipboard**, you can get any value from an Explore table. For example, when creating a tag, you can copy an operating system value from a cell in the **Assets** table and add it to your tag.

To use **Copy to Clipboard**, from either the **Findings** or **Assets** table, right-click any cell and click  **Copy to Clipboard**.



Customize an Explore Table

In the **Explore** section, on the **Findings** or **Assets** pages, you can customize the columns in the tables that display your data.

To customize an Explore table:

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

The left navigation plane appears.

2. Do one of the following:

- In the left navigation plane, under **Explore**, click **Assets**.

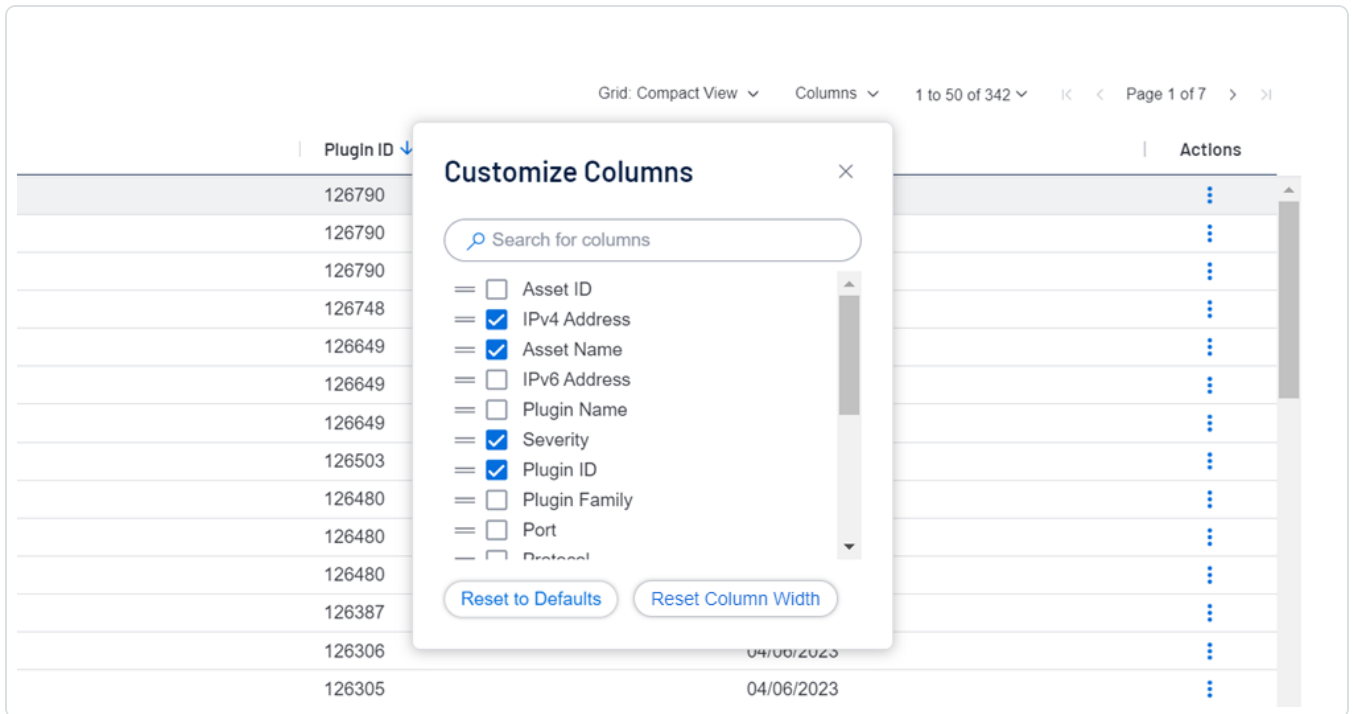
The **Assets** page appears.

- In the left navigation plane, under **Explore**, click **Findings**.

The **Findings** page appears.

3. On the right side, above the table that contains your data, click **Columns**.

The **Customize Columns** dialog appears.



4. Do one of the following:

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



Manage Tenable Web App Scanning Scans

Required Additional License: Tenable Web App Scanning

Note: The topics in this section describe web application scans in the new interface only. If you activate the new interface, you can view a historical snap shot of scan configurations in the classic interface, but you can modify those configurations in the new interface only.

For information about scans in the classic interface, see [Scans \(Classic Interface\)](#).

Configure web application scans to collect data about your web applications for analysis. This overview walks you through the main steps you need to create, configure, launch, and manage Tenable Web App Scanning scans.

Depending on your organization, one person may perform all of the steps, or several people may share the steps.

Create and launch a Tenable Web App Scanning scan

1. [Create](#) a Tenable Web App Scanning scan.
2. Select a scan, or scan template that fits your needs.
 - Use a Tenable Web App Scanning scan type(LINK!).
 - Use a [Tenable-provided scan template](#).
 - Create and use a [user-defined scan template](#).
3. Configure the scan:
 - Configure the [scan settings](#) available for your scan template.
 - (Optional) To run a credentialed scan, [configure credentials](#).
4. [Launch](#) the scan.
 - Monitor the [scan status](#).
 - View details about the scan's efficiency in the [Notes tab](#).

View and manage scans



1. [View](#) your scan results.
2. [View](#) details about the plugin results in attachments to scan results.
3. Remove legacy scans and scan results from your [dashboard](#).
 - [Delete the results](#) from a single scan job.
 - [Move a Scan to the Trash Folder](#) a scan and the associated results to the **Trash** folder.
 - [Delete a scan](#), along with all the scan results for that scan.



Create and Launch a Scan

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

To create a scan in the new Tenable Web App Scanning interface:

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

The left navigation plane appears.

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

The **My Scans** page appears.

3. Do one of the following:

- To launch a single scan:

- a. In the scans table, roll over the scan you want to launch.
- b. On the right side of the row, click the ▷ button.

The scan launches and the **Status** column updates to reflect the status of the scan.

- To launch multiple scans:

- a. In the scans table, select the check box(es) next to the scans you want to launch.

The action bar appears at the bottom of the page.

- b. In the action bar, click the ▷ button.

The scans launch and the respective **Status** columns update to reflect the statuses of the scans.

- To create and launch a new scan without a scan template:

- a. In the upper-right corner of the page, click the  **Create Scan** button.

The **Create Scan** page appears. By default, the **Scans** tab is active.



- b. Select either **Quick Scan**, **Basic Scan**, **Full Scan**, or **Custom Scan**. For more information on scan types, see Tenable Web App Scanning [Scan Types](#).

Enter your scan information and click **Save** to save the scan setup, or click **Save and Run** to launch the scan.

- To create and launch a new scan with **Tenable Templates**:
 - a. In the upper-right corner of the page, click the **+** **Create Scan** button.

The **Create Scan** page appears. By default, the **Scans** tab is active.
 - b. Select **Tenable Templates**.
 - c. Select a template from the list. For more information on scan templates, see [Tenable-Provided Tenable Web App Scanning Templates](#).
 - d. After configuring your scan template, click **Save and Run**.
- To create and launch a new scan with a previously created **User Template**:
 - a. In the upper-right corner of the page, click the **+** **Create Scan** button.

The **Create Scan** page appears. By default, the **Scans** tab is active.
 - b. Select **User Templates**.
 - c. Select a template from the list. For more information on scan templates, see [Tenable-Provided Tenable Web App Scanning Templates](#).
 - d. After configuring your scan template, click **Save and Run**.

Note: To create a new user template, see User Templates.

4. Enter your scan information and click **Save** to save the scan setup, or click **Save and Run** to launch the scan.

Tenable Web App Scanning launches the scan.

Note: When you launch a scan, the time the scanner takes to complete the scan varies depending on the system load. To prevent lengthy scan times, avoid launching an excessive number of scans simultaneously. Excessive numbers of concurrent scans may exhaust the system's scanning capacity. If



necessary, Tenable Web App Scanning automatically staggers concurrent scans to ensure consistent scanning performance.

Note: Tenable Web App Scanning aborts scans that remain in **pending** status for more than four hours. If Tenable Web App Scanning aborts a scan, modify your scan schedules to reduce the number of overlapping scans. If you still have issues, contact Tenable Support.



Edit Tenable Web App Scanning Scan Settings

Required Additional License: Tenable Web App Scanning

Required Tenable Web App Scanning User Role: WAS Scan Manager or Administrator

Required Scan Permissions: Can Configure

Note: This topic describes how to configure scan settings in the new interface only. If you activate the new interface, you can view a snapshot of your historical scan configurations in the classic interface, but you cannot modify configurations for scans run using any scan template other than the **PCI WAS Scan** template from the classic interface.

The settings you can configure in a Tenable Web App Scanning scan or user-defined scan template depend on the Tenable-provided scan template type. For more information, see [Scan Templates](#).

To configure scan settings in the new interface:

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

The left navigation plane appears.

2. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.

The Web Application Scanning **Scans** page appears.

NAME	SCHEDULE	TARGETS	LAST MODIFIED	LAST RUN	STATUS	ACTIONS
Config Audit	On Demand	1	02/17/2022	02/17/2022	Completed	⋮
OWASP Juice Shop API	On Demand	1	02/17/2022	02/17/2022	Completed	⋮
CS-47008	On Demand	1	02/08/2022	02/08/2022	Completed	⋮
Copy of CS-46300	On Demand	1	01/20/2022	01/20/2022	Completed	⋮
CS-46300	On Demand	1	01/20/2022	Never Run	Aborted	⋮

Note: If your Tenable Web App Scanning license expires, your web application scans no longer appear in the scans table.

3. In the scans table, roll over the scan you want to configure.

The action buttons appear in the row.



4. Click the  button.

The **Update a Scan** page appears.

5. Modify the scan settings.
6. (Optional) In the **Advanced Settings** section, add **Session Settings**.

Note: Specifying this token speeds up the scan by allowing the scanner to skip token verification. Only available while you are editing an existing scan. For more information, see [Advanced Settings](#).

7. Click **Save**.

Tenable Vulnerability Management saves the scan settings.

Set Tenable Web App Scanning Scan Permissions

Required Additional License: Tenable Web App Scanning

Required User Role: Administrator

Note: For a complete overview of Tenable Web App Scanning permissions and user roles, see [Permissions](#) in the *Tenable Developer Portal*.

