Tenable Web App Scanning User Guide

Last Revised: April 25, 2024

Table of Contents

Welcome to 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.

For more information, on Tenable Web App Scanning architecture and scanning, refer to Get Started with Tenable Web App Scanning.

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

Tip: The *Tenable Web App Scanning User Guide* is available in English and Japanese. The Tenable Web App Scanning user interface is available in English, Japanese, and French. To switch the user interface language, see General Settings.

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 Oneproducts, check out the Tenable One Deployment Guide.

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.

Tenable Web App Scanning Deployment Options

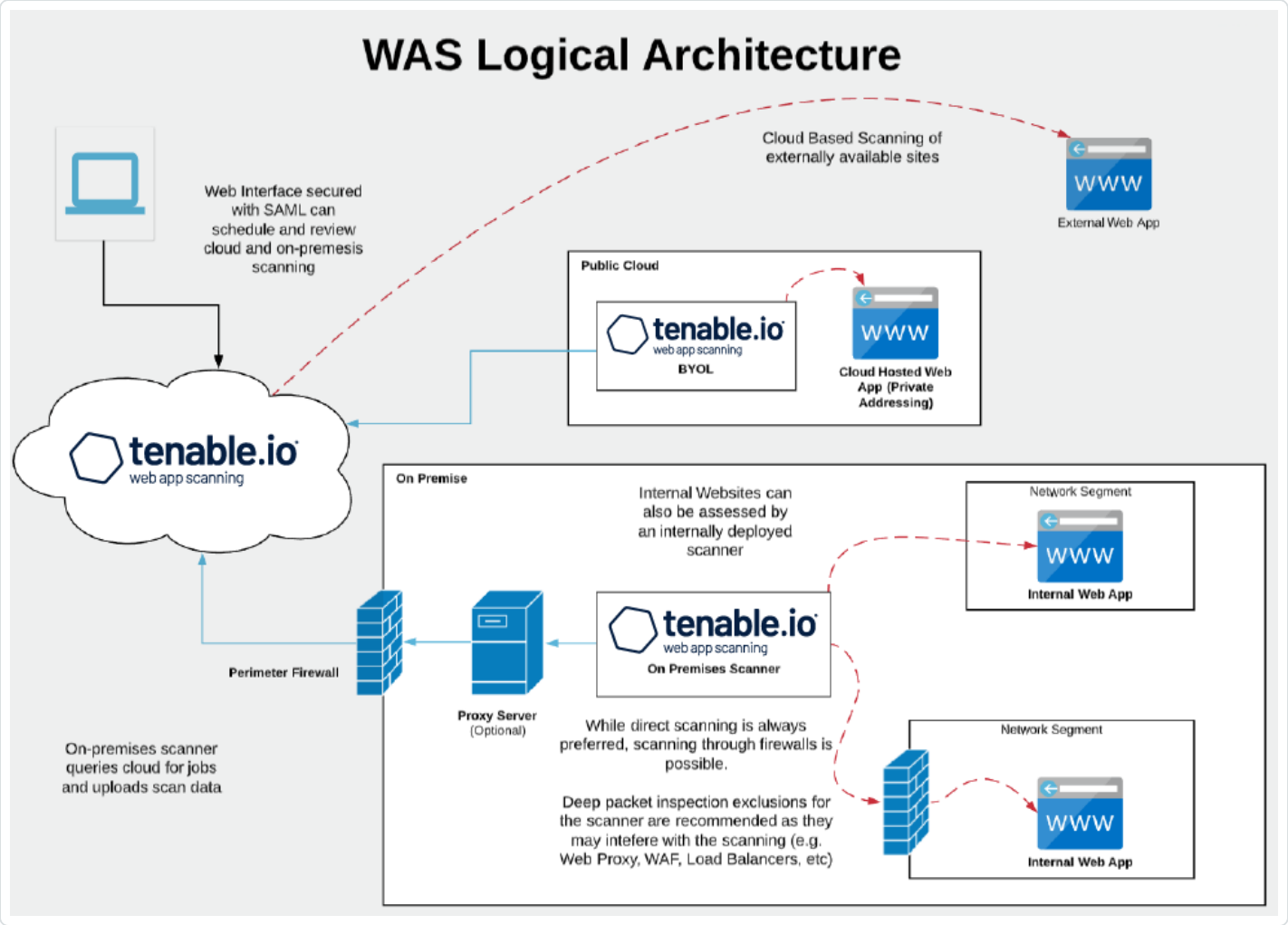
Tenable offers many deployment options for Tenable Web App Scanning. For more information, refer to the following product pages:

- Tenable Core + Web App Scanning - You can use the Tenable Core operating system to run an instance of Tenable Web App Scanning in your environment. After you deploy Tenable Core + Tenable Web App Scanning, you can monitor and manage your Tenable Web App Scanning processes through the secure Tenable Core platform.
- Tenable Web App Scanning in Tenable Nessus Expert - Tenable Web App Scanning in Tenable Nessus Expert allows you to scan and address web application vulnerabilities that traditional Tenable Nessus scanners, Tenable Nessus Agents, or Tenable Nessus Network Monitor cannot scan.
- Tenable Web App Scanning Docker Image - You can deploy 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. Once the Docker image is deployed, you can also update it, or collect scanner logs.
- Tenable Web App Scanning CI/CD Application Scan - You can deploy the Tenable Web App Scanning Docker image as a continuous integration and continuous delivery/continuous deployment (CI/CD) tool to run Tenable Web App Scanning scans on software before merging it. Scanning your CI/CD applications and services at any point in your application's lifecycle can greatly improve your security stance by finding vulnerabilities as early as possible.

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 therefore 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 a 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:**

Some 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 vulnerability 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. 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 finish allowing you to 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 Licenses

This topic breaks down the licensing process for Tenable Web App Scanning as a standalone product. It also explains how assets are counted, lists add-on components you can purchase, and describes what happens during license overages or expirations. To learn how to use Tenable Web App Scanning, see the Tenable Web App Scanning User Guide.

Licensing Tenable Web App Scanning

Tenable Web App Scanning has two versions: a cloud version and an on-premises version. For the cloud version, Tenable offers a subscription model. For the on-premises version, Tenable offers a subscription model as well as perpetual and maintenance licenses.

> **Note**: A Tenable Security Center license is required for the Tenable Web App Scanning on-premises version.

To use Tenable Web App Scanning, you purchase licenses based on your organizational needs and environmental details. Tenable Web App Scanning then assigns those licenses to *assets* in your environment: unique fully qualified domain names (FQDNs).

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

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

How Assets are Counted

Tenable Web App Scanning determines your licensed asset count by scanning resources in your environment to identify FQDNs. FQDNs that have been scanned for vulnerabilities in the past 90 days count towards your license.

FQDNs are listed as complete URLs, as per the RFC-3986 internet standard. Under this standard, each FQDN has 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.

For example, the following targets count towards one asset:

```
hostname.parent-domain.top-level-domain/path1
hostname.parent-domain.top-level-domain/path2
hostname.parent-domain.top-level-domain/path2/path3
```

The following table shows when scan targets are considered to be the same asset and when they are considered to be separate assets, based on whether or not all the FQDN components match.

Same Asset	Separate Assets
• https://example.com • https://example.com/welcome • https://example.com/welcome/get-started • https://example.com/welcome/get-started/create-new-user • http://example.com	• *https://en.example.com (different hostname)* • *https://www.ex-ample.com (different parent domain)* • *https://www.example.org (different top-level domain)*

Tenable Tenable Web App Scanning Components

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

Included with Purchase	Add-on Component
• External scanning functionality. • OWASP Top 10 Issues.	Additional cloud scan concurrency. **Tip**: Concurrency is based on your licensed assets and determines how many Tenable-managed cloud scanners you can

• HTML5 crawling. • Integration with Tenable Vulnerability Management (if owned). • Use of the API.	run simultaneously.

Reclaiming Licenses

When you purchase assets, your total asset count remains static for the length of your contract unless you purchase more assets. However, Tenable Web App Scanning reclaims licenses from deleted assets within 24 hours. In addition, it reclaims licenses from assets which are not scanned for 90 days or a period you specify.

Exceeding the License Limit

To allow for usage spikes due to sudden environment growth or unanticipated threats, Tenable Web App Scanning licenses are elastic by 10%. However, when you scan more assets than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages.

Scenario	Result
You scan more assets than are licensed for three consecutive days.	A message appears in Tenable Web App Scanning.
You scan more assets than are licensed for 15+ days.	A message and warning about reduced functionality appears in Tenable Web App Scanning.
You scan more assets than are licensed for 45+ days.	A message appears in Tenable Web App Scanning; export features are disabled.

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

Expired Licenses

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

After your license expires, you can no longer sign in to the Tenable platform.

Tenable Web App Scanning Requirements

Hardware Requirements

Scenario	Hardware Recommendations
Tenable Web App Scanning up to four concurrent web applications.	**CPU:** (4) 2 GHz cores **Core Ram:** 16 GB RAM **Hard Drive:** 100 GB

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.

Log In to Tenable Web App Scanning

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, 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).

Navigate Tenable Web App Scanning

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

Quick Actions Menu

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

To access the quick actions menu:

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

   The quick actions menu appears.

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

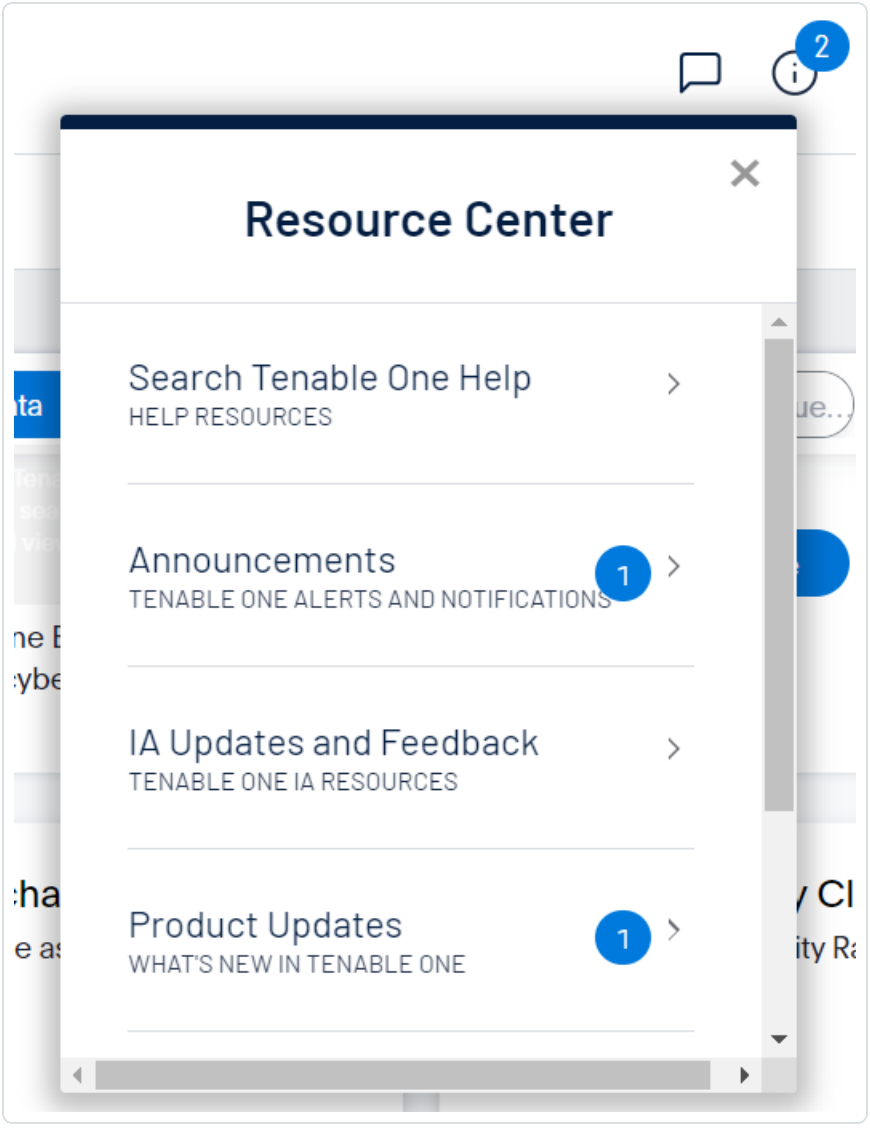
Resource Center

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

To access the Resource Center:

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

   The **Resource Center** menu appears.



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

Notifications

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

> **Note:** Tenable Web App Scanning groups similar notifications together.

To view notifications:

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

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

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

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

Settings Icon

Workspace

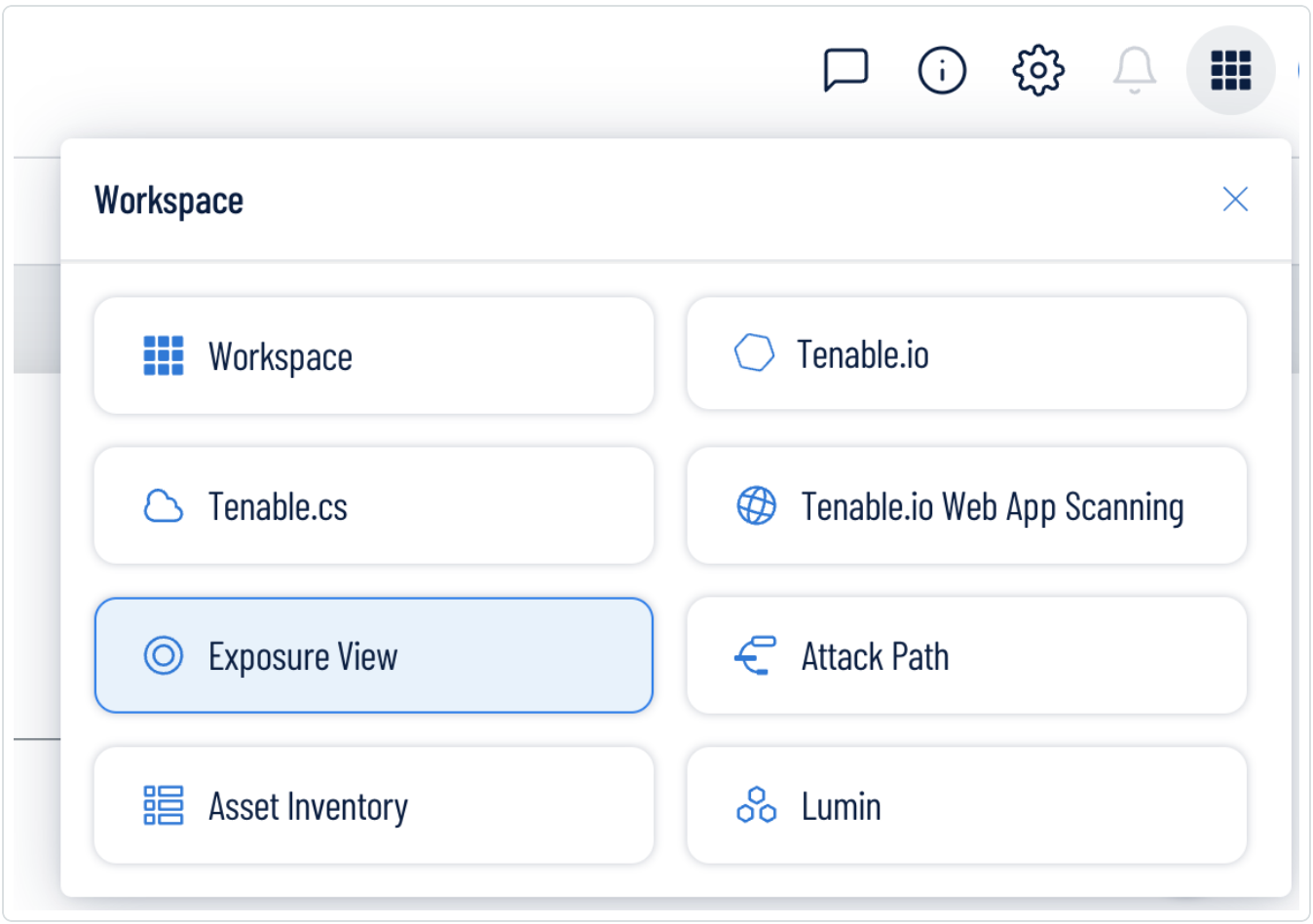
When you log in to Tenable, the **Workspace** page appears by default. On the **Workspace** page, you can switch between your Tenable applications or set a default application to skip the **Workspace** page in the future. You can also switch between your applications from the **Workspace** menu, which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

Open the Workspace Menu

To open the **Workspace** menu:

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

   The **Workspace** menu appears.



2. Click an application tile to open it.

View the Workspace Page

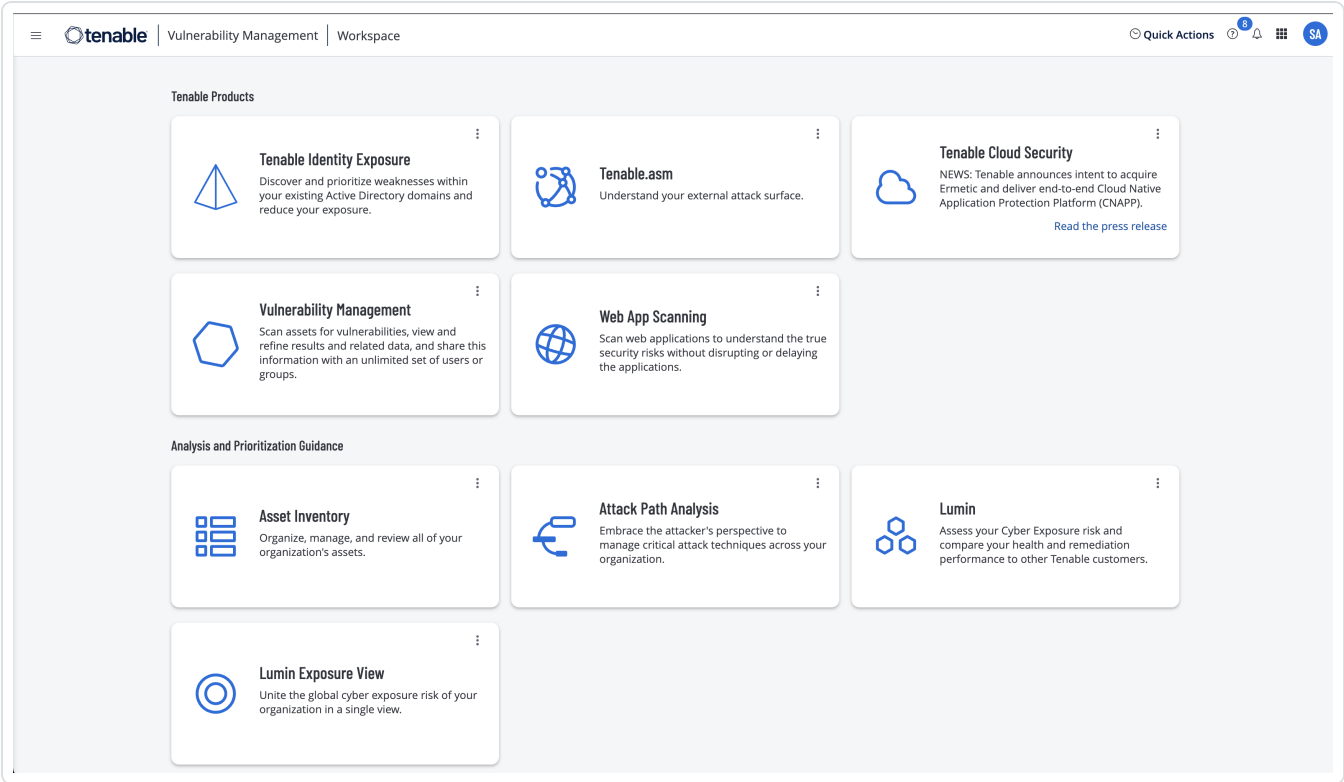
To view the Workspace page:

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

   The **Workspace** menu appears.

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

The **Workspace** page appears.



Set a Default Application

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

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

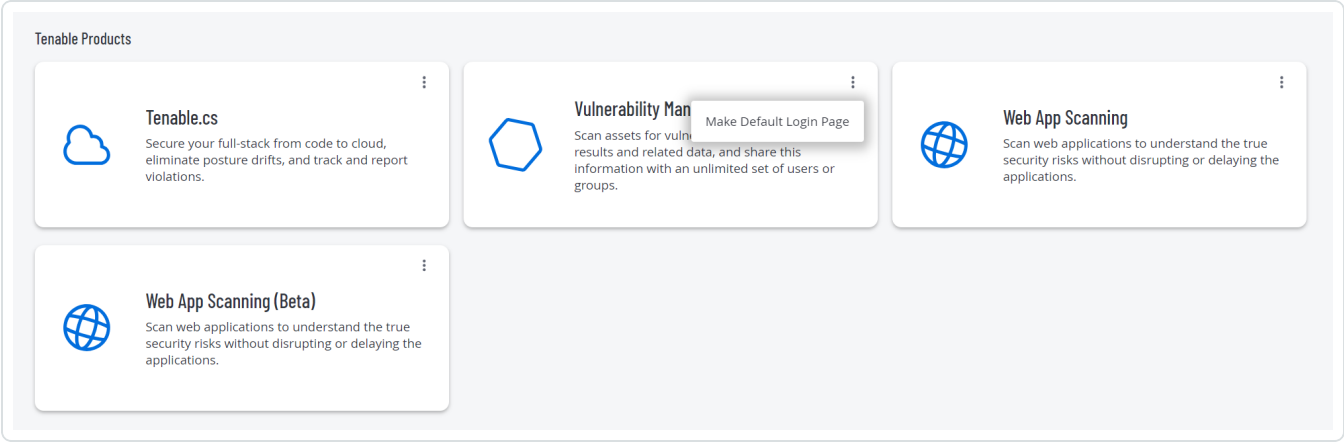
To set a default login application:

1. Log in to Tenable.

   The **Workspace** page appears.

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

   A menu appears.



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

   This application now appears when you log in.

Remove a Default Application

To remove a default login application:

1. Log in to Tenable.

   The **Workspace** page appears.

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

   A menu appears.

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

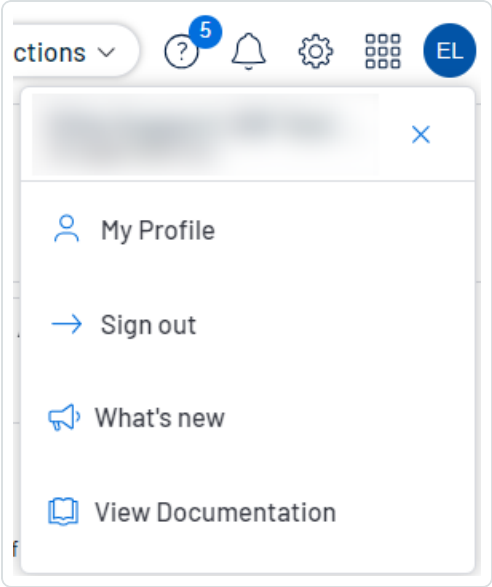
   The **Workspace** page now appears when you log in.

User Account Menu

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

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

   The user account menu appears.



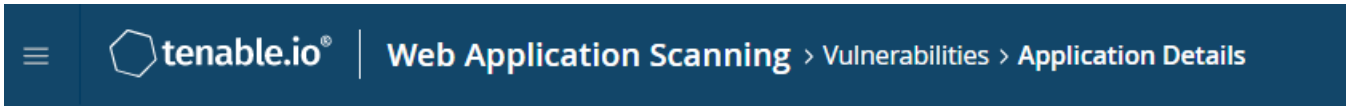
2. Do one of the following:

   - Click **My Profile** to configure your own user account. You navigate directly to the **My Account** settings page.
   - Click **Sign out** to sign out of Tenable Web App Scanning.
   - Click **What's new** to navigate directly to the Tenable Web App Scanning Release Notes.
   - Click **View Documentation** to navigate directly to the Tenable Web App Scanning User Guide documentation.

For additional information about navigating the Tenable Web App Scanning interface, see the following topics:

Navigate Breadcrumbs

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



To navigate breadcrumbs:

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

Navigate Planes

Tenable Web App Scanning combines fixed pages with overlapping planes.

To navigate planes in the new interface:

1. Access a plane using one of the following methods:

   - Click a widget on a dashboard.
   - Use the left navigation plane as follows:

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

     The left navigation plane appears.

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

   With the exception of the left navigation plane, planes open from the right side of the screen.

2. Manipulate a plane using the following buttons at the left edge of the plane:

Button	Short Name	Action
⤢	expand	Expand a plane. Some planes can expand to full screen.
⤡	retract	Retract an expanded plane to its default size.
×	close	Close a plane.
←	expand preview	Expand a preview plane.
→	retract preview	Retract an expanded plane to the preview plane.

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

Tenable Web App Scanning Tables

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

Tenable Web App Scanning Workbench Tables

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

Explore Tables

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

Tenable Web App Scanning Workbench Tables

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

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

Tenable Web App Scanning Workbench tables are any tables in the Tenable Web App Scanning interface outside of the **Explore** section.

To interact with a Tenable Web App Scanning workbench table:

1. View a workbench table.
2. Do any of the following:
   - Navigate the table:
     - To adjust the sort order, click a column title.

       Tenable Web App Scanning sorts all pages of the table by the data in the column you selected.
     - In Tenable Web App Scanning, to increase or decrease the number of rows displayed per page, click **Results per page** ⌄ and select a number.

       Tenable Web App Scanning refreshes the table.
     - To view all action buttons available in a table row, click the ⋮ button.

       This button appears instead of individual action buttons if 5 or more actions are possible for the row.
     - To navigate to another page of the table, click the arrows:

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

>|	Navigate to the last page of the table.

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

- Search the table:

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

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

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

  b. Click the 🔎 button.

     Tenable Web App Scanning filters the table by your search criteria.

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

- Remove or add columns:

  a. Roll over any column.

     The ☰ button appears in the header.

  b. Click the ☰ button.

     A column selection box appears.

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

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

     The table updates based on your selection.

- Adjust column width:

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

   Click and drag the column width to the desired width.

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

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

  Tenable Web App Scanning sorts all pages of the table by the data in the column you selected.

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

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

  Tenable Web App Scanning sorts all pages of the table in the order in which you selected the columns.

Filter a Table

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

In Tenable Web App Scanning, a **Filters** box appears above individual tables in various pages and planes.

To filter a table:

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

   The filter settings appear.

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

   A drop-down list appears.

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

      The list updates based on your search criteria.

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

      The selected filters appear in the filter section.

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

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

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

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

   - For the most accurate and complete search results, use full words in your search value.
   - Do not use periods in your search value.
   - Remember that when filtering assets, the search values are case sensitive.

- Where applicable, Tenable recommends using the **contains** or **does not contain** instead of the **is equal to** or **is not equal to** operators.

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

Value Type	Action
Text	Type the value on which you want to filter. An example of the expected input is present in the box until you start typing. If what you type is invalid for the attribute, a red outline appears around the text box.
Single valid value	If a default value is associated with the attribute, Tenable Web App Scanning selects the default value automatically. To change the default value, or if there is not an associated default value present: a. Click the box to display the drop-down list. b. Search for and select one of the listed values.
Multiple valid values	To select one or more values: a. Click the box to display the drop-down list. b. Search for and select a value. The selected value appears in the box. c. Repeat until you have selected all appropriate values d. Click outside the drop-down list to close it. To deselect values: a. Roll over the value you want to remove. The × button appears over the value. b. Click the × button.

	The value disappears from the box.

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

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

      Tenable Web App Scanning clears all filters from the table, including saved searches.

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

Deploy Tenable Web App Scanning as a Docker Image

You can deploy 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. Once the Docker image is deployed, you can also update it, or collect scanner logs.

> **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.

Deploy or Remove Docker Image

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:

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

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>
```

Operators

Operator	Description
`--name`	Sets the name of the container in Docker.
`-d`	Starts a container in detached mode.
`-e`	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 (for example, "scanner-group-1, sec-scanner-group").
`WAS_AUTO_UNLINK_ON_EXIT`	No	Automatically unlinks scanner when scanner stops.
`WAS_PLATFORM_URL`	No	Defaults to `https://cloud.tenable.com`.

`WAS_PROXY_URL`	No	URL to use for proxy to platform.

Update Docker Image

To update the Docker image:

- Run `docker pull tenable/was-scanner`.

  This pulls the latest version of the scanner from Docker.

Collect Scanner Logs

To collect scanner logs use one of the following options:

- Run `WAS_LOG_TO_STDOUT`.

  This prints the logs to `stdout`, and you should be able to collect them with `docker logs <container id>`.

- Set `WAS_SCANNER_LOG_FILE` to a specific location that you mount on the host.

  For example, `docker run -e WAS_SCANNER_LOG_FILE=/scanner/scanner.log -v $PWD:/scanner`.

  > **Note:** This option should cause the log file to exist in your `PWD` even after the container has stopped.

Tenable Web App Scanning CI/CD Application Scan Overview

You can deploy the Tenable Web App Scanning Docker image as a continuous integration and continuous delivery/continuous deployment (CI/CD) tool to run Tenable Web App Scanning scans on software before merging it. Scanning your CI/CD applications and services at any point in your application's lifecycle can greatly improve your security stance by finding vulnerabilities as early as possible.

Before you begin:

- Ensure your CI/CD build system supports using the Docker container.

> **Note:** Scanning CI/CD builds is limited to a single scan run at a time.

Scan CI/CD build with Tenable Web App Scanning Docker image:

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

   The left navigation plane appears.

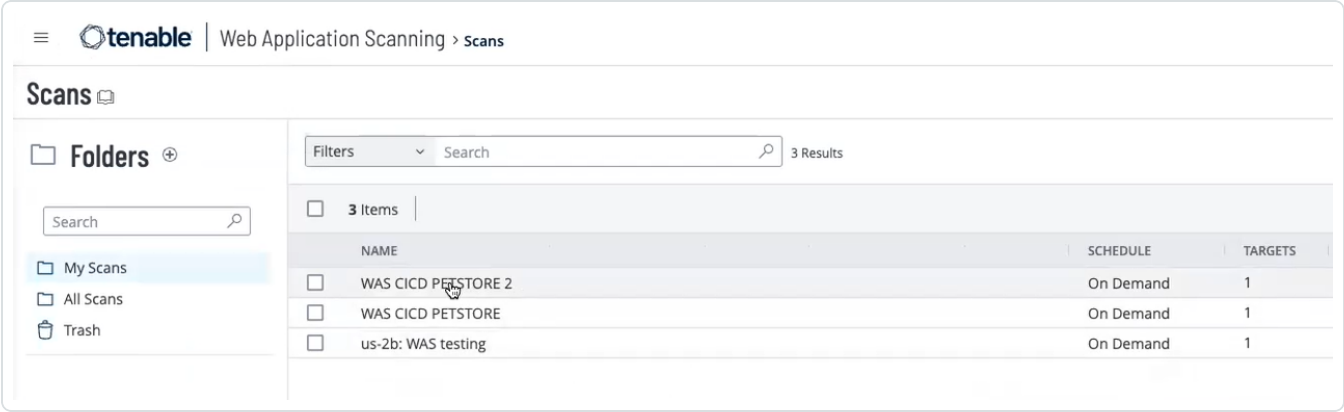
2. In the left navigation plane, click **Integrations**.

   The **Integrations** page appears.

3. In the left navigation plane, select an integration type:

   - Atlassian Bamboo
   - CircleCI
   - GitHub
   - GitLab
   - Jenkins

4. Locate your scan in the Tenable Web App Scanning user interface.



Note: The **Scanner Type** and **Scanner** fields do not apply to CI/CD scans and should remain at their default setting.

Note: When configuring a scan for integration into a CI/CD pipeline, Tenable recommends selecting a Scan Template with a relatively short runtime to avoid potential delays in your build process. For more information, refer to the Scan Templates section.

Note: Ensure that the target hostname is distinct from your production application. This ensures that vulnerabilities found during builds do not intermix with your production application's vulnerabilities.

5. Export the scan configuration for the selected scan to the scan pipeline stages.

   On the **Scans** page, click the ⋮ button for the scan you have chosen and select **Export for CI/CD**.

6. Upload your scan configuration file to your Git repository.

7. (Optional) Make Credentialed Scan Edits in your configuration file.

8. Generate an API key.

   Note: If you don't have an API Key, you can generate one on your **Account** page. For more information, see Generate API Keys.

9. Copy generated API keys to your preferred secret storage provider.

   Caution: Tenable recommends that you always take measures to hide any sensitive information, such as API keys used to link the scanner to Tenable and the username/password combination used

by the scanner to authenticate to the web app being scanned. Keep these out of source control and placed in secure storage provided by the repository, or the continuous integration tooling in use.

10. Run the following steps to run the scan:

```
docker pull tenable/was-scanner:latest
docker run -e WAS_MODE=cicd -e ACCESS_KEY=${TENABLE_IO_ACCESS_KEY}
SECRET_KEY=${TENABLE_IO_SECRET_KEY} -v ./:/scanner tenable/was-
scanner:latest
```

11. Set the `vulnerability_threshold` field parameter to either **Critical**, **High**, **Medium**, or **Low**.

    Note: The threshold you set for this field causes your build to pass or fail if your build meets, or does not meet, the threshold, respectively. Builds can also fail due to scan errors or incomplete configurations.

12. (Optional) Follow the specific outline of the pipeline workflow file required for your CI/CD integration, as described in the following CI/CD Pipeline Workflow File section.

13. Go to the selected scan in the **Scans** page to view the results.

14. (Optional) Retrieve your logs. Refer to the following Reports and Logs section.

Note: The scanner Docker image uses the `/scanner` directory for seamless file exchange between the host and the docker container. To mount your `tenable_was.conf` file located in your repository, use `-v $PWD:/scanner` in the docker run command. If your configuration file is at the top level of your repository, this directory is where you can retrieve the `tenable_was_scan.html` and `scanner.log` files after the scan.

Credentialed Scan Edits

When creating a scan configuration and adding credentials to that scan, you can also edit the credentials in the CI/CD file you exported. In the exported `tenable_was.conf` file, there may be placeholder text instead of sensitive information related to those credentials (passwords, auth tokens, etc.). For example, `${?USER_PASS_PASSWORD}` and `${?USER_PASS_USERNAME}` are placeholders in the following example file:

Note: Credentialed scan edits are necessary for Login Form, Cookie Auth, and API Key authentication methods.