In an existing scan, you can add new user or group permissions or update existing permissions.

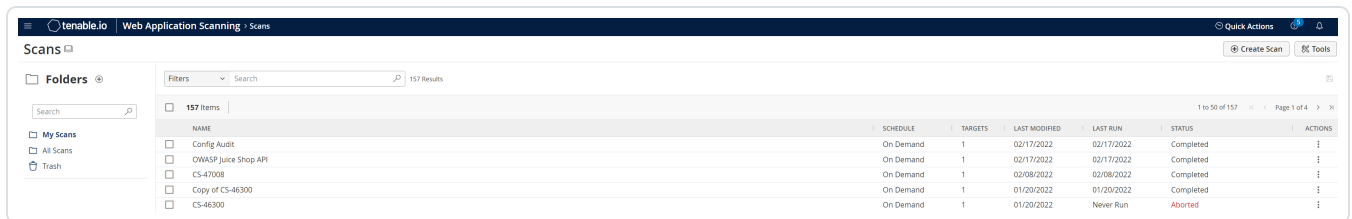
To add permissions in the new interface:

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

The left navigation plane appears.

2. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.

The Web Application Scanning **Scans** page appears.



NAME	SCHEDULE	TARGETS	LAST MODIFIED	LAST RUN	STATUS	ACTIONS
Config Audit	On Demand	1	02/17/2022	02/17/2022	Completed	⋮
OWASP Juice Shop API	On Demand	1	02/17/2022	02/17/2022	Completed	⋮
CS-47008	On Demand	1	02/06/2022	02/06/2022	Completed	⋮
Copy of CS-46300	On Demand	1	01/20/2022	01/20/2022	Completed	⋮
CS-46300	On Demand	1	01/20/2022	Never Run	Aborted	⋮

Note: If your Tenable Web App Scanning license expires, your web application scans no longer appear in the scans table.

3. In the scans table, hover over the row for the scan for which you want to set permissions.
4. On the right side of the row, click the ✎ button.

The **Update a Scan** page appears.

5. In the **User Permissions** section, click the ⊕ button.

The **Add User Permission** plane appears.



6. In the **Add Users or Groups** drop-down box, select user name or group with whom you want to share the scan.

The user name or group appears in the list of users below the drop-down box.

Tip: If you being typing the name of the user name or group in the drop-down box, Tenable Web App Scanning displays a list of options that match your text.

7. Next to the user or group name, in the drop-down box, select the permissions you want to apply to the user or group.

8. Click **Add**.

The **Add User Permission** plane disappears.

The user or group name appears under the **User Permissions** section, along with the permissions you selected.

9. Click **Save**.

Tenable Web App Scanning updates the scan permissions.

To update existing permissions in the new interface:

Note: You cannot update permissions for the user that owns the scan.

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

The left navigation plane appears.


2. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.

The Web Application Scanning **Scans** page appears.

NAME	SCHEDULE	TARGETS	LAST MODIFIED	LAST RUN	STATUS	ACTIONS
Config Audit	On Demand	1	02/17/2022	02/17/2022	Completed	
OWASP Juice Shop API	On Demand	1	02/17/2022	02/17/2022	Completed	
CS-47008	On Demand	1	02/08/2022	02/08/2022	Completed	
Copy of CS-46300	On Demand	1	01/20/2022	01/20/2022	Completed	
CS-46300	On Demand	1	01/20/2022	Never Run	Aborted	





Note: If your Tenable Web App Scanning license expires, your web application scans no longer appear in the scans table.

3. In the scans table, hover over the row corresponding to the scan for which you want to set permissions.
4. On the right side of the row, click the  button.

The **Update a Scan** page appears.

5. In the **User Permissions** section, you can:

Action	Steps
Update permissions for a user or group	In the drop-down box next to the user or group name, select the permissions you want to apply.
Remove all permissions from a user or group	<ul style="list-style-type: none">• Roll over the user or group name. A  button appears next to the drop-down box.• Click the  button. The user or group name disappears from the list.

6. Click **Save**.

Tenable Web App Scanning updates the permissions.



Launch a Tenable Web App Scanning API Scan

Required Additional License: Tenable Web App Scanning

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

Required Scan Permissions: Can Control

Note: When you launch a scan, the time the scanner takes to complete the scan varies depending on the system load. To prevent lengthy scan times, avoid launching an excessive number of scans simultaneously. Excessive numbers of concurrent scans may exhaust the system's scanning capacity. If necessary, Tenable Web App Scanning automatically staggers concurrent scans to ensure consistent scanning performance.

In Tenable Web App Scanning, you can create discovery, assessment, and API scans using scan templates. For general information about templates and settings, see [Scan Templates and Settings](#).

Note: You cannot have more than 25 scans running in your container simultaneously.

Before you begin:

- Have the swagger file used to describe the API available for reference.

To launch a Tenable Web App Scanning API scan:

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

The Tenable Web App Scanning **Scans** page appears.

Note: If your Tenable Web App Scanning license ages out, your Tenable Web App Scanning scans no longer appear in the scans table.

2. In the top navigation, select **Web Application Scans**.
3. Click the **Create Scan** button in the upper right-hand corner of the page.

The Scans Template page appears.

4. Select the **API** scan template.



5. In the **Settings** section of the Create a Scan - API Scan page, populate the following minimum required settings:

Note: While not required, Tenable recommends putting all scans on a repeating schedule. For more information about Tenable Web App Scanning Scan schedules, see [Schedule](#).

- Name
- Scanner
- Target

6. In the **Scope** section, add the OpenAPI (Swagger) file for the API you are scanning.

Note: For more information on Swagger specification files. see [OpenAPI \(Swagger\) Specification](#).

7. Click **Save**.

Tenable Vulnerability Management returns to the list of configured Tenable Web App Scanning scans.

8. To launch the scan, click the **⋮** button in the **Actions** column for the scan that needs to be run and select **Launch**.
9. When the scan has completed, click the scan to view the results.

Note: Tenable Web App Scanning aborts scans that remain in **pending** status for more than four hours. If Tenable Web App Scanning aborts a scan, modify your scan schedules to reduce the number of overlapping scans. If you still have issues, contact Tenable Support.



Tenable Web App Scanning Scan Filters

On the **Scans** page, you can filter Tenable Web App Scanning scans using Tenable-provided filters.

Filter	Description
Created Date	The date the scan configuration was created.
Description	The description of the scan configuration.
Finalized Date	The date on which the scan last completed.
Last Modified Date	The date on which the scan configuration was last modified.
Last Scanned Date	The date on which the scan was last ran.
Name	The name of the scan configuration.
Schedule	Whether a scan schedule is enabled or on demand.
Status	The status of the scan. For more information about scan statuses, see Scan Status .
Target	The target URL used to launch the scan.
Template	The Tenable-provided scan template the scan configuration was based on.
User Template	The user-defined scan template the scan configuration was based on.



View Tenable Web App Scanning Scan Details

Required Additional License: Tenable Web App Scanning

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

Required Scan Permissions: Can View

Note: This topic describes the process for viewing scan results in the new interface only.

If you activate the new interface, you can view scan results as follows:

- For scans run based on historical scan configurations, view results in either interface.
- For scans run based on new scan configurations, view results in the new interface only.

You can view scan results for web application scans you own or that the scan owners have shared with you.

Note: After Tenable Vulnerability Management completes the scan, it can take up to 10 minutes for the scan results to appear in the dashboard.

To view scan details for an individual web application scan:

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

The left navigation plane appears.

2. In the left navigation plane, in the **Web App Scanning** section, click **Scans**.

The Web Application Scanning **Scans** page appears.

NAME	SCHEDULE	TARGETS	LAST MODIFIED	LAST RUN	STATUS	ACTIONS
Config Audit	On Demand	1	02/17/2022	02/17/2022	Completed	⋮
OWASP Juice Shop API	On Demand	1	02/17/2022	02/17/2022	Completed	⋮
CS-47008	On Demand	1	02/08/2022	02/08/2022	Completed	⋮
Copy of CS-46300	On Demand	1	01/20/2022	01/20/2022	Completed	⋮
CS-46300	On Demand	1	01/20/2022	Never Run	Aborted	⋮



Note: If your Tenable Web App Scanning license expires, your web application scans no longer appear in the scans table.

3. In the **Folders** section, click a folder to load the scans you want to view.

The scans table updates to display the scans in the folder you selected.

4. In the scans table, click the scan where you want to view details.

The **Scan Details** page appears. By default, this page displays details of the latest run of the scan.

5. Do any of the following:

Section	Action
Table header	<ul style="list-style-type: none">• Edit the scan configuration.• Move a scan to the trash folder.
Severity summaries	For the scan job currently displayed, view the number of vulnerabilities with a Critical , High , Medium , or Low vulnerability severity.
Scan Details section	For the scan job currently displaying, view the following details: <ul style="list-style-type: none">• Status – The status of the scan.• Start Time – The start date and time for the scan.• Template – The scan template you used to configure and run the scan.• End Time – The end date and time for the scan.• Scanner – The scanner that performed the scan.• Target – The target the scan evaluated.
Vulns by Plugin tab	For the scan job currently displayed, view vulnerability data, organized by plugin. On this tab, you can: <ul style="list-style-type: none">• View information about each vulnerability:



	<ul style="list-style-type: none">• Severity icon – The severity of the vulnerability.• Name – The name of the vulnerability, as defined in the Common Vulnerabilities and Exposures (CVE) system.• Family – The plugin family.• Vulnerabilities – The number of vulnerability instances. <div data-bbox="646 506 1479 659" style="border: 1px solid green; padding: 5px;"><p>Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by the vulnerable URL and the input used to identify the vulnerability.</p></div> <ul style="list-style-type: none">• To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see Tenable Vulnerability Management Tables.• To view vulnerability details, click the row for that vulnerability. The Vulnerability Details page appears. <p>From the Vulnerabilities Details page, you can view plugin attachments for more information about each plugin.</p>
Notes tab	<p>For the scan job currently displayed, view the scan notes that Tenable Web App Scanning generates to provide context about your scan's success and efficiency.</p> <p>The Notes tab appears and displays scan notes only if the scanner identifies information during the scan that can help you configure your scan for more effective results.</p> <p>On this tab, you can:</p> <ul style="list-style-type: none">• View information about the scan notes:<ul style="list-style-type: none">• Severity – Metric used to quantify how significant the finding is for the scan's performance, displayed as Critical, High, Medium, Low, or Info. For information about scan notes vulnerability metrics, see Scan Notes Severity Details in Ten-



	<p>able Web App Scanning.</p> <ul style="list-style-type: none">• Scan Notes – Descriptive title for the scan note.• Description – Detailed information about the scan findings, along with troubleshooting advice and suggestions to improve your overall scan quality.
History tab	<p>View the scan history.</p> <p>This tab contains a table listing each time the scan has run. For the scan run currently displaying in the Scan Details page, Tenable Vulnerability Management adds the label Current to the run. By default, the latest scan run is labeled Current.</p> <div data-bbox="483 779 1479 890" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: Scan history is unavailable for imported scans and for configured scans that have not yet run.</p></div> <p>On this tab, you can:</p> <ul style="list-style-type: none">• View summary information about each time the scan was run:<ul style="list-style-type: none">• Created At – The start date and time the scan was created.• Start Time – The start date and time the scan was started by the scanner.• End Time – The end date and time the scan was completed.• Duration – The duration of the scan. <div data-bbox="646 1446 1479 1793" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: The Duration time span includes the time Tenable Web App Scanning takes to run the scan and process the results, as well as any time the scan spent in Pending status.</p><p>As a result, Duration time differs from the Overall Max Scan Time you specified in the Advanced settings, which applies only to the scan run time.</p></div>



- **Status** – The [status](#) of the scan.

- [Filter](#) the data displayed in the table.

- Sort or navigate to another page of the table. For more information, see [Tenable Vulnerability Management Tables](#).

- View details for a historical scan by clicking a scan job row in the table.

Tenable Web App Scanning marks the scan job you selected as **Current** and updates the **Scan Details** section to show data for the selected job.



Scan Notes Severity Details in Tenable Web App Scanning

Tenable Web App Scanning uses the severity ratings described below to categorize scan notes that appear in your scan results.

Rating	Description	Example
Critical	<p>Information explaining that the scan may have impacted the web application's availability or integrity.</p> <p>The scan note title appears in red.</p>	<p>Service Stopped Responding – The scanner aborted the scan after encountering too many consecutive request timeouts. The scan results may be incomplete, and you should verify that the target is not corrupted or unavailable.</p> <p>Tenable recommends that you investigate the repeated timeouts to determine why the target cannot support the requests the scanner sent. You may need to decrease performance configurations in the scan template.</p>
High	<p>Information explaining that the scan stopped unexpectedly before the scanner finished analyzing the web application targets. As a result, the scan did not sufficiently analyze the web application for vulnerabilities, and the user should troubleshoot and re-attempt the scan.</p> <p>The scan note title appears in yellow.</p>	<p>Scan Crashed – The scan crashed for an unexpected reason. As a result, the scan results are missing or incomplete.</p>
Medium	<p>Information explaining why scan results are missing or incomplete. The findings usually concern scans that could not be started due to configuration errors. The</p>	<p>Out of Scope URL – The scanner did not scan the target URL because it matches one of the scope exclusion criteria specified</p>



	<p>web application is not impacted.</p> <p>The scan note title appears in black and white.</p>	<p>in the scan template settings.</p>
Low	<p>Information explaining variations in scan duration. The findings do not impact the web application or scan results.</p> <p>The scan note title appears in green.</p>	<p>Target Response Has Been Truncated – The target scan results exceeded the Max Response Size specified in the scan configurations. As a result, the content is truncated, which could cause data collection and assessment errors.</p>
Info	<p>Information that does not impact the scan results, but that can help you configure your scan settings more efficiently.</p> <p>The scan note title appears in blue.</p>	<p>Authentication Detected – The scanner detected an HTTP server authentication or login form. You can configure your credentials to allow the scanner to access more pages.</p>



View Tenable Web App Scanning Scan Progress

Required Additional License: Tenable Web App Scanning

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

Required Scan Permissions: Can Control

When you launch a Tenable Web App Scanning scan, you can view the progress of the scan as it runs. Because scan progress information is based on historical data, Tenable Web App Scanning scan progress data appears only for historical scans.

To view scan progress for a Tenable Web App Scanning scan:

1. [Launch](#) an existing scan.

The scan status appears in the **Status** column.

2. After the status changes from **Pending** to **Running**, next to the scan status, view the following scan progress indicators:

Progress Indicator	Description
Percentage	Portion of the scan job that the scanner has already completed, displayed as a percentage of the total estimated scan time.
Estimate	Estimated time remaining for the scanner to complete the scan, displayed in minutes.
Overdue	Amount of extra time the scan job is taking compared to previous scan jobs. This indicator only appears if the scan is running longer than previous scans.
Progress bar	Visual indicator of the time remaining for the scanner to complete the scan. When the scan is complete or stops for any other reason (for example, if Tenable Vulnerability Management aborts the scan), the progress bar disappears.



Export Scan Results

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

Required Scan Permissions: Can View

You can export both imported scan results and results that Tenable Web App Scanning collects directly from scanners.

Tenable Web App Scanning retains individual scan results until the results are 15 months old.

Note: For archived scan results (that is, results older than 35 days), the export format is limited to .nessus and .csv files.

Note: When a scan is actively running, the **Export** button does not appear in the Tenable Vulnerability Management interface. Wait until the scan completes, then export the scan results.

To export results for an individual scan in the new interface:

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

The left navigation plane appears.

2. Do one of the following: In the left navigation plane, click **Scans**.
3. In the **Folders** section, click a folder to load the scans you want to view.

The scans table updates to display the scans in the folder you selected.



4. Do one of the following:

Location	Scope of Export
Scans table	<ol style="list-style-type: none">In the scans table, roll over the scan you want to export.Click the ⋮ button. A menu appears.Click ↗Export. The Export plane appears.
Scan Details	<ol style="list-style-type: none">In the scans table, click the scan you want to export.Next to the scan name, click ↗Export. The Export plane appears.

5. Select an export format:

Format	Description	Supported for Archived Scan Results
Tenable Web App Scanning		
HTML	A web-based .html file that contains the list of targets, scan results, and scan notes.	n/a
PDF	An Adobe .pdf file that contains the list of targets, scan results, and scan notes. <div style="border: 1px solid blue; padding: 5px;">Note: Tenable Vulnerability Management cannot export PDF files with more than 400,000 individual scan results.</div>	n/a
Nessus	A .nessus file in XML format that contains the list of targets, scan settings defined by the user, and scan results. Password credentials are stripped so they are not exported as plain text in the XML.	n/a



CSV	A .csv text file with only scan results.	n/a
JSON	A .json file that contains the list of targets, scan settings defined by the user, scan results, and scan notes. Password credentials are stripped so they are not exported as plain text in the .json file.	n/a
ZIP	Returns a .zip file containing debug information for the specified Tenable Web App Scanning scan. The ZIP file includes browser console logs, HTTP requests and responses, and Selenium information if applicable.	Yes

6. For Tenable Vulnerability Management scans, if you select the **PDF - Custom** or **HTML - Custom** formats:

- Retain the default **Data** setting (**Vulnerabilities** selected).
- Select either **Assets** or **Plugin** from the **Group By** list, depending on how you want to group the scan results in the export file.

7. Click **Export**.

Tenable Vulnerability Management generates the export file. Depending on your browser settings, your browser may automatically download the export file to your computer, or may prompt you to confirm the download before continuing.



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, its target, whether the scan is scheduled, and who has access to the scan.

You can configure **settings** when you create a scan or user-defined scan template and select any scan type. For more information, see [Scan Templates](#).

Tip: If you want to save your settings configurations and apply them to other scans, you can [create and configure a user-defined scan template](#).

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

- [General](#)
- [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
Target	none	Specifies the URL for the target you want to scan, as it appears on your Tenable Web App Scanning license. Regular expressions and wildcards are not allowed.	Yes



Setting	Default Value	Description	Required
		<p>Caution: When removing targets from a WAS scan (for example, going from two, or more, targets down to one target), the scan must be re-launched before any exports can be delivered.</p> <p>Note: If the URL you type in the Target box has a different FQDN host from the URL that appears on your license, and your scan runs successfully, the new URL you type counts as an additional asset on your license.</p> <p>Note: If you create a user-defined scan template, the target setting is not saved to the template. Type a target each time you create a new scan.</p>	
Folder	My Scans	Specifies the folder where the scan appears after being saved.	Yes
Scanner Type	Internal Scanner	Specifies whether a local, internal scanner or a cloud-managed scanner performs the scan, and determines whether the Scanner field lists local or cloud-managed scanners to choose from.	Yes
Scanner	varies	Specifies the scanner that performs the scan.	Yes

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. You must configure the schedule settings each time you create a new scan.



Setting	Default	Description
Schedule	off	<p>A toggle that specifies whether the scan is scheduled. By default, scans are not scheduled.</p> <p>When the Schedule toggle is disabled, the other schedule settings remain hidden.</p> <p>Click the toggle to enable the schedule and view the remaining Schedule settings.</p>
Frequency	Once	<p>Specifies how often the scan is launched.</p> <div data-bbox="609 676 1479 871" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: The frequency with which you scan your target 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">• Once: Schedule the scan at a specific time.• Daily: Schedule the scan to occur on a daily basis, at a specific time, up to 20 days.• Weekly: Schedule the scan to occur on a recurring basis, by time and day of week, up to 20 weeks.• Monthly: Schedule the scan to occur every 1-20 months, by:<ul style="list-style-type: none">• Day of Month: The scan repeats on a specific day of the month at the selected time.• Week of Month: The scan repeats monthly on the week you begin the scan. For example, if you select a start date of October 3rd, and that falls on the first week of the month, then the scan repeats the first week of each subsequent month at the selected time. <div data-bbox="688 1776 1479 1843" style="border: 1px solid #0070C0; padding: 5px;"><p>Note: If you schedule your scan to recur monthly and by</p></div>



Setting	Default	Description
		<p>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.</p> <ul style="list-style-type: none"> • Yearly: Schedule the scan to occur every year, by time and day, up to 20 years.
Starts	varies	<p>Specifies the exact date and time at which a scan launches.</p> <p>Note: If you schedule an excessive number of scans to run concurrently, you may exhaust the scanning capacity on Tenable Web App Scanning. If necessary, Tenable Web App Scanning staggers concurrent scans to ensure consistent scanning performance.</p> <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 <i>10/31/2019 and 22:00</i>.</p>
Timezone	varies	The time zone of the value set for Starts .