```
scan {
  credentials {
    "user_pass" {
    "auth_type"=auto
    password=${?USER_PASS_PASSWORD}
    username=${?USER_PASS_USERNAME}
  }
}
```

When you run the docker image, those placeholders represent environment variables that where the scanner retrieves the actual values from, so make sure they are present. In the previous example, you would run the docker image with the environment variables necessary to fill in those values, As shown in the following example:

```
`docker run -e WAS_MODE=cicd -e USER_PASS_USERNAME=<the username here> -e
USER_PASS_PASSWORD=<the password here> ..etc, etc`
```

In cases where values serve as both keys and values, you must provide them as a JSON object containing the corresponding key-value pairs. For instance, if your web application uses Login Form authentication and requires both field names and values, such as "username" and "password," you should configure it as follows:

```
scan {
  credentials {
    "login_form" {
    "auth_headers"=${?LOGIN_FORM_AUTH_HEADERS}
    "login_check"=Welcome
    "login_check_pattern"=Welcome
    "login_check_url"="http://app:3000/home.html"
    "login_parameters"=${?LOGIN_FORM_LOGIN_PARAMETERS};
  }
}
```

You can use the following example inputs:

```
`docker run -e WAS_MODE=cicd -e LOGIN_FORM_LOGIN_PARAMETERS='{"username": "my_username", "password":"my_password"}'-e LOGIN_FORM_AUTH_HEADERS='{}' …etc, etc`
```

Note: Make sure there is a value present for all placeholder values, even if the value is empty.

CI/CD Pipeline Workflow File

You can apply the setup for pipeline workflow files to many available tools, once you understand the principles involved. The following is an example pipeline workflow file for Jenkins:

```
pipeline {
  agent any
  stages {
    stage('build-run-scan') {
      environment {
        ACCESS_KEY = credentials('ACCESS_KEY')
        SECRET_KEY = credentials('SECRET_KEY')
      }
      steps {
        sh '''
        docker pull swaggerapi/petstore
        docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_
PATH=/v2 --name petstore swaggerapi/petstore
        docker pull tenable/was-scanner:latest
        docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_
KEY=${ACCESS_KEY} -e SECRET_KEY=${SECRET_KEY} --link petstore tenable/was-
scanner:latest
        '''
      }
    }
  }
  post {
    always {
```

```
      sh '''
      docker rm $(docker stop $(docker ps -a -q --filter
ancestor="tenable/was-scanner:latest" --format="{{.ID}}")) || true
      docker rm $(docker stop $(docker ps -a -q --filter
ancestor="swaggerapi/petstore" --format="{{.ID}}")) || true
      docker system prune -f --volumes
      '''
      archiveArtifacts 'scanner.log'
      publishHTML([allowMissing: false, alwaysLinkToLastBuild: false,
keepAll: true, reportDir: '', reportFiles: 'tenable_was_scan.html',
reportName: 'WAS Report'])
      cleanWs()
    }
  }
}
```

Reports and Logs

You can generate the console output, HTML report (`tenable_was_scan.html`), and scanner log file (`scanner.log`) after each build. Use command lines to archive your HTML report and scanner log. These are specific to each CI/CD tool. The console output after completion of your build indicates a build pass or failure and potential causes. The HTML report indicates further scan results based on the `vulnerability_threshold` you input into the `tenable-was.conf` file.

> **Note:** Tenable recommends that you retain scanner logs as they can be useful for debugging.

Example archive command lines for a Jenkins pipeline workflow file:

```
archiveArtifacts 'scanner.log' publishHTML([allowMissing: false,
alwaysLinkToLastBuild: false, keepAll: true, reportDir: '', reportFiles:
'tenable_was_scan.html', reportName: 'WAS Report']
```

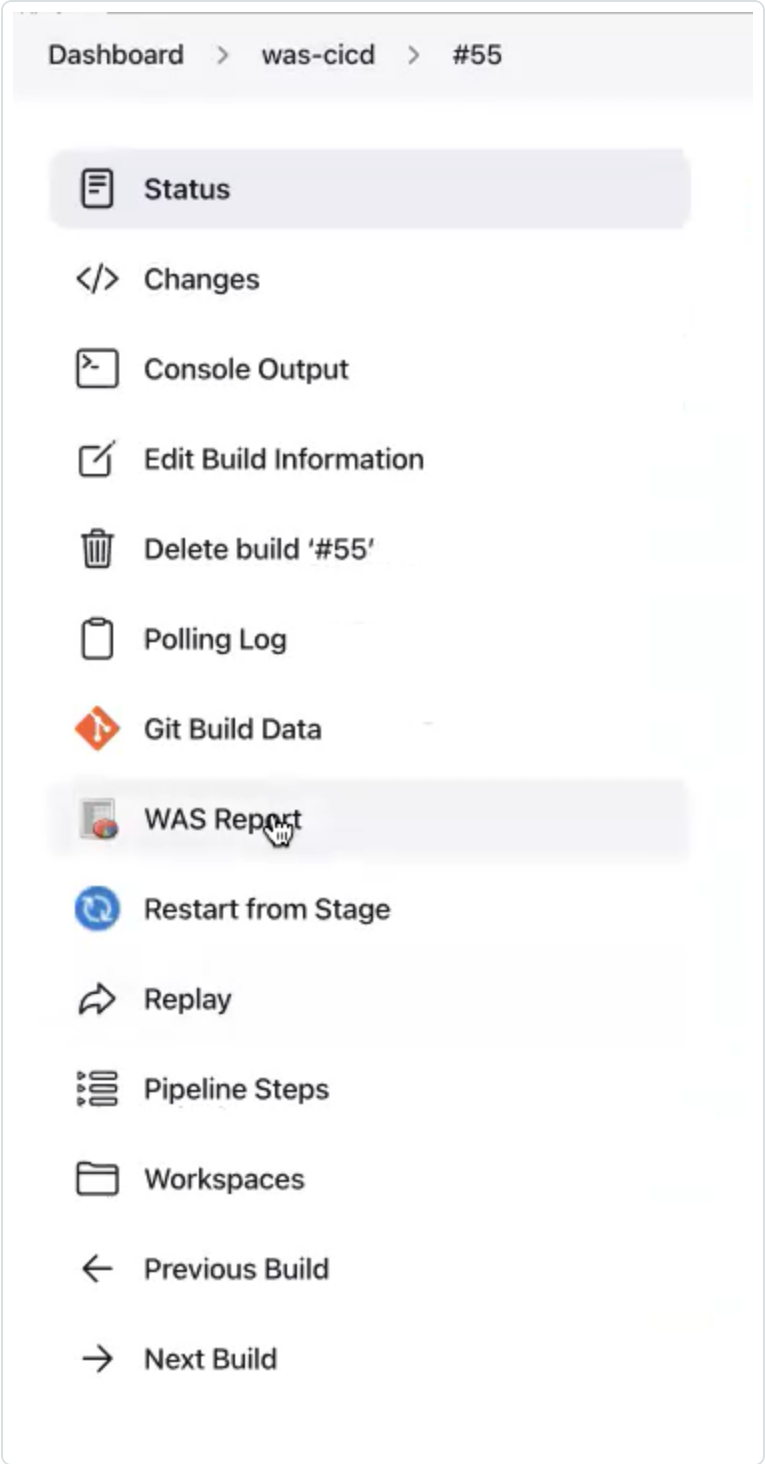
Example console output:

```
Dashboard > was-cicd > #55

2022-10-17 17:26:29:1666027589 [CI/CD] [ [0;32mINFO [0m] getting scan status (status: succeeeded, attempt: 1/10)
2022-10-17 17:26:29:1666027589 [CI/CD] [ [0;32mINFO [0m] status of scan: running
2022-10-17 17:26:29:1666027589 [CI/CD] [ [0;32mINFO [0m] sleeping 10 seconds
2022-10-17 17:26:39:1666027599 [CI/CD] [ [0;32mINFO [0m] getting scan status (status: succeeeded, attempt: 1/10)
2022-10-17 17:26:39:1666027599 [CI/CD] [ [0;32mINFO [0m] status of scan: running
2022-10-17 17:26:39:1666027599 [CI/CD] [ [0;32mINFO [0m] sleeping 10 seconds
2022-10-17 17:26:49:1666027609 [CI/CD] [ [0;32mINFO [0m] getting scan status (status: succeeeded, attempt: 1/10)
2022-10-17 17:26:49:1666027609 [CI/CD] [ [0;32mINFO [0m] scan finalized with status: completed
2022-10-17 17:26:51:1666027611 [CI/CD] [ [0;32mINFO [0m] requesting export of scan report (status: succeeeded, attempt: 1/10)
2022-10-17 17:26:51:1666027611 [CI/CD] [ [0;32mINFO [0m] sleeping 30 seconds
2022-10-17 17:27:21:1666027641 [CI/CD] [ [0;32mINFO [0m] scanner stopped
Scanner process stopped, PID 9.
2022-10-17 17:27:21:1666027641 [CI/CD] [ [0;32mINFO [0m] getting vulns for scan (status: succeeeded, attempt: 1/10)
2022-10-17 17:27:23:1666027643 [CI/CD] [ [0;32mINFO [0m] requesting scan report (status: succeeeded, attempt: 1/10)
2022-10-17 17:27:23:1666027643 [CI/CD] [ [0;33mWARN [0m] vulns over threshold found: 1
2022-10-17 17:27:23:1666027643 [CI/CD] [ [0;33mWARN [0m] vulnerability threshold met, test failed!
[Pipeline] }
[Pipeline] // withCredentials
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Declarative: Post Actions)
[Pipeline] sh
+++ docker ps -a -q --filter ancestor=058789384427.dkr.ecr.us-east-1.amazonaws.com/was-cicd '--format={{.ID}}'
++ docker stop 78970995e6bc
+ docker rm 78970995e6bc
78970995e6bc
+++ docker ps -a -q --filter ancestor=swaggerapi/petstore '--format={{.ID}}'
++ docker stop 6d6bfd6cf842
+ docker rm 6d6bfd6cf842
6d6bfd6cf842
+ docker system prune -f --volumes
Deleted Volumes:
e21c9dc03e1660746cc421632d598b0d25b896d781e8fa4d46c4825a6550c7f5
b972fe24d71ad1685edea621ee257bf60a915cf3cafa74339cbeb9e35d2e7499

Total reclaimed space: 690.1MB
[Pipeline] archiveArtifacts
```

Example HTML report:


Dashboard > was-cicd > #55
Status
Changes
Console Output
Edit Build Information
Delete build '#55'
Polling Log
Git Build Data
WAS Report
Restart from Stage
Replay
Pipeline Steps
Workspaces
Previous Build
Next Build

Scan Results

Vulnerabilities

Severity	Plugin Id	Name	Family	Instances
High	112543	HTTPS Not Detected	SSL/TLS	1
Low	98060	Missing 'X-Frame-Options' Header	HTTP Security Header	1
Low	98618	HTTP Header Information Disclosure	HTTP Security Header	1
Low	98057	Insecure 'Access-Control-Allow-Origin' Header	HTTP Security Header	1
Low	112551	Missing Content Security Policy	HTTP Security Header	1
Low	112553	Missing 'Cache-Control' Header	HTTP Security Header	1
Low	112529	Missing 'X-Content-Type-Options' Header	HTTP Security Header	1

HTTPS Not Detected

VULNERABILITY HIGH PLUGIN ID 112543

Description

HTTPS is a protocol that protects the integrity and confidentiality of data between client and server. HTTPS is highly recommended to protect connections to website regardless of its content.

Solution

Enable HTTPS following best practices.

See Also
https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

Plugin Details

PUBLICATION DATE	2019-02-05T00:00:00+00:00
MODIFICATION DATE	2021-11-26T00:00:00+00:00
FAMILY	SSL/TLS
SEVERITY	High
PLUGIN ID	112543

Risk Information

Example integrations for CI/CD tools:

- Atlassian Bamboo
- CircleCI
- GitHub
- GitLab
- Jenkins

Tenable Web App Scanning CI/CD Scanning with Atlassian Bamboo Integration

You can deploy a Tenable Web App Scanning Docker image in continuous integration and continuous delivery/continuous deployment CI/CD against your application in Atlassian Bamboo. For more information on this integration, see the Atlassian Bamboo documentation.

Before you begin:

- Be able to deploy your app to an integration environment available to your Bamboo build agent, or run it directly on the build agent for testing.
- Review the overview information in CI/CD Application Scan Overview.

Pipeline workflow file example for Atlassian Bamboo:

```
#!/usr/bin/env bash

# start your application
docker pull swaggerapi/petstore
docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_PATH=/v2 -
-name petstore swaggerapi/petstore

# run the scanner
docker pull tenable/was-scanner:latest
docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_KEY=${bamboo_
ACCESS_KEY} -e SECRET_KEY=${bamboo_SECRET_KEY} --link petstore tenable/was-
scanner:latest
```

Example integrations for CI/CD tools:

- CircleCI
- GitHub
- GitLab
- Jenkins

Tenable Web App Scanning CI/CD Scanning with CircleCI Integration

You can deploy a Tenable Web App Scanning Docker image in continuous integration and continuous delivery/continuous deployment CI/CD against your application in CircleCI. For more information on this integration, see the CircleCI documentation.

Before you begin:

- Be able to deploy your app to an integration environment available to your GitLab build agent, or run it directly on the build agent for testing.
- Review the overview information in CI/CD Application Scan Overview.

Pipeline workflow file example for CircleCI:

```
version: 2.1

jobs:
  build-run-scan:
    machine:
      image: ubuntu-2204:2022.04.2
    steps:
      - checkout
      - run: |
          docker pull swaggerapi/petstore
          docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_
PATH=/v2 --name petstore swaggerapi/petstore
          docker pull tenable/was-scanner:latest
          docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_
KEY=${ACCESS_KEY} -e SECRET_KEY=${SECRET_KEY} --link petstore tenable/was-
scanner:latest
workflows:
  was-workflow:
    jobs:
      - build-run-scan
```

Example integrations for CI/CD tools:

- Atlassian Bamboo
- GitHub
- GitLab
- Jenkins

Tenable Web App Scanning CI/CD Scanning with GitHub Integration

You can deploy a Tenable Web App Scanning Docker image in continuous integration and continuous delivery/continuous deployment CI/CD against your application in GitHub. For more information on this integration, see the GitHub documentation.

Before you begin:

- Be able to deploy your app to an integration environment available to your GitHub build agent, or run it directly on the build agent for testing.
- Review the overview information in CI/CD Application Scan Overview.

Pipeline workflow file example for GitHub:

```
name: CI WAS Scan
on:
  push:
    branches:
      - main
  pull_request:
jobs:
  tenablescan:
    name: was-cicd
    runs-on: ubuntu-latest
    steps:
      - name: Clone repo
        uses: actions/checkout@v2
      - name: Build + Run PetStore
        run: |
          docker pull swaggerapi/petstore
          docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_
PATH=/v2 --name petstore swaggerapi/petstore
      - name: Run WAS
        run: |
```

```
          docker pull tenable/was-scanner:latest
          docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_
KEY=${ACCESS_KEY} -e SECRET_KEY=${SECRET_KEY} --link petstore tenable/was-
scanner:latest || true
          ls $(pwd)
        env:
          ACCESS_KEY: ${{ secrets.ACCESS_KEY }}
          SECRET_KEY: ${{ secrets.SECRET_KEY }}
```

Example integrations for CI/CD tools:

- Atlassian Bamboo
- CircleCI
- GitHub
- GitLab
- Jenkins

Tenable Web App Scanning CI/CD Scanning with GitLab Integration

You can deploy a Tenable Web App Scanning Docker image in continuous integration and continuous delivery/continuous deployment CI/CD against your application in GitLab. For more information on this integration, see the GitLab documentation.

Before you begin:

- Be able to deploy your app to an integration environment available to your GitLab build agent, or run it directly on the build agent for testing.
- Review the overview information in CI/CD Application Scan Overview.

Pipeline workflow file example for GitLab:

```
stages:
       - build
build-run-scan:
       stage: build
       image: docker
       services:
       - docker:dind
       script:
       - docker pull swaggerapi/petstore
       - docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_
PATH=/v2 --name petstore swaggerapi/petstore
       - docker pull tenable/was-scanner:latest
       - docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_KEY=${ACCESS_
KEY} -e SECRET_KEY=${SECRET_KEY} --link petstore tenable/was-scanner:latest
```

Example integrations for CI/CD tools:

- Atlassian Bamboo
- CircleCI

- GitHub
- Jenkins

Tenable Web App Scanning CI/CD Scanning with Jenkins Integration

You can deploy a Tenable Web App Scanning Docker image in continuous integration and continuous delivery/continuous deployment CI/CD against your application in Jenkins. For more information on this integration, see the Jenkins documentation.

Before you begin:

- Be able to deploy your app to an integration environment available to your Jenkins build agent, or run it directly on the build agent for testing.
- Review the overview information in CI/CD Application Scan Overview.

Pipeline workflow file example for Jenkins:

```
pipeline {
  agent any
  stages {
    stage('build-run-scan') {
      environment {
        ACCESS_KEY = credentials('ACCESS_KEY')
        SECRET_KEY = credentials('SECRET_KEY')
      }
      steps {
        sh '''
        docker pull swaggerapi/petstore
        docker run -d -e SWAGGER_URL=http://petstore:8080 -e SWAGGER_BASE_
PATH=/v2 --name petstore swaggerapi/petstore
        docker pull tenable/was-scanner:latest
        docker run -v $(pwd):/scanner -t -e WAS_MODE=cicd -e ACCESS_
KEY=${ACCESS_KEY} -e SECRET_KEY=${SECRET_KEY} --link petstore tenable/was-
scanner:latest
        '''
      }
    }
```