Notifications

The notification settings for a scan.

The following feature is not supported in Tenable Vulnerability Management Federal Risk and Authorization Management Program (FedRAMP) environments. For more information, see the [FedRAMP Product Offering](#).

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 Tenable Web App Scanning Scan Permissions](#).

Permission	Description
No Access	(Default) Users set to this permission cannot interact with the scan in any way.
Can View	Users set to this permission can view the results of the scan.
Can Control	In addition to the tasks allowed by Can View , users with this permission can launch and stop a scan. They cannot view or edit the scan configuration or delete the scan.
Can Configure	In addition to the tasks allowed by Can Control , users with this permission can view the scan configuration and modify any setting for the scan except scan ownership. They can also delete the scan.

Data Sharing

Setting	Default Value	Description
Scan Results	Show in dashboard	Specifies whether the results of the scan should be kept private or should appear on users' dashboards. When set to Keep private , users must access the scan directly to view the results.



Scope Settings in Tenable Web App Scanning Scans

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

You can configure **Scope** settings when you create a scan or user-defined scan template and select the **Overview** or **Scan** template type. For more information, see [Scan Templates](#).

Tip: If you want to save your settings configurations and apply them to other scans, you can [create and configure a user-defined scan template](#).

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

- [Crawl Scripts](#)
- [OpenAPI \(Swagger\) Specification](#)
- [Scan Inclusion](#)
- [Scan Exclusion](#)

Crawl Scripts

Selenium scripts you want to add to your scan to enable the scanner to analyze pages with complex access logic.

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.

OpenAPI (Swagger) Specification

The specification file for the RESTful API that you want to scan. The file should be OpenAPI Specification (v2 or v3) compliant and represented in either JSON or YAML format.

Setting	Description
Add File	Hyperlink that allows you to add one or more OpenAPI (v2 or v3) specification



files. The specification files should be represented in either JSON or YAML format.

Scan Inclusion

The URLs you want the scanner to include, along with how you want the scanner to crawl them.

Setting	Default	Description
List of URLs	none	<p>A list of any URLs you want to ensure the scanner analyzes, in addition to the target URL you specified in the Basic settings.</p> <p>Type each URL as an absolute URL.</p> <p>Type each URL on a separate line.</p> <div style="border: 1px solid #0070C0; padding: 5px;"><p>Note: All URLs should have the same domain and wildcards are not allowed.</p></div>
Specify how the scanner handles URLs found during the application crawl	Crawl all URLs detected	<p>Specifies the limits you want the scanner to adhere to as it crawls URLs.</p> <p>Select one of the following:</p> <ul style="list-style-type: none">• Crawl all URLs detected – The scanner crawls all URLs and child paths it detects on the target URL's domain host.• Limit crawling to specified URLs and child paths – The scanner crawls only the target URL and child paths.• Limit crawling to specified URLs – The scanner crawls the target URL only. It does not crawl child paths for the target URL.

Scan Exclusion



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

Setting	Default Value	Description
Regex for Excluded URLs	logout	<p>Text box option in which you can specify a regex pattern that the scanner can look for in URLs to exclude from the scan. You can specify multiple regex patterns separated by new lines.</p> <p>Note: The regex values should be values contained within the URL to be excluded. For example, in the URL <code>http://www.example.com/blog/today.htm</code>, valid regex values would be <code>blog</code> or <code>today</code> (not the full URL). Additionally, regex values are case-sensitive.</p>
File Extensions to Exclude	js, css, png, jpeg, gif, pdf, csv, svn-base, svg, jpg, ico, woff, woff2, exe, msi, zip	<p>Text box option in which you can specify the file types you want the scanner to exclude from the scan.</p> <p>Separate each file type with a comma.</p> <p>Note: Excluding certain file extensions may be useful as the scanner may not realize something is not a web page and attempt to scan it, as if it actually is a web page. This wastes time and slows down the scan. You can add additional file extensions if you know you use them, and are certain they do not need to be scanned. For example, Tenable includes different image extensions by default: <code>.png</code>, <code>.jpeg</code>, etc.</p>
Decompose Paths	not selected	<p>Check box option that allows you to specify whether you want the scanner to break down each URL identified during the scan into additional URLs, based on directory path level.</p> <p>For example, if you specify <code>www.example.com/dir1/dir2/dir3</code> as your target and select Decompose Paths, the scanner analyzes each of the following as separate URLs of the target:</p> <ul style="list-style-type: none">• <code>www.example.com/dir1/dir2/dir3</code>• <code>www.example.com/dir1/dir2</code>



Setting	Default Value	Description
		<ul style="list-style-type: none">• www.example.com/dir1 <p>Select this option to increase the surface coverage of your web application scan.</p> <p>Note: Scans that include path decomposition can take longer to complete than scans that do not.</p>
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> <p>Note: Scans that include binaries can take longer to complete, because the scanner cannot read the binary responses.</p>

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.



Assessment Settings in Tenable Web App Scanning Scans

Assessment settings specify which web application elements you want the scanner to audit as it crawls your URLs. You can configure **Assessment** settings when you [create](#) a scan or [user-defined](#) scan template. For more information, see [Scan Templates](#).

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

- [Scan Type](#)
- [Common and Backup Pages](#)
- [Credentials Bruteforcing](#)
- [Elements to Audit](#)
- [Optional](#)
- [DOM Element Exclusion](#)

Scan Type

These settings specify the intensity of the assessment you want the scanner to perform.

Setting	Default Value	Description	Required
Assessment	Recommended	<p>Drop-down box that allows you to choose from the following options to specify the scan type you want the scanner to perform.</p> <ul style="list-style-type: none">• Recommended – The scanner audits elements based on Tenable's recommendations.• None – The scanner does not audit any elements.• Quick – The scanner audits the most common elements listed.	Yes



Setting	Default Value	Description	Required
		<ul style="list-style-type: none">• Extensive – The scanner audits all the elements listed.• Custom – The scanner audits only the elements you select. <p>Note: If you select Recommended, Quick, or Extensive and then make changes to the settings in this section, the Scan Type setting automatically changes to Custom.</p>	

Common and Backup Pages

Setting	Default Value	Description
Detection Level	Most Detected Pages	<p>Drop-down box that allows you to choose from the following options to specify which pages you want the scanner to crawl.</p> <ul style="list-style-type: none">• Most Detected Pages - The scanner crawls only the most detected pages.• Extended Dictionary - The scanner tests more path variations for detecting hidden pages, increasing the overall scan duration. <p>Note: The Detection Level drop-down box is available only when you select Custom in the Scan Type settings.</p>

Credentials Bruteforcing

The **Credentials Bruteforcing** setting is available only for the **Scan** template.



Setting	Default	Description
Credentials Bruteforcing	Disabled	<p>When enabled, any plugins that perform bruteforcing included in the Plugins settings run.</p> <p>When disabled, bruteforcing plugins do not run, even if they are included in the Plugins settings.</p> <div style="border: 1px solid #0070C0; padding: 5px;"><p>Note: The Credentials Bruteforcing setting is available only when you select Custom in the Scan Type settings.</p></div>

Elements to Audit

These settings specify the elements in your web application that you want the scanner to analyze for vulnerabilities.

Setting	Scanner Action
Cookies	Checks for cookie-based vulnerabilities.
Headers	Checks for header vulnerabilities and insecure configurations (for example, missing X-Frame-Options).
Forms	Checks for form-based vulnerabilities.
Links and Query String Parameters	Checks for vulnerabilities in links and their parameters.
Parameter Names	Performs extensive fuzzing of parameter names.
Parameter Values	Performs extensive fuzzing of parameter values.
Path Parameters	<p>Assesses path parameters. Path parameters are used in URL rewrite to identify the object of the action within the URL. For example, <code>scanId</code> is a path parameter for the below URL, used to identify the scan to display results:</p> <p><code>http://example.com/scan/scanId/results</code></p>
JSON Elements / Request Body	Audits JSON request data.



Setting	Scanner Action
(JSON)	
XML Elements / Request Body (XML)	Audits XML request data.
UI Forms	Checks input and button groups associated with JavaScript code.
UI Inputs	Checks orphan input elements against associated document object model (DOM) events.

Optional

Setting	Default	Description
URL for Remote Inclusion	None	<p>Specifies a file on a remote host that Tenable Web App Scanning can use to test for a Remote File Inclusion (RFI) vulnerability.</p> <p>If the scanner cannot reach the internet, the scanner uses this internally-hosted file for more accurate RFI testing.</p> <div style="border: 1px solid #0070C0; padding: 5px;"><p>Note: If you do not specify a file, Tenable Web App Scanning uses a safe, Tenable-hosted file for RFI testing.</p></div>

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	<p>Excludes elements based on text contents.</p> <p>For example, if you want to prevent the scanner from clicking a logout button named Log Out, you could match the text Log Out.</p>
CSS Attribute	None	<p>Excludes elements based on a CSS attribute key-value pair.</p> <p>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.</p>



Report Settings in Tenable Web App Scanning Scans

Report settings specify extra items to include in the scan report. For example, scan reports for Tenable PCI ASV scans require load balancer usage details if applicable.

You can configure **Report** settings when you [create](#) a scan or [user-defined](#) scan template using the Tenable-provided scan template, **PCI**. For more information, see [Scan Templates](#).

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

- [\(Tenable PCI ASV 6.1\) Load Balancers Usage](#)

(Tenable PCI ASV 6.1) Load Balancers Usage

This setting specifies load balancer usage to include in the scan report.

Setting	Default Value	Description	Required
(Tenable PCI ASV 6.1) Load Balancers Usage	None	Text box that allows you to enter a list of load balancers and their configuration as required for Tenable PCI ASV if applicable.	No



Advanced Settings in Tenable Web App Scanning Scans

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

You can configure **Advanced** settings when you [create](#) a scan or [user-defined](#) scan template using any Tenable-provided scan template. However, the **Overview** and **Scan** template types have more configurable **Advanced** settings than the **Config Audit** and **SSL TLS** template types. For more information, see [Scan Templates](#).