```
  }
  post {
    always {
      sh '''
        docker rm $(docker stop $(docker ps -a -q --filter
ancestor="tenable/was-scanner:latest" --format="{{.ID}}")) || true
        docker rm $(docker stop $(docker ps -a -q --filter
ancestor="swaggerapi/petstore" --format="{{.ID}}")) || true
        docker system prune -f --volumes
        '''
        archiveArtifacts 'scanner.log'
        publishHTML([allowMissing: false, alwaysLinkToLastBuild: false,
keepAll: true, reportDir: '', reportFiles: 'tenable_was_scan.html',
reportName: 'WAS Report'])
        cleanWs()
    }
  }
}
```

Example integrations for CI/CD tools:

- Atlassian Bamboo
- CircleCI
- GitHub
- GitLab

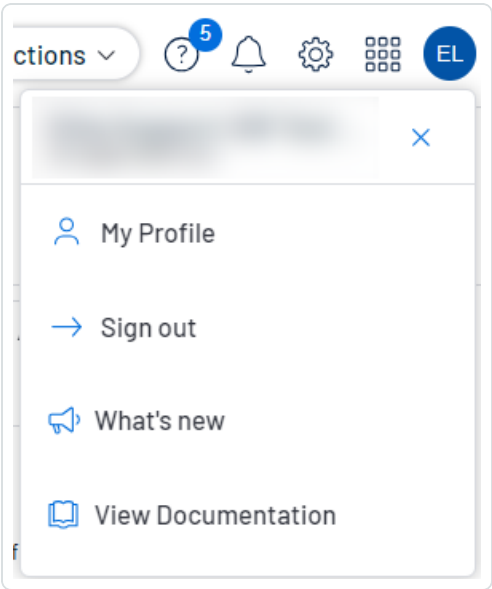
Log Out of Tenable Web App Scanning

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

To log out of Tenable Web App Scanning:

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

   The user account menu appears.



2. Click **Sign Out**.

Tenable Web App Scanning Dashboard

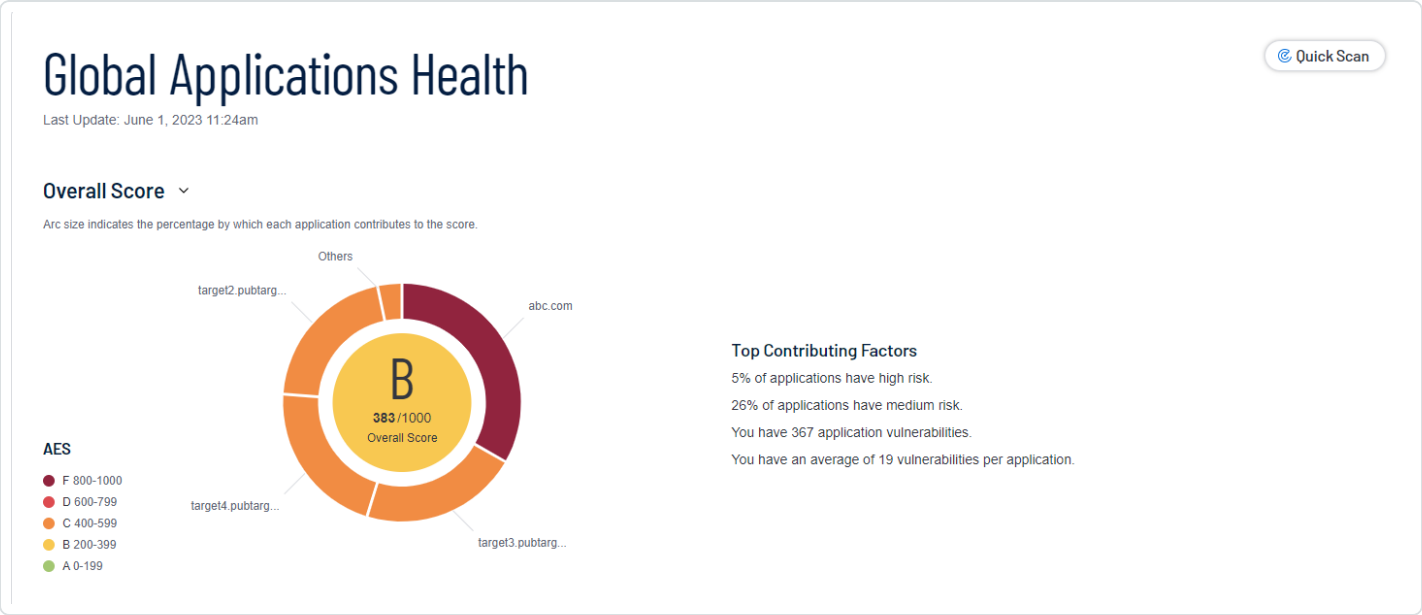
The default **Web Applications Scanning** dashboard shows the data that Tenable Web App Scanning collects.

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

Did You Know? Web Application Exposure: The average exposure score for all applications across WAS customers is 460.

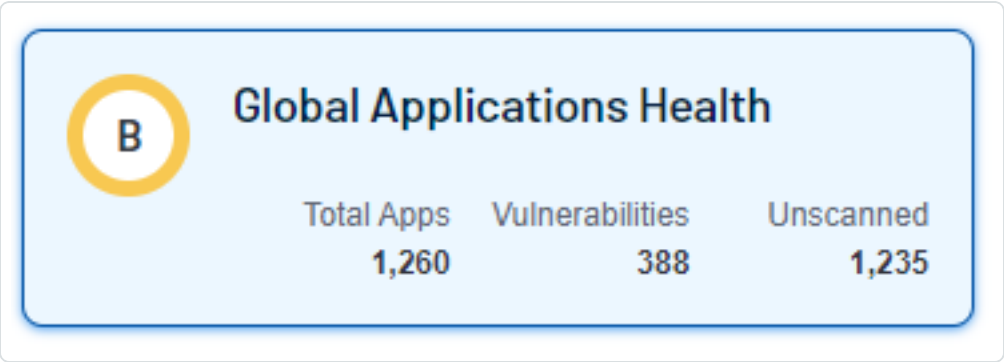
Tenable Web App Scanning uses several metrics to help you assess your risk:

- Overall Score
- Asset Exposure Score (AES)
- Top Contributing Factors
- Remediation
- Prevention



Tenable Web App Scanning Global Applications Health

The following tables describe the sections and widgets shown in the **Global Applications Health** section of the **Web Applications Scanning** dashboard. You can view details about the data in a widget by clicking the widget. The **Global Applications Health** widget in the left panel shows information for **Total Apps**, **Vulnerabilities**, and **Unscanned** applications:



Overall Score

The outer circle of the dashboard ring chart tracks the Asset Exposure Score (AES) of four of your scanned applications and a small **Other** segment of the remaining applications. You can click this segment to see the next four of your applications and their related details. Each segment's color changes along with the current AES score. The center of the dashboard ring chart shows your overall Cyber Exposure Score (CES) score and the color changes along with your current CES grade. For more information on your application details, see Findings.

Tip: Dashboard Ring Chart The inner circle represents the overall score across all applications (CES), while the outer ring represents individual application scores (AES). While the inner circle may appear healthy, you may have an unhealthy application appear in the outer ring.

Widget	Description
Overall Score	Number of findings Tenable Web App Scanning has discovered. Tenable Web App Scanning categorizes the findings by severity (**Critical** and **High**). For information about vulnerability ratings and the severity metrics Tenable uses to analyze risk, see Severity vs. VPR in the *Tenable Vulnerability Management User Guide*.
Web Applications Scanned	Number of applications scanned over time.

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

Asset Exposure Score (AES)

Tenable Web App Scanning calculates a dynamic AES for each application on your network to represent the application's relative exposure as an integer between zero and 1000. A higher AES indicates higher exposure.

Tenable Web App Scanning calculates AES based on the current ACR (Tenable-provided or custom) and the VPRs associated with the application.

AES Category	AES Range
High	650 to 1000
Medium	350 to 649
Low	0 to 349

Note: Asset Exposure Score (AES) is only available in Tenable Web App Scanning for customers with a valid Lumin license.

Top Contributing Factors

The list of top contributing factors in the right side of the user interface shows what severity classifications of scanned applications are present for your Tenable Web App Scanning instance. These items contribute to your overall scores. Investigate and address the following to help reduce your score:

- **% of applications have critical, high, medium, or low risk**
- **% of applications have critical, high, medium, or low risk**

- **You have (xyz amount) application vulnerabilities**
- **You have an average of (xyz amount) vulnerabilities per application**

> **Note:** Tenable Web App Scanning only shows four items in the list. The first two always show the two highest severity risks applications available. The last two contributing factor items are always present in the dashboard.

Manage Your Application Exposure

Remediation

Remediation metrics help with addressing and resolving critical vulnerabilities and unauthenticated scans across your web applications.

Widget	Description
Fix Critical Vulnerabilities	Number of findings Tenable Web App Scanning has discovered. Tenable Web App Scanning categorizes the findings by severity (**Critical** and **High**). For information about vulnerability ratings and the severity metrics Tenable uses to analyze risk, see Severity vs. VPR in the *Tenable Vulnerability Management User Guide*.
Address Incomplete Scans	Number of non-authenticated scans in the past 90 days. **Note:** Incomplete scans are scans whose status is either aborted, canceled, or partial failure.
Address Non-Authenticated Scans	Number of non-authenticated scans in the past 90 days.
Fix OWASP Top 10 Vulnerabilities	Number of non-authenticated scans in the past 90 days.

Prevention

Prevention metrics help with early identification and mitigation of potential vulnerabilities from unscanned applications and total findings in your scanned applications.

Widget	Description
Scan Unscanned Web Applications	Number of incomplete scans in the past 90 days.
Investigate Total Findings	Number of applications scanned over time.

Tenable Web App Scanning Statistics

The following table describes the widgets shown 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. Tenable Web App Scanning categorizes the findings by severity (**Critical** and **High**). For information about vulnerability ratings and the severity metrics Tenable uses to analyze risk, see Severity vs. VPR in the *Tenable Vulnerability Management User Guide*.
Web Assets Scanned	Number of assets scanned over time.
Incomplete Scans	Number of incomplete scans in the past 90 days.
Non-Authenticated Scans	Number of non-authenticated scans in the past 90 days.

OWASP Top 10

This chart shows 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.

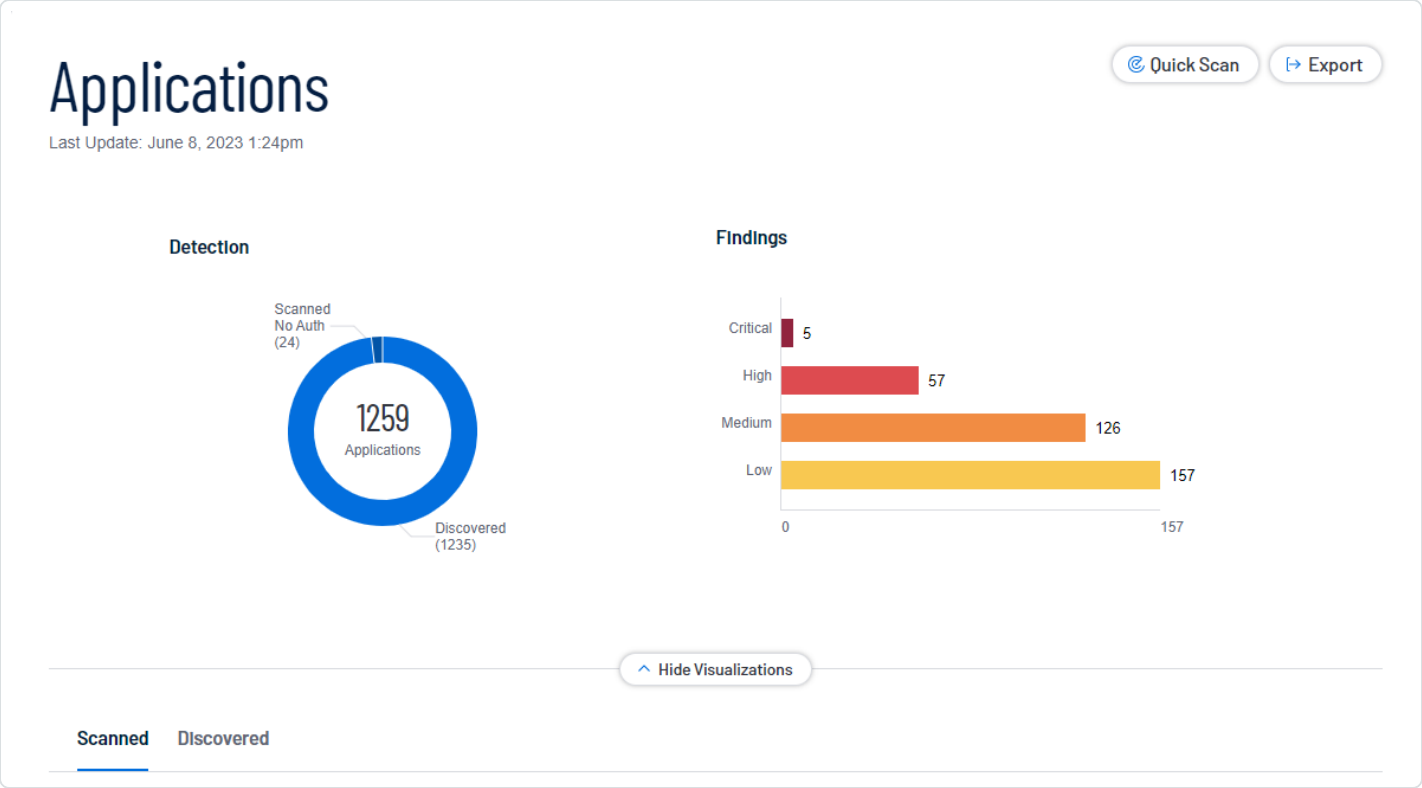
Next Steps

To view scores and details of specific applications, see the following pages:

- Scanned Applications
- Discovered Applications

Scanned Applications

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



On the **Applications** page, you can drill down to view only your **Scanned** applications. While on the **Scanned** applications tab, you can also export your scanned application assets. For more information, see Export Applications.

To view your scanned applications:

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

   The left navigation plane appears.

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

   The **Applications** page appears. By default, the **Scanned** tab is visible and applications visualizations are shown.

3. In the scanned applications table, you can perform any, or all, of the following actions by clicking the ⋮ button:

    - Export your asset.
    - Add a Tag to your asset.
    - Remove Tag from your asset.
    - Delete the asset from your list.

You can view basic information about your scanned applications in the following table.

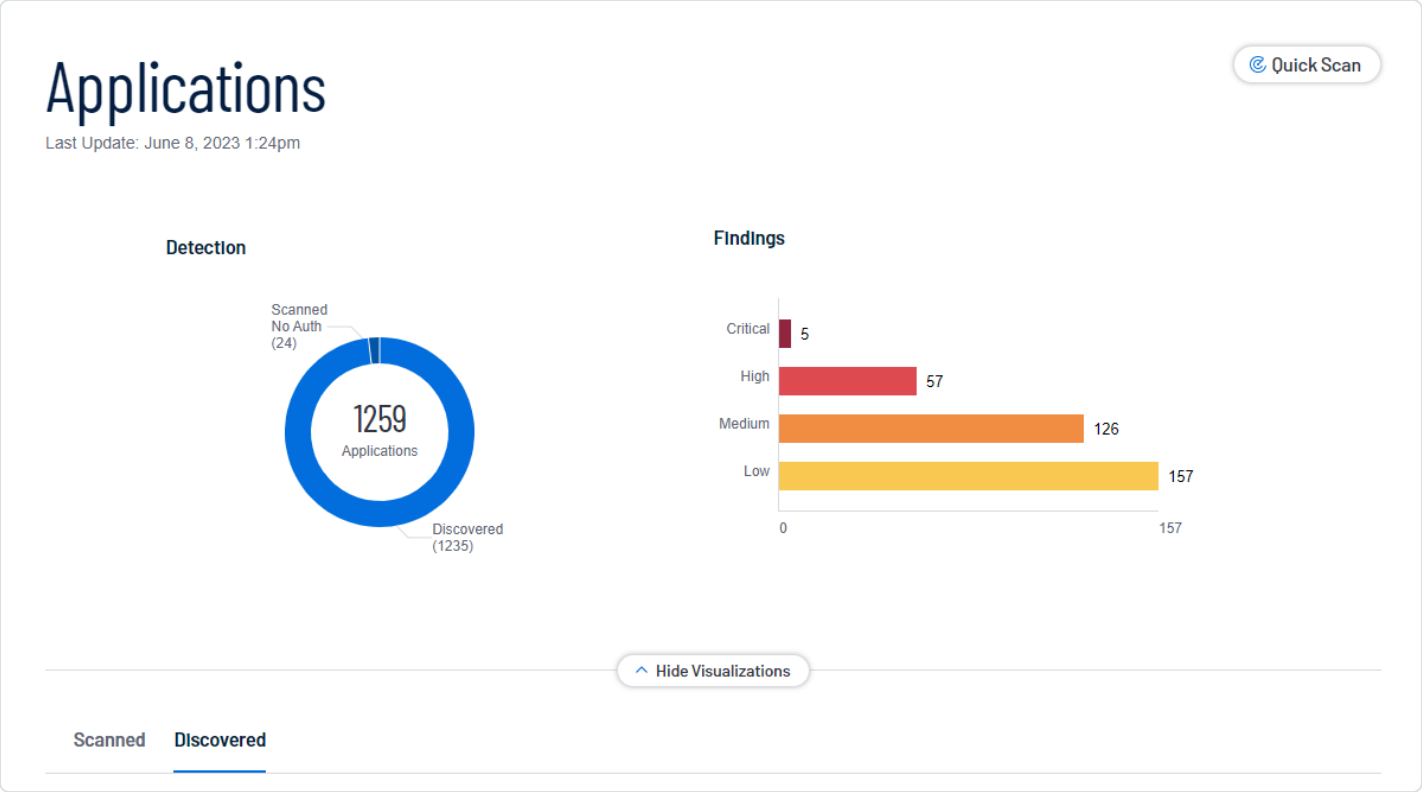
Filter	Description
ACR	(Requires Tenable Lumin license)The asset's ACR.
AES	(Requires Tenable Lumin license)The AES category of the AES calculated for the asset.
Application ID	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Web App Scanning.
Created Date	The time and date when Tenable Vulnerability Management created the asset record.
First Seen	The date when a scan first found the vulnerability on an application.
IPv4 Address	The IPv4 address for the affected asset. You can add up to 256 IP addresses to this filter.
Last Authenticated Scan	The date and time of the last authenticated scan run against the asset. An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field.
Last Licensed Scan	The time and date of the last scan that identified the asset as licensed. For more information about licensed assets, see License Information.
Last Scanned	The date and time at which the asset was last observed as part of a scan.
Last Seen	The date when a scan last found the vulnerability on an asset.
Licensed	Specifies whether the asset is included in the asset count for the Tenable Web App Scanning instance.

Name	The asset identifier that Tenable Web App Scanning assigns based on the presence of certain asset attributes in the following order: 1. Agent Name (if agent-scanned) 2. NetBIOS Name 3. FQDN 4. IPv6 address 5. IPv4 address For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.
Operating System	The operating system that a scan identified as installed on the asset.
Source	The source of the scan that identified the asset. Possible values are: • Agent (Tenable Nessus Agent) • Nessus (Tenable Nessus scan) • PVS/NNM (Tenable Nessus Network Monitor) • WAS (Tenable Web App Scanning) • AWS Connector • Azure Connector • GCP Connector • Qualys Connector
SSL/TLS	Specifies whether the application on which the asset is hosted uses SSL/TLS public-key encryption.
Tags	A unique filter that searches tag (category: value) pairs. When you type a tag value, you must use the *category: value* syntax, including the space after the colon (:). You can use commas (,) to separate values. If there is a comma in the tag name, insert a backslash (\) before the comma. You can add a maximum of 100 tags.

	For more information, see tags. **Note:** If your tag name includes double quotation marks (" "), you must use the UUID instead.
Updated Date	The time and date when a user last updated the asset.
Vulnerabilities	The number of vulnerabilities found on the scanned application.

Discovered Applications

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



On the **Applications** page, you can drill down to view only your **Discovered** applications.

To view your discovered applications:

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

   The left navigation plane appears.

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

   The **Applications** page appears. By default, the **Scanned** tab is visible and applications visualizations are shown.

3. In the lower-left, click **Discovered**.

   The **Discovered** applications list appears.

4. In the discovered applications assets table, you can perform any, or all, of the following actions by clicking the ⋮ button:

    - Create a Scan.
    - Add Tag to your finding.
    - Remove Tag from your finding.
    - Delete the finding from your list.

You can view basic information about your discovered applications in the following table.

Column	Description
Application ID	The UUID of the asset where a scan detected the vulnerability. This value is unique to Tenable Web App Scanning.
Created Date	The time and date when Tenable Vulnerability Management created the asset record.
Domain	The domain name for the asset.
DNS (FQDN) (ASM)	The fully qualified domain name of the asset host.
First Seen	The date when a scan first found the vulnerability on an application.
IP Address	The IP address for the asset, if any.
Host Name	The hostname for the asset.
Hosting Provider	The hosting provider for the asset.
Last Seen	The date when a scan last found the vulnerability on an asset.
Licensed	Specifies whether the asset is included in the asset count for 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: 1. Agent Name (if agent-scanned)

	2. NetBIOS Name 3. FQDN 4. IPv6 address 5. IPv4 address For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the asset name. This column appears in the table by default.
Port	The port associated with the asset.
Record Type	The type of asset.
Record Value	The value of the asset.
Source	The source of the scan that identified the asset. Possible values are: • Agent (Tenable Nessus Agent) • Nessus (Tenable Nessus scan) • PVS/NNM (Tenable Nessus Network Monitor) • WAS (Tenable Web App Scanning) • AWS Connector • Azure Connector • GCP Connector • Qualys Connector
Tags	A unique filter that searches tag (category: value) pairs. When you type a tag value, you must use the *category: value* syntax, including the space after the colon (*:*). You can use commas (,) to separate values. If there is a comma in the tag name, insert a backslash (\) before the comma. You can add a maximum of 100 tags.

	For more information, see tags. **Note:** If your tag name includes double quotation marks (" "), you must use the UUID instead.
Updated Date	The time and date when a user last updated the asset.
Vulnerabilities	The number of vulnerabilities found on the scanned application.

Export Application Assets

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

On the **Applications** 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 age out.

Note: You cannot export Domain Inventory assets.

Export Application Assets from the Applications Page

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

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

   The left navigation plane appears.

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

   The **Applications** page appears.

3. 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.

4. In the action bar, click ⇥ **Export**.

   The **Export** window appears.

5. (Optional) In the row for the finding, click the ⋮ button.

   The **Export** window appears.

6. In the **Export** window, 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 Web App Scanning 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 Web App Scanning 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 Web App Scanning 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 Web App Scanning 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 Web App Scanning may take several minutes to finish processing the export. When processing completes, Tenable Web App Scanning downloads the export file to your computer.

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

Export an Asset from the Applications Details Page

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

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

   The left navigation plane appears.

2. In the left navigation window, click **Applications**.

   The **Applications** page appears.

3. Click the application asset to export.

4. In the top-right corner, click [→ **Export**.

   The **Export** window appears.

5. In the **Export** window, 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 assets. **Note:** If your .csv export file includes a cell that begins with any

	of the following characters (=, +, -, @), Tenable Web App Scanning 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 Web App Scanning 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 Web App Scanning 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.

6. (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 Web App Scanning 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.

7. (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.

8. Click **Export**.

   Tenable Vulnerability Management downloads the export file to your computer. If you close the **Export** window 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 Web App Scanning User Role: Basic, Scan Operator, Standard, Scan Manager, or Administrator

When you delete an asset, Tenable Web App Scanning 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.

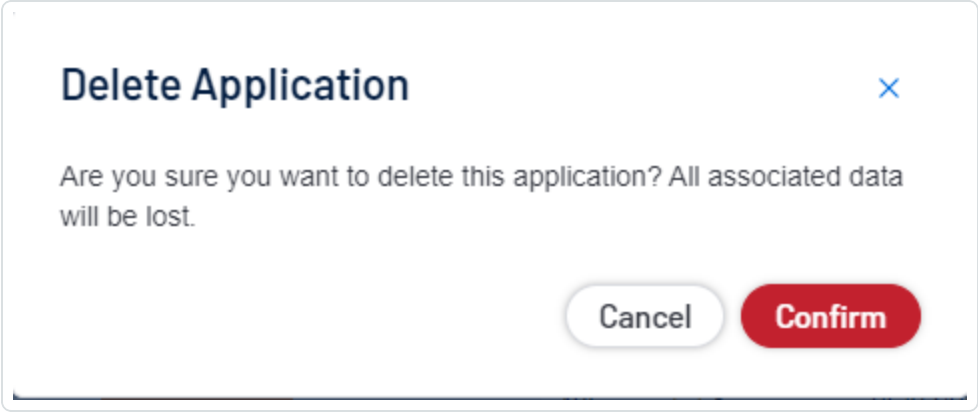
To delete a single asset:

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

   The left navigation plane appears.

2. Do one of the following:

Location	Action
Assets page	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	a. View the asset details. b. In the upper-right corner, click 🗑 **Delete**. A confirmation window appears.



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

   Tenable Web App Scanning deletes the asset.

To delete multiple assets:

> **Note**: Tenable Web App Scanning limits application deletion to 1,000 records at a time in the **Applications** table. If you select more than the 1,000 record limit (through individual selections or the **Select All Applications** 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:

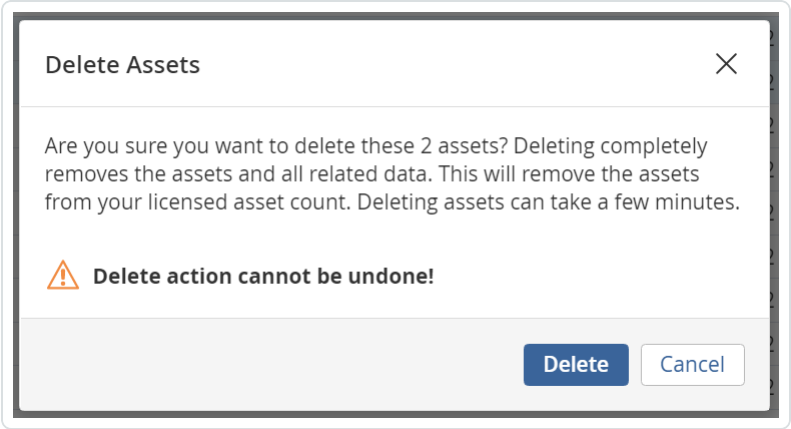
   - View your Scanned Applications.
   - View your Discovered Applications.

3. In the applications 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 Web App Scanning deletes the selected assets.

Applications Filter Search

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

In the **Applications** section, you can filter your organization's applications and findings on the **Scanned** and **Discovered** pages. For a list of available filters, see Discovered Applications or Scanned Applications.

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 **Applications** section:

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

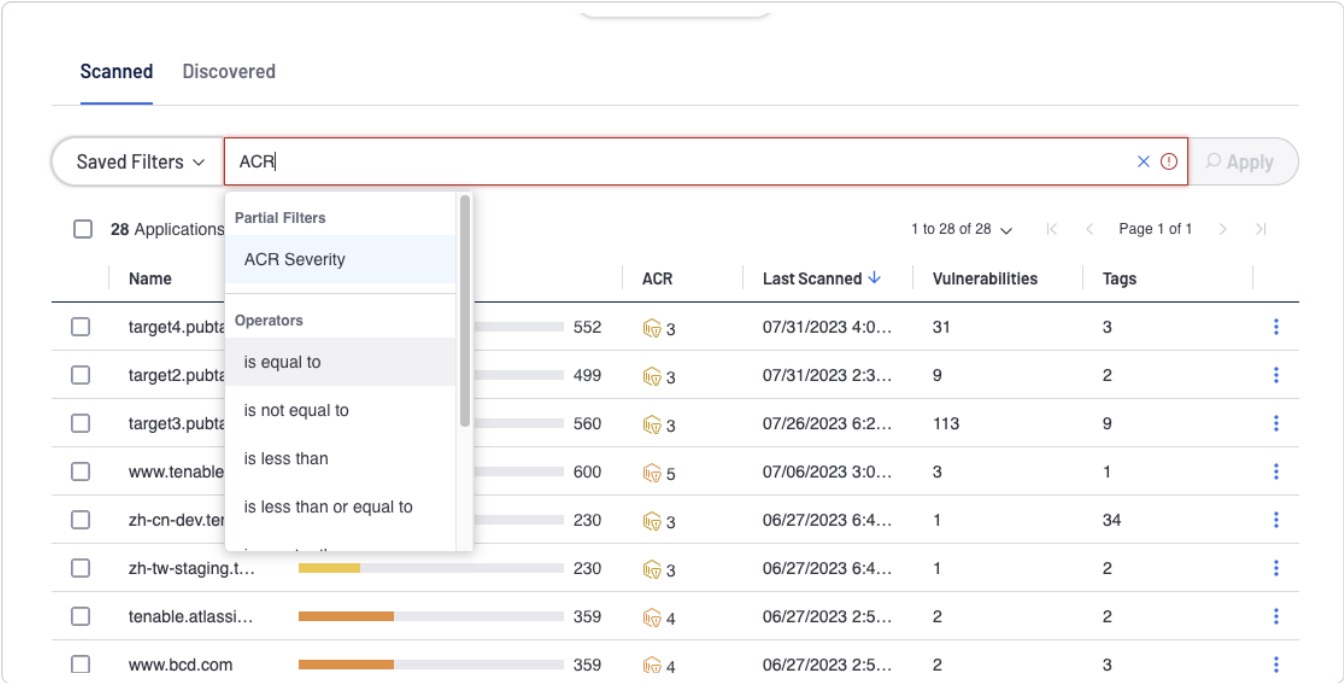
   The left navigation plane appears.

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

   The **Applications** page appears. By default, the **Scanned** tab is visible and applications visualizations are shown.

3. Above your list of applications, **click** in the search box.

A drop-down box appears with the current filters as shown in the following image:



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

4. In the drop-down box, select the **AND** or **OR** conditions or type them in the text box.
5. In the drop-down box, select a filter or type its name in the text box.
6. 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 (**"**).

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

Operator	Description
exists	Filters for items for which the selected filter exists.
does not exist	Filters for items for which the selected filter does not exist.

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

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

7. 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**.

8. (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.
9. Click **Apply**.

   Tenable Web App Scanning filters your data.
10. (Optional) Save the filters to access later or share with other team members.

> **Tip**: Tenable Web App Scanning 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 Web App Scanning 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.

View Application Details

Required Additional License: Tenable Web App Scanning

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, 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, click **Applications**.

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

3. (Optional) Refine the table data.

4. In the applications table, click the row for the application for which you want to see details.

   The **Application Details** page appears.

Tenable Web App Scanning Findings

Required Additional License: Tenable Web App Scanning

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

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

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.

Note: Tenable retains findings data for only 15 months.

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, click **Findings**.

   The **Findings** page appears, showing a table that lists your findings.

3. In the Findings table, you can perform any, or all, of the following actions by clicking the ⋮ button:

   - Accept your finding.
   - Export your finding.
   - View all findings of the selected type.

You can view basic information about your web application vulnerability findings in the following table. Some column options that you can display are hidden by default. You must add them to your display by selecting the **Columns** drop-down button and checking any additional options.

Column	Description
Application ID	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Web App Scanning.
Application Name	The name of the application where the scanner detected the vulnerability. This value is unique to Tenable Web App Scanning. This filter appears on the filter plane by default.
CVSSv2 Base Score	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
Family	The family of the plugin that identified the vulnerability. This column appears in the table by default.
First Seen	The date when a scan first found the vulnerability on an application.
ID	The UUID of the application where a scan detected the vulnerability. This value is unique to Tenable Web App Scanning.
IPv4 Address	The IPv4 address for the affected asset. You can add up to 256 IP addresses to this filter.
Last Seen	The date when a scan last found the vulnerability on an asset.
Last Updated	The date when a scan last found the vulnerability on an application. This column appears in the table by default.
Name	The name of the plugin that identified the vulnerability detected in the finding. This column appears in the table by default.
Plugin ID	The ID of the plugin that identified the vulnerability detected in the finding. This column appears in the table by default.
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR. This column appears in the table by default.

State	The state of the vulnerability. This column appears in the table by default.
VPR	The Vulnerability Priority Rating Tenable calculated for the vulnerability.

View Findings Details

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, 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.

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, click **Findings**.

   The **Findings** page appears, showing a table that lists your findings.

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

   The **Findings Details** page appears.

4. (Optional) In the upper-right corner, turn on **Include Info Severity** to list findings with info-level severity. This option is off by default. For more information on severity level, see Vulnerability Severity Indicators.

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

Section	Description
Description	A description of the Tenable plugin that identified the vulnerability detected in the finding.
Solution	A brief summary of how you can remediate the vulnerability detected in the finding. Only appears if an official solution is available.
See Also	Links to external websites that contain helpful information about the vulnerability detected in the finding.
Vulnerability Properties	Information about the vulnerability that the plugin identified, including: • **Severity** — The severity of the vulnerability.

	• **Exploitability** — Characteristics of the vulnerability that factor into its potential exploitability. • **Exploited With** — The most common ways that the vulnerability may be exploited. • **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.
Discovery	Information about when Tenable Web App Scanning first discovered the vulnerability, including: • **First Seen** — The date when a scan first found the vulnerability on an application. • **Last Seen** — The date when a scan last found the vulnerability on an application. • **Age** — The number of days since a scan first found the vulnerability on an application in your network.
VPR Key Drivers	VPR Key Drivers are the vulnerability and threat intelligence attributes that were significant factors in the calculation of the VPR: • **Threat Intensity** — The threat intensity based on the number and frequency of threat events (e.g., vulnerability and exploit activity on social media and the dark web) observed in recent weeks. • **Exploit Code Maturity** — Based on the availability of exploit code in various databases and frameworks such as Reversinglabs, Exploit-db, Metasploit, Canvas etc. • **Age of Vulnerability** — Number of days since the vulnerability was published on NVD. • **Product Coverage** — The relative number (low, medium, high, or very high) of unique products affected by the vulnerability.

	• **CVSSv3 Impact Score** — Impact Score provided by NVD or predicted by Tenable. • **Threat Sources** — A list of all sources (e.g., social media, dark web, etc.) where threat events (vulnerability and exploit activity) were observed in recent weeks.
Plugin Details	Information about the plugin that detected the vulnerability detected in the finding, including: • **Plugin ID** — The ID of the plugin that identified the vulnerability detected in the finding. • **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. • **Severity** — The severity of the plugin that identified the vulnerability.
Risk Information	Information about the relative risk that the vulnerability presents to the affected asset, including: • **Risk Factor** — The CVSS-based risk factor associated with the plugin. • **Risk Modified** — Indicates any action applied to modify the risk for the plugin. Can be Accept or Recast. • **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	A list of references to third-party information about the vulnerability, exploit, or update associated with 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, click **Findings**.

   The **Findings** page appears.

3. On the left side, select the check box 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.

   A drop-down box of options appears.

4. In the drop-down box, click [→ **Export**.

   The **Export** plane appears.

5. 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 Web App Scanning 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 Web App Scanning 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.

6. (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.

7. (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.

8. Click **Export**.

   Depending on the size of the export, Tenable Web App Scanning may take several minutes to finish processing the export. When processing completes, Tenable Web App Scanning 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, click **Findings**.

   The **Findings** page appears.

3. In the row, click the Finding.

   The **Finding Details** page appears.

4. In the top row, click [→ **Export**.

   The **Export** plane appears.

5. 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 Web App Scanning 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 Web App Scanning 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.

6. (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
7. (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.
8. Click **Export**.

    Tenable Web App Scanning 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**.

Generate a Report from Tenable Web App Scanning Findings

You can generate a report for one or more vulnerabilities from the **Findings** page.

To create a report from the **Findings** page:

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

   The left navigation plane appears.

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

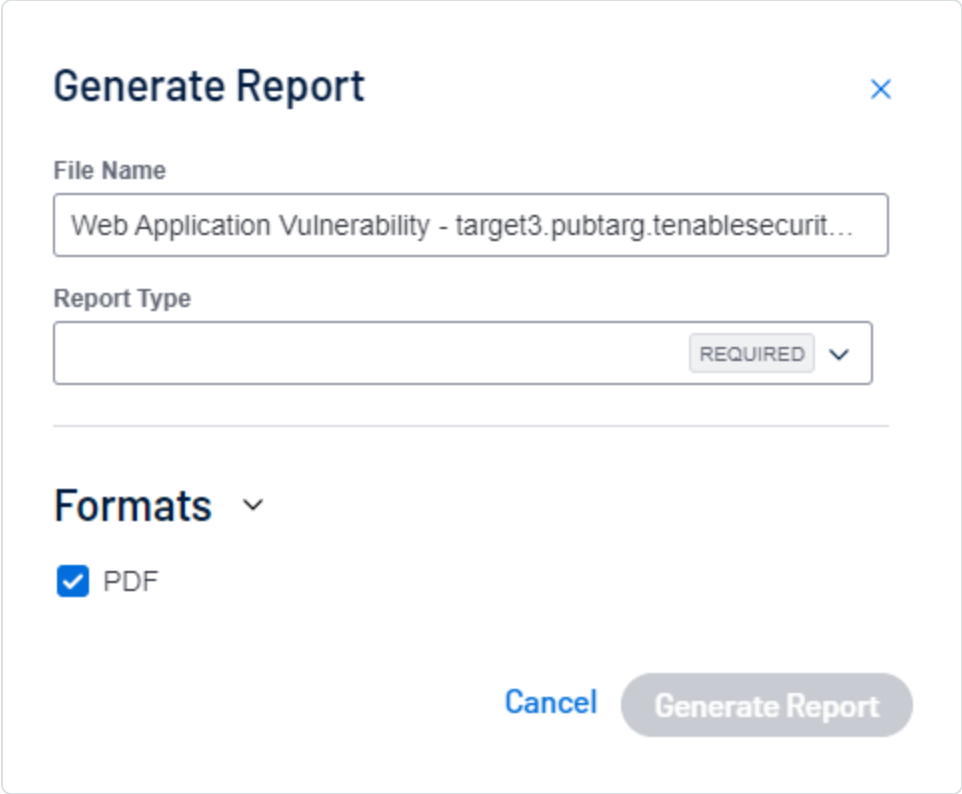
   The **Findings** page appears.

3. In the row, click the ⋮ button.

   A drop-down menu appears.

4. In the drop-down box, click [→ **Generate Report**.

   The **Generate Report** plane appears.



5. Select the findings for which you want to create a report.

Scope	Action
Create a report for a single vulnerability	Do one of the following: • In the **Actions** column, click the ⋮ button in the row for the vulnerability for which you want to create a report. The action options appear in the row.
Create a report for multiple vulnerabilities	Do one of the following: • Select more than one vulnerability for which you want to create a report. To select all vulnerabilities, select the check box at the top of the list. Tenable Web App Scanning enables the action bar.

6. Click **Generate Report**.

   The **Generate Report** pop-up appears.

7. (Optional) In the **Name** box, type a new name for the report.

8. From the **Report Type** drop-down box, select a report type.

Report Type
Web App Scanning Executive Findings Report
Web App Scanning Vulnerability Finding Details By Asset Report
Web App Scanning Vulnerability Finding Details By Plugin Report

9. (Optional) Click the **Schedule** toggle to enable scheduling of the report.

   The fields to schedule the report appear.

   - To schedule a report, modify the following settings:
     - In the **Start Date** and **Time** box, select when to schedule the report. The default is the current date and time.

- In the **Time Zone** box, select the required time zone or retain the default timezone.
- In the **Repeat** drop-down box, select frequency of report generation: **Daily**, **Weekly**, **Monthly**, **Custom**, or **Does not repeat**. The default is **Daily**.
- In the **Repeat Ends** drop-down box, select when you want the scheduling to end: **On** or **Never**. If you select **On**, specify a date in the **End Date** box for when you want the report scheduling to end.
- In the **Add Recipients** box, type the email addresses of the recipients to whom you want to send the report.

- Click **Schedule Report**.

  Tenable Web App Scanning schedules the report and displays a confirmation message.

10. Click **Generate Report**.

    Tenable Web App Scanning generates the report. In the notification message, you can click the **Report Results** link and view the new report on the **Report Results** page. The new report appears highlighted.

Launch a Remediation Scan

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