The **Advanced Settings** options allow you to control the efficiency and performance of the scan.

- [General](#)
- [HTTP Settings](#)
- [Screen Settings](#)
- [Limits](#)
- [Selenium Settings](#)
- [Performance Settings](#)
- [Session Settings](#)

General

You can configure **General** options in scans and user-defined scan templates based on the **Overview** and **Scan** templates only.

Setting	Default	Description
Target Scan Max Time (HH:MM:SS)	08:00:00	Specifies the maximum duration the scanner runs a scan job runs before stopping, displayed in hours, minutes, and seconds. Note: The maximum duration you can set is 99:59:59 (hours: minutes: seconds).
Maximum Queue Time (HH:MM:SS)	08:00:00	Specifies the maximum duration the scan remains in the Queued state, displayed in hours, minutes, and seconds.



		Note: The maximum duration you can set is 48:00:00 (hours: minutes: seconds).
Enable Debug logging for this scan	disabled	Specifies whether the scanner attaches available debug logs from plugins to the vulnerability output of this scan.
Debug Flags	disabled	(Only visible when you enable the Enable Debug logging for this scan feature). Allows you to specify key and value pairs, provided by support, for debugging.

HTTP Settings

These settings specify the user-agent you want the scanner to identify and the HTTP response headers you want the scanner to include in requests to the web application.

You can configure **Crawl Settings** options in scans and user-defined scan templates based on any Tenable-provided scan template.

Setting	Default	Description
Use a different User Agent to identify scanner	disabled	Specifies whether you want the scanner to use a user-agent header other than Chrome when sending an HTTP request.
User Agent	Chrome's user-agent	<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 Use a different User Agent to identify scanner 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>



		<p>Note: The current Tenable Web App Scanning user-agent header is: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90 Safari/537.36</p> <p>Note: Not all requests from scanner are guaranteed to have the User Agent sent.</p>
Add Scan ID HTTP Header	disabled	Specifies whether the scanner adds an additional X-Tenable-Was-Scan-Id header (set with the scan ID) to all HTTP requests sent to the target, which allows you to identify scan jobs in web server logs and modify your scan configurations to secure your sites.
Custom Headers	none	<p>Specifies the custom headers you want to inject into each 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> <p>Note: If you enter a custom User-Agent header, that value overrides the value entered in the User Agent setting box.</p>

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	Specifies the maximum number of sub-directories the scanner crawls. For example, if your target is <code>www.example.com</code> , and you want the scanner to crawl <code>www.example.com/users/myname</code> , type <code>2</code> 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 Direct 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 in Tenable Web App Scanning Scans](#).

You can configure **Selenium Settings** options in scans and user-defined scan templates based on the **Overview** and **Scan** templates only.



Setting	Default	Description
Page Rendering Delay	30000	Specifies the time, in milliseconds, the scanner waits for the page to render.
Command Execution Delay	500	Specifies the time, in milliseconds, the scanner waits after processing a command before proceeding to the next command.
Script Completion Delay	5000	Specifies the time, in milliseconds, the scanner waits for all commands to render new content to finish processing.

Performance Settings

Setting	Default	Description
Max Number of Concurrent HTTP Connections	10	Specifies the maximum number of established HTTP sessions allowed for a single host.
Max Number of HTTP Requests Per Second	25	Specifies the maximum number of HTTP requests allowed for a single host for the duration of the scan.
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.



Credentials in Tenable Web App Scanning Scans

Note: The topics in this section describe credentials in the new interface only. If you activate the new interface, you can view a snapshot of historical credentials that you configured in the classic interface, but you cannot modify those credentials.

For information about credentials in the classic interface, see [Credentials \(Classic Interface\)](#).

In Tenable Web App Scanning scans, you can configure credentials settings that allow Tenable Web App Scanning to perform an authenticated scan on a web application. Credentialed scans can perform a wider variety of checks than non-credentialed scans, which can result in more accurate scan results.

Scans in Tenable Web App Scanning use [managed credentials](#). Managed credentials allow you to store credential settings centrally in a credential manager. You can then add those credential settings to multiple scan configurations instead of configuring credential settings for each individual scan.

Tenable Web App Scanning scans support credentials in the following authentication types:

- [HTTP Server Authentication](#)
- [Web Application Authentication](#)
- [Client Certificate Authentication](#)

Tip: If want to scan an API with the API scan template, and your API requires keys or a token for authentication, you can add the expected custom headers in the [Advanced](#) settings in the **HTTP Settings** section.

You can configure credentials settings in Tenable Web App Scanning scans using the following methods:

Credentials Category	Authentication Type	Configuration Method
HTTP Server Authentication	-	Use the Tenable Web App Scanning user interface to manually configure credentials settings in scans .



Web Application Authentication	Login Form	<p>Do one of the following:</p> <ul style="list-style-type: none">Use the Selenium Integrated Development Environment (IDE) extension in Chrome to record credentials, then manually add the credentials to scans via the Tenable Web App Scanning user interface. <div data-bbox="846 709 1479 863" style="border: 1px solid blue; padding: 5px;"><p>Note: For information about the Selenium IDE extension in Chrome, see the Google Chrome documentation.</p></div> <ul style="list-style-type: none">Use the Tenable Web App Scanning Chrome Extension to record credentials and automatically add the credentials to your scan configurations. <div data-bbox="764 1115 1479 1268" style="border: 1px solid green; padding: 5px;"><p>Tip: For information about Selenium scripts you can use with Tenable Web App Scanning, see Tenable Web App Scanning Selenium Commands.</p></div>
	Cookie Authentication	
	Selenium Authentication	
	API Key	
	Bearer Authentication	Use the Tenable Web App Scanning user interface to manually configure credentials settings in scans .
Client Certificate Authentication	-	Use the Tenable Web App Scanning user interface to manually configure credentials settings in scans .



Configure Credentials Settings in a Tenable Web App Scanning Scan

Required Additional License: Tenable Web App Scanning

Required Tenable Web App Scanning User Role: WAS Scan Manager or Administrator

Before you begin:

- (Cookie authentication) Determine the cookie authentication credentials for the web application you want to scan.
- (Selenium authentication) In the [Chrome Web Store](#), download the Selenium IDE extension, do one of the following:
 - To configure credentials using the Selenium IDE extension, download the Selenium IDE extension.
 - To configure credentials via the Tenable Web App Scanning Chrome Extension, download the Tenable Web App Scanning Chrome Extension.

To configure credentials settings in a Tenable Web App Scanning scan:

1. [Create](#) or [edit](#) a scan.
2. Click **Credentials**.

The credentials details appear.

3. Next to **Add Credentials**, click the **+** button.


The **Select Credential Type** plane appears.

4. Do one of the following:

- Add existing credentials.

The **Managed Credentials** section of the **Select Credential Type** plane contains any credentials where you have **Can Use** or **Can Edit** permissions.



- a. (Optional) Search for a managed credential in the list by typing your search criteria in the text box and clicking the  button.
- b. In the **Managed Credentials** section, click each managed credential you want to add.

The **Select Credential Type** plane remains open.

- c. To close the **Select Credential Type** plane, click the **X** button in the upper-right corner of the plane.

- Create new credentials.

- a. In the **Web Application Authentication** section, click the credentials type you want to create:

- **HTTP Server Application**
- **Web Application Authentication**

The settings plane for that credential type appears.

- b. In the first text box, type a name for the credentials.
- c. (Optional) In the second text box, type a description for the credentials.
- d. Configure the settings for the credentials type:

- [HTTP Server Application](#)
- [Web Application Authentication](#)

5. [Add user permissions](#).

6. Click **Save** to save the credentials changes.

Tenable Web App Scanning closes the settings plane and adds the credentials to the credentials table for the scan.

If you created new credentials, Tenable Web App Scanning adds the credentials to the credential manager.

7. Click **Save** to save the scan changes.



Configure Selenium Credentials Settings Automatically

Required Additional License: Tenable Web App Scanning

You can use the Tenable Web App Scanning Chrome Extension to record Selenium credentials and add those credentials automatically to new or existing scans.

Note: The Tenable Web App Scanning Chrome Extension updates only Selenium credentials settings in web application scans. You must [configure](#) the other scan options via the Tenable Web App Scanning Chrome Extension interface.

Before you begin:


- Download the Tenable Web App Scanning Chrome Extension from the [Chrome Web Store](#).
- Log in to Tenable Vulnerability Management, as described in [Log in to Tenable Vulnerability Management](#).

To record selenium credentials via the Tenable Web App Scanning Chrome Extension:

1. In the upper-right corner of your browser, click the  Tenable Vulnerability Management logo.

The Tenable Web App Scanning Chrome Extension **Create a Scan** window appears.

2. Do one of the following:

Task	Action
Record and add Selenium credentials to an existing scan	<ul style="list-style-type: none">• Click Add to Existing Scan. <p>The Add to Existing Scan window appears, displaying a list of your existing scans.</p> <ul style="list-style-type: none">• In the search box, type the name of the scan you want to add Selenium credentials to.• Click the  button. <p>The Tenable Web App Scanning Chrome Extension filters the list by the name you typed.</p>



	<ul style="list-style-type: none">• Click the scan you want to add Selenium credentials to.
Record and add Selenium credentials to a new scan	<ul style="list-style-type: none">• Click Create New Scan. <p>The New Scan window appears.</p> <ul style="list-style-type: none">• In the Name box, type a name for your scan.• In the URL box, type the target in URL format for the web application you want to scan.

3. Click **Next**.

The extension opens to the link you provided as your scan target.

4. Click **Record**.

The Tenable Web App Scanning Chrome Extension begins recording your session.

A message appears to indicate recording has begun.

5. Perform the log in sequence you use to authenticate in to your web application.

6. After you successful authenticate in to the system, highlight a section of text on the web page that appears only upon successful authentication (for example, **Welcome, [your username]!**).

7. In the lower-right corner, click **Done**.

8. (Optional) To play back your recorded login sequence, click **Play**.

9. After you have successfully recorded your authentication login sequence, click **Save**.

Tenable Web App Scanning Chrome Extension saves and imports your credentials to the scan.