On the **Findings** page or the **Finding Details** page, you can create a remediation scan to run a follow-up scan against existing scan results. Remediation scans allow you to validate whether your vulnerability remediation actions on the scan targets have been successful. If a remediation scan cannot identify a vulnerability on targets where the vulnerability was previously identified, the system changes the status of the vulnerability to **Fixed**.

To launch a remediation scan in the 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 **Findings**.

   The **Findings** page appears.

3. In the row, click the ⋮ button.

   A drop-down menu appears.

4. In the drop-down box, click **Launch Remediation Scan**.

   The **Create Remediation Scan** configuration page appears.

   (Optional) You can also access the **Launch Remediation Scan** button in the **Findings Details** of a finding you select.

   Note: If your original scan configuration was for a multi-target scan, Tenable attempts to determine the correct target for remediation, but Tenable recommends that you double check the target and confirm.

   Note: The configuration page displays the same scan template settings used to create the original scan except for three items: A file under **Crawl Scripts** is created and used by the remediation scan process. The **Elements to Audit** section under **Assessment** which displays aspects of the plugin to be remediated. The configured plugins are also different,

> as only the plugin and related dependencies are enabled.

5. (Optional) Enter your scan information.
6. Click **Save** to save the scan setup, or click **Save and Run** to launch the scan.

   > **Note:** You may get an error displaying the note "Could not reproduce vulnerability page for remediation." This scan note indicates that the scanner could not replicate the page seen in the vulnerability data. To remediate this vulnerability, try rerunning the original scan.

   Tenable Web App Scanning launches the scan.

What to do next:

- In the **Remediation Scans** folder on the **Scans** page, do one of the following:
  - Edit the scan configuration.
  - Launch the scan.
- Once the scan completes:
  a. In the **Remediation Scans** folder, on the **Scans** page:
     - Verify that the finding does not appear in your completed remediation scan by clicking on it and reviewing the list of findings.

  b. On the **Findings** page:
     - Verify that the status for the selected vulnerabilities is now **Fixed** on the assets that the remediation scan targeted.

Remediation Scan Plugin Considerations

There are plugin types that are not supported in remediation scans, and plugin types that are full-scan remediation only. These are listed in the following tables:

List of non-remediable plugins:

These are plugins for which remediation scanning is not meaningful, or not currently supported.

Plugin Name	Plugin Number
OpenAPI Import Success	112569
OpenAPI Import Failed	112570
Allowed HTTP Versions	112613
API Detected	112616
Session Cookies Detected	112798
API Key Authentication Succeeded	113010
API Key Authentication Failed	113011
OpenAPI Import Failed	112570
Allowed HTTP Versions	112613
API Detected	112616
Session Cookies Detected	112798
API Key Authentication Succeeded	113010
API Key Authentication Failed	113011
OpenAPI Import Failed	112570
Allowed HTTP Versions	112613
API Detected	112616

Session Cookies Detected	112798
API Key Authentication Succeeded	113010
Bearer Token Authentication Succeeded	113012
Bearer Token Authentication Failed	113013
Basic Authentication Detected	113063
Kerberos Authentication Succeeded	113224
Kerberos Authentication Failed	113225
Client Certificate Authentication Succeeded	113329
Client Certificate Authentication Failed	113330
Performance Telemetry	113393
SOAP API Detected	114166
gRPC Detected	114167
Amazon Web Services Detected	114199
Google Cloud Platform Detected	114200
Microsoft Azure Detected	114201
Microsoft Entra ID Detected	114202
GraphQL Batching	114211
HTTP/2 Cleartext Upgrade Support Detected	114219
Serialized Data Detected	114224
Scan Information	98000
URI Blocked Due to Exclusion Rule	98007
Web Application Firewall Detected	98008
Web Application Sitemap	98009

Network Timeout Encountered	98019
HTTP Server Authentication Detected	98024
HTTP Server Authentication Succeeded	98025
HTTP Server Authentication Failed	98026
Login Form Authentication Failed	98034
Login Form Authentication Succeeded	98035
Scan Logged-out Intermittently	98043
Scan Aborted After Being Logged Out	98044
Allowed HTTP Methods	98047
Interesting Response	98050
Technologies Detected	98059
Cookies Collected	98061
DOM Elements Excluded	98111
Target Information	98136
Scan aborted after too many timeouts	98137
Screenshot	98138
Cookie Authentication Succeeded	98139
Cookie Authentication Failed	98140
Selenium Authentication Succeeded	98141
Selenium Authentication Failed	98142
Selenium Crawl Succeeded	98143
Selenium Crawl Failed	98145
External URLs	98154

Error Message	98611
Basic Authentication Without HTTPS	98615
Fetch/XHR Detected	98772

Full-scan remediation plugins:

A full crawl of the application is performed for these plugins rather than the specific vulnerability page replicated. It may take longer for this form of remediation scan to run.

Plugin Number	Plugin Name
HTTP to HTTPS Redirect Not Enabled	112544
Full Path Disclosure	112550
JSON Web Token Weak Secret	112697
API Versions Detected	112714
Microsoft FrontPage Insecure Extension Configuration	112772
GraphQL Detected	112809
GraphQL Introspection Enabled	112894
GraphQL Field Suggestions Detected	112895
Power Apps OData Feeds Detected	112949
Magento Administration Panel Login Form Bruteforced	113117
Magento Connect Manager Bruteforced	113118
Joomla Administration Panel Login Form Bruteforced	113133
Wordpress Administration Panel Login Form Bruteforced	113136
Drupal Administration Panel Login Form Bruteforced	113137
Weblogic Console Login Form Bruteforced	113138

OpenAPI Unencrypted Traffic Allowed	113143
Google Cloud Service Account Private Key Disclosure	113150
AWS Credentials Disclosure	113164
Apache mod_negotiation Alternative Filename Disclosure	113165
Stored Cross-Site Scripting (XSS)	113250
Login Form Cross-Site Request Forgery	113332
Web Cache Poisoning	113338
ASP.NET ViewState Remote Code Execution	113340
Amazon Cognito User Enumeration	113371
Amazon Cognito Insecure Permissions	113374
SQL Statement Disclosure	113555
External Backend API Detected	114128
Bearer Token Authentication Detected	114136
NTLM Authentication Detected	114137
Digest Authentication Detected	114138
Private IP Address Disclosure	98077
E-mail Address Disclosure	98078
Missing Subresource Integrity	98647
Invalid Subresource Integrity	98649
Source Code Passive Disclosure	98779

Create Recast/Accept Rules in Findings

In Tenable Web App Scanning, 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 in the Findings page.

> **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 in the *Tenable Vulnerability Management User Guide*.

Create a Recast Rule in Findings

To create a Recast rule:

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

   The left navigation plane appears.

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

   The **Findings** page appears.

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

   A drop-down menu appears.

4. Click **Recast**.

   The **Recast** plane appears.

5. Complete the following options:

   a. **New Severity** – Select the desired severity level for the vulnerability.

   b. **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.

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**: You can only specify 1000 comma-separated custom entries. If you want to target a larger number of custom entries, create multiple rules.

d. (Optional) **Expires** – Select when you want the rule to age out.

e. (Optional) **Comments** – Type a description of the rule. This option is only visible when the rule is modified.

6. Click **Save**.

   Tenable Web App Scanning 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 Web App Scanning 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 click **Findings**.

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

   A drop-down menu appears.

4. Click **Accept**.

   The **Accept Risk** window appears.

5. Complete the following options:

a. **Targets** – Select **All** to target all assets or **Custom** to specify targets that you want the rule to run against.

b. **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**: You can only specify 1000 comma-separated custom entries. If you want to target a larger number of custom entries, create multiple rules.

c. (Optional) **Expires** – Select when you want the rule to age out.

d. (Optional) **Comments** – Type a description of the rule. This option is only visible when the rule is modified.

6. (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.

7. Click **Save**.

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

Vulnerability Severity Indicators

Tenable assigns all vulnerabilities a severity (**Info**, **Low**, **Medium**, **High**, or **Critical**) based on the vulnerability's static CVSSv2 score

The Tenable Web App Scanning interface uses different icons for each severity category and accepted or recasted status. For more information on recasting, see Create Recast Rules in Findings.

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

Vulnerability States

Tenable assigns a vulnerability state to all vulnerabilities detected on your network. You can track and filter by vulnerability state to see the detection, resolution, and reappearance of vulnerabilities over time.

Vulnerability State Tracking Now Available As of January 2024, new, or additional scans run on your assets with existing vulnerabilities may result in remediated vulnerabilities. Users can expect to see this change in the Tenable Web App Scanning and the Tenable Vulnerability Management Explore workbench. While no action is required, Tenable recommends you run one or more scans to see these updates.

Note: This feature is currently not available in Tenable Web App Scanning FedRAMP Moderate.

Note: If you filter vulnerabilities using the **Active** state, Tenable Web App Scanning also returns vulnerabilities in the **New** state. For filtering purposes, **New** is a sub-category of **Active**.

Vulnerability State	Visibility	Description
New	Visible in dashboards	On the Explore page, **New** indicates that Tenable Web App Scanning detected the vulnerability one time. On the vulnerability assets and findings tabs, **New** indicates that Tenable Web App Scanning detected the vulnerability one time or multiple times up to 14 days after the original detection.
Active	Visible in dashboards	On the Explore page, **Active** indicates that Tenable Web App Scanning detected the vulnerability more than one time. On the vulnerability assets and findings tabs, **Active** indicates that Tenable Web App Scanning detected the vulnerability more than one time, and that the first detection occurred more than 14 days ago.
Fixed	Hidden in dashboards, but visible with	The vulnerability was present on a host, but is no longer present.

Vulnerability State	Visibility	Description
	filters	
Resurfaced	Visible in dashboards	The vulnerability was previously marked as fixed on a host, but Tenable Web App Scanning detected it again. When a vulnerability is **Resurfaced**, it remains in this state until: • A later scan identifies the vulnerability as remediated, at which point the vulnerability returns to a **Fixed** state.

Findings Filters

On the **Findings** page, you can view analytics.

Web Application Findings Filters

Column	Description
Application ID	The UUID of the asset where a scan detected the finding. This value is unique to Tenable Web App Scanning.
Application Name	The name of the application where the scanner detected the vulnerability. This value is unique to Tenable Web App Scanning. This filter appears on the filter plane by default.
CVSSv2 Base Score	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
Family	The family of the plugin that identified the vulnerability. This column appears in the table by default.
First Seen	The date when a scan first found the vulnerability on an application.
IPv4 Address	The IPv4 address for the affected asset. You can add up to 256 IP addresses to this filter.
Last Seen	The date when a scan last found the vulnerability on an asset.
Last Updated	The date when a scan last found the vulnerability on an application. This column appears in the table by default.
Plugin Name	The name of the plugin that identified the vulnerability detected in the finding. This column appears in the table by default.
Plugin ID	The ID of the plugin that identified the vulnerability detected in the finding. This column appears in the table by default.
Severity	The vulnerability's CVSS-based severity. For more information, see CVSS vs. VPR.

	This column appears in the table by default.
State	The state of the vulnerability. This column appears in the table by default.
VPR	The Vulnerability Priority RatingTenable calculated for the vulnerability.

Group Your Findings

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

	findings.
Plugin	
Severity	The CVSS-based severity score identified on each set of grouped findings. For more information, see CVSS vs. VPR.
Name	The name of the plugin that identified the vulnerability.
Family	The family of the plugin that identified the vulnerability.
CVSSv2 Base Score	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments). **Note:** Based on your severity metric settings, this parameter may display CVSSv3 base scores. For more information, see General Settings.
Plugin ID	The ID of the plugin that identified the vulnerability.
Asset Count	The number of assets that Tenable Vulnerability Management identified on each set of grouped findings.
Vuln Count	The number of vulnerabilities that Tenable Vulnerability Management identified on each set of grouped findings.
Actions	The actions you can perform with each set of grouped findings.

5. (Optional) Refine the table data. For more information, see Tenable Web App Scanning 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.

Tenable Web App Scanning Scan Workflow

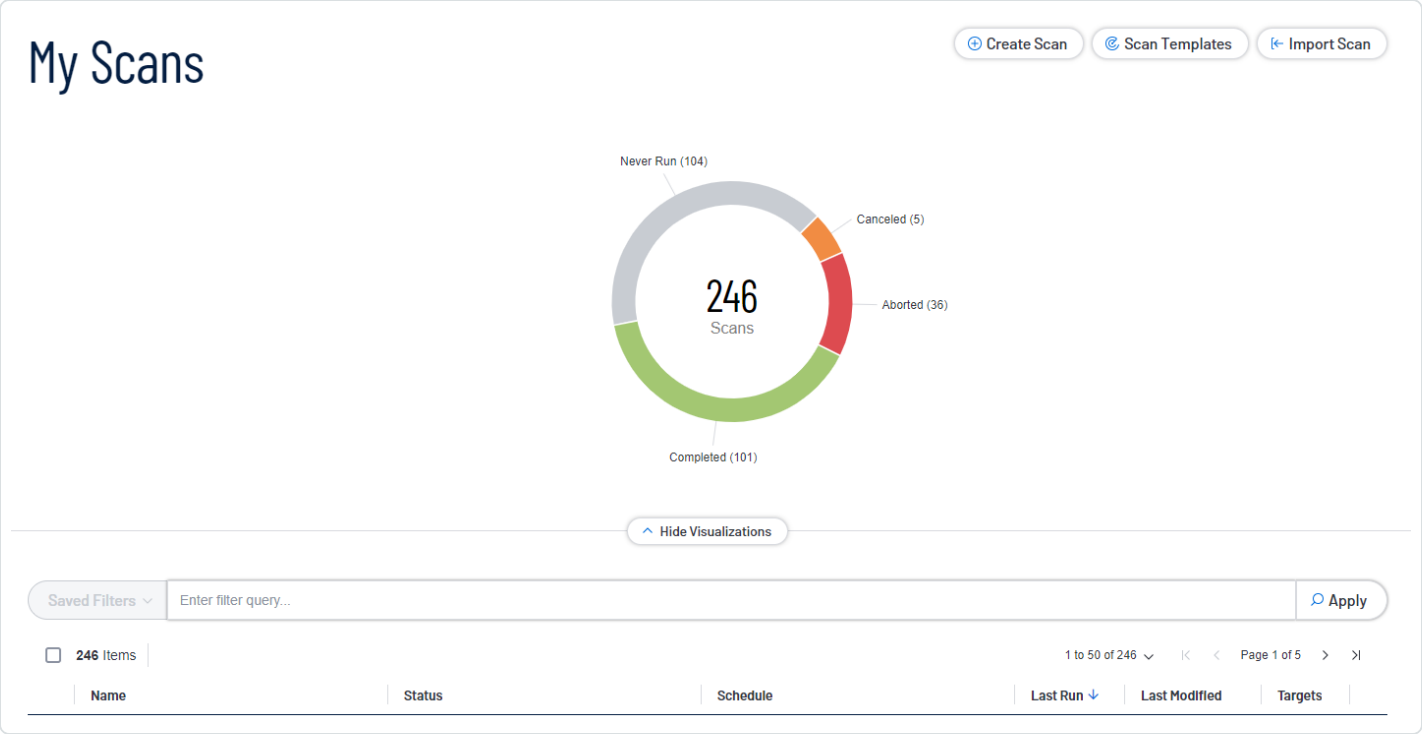
Configure web application scans to collect data about your web applications for analysis. This overview walks you through the main steps you need to create, configure, launch, and manage Tenable Web App Scanning scans. Depending on your organization, one person may perform all of the steps, or several people may share the steps.

Vulnerability State Tracking Now Available As of August 2023, new or additional scans run on your assets with existing vulnerabilities may result in remediated vulnerabilities. Users can expect to see this change in the Tenable Web App Scanning and the Tenable Vulnerability Management Explore workbench. While no action is required, Tenable recommends you run one or more scans to see these updates.

Did You Know? Scanning: 65% of WAS customers prefer to run a Quick Scan.

My Scans

The **My Scans** page shows your total number of scans and visualization widgets for several categories of scan statuses: **Never Run**, **Canceled**, **Aborted**, **Completed**. These visualizations can be hidden, and unhidden, by clicking the **Hide Visualizations** (or **Show Visualizations**) button. For more information, see Scan Status.



Tip: My Scans Ring Chart You can **click** on a segment of the ring chart to filter by that status. To deselect a segment, **click** on the selected segment a second time.

View your My Scans page

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. On your **My Scans** page, you can perform any, or all, of the following actions to your scan by clicking the ⋮ button:

   - Edit
   - Launch
   - Move
   - Copy
   - Trash

   Note: Not all scan actions are available for all scans in your list. For example, a scan that is tagged as **imported** only has **Move** and **Trash** actions.

Next steps:

- Create and Launch a Scan
- View your Applications Dashboard
- View your Findings
- View your Settings

Create and Launch a Scan

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

Vulnerability State Tracking Now Available As of August 2023, new or additional scans run on your assets with existing vulnerabilities may result in remediated vulnerabilities. Users can expect to see this change in the Tenable Web App Scanning and the Tenable Vulnerability Management Explore workbench. While no action is required, Tenable recommends you run one or more scans to see these updates.

To create a scan in the 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, click the ⋮ button for the scan you want to launch.

     b. On the right side of the row, click the ▷ **Launch** 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 one or more check boxes next to the scans you want to launch.

     The action bar appears at the top of the page.

     b. In the action bar, click the ▷ **Launch** 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. 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.

Scan Types in Tenable Web App Scanning

Scan types in Tenable Web App Scanning scans are available to help you quickly start your scans with the appropriate level of options.

Did You Know? Scanning: 65% of WAS customers prefer to run a Quick Scan.

Scan Types

Types	Description	Scan Duration
Quick Scan	Quick overview scan that discovers up to 70% of vulnerabilities. This scan focuses on configuration issues related to SSL/TLS and HTTP security headers. This scan type is available for launch via a button on most pages in your Tenable Web App Scanning user interface.	Three minutes or less
Basic Scan	Normal scan that crawls the entire application and discovers up to 85% of vulnerabilities. This scan focuses on the misconfigurations and the component vulnerabilities.	Under an hour
Full Scan	Comprehensive scan that crawls the entire application and discovers all known vulnerabilities. This scan focuses on the misconfigurations, the component vulnerabilities, and the common generic vulnerabilities.	A few hours
Custom Scan	Control all settings and choose the plugins you want to run.	Variable

Note: Each scan type (and scan template) supports families of plugins and individual plugins. For more information, see View Your Scan Plugins.

Set Scan Permissions

Required Additional License: Tenable Web App Scanning

Required User Role: Administrator

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

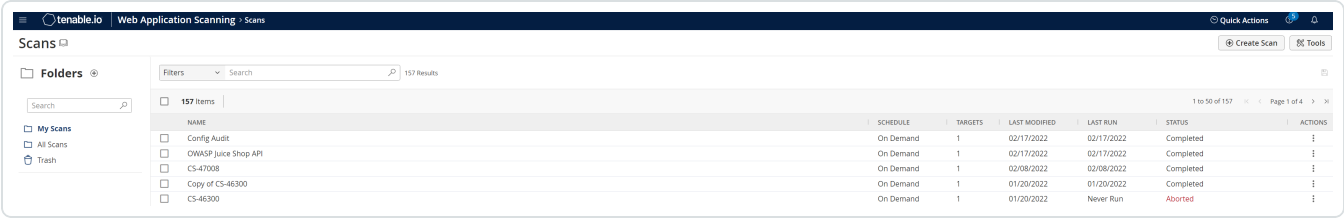
To add permissions:

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



   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:

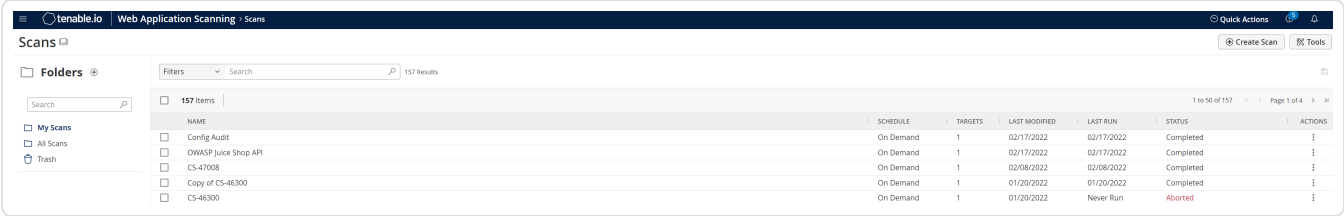
> **Note**: You cannot update permissions for the user that owns the scan.

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



> **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	• 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.

Edit Scan Settings

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

Required Scan Permissions: Can Configure

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 Tenable Web App Scanning Scan Template Settings.

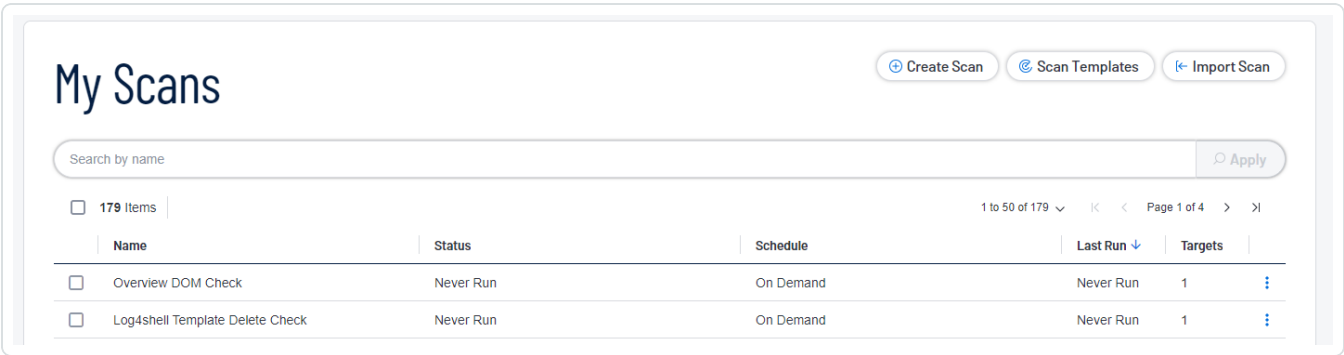
To configure scan settings in the new interface:

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

   The left navigation plane appears.

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

   The Tenable Web App Scanning **My Scans** page appears:



3. In the list, click the ⋮ button for the scan you want to edit.

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 Web App Scanning saves the scan settings.

Launch an API Scan

Required Additional License: Tenable Web App Scanning

Required Tenable Web App Scanning User Role: Scan Operator, Standard, 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**: Attaching an OpenAPI (Swagger) file larger than 1 MB to an API scan, results in an error message. For more information on this limit, see the Knowledge Article. 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 Template 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.

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 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. If you want to modify these settings for individual scans, create individual scans based on a Tenable-provided template instead.

  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

- 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-Provided Tenable Web App Scanning Template Types

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

> **Note:** Each scan type (and template) supports families of plugins and individual plugins. For more information, see View Your Scan Plugins.

Tenable Web App Scanning provides the following scanner templates.

Template	Description
API	A scan that checks an API for vulnerabilities. This scan analyzes RESTful APIs described via an OpenAPI (Swagger) specification file. File attachment size is limited to 1 MB. **Tip:** If the API you want to scan requires keys or a token for authentication, you can add the expected custom headers in the Advanced settings in the **HTTP Settings** section. **Note:** The API scan template is available as a public beta. Its functionality is subject to change as ongoing improvements are made throughout the beta period. **Note:** API scans support only one target at a time. **Note:** Attaching an OpenAPI (Swagger) file larger than 1 MB to an API scan, results in an error message. For more information on this limit, see the Knowledge Article. For more information on Swagger specification files. see OpenAPI (Swagger) Specification.
Config Audit	A high-level scan that analyzes HTTP security headers and other externally facing configurations on a web application to determine if the application is compliant with common security industry standards. If you create a scan using the **Config Audit** scan template, Tenable Web App Scanning analyzes your web application only for plugins related to security industry standards compliance.
Log4Shell	Detects the Log4Shell vulnerability (CVE-2021-44228) in Apache Log4j via local checks.

Overview	A high-level preliminary scan that determines which URLs in a web application Tenable Web App Scanning scans by default. The **Overview** scan template does not analyze the web application for active vulnerabilities. Therefore, this scan template does not offer as many plugin family options as the **Scan** template. **Note**: This scan template is equivalent to the **Web App Overview** template in the classic Tenable Web App Scanning interface.
PCI	A scan that assesses web applications for compliance with Payment Card Industry Data Security Standards (PCI DSS) for Tenable PCI ASV. (This scan also allows you to view and edit the **Request Redirect Limit**. The default value for this limit is 3.)
Quick Scan	A high-level scan similar to the **Config Audit** scan template that analyzes HTTP security headers and other externally facing configurations on a web application to determine if the application is compliant with common security industry standards. Does not include scheduling. If you create a scan using the **Quick Scan** scan template, Tenable Web App Scanning analyzes your web application only for plugins related to security industry standards compliance.
Scan	A comprehensive scan that assesses web applications for a wide range of vulnerabilities. The **Scan** template provides plugin family options for all active web application plugins. If you create a scan using the **Scan** template, Tenable Web App Scanning analyzes your web application for all plugins that the scanner checks for when you create a scan using the **Config Audit**, **Overview**, or **SSL TLS** templates, as well as additional plugins to detect specific vulnerabilities. A scan run with this scan template provides a more detailed assessment of a web application and take longer to complete that other Tenable Web App Scanning scans.

	Note: This scan template is equivalent to the **Web App Scan** template in the classic Tenable Web App Scanning interface.
SSL TLS	A scan to determine if a web application uses SSL/TLS public-key encryption and, if so, how the encryption is configured. When you create a scan using the **SSL TLS** template, Tenable Web App Scanning analyzes your web application only for plugins related to SSL/TLS implementation. The scanner does not crawl URLs or assess individual pages for vulnerabilities.

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 Web App Scanning 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.

View Your Scan Plugins

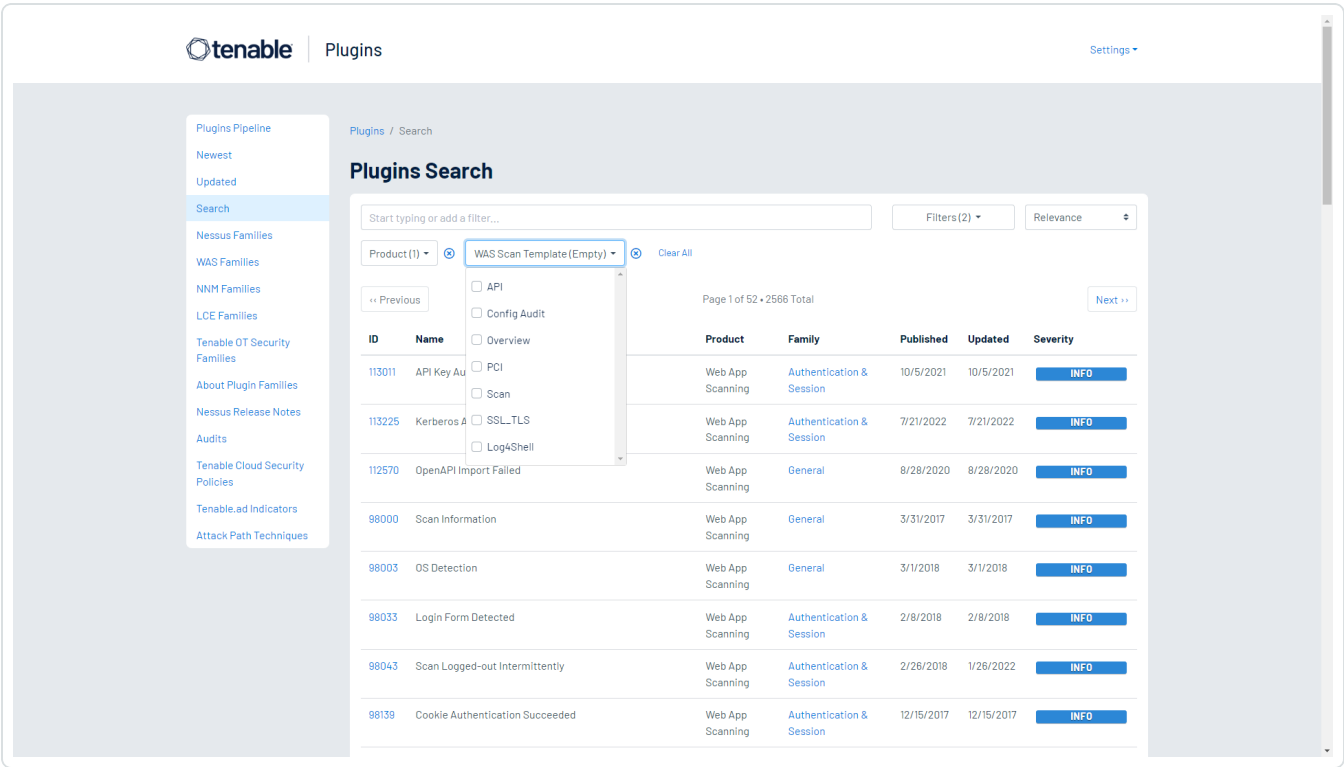
You can view the Tenable Web App Scanning plugins and plugin families your scan templates and scan types are using by viewing the Web App Scanning Plugin Families page in the Tenable Plugins Pipeline.

To view your current scan plugins, use one of the following two methods:

Using the Search Box

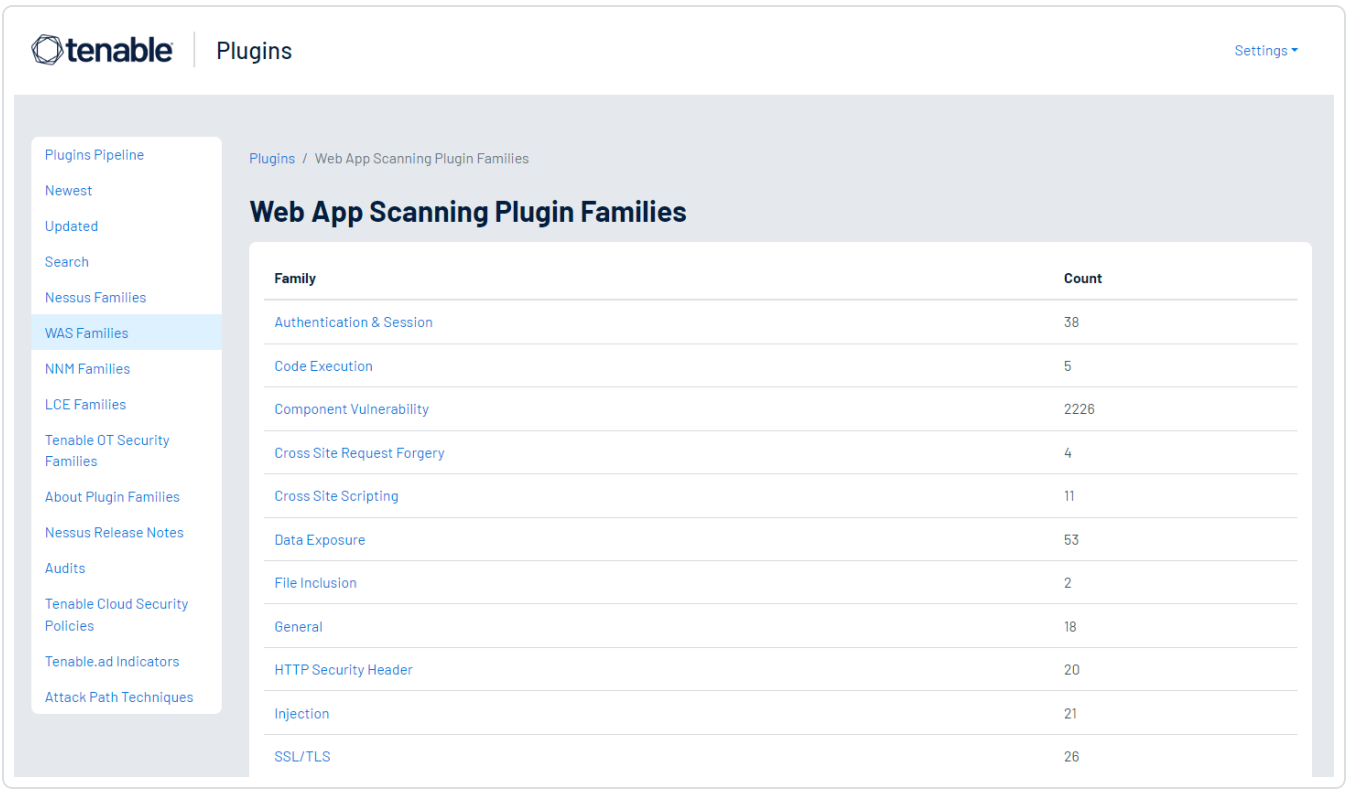
1. Go to the Web App Scanning Plugin Families page.
2. In the left-side navigation, click **Search**.

   The **Plugins Search** page appears.
3. In the **Add Filter** box, select **Product**, and choose **Web App Scanning**.
4. In the **Add Filter** box, select **WAS Scan Template**, then select the template you want.
5. All plugins with the selected template are displayed:

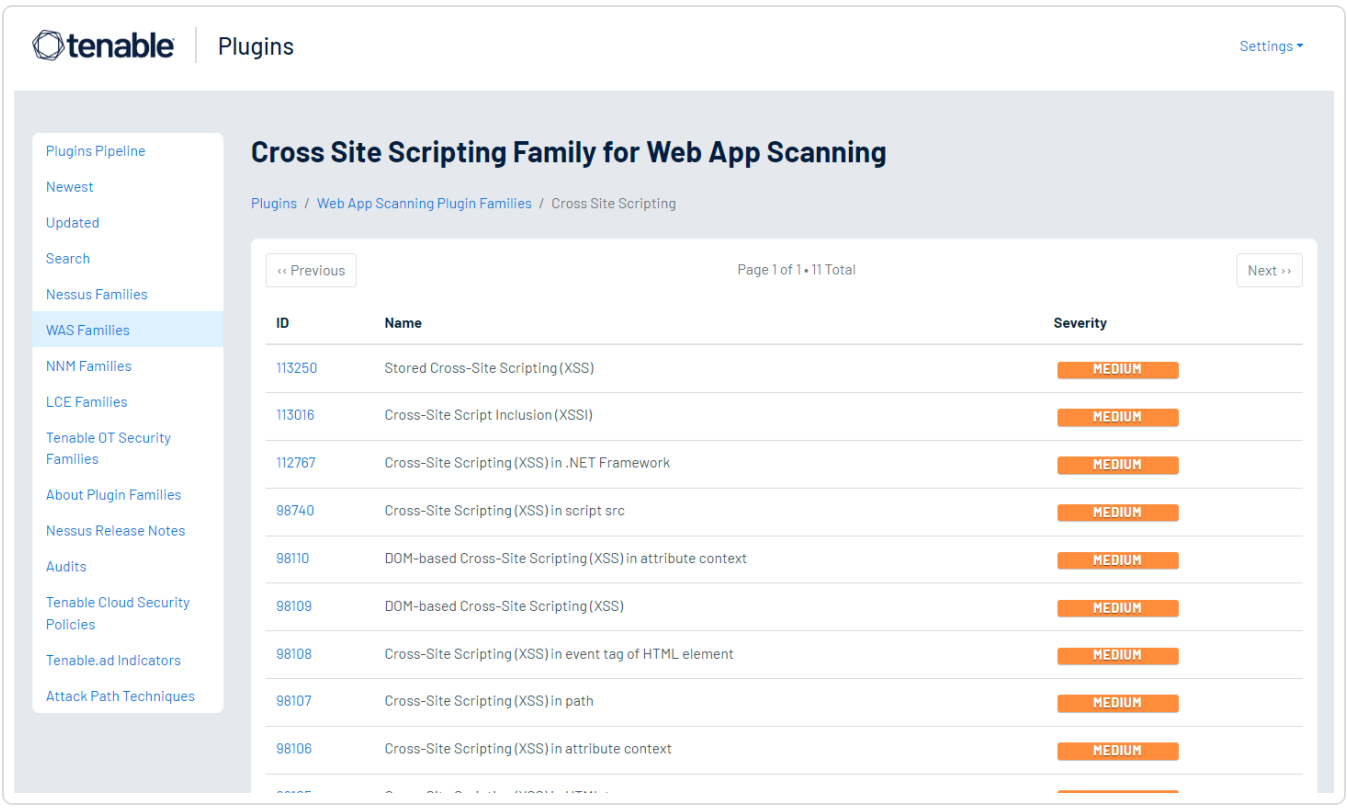


Navigate Plugins and Plugin Families

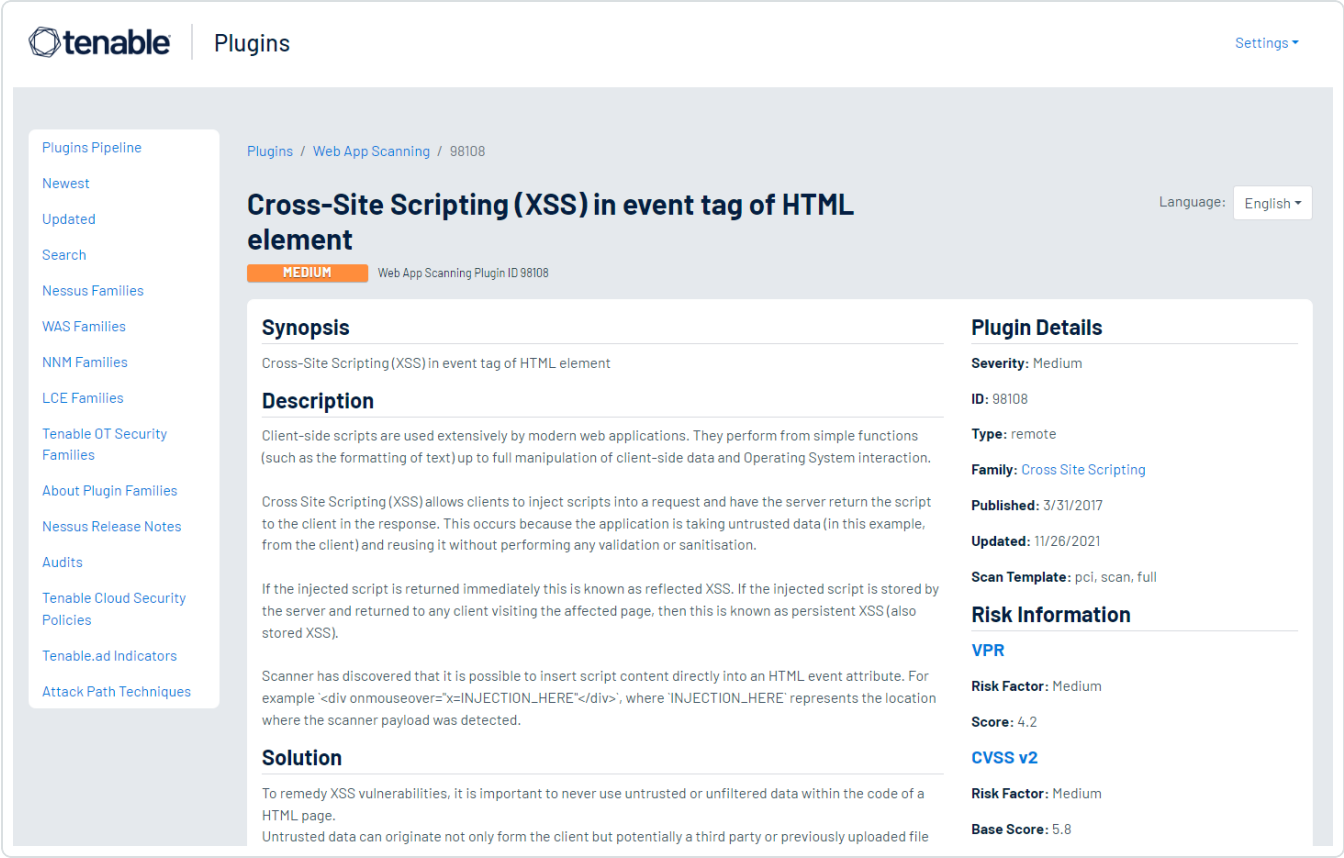
1. Go to the Web App Scanning Plugin Families page.



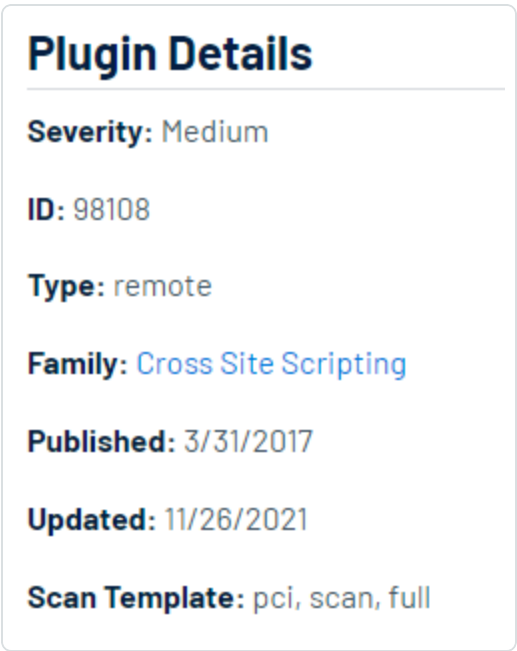
2. Select a family to display the list of its plugins.



3. Select a specific plugin **ID** to display the plugin output that displays as seen in a report.



4. In the upper-right of the plugin information, view the **Plugin Details** and the scan types and templates listed next to **Scan Template**:



Note: You can configure **Plugin** settings when you create a scan or user-defined scan template and select the **API**, **Overview**, **(Basic) Scan**, **Standard Scan**, or **Custom** template or scan type. For more information, see Plugin Settings in Tenable Web App Scanning Scans.

Basic Settings in Tenable Web App Scanning Scans

Configure **settings** to specify basic organizational and security-related aspects of your scan configuration. This includes specifying the name of the scan, 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
		Caution: When removing targets from a Tenable Web App Scanning scan (for example, going from two, or more, targets down to one target), the scan must be re-launched before any exports can be delivered. **Note**: If the URL you type in the **Target** box has a different FQDN host from the URL that appears on your license, and your scan runs successfully, the new URL you type counts as an additional asset on your license. **Note**: If you create a user-defined scan template, the target setting is not saved to the template. Type a target each time you create a new scan.	
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. Configure the schedule settings each time you create a new scan.

Setting	Default	Description
Schedule	off	A toggle that specifies whether the scan is scheduled. By default, scans are not scheduled. When the **Schedule** toggle is disabled, the other schedule settings remain hidden. Click the toggle to enable the schedule and view the remaining **Schedule** settings.

Frequency	Once	Specifies how often the scan is launched.
		
		Note: The frequency with which you scan your target depends on several factors (e.g., how often you update your web application, the content your web application contains, etc.). For most web applications, Tenable recommends at least monthly scans.
		
		• **Once**: Schedule the scan at a specific time.
		• **Daily**: Schedule the scan to occur on a daily basis, at a specific time, up to 20 days.
		• **Weekly**: Schedule the scan to occur on a recurring basis, by time and day of week, up to 20 weeks.
		• **Monthly**: Schedule the scan to occur every 1-20 months, by:
		  • **Day of Month**: The scan repeats on a specific day of the month at the selected time.
		  • **Week of Month**: The scan repeats monthly on the week you begin the scan. For example, if you select a start date of October 3rd, and that falls on the first week of the month, then the scan repeats the first week of each subsequent month at the selected time.
		
		Note: If you schedule your scan to recur monthly and by

Setting	Default	Description
		time and day of the month, Tenable recommends setting a start date no later than the 28th day. If you select a start date that does not exist in some months (e.g., the 29th), Tenable Vulnerability Management cannot run the scan on those days. • **Yearly**: Schedule the scan to occur every year, by time and day, up to 20 years.
Starts	varies	Specifies the exact date and time at which a scan launches. **Note**: If you schedule an excessive number of scans to run concurrently, you may exhaust the scanning capacity on Tenable Web App Scanning. If necessary, Tenable Web App Scanning staggers concurrent scans to ensure consistent scanning performance. The starting date defaults to the date you create the scan. The starting time is the next hour interval, displayed in 24-hour clock format. For example, if you create your scan on October 31, 2019 at 9:12 PM, the default starting date and time is *10/31/2019* and *22:00*.
Timezone	varies	The time zone of the value set for **Starts**.

Notifications

The notification settings for a scan.

Setting	Default Value	Description
Email Recipient(s)	None	Specifies zero or more email addresses, separated by commas, whitespace, or new lines that are alerted when a scan completes and the results are available.

User Permissions