What to do next:

- If you used the Tenable Web App Scanning Chrome Extension to create a new scan, you must [configure](#) the other scan options in the Tenable Web App Scanning Chrome Extension interface.



Tenable Web App Scanning Selenium Commands

Selenium commands in Tenable Web App Scanning are used to record authentication and crawling scripts so that users can tell the scanner exactly what to do in certain scenarios. You can run these commands in the Selenium IDE Extension or in the Tenable Web App Scanning Chrome Extension, both available for download in the [Chrome Web Store](#).

Support for Selenium commands in Tenable Web App Scanning is detailed below:

Commands Supported	Commands Not Supported
<ul style="list-style-type: none">• addSelection• answerOnNextPrompt• assert• assertAlert• assertChecked• assertConfirmation• assertEditable• assertElementNotPresent• assertElementPresent• assertNotChecked• assertNotEditable• assertNotSelectedValue• assertNotText• assertPrompt• assertSelectedLabel• assertSelectedValue• assertText• assertTitle	<ul style="list-style-type: none">• close• debugger• do• else• else if• end• execute async script• execute script• for each• if• repeat if• run• select window• store• store attribute• store json• store text• store title



- assertValue
- check
- chooseCancelOnNextConfirmation
- chooseCancelOnNextPrompt
- chooseOkOnNextConfirmation
- click
- clickAt
- doubleClick
- doubleClickAt
- echo
- editContent
- mouseDown
- mouseDownAt
- mouseMoveAt
- mouseOut
- mouseOver
- mouseUp
- mouseUpAt
- open
- pause
- removeSelection
- runScript
- select
- selectFrame
- store value
- store window handle
- store xpath count
- times
- while



- sendKeys

Note: In addition to arbitrary text, the sendKeys command only supports the following escape sequences:

- `${KEY_ENTER}`
- `${KEY_DELETE}`
- `${KEY_BACKSPACE}`

- setSpeed
- setWindowSize
- submit
- type
- uncheck
- verify
- verifyChecked
- verifyEditable
- verifyElementNotPresent
- verifyElementPresent
- verifyNotChecked
- verifyNotEditable
- verifyNotSelectedValue
- verifyNotText
- verifySelectedLabel
- verifySelectedValue
- verifyText
- verifyTitle



- `verifyValue`
- `waitForElementEditable`
- `waitForElementNotEditable`
- `waitForElementNotPresent`
- `waitForElementNotVisible`
- `waitForElementPresent`
- `waitForElementVisible`
- `webdriverAnswerOnNextPrompt`
- `webdriverAnswerOnVisiblePrompt`
- `webdriverChooseCancelOnNextConfirmation`
- `webdriverChooseCancelOnNextPrompt`
- `webdriverChooseCancelOnVisibleConfirmation`
- `webdriverChooseCancelOnVisiblePrompt`
- `webdriverChooseOkOnNextConfirmation`
- `webdriverChooseOkOnVisibleConfirmation`



HTTP Server Authentication Settings in Tenable Web App Scanning Scans

In a Tenable Web App Scanning scan, you can configure the following settings for HTTP server-based authentication credentials.

Option	Action
Username	Type the username Tenable Web App Scanning uses to authenticate to the HTTP-based server.
Password	Type the password Tenable Web App Scanning uses to authenticate to the HTTP-based server.
Authentication Type	In the drop-down list, select one of the following authentication types: <ul style="list-style-type: none">• Basic/Digest• NTLM• Kerberos
Kerberos Domain	(Required when enabling the Kerberos Authentication Type) The realm to which Kerberos Target Authentication belongs, if applicable.
Key Distribution Center (KDC)	(Required when enabling the Kerberos Authentication Type) This host supplies the session tickets for the user.

Note: Tenable Vulnerability Management does not support multiple HTTP authentication types for a single target.



Web Application Authentication

In a Tenable Web App Scanning scan, you can configure one of the following types of **Web Application Authentication** credentials:

- [Login Form Authentication](#)
- [Cookie Authentication](#)
- [Selenium Authentication](#)
- [API Key Authentication](#)
- [Bearer Authentication](#)

Login Form Authentication

Option	Action						
Authentication Method	In the drop-down box, select Login Form .						
Login Page	Type the URL of the login page for the web application you want to scan.						
Credentials	<p>For each field in the target's login form (that is, username, password, and domain, etc.) complete a credential entry as follows:</p> <ol style="list-style-type: none">In the left-hand text box, type the value of the login field's name or id HTML DOM attribute.In the right-hand text box in the row, type the literal value to insert in that text field at login. <p>A typical configuration example:</p> <div data-bbox="451 1587 1045 1713"><table border="1"><thead><tr><th colspan="2">CREDENTIALS</th></tr></thead><tbody><tr><td>username-1</td><td>wasScannerUsername</td></tr><tr><td>password-1</td><td>myWasPassword!</td></tr></tbody></table></div> <p>Tip: To see a text field's name or id HTML DOM attribute, right-click on the text field and select "Inspect" in either your Firefox or Chrome browser.</p>	CREDENTIALS		username-1	wasScannerUsername	password-1	myWasPassword!
CREDENTIALS							
username-1	wasScannerUsername						
password-1	myWasPassword!						



	<p>Tip: If you perform an unauthenticated Overview scan, plugin 98033 (Login Form Detected) may automatically detect and display the required login boxes in the plugin output.</p>
Pattern to Verify Successful Authentication	Type a word, phrase, or regular expression that appears on the website only if the authentication is successful (for example, Welcome , <i>your username!</i>). Note that leading slashes will be escaped and <code>.*</code> is not required at the beginning or end of the pattern.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, Hello , <i>your username.</i>). Note that leading slashes will be escaped and <code>.*</code> is not required at the beginning or end of the pattern.

Cookie Authentication

Option	Action
Authentication Method	In the drop-down box, select Cookie Authentication .
Session Cookies	Do the following: <ul style="list-style-type: none">a. In the first text box, type the name of the cookie authentication credentials.b. In the second text box, type the value of the cookie authentication credentials.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, Hello , <i>your username.</i>). Note that leading slashes will be escaped and <code>.*</code> is not required at the beginning or end of the pattern.



Selenium Authentication

Option	Action
Authentication Method	Select Selenium Authentication .
Selenium Script (.side)	Do the following: <ol style="list-style-type: none">In the Selenium IDE extension, record your authentication credentials in the Selenium IDE extension.Click Add File. The file manager for your operating system appears.Navigate to and select your Selenium credentials <code>.side</code> file. Tenable Web App Scanning imports the credentials file.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, Hello, your username.). Note that leading slashes will be escaped and <code>.*</code> is not required at the beginning or end of the pattern.

API Key Authentication

Option	Action
Authentication Method	Select API Key .
Headers	Do the following: <ol style="list-style-type: none">In the first text box, type the name of the HTTP header.In the second text box, type the value of the HTTP header.



	c. (Optional) Add additional headers by clicking the + button.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, Hello, your username.). Note that leading slashes will be escaped and <code>.*</code> is not required at the beginning or end of the pattern.

Bearer Authentication

Option	Action
Authentication Method	Select Bearer Authentication .
Bearer Token	Type the value of the bearer token. Note: Bearer Token is a part of OAuth. Tenable Web App Scanning supports OAuth in cases where it is a part of OpenIDConnect and recordable via a selenium script. Implementations of OAuth that are not a part of OpenIDConnect are supported only where the token is dynamic, or you craft a special static (non-dynamic) token for authentication purposes.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, Hello, your username.). Note that leading slashes will be escaped and <code>.*</code> is not required at the beginning or end of the pattern.



Client Certificate Authentication

In a Tenable Web App Scanning scan, you can configure **Client Certificate Authentication** credentials.

Option	Action
Client Certificate	The file that contains the PEM-formatted certificate used to communicate with the host.
Client Certificate Private Key	The file that contains the PEM-formatted private key for the client certificate.
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
Page to Verify Successful Authentication	Type the URL that Tenable Web App Scanning can access to validate the authenticated session.
Pattern to Verify Successful Authentication	Type a word, phrase, or regular expression that appears on the website only if the authentication is successful (for example, Welcome, your username!). Leading slashes will be escaped and .* is not required at the beginning or end of the pattern.



Plugin Settings in Tenable Web App Scanning Scans

Required Tenable Web App Scanning User Role: WAS Scan Manager or Administrator

Configure **Plugin** settings to specify the plugins and plugin families you want the scanner to use as it scans your web application.

When you create and launch a scan, Tenable Web App Scanning uses plugins in various plugin families, each designed to identify certain types of finding or vulnerabilities, to analyze your web application. Tenable Web App Scanning uses the 98000-98999 and 112290-117290 plugin ID ranges for scanning. For more information about Tenable Web App Scanning plugin families, see the [Tenable Web App Scanning Plugin Families](#) site.

Note: Tenable Web App Scanning displays only the first detected 25 instances of an individual plugin per scan in your scan results. If you see 25 instances of a single plugin in your scan results, Tenable recommends taking remediation steps to address the corresponding vulnerability and then rescanning your target.

You can configure **Plugin** settings when you create a scan or user-defined scan template and select the **Overview** or **Scan** template type. However, the **Scan** template type has more plugin families to view and configure. For more information, see [Scan Templates](#).

Tip: If you want to save your settings configurations and apply them to other scans, you can [create and configure a user-defined scan template](#).

The plugins settings contains the following sections:

- [All enabled](#)
- [Plugins table](#)

All Enabled

A toggle you can click to enable or disable all plugins simultaneously.

Plugins Table



Column	Description	Actions
Name	Specifies the plugin family to which the grouped plugins belong.	<ul style="list-style-type: none">• View the name of each plugin family.• Select the column to sort the alphabetically table by family name.
Total	Specifies the number of plugins in the plugin family.	<ul style="list-style-type: none">• View the number of plugins in the family.• Select the column to sort the table by number of plugins in each family.
Status	Toggle that allows you to specify if you want the scanner to use the plugins in the plugin family to analyze your target.	<ul style="list-style-type: none">• Click the Status toggle to disable the plugins in the plugin family.• (Optional) To enable a disabled plugin family, click the Status toggle.

In the plugins table, you can view details about or disable individual plugins.

To view details about individual plugins:

1. In the table, click the row for the family that contains a plugin you want to view.

A plugin family details plane appears, displaying the name, ID, and status for each plugin in the family in a paginated list.

2. (Optional) To locate a specific plugin, in the **Search** box, type the name or ID.
3. Click the plugin for which you want to view details.

To disable individual plugins:



1. In the table, click the row for the family that contains the plugin you want to disable.

A plugin family details plane appears, displaying the name, ID, and status for each plugin in the family in a paginated list.

2. (Optional) To locate a specific plugin, in the **Search** box, type the name or ID.
3. In the **Status** column, select the check box next to the plugin you want to disable.
4. (Optional) To enable a disabled plugin, select the check box.
5. Click **Save**.

The details plane disappears.

Tenable Vulnerability Management updates your plugin selections.



Tenable-Provided Tenable Web App Scanning Templates

Tenable Web App Scanning provides scanner templates for specific scanning purposes.

Tenable Web App Scanning provides the following scanner templates.

Template	Description
API	<p>A scan that checks an API for vulnerabilities. This scan analyzes RESTful APIs described via an OpenAPI (Swagger) specification file.</p> <p>Tip: If the API you want to scan requires keys or a token for authentication, you can add the expected custom headers in the Advanced settings in the HTTP Settings section.</p> <p>Note: The API scan template is available as a public beta. Its functionality is subject to change as ongoing improvements are made throughout the beta period.</p> <p>Note: API scans support only one target at a time.</p>
Config Audit	<p>A high-level scan that analyzes HTTP security headers and other externally facing configurations on a web application to determine if the application is compliant with common security industry standards.</p> <p>If you create a scan using the Config Audit scan template, Tenable Web App Scanning analyzes your web application only for plugins related to security industry standards compliance.</p>
Log4Shell	<p>Detects the Log4Shell vulnerability (CVE-2021-44228) in Apache Log4j via local checks.</p>
Overview	<p>A high-level preliminary scan that determines which URLs in a web application Tenable Web App Scanning scans by default.</p> <p>The Overview scan template does not analyze the web application for active vulnerabilities. Therefore, this scan template does not offer as many plugin family options as the Scan template.</p> <p>Note: This scan template is equivalent to the Web App Overview template in the classic Tenable Web App Scanning interface.</p>



PCI	<p>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.)</p>
Quick Scan	<p>A high-level scan similar to the Config Audit scan template that analyzes HTTP security headers and other externally facing configurations on a web application to determine if the application is compliant with common security industry standards. Does not include scheduling.</p> <p>If you create a scan using the Quick Scan scan template, Tenable Web App Scanning analyzes your web application only for plugins related to security industry standards compliance.</p>
Scan	<p>A comprehensive scan that assesses web applications for a wide range of vulnerabilities.</p> <p>The Scan template provides plugin family options for all active web application plugins.</p> <p>If you create a scan using the Scan template, Tenable Web App Scanning analyzes your web application for all plugins that the scanner checks for when you create a scan using the Config Audit, Overview, or SSL TLS templates, as well as additional plugins to detect specific vulnerabilities.</p> <p>A scan run with this scan template provides a more detailed assessment of a web application and take longer to complete than other Tenable Web App Scanning scans.</p> <div style="border: 1px solid blue; padding: 5px;"><p>Note: This scan template is equivalent to the Web App Scan template in the classic Tenable Web App Scanning interface.</p></div>
SSL TLS	<p>A scan to determine if a web application uses SSL/TLS public-key encryption and, if so, how the encryption is configured.</p> <p>When you create a scan using the SSL TLS template, Tenable Web App Scanning analyzes your web application only for plugins related to SSL/TLS implementation. The scanner does not crawl URLs or assess individual pages for vulnerabilities.</p>



The settings you can configure in a scan or in a user-defined scan template depend on the Tenable-provided scan template type you use to create your scan.



User-Defined Templates

Required Template Permissions: Owner

Tenable provides a variety of scan templates for specific scanning purposes. If you want to customize a Tenable-provided scan template and share it with other users, you can create a user-defined scan template.

You can create, edit, copy, export, or delete user-defined Tenable Web App Scanning templates from the **Scans** page. You can also export Tenable Web App Scanning scan templates.

Click a template to view or [edit](#) its settings and parameters, or use the following procedures to manage your user-defined templates:

Create a user-defined template

You can create user-defined scan templates to save and share custom scan settings with other Tenable Web App Scanning users.

When you define a scan template, Tenable Vulnerability Management assigns you owner permissions for the scan template. You can share the scan template by assigning [template permissions](#) to other users, but only you can [delete](#) the scan template.

To create a user-defined scan template:

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

The left navigation plane appears.

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

The **My Scans** page appears.

3. In the upper-right corner of the page, click the  **Scan Templates**.

The **Scan Templates** page appears.

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

The **Select a Template** page appears.



5. Click the tile for the template you want to use as the base for your user-defined scan template.
The **Create a Template** page appears.
6. Configure the scan.

Tab	Action
Settings	Configure the settings available in the scan template. For more information, see Basic Settings in Tenable Web App Scanning Scans .
Scope	Specify the URLs and file types that you want to include in or exclude from your scan. For more information, see Scope Settings in Tenable Web App Scanning Scans .
Assessment	Specify how a scan identifies vulnerabilities and what vulnerabilities the scan identifies. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications. For more information, see Assessment Settings in Tenable Web App Scanning Scans .
Advanced	Specify advanced controls for scan efficiency.
Credentials	Specify credentials you want Tenable Vulnerability Management to use to perform a credentialed scan.
Plugins	Select security checks by plugin family or individual plugin .

The scan template table updates based on your selection.

Edit a user-defined template

Required Template Permissions: Can Configure

To edit a user-defined scan template:

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

The left navigation plane appears.



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



The **My Scans** page appears.

3. In the upper-right corner of the page, click the  **Scan Templates**.

The **Scan Templates** page appears.

4. In the scan templates table, In the row of the scan you want to edit, click the  button.
5. Select  Edit.
6. Configure the scan template options.

Tab	Action
Settings	Configure the settings available in the scan template. For more information, see Basic Settings in Tenable Web App Scanning Scans .
Scope	Specify the URLs and file types that you want to include in or exclude from your scan. For more information, see Scope Settings in Tenable Web App Scanning Scans .
Assessment	Specify how a scan identifies vulnerabilities and what vulnerabilities the scan identifies. This includes identifying malware, assessing the vulnerability of a system to brute force attacks, and the susceptibility of web applications. For more information, see Assessment Settings in Tenable Web App Scanning Scans .
Advanced	Specify advanced controls for scan efficiency.
Credentials	Specify credentials you want Tenable Vulnerability Management to use to perform a credentialed scan.
Plugins	Select security checks by plugin family or individual plugin .

7. Click **Save**.

Tenable Web App Scanning saves the user-defined scan template and adds it to the list of templates on the **Scan Templates** page.

Copy a user-defined template



When you copy a user-defined scan template, Tenable Web App Scanning assigns you owner permissions for the copy. You can share the copy by assigning [template permissions](#) to other users, but only you can [delete](#) the copied scan template.

To copy a user-defined scan template:

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

The left navigation plane appears.

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

The **My Scans** page appears.

3. In the upper-right corner of the page, click the  **Scan Templates**.

The **Scan Templates** page appears.

4. In the scan templates table, In the row of the scan you want to edit, click the ⋮ button.

A menu appears.

5. In the menu, click the  button.

A **Template copied** message appears. Tenable Web App Scanning creates a copy of the scan template with *Copy of* prepended to the name and assigns you owner permissions for the copy. The copy appears in the scan templates table.

Delete a user-defined template

If you delete a user-defined scan template, Tenable Vulnerability Management deletes it from all user accounts.

Before you begin:

- [Delete](#) any scans that use the template you want to delete. You cannot delete a scan template if a scan is using the template.

To delete a user-defined scan template or templates:



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

The left navigation plane appears.

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

The **My Scans** page appears.

3. In the upper-right corner of the page, click the  **Scan Templates**.

The **Scan Templates** page appears.

4. Select the scan template or templates you want to delete:

- **Select a single scan template:**

- a. In the scans table, roll over the scan you want to launch.
- b. In the row, click the ⋮ button.

A menu appears.


- c. In the menu, click the  button.

A confirmation window appears.

- **Select multiple scan templates:**

- a. In the scan templates table, select the check box for each scan template you want to delete.

The action bar appears at the bottom of the pagetop of the table.

- b. In the action bar, click the  button.

A confirmation window appears.

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

Tenable Web App Scanning deletes the user-defined scan template or templates you selected.



Scan Settings

Scan settings enable you to refine parameters in scans to meet your specific network security needs. The scan settings you can configure vary depending on the [Tenable-provided template](#) on which a scan or user-defined template is based.

You can configure these settings in [individual scans](#) or in [user-defined templates](#) from which you create individual scans.

Scan settings are organized into the following categories:

Tenable Vulnerability Management Scans	Tenable Web App Scanning Scans
<ul style="list-style-type: none">• Basic Settings in User-Defined Templates• Basic Settings in Vulnerability Management Scans• Discovery Settings in Vulnerability Management Scans• Assessment Settings in Vulnerability Management Scans• Report Settings in Vulnerability Management Scans• Advanced Settings in Vulnerability Management Scans• Credentials• Compliance in Vulnerability Management Scans• SCAP Settings in Vulnerability Management Scans• Configure Plugins	<ul style="list-style-type: none">• Basic Settings in User-Defined Templates• Basic Settings in Tenable Web App Scanning Scans• Scope Settings in Tenable Web App Scanning Scans• Report Settings in Tenable Web App Scanning Scans• Assessment Settings in Tenable Web App Scanning Scans• Advanced Settings in Tenable Web App Scanning Scans• Credentials in Tenable Web App Scanning Scans• Plugin Settings in Tenable Web App Scanning Scans

Settings in User-Defined Templates



When configuring settings for user-defined templates, note the following:

- If you configure a setting in a user-defined template, that setting applies to any scans you create based on that user-defined template.
- You base a user-defined template on a Tenable-provided template. Most of the settings are identical to the settings you can configure in an individual scan that uses the same Tenable-provided template.