Share the scan or user-defined scan template with other users by setting permissions for users. For more information on adding or editing user permissions, see Set Scan Permissions.

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

Data Sharing

Setting	Default Value	Description
Scan Results	Show in dashboard	Specifies whether the results of the scan should be kept private or appear on your **Dashboard** and **Findings** pages. When set to **Keep private**, the scan results **Last Seen** dates do not update and you must access the scan directly to view the results.

Advanced Settings in Tenable Web App Scanning Scans

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

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

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

- General
- HTTP Settings
- Screen Settings
- Limits
- Selenium Settings
- Performance Settings
- Session Settings

General

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

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

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

HTTP Settings

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

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

Setting	Default	Description
Use a different User Agent to identify scanner	disabled	Specifies whether you want the scanner to use a user-agent header other than Chrome when sending an HTTP request.
User Agent	Chrome's user-agent	Specifies the name of the user-agent header you want the scanner to use when sending an HTTP request. You can configure this option only after you select the **Use a different User Agent to identify scanner** checkbox. By default, Tenable Web App Scanning uses the user-agent that Chrome uses for the operating system and platform that corresponds to your machine's operating system and platform. For more information about Chrome's user-agents, see the *Google Chrome Documentation*.

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

Screen Settings

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

Setting	Default	Description
Screen 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 `www.example.com`, and you want the scanner to crawl `www.example.com/users/myname`, type *2* in the text box.
Page DOM Element Depth	5	Specifies the maximum number of HTML nested element levels the scanner crawls.
Max Response Size	500000	Specifies the maximum load size of a page, in bytes, which the scanner analyzes. If the scanner crawls a URL and the response exceeds the limit, the scanner does not analyze the page for vulnerabilities.
Request Redirect Limit	3	Specifies the number of redirects the scanner follows before it stops trying to crawl the page.

Selenium Settings

These settings specify how the scanner behaves when it attempts to authenticate to a web application using your recorded Selenium credentials.

Configure these options if you configured your scan to authenticate to the web application with Selenium credentials. For more information see Credentials in Tenable Web App Scanning Scans.

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

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

Performance Settings

Setting	Default	Description
Max Number of Concurrent HTTP Connections	10	Specifies the maximum number of established HTTP sessions allowed for a single host.
Max Number of HTTP Requests Per Second	25	Specifies the maximum number of HTTP requests allowed for a single host for the duration of the scan.
Slow down the scan when network congestion is detected	disabled	Specifies whether the scanner throttles the scan in the event of network congestion.
Network Timeout (In Seconds)	5	Specifies the time, in seconds, the scanner waits for a response from a host before aborting the scan, unless otherwise specified in a plugin. If your internet connection is slow, Tenable recommends that you specify a longer wait time.

Browser Timeout (In Seconds)	30	Specifies the time, in seconds, the scanner waits for a response from a browser before aborting the scan, unless otherwise specified in a plugin. If your internet connection is slow, Tenable recommends that you specify a longer wait time.
Timeout Threshold	100	Specifies the number of consecutive timeouts allowed before the scanner aborts the scan.

Session Settings

Specifying these tokens speeds up the scan by allowing the scanner to skip token verification. Session Settings are only available when you are editing an existing scan.

Token Type	Default	Description
Cookie	None	Name of your application's authentication cookie for the scanner to use.
Header	None	Name of your application's authentication header for the scanner to use.

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 `.side` 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	A list of any URLs you want to ensure the scanner analyzes, in addition to the target URL you specified in the Basic settings. Type each URL as an absolute URL. Type each URL on a separate line. **Note:** All URLs should have the same domain and wildcards are not allowed.
Specify how the scanner handles URLs found during the application crawl	Crawl all URLs detected	Specifies the limits you want the scanner to adhere to as it crawls URLs. Select one of the following: • **Crawl all URLs detected** — The scanner crawls all URLs and child paths it detects on the target URL's domain host. • **Limit crawling to specified URLs and child paths** — The scanner crawls only the target URL and child paths. • **Limit crawling to specified URLs** — The scanner crawls the target URL only. It does not crawl child paths for the target URL.

Scan Exclusion

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

Setting	Default Value	Description
Regex for Excluded URLs	logout	Text box option in which you can specify a regex pattern that the scanner can look for in URLs to exclude from the scan. You can specify multiple regex patterns separated by new lines. **Note**: The regex values should be values contained within the URL to be excluded. For example, in the URL `http://www.example.com/blog/today.htm`, valid regex values would be `blog` or `today` (not the full URL). Additionally, regex values are case-sensitive.
File Extensions to Exclude	js, css, png, jpeg, gif, pdf, csv, svn-base, svg, jpg, ico, woff, woff2, exe, msi, zip	Text box option in which you can specify the file types you want the scanner to exclude from the scan. Separate each file type with a comma. **Note**: Excluding certain file extensions may be useful as the scanner may not realize something is not a web page and attempt to scan it, as if it actually is a web page. This wastes time and slows down the scan. You can add additional file extensions if you know you use them, and are certain they do not need to be scanned. For example, Tenable includes different image extensions by default: .png, .jpeg, etc.
Decompose Paths	not selected	Check box option that allows you to specify whether you want the scanner to break down each URL identified during the scan into additional URLs, based on directory path level. For example, if you specify *www.example.com/dir1/dir2/dir3* as your target and select **Decompose Paths**, the scanner analyzes each of the following as separate URLs of the target: • www.example.com/dir1/dir2/dir3 • www.example.com/dir1/dir2

Setting	Default Value	Description
		• www.example.com/dir1 Select this option to increase the surface coverage of your web application scan. **Note**: Scans that include path decomposition can take longer to complete than scans that do not.
Exclude Binaries	selected	Check box option that allows you to specify whether you want the scanner to audit URLs with responses in binary format. Select this option to increase the surface coverage of your web application scan. **Note**: Scans that include binaries can take longer to complete, because the scanner cannot read the binary responses.

Miscellaneous

Setting	Description
Deduplicate Similar Pages	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	Drop-down box that allows you to choose from the following options to specify the scan type you want the scanner to perform. • **Recommended** — The scanner audits elements based on Tenable's recommendations. • **None** — The scanner does not audit any elements. • **Quick** — The scanner audits the most common elements listed. • **Extensive** — The scanner	Yes

Setting	Default Value	Description	Required
		audits all the elements listed. • **Custom** — The scanner audits only the elements you select. **Note:** If you select **Recommended**, **Quick**, or **Extensive** and then make changes to the settings in this section, the **Scan Type** setting automatically changes to **Custom**.	

Common and Backup Pages

Setting	Default Value	Description
Detection Level	Most Detected Pages	Drop-down box that allows you to choose from the following options to specify which pages you want the scanner to crawl. • **Most Detected Pages** - The scanner crawls only the most detected pages. • **Extended Dictionary** - The scanner tests more path variations for detecting hidden pages, increasing the overall scan duration. **Note:** The **Detection Level** drop-down box is available only when you select **Custom** in the **Scan Type** settings.

Credentials Bruteforcing

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

Setting	Default	Description
Credentials Bruteforcing	Disabled	When enabled, any plugins that perform bruteforcing included in the **Plugins** settings run. When disabled, bruteforcing plugins do not run, even if they are included in the **Plugins** settings. **Note:** The **Credentials Bruteforcing** setting is available only when you select **Custom** in the **Scan Type** settings.

Elements to Audit

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

Setting	Scanner Action
Cookies	Checks for cookie-based vulnerabilities.
Headers	Checks for header vulnerabilities and insecure configurations (for example, missing X-Frame-Options).
Forms	Checks for form-based vulnerabilities.
Links and Query String Parameters	Checks for vulnerabilities in links and their parameters.
Parameter Names	Performs extensive fuzzing of parameter names.
Parameter Values	Performs extensive fuzzing of parameter values.
Path Parameters	Assesses path parameters. Path parameters are used in URL rewrite to identify the object of the action within the URL. For example, **`scanId`** is a path parameter for the following URL, used to identify the scan to display results: `http://example.com/scan/`**`scanId`**`/results`
JSON Elements / Request Body	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. **Note**: With UI Forms, Tenable Web App Scanning takes the inputs on the page, and any buttons, and creates form-like elements from them (UI Forms). For each button, Tenable Web App Scanning creates a `UIForm` element with inputs that are all the inputs on the page.
UI Inputs	Checks orphan input elements against associated document object model (DOM) events. **Note**: UI Inputs are when there is an input that responds to an event. For example, after typing in the input in a search bar, the search bar responds to an "onEnter" event which loads the next page. So, Tenable Web App Scanningcreates a `UIInput` element to audit this vector as well.

Optional

Setting	Default	Description
URL for Remote Inclusion	None	Specifies a file on a remote host that Tenable Web App Scanning can use to test for a Remote File Inclusion (RFI) vulnerability. If the scanner cannot reach the internet, the scanner uses this internally-hosted file for more accurate RFI testing. **Note**: If you do not specify a file, Tenable Web App Scanning uses a safe, Tenable-hosted file for RFI testing.

DOM Element Exclusion

DOM element exclusions prevent scans from interacting with specific page elements and their children. This setting is available for Scan, Overview, and PCI scan templates.

> **Note:** When the scanner is deciding whether to exclude an element based on an attribute value, it performs an equality check. So, if you want to exclude any element with css `class foo`, the scanner excludes an element that has `class="foo"`, but not an element that has `class="foo bar"`.

You can add exclusions by clicking the ⊕ button and selecting **Text Contents** or **CSS Attribute**.

Setting	Default	Description
Text Contents	None	Excludes elements based on text contents. For example, if you want to prevent the scanner from clicking a logout button named Log Out, you could match the text `Log Out`.
CSS Attribute	None	Excludes elements based on a CSS attribute key-value pair. For example, if you want to prevent the scanner from interacting with a form that contains the CSS attribute key-value pair `id="logout"`, type `id` for the key and `logout` for the value.

Report Settings in Tenable Web App Scanning Scans

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

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

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

- (Tenable PCI ASV 6.1) Load Balancers Usage

(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

Plugin Settings in Tenable Web App Scanning Scans

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

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

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

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

You can configure **Plugin** settings when you create a scan or user-defined scan template and select the **API**, **Overview**, **(Basic) Scan**, **Standard Scan**, or **Custom** template or scan type. For more information, see View Your Scan Plugins.

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

The plugins settings contain the following sections:

- All enabled
- Plugins table

All Enabled

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

Plugins Table

Column	Description	Actions
Name	Specifies the plugin family to which the grouped plugins belong.	• View the name of each plugin family. • Select the column to sort the table alphabetically or by family name.
Total	Specifies the number of plugins in the plugin family.	• View the number of plugins in the family. • Select the column to sort the table by number of plugins in each family.
Status	Toggle that allows you to specify if you want the scanner to use the plugins in the plugin family to analyze your target.	• Click the **Status** toggle to disable the plugins in the plugin family. • (Optional) To enable a disabled plugin family, click the **Status** toggle.

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

To view details about individual plugins:

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

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

2. (Optional) To locate a specific plugin, in the **Search** box, type the name or ID.

3. Click the plugin for which you want to view details.

To disable individual plugins:

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

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

2. (Optional) To locate a specific plugin, in the **Search** box, type the name or ID.

3. In the **Status** column, select the check box next to the plugin you want to disable.

4. (Optional) To enable a disabled plugin, select the check box.

5. Click **Save**.

   The details plane disappears.

   Tenable Web App Scanning updates your plugin selections.

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.

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

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

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

- HTTP Server Authentication
- Web Application Authentication
- Client Certificate Authentication

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

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

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

Web Application Authentication	Login Form	
	Cookie Authentication	
	API Key	Use the Tenable Web App Scanning user interface to manually configure credentials settings in scans.
	Bearer Authentication	
Client Certificate 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 Tenable Web App Scanning User Role: 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 ✕ 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.

HTTP Server Authentication Settings in Tenable Web App Scanning Scans

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

Option	Action
Username	Type the username Tenable Web App Scanning uses to authenticate to the HTTP-based server.
Password	Type the password Tenable Web App Scanning uses to authenticate to the HTTP-based server.
Authentication Type	In the drop-down list, select one of the following authentication types: • **Basic/Digest** • **NTLM** • **Kerberos**
Kerberos Domain	(Required when enabling the Kerberos Authentication Type) The realm to which Kerberos Target Authentication belongs, if applicable.
Key Distribution Center (KDC)	(Required when enabling the Kerberos Authentication Type) This host supplies the session tickets for the user.

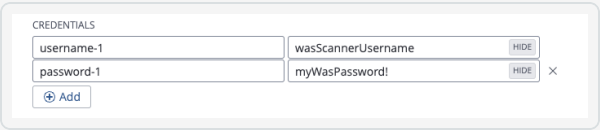
Note: Tenable Web App Scanning does not support multiple HTTP authentication types for a single target.

Web Application Authentication

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

- Login Form Authentication
- Cookie Authentication
- Selenium Authentication
- API Key Authentication
- Bearer Authentication

Login Form Authentication

Option	Action
Authentication Method	In the drop-down box, select **Login Form**.
Login Page	Type the URL of the login page for the web application you want to scan.
Credentials	For each field in the target's login form (that is, username, password, and domain, etc.) complete a credential entry as follows: a. In the left-hand text box, type the value of the login field's `name` or `id` HTML DOM attribute. b. In the right-hand text box in the row, type the literal value to insert in that text field at login. A typical configuration example:  **Tip:** To see a text field's `name` or `id` HTML DOM attribute, right-click on the text field and select "Inspect" in either your Firefox or Chrome browser.

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

Cookie Authentication

Option	Action
Authentication Method	In the drop-down box, select **Cookie Authentication**.
Session Cookies	Do the following: a. In the first text box, type the name of the cookie authentication credentials. b. In the second text box, type the value of the cookie authentication credentials.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, **Hello,** *your username***.**). Note that leading slashes will be escaped and `.*` is not required at the beginning or end of the pattern.

Selenium Authentication

Option	Action
Authentication Method	Select **Selenium Authentication**.
Selenium Script (.side)	Do the following: a. In the Selenium IDE extension, record your authentication credentials in the Selenium IDE extension. b. Click **Add File**. The file manager for your operating system appears. c. Navigate to and select your Selenium credentials `.side` file. Tenable Web App Scanning imports the credentials file.
Page to Verify Active Session	Type the URL that Tenable Web App Scanning can continually access to validate the authenticated session.
Pattern to Verify Active Session	Type a word, phrase, or regular expression that appears on the website only if the session is still active (for example, **Hello,** *your username*.). Note that leading slashes will be escaped and `.*` is not required at the beginning or end of the pattern.

API Key Authentication

Option	Action
Authentication Method	Select **API Key**.
Headers	Do the following: a. In the first text box, type the name of the HTTP header. b. In the second text box, type the value of the HTTP header. c. (Optional) Add additional headers by clicking the ⊕ button.

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

Bearer Authentication

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

Client Certificate Authentication

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

Option	Action
Client Certificate	The file that contains the PEM-formatted certificate used to communicate with the host.
Client Certificate Private Key	The file that contains the PEM-formatted private key for the client certificate.
Client Certificate 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.

View Scan Details

Required Scan Permissions: Can View

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

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, click **Scans**.

   The **My Scans** page appears.

3. 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.

4. Do any of the following:

Section	Action
Table header	• 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: • **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:
	
	• View information about each vulnerability:
	  • 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.
	  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.
	
	• To sort, increase or decrease the number of rows per page, or navigate to another page of the table, see Tenable Web App Scanning Tables.
	• To view vulnerability details, click the row for that vulnerability.
	  The **Vulnerability Details** page appears.
	  From the **Vulnerabilities Details** page, you can view plugin attachments for more information about each plugin.

Notes tab	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. 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.
	
	On this tab, you can:
	
	• View information about the scan notes:
	
	  • **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 in Severity Details .
	
	  • **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	View the scan history.
	
	This tab contains a table listing each time the scan has run. For the scan run currently displaying in the **Scan Details** page, Tenable Web App Scanning adds the label **Current** to the run. By default, the latest scan run is labeled **Current**.
	
	Note: Scan history is unavailable for imported scans and for configured scans that have not yet run.
	
	On this tab, you can:
	
	• View summary information about each time the scan was run:
	
	  • **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.

	> **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. > 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. • **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 Web App Scanning 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 Status

In Tenable Web App Scanning, depending on its state, scans can have the following status values:

> **Note:** The percentage on the Tenable Web App Scanning scan progress indicator represents the percentage of completed tasks in the scan. A scan with one task shows 0% progress until the scan completes.

> **Tip:** For Tenable Web App Scanning scans, you can hover over the scan status to view more status information in a pop-up window, such as the number of targets scanned and the elapsed or final scan time. The window shows different information based on the scan's current status.

Status	Description
Tenable Web App Scanning Scans	
Aborted	The scanner did not complete the scan's latest scan job. Tenable Web App Scanning may abort a scan job because the job was queued without running for more than four hours, or because Tenable Web App Scanning, or the scanner, encountered other problems and aborted the scan. For more information about why Tenable Web App Scanning aborted a scan, view the scan notes.
Canceled	At the user's request, Tenable Web App Scanning successfully stopped the latest scan job.
Completed	The scanner completed the scan's latest scan job.
Never Run	The scan is either empty (the scan is new or has yet to run) or pending (Tenable Web App Scanning is processing a request to run the scan).
Pending	Tenable Web App Scanning has the scan queued to launch. **Note**: Tenable Web App Scanning aborts scans that remain in **Pending** status for more than four hours. If Tenable Web App Scanning aborts your scan, modify your scan schedules to reduce the number of overlapping scans. If you still have issues, contact Tenable Support.
Processing	The scan has been completed but the results are still being processed. The

Status	Description
	scanner is processing vulnerability findings, attachments, notes, and other metadata.
Running	The scanner is currently running the scan.
Stopping	The scanner acknowledged the stop request and is in the process of stopping.

View Scan Progress

Required Additional License: Tenable Web App Scanning

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, 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	The portion of the scan job that the scanner has already completed, displayed as a percentage of the total estimated scan time.
Estimate	The estimated time remaining for the scanner to complete the scan, displayed in minutes.
Overdue	The 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	A 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.

To view scan progress for a Tenable Web App Scanning scan not in progress, see Scan Status.

Scan Notes in Severity Details

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

Rating	Description	Example
Critical	Information explaining that the scan may have impacted the web application's availability or integrity. The scan note title appears in red.	**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. 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.
High	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. The scan note title appears in yellow.	**Scan Crashed** — The scan crashed for an unexpected reason. As a result, the scan results are missing or incomplete.
Medium	Information explaining why scan results are missing or incomplete. The findings usually concern scans that could not be	**Out of Scope URL** — The scanner did not scan the target URL because it matches one of the

	started due to configuration errors. The web application is not impacted. The scan note title appears in black and white.	scope exclusion criteria specified in the scan template settings.
Low	Information explaining variations in scan duration. The findings do not impact the web application or scan results. The scan note title appears in green.	**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.
Info	Information that does not impact the scan results, but that can help you configure your scan settings more efficiently. The scan note title appears in blue.	**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.

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.

Copy a Scan Configuration

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

When you copy a scan configuration, Tenable Web App Scanning assigns you owner permissions for the copy and assigns the copy scan permissions from the original scan.

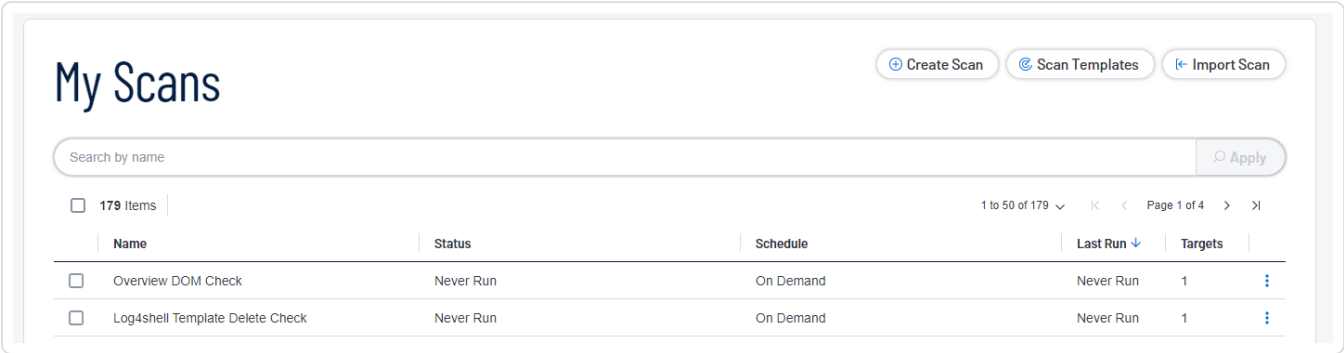
To copy a scan configuration:

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

   The left navigation plane appears.

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

   The Tenable Web App Scanning **My Scans** page appears:



3. In the row, click the ⋮ button.

   A drop-down box of options appears.

4. Click **Copy**.

   The **Copy to Folder** plane appears, which contains a list of your scan folders.

5. Click the folder where you want to save the copy.

6. Click **Copy**.

   Scan Copied Successfully: Tenable Web App Scanning creates a copy of the scan with *Copy of* prepended to the name and assigns you owner permissions for the copy. The copy appears in the scans table of the folder you selected.

Export Scan Results

Required Tenable Web App Scanning User Role: Basic, Scan Operator, Standard, 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: Filters are not applicable for Tenable Web App Scanning exports, All results will are exported.

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	a. In the scans table, roll over the scan you want to export. b. Click the ⋮ button. A menu appears. c. Click ↦**Export**. The **Export** plane appears.
Scan Details	a. In the scans table, click the scan you want to export. b. 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. **Note:** Tenable Vulnerability Management cannot export PDF files with more than 400,000 individual scan results.	n/a
Nessus	A `.nessus` file in XML format that contains the list of targets, scan settings defined by the user, and scan results. Password credentials are stripped so they are not exported as plain text in the XML.	n/a

	Note: To learn more about the `.nessus` file format, see Nessus File Format.	
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.

Import a Tenable Web App Scanning Scan

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

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

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

   The left navigation plane appears.

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

   The **My Scans** page appears.

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

   Your file directory appears.

   Note: Only `.json` file types are supported in Tenable Web App Scanning scan import.

4. Browse to and select the scan file you want to import.

5. Click **Open**:

   Note: Clicking **Cancel** cancels the import.

   The **Scans** page appears, and the imported scan appears in the scans table.

   Note: You can click on the **Last Modified** row in your scans table so your imported scan appears at the top of your scans list.

   Tenable Web App Scanning begins processing the imported scan results. Once this process is complete, the imported data appears in the individual scan details and aggregated data views (such as dashboards). This process can take up to 30 minutes, depending on the size of the import file.

   Tip: If the imported data does not appear in the individual scan results or aggregated data views after a reasonable processing time, verify that you are assigned adequate permissions for the imported targets in access groups.