However, certain **Basic** settings are unique to creating a user-defined template, and do not appear when configuring an individual scan. For more information, see [Basic Settings in User-Defined Templates](#).

- You can configure certain settings in a user-defined template, but cannot modify those settings in an individual scan based on a user-defined template. These settings include [Discovery](#), [Assessment](#), [Report](#), [Advanced](#), [Compliance](#), [SCAP](#), and [Plugins](#). If you want to modify these settings for individual scans, create individual scans based on a Tenable-provided template instead.
- If you configure [Credentials](#) in a user-defined template, other users can override these settings by adding scan-specific or managed credentials to scans based on the template.



Tenable Web App Scanning Scan Settings

Scan settings enable you to refine parameters in scans to meet your specific network security needs. The scan settings you can configure vary depending on the [Tenable-provided template](#) on which a scan or user-defined template is based.

You can configure these settings in [individual scans](#) or in [user-defined templates](#) from which you create individual scans.

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

- [Basic Settings in User-Defined Templates](#)
- [Basic Settings in Tenable Web App Scanning Scans](#)
- [Scope Settings in Tenable Web App Scanning Scans](#)
- [Report Settings in Tenable Web App Scanning Scans](#)
- [Assessment Settings in Tenable Web App Scanning Scans](#)
- [Advanced Settings in Tenable Web App Scanning Scans](#)
- [Credentials in Tenable Web App Scanning Scans](#)
- [Plugin Settings in Tenable Web App Scanning Scans](#)

Settings in User-Defined Templates

When configuring settings for user-defined templates, note the following:

- If you configure a setting in a user-defined template, that setting applies to any scans you create based on that user-defined template.
- You base a user-defined template on a Tenable-provided template. Most of the settings are identical to the settings you can configure in an individual scan that uses the same Tenable-provided template.

However, certain **Basic** settings are unique to creating a user-defined template, and do not appear when configuring an individual scan. For more information, see [Basic Settings in User-Defined Templates](#).



- You can configure certain settings in a user-defined template, but cannot modify those settings in an individual scan based on a user-defined template. These settings include [Discovery](#), [Assessment](#), [Report](#), [Advanced](#), [Compliance](#), [SCAP](#), and [Plugins](#). If you want to modify these settings for individual scans, create individual scans based on a Tenable-provided template instead.
- If you configure [Credentials](#) in a user-defined template, other users can override these settings by adding scan-specific or managed credentials to scans based on the template.



Tenable Web App Scanning Settings

The **Settings** page allows you to view and manage all of your Tenable Web App Scanning settings and configurations.

To access the Settings page:

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

The left navigation plane appears.

2. Click **Settings**.

The **Settings** page appears.

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

Topic	Description
General	View and manage your general settings.
My Account	View and manage your account settings.
SAML	Manage SAML credentials and self service.
License	View licensing details and statistics.
Access Control	View and manage which hosts users can scan and can view in scan results and aggregated data.
Access Groups	Manage access groups. <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"><p>Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.</p></div>
Activity Logs	View activity logs for your organization's account.
Exports	View export activity and manage scheduled exports.



Recast	View and manage recast and accept rules.
Tagging	View and manage tags and tagging rules.
Sensor Management	Manage sensors and sensor groups.
Credentials	View and manage scanning credentials.
Exclusions	View and manage scanning restrictions.
Connectors	Enable Frictionless Assessment and Cloud Connectors.



View your License Information

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

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

The **License** page contains information about your Tenable Vulnerability Management instance, including license and environment details. For more information about how licenses are counted or reclaimed, see [Tenable Vulnerability Management Licenses](#) and [Tenable Web App Scanning Licenses](#).

To view details about your Tenable Vulnerability Management instance and license:

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

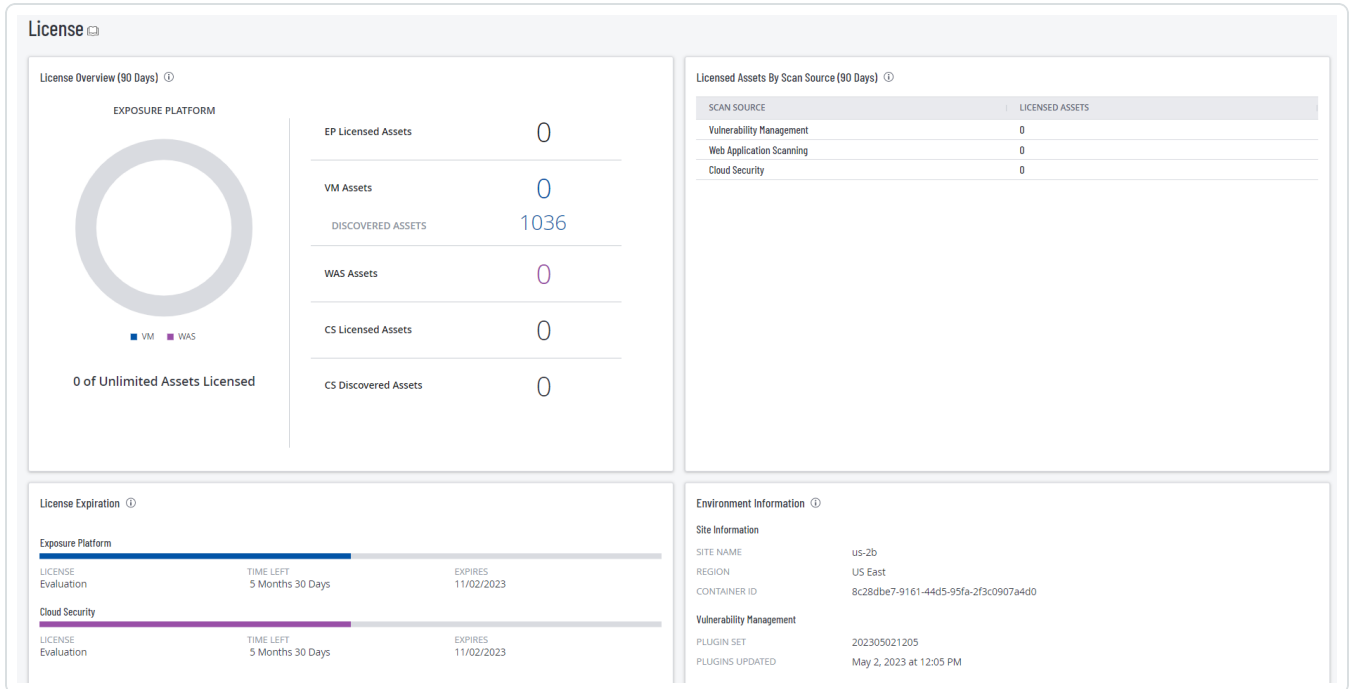
The left navigation plane appears.

2. Click **Settings**.

The **Settings** page appears.

3. Click the **License** tile.

The **License** page appears.



Widget	Description	Actions
License Overview (90 Days)	<p>The ring chart visualizes your licensed asset usage by product. The count next to the chart summarizes your licensed assets currently in use compared to your total licensed amount.</p> <p>The counts to the right of the chart provide a more detailed asset count breakdown by:</p> <ul style="list-style-type: none"> • Product license – The number of assets associated with each individual product license. For example, if you have a Tenable.ep license, you see a count for your licensed assets currently in use and platform-specific counts for each contributing Tenable Vulnerability Management product. • Discovered Assets – The number of discovered assets (not assessed) within 	<p>Click the widget to view the licensed assets in the Assets plane for further analysis or to configure scanning for discovered assets.</p>



	the last 90 days.	
Licensed Assets By Scan Source (90 Days)	The number of licensed assets by scan source.	Click a row in the table to view the licensed assets in the Assets plane, filtered by scan source.
License Expiration	The type of license, the amount of time remaining on the license, and the expiration date for the license.	None.
Environment Information	<p>Information about the region in which your Tenable Vulnerability Management container resides and its container ID. Additionally, this widget contains information about your Tenable Vulnerability Management plugin set and the last time the plugins were updated.</p> <div style="border: 1px solid green; padding: 5px;"><p>Tip: Your site is a geographical location that corresponds with your region. You can provide this information directly to Tenable Support when reporting a potential issue.</p></div>	None.



Tenable Web App Scanning Licenses

Your Tenable Web App Scanning instance has a licensed asset limit that determines the number of web application assets you can scan for vulnerabilities. If you exceed your limit, you can temporarily continue to use Tenable Web App Scanning to scan your assets before adjusting your license as needed.

You can view your license information to see how many assets are currently counted against your Tenable Web App Scanning license. You can use this information to evaluate how effectively you are using your asset licenses.

How Assets are Counted

Tenable Web App Scanning determines asset count by the number of fully-qualified domain names (FQDNs) that Tenable Web App Scanning successfully scans for your user account. An asset does not count against your license limit until Tenable Web App Scanning has successfully scanned the asset for vulnerabilities.

FQDNs appear on your license as complete URLs. Per the RFC-3986 internet standard, each FQDN includes the following components and format:

```
hostname.parent domain.top-level domain
```

When you specify a web application target in a scan, Tenable Web App Scanning counts that target as a separate asset if any component of the FQDN differs from that of another scanned target or previously scanned asset. Multiple targets with different paths appended to the FQDN count as a single asset, as long as all components of the FQDNs match.

The following targets would count toward a single asset in Tenable Web App Scanning:

```
hostname.parent domain.top-level domain/path1  
hostname.parent domain.top-level domain/path2  
hostname.parent domain.top-level domain/path2/path3
```

Note: When a licensed target has not been scanned for 90 days, it ages out of the licensed count.

Example



In this example, Tenable Web App Scanning successfully scans the following target and counts it toward your licensed asset limit.

`https://www.example.com`

In the following table, targets in the first column would count as the same asset as the example asset, and targets in the second column would count as separate assets from the example.

Same Asset (all FQDN components match)	Separate Assets (FQDN components do not all match)
<ul style="list-style-type: none">• <code>https://example.com/welcome</code>• <code>https://example.com/welcome/get-started</code>• <code>https://example.com/welcome/get-started/create-new-user</code>	<ul style="list-style-type: none">• <code>https://en.example.com</code> (different hostname)• <code>https://www.ex-ample.com</code> (different parent domain)• <code>https://www.example.org</code> (different top-level domain)