Move a Scan to a Scan Folder

Required Scan Permissions: Can View

You can move a scan from a default folder to either the **My Scans** default folder or a custom scan folder. You can also move a scan from a custom folder to the **My Scans** default folder or a different custom folder.

If you move a scan from the **All Scans** default folder, the scan appears in both the folder you select and the **All Scans** folder.

If you move a scan from the **My Scans** default folder, the scan appears in the custom folder only.

For information about moving a scan to the trash, see Move a Scan to the Trash Folder.

To move a scan to a scan folder:

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

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

4. In the scans table, roll over the scan you want to move.
5. In the row, click the ⋮ button.

   A menu appears.

6. In the menu, click **Move**.

   The **Move to Folder** plane appears. This plane contains a list of your scan folders.

7. Search for a folder:

    a. In the search box, type the folder name.

    b. Click the 🔍 button.

    Tenable Web App Scanning limits the list to folders that match your search.

8. In the folder list, click the folder where you want to move the scan.

9. Click **Move**.

    Tenable Web App Scanning moves the scan to the selected folder.

Move a Scan to the Trash Folder

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

Required Scan Permissions: Can View

When you move a shared scan to the **Trash** folder, Tenable Web App Scanning moves the scan for your account only. The scan remains in the original folder for all other users who have **Can View** permissions or higher for the scan.

Scans moved to the **Trash** folder also appear in the **All Scans** folder, marked with the label, **Trash**.

Note: After you move a scan to the **Trash** folder, the scan remains in the **Trash** folder until a user with **Can Configure** permissions permanently deletes the scan.

Note: Scheduled scans do not run if they are in the scan owner's **Trash** folder.

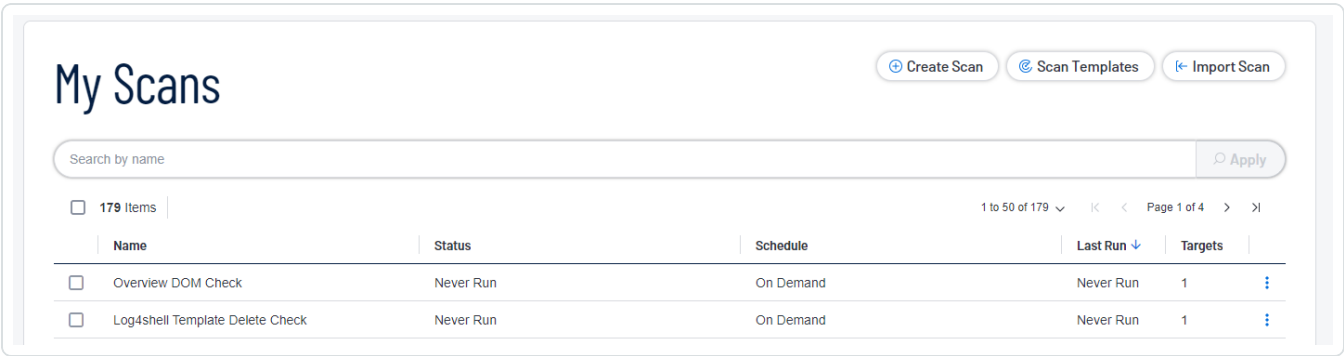
To move a scan or scans to the **Trash** folder:

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

   The left navigation plane appears.

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

   The Tenable Web App Scanning **My Scans** page appears:



3. In the row, click the ⋮ button.

   A drop-down box of options appears.

4. Do one of the following:

   - Select a single scan:

     a. In the scans table, roll over the scan you want to move.

        The action buttons appear in the row.

     b. Click the ⋮ button.

        A menu appears.

     c. Click **Trash**.

   - Select multiple scans:

     a. In the scans table, select the check box next to each scan you want to move.

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

     b. In the action bar, click **Trash**.

   Tenable Web App Scanning moves the scan, or scans, you selected to the **Trash** folder.

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-right corner, click the ⚙ button.

   The left navigation plane appears.

2. Click **Settings**.

   The **Settings** page appears.

> **Note:** All **Settings** options are managed directly within Tenable Vulnerability Management. When you access the Settings section, you are automatically redirected to the Tenable Vulnerability Management user interface and documentation.

General Settings

Required User Role: Administrator

On the **General** page, you can configure general settings for your Tenable Web App Scanning instance.

To access general settings:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

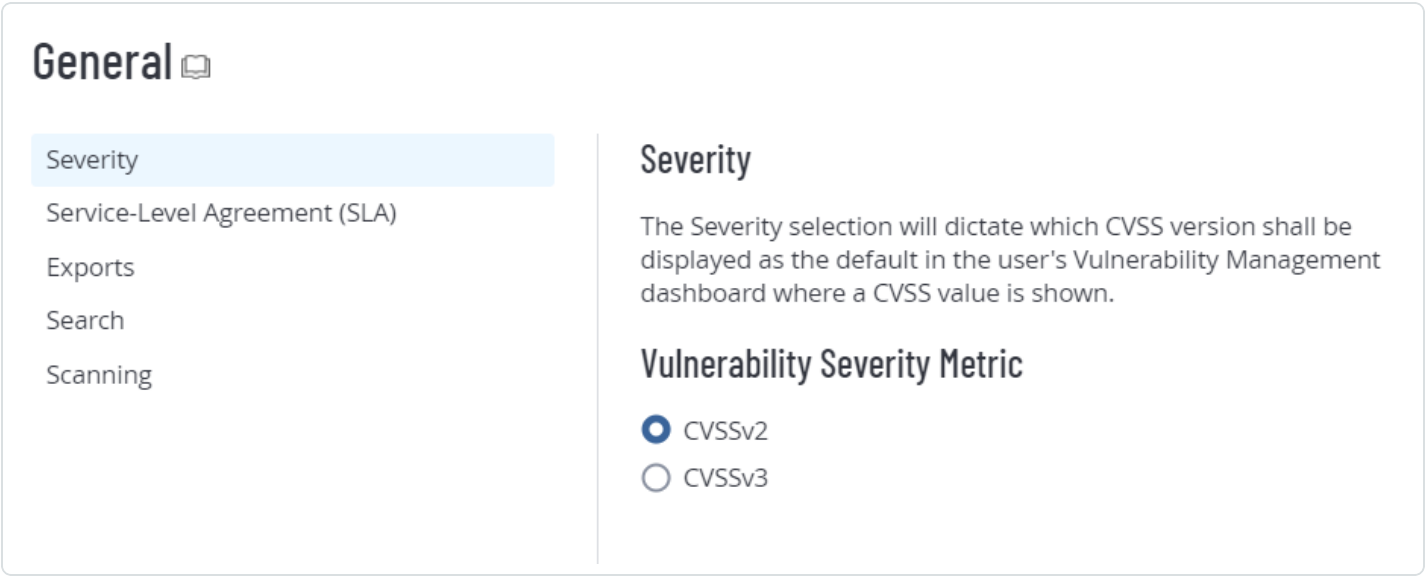
3. Click the **General** tile.

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

Here, you can configure the following options:

Severity

By default, Tenable Web App Scanning uses CVSSv2 scores to calculate severity for individual vulnerability instances. If you want Tenable Web App Scanning to calculate the severity of vulnerabilities using CVSSv3 scores (when available), you can configure your severity metric setting.



Tip: A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

For information about severity and the ranges for CVSSv2 and CVSSv3, see CVSS Scores vs. VPR.

Note: This setting does not affect the following:

- Tenable Web App Scanning vulnerabilities.
- Tenable Container Security vulnerabilities.
- The calculations displayed in the **SLA Progress: Vulnerability Age** widget. To modify your SLA severity, navigate to the **Service-Level Agreement (SLA)** tab on the **General** page.

Caution: When changing your CVSS severity metric setting, the new setting is only reflected in new findings that come into your system. Any existing findings only reflect the previous severity setting (unless otherwise recasted). For more information on recast rules, see Recast/Accept Rules.

To configure your severity setting:

1. On the **Severity** tab, select the metric that you want Tenable Web App Scanning to use for severity calculations.

- **CVSSv2** — Use CVSSv2 scores for all severity calculations.
- **CVSSv3** — Use CVSSv3 scores, when available, for all severity calculations. Use CVSSv2 only if a CVSSv3 score is not available.

2. Click **Save**.
3. The system saves your change and begins calculating severity based on your selection.

   All vulnerabilities seen before the change retain their severity. After the change, all vulnerabilities seen during scans receive severities based on your new selection. Because of this, you could see two sightings of the same vulnerability have two different CVSS scores and severities.

   > **Tip:** A vulnerability instance is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

Service-Level Agreement (SLA)

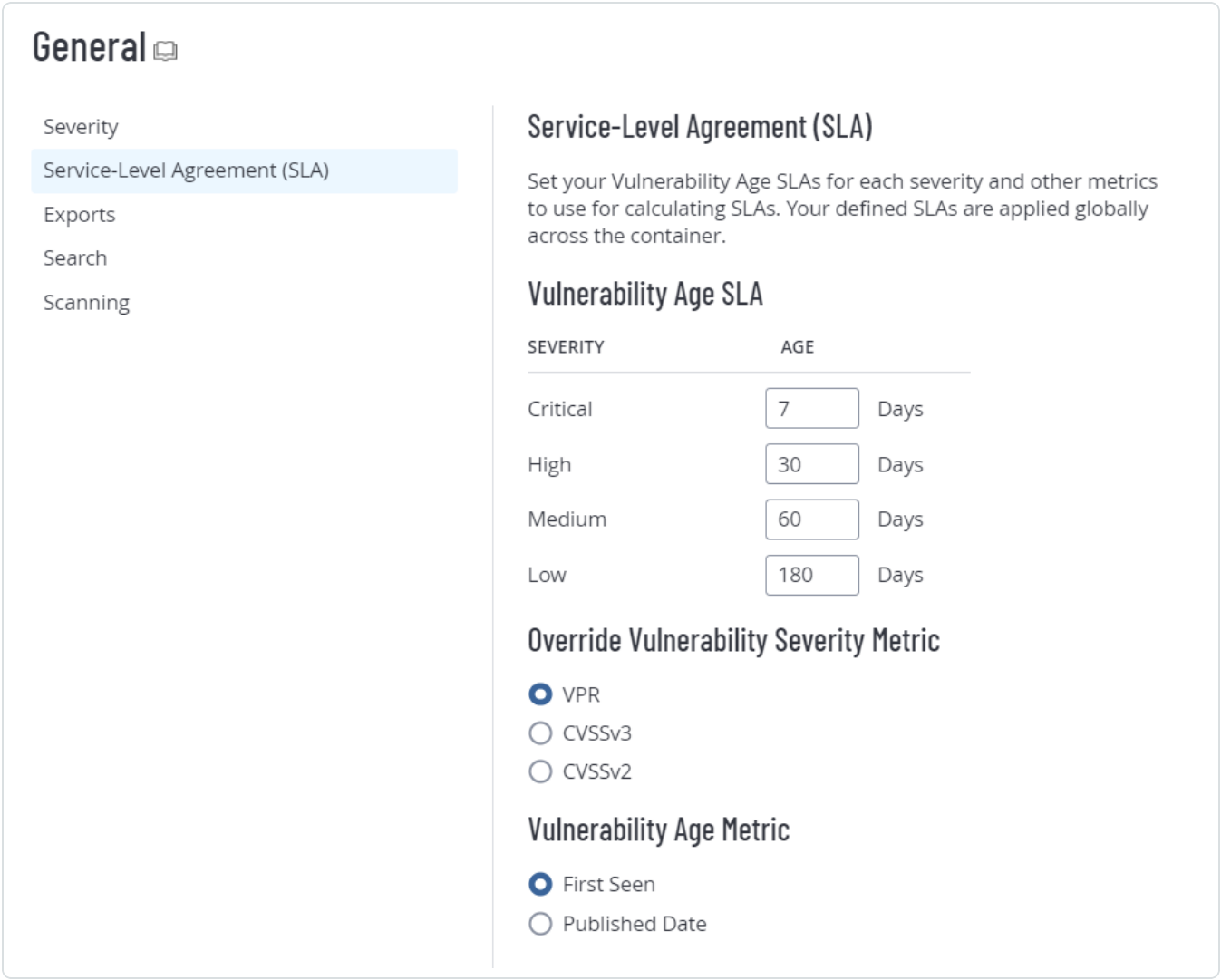
You can configure Service Level Agreement (SLA) settings to modify how Tenable calculates your SLA data.

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

To configure your SLA settings:

1. Click the **Service-Level Agreement (SLA)** tab.

   The SLA options appear.



2. Configure the following options:

Option	Default	Description/Actions
Vulnerability Age SLA	• **Critical** 7 days • **High** 30 days • **Medium** 60 days	To modify the number of days included for each severity, type an integer in the box next to **Critical**, **High**, **Medium**, or **Low**.

	• **Low** 180 days	
Override Vulnerability Severity Metric	VPR	Specifies whether Tenable uses VPR severity, CVSSv2 severity, or CVSSv3 severity to calculate SLA data. For more information about these metrics, see CVSS vs. VPR. **Note:** This option affects only the calculations displayed in the **SLA Progress: Vulnerability Age** widget. To modify the severity metric for all other areas of the product, navigate to the **Severity** tab on the **General** page.
Vulnerability Age Metric	First Seen	Specifies whether Tenable uses **First Seen** or **Published Date** to calculate SLA data.

3. Click **Save**.

   Tenable Web App Scanning saves your SLA settings.

Language

On the **General** page, you can change the plugin language in your Tenable Web App Scanning container to English, Japanese, Simplified Chinese, or Traditional Chinese. This setting affects all users in the container.

To change the plugin language:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **General** tile.

   The **General** tile appears. By default, the **Severity** tab is active.

4. Click the **Language** tab.

   The **Language** tab appears.

5. Under **Language**, select a new language.

   Tenable Web App Scanning updates the plugin language for your container.

Exports

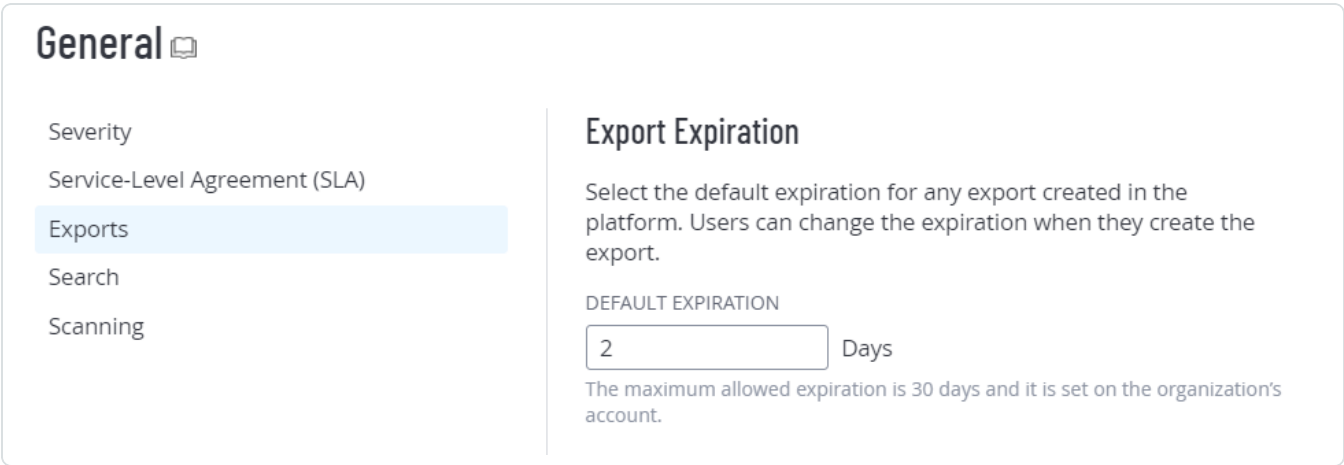
To configure your default export expiration:

When you create an export, you can set an expiration delay for the export file up to 30 calendar days, which is the maximum number of days that Tenable Web App Scanning allows before your export files expire.

By default, any exports you create in Tenable Web App Scanning have an expiration date of 30 days. If you want to decrease the number of days that Tenable Web App Scanning allows before your export files expire, you can configure your default export expiration days.

1. Click the **Exports** tab.

   The **Export Expiration** options appear.



2. In the **Default Expiration** box, type the number of days you want to Tenable Web App Scanning to allow before your exports expire.

   > **Note**: Tenable Web App Scanning allows you to set a maximum of 30 calendar days for export expiration.

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

3. Click **Save**.

   Tenable Web App Scanning saves your settings and updates the number of allowable days before your exports expire.

Search

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

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

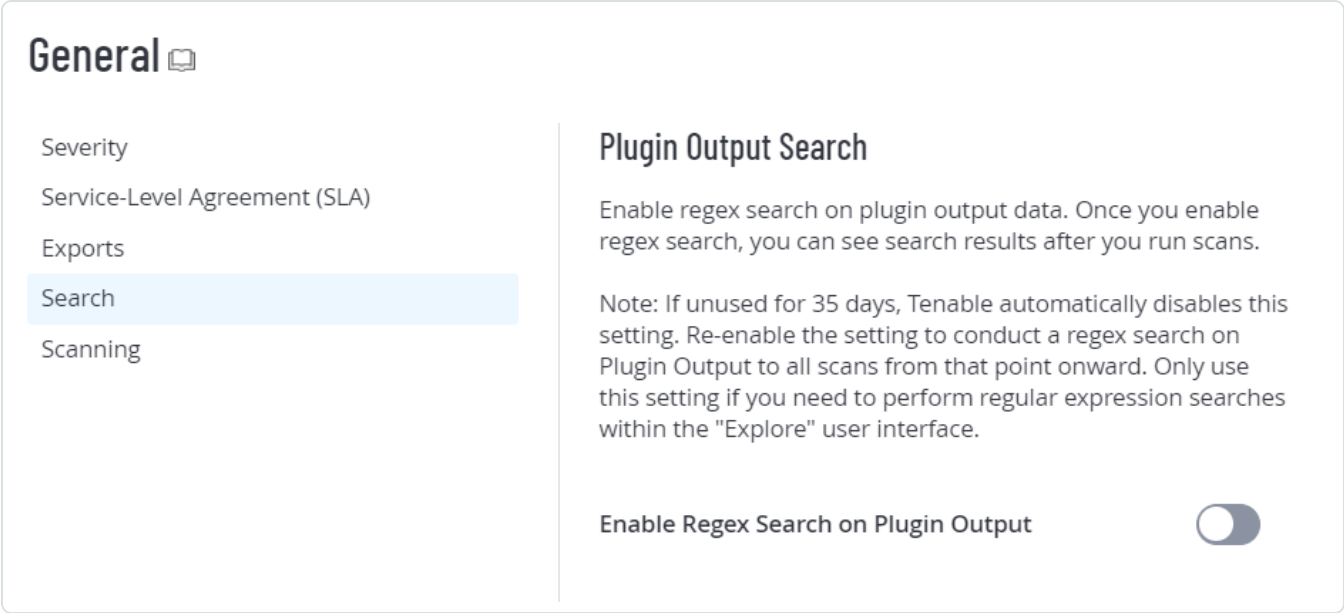
Once you have enabled plugin output data retention, you must launch a scan so that Tenable Web App Scanning can identify and store your plugin output data.

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

To enable plugin output data retention:

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

   The search options appear.



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

   Tenable Web App Scanning enables plugin output data retention on your account.

What to do next:

- Launch a scan for your host assets.

Scanning

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

> **Caution**:Tenable is removing these settings *for all customers* over the coming weeks. Contact your Tenable representative for more information.

Process High-Traffic Info Plugins

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

The following plugin IDs are impacted

- 34220 - Netstat Portscanner (WMI)
- 34252 - Microsoft Windows Remote Listeners Enumeration (WMI)
- 11219 - Nessus SYN Scanner
- 14272 - Netstat Portscanner (SSH)
- 25221 - Remote listeners enumeration (Linux / AIX)
- 10736 - DCE Services Enumeration
- 99265 - macOS Remote Listeners Enumeration
- 10335 - Nessus TCP scanner
- 14274 - Nessus SNMP Scanner
- 34277 - Nessus UDP Scanner

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

Relocate Open Port Findings

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

Note: When you enable **Relocate Open Port Findings**, you no longer receive open port findings data in your third-party integrations, since open ports are no longer stored as individual findings.

This setting does the following:

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

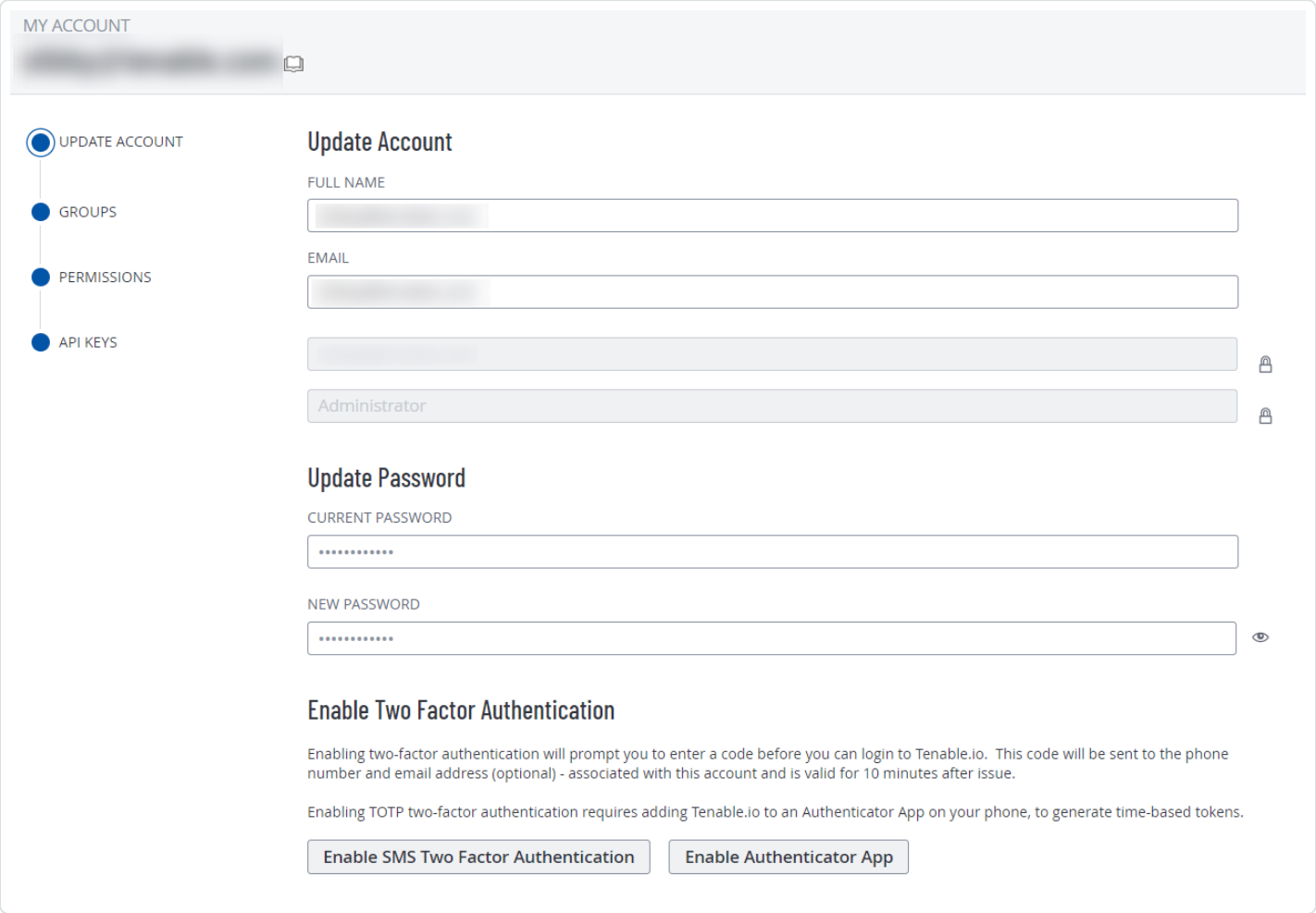
  Open port findings from the following high-traffic plugins move to the Asset Details page

- 34220 - Netstat Portscanner (WMI)
- 34252 - Microsoft Windows Remote Listeners Enumeration (WMI)
- 11219 - Nessus SYN Scanner
- 14272 - Netstat Portscanner (SSH)
- 25221 - Remote listeners enumeration (Linux / AIX)
- 10736 - DCE Services Enumeration
- 99265 - macOS Remote Listeners Enumeration
- 10335 - Nessus TCP scanner
- 14274 - Nessus SNMP Scanner
- 34277 - Nessus UDP Scanner

- Enables the **Open Ports** tab on the **Asset Details** page, which now contains open port findings.
- Enables the **Open Ports** filter on the **Assets** workbench, where you can search for open ports on host assets.
- Enables the **Open Ports** rule on the **Tags** page, so you can tag open ports.
- Adds an Open Ports field to the **Assets** workbench, so you can export open port data.
- (Optional) Adds open port findings to the bulk asset export API. To learn more, see the API changelog in the *Tenable Developer Portal*. To request this feature, contact your Tenable Customer Success Manager.

My Account

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



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

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

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

     The left navigation plane appears.

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

     The **Settings** page appears.

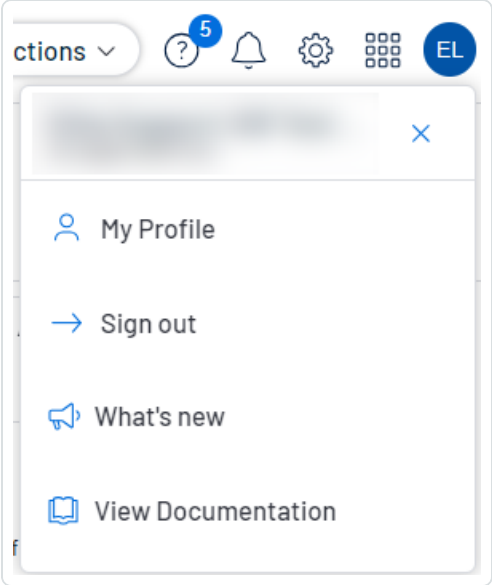
c. Click the **My Account** tile.

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

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

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

The user account menu appears.



b. Click **My Profile**.

The **My Account** page appears.

View Your Account Details

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

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

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

To view your account details:

1. Do one of the following:
   - In the upper-left corner, click the ☰ button.

     The left navigation plane appears.

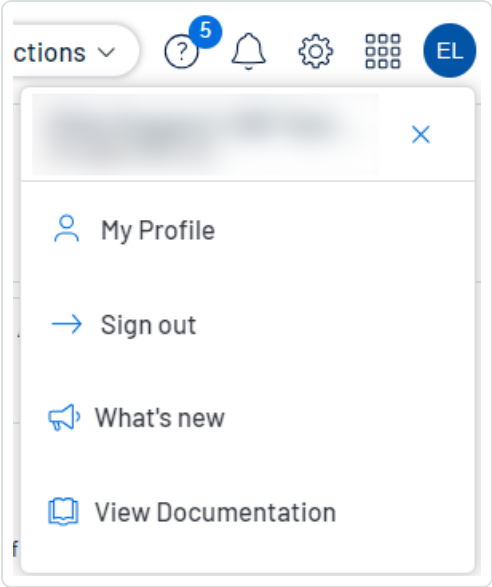
     a. In the left navigation plane, click **Settings**.

        The **Settings** page appears.

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

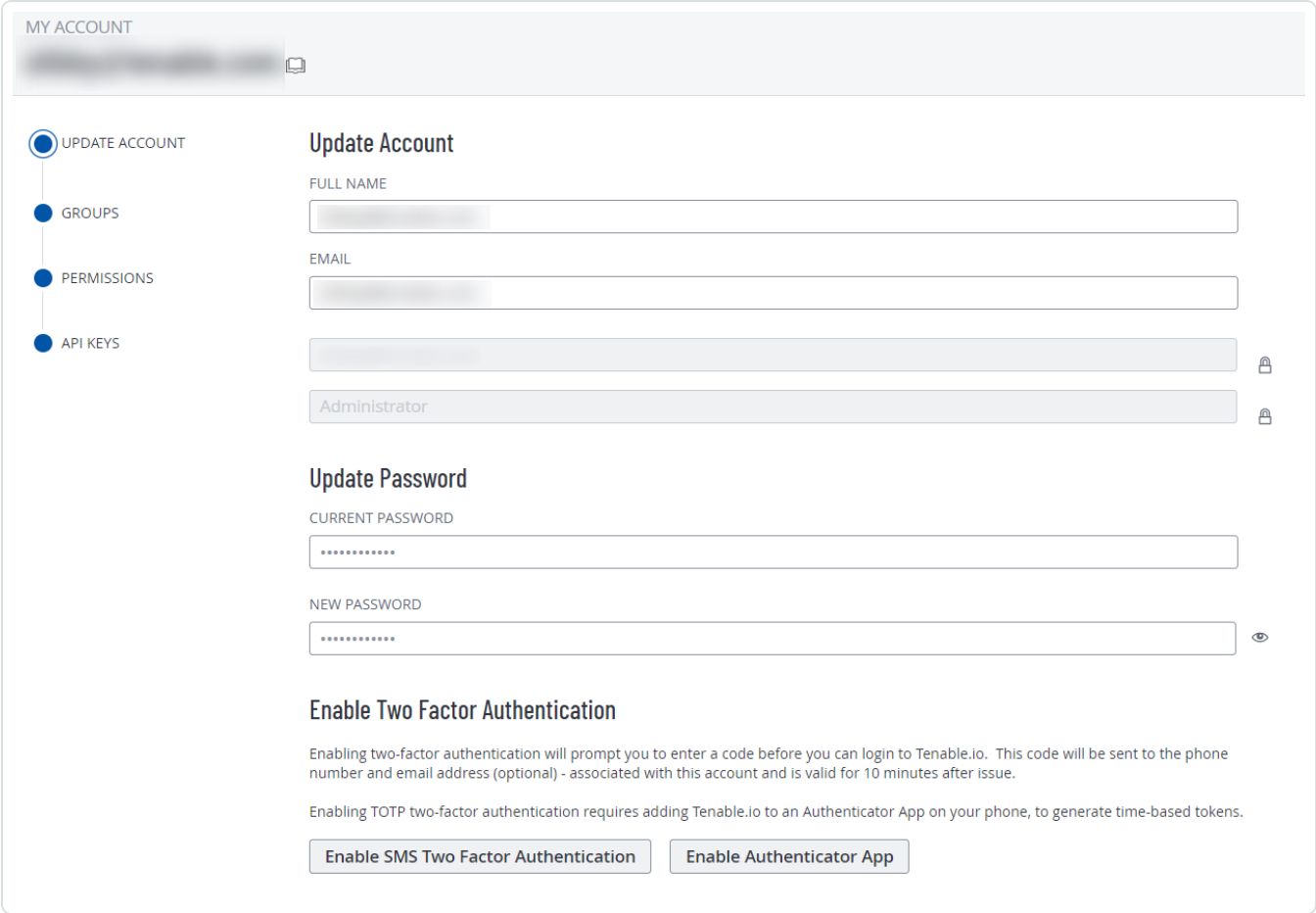
        The **My Account** page appears, where you can view and update your account details.
   - In the upper-right corner, click the blue user circle.

     The user account menu appears.



a. Click **My Profile**.

   The **My Account** page appears.



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

Option	Action
Update Account	• Click **Update Account**. The **Update Account** section appears, showing the following details for your account: ○ **Full Name** ○ **Email** ○ **Username** ○ **Role** • (Optional) Update your basic account information, including name and email address.

	Note: You cannot change your username or role. • (Optional) Change your password. • (Optional) Configure or disable two-factor authentication on your account. • (Optional) Enable or disable Explore beta features on your account.

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

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

API Keys	• Click **API Keys**.

	• View a description of API keys. • Generate API Keys. **Caution:** Any existing API keys are replaced when you click the **Generate** button. You must update the applications where the previous API keys were used. **Caution**: Be sure to copy the access and secret keys before you close the **API Keys** tab. After you close this tab, you cannot retrieve the keys from Tenable Web App Scanning.

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

Update Your Account

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

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

Before you begin:

- (Optional) View your account details.

To update your account:

1. Do one of the following:
   - In the upper-left corner, click the ☰ button.

     The left navigation plane appears.

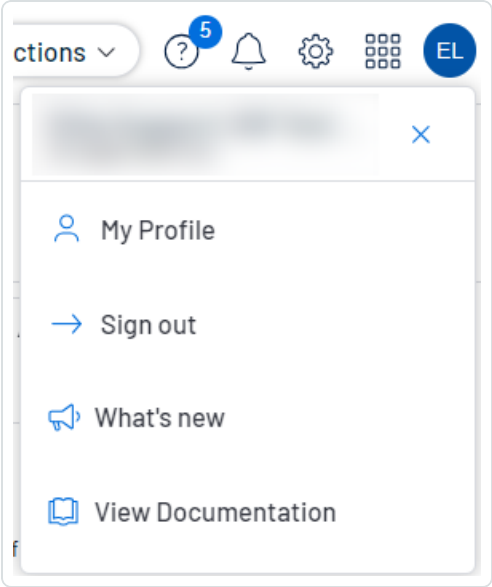
     a. In the left navigation plane, click **Settings**.

        The **Settings** page appears.

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

        The **My Account** page appears, where you can view and update your account details.
   - In the upper-right corner, click the blue user circle.

     The user account menu appears.



a. Click **My Profile**.

The **My Account** page appears.

2. (Optional) Edit your **Name**.
3. (Optional) Edit your **Email**.

   A valid email address must be in the format:

   name@domain

   where *domain* corresponds to a domain approved for your Tenable Web App Scanning instance.

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

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

4. Click **Save**.

   Tenable Web App Scanning saves the changes to the account.

5. (Optional) Change your password.
6. (Optional) Configure two-factor authentication.

7. (Optional) Generate an API key.

Change Your Password

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

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

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

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

To change your password:

1. Do one of the following:
   - In the upper-left corner, click the ☰ button.

     The left navigation plane appears.

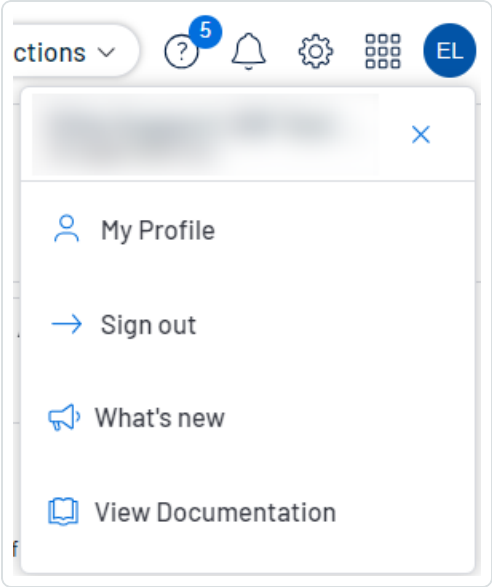
     a. In the left navigation plane, click **Settings**.

        The **Settings** page appears.

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

        The **My Account** page appears, where you can view and update your account details.
   - In the upper-right corner, click the blue user circle.

     The user account menu appears.



a. Click **My Profile**.

   The **My Account** page appears.

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

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

5. Log in to Tenable Web App Scanning using your new password.

Configure Two-Factor Authentication

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, Scan Operator, Standard, Scan Manager, or Administrator

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

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

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

To add or modify two-factor authentication:

1. Do one of the following:
   - In the upper-left corner, click the ☰ button.

     The left navigation plane appears.

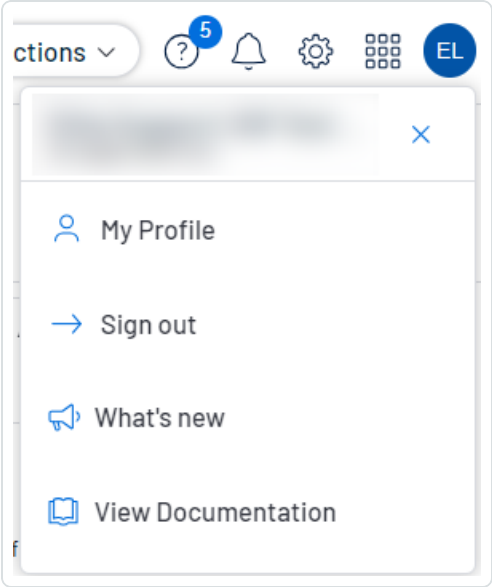
     a. In the left navigation plane, click **Settings**.

        The **Settings** page appears.

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

        The **My Account** page appears, where you can view and update your account details.
   - In the upper-right corner, click the blue user circle.

     The user account menu appears.



a. Click **My Profile**.

   The **My Account** page appears.

2. In the **Enable Two Factor Authentication** section, do one of the following:

   - To enable SMS two factor authentication:

     a. Click **Enable SMS Two Factor Authentication**.

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

     b. In the **Current Password** box, type your Tenable Web App Scanning password.

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

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

     d. Click **Next**.

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

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

     f. Click **Next**.

A **Two-Factor Setup Successful** message appears and Tenable Web App Scanning applies your settings to your Tenable Web App Scanning account.

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

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

   b. Click **Update**.

      Tenable Web App Scanning updates your backup email settings.

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

- To enable authenticator application based authentication:

  a. Click **Enable Authenticator App**.

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

  b. In the **Current Password** box, type your Tenable Web App Scanning password.

  c. Click **Next**.

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

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

     In the authenticator application, a Tenable Web App Scanning verification code appears.

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

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

  f. Click **Next**.

A **Two-Factor Setup Successful** message appears and Tenable Web App Scanning applies your settings to your Tenable Web App Scanning account.

To disable two-factor authentication in the new interface:

1. Do one of the following:

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

     The left navigation plane appears.

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

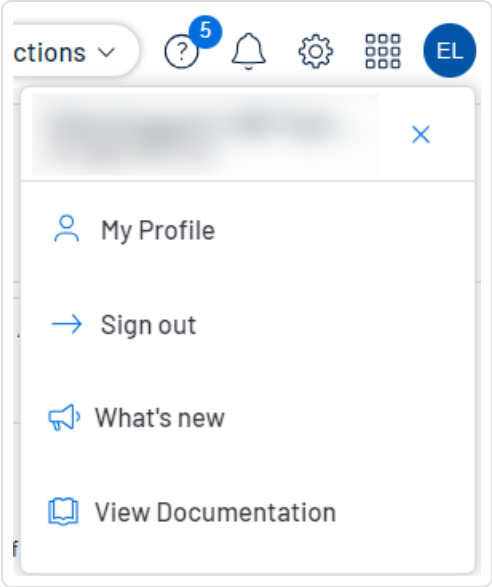
        The **Settings** page appears.

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

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

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

     The user account menu appears.

     a. Click **My Profile**.

        The **My Account** page appears.

2. In the **Change Password** section, in the **Current Password** box, type your current password.

3. In the **Enable Two Factor Authentication** section, click **Disable**.

   A **Disable Two-Factor** confirmation message appears.

4. Read the warning message, then click **Continue**.

   Tenable Web App Scanning disables two-factor authentication for your account.

Generate API Keys

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, Scan Operator, Standard, Scan Manager, or Administrator

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

Note: Tenable Web App Scanning API access and secret keys are required to authenticate with the Tenable Web App Scanning API.

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

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

- Tenable Web App Scanning integration
- Third-party integration
- Other custom applications, including those from Tenable Professional Services

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

To generate API keys for your own account:

1. Do one of the following:
    - In the upper-left corner, click the ☰ button.

      The left navigation plane appears.

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

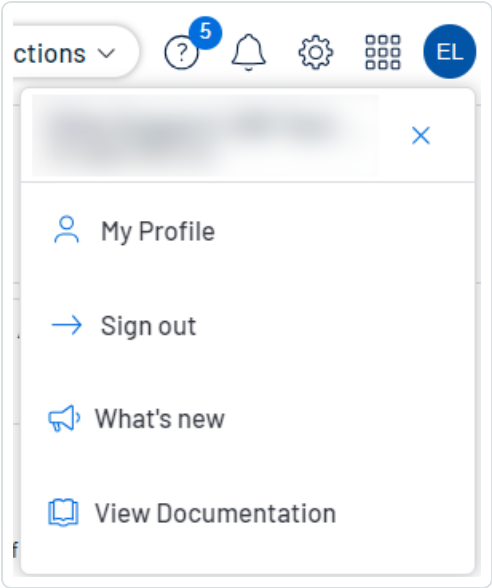
   The **Settings** page appears.

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

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

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

  The user account menu appears.



a. Click **My Profile**.

   The **My Account** page appears.

2. Click the **API Keys** tab.

   The **API Keys** section appears.

3. Click **Generate**.

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

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

4. Review the warning and click **Generate**.

   Tenable Web App Scanning generates new access and secret keys, and displays the new keys in the **Custom API Keys** section of the page.

   > **Tip:** If the **Generate** button is inactive, contact your administrator to ensure they've enabled API access for your account. For more information, see Edit a User Account.

5. Copy the new access and secret keys to a safe location.

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

Unlock Your Account

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, Scan Operator, Standard, Scan Manager, or Administrator

Tenable Web App Scanning locks you out if you attempt to log in and fail 5 consecutive times.

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

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

To unlock your account:

1. On the Tenable Web App Scanning login page, click the **Forgot your password?** link.

   The password reset page appears.

2. In the **Username** box, enter your Tenable Web App Scanning username.

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

4. Click **Send**.

   Tenable Web App Scanning sends password recovery instructions to the email address specified in your user account.

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

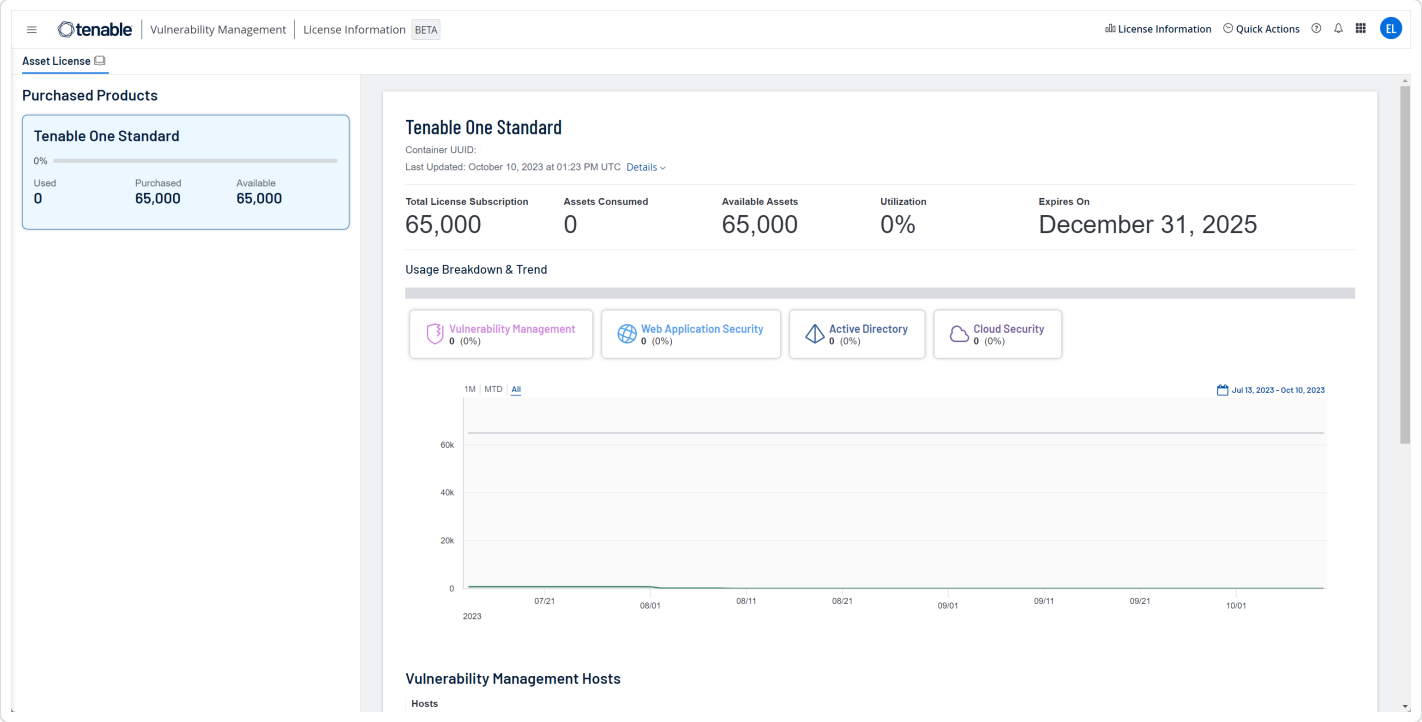
License Information

On the **License Information** page, you can view a complete breakdown of your Tenable products and their license usage. You can view this information in multiple ways, including visual overviews by product or time period that enable you to spot trends such as temporary usage spikes or product misconfigurations.

> **Tip**: For details on how Tenable licenses work in each product that appears on the **License Information** page, see Licensing Tenable Products. To learn about license overages, see Tenable Cloud Overage Process.

View the License Information Page

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



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

Section	Description
Purchased	On the left, click a product tile to view details. If a product is still being

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

Usage Breakdown & Trend	See visual breakdowns of your asset usage: • **Bar Chart** — (Tenable One only) View your total license use by Tenable One component in a bar chart. > **Note**: If you have the new version of Tenable Cloud Security, your licensed asset count is calculated by multiplying your **Compute**, **Serverless**, and **Container Repositories** assets against any ratio and adding your **Container Images** (if you have Tenable Container Security). If your organization has a ratio, it appears in the **Cloud Security** section, in the **License Ratio** field. To learn more about the ratio Tenable may apply to your cloud resources, contact your Tenable representative. • **Usage Over Time** – View your license use over time in a line chart where the X-axis is the time period and the Y-axis is the number of assets used. With the filters at the top of the chart, switch between time periods on the left, or specify a custom date range on the right. > **Tip**: (Tenable One-only) Click the tiles above the chart to select or deselect products.
Vulnerability Management Hosts	View the number of Tenable Vulnerability Management assets that count towards your license: • **Hosts** — The number of hosts that count towards your license.
Cloud Security Resources	View the number of cloud resources in your environment identified by Tenable Cloud Security. > **Note** Tenable Cloud Security has two versions. If you have the latest version, your licensed cloud asset counts appear in the **Compute, Serverless**, and **Container Repositories** fields, as well as the **Container Images** field if you have Tenable Container Security. To view your *total* licensed cloud assets, see the **Usage Breakdown & Trend** section. • **License Ratio** — (New version only) Any ratio applied to your **Compute**, **Serverless**, and **Container Repositories** resources. For example, if your organization has a ratio of 3, 10 Compute resources equals 30 *licensed* Tenable assets. To learn more about the ratio

	Tenable may apply to cloud resources, contact your Tenable representative. • **Compute** — (New version only) Cloud computing resources such as AWS EC2 instances or Azure virtual machines. Hover on this field to view your *billable* resources, or the total number of resources before any ratio is applied. • **Serverless** — (New version only) Cloud serverless resources such as AWS Lambda or Azure Functions. Hover on this field to view your *billable* resources, or the total number of resources before any ratio is applied. • **Container Repositories** — (New version only) Cloud container repositories scanned by Tenable Cloud Security. Hover on this field to view your *billable* resources, or the total number of resources before any ratio is applied. • **Container Images (Legacy Container Security)** — The number of packaged applications that count towards your license. Only used if you have Tenable Container Security. • **Billable** — (Legacy only) A subset of cloud assets that are considered licensed, typically cloud compute, storage, or network resources scanned in the past 90 days. **Tip**: If you have the new version of Tenable Cloud Security, these assets do not count towards your license. • **Non-Billable** — (Legacy only) Infrastructure as code (IaC) assets scanned locally, in a repository or a pipeline. These are not considered licensed.
Web App Scanning FQDNs	View the number of Tenable Web App Scanning resources that count towards your license: • **FQDNs** — The number of fully qualified domain names that count towards your license.

	Note: Tenable Web App Scanning determines asset count by the number of *fully qualified domain names* (FQDNs) that are scanned for your user account. An asset does not count against your license limit until it has been successfully scanned for vulnerabilities.
Attack Surface Management Assets	View your Tenable Attack Surface Management resources: • **Observable Objects** — The number of assets discovered and added to your inventory in Tenable Attack Surface Management. **Note**: If you are a Tenable One Standard customer, these resources do not count towards your asset license.
Active Directory Users	View the number of Tenable Identity Exposure resources that count towards your license: • **Users** — The number of enabled active users.

Tenable Web App Scanning Licenses

This topic breaks down the licensing process for Tenable Web App Scanning as a standalone product. It also explains how assets are counted, lists add-on components you can purchase, and describes what happens during license overages or expirations. To learn how to use Tenable Web App Scanning, see the Tenable Web App Scanning User Guide.

Licensing Tenable Web App Scanning

Tenable Web App Scanning has two versions: a cloud version and an on-premises version. For the cloud version, Tenable offers a subscription model. For the on-premises version, Tenable offers a subscription model as well as perpetual and maintenance licenses.

> **Note**: A Tenable Security Center license is required for the Tenable Web App Scanning on-premises version.

To use Tenable Web App Scanning, you purchase licenses based on your organizational needs and environmental details. Tenable Web App Scanning then assigns those licenses to *assets* in your environment: unique fully qualified domain names (FQDNs).

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

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

How Assets are Counted

Tenable Web App Scanning determines your licensed asset count by scanning resources in your environment to identify FQDNs. FQDNs that have been scanned for vulnerabilities in the past 90 days count towards your license.

FQDNs are listed as complete URLs, as per the RFC-3986 internet standard. Under this standard, each FQDN has 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.

For example, the following targets count towards one asset:

```
hostname.parent-domain.top-level-domain/path1
hostname.parent-domain.top-level-domain/path2
hostname.parent-domain.top-level-domain/path2/path3
```

The following table shows when scan targets are considered to be the same asset and when they are considered to be separate assets, based on whether or not all the FQDN components match.

Same Asset	Separate Assets
• https://example.com • https://example.com/welcome • https://example.com/welcome/get-started • https://example.com/welcome/get-started/create-new-user • http://example.com	• *https://en.example.com (different hostname)* • *https://www.ex-ample.com (different parent domain)* • *https://www.example.org (different top-level domain)*

Tenable Tenable Web App Scanning Components

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

Included with Purchase	Add-on Component
• External scanning functionality. • OWASP Top 10 Issues. • HTML5 crawling.	Additional cloud scan concurrency. **Tip**: Concurrency is based on your licensed assets and determines how many Tenable-managed cloud scanners you can run simultaneously.

• Integration with Tenable Vulnerability Management (if owned). • Use of the API.	

Reclaiming Licenses

When you purchase assets, your total asset count remains static for the length of your contract unless you purchase more assets. However, Tenable Web App Scanning reclaims licenses from deleted assets within 24 hours. In addition, it reclaims licenses from assets which are not scanned for 90 days or a period you specify.

Exceeding the License Limit

To allow for usage spikes due to sudden environment growth or unanticipated threats, Tenable Web App Scanning licenses are elastic by 10%. However, when you scan more assets than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages.

Scenario	Result
You scan more assets than are licensed for three consecutive days.	A message appears in Tenable Web App Scanning.
You scan more assets than are licensed for 15+ days.	A message and warning about reduced functionality appears in Tenable Web App Scanning.
You scan more assets than are licensed for 45+ days.	A message appears in Tenable Web App Scanning; export features are disabled.

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

Expired Licenses

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

After your license expires, you can no longer sign in to the Tenable platform.

License Types in Tenable Web App Scanning

License types in Tenable Web App Scanning can vary according to the feature set supported. Most notably, the Lumin Exposure View feature adds dynamic calculations and exposure risk scores to your Tenable user interface. For more information on Lumin Exposure View metrics, see Applications Dashboard.

View the following table to see the features each Tenable Web App Scanning license type supports.

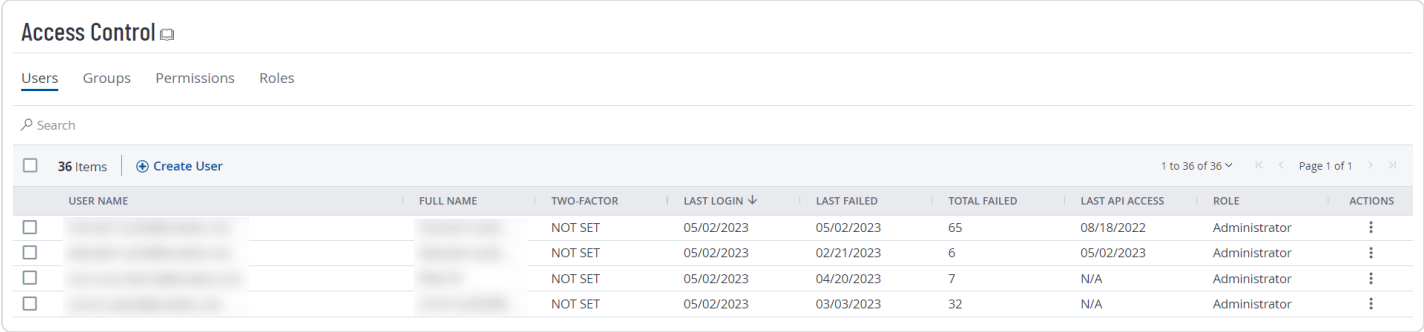
License Matrix

License	AES/CES/ACR Scores Supported
WAS Only	No
WAS + Lumin Only	Yes
EP License (Includes WAS + Lumin)	Yes
Tenable One License (Standard and Enterprise)	Yes

Access Control

Required User Role: Administrator

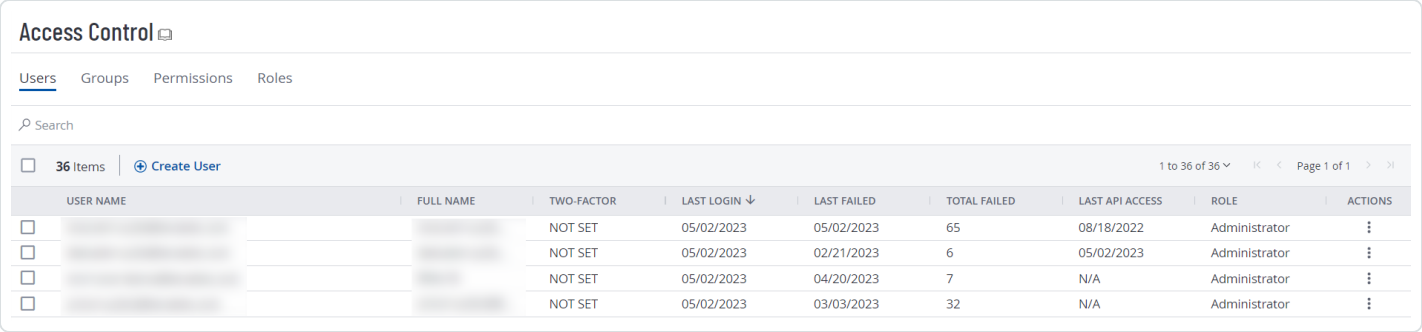
From the **Access Control** page, you can view and configure the list of users and groups on your account and the permissions assigned to them.



Users

> Topics in this section have been modified to reflect feature updates in Tenable Vulnerability Management Key Enhancements. For more information, see Tenable Vulnerability Management Key Enhancements.

On the **Access Control** page, in the **Users** tab, administrator users can create and manage user accounts for an organization's resources in Tenable Web App Scanning.



Users Table

Column	Description
Name	The username for the account.
Full Name	The full name of the user.
Last Login	The date on which the user last successfully logged in to the Tenable Web App Scanning interface.
Last Failed	The date on which the user failed to log in to the Tenable Web App Scanning interface.
Total Failed	The total number of failed login attempts for the user. This number resets when either an administrator or the user resets the password for the user account.
Last API Access	The date on which the user last generated API keys.
Role	The role assigned to the user. For more information, see Roles.

Actions	The actions an administrator user can take with the user (e.g. export a user).

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

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

Create a User Account

Required User Role: Administrator

On the **Users** page, you can create an account for a new user.

Tip: Looking for account creation via a SAML IdP? See the SAML documentation.

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

To create a user account:

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

   The left navigation plane appears.

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

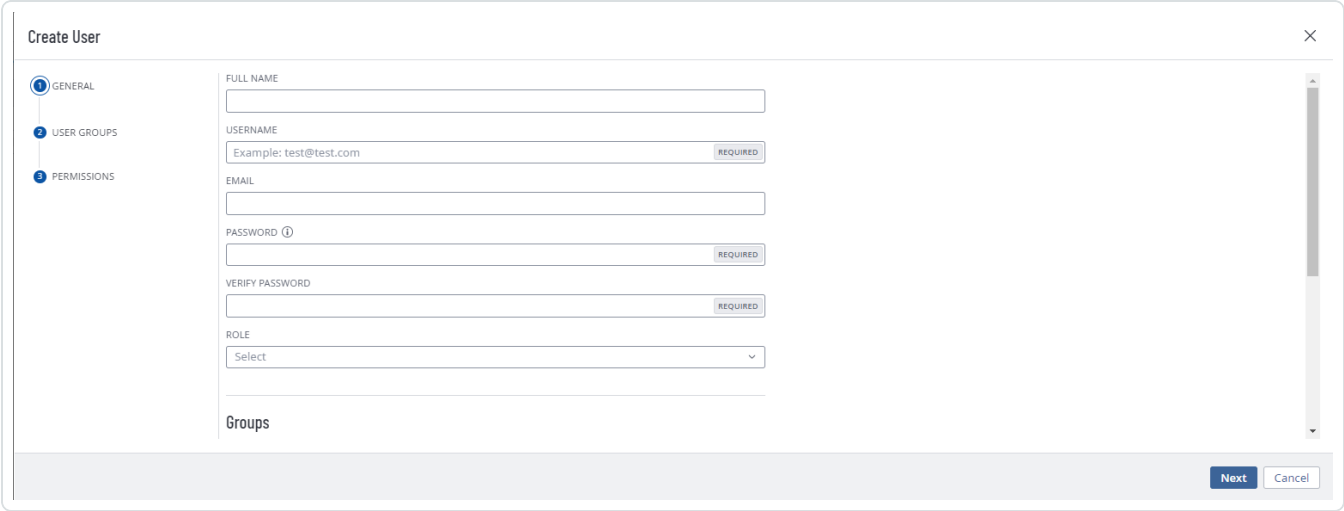
   The **Settings** page appears.

3. Click the **Access Control** tile.

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

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

   The **Create User** page appears.



5. Configure the following options:

> **Note**: To view and configure options in each section, you must select the section in the left menu.

Option	Action
General Section	
Full Name	Type the first and family name of the user.
Username	Type a valid username. A valid username must be in the format: *name@domain* where *domain* corresponds to a domain approved for your Tenable Web App Scanning instance. **Note:** During initial setup, Tenable configures approved domains for your Tenable Web App Scanning instance. To add domains to your instance, contact your Tenable representative. **Note:** Tenable Vulnerability Management usernames cannot include the following characters: ', !, #, $, %, ^, &, *, (,), /, \, |, {, }, [,], ", :, ;, ~, `, <, > and the

	comma "," itself.
Email	Type a valid email address in the format: *name@domain* where *domain* corresponds to a domain approved for your Tenable Web App Scanning instance. This email address overrides the email address set in the **Username** box. If you leave this option empty, Tenable Web App Scanning uses the **Username** value as the user's email address. **Note:** As an Administrator, you can create user accounts with email addresses from unapproved domains. Once a user account is created, you can only change the email address to another approved domain.
Password	Type a valid password. See Password Requirements for more information. In Tenable Web App Scanning, passwords must be at least 12 characters long and contain the following: • An uppercase letter • A lowercase letter • A number • A special character
Verify Password	Type the password again.
Role	In the drop-down box, select the role that you want to assign to the user. **Note**: Administrator users have complete access to all resources on your Tenable Web App Scanning account.

Authentication	Select or deselect the available security setting options. When selected, these settings: **Note**: If you enable the **Password Access** or **SAML** options for a user with a custom role, the user automatically has basic access to your dashboards and widgets. • **API Key** — Allow the user to generate API keys. **Tip**: You can select only this setting to create an API-only user account. • **SAML** —Allow the user to log in to their account using a SAML single sign-on (SSO). For more information, see SAML. • **Username/Password** — Allow the user to log in to their account using a password. **Note**: If you deselect this option, you cannot select the MFA option. • **Two-Factor Required** — Require the user to provide two-factor authentication to log in to their account. **Tip**: You can configure two-factor authentication for your own account on the My Account page.
User Groups Section	
User Groups	Select the user group or groups to which you want to assign the user. By default, a new user belongs to the system-generated **All Users** user group, which assigns the user

	the **Basic** role. Add a user group: • Click anywhere in the **User Groups** box. A search box and drop-down list of roles appear. • (Optional) In the **Search** box, type a user group name. As you type, a list of user groups matching your search appears. • Click the user group you want to add. In the **User Groups** box, Tenable Web App Scanning adds a label representing the user group. • Repeat these steps to add the user to another user group.
Permission Section	
Permissions	In the **Permissions** table, select the permission configurations you want to assign to the user.

6. Click **Save**.

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

Tenable Web App Scanning lists the new user account on the users table.

Edit a User Account

Required User Role: Administrator

To edit a user account:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

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

   The **Edit User** page appears.

5. Configure the following options:

Option	Action
Account Settings	
Full Name	Edit the first and last name of the user.
Username	You cannot edit this option.
Email	Type a valid email address in the format: *name@domain* where *domain* corresponds to a domain approved for your Tenable Web App Scanning instance. This email address overrides the email address set in the **Username** box. If you leave this option empty, Tenable Web App Scanning uses the **Username** value as the user's email address.

	Note: As an Administrator, you can create user accounts with email addresses from unapproved domains. Once a user account is created, you can only change the email address to another approved domain.
New Password	Type a valid password. See Password Requirements for more information. In Tenable Web App Scanning, passwords must be at least 12 characters long and contain the following: • An uppercase letter • A lowercase letter • A number • A special character
Role	In the drop-down box, select the role that you want to assign to the user.
Groups	
User Groups	Select the user group or groups to which you want to assign the user. The user inherits the roles and permissions associated with the user group.
security settings	Select or deselect the available security setting options. When selected, these settings: • **API** — Allow the user to generate API keys. **Tip**: You can select only this setting to create an API-only user account. • **SAML** —Allow the user to log in to their account using a SAML single-sign on (SSO). For more information, see SAML. • **Password Access** — Allow the user to log in to their account using a password.

	Note: If you deselect this option, you cannot select the MFA option. • **MFA** — Require the user to provide two-factor authentication to log in to their account. **Tip**: You can configure two-factor authentication for you own account on the My Account page.

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

   Tenable Web App Scanning saves the changes to the account.

View Your List of Users

Required User Role: Administrator

On the Access Control page, in the **Users** tab, you can view a list of all the users on your Tenable Web App Scanning instance.

To view users and user data for your Tenable Web App Scanning instance:

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

   The **Settings** page appears.

2. Click the **Access Control** tile.

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

3. Click the **Users** tab.

   The **Users** tab appears, containing a table of all Tenable Web App Scanning user accounts on your Tenable Web App Scanning instance. This documentation refers to that table as the *users table*.

Users Table

On the users table, you can view the following information about users on your Tenable Web App Scanning instance.

Column	Description
Name	The username for the account.
Last Login	The date on which the user last successfully logged in to the Tenable Web App Scanning interface.
Last Failed	The date on which the user failed to log in to the Tenable Web App Scanning interface.
Total Failed	The total number of failed login attempts for the user. This number resets when either an administrator or the user resets the

	password for the user account.
Last API Access	The date on which the user last generated API keys.
Role	The role assigned to the user. For more information, see Roles.
Actions	The actions an administrator user can take with the user (e.g. export a user).

Tenable Web App Scanning Password Requirements

Tenable Web App Scanning enforces the following password requirements for all accounts:

Password Criteria

Passwords must be at least 12 characters long and contain the following:

- An uppercase letter
- A lowercase letter
- A number
- A special character

Password Expiration

Tenable Web App Scanning passwords do not expire.

Account Lockout

By default, after 5 failed login attempts, Tenable Web App Scanning locks the user out of their account. When a user is locked out of their account, they can unlock their own account, or an administrator can reset their password.

Password History

You cannot reuse a current or former password.

Change Another User's Password

Required User Role: Administrator

To change the password for another user's account, you must be an administrator. To change your own password, see Change Your Password.

To change another user's password:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

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

   The **Edit User** page appears.

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

6. Click **Save**.

   Tenable Web App Scanning saves the new password for the user account.

Assist a User with Their Account

Required User Role: Administrator

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

As an administrator, you can use the user assist functionality to simulate being logged in as another account. While assisting a user account, you can perform operations in Tenable Vulnerability Management as that user without needing to obtain their password or having to log out of your administrator account.

Note: **User Assist** is available only for user accounts that have one or both of these authentication settings enabled:

- **Username/Password**
- **SAML**

To enable these security settings, see Edit a User Account.

To assist a user with their account:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. In the users table, click the check box for the user account you want to assist.

   The action bar appears at the top of the table.

   Note: You can select only one user to assist at a time.

5. In the action bar, click the 👤 button.

refreshes and displays the default dashboard for the user you are assisting. While you are assisting the user, displays an overlay at the top of each page with the role of the user you are assisting.

To stop assisting a user with their account:

- At the top of any page, in the overlay that displays the role of the user you are assisting, click the ╳ button.

Generate Another User's API Keys

Required User Role: Administrator

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

Administrators can generate API keys for any user account. Other roles can generate API keys for their own accounts. For more information, see Generate API Keys.

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

To generate API keys for another user:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

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

   The **Edit User** page appears.

5. In the **API Keys** section, click **Generate API Keys**.

   Caution: Any existing API keys are replaced when you generate new API keys. You must update the applications where the previous API keys were used.

   A warning message appears.

6. Review the warning and click **Replace & Generate**.

   The **Generate API Keys** text box appears.

   The new access and secret keys for the account appear in the text box.

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

8. Copy the new access and secret keys to a safe location.

   > **Caution**: Be sure to copy the access and secret keys before you navigate away from the **Edit User** page. After you close this page, you cannot retrieve the keys from Tenable Web App Scanning.

Unlock a User Account

Tenable Web App Scanning locks you out if you attempt to log in and fail 5 consecutive times.

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

You can unlock a user account in one of the following ways:

- If a user has access to the email address specified in the user account, they can unlock their own account.
- If a user no longer has access to that email address, another user with administrator privileges can reset the user's password.

Disable a User Account

Required User Role: Administrator

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

Important: Disabling a user account does not disable scheduled reports for that user. Additionally, if the disabled user shared a report with other users, these other users can still generate that report. For more information, see Reports.

To disable a user account:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Select the user or users you want to disable:

   - Select a single user:

     a. In the users table, in the row for the user account you want to disable, click the ⋮ button.

     The action buttons appear in the row.

     b. In the row, click the ⊘ button.

     A confirmation window appears.

   - Select multiple users:

a. In the users table, click the check box for each user you want to disable.

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

b. In the action bar, click the ⊘ button.

   A confirmation window appears.

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

   A success message appears.

   Tenable Web App Scanning disables the selected user or users. In the users table, a disabled user appears in light gray.

   > **Note:** If the user you disable has a session in progress, they may continue to have limited access. However, once they log out, they cannot log back in.

Enable a User Account

Required User Role: Administrator

When you disable a user account, you can enable an account again to restore a user's access.

To enable a user account:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Select the user or users you want to enable:

   Select a single user:

   a. In the users table, in the row for the user account you want to enable, click the ⋮ button.

      The action buttons appear in the row.

      Note: Users appear grayed out while they are disabled.

   b. In the row, click the ✓ button.

      A confirmation window appears.

   Select multiple users:

   a. In the users table, click the check box for each user you want to enable.

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

   b. In the action bar, click the ✓ button.

      A confirmation window appears.

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

   A success message appears.

   Tenable Web App Scanning enables the selected user or users. In the users table, an enabled user appears in black.

Manage User Access Authorizations

Users can access Tenable Web App Scanning using the following methods:

- Username and password login.
- Single sign-on (SSO). For more information, see SAML.
- Tenable Web App Scanning REST API with API keys. For more information, see Generate Another User's API Keys.

When you create a new user, all access methods are authorized by default. Depending on your organization's security policies, you may need to disable certain access methods, for example, disable username and password login to enforce SSO.

Use the Tenable Web App Scanning Platform API to view, grant, and revoke access authorizations for a user. For more information, see Get User Authorizations and Update User Authorizations in the Tenable Developer Portal.

Audit User Activity

Required User Role: Administrator

In Tenable Web App Scanning, the audit log records user events that take place in your organization's Tenable Web App Scanning account. For each event, the log includes information about:

- The action taken
- The time at which the action was taken
- The user ID
- The target entity ID

The audit log provides visibility into the actions that users in your organization take in Tenable Web App Scanning, and can be helpful for identifying security issues and other potential problems.

To view the audit log for your organization's Tenable Web App Scanning account:

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

Logged Events

Audit log events include the following:

Action	Description
audit.log.view	The system received and processed an audit-log request.
session.create	The system created a session for the user. A user login triggers this event.
session.delete	The session aged out, or the user ended a session.
session.impersonation.end	An administrator ended a session where they impersonated another user.
session.impersonation.start	An administrator started a session where they impersonated another user.

user.authenticate.mfa	Two-factor authentication was successful, and login was allowed.
user.authenticate.password	The user authenticated a session start using a password.
user.create	An administrator created a new user account.
user.delete	An administrator deleted a user account.
user.impersonation.end	An administrator stopped impersonating another user.
user.impersonation.start	An administrator started impersonating another user.
user.logout	The user logged out of their session.
user.update	Either an administrator or the user updated a user account.

Export Users

Required User Role: Administrator

On the **Users** page, you can export one or more users in CSV or JSON format.

To export your users:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Users** tab.

   The **Users** page appears. This page contains a table that lists all users for your Tenable Web App Scanning instance.

5. (Optional) Refine the table data. For more information, see Tenable Web App Scanning Workbench Tables.

6. Select the users that you want to export:

Export Scope	Action
Selected users	To export selected users: a. In the users table, select the check box for each user you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**.

	Note: The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 users, select all the users in the list and then click [→ **Export**.
A single user	To export a single user: a. In the users table, right-click the row for the user you want to export. The action options appear next to your cursor. -or- In the users table, in the **Actions** column, click the ⋮ button in the row for the user you want to export. The action buttons appear in the row. b. Click **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  Note: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

7. In the **Name** box, type a name for the export file.
8. Click the export format you want to use:

Format	Description

CSV	A CSV text file that contains a list of users. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Web App Scanning automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of users. Empty fields are not included in the JSON file.

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

    Note: Tenable Web App Scanning allows you to set a maximum of 30 calendar days for export expiration.

11. (Optional) To set a schedule for your export to repeat:
    - Click the **Schedule** toggle.

      The **Schedule** section appears.
    - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
    - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
    - In the **Repeat** drop-down box, select how often you want the export to repeat.
    - In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

      Note: If you select never, the schedule repeats until you modify or delete the export schedule.

12. (Optional) To send email notifications on completion of the export:

    Note: You can enable email notifications with or without scheduling exports.

- Click the **Email Notification** toggle.

  The **Email Notification** section appears.

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

- (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

  > **Note**: Tenable Web App Scanning sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

13. Click **Export**.

    Tenable Web App Scanning begins processing the export. Depending on the size of the exported data, Tenable Web App Scanning may take several minutes to process the export.

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

14. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Delete a User Account

Required User Role: Administrator

Before you delete a user account, you must first disable the user account.

Caution: Once you delete a user account, the account cannot be recovered and the action cannot be reversed.

Caution: Tenable Web App Scanning does not support object migration. When you delete a Tenable Web App Scanning user, the application does not reassign objects belonging to the deleted users. Note that you cannot reassign a Tenable Web App Scanning scan to a new owner if its owner is deleted.

Caution: Before you delete a user account, reassign any associated Remediation projects. These will not be reassigned automatically.

The following table describes what objects are migrated, retained, or permanently deleted upon user deletion:

Object Type	Deleted	Notes
Audit Files in Scans	Yes	Permanently deleted
Scan Schedules	No	Migrated to the new object owner **Note:** Migrated scan schedules may be disabled if they rely on other permanently deleted objects, such as Audit files, Target Groups, or Unmanaged Credentials.
Historical Scan Results	No	Migrated to the new object owner
Scan Templates	No	Migrated to the new object owner
Unmanaged Credentials in Scans	Yes	Permanently deleted
Custom Dashboards/Widgets	Yes	Permanently deleted
Managed Credentials	No	Retained (**Created By** value displays as **null**)

Object Type	Deleted	Notes
Tags	No	Retained (**Created By** value displays as **null**)
Recast/Accept Rules	No	Retained (**Owner** value displays as **Unknown User**)
Exclusions	No	Retained
System Target Groups	No	Retained
User Target Groups	No	Migrated to the new object owner
Saved Searches	Yes	Permanently deleted
Connectors	No	Retained
Sensors	No	Retained

To delete a user account:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. In the users table, in the row for the user account you want to delete, click the ⋮ button.

   A menu appears.

5. In the menu, click the 🗑 button.

   > **Note**: If a user is not disabled, then the 🗑 button does not appear. Disable the user before deleting them.

> **Note:** You cannot delete the Default Administrator account. If you want to delete the Default Administrator account, you must contact Tenable Support.

The user plane appears.

6. In the **Select New Object Owner** drop-down box, select the user to which you want to transfer any of the user's objects (e.g., scan results, user-defined scan templates).
7. Click **Delete**.

   A confirmation message appears.
8. Click **Delete**.

   Tenable Web App Scanning deletes the user and transfers any user objects to the user you designated.

User Groups

User groups allow you to manage user permissions for various resources in Tenable Web App Scanning. When you assign users to a group, the users inherit the permissions assigned to the group. Your organization may utilize groups to provide permissions to batches of users based on the roles of those users and your organization's security posture.

To view your user groups:

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

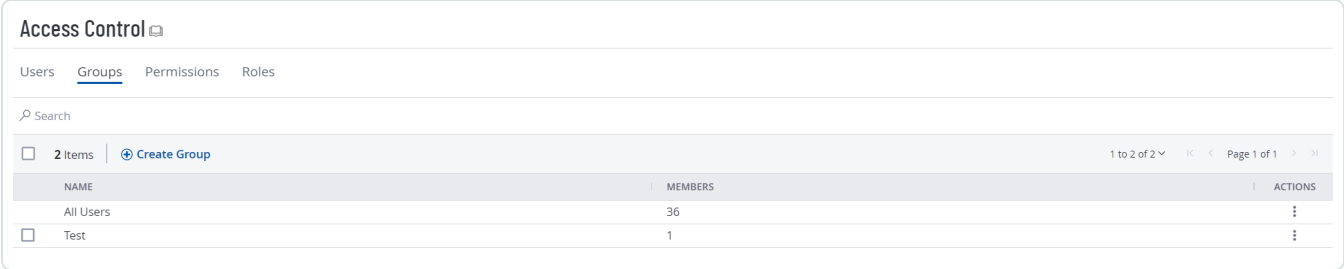
   The **Settings** page appears.

2. Click the **Access Control** tile.

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

3. Click the **Groups** tab.

   The **Groups** page appears.



The **User Groups** page displays a table of all user groups in your Tenable Web App Scanning instance. This documentation refers to that table as the *user groups table*.

The user groups table contains the following columns:

Column	Description
Name	The group name. You can define this name for all user groups except the Tenable-provided **All Users** and **Administrator** groups.
Members	The number of users assigned to the user group.
Actions	The actions you can take with the group.

On the **Groups** tab, you can perform the following actions:

- Create a Group
- Edit a Group
- Export Groups
- Delete a Group

Create a User Group

Required User Role: Administrator

To create a user group:

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

   The left navigation plane appears.

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

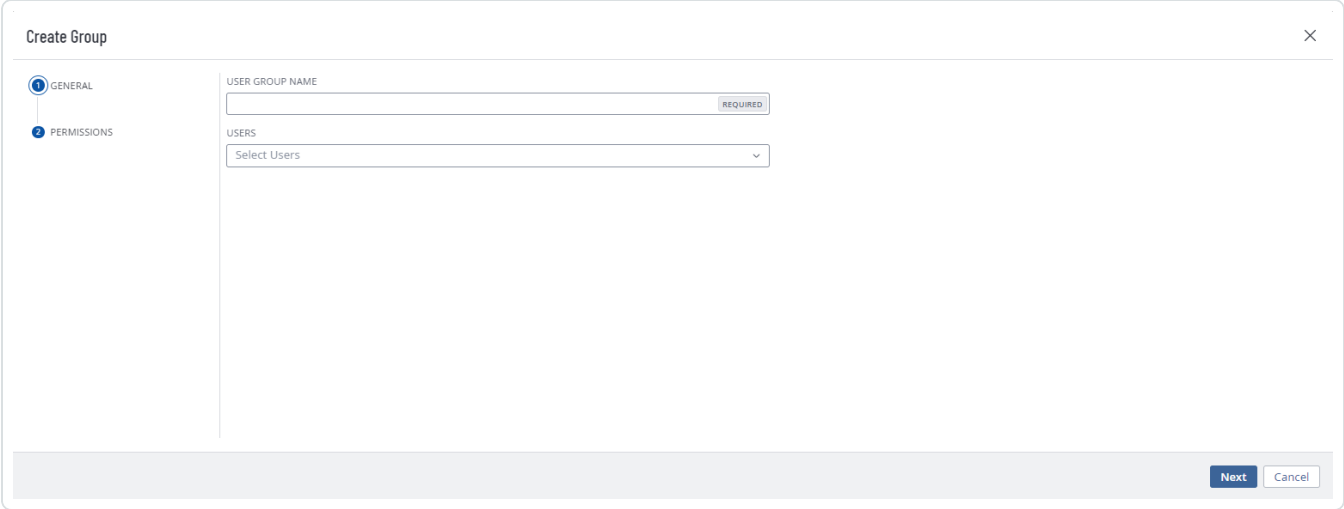
   The **Settings** page appears.

3. Click the **Access Control** tile.

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

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

   The **Create Group** page appears.



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

6. Add users to the group:

a. For each user you want to add, click the Users drop-down box and begin typing a user name.

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

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

   Tenable Web App Scanning adds the user to the list of users to be added to the user group.

   > **Tip:** To remove a user from the list of users to be added, roll over the user and click the ✕ button.

7. Click **Save**.

   Tenable Web App Scanning creates the user group and adds the listed users as members.

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

Edit a User Group

Required User Role: Administrator

To edit a group:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

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

   The **Edit User Group** page appears.

5. Do any of the following:

   - In the **User Group Name** box, type a new group name.
   - Add users to the group:

     a. For each user you want to add, click the **Users** drop-down box and begin typing a user name.

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

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

        Tenable Web App Scanning adds the user to the list of users to be added to the user group.

   - Remove a user from the group:

a. In the **Users** list, click the ✕ button next the user account you want to remove.

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

- Add or remove permissions from the group.

6. Click **Save**.

   Tenable Web App Scanning saves the user group with any changes you made.

Export Groups

Required User Role: Administrator

On the Access Control page, in the **Groups** tab, you can export one or more user groups in CSV or JSON format.

To export your user groups:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Groups** tab.

   The **Groups** tab appears, containing a table that lists all user groups in your Tenable Web App Scanning instance.

5. (Optional) Refine the table data. For more information, see Tenable Web App Scanning Workbench Tables.

6. Do one of the following:

   To export a single group:

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

      The action options appear next to your cursor.

      -or-

      In the groups table, in the **Actions** column, click the ⋮ button in the row for the group you want to export.

The action buttons appear in the row.

b. Click **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

> **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.

To export multiple groups:

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

The action bar appears at the top of the table.

b. In the action bar, click [→ **Export**.

> **Note**: You can individually select and export up to 200 groups. If you want to export more than 200 groups, you must select all the groups on your Tenable Web App Scanning instance by selecting the check box at the top of the groups table and then click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

> **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.

The **Export** plane appear. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  > **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

7. In the **Name** box, type a name for the export file.
8. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of groups. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Web App Scanning automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of groups. Empty fields are not included in the JSON file.

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

    > **Note**: Tenable Web App Scanning allows you to set a maximum of 30 calendar days for export expiration.

11. (Optional) To set a schedule for your export to repeat:

    - Click the **Schedule** toggle.

      The **Schedule** section appears.

- In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
- In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
- In the **Repeat** drop-down box, select how often you want the export to repeat.
- In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

> **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

12. (Optional) To send email notifications on completion of the export:

> **Note**: You can enable email notifications with or without scheduling exports.

- Click the **Email Notification** toggle.

  The **Email Notification** section appears.
- In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
- (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

> **Note**: Tenable Web App Scanning sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

13. Click **Export**.

    Tenable Web App Scanning begins processing the export. Depending on the size of the exported data, Tenable Web App Scanning may take several minutes to process the export.

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

14. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Delete a Group

Required User Role: Administrator

Note: You cannot delete the Tenable-provided **Administrator** or **All Users** user group.

Before you begin:

- Remove all users from the user group. You cannot delete a user group that contains any users.

To delete one or more user groups:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Groups** tab.

   The **Groups** page appears. This page displays a table with all the user groups on your Tenable Web App Scanning account.

5. Do one of the following:

   - To delete a single user group:

     a. In the user groups table, click the ⋮ button for the user group you want to delete.

     A menu appears.

     b. Click the 🗑 **Delete** button.

     A confirmation window appears.

- To delete multiple user groups.

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

    The action bar appears at the top of the table.

    b. In the action bar, click the **Delete** button.

    A confirmation window appears.

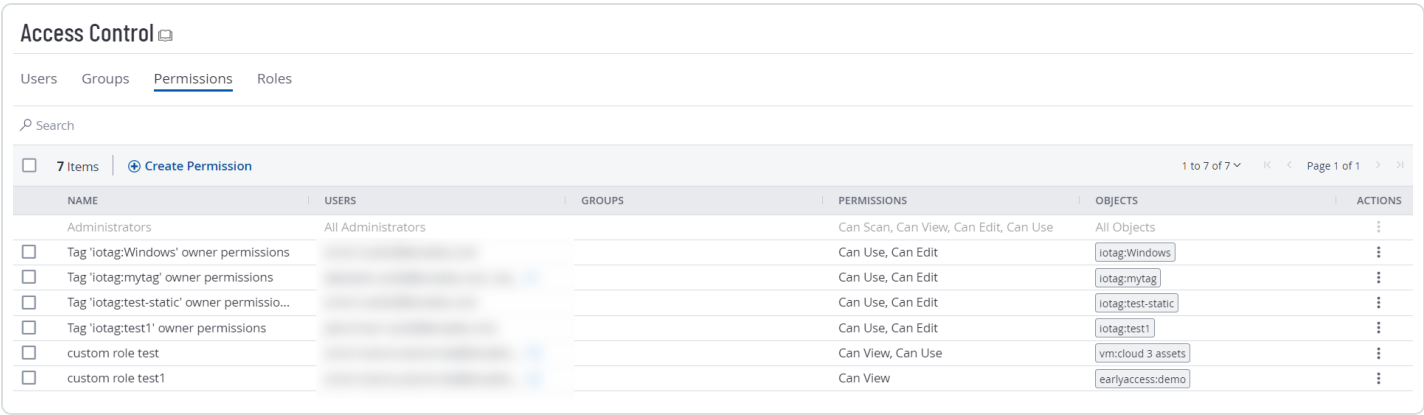
6. In the confirmation window, click **Delete**.

Tenable Web App Scanning deletes the selected user group or groups. The deleted group or groups no longer appear in the user groups table.

Permissions

Tenable Web App Scanning allows you to create and manage configurations that determine which users on your organization's account can perform specific actions with the organization's resources and data. This documentation refers to these configurations as ***permission configurations***[1].

On the **My Accounts** page, each user can view the permission configurations assigned to them. However, only administrator users can view or manage permission configurations for other users. For more information, see Tenable-Provided Roles and Privileges.



When you create a user or user group, you can assign existing permission configurations to them for assets that meet the criteria specified by a previously created tag. In Tenable Web App Scanning, these assets and the tags that define them are called ***objects***[2].

Roles vs. Permissions: What's the difference?

- Roles — Roles allow you to manage privileges for major functions in Tenable Web App Scanning and control which Tenable Web App Scanning modules and functions users can access.
- Permissions — Permissions allow you to manage access to your own data, such as Tags, Assets, and their Findings.

When you create a permission configuration, you must select one or more of the following predefined permissions. These permissions determine the actions users can take with the object or objects defined in the permission configuration.

---

[1]A configuration that administrators can create to determine what actions certain users and groups can perform with a given set of resources.
[2]In a permission configuration, an asset and the tag that defines it.

Permission	Description
Can View	Allows the user or group to view the assets defined by the object. **Note**: If you have a Tenable Lumin license, you must have the **Can View** permission for an asset to view that asset's details. However, you can view the total number of assets licensed to the account regardless of your permissions. You can also view your Cyber Exposure Score (CES) and Asset Exposure Score (AES) values, which are based on the combined risk of all assets licensed to the account. For more information, see Tenable Lumin Metrics.
Can Scan	Allows the user or group to scan the assets defined by the object. **Note:** For a manually entered target to be considered valid, it must meet the following criteria: • The user is an administrator OR • The user has at least Scan Operator role privileges, AND • If the target does not exist within the Tenable Web App Scanning system, the user must have **CanScan** permissions on an object that refers to the target explicitly via IPv4, IPV6 or FQDN. If the object has more than one rule, the rules must be joined by the "Match Any" filter, OR • If the target already exists within the Tenable Web App Scanning system, then it must be tagged by an object for which the user has **CanScan** permissions.
Can Edit	Allows the user or group to edit the tag that defines the object.
Can Use	Allows the user or group to use the tag that defines the object.

To view your permission configurations in Tenable Web App Scanning:

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

   The left navigation plane appears.

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

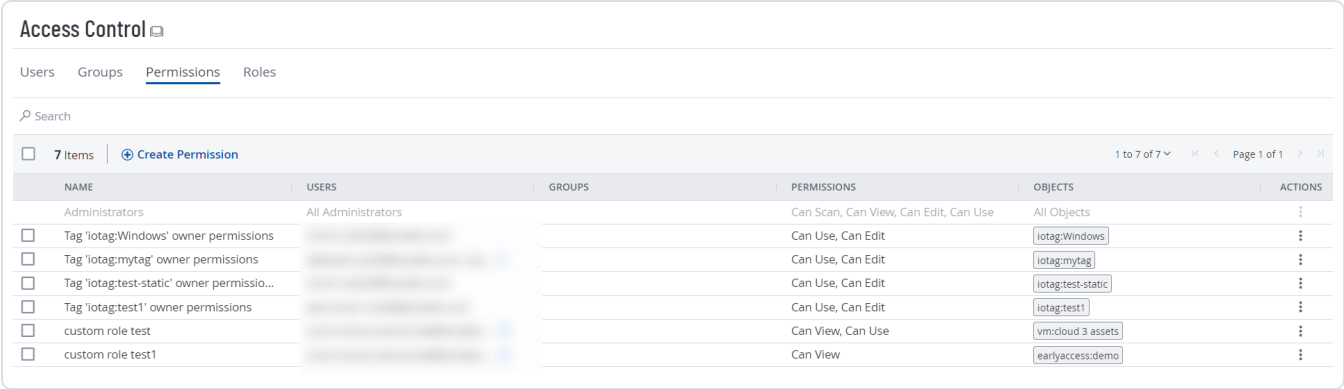
The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Permissions** tab.

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



> **Note**: The first row of the permissions table contains a read-only entry for Administrators. This entry exists to remind you that Administrators have all permissions for every resource on your account. For more information, see Roles.

On the **Permissions** tab, you can perform the following actions:

- Create and Add a Permission Configuration
- Add a Permission Configuration to a User or Group
- Edit a Permission Configuration
- Export Permission Configurations
- Remove a Permission Configuration from a User or Group
- Delete a Permission Configuration

Create and Add a Permission Configuration

Required User Role: Administrator

When you create a permission configuration in Tenable Web App Scanning, you can apply that configuration to one or more users or groups.

Before you begin:

- Create a user or group for your Tenable Web App Scanning account.
- Create a tag for the object for which you want to create a permission.

To create and add a permission configuration to a user or group:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

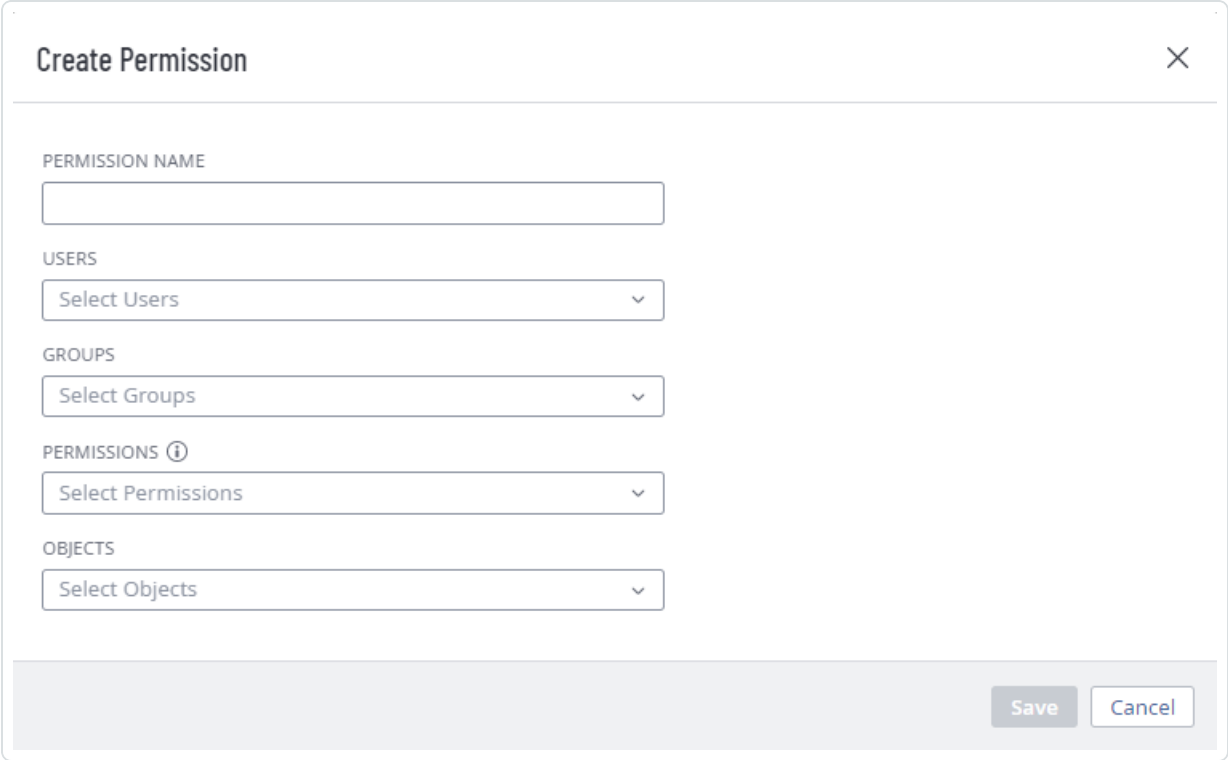
   The **Access Control** page appears. On this page, you can control user and group access to resources in your Tenable Web App Scanning account.

4. Click the **Permissions** tab.

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

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

   The **Create Permission** window appears.



6. In the **Permission Name** box, type a name for the permission configuration.
7. (Optional) In the **Users** drop-down box, select one or more users.

> **Note**: Although the **Users** box is optional, you cannot save the permission configuration unless at least one user or user group is selected.

8. (Optional) In the **Groups** drop-down box, select one or more user groups.

> **Note**: Although the **Groups** box is optional, you cannot save the permission configuration unless at least one user or user group is selected.

> **Note**: You can select **All Users** in the **Groups** drop-down box to assign the permission configuration to all users on your Tenable Web App Scanning instance. However, Tenable recommends that you use caution when assigning the permission configuration to all users because doing so goes against security best practices.

9. In the **Permissions** drop-down box, select one or more permissions.

> **Caution**: Adding the **Can Edit** permission to your permission configuration along with the **Can View** or **Can Scan** permission allows assigned users to change the scope of the assets they can view and scan. Tenable recommends that you combine the **Can Edit** permission with the **Can View** or **Can Scan** permission only for administrator users.

> **Note**: If you select the **Can Edit** permission, Tenable Web App Scanning automatically adds the **Can Use** permission.

10. In the **Objects** drop-down box, select one or more objects to which to apply the permission configuration.

    > **Note**: The objects in the drop-down box are previously created tags that identify and define your assets. For more information, see Permissions.

    > **Tip**: You can select **All Assets** to allow users and group to view or scan all the assets on your instance, regardless of whether the assets match any existing objects. You can also select **All Tags** to allow users and groups on your instance to edit or use all objects on your instance. For more information about objects, see Permissions.

11. Click **Save**.

    A confirmation message appears.

    Tenable Web App Scanning saves your changes. The permission configuration appears on the **Permissions** tab.

Add a Permission Configuration to a User or Group

Required User Role: Administrator

Before you begin:

- Create a user or group for your Tenable Web App Scanning account.
- Create a permission configuration.

To add a permission configuration to a user or group:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Do one of the following:

   - Add a permission configuration to a user:

     a. Click the **Users** tab.

     The **Users** tab appears. This tab contains a list of all the users on your Tenable Web App Scanning instance.

     b. In the users table, click the user to which you want to add a permission configuration.

     The **Edit User** page appears.

     c. In the **Permissions** section, at the top of the table, click **Add Permissions**.

     The **Add Permissions** window appears.

d. Select the check box next to one or more permission configurations.

e. Click **Add**.

The permission configuration appears in the **Permissions** table on the **Edit User** page.

- Add a permission configuration to a user group:

a. Click the **Groups** tab.

The **Groups** tab appears. This tab contains a list of all the user groups on your Tenable Web App Scanning instance.

b. In the groups table, click the group to which you want to add a permission configuration.

The **Edit User Group** page appears.

c. In the **Permissions** section, at the top of the table, click **Add Permissions**.

The **Add Permissions** window appears.

d. Select the check box next to one or more permission configurations.

e. Click **Add**.

The permission configuration appears in the **Permissions** table on the **Edit User Group** page.

5. Click **Save**.

Tenable Web App Scanning saves your changes and adds the permission configuration to the user or group.

Edit a Permission Configuration

Required User Role: Administrator

To edit a permission configuration:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Permissions** tab.

   The **Permissions** tab appears. This tab contains a list of all the permission configurations on your Tenable Web App Scanning instance.

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

   The **Permission Details** page appears.

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

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

8. (Optional) Add or remove a permission:

   Caution: Adding the *Can Edit* permission to your permission configuration along with the *Can View* or *Can Scan* permission allows the users selected in the permission configuration to change the scope of the assets they can view and scan. Tenable recommends that you combine the *Can Edit* permission with the *Can View* or *Can Scan* permission only for administrator users.

   Note: If you select the **Can Edit** permission, Tenable Web App Scanning automatically adds the **Can Use** permission.

> **Note**: You cannot assign permissions to user or groups for a given object that overlap with permissions assigned to them via another permission configuration. For example, if you selected the *Can Edit* permission for an object, but a user listed under **Users** already has the ability to edit that object based on an existing permission configuration, Tenable Web App Scanning generates an error message and prevents you from saving the current permission configuration until you modify your selections to remove the redundancy.

   a. To add a permission, in the **Permissions** drop-down box, select one or more permissions.

   b. To remove a permission, in the **Permissions** drop-down box, click the ✕ button next to each permission you want to remove.

9. (Optional) Add or remove an object.

   a. To add an object, in the **Objects** drop-down box, select one or more objects.

   b. To remove an object, in the **Objects** drop-down box, click the ✕ button next to each object you want to remove.

10. Click **Save**.

    Tenable Web App Scanning saves your changes. The updated permission configuration appears on the **Permissions** tab.

Export Permission Configurations

Required User Role: Administrator

On the **Permissions** page, you can export one or more permission configurations in CSV or JSON format.

To export your permission configurations:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Permissions** tab.

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

   > **Note**: The first row of the permissions table contains a read-only entry for Administrators. This entry exists to remind you that Administrators have all permissions for every resource on your account. For more information, see Roles.

5. (Optional) Refine the table data. For more information, see Tenable Web App Scanning Workbench Tables.

6. Do one of the following:

   ### To export a single permission configuration:

   a. In the permission configurations table, right-click the row for the permission configuration you want to export.

      The action options appear next to your cursor.

-or-

In the permission configurations table, in the **Actions** column, click the ⋮ button in the row for the permission configuration you want to export.

The action buttons appear in the row.

b. Click **Export**.

To export multiple permission configurations:

a. In the permission configurations table, select the check box for each permission configuration you want to export.

The action bar appears at the top of the table.

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

A menu appears.

c. Click [→ **Export**.

> **Note**: You can individually select and export up to 200 permission configurations. If you want to export more than 200 permission configurations, you must select all the permission configurations on your Tenable Web App Scanning instance by selecting the check box at the top of the permission configurations table and then click [→**Export**.

The **Export** plane appears. This plane contains the following:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

> **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

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

8. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of permission configurations. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Web App Scanning automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of permission configurations. Empty fields are not included in the JSON file.

9. (Optional) Deselect any fields you do not want to appear in the export file.

10. In the **Expiration** box, type the number of days before the export file expires.

    Note: Tenable Web App Scanning allows you to set a maximum of 30 calendar days for export expiration.

11. (Optional) To set a schedule for your export to repeat:

    - Click the **Schedule** toggle.

      The **Schedule** section appears.

    - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.

    - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.

    - In the **Repeat** drop-down box, select how often you want the export to repeat.

    - In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

      Note: If you select never, the schedule repeats until you modify or delete the export schedule.

12. (Optional) To send email notifications on completion of the export:

> **Note**: You can enable email notifications with or without scheduling exports.

- Click the **Email Notification** toggle.

  The **Email Notification** section appears.

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

- (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

  > **Note**: Tenable Web App Scanning sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

13. Click **Export**.

    Tenable Web App Scanning begins processing the export. Depending on the size of the exported data, Tenable Web App Scanning may take several minutes to process the export.

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

14. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Remove a Permission Configuration from a User or Group

Required User Role: Administrator

Note: You cannot remove a permission configuration from the Tenable-provided **Administrator** or **All Users** user groups.

To remove a permission configuration from a user or user group:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. To remove a permission configuration from a user:

   - Do one of the following:

     - Remove the permission configuration via the **Users** tab:

       a. Click the **Users** tab.

       The **Users** tab appears. This tab contains a list of all the users on your Tenable Web App Scanning instance.

       b. In the users table, click the user from which you want to remove a permission configuration.

       The **Edit User** page appears.

       c. In the **Permissions** table, in the **Actions** column, click the ⋮ button next to the permission configuration you want to remove.

d. Click the **Remove** button.

   Tenable Web App Scanning removes the permission configuration from the user.

e. (Optional) Repeat for each user from which you want to remove a permission configuration.

- Remove the permission via the **Permissions** tab:

  a. Click the **Permissions** tab.

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

  b. In the table, click the permission configuration you want to remove.

     The **Permission Details** page appears.

  c. Under **Users**, click the button next to each user from which you want to remove the permission configuration.

     Tenable Vulnerability Management removes the permission configuration from the **Users** list.

5. To remove a permission configuration from a user group:

   - Do one of the following:

     - Remove the permission configuration via the **Groups** tab:

       a. Click the **Groups** tab.

          The **Groups** tab appears. This tab contains a list of all the user groups on your Tenable Vulnerability Management instance.

       b. In the user groups table, click the group from which you want to remove a permission configuration.

          The **Edit User Group** page appears.

c. In the **Permissions** table, in the **Actions** column, click the ⋮ button next to the permission configuration you want to remove.

d. Click the **Remove** button.

   Tenable Vulnerability Management removes the permission configuration from the user group.

e. (Optional) Repeat for each user group from which you want to remove a permission configuration.

- Remove the permission configuration via the **Permissions** tab:

a. Click the **Permissions** tab.

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

b. In the table, click the permission you want to remove.

   The **Permission Details** page appears.

c. Under **Groups**, click the ✕ button next to each user group from which you want to remove the permission configuration.

   Tenable Vulnerability Management removes the permission configuration from the **Groups** list.

6. Click **Save**.

   Tenable Vulnerability Management saves your changes and removes the permission from the user or group.

Delete a Permission Configuration

Required User Role: Administrator

Note: You cannot delete the default permission configuration.

To remove a permission configuration from a user or user group:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Permissions** tab.

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

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

6. Click the **Delete** 🗑 button.

   Tenable Web App Scanning deletes the permission configuration.

Roles

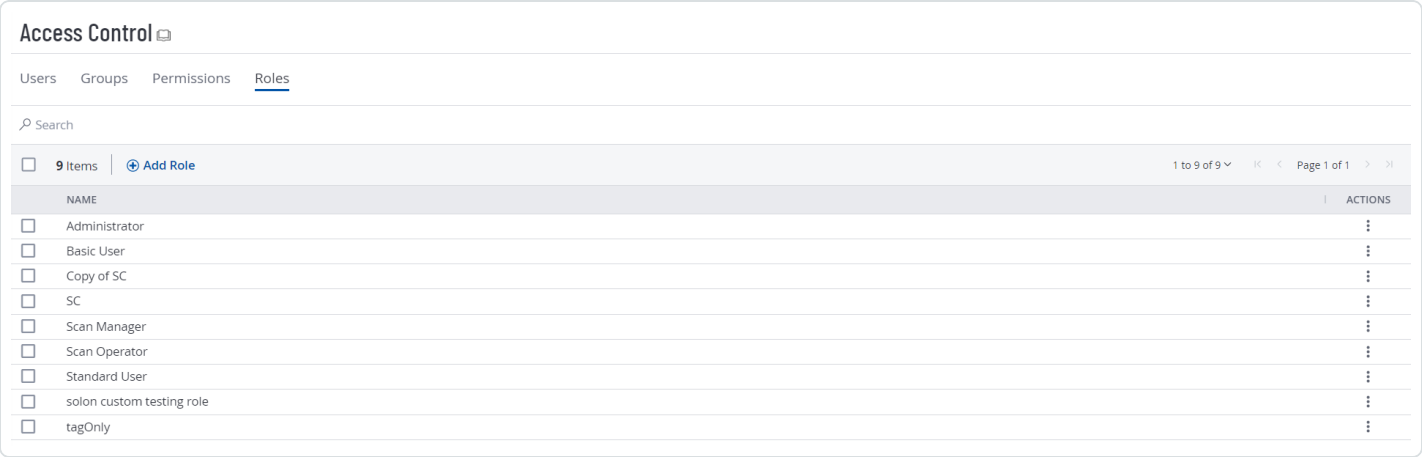
Roles allow you to manage privileges for major functions in Tenable Web App Scanning and control which Tenable Web App Scanning resources users can access in Tenable Web App Scanning.

When you create a user, you must select a role for that user that broadly determine the actions the user can perform.

> **Note**: You can further refine user access to specific resources by assigning permissions to individual users or groups. For more information, see Permissions.

> **Roles vs. Permissions: What's the difference?**
>
> - Roles — Roles allow you to manage privileges for major functions in Tenable Web App Scanning and control which Tenable Web App Scanning modules and functions users can access.
> - Permissions — Permissions allow you to manage access to your own data, such as Tags, Assets, and their Findings.

On the **Roles** page, you can view all Tenable-provided roles and any custom roles created on your Tenable Web App Scanning instance.



You can assign one of the following role types to users:

Role Type	Description
Tenable-Provided Roles and	Contains a predefined set of privileges determined by the Tenable Web App Scanning product specified on your account license. Each role encompasses the privileges of lower roles and adds new privileges. Administrators have the

Privileges	most privileges. Basic users have the fewest.
Custom Roles	Contains a custom set of privileges that allow you to tailor user privileges and access to resources on your Tenable Web App Scanning instance.

To view your user roles:

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

   The left navigation plane appears.

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

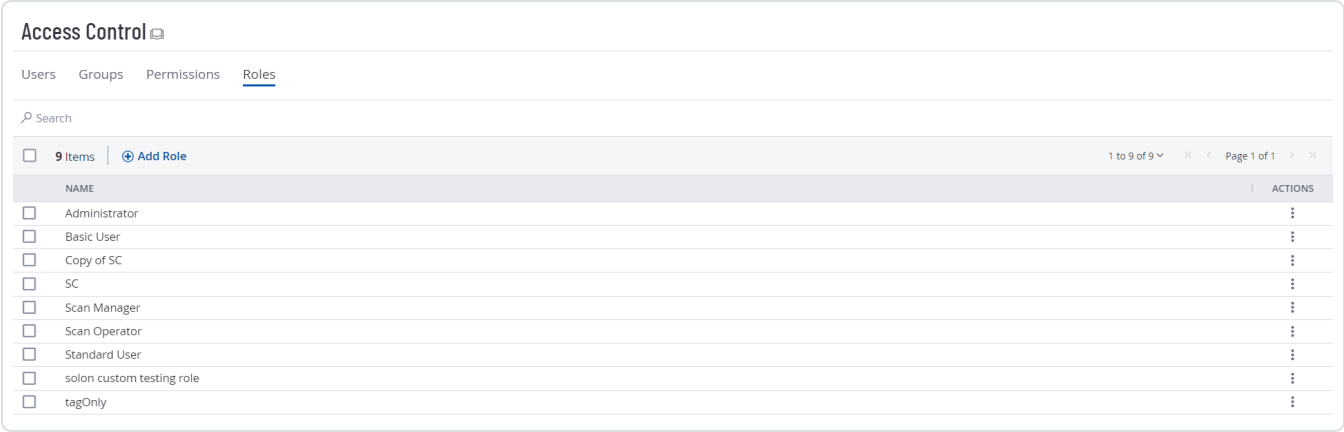
   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Roles** tab.

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



On the **Roles** page, you can complete the following actions:

- Create a Custom Role
- Duplicate a Role
- Edit a Custom Role

- Export Roles
- Delete a Custom Role

Tenable-Provided Roles and Privileges

The following tables describe privileges associated with each Tenable-provided user role, organized by function in their respective product.

> **Note**: You can further refine user access to specific resources by assigning permissions to individual users or groups. For more information, see Permissions.

Area	Tenable Web App Scanning-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
Activity Logs	view, export	-	-	-	-
API Keys	view, modify	view, modify	view, modify	view, modify	view, modify
Account Settings	view, modify	view, modify	view, modify	view, modify	view, modify
Agents	view, delete	view, delete	-	-	-
Agent Freeze Windows	view, create, modify, delete	view, create, modify, delete	-	-	-
Agent Groups	view, create, modify, delete	view, create, modify, delete	-	-	-
Agent Settings	view, modify	view, modify	-	-	-
Assets	view, modify, export, delete	view, modify, export,	view, modify, export,	view, modify, export,	view, export

Area	Tenable Web App Scanning-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
		delete	delete	delete	
Connectors	view, create, modify, delete	-	-	-	-
Dashboards	view, create, modify, export, delete	view, create, modify, export, delete	view, create, modify, export, delete	view, create, modify, export, delete	view, create, modify, export, delete
Exclusions	view, import, export, delete	view, import, export, delete	-	-	-
Exports	view, modify, export, delete	-	-	-	-
General Settings	view, modify	-	-	-	-
Health and Status	view	-	-	-	-
Managed Credentials	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete
PCI Managing	view, import, export, create, modify, delete	-	-	-	-
Recast Rules	view, create,	-	-	-	-

Area	Tenable Web App Scanning-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
	modify, delete				
Reports	view, run, create, modify, delete	view, run, create, modify, delete	view, run, create, modify, delete	view, run, create, modify, delete	view
Report Results	view, delete	view, delete	view, delete	view, delete	view
Scans[1]	view, import, run, create, modify, delete	view, import, run, create, modify, delete	view, import, run, create, modify, delete	view, import, run, create[2], modify, delete	view[3], import
Scan Results	view, export, delete	view, export, delete	view, export, delete	view, export, delete	view, export, delete
Sensors	view, add, modify, delete	view, add, modify, delete	-	-	-
Scanner Groups	view, create, modify, delete	view, create, modify,	-	-	-

[1]User roles determine a user's abilities, but the permissions that a user has for a particular scan are dictated by scan permissions.
[2]Can create scans using existing user-defined policies that are shared with the user.
[3]Can view list of scans, but not scan configuration details.

Area	Tenable Web App Scanning-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
		delete			
Tags[1]	view, create tag category, create tag value, delete, export, assign, unassign	view, create tag value, delete, assign, unassign	view, delete, assign, unassign[2]	view, delete, assign, unassign	view, assign, unassign
User Groups	view, create, modify, delete, export	-	-	-	-
User-Defined Scan Templates	view, import, export, create, modify, delete	view, import, export, create, modify, delete	view, import, export, create, modify, delete	-	-
Users	view, create, modify, delete	-	-	-	-
Vulnerabilities	view, export	view, export	view, export	view, export	view, export

[1]Assigning and Unassigning tags can be done from the Asset Details page.

[2]Standard users must have the **Can Use** permission to view, delete, assign, and unassign tags.

Area	Tenable Web App Scanning-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
Dashboards	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view
Tenable-Provided Scan Templates	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view	-
User-Defined Templates	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	-
Scans (also requires scan permissions)	view, import, create, modify, run, delete	view, import, create, modify, run, delete	view, create, modify, run, delete	view, create[1], modify, run, delete, move to trash	view
Managed Credentials	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete

[1]Can create scans using existing user-defined policies that are shared with the user.

Area	Tenable Web App Scanning-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
Scan Permissions	view, create, modify, delete[1]	view, create, modify, delete[2]	view, create, modify, delete[3]	view, create, modify, delete[4]	-
Scan Results (also requires scan permissions)	view, delete	view, delete	view, delete	view, delete	view, delete

Area	Lumin Exposure View-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
Settings	manage, read	read	read	read	read
Access to Asset Type	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity
Export	manage own	manage own	manage own	manage own	manage own

[1]Administrator users can create, modify, and delete permissions for scans that any user on the account owns.
[2]Scan Manager users can create, modify, or delete permissions only on scans they own.
[3]Standard users can create, modify, or delete permissions only on scans they own.
[4]Scan Operator users can create, modify, or delete permissions only on scans they own.

Area	Lumin Exposure View-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
Exposure Card	create, share, read	create, share, read	create, share, read	share, read	read

Area	Asset Inventory-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
Access to Asset Type	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity
Export	manage own	manage own	manage own	manage own	manage own
Tag	create, edit	create, edit	-	-	-

Area	Attack Path Analysis-Provided Roles and Privileges				
	Administrator	Scan Manager	Standard	Scan Operator	Basic
Export	manage own	manage own	manage own	manage own	manage own
Finding	manage, read	manage, read	read	read	read
Query	search, save	search, save	search, save	search	search

Area	Tenable Identity Exposure-Provided Roles and Privileges	
	Administrator	Custom
Entire Application	Read, Edit, Create	Defined in-application

Area	Tenable Attack Surface Management-Provided Roles and Privileges		
	Business Administrator	Active User	View-Only User
Inventory	manage, add, modify, delete	add, modify, leave	view
Suggestions	manage, add, modify, delete	manage, add, modify, delete	view
Subscriptions	manage, add, modify, delete	manage, add, modify, delete	view
Reports	manage, add, modify, delete	manage, add, modify, delete	view
Txt Records	manage, modify, delete	manage, modify, delete	view
User Accounts	manage, modify, delete	-	-
Business	manage, modify	-	-

Note: By default, Tenable Attack Surface Management users created within Tenable One are given the **Active User** role.

Area	Tenable Cloud Security-Provided Roles and Privileges		
	Administrator	Collaborator	Viewer
Console Tabs	view	view	view
Reports	view, create, schedule, delete	view, create, schedule, delete	view, create

Area	Tenable Cloud Security-Provided Roles and Privileges		
	Administrator	**Collaborator**	**Viewer**
Inventory	view, manage, generate policy	view, manage, generate policy	-
Findings	view, share, manage, disable	view, share, manage	view, share
Administration	view, manage, audit	-	-

Custom Roles

You can create custom roles for users on your Tenable Web App Scanning instance to give those users privileges that are specific to your organization's needs.

When you create a custom role, you can add all or some of the following privileges. You can also edit a custom role to remove privileges. Which privileges you can add to or remove from a role depend on the area of Tenable Web App Scanning where each privilege applies.

> **Note**: A user's access to resources on the account may be limited by their permissions, regardless of their role.

- **Create** — Allows users to create an exposure card or a tag. This privilege is specific to Lumin Exposure View and Asset Inventory, respectively.
- **Manage** — Allows the user to create, modify, and delete in the area where the privilege applies.

  > **Note**: When you add the **Manage** privilege to a custom role, Tenable Web App Scanning automatically adds the **Read** privilege as well. You cannot disable the **Read** privilege unless you first disable the **Manage** privilege.

- **Manage All** — Allows the user to view, modify, and delete exports, including exports that others created.
- **Manage Own** — Allows the user to view, modify, and delete only exports that the user created.
- **Share** — Allows the user to share objects with other users or groups.

  > **Note**: If a custom role does not also have the **Read** permission enabled, they cannot access a list of other users with which to share objects.

- **Read** — Allows the user to view items in the area where the privilege applies.
- **Use** — Allows the user to use Tenable-provided scan templates during Tenable Web App Scanning scan creation.
- **Submit PCI** — Allows the user to submit the scan for PCI validation. For more information, see the *Tenable PCI ASV User Guide*.

- **Search** — Allows the user to search for a query where the privilege applies. This privilege is specific to Attack Path Analysis.
- **Save** — Allows the user to save a query where the privilege applies. This privilege is specific to Attack Path Analysis.
- **Cloud Resource** — Allows the user to access assets from **Cloud Resource** data sources. This privilege is specific to Lumin Exposure View and Asset Inventory.
- **Computing Resource** — Allows the user to access assets from **Computing Resource** data sources. This privilege is specific to Lumin Exposure View and Asset Inventory.
- **Identity** — Allows the user to access assets from **Identity** data sources. This privilege is specific to Lumin Exposure View and Asset Inventory.
- **Web Application** — Allows the user to access assets from **Web Application** data sources. This privilege is specific to Lumin Exposure View and Asset Inventory.

The following table describes the privilege options available for custom roles in different sections of Tenable Web App Scanning.

> **Note**: When you create a custom role, you must include **Read** privileges for the **General Settings**, **License**, and **My Account** sections. If you do not include **Read** privileges for these sections, users assigned to the role cannot log in to Tenable Web App Scanning.

Section	Privilege Options
Asset Inventory	
Access to Asset Type	**Cloud Resource**, **Computing Resource**, **Identity**, **Web Application**
Inventory	**Read**
Export	**Manage Own**
Tag	**Create**, **Edit**
Attack Path Analysis	
Export	**Manage Own**
Finding	**Read**, **Manage**

Query	**Save**, **Search**
Lumin Exposure View	
Access to Asset Type	**Cloud Resource**, **Computing Resource**, **Identity**, **Web Application**
Export	**Manage Own**
Exposure Card	**Read**, **Create**, **Share**
Settings	**Read**, **Manage**
Platform Settings	
Asset	**Read**
Findings	**Read**
My Account	**Read**, **Manage**
Access Control	**Read**, **Manage** **Caution**: Adding the **Manage** privilege in Access Control allows any user with that custom role to create an Administrator user, log in as that user, and change the privileges or permissions for any user on your Tenable Vulnerability Management instance, including their own. If you want to create a user account with the ability to manage your Access Control configurations, Tenable recommends that you assign that user the Administrator role. For more information, see Tenable-Provided Roles and Privileges.
Activity Log	**Read**
General Setting	**Read**, **Manage**
License Information	**Read**
Workspaces	
Asset	**Read**

Finding	**Read**
Vulnerability Management	
Dashboard	**Manage**, **Share** **Note**: Custom role privileges in the Dashboards section do not include the ability to export a dashboard. Assign a Tenable-provided role to a user if you want the user to be able to export dashboards. **Note**: All users can view the dashboards they create or that others share with them regardless of the privileges you assign to them.
Export	**Manage All**, **Manage Own**
Recast/Accept Rule	**Read**, **Manage**
Scan	
Nessus/Agent Scan	**Read**, **Manage**, **Submit PCI**
Scan Exclusion	**Read**, **Manage**
Tenable-Provided Scan Template	**Use**
User-Defined Scan Template	**Read**, **Manage**
Managed Credential	**Read**, **Manage**
Target Group	**Read**, **Manage**

Create a Custom Role

Required User Role: Administrator

Note: Tenable applications do not currently support managing scans and sensors via Custom Roles.

To create a custom role:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Roles** tab.

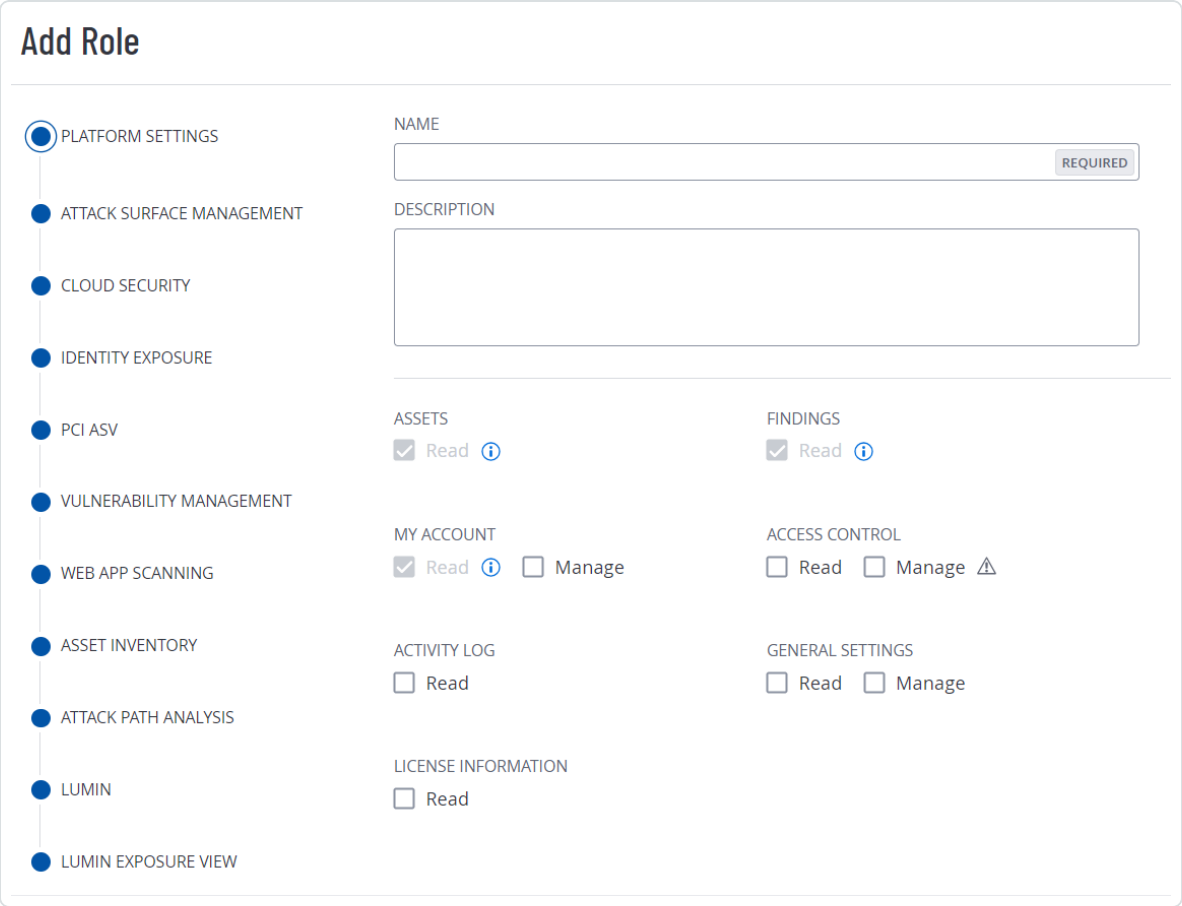
   The **Roles** page appears. This page contains a table that lists all the user roles available on your Tenable Web App Scanning instance.

5. Do one of the following:

   - Duplicate and modify an existing role.
   - Add a new role:

     a. At the top of the table, click **Add Role**.

     The **Add Role** page appears.



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

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

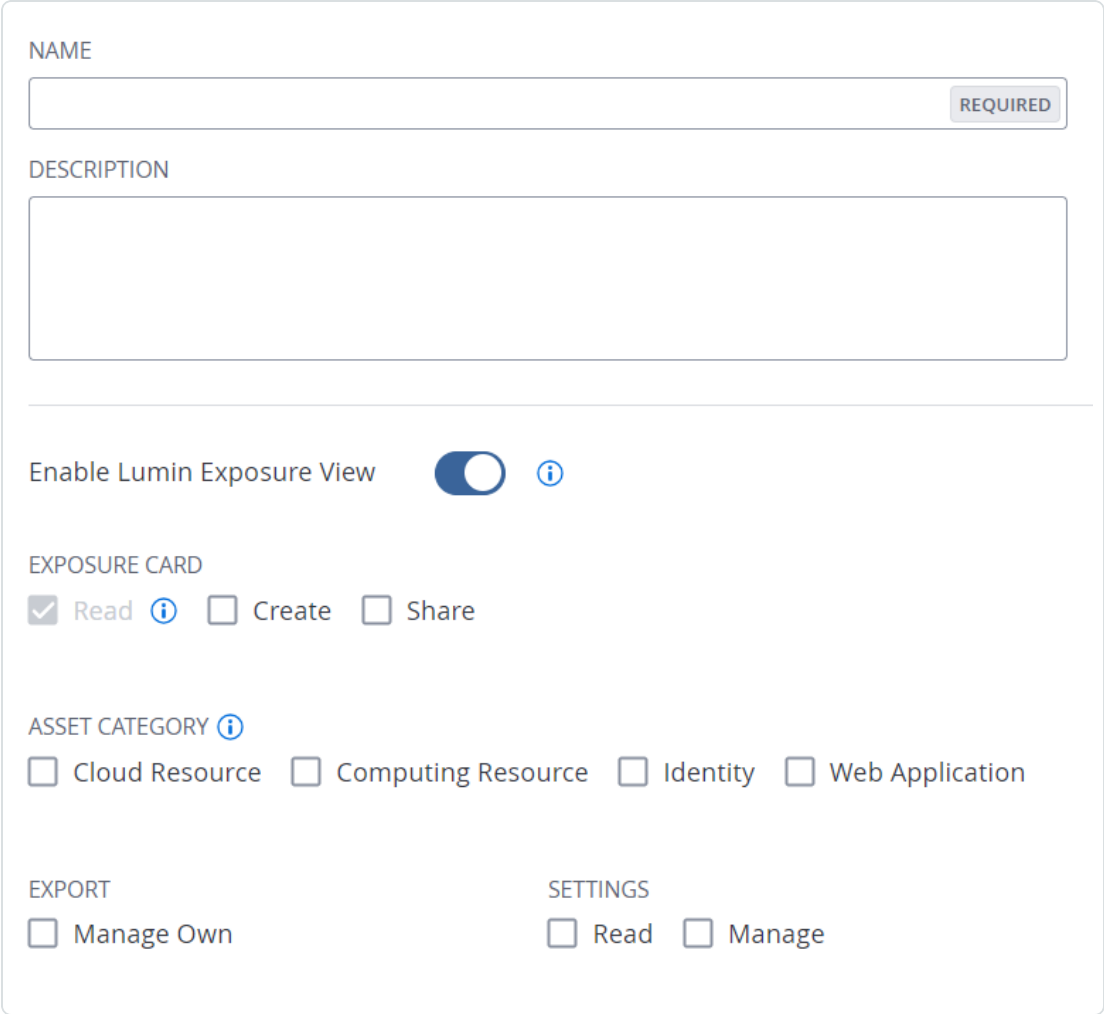
d. Determine the applications to which the custom role has access:

   i. In the left panel, click the application name.

      An **Enable** toggle appears.

   ii. Click the **Enable** toggle to enable or disable access to this application for the custom role you're creating.

      For some applications, privileges associated with the application appear.



iii. Select the check box for each privilege you want to add to your custom role.

e. Click **Save**.

Tenable Web App Scanning saves the role and adds it to the roles table.

Duplicate a Role

Required User Role: Administrator

You can create a custom role by duplicating any existing custom role and then modifying the new role configurations as desired.

Note: You cannot duplicate Tenable-provided roles.

To create a custom role via duplication:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Roles** tab.

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

5. In the roles table, select the check box next to the role you want to duplicate.

   The action bar appears at the top of the table.

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

   A menu appears.

7. Click **Duplicate**.

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

8. Click the duplicated role.

The **Roles Details** page appears. The name, description, and selected privileges for the duplicate role are copied from the original role.

9. Update one or more of the following configurations:

    - Name — In the **Name** box, type a new name for the role.
    - Description — In the **Description** box, type a description for the role.
    - Privileges — Under each Tenable Web App Scanning area, select or deselect the check box next to each privilege you want to add to or remove from the role.

10. Click **Save**.

    Tenable Web App Scanning saves your changes to the duplicate role.

Edit a Custom Role

Required User Role: Administrator

Note: Tenable applications do not currently support managing scans and sensors via Custom Roles.

To edit a custom role:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Roles** tab.

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

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

   The **Roles Details** page appears.

6. Update one or more of the following configurations:

   - Name — In the **Name** box, type a new name for the role.
   - Description — In the **Description** box, type a description for the role.
   - Privileges — Under each Tenable Web App Scanning area, select or deselect the check box next to each privilege you want to add to or remove from the role.

7. Click **Save**.

   Tenable Web App Scanning saves your changes.

Delete a Custom Role

Required User Role: Administrator

Note: You can delete only custom roles. You cannot delete Tenable-Provided Roles and Privileges.

To delete a custom role:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Roles** tab.

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

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

6. Click the **Delete** 🗑 button.

   Tenable Web App Scanning deletes the role and removes it from the roles table.

Export Roles

Required User Role: Administrator

On the **Roles** page, you can export one or more user groups in CSV or JSON format.

To export your user roles:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Roles** tab.

   The **Roles** page appears. This page contains a table that lists all the Tenable-provided and custom roles on your Tenable Web App Scanning instance.

5. (Optional) Refine the table data. For more information, see Tenable Web App Scanning Workbench Tables.

6. Do one of the following:

   To export a single role:

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

      The action options appear next to your cursor.

      -or-

      In the roles table, in the **Actions** column, click the ⋮ button in the row for the role you want to export.

      The action buttons appear in the row.

b. Click **Export**.

To export multiple roles:

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

   The action bar appears at the top of the table.

b. In the action bar, click [→ **Export**.

> **Note**: You can individually select and export up to 200 roles. If you want to export more than 200 roles, you must select all the roles on your Tenable Web App Scanning instance by selecting the check box at the top of the roles table and then click [→**Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  > **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

7. In the **Name** box, type a name for the export file.
8. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of roles. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Web App Scanning automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.

JSON	A JSON file that contains a nested list of roles. Empty fields are not included in the JSON file.

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

    > **Note**: Tenable Web App Scanning allows you to set a maximum of 30 calendar days for export expiration.

11. (Optional) To set a schedule for your export to repeat:

    - Click the **Schedule** toggle.

      The **Schedule** section appears.

    - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
    - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
    - In the **Repeat** drop-down box, select how often you want the export to repeat.
    - In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

      > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

12. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

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

- (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

> **Note**: Tenable Web App Scanning sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

13. Click **Export**.

    Tenable Web App Scanning begins processing the export. Depending on the size of the exported data, Tenable Web App Scanning may take several minutes to process the export.

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

14. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Access Groups

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Note: System target group permissions that controlled viewing scan results and scanning specified targets have been migrated to access groups. For more information, see Scan Permissions Migration.

With access groups, you can control which users or groups in your organization can:

- View specific assets and related vulnerabilities in aggregated scan result views (dashboards in the new interface and workbenches in classic interface).
- Run scans against specific targets and view individual scan results for the targets.

An access group contains assets or targets as defined by the rules you set. Access group rules specify identifying attributes that Tenable Vulnerability Management uses to associate assets or targets with the group (for example, an AWS Account ID, FQDN, or IP address). By assigning permissions in the access group to users or user groups, you grant the usersthe users in the groups view or scan permissions for assets or targets associated with the access group.

Note: When you create or edit an access group, Tenable Vulnerability Management may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.

You can view the status of this assignment process in the **Status** column of the access groups table on the **Access Groups** page.

Only administrators can view, create, and edit access groups. As a user assigned any other role, you can see the access groups to which you belong and the related rules, but not the other users that are in the access group.

Note: The **Access Group** tile appears only if you have one or more assigned access groups or if you are an administrator and users on your Tenable Vulnerability Management are assigned to access groups. Once you convert all your access groups to permission configurations, the **Access Group** tile will no longer appear on your account.

By default, all users have **No Access** to all assets on your Tenable Vulnerability Management instance. Therefore, if you want to assign permissions for assets, you must create an access group and configure user permissions for the group.

> **Note:** Tenable Vulnerability Management applies dynamic tags to any assets, regardless of access group scoping. As a result, it may apply tags you create to assets outside of the access groups to which you belong.

Your organization can create up to 5,000 access groups.

Transition to Permission Configurations

Required User Role: Administrator

Tenable is converting all access groups into permission configurations. As this conversion runs, you may notice your existing access groups undergoing changes. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance. For more information, see Transition to Permission Configurations.

Tenable Vulnerability Management has consolidated and moved user and group management to the **Access Control** page to make access management more intuitive and efficient.

As part of this effort, Tenable Vulnerability Management is replacing Access Groups with Permissions, a feature that allows you to create permission configurations. These permission configurations use tags to determine which users and groups on your Tenable Vulnerability Management instance can perform specific tasks with your organization's resources.

Previously, you had to create access groups to customize access settings for users on your instance. When you create a permission configuration, you can view and manage access settings for users and groups on the **Access Control** page, where you manage users and groups.

Tenable Vulnerability Management plans to retire access groups once all existing access groups are converted into permissible configurations. Tenable Vulnerability Management encourages you to use permission configurations to manage user access to your resources.

What to Expect

As Tenable Vulnerability Management converts your access group data into permission configurations, you may notice the following changes:

- Tenable Vulnerability Management has split up your access groups that have more than one access group type and recreated them as separate groups based on type. For more information about access group types, see Access Group Types.
- Tenable Vulnerability Management has converted all your **Scan Target** type access groups into **Manage Assets** type access groups.

- Tenable Vulnerability Management has updated access group rule filters to match tag rule filters and operators.
- For each access group on your instance that is based on rules instead of tags, Tenable Vulnerability Management has created tags based on the access group rules and updated the groups to reference the new tags. For more information about tag rules, see Tag Rules.
- For each access group on your install, Tenable Vulnerability Management has created permission configurations based on the rules and user permissions defined in that access group.

Task Parity

The following table lists common tasks you may perform on the **Access Groups** page and their equivalent tasks on the **Permissions** page.

Access Groups	Permissions
Create an Access Group	Create and Add a Permission Configuration
View Your Assigned Access Groups	View Your Account Details
Edit an Access Group	Edit a Permission Configuration
Configure User Permissions for an Access Group	• Add a Permission Configuration to a User or Groups • Remove a Permission Configuration from a User or Group
Delete an Access Group	Delete a Permission Configuration

Convert an Access Group to a Permission Configuration

Required User Role: Administrator

Tenable is converting all access groups into permission configurations. As this conversion runs, you may notice your existing access groups undergoing changes. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance. For more information, see Transition to Permission Configurations.

On the **Access Groups** page, you can convert your existing access groups into permission configurations.

Note: Once you convert an access group into a permission configuration, you cannot revert the converted permission configuration into an access group.

Note: The **Access Group** tile appears only if you have one or more assigned access groups or if you are an administrator and users on your Tenable Vulnerability Management are assigned to access groups. Once you convert all your access groups to permission configurations, the **Access Group** tile will no longer appear on your account.

To convert an access group into a permission configuration:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Groups** tiletab.

   The **Access Groups** pagetab appears. This pagetab contains a table that lists the access groups to which you have access.

4. In the access groups table, select the check box for the access group you want to convert.

   The action bar appears at the top of the table.

5. Click **Migrate To Permissions**.

A confirmation message appears.

6. In the confirmation window, click **Migrate To Permissions**.

   Tenable Vulnerability Management begins converting your access group into a permission configuration.

   Tenable Vulnerability Management updates the **Status** column for the access group to reflect the current migration status.

Access Group Types

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

You can create the following types of access groups. Select an access group type based on the identifiers for the targets you want to scan.

Type	Description
Manage Assets	Users can view the asset records created during previous scans and scan the associated targets for those assets. Use this type of access group if the targets you want to view and scan have been scanned before and can be best identified using tags based on asset attributes (for example, operating system or AWS Account ID).
Scan Targets	Users can scan targets associated with the access group and view the results of those scans. Use this type of access group if the targets you want to view and scan have never been scanned before and can only be identified using certain asset identifiers (specifically, FQDN, IPv4 address, or IPv6 address).

Note: The access group type names do not represent a limitation on the user actions that each group controls in relation to the specified targets. For both **Manage Assets** and **Scan Targets** groups, you can grant user permissions to view analytical results for the specified targets in dashboards, to scan the specified targets, or to both view and scan. For more information on user permissions, see Configure User Permissions for an Access Group. For more information on user permissions, see Edit a User Group.

Tip: You can add a user to both access group types if you want to allow the user to scan both types of scan targets.

Restrict Users for All Assets Group

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

The **All Assets** group is the default, system-generated access group to which all assets belong.

By default, the following conditions are true:

- The **All Users** user group, which contains all users in your organization, is assigned to the **All Assets** access group.
- The permissions for the **All Users** group are set to **Can View** and **Can Scan**.

If you do not want all users to scan all assets and view the individual and aggregated results, you must set the permissions for the **All Users** group to **No Access**. Optionally, you can then add specific users or user groups to provide individuals with access to all assets.

Note: When you create or edit an access group, Tenable Vulnerability Management may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.

You can view the status of this assignment process in the **Status** column of the access groups table on the **Access Groups** page.

To restrict user permissions for the **All Assets** group:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Groups** tiletab.

The **Access Groups** pagetab appears. This pagetab contains a table that lists the access groups to which you have access.

4. In the access groups table, click the **All Assets** group.

   The **Edit All Assets Access Group** page appears.

5. In the **Users & Groups** section, locate the listing for the **All Users** group.

6. Remove both the **Can Edit** and **Can Scan** labels from the **All Users** group listing:

   a. Roll over the label.

      The ✕ button appears on the label.

   b. Click the ✕ button.

      Tenable Vulnerability Management removes the label.

   > **Note:** When configuring permissions for the **All Users** user group, Tenable recommends keeping the following in mind:
   >
   > - If you retain the permissions for **All Assets** as **Can View**, all users can view scan results for all assets or targets for your organization.
   > - If you set the permissions for **All Assets** to **Can Scan**, all users can scan all assets or targets for your organization and view the related scan results.

7. (Optional) Configure user permissions for each user or group you want to add to the **All Assets** group.

8. Click **Save**.

   The **Access Groups** page appears. Access to the **All Assets** group is restricted to the user(s) or group(s) you added.

   The **User Groups** tab appears. No users can access assets for your organization.

9. (Optional) In any user group you want to access the **All Assets** group, configure permissions for the **All Assets** access group.

Create an Access Group

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

You can create an access group to group assets based on rules, using information such as an AWS Account ID, FQDN, IP address, and other identifying attributes. You can then assign permissions for users or user groups to view or scan the assets in the access group.

To create an access group:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Access Groups** tiletab.

   The **Access Groups** pagetab appears. This pagetab contains a table that lists the access groups to which you have access.

5. In the upper-right corner of the page, click the ⊕ **Create Access Group** button.

   The **Create Access Group** page appears.

6. In the **General** section, in the **Name** box, type a name for the access group.

   Note: The name must be unique within your organization.

7. In the **Type** section, select the appropriate access group type based on the type of targets you want to scan.

   If you create an access group of one type, then change the type during configuration, Tenable Vulnerability Management prompts you to confirm the action. If you confirm, Tenable Vulnerability Management clears any previously added rule filterscriteria.

8. In the **Rules** section, add rules for the access group.

   Access group rules specify the conditions Tenable Vulnerability Management evaluates when determining whether to include assets or targets in the access group.

   > **Note:** You can add up to 1,000 rules per access group.

   a. In the **Category** drop-down box, select an attribute to filter assets or targets.

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

      Possible operators include:

      • **is equal to**: Tenable Vulnerability Management matches the rule to assets or targets based on an exact match of the specified term.

      > **Note:** Tenable Vulnerability Management interprets the operator as 'equals' for rules that specify a single IPv4 address, but interprets the operator as 'contains' for rules that specify an IPv4 range or CIDR range.

      • **contains**: Tenable Vulnerability Management matches the rule to assets or targets based on a partial match of the specified term.

      • **starts with**: Tenable Vulnerability Management matches the rule to assets or targets that start with the specified term.

      • **ends with**: Tenable Vulnerability Management matches the rule to assets or targets that end with the specified term.

   c. In the text box, type a valid value for the selected category.

> **Tip:** You can enter multiple values separated by commas. For **IPV4 Address**, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

d. (Optional) To add another rule, click the ⊕ **Add** button.

> **Note:** If you configure multiple rules for an access group, the access group includes assets or targets that match *any* of the rules. For example, if you configure two rules -- one that matches on the **Network Name** attribute and one that matches on **IPv4 Address**, the access group includes any assets in the specified network, plus any asset with the specified IPv4 address, regardless of whether that asset belongs to the specified network.

9. In the **Criteria** section, specify the criteria you want Tenable Vulnerability Management to match assets or targets to the access group:

Option	Action
Tags	(Manage Assets groups only) To specify tags criteria for the access group: a. Click the **Tags** option. The **Search** box appears. b. In the **Search** box, click anywhere. A list of your organization's tags appears. c. Click a tag. Tenable Vulnerability Management adds a label representing the tag to the **Search** box. d. Do either of the following: • To add another tag, repeat these steps. • To remove a tag, roll over a tag in the box , then click the ✕ button next to the label. **Note:** Use this option if you want to match assets to the access group using tags as the *only* criteria. To match assets on tags *and* on additional asset

	attributes, use the **Rules** option, then specify one or more tags as rules in addition to other rules.
Rules	Access group rules specify the conditions Tenable Vulnerability Management evaluates when determining whether to include assets or targets in the access group. **Note:** You can add up to 1,000 rules per access group. To specify rules criteria for the access group: a. Click the **Rules** option. b. In the **Category** drop-down box, select an attribute to filter assets or targets. **Note:** You can create a rule based on an existing tag. For more information, see Tags. c. In the **Operator** drop-down box, select an operator. Possible operators include: • **is equal to**: Tenable Vulnerability Management matches the rule to assets or targets based on an exact match of the specified term. **Note:** Tenable Vulnerability Management interprets the operator as 'equals' for rules that specify a single IPv4 address, but interprets the operator as 'contains' for rules that specify an IPv4 range or CIDR range. • **contains**: Tenable Vulnerability Management matches the rule to assets or targets based on a partial match of the specified term. • **starts with**: Tenable Vulnerability Management matches the rule to assets or targets that start with the specified term. • **ends with**: Tenable Vulnerability Management matches the rule to assets or targets that end with the specified term.

d. In the text box, type a valid value for the selected category.

> **Tip:** You can enter multiple values separated by commas. For **IPV4 Address**, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

e. (Optional) To add another rule, click the **Add** button.

> **Note:** If you configure multiple rules for an access group, the access group includes assets or targets that match *any* of the rules. For example, if you configure two rules -- one that matches on the **Network Name** attribute and one that matches on **IPv4 Address**, the access group includes any assets in the specified network, plus any asset with the specified IPv4 address, regardless of whether that asset belongs to the specified network.

> **Note:** In the **Users & Groups** section, you can view the permissions assigned to user groups for the access group. By default, Tenable Vulnerability Management assigns **No Access** permissions to the **All Users** user group for any new access group. You can modify these permissions in the **All Users** group, or you can retain the default permissions and assign higher levels of permissions for the access group in additional user groups. For more information, see Edit a User Group.

10. In the **Users & Groups** section, configure user permissions for the access group.

11. Click **Save**.

    Tenable Vulnerability Management creates the access group. The **Access Groups** page appears.

> **Note:** When you create or edit an access group, Tenable Vulnerability Management may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.
>
> You can view the status of this assignment process in the **Status** column of the access groups table on the **Access Groups** page.

What to do next:

- In a user group, assign permissions for this access group.

Configure User Permissions for an Access Group

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

You can configure access group permissions for individual users or a user group. If you configure access group permissions for a group, you assign all users in that group the same permissions. For more information, see User Groups.

You can assign the following access group permissions to a user or user group:

- **No Access** — (**All Users** user group only) No users (except for users or groups you specifically assign permissions) can scan the assets or targets specified in the access group. Also, no users can view related individual or aggregated scan results for the specified assets or targets.
- **Can View** — The user's view in aggregated scan results (workbenches/dashboards) includes data from scans of the assets or targets specified in the access group. If you assign this permission to the **All Users** group for the access group, all users can view aggregated scan results for the assets or targets in the access group.
- **Can Scan** — Users can scan assets or targets specified in the access group and view individual scan results for the assets or targets. If you do not have this permission, Tenable Vulnerability Management does not prevent you from configuring a scan using assets or targets specified in the access group; however, the scanner does not scan the assets or targets. If you assign this permission to the **All Users** group for the access group, all users can scan the assets or targets in the access group and view the related individual scan results.

User permissions in an access group are cumulative, rather than hierarchical. To allow a user to scan an asset or target *and* view results for that asset or target in aggregated results, you must set the user's permissions in the access group to both **Can View** and **Can Scan**.

Tip: To run scans auditing cloud infrastructure, configure a **Scan Target** access group that includes the target 127.0.0.1, and set user permissions to **Can Scan**.

To configure user permissions for an access group:

1. Create or edit an access group.
2. In the **Users & Groups** section, do any of the following:

   - Edit permissions for the **All Users** user group.

     The default values for the **All Users** user group depends on the access group:

     - For the **All Assets** access group, Tenable Vulnerability Management assigns **Can View** and **Can Scan** permissions to the **All Users** group by default. Tenable recommends you restrict these permissions during initial configuration.
     - For all other access groups, Tenable Vulnerability Management assigns **No Access** permissions to the **All Users** group by default. For these access groups, set permissions for the **All Users** group as follows:

       a. Next to the permission drop-down for the **All Users** group, click the ⌄ button.

       b. Click **Can View**.

       c. Next to the permission drop-down, click the ⌄ button again.

       d. Click **Can Scan**.

       e. Click **Save**.

       Tenable Vulnerability Management allows any user to view or scan the assets or targets in the group.

   - Add a user to the access group.

     a. In the search box, type the name of a user or group.

     As you type, a filtered list of users and groups appears.

     b. Select a user or group from the search results.

     Tenable Vulnerability Management adds the user to the access group with the default **Can View** permissions and adds the related label to the user listing.

     c. (Optional) Add **Can Scan** permissions for the user.

i. Next to the permission drop-down for the user or group, click the ⌄ button.

ii. Click **Can Scan**.

Tenable Vulnerability Management adds a **Can Scan** label to the user listing.

d. Click **Save**.

Tenable Vulnerability Management adds the user to the access group.

- Add permissions for an existing user.

a. Locate the user or group you want to edit.

b. Next to the permission drop-down for the user or group, click the ⌄ button.

c. Click **Can View** or **Can Scan** as appropriate.

Tenable Vulnerability Management adds a label representing the new permission to the user listing.

d. Click **Save**.

Tenable Vulnerability Management saves your changes to the access group.

- Remove permissions from an existing user.

a. Locate the user or group you want to edit.

b. In the label representing the permission you want to remove, click the ✕ button.

Tenable Vulnerability Management removes the permission label from the user listing.

If you remove the last permission for the **All Users** group, Tenable Vulnerability Management sets the group permissions to **No Access**.

If you remove the last permission for an individual user or group, Tenable Vulnerability Management prompts you to remove the user from the access group.

- Remove a user from the access group.

a. Click the ✕ button next to the user or user group you want to delete.

   The user or group disappears from the **Users & Groups** list.

b. Click **Save**.

   Tenable Vulnerability Management saves your changes to the access group.

Edit an Access Group

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

You can edit rules for an existing access group, as well as add or remove users and user groups assigned to the access group.

Note: You cannot edit the name or rulescriteria for the system-generated **All Assets** access group.

You can edit the name and criteria for a user-defined access group. You cannot edit the name or criteria for the system-generated **All Assets** access group.

Note: In the **Users & Groups** section, you can view but not edit the user groups in which you've configured permissions for the access group. To change these permissions, edit each user group.

To edit an access group:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Control** tile.

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

4. Click the **Access Groups** tiletab.

   The **Access Groups** pagetab appears. This pagetab contains a table that lists the access groups to which you have access.

5. In the access groups table, click the access group you want to edit.

   The **Edit Access Group** page appears.

6. In the **General** section, in the **Name** box, type a new name for the access group.

7. In the **Type** section, edit the access group type.

   a. Select the access group type to which you want to change.

      Tenable Vulnerability Management prompts you to confirm the action.

   b. Click **Confirm**.

      Tenable Vulnerability Management clears any previously added rule filterscriteria.

8. In the **Rules** section, edit the access group rules.

   Access group rules specify the conditions Tenable Vulnerability Management evaluates when determining whether to include assets or targets in the access group.

   - To edit an existing rule, modify the category, operator, and/or value as needed.
   - To delete an existing rule, click the ✕ button next to the rule.
   - To add a new rule, click ⊕ **Add** and create a new rule.

9. In the **Criteria** section, specify the criteria you want Tenable Vulnerability Management to use when matching assets or targets to the access group:

Option	Action
Tags	(Manage Assets groups only) To specify tags criteria for the access group: a. Click the **Tags** option. The **Search** box appears. b. In the **Search** box, click anywhere. A list of your organization's tags appears. c. Click a tag.

	Tenable Vulnerability Management adds a label representing the tag to the **Search** box. d. Do either of the following: • To add another tag, repeat these steps. • To remove a tag, roll over a tag in the box , then click the ✕ button next to the label. **Note:** Use this option if you want to match assets to the access group using tags as the *only* criteria. To match assets on tags *and* on additional asset attributes, use the **Rules** option, then specify one or more tags as rules in addition to other rules.
Rules	Access group rules specify the conditions Tenable Vulnerability Management evaluates when determining whether to include assets or targets in the access group. **Note:** You can add up to 1,000 rules per access group. To specify rules criteria for the access group: a. Click the **Rules** option. b. In the **Category** drop-down box, select an attribute to filter assets or targets. **Note:** You can create a rule based on an existing tag. For more information, see Tags. c. In the **Operator** drop-down box, select an operator. Possible operators include: • **is equal to**: Tenable Vulnerability Management matches the rule to assets or targets based on an exact match of the specified term.

> **Note:** Tenable Vulnerability Management interprets the operator as 'equals' for rules that specify a single IPv4 address, but interprets the operator as 'contains' for rules that specify an IPv4 range or CIDR range.

• **contains**: Tenable Vulnerability Management matches the rule to assets or targets based on a partial match of the specified term.

• **starts with**: Tenable Vulnerability Management matches the rule to assets or targets that start with the specified term.

• **ends with**: Tenable Vulnerability Management matches the rule to assets or targets that end with the specified term.

d. In the text box, type a valid value for the selected category.

> **Tip:** You can enter multiple values separated by commas. For **IPV4 Address**, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

e. (Optional) To add another rule, click the **Add** button.

> **Note:** If you configure multiple rules for an access group, the access group includes assets or targets that match *any* of the rules. For example, if you configure two rules -- one that matches on the **Network Name** attribute and one that matches on **IPv4 Address**, the access group includes any assets in the specified network, plus any asset with the specified IPv4 address, regardless of whether that asset belongs to the specified network.

10. In the **Users & Groups** section, configure user permissions for the access group.

11. Click **Save**.

    Tenable Vulnerability Management updates the access group with your changes. The **Access Groups** page appears.

> **Note:** When you create or edit an access group, Tenable Vulnerability Management may take some time to assign assets to the access group, depending on the system load, the number of matching assets, and the number of vulnerabilities.

> You can view the status of this assignment process in the **Status** column of the access groups table on the **Access Groups** page.

What to do next:

- (Optional) Modify the access group permissions in a user group.

View Assets Not Assigned to an Access Group

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

If an asset does not match any access group rulescriteria, Tenable Vulnerability Management does not assign the asset to any access group. These unassigned assets are only visible to usersuser groups assigned permissions in the **All Assets** group. If your organization limits membership in the **All Assets** group, users who are not members of users in user groups without permissions in the **All Assets** group are unable to see these unassigned assets, but this limited visibility may not be immediately obvious to them. If you are a member of a user group with permissions in the the **All Assets** group, you can use a filter to identify these unassigned assets.

To view assets that are not assigned to an access group:

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

   The left navigation plane appears.

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

   The **Assets** page appears.

3. Create a filter with the following settings:

   - Category: **Belongs to Access Group**
   - Operator: **is equal to**
   - Value: **false**

4. Click **Apply**.

   The assets table updates to display all assets that are not assigned to an access group.

View Your Assigned Access Groups

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

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

As an administrator, you can view the rules and assigned users and user groups for any access group. You can also edit access group parameters.

As a user in any other role, you can view your assigned access groups. This view includes the rules associated with each access group, but excludes the other users or user groups assigned to the access group. You cannot edit any access group settings.

Note: The **Access Group** tile appears only if you have one or more assigned access groups or if you are an administrator and users on your Tenable Vulnerability Management are assigned to access groups. Once you convert all your access groups to permission configurations, the **Access Group** tile will no longer appear on your account.

To view your assigned access groups:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Groups** tiletab.

   The **Access Groups** pagetab appears. This pagetab contains a table that lists the access groups to which you have access.

4. The **Access Groups** page contains a table that includes the following information:

- **Name** — The access group name.
- **Owner** — The access group owner.
- **Permission Type** — The access group type.
- **Last Modified** — The date on which a user in your organization last changed the access group configuration.
- **Last Modified By** — The user in your organization who last changed the access group configuration.
- **Status** — The status of the Tenable Vulnerability Management process matching assets to the access group. Possible values are **Processing** or **Completed**. To view the percentage complete for an ongoing process, roll over the Processing status.

5. (Optional) Click an access group to view more details.

   The **Edit Access Group** page appears.

   For administrators, this page contains both rules and assigned users and user groups, and you can edit all access group parameters.

   For users in any other role, this page contains rules only, and you cannot edit the rules.

Delete an Access Group

Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

Required User Role: Administrator

Note: You cannot delete the system-generated **All Assets** group.

To delete one or more access groups:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Access Groups** tiletab.

   The **Access Groups** pagetab appears. This pagetab contains a table that lists the access groups to which you have access.

4. Select the access groups you want to delete:

   - Select a single access group:

     a. In the access groups table, roll over the access group you want to delete.

        The action buttons appear in the row.

     b. Click the 🗑 button.

        A confirmation window appears.

   - Select multiple access groups:

a. In the access groups table, select the check boxes next to the access groups you want to delete.

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

b. In the action bar, click the 🗑 button.

   A confirmation window appears.

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

   Tenable Vulnerability Management deletes the selected access group or groups and updates the access group table.

Access Group Rule Filters

> Tenable is retiring access groups. Moving forward, Tenable recommends that you use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance and that you convert your existing access groups into permission configurations. For more information, see Transition to Permission Configurations.

You can use the filters described in the following sections to create rules for access groups. For more information, see:

- Tenable-provided Filters
- Guidelines for Tenable-provided Filters
- Tag Filters

Tenable-provided Filters

The last two columns in the following table indicate whether you can use the filter with the **Manage Assets** or **Scan Targets** group type.

Filter	Description	Manage Assets	Scan Targets
AWS Account ID	The canonical user identifier for the Amazon Web Services (AWS) account associated with the asset. For more information, see "AWS Account Identifiers" in the AWS documentation.	yes	no
AWS Availability Zone	The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see "Regions and Availability Zones" in the AWS documentation.	yes	no
AWS EC2 AMI ID	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see	yes	no

	the Amazon Elastic Compute Cloud Documentation.		
AWS EC2 Instance ID	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.	yes	no
AWS EC2 Name	The name of the virtual machine instance in Amazon EC2.	yes	no
AWS EC2 Product Code	The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2.	yes	no
AWS Region	The region where AWS hosts the virtual machine instance, for example, 'us-east-1'. For more information, see "Regions and Availability Zones" in the AWS documentation.	yes	no
AWS Security Group	The security group to which you have assigned the virtual machine instance in Amazon EC2. For more information, see Security Groups in the Amazon Virtual Private Cloud User Guide.	yes	no
AWS Subnet ID	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.	yes	no
AWS VPC ID	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.	yes	no
Azure Resource ID	The unique identifier of the resource in the Azure Resource Manager. For more	yes	no

	information, see the Azure Resource Manager Documentation.		
Azure VM ID	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see "Accessing and Using Azure VM Unique ID" in the Microsoft Azure documentation.	yes	no
FQDN/Hostname	One of the following: • The fully-qualified domain name of the asset. • The hostname of the asset.	yes	yes
Google Cloud Instance ID	The unique identifier of the virtual machine instance in Google Cloud Platform (GCP).	yes	no
Google Cloud Project ID	The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see "Creating and Managing Projects" in the GCP documentation.	yes	no
Google Cloud Zone	The zone where the virtual machine instance runs in GCP. For more information, see "Regions and Zones" in the GCP documentation.	yes	no
IPv4 Address	An IPv4 address for the asset. For this filter, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).	yes	yes
IPv6 Address	An IPv6 address for the asset.	no	yes

MAC Address	The MAC address of the asset.	yes	no
NetBIOS Name	The NetBIOS name for the asset.	yes	no
Network Name	The name of the network to which the asset belongs.	yes	no
Operating System	The operating system installed on the asset.	yes	no
Qualys Asset ID	The Asset ID of the asset in Qualys. For more information, see the Qualys documentation.	yes	no
Qualys Host ID	The Host ID of the asset in Qualys. For more information, see the Qualys documentation.	yes	no
ServiceNow Sys ID	The unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.	yes	no

Guidelines for Tenable-provided Filters

- When configuring rules for **Scan Targets** access groups, the asset attribute type must match the target format used in the related scan. For example, if a **Scan Targets** access group rule filters on the **FQDN/Hostname** attribute, the related scan succeeds if the scan target is specified in FQDN or hostname format, but fails if the scan target is specified in IPv4 address format.

Tag Filters

In Tenable Vulnerability Management, tags allow you to add descriptive metadata to assets that helps you group assets by business context. For more information, see Tags.

You can use the tags you create to assign assets to **Manage Assets** access groups.

To add a tag filter to a rule:

1. In the **Category** drop-down box, select **Tags**.
2. In the **Operator** drop-down box, select **contains**.
3. In the text box, type the tag category and value you want to search for in the following format:

   `Category Name:Value Name`

4. Continue creating rules and/or save the access group as described in Create an Access Group.

> **Note:** Tag categories with 100,000 or more associated values cannot be applied as a rule to access groups.

Scan Permissions Migration

System target group permissions that controlled whether users can scan specified targets have been migrated to access groups.

> **Note**: Tenable plans to deprecate access groups in the near future. Currently, you can still create and manage access groups. However, Tenable recommends that you instead use permissions to manage user and group access to resources on your Tenable Vulnerability Management instance.

This migration affects your existing Tenable Vulnerability Management configuration as follows:

Component	Action
Existing access group	Tenable Vulnerability Management: • Updates any existing access group to an access group of the **Manage Assets** type. • Replaces the **All Users** toggle with a default **All Users** group. • Assigns **Can View** permissions to any existing users or user groups that currently have view access.
Existing system target groups	For each existing system target group, Tenable Vulnerability Management: • Creates a new access group with a type of **Scan Targets**. This access group specifies the same scan targets as the existing system target group. Tenable Vulnerability Management lists `migration` as the owner of the migrated access groups. • Moves any user with **Can Scan** permissions in the system target group to the new access group, and assigns the user **Can Scan** permissions for that access group. To ensure users can view results for the targets, configure **Can View** permissions for users in the access group. **Note:** This migration does *not* delete existing system target groups. The migration removes only the **Can Scan** permissions from the system target groups.

	Note: If, at the time of migration, an existing target group includes scan permissions, a **Scan** label may appear for the group in the **Permissions** column of the target groups table in the new Tenable Vulnerability Management user interface. This label indicates historical scan permissions only; access groups specify the current scan permissions.
Existing scan configurations, dashboard filters, and saved searches	Existing scan configurations retain the system target group as a target setting. Existing dashboard filters and saved searches retain the system target group as a filter setting. If you have **Can Use** permissions for a system target group, you can continue to use the system target group to specify a group of targets in a scan configuration and to use the system target group in filters for dashboards and searches. However, to specify which users can view scan results for the targets, configure **Can View** permissions in the appropriate access group.

Activity Logs

Required User Role: Administrator

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

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

To view your activity logs:

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

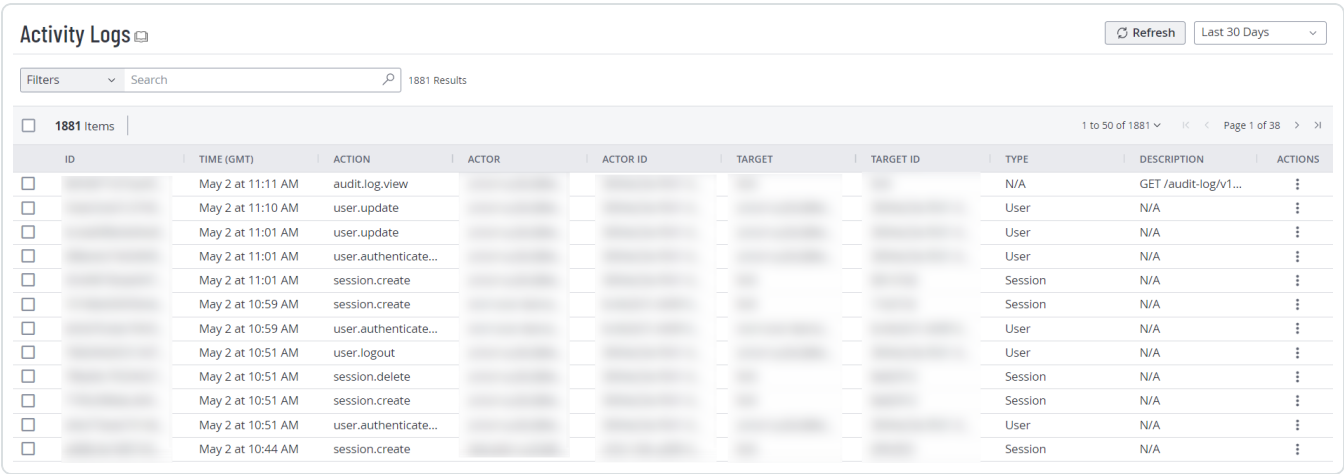
   The left navigation plane appears.

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

   The **Settings** page appears.

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

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



4. (Optional) Refine the table data. For more information, see Tenable Web App Scanning Tables.

5. (Optional) Apply a filter to the table:

Filter	Description
Actor ID	The ID of the account performing the action.
Target ID	The ID of the account affected by the action, if any.
Action	The type of action.
Date	The date the action was performed.

6. (Optional) To refresh the activity logs table, in the upper-right corner, click the **Refresh** button.
7. (Optional) Filter the table by a specific time period:
   - **Last 7 Days**
   - **Last 14 Days**
   - **Last 30 Days**
   - **Last 90 Days**
   - **All**

What to do next:

- (Optional) Export one or more activity logs.

Export Activity Logs

Required User Role: Administrator

On the **Activity Logs** page, you can export one or more activity logs in CSV or JSON format.

To export your activity logs:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

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

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

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

5. Select the activity logs that you want to export:

Export Scope	Action
Selected activity logs	To export selected activity logs: a. In the activity logs table, select the checkbox for each activity log you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 activity logs, select all the activity logs in the list and then click [→ **Export**.

A single activity log	To export a single activity log: a. In the activity logs table, right-click the row for the activity log you want to export. The action options appear next to your cursor. -or- In the activity logs table, in the **Actions** column, click the ⋮ button in the row for the activity log you want to export. The action buttons appear in the row. b. Click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  > **Note**: By default, all fields are selected.

- A text box to set the number of days before the export ages out.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

6. In the **Name** box, type a name for the export file.
7. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of activity logs. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Web App Scanning automatically inputs a single

	quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of activity logs. Empty fields are not included in the JSON file.

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

   > **Note**: Tenable Web App Scanning allows you to set a maximum of 30 calendar days for export expiration.

10. (Optional) To set a schedule for your export to repeat:

    - Click the **Schedule** toggle.

      The **Schedule** section appears.

    - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
    - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
    - In the **Repeat** drop-down box, select how often you want the export to repeat.
    - In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

      > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

11. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

- In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
- (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

> **Note**: Tenable Web App Scanning sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

12. Click **Export**.

    Tenable Web App Scanning begins processing the export. Depending on the size of the exported data, Tenable Web App Scanning may take several minutes to process the export.

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

13. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file from the Exports page.

Tags

You can add your own business context to assets by tagging them with descriptive metadata in Tenable Web App Scanning. An asset tag is primarily composed of a *Category*:*Value* pair. For example, if you want to group your assets by location, create a *Location* category with the value *Headquarters*. You can then manually apply the tag to individual assets, or you can add rules to the tag that enable Tenable Web App Scanning to apply the tag automatically to matching assets.

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

> **Note:** If you want to create tags without individual categories, Tenable recommends that you add the generic category *Category*, which you can use for all your tags.

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

To view your tags:

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

   The left navigation plane appears.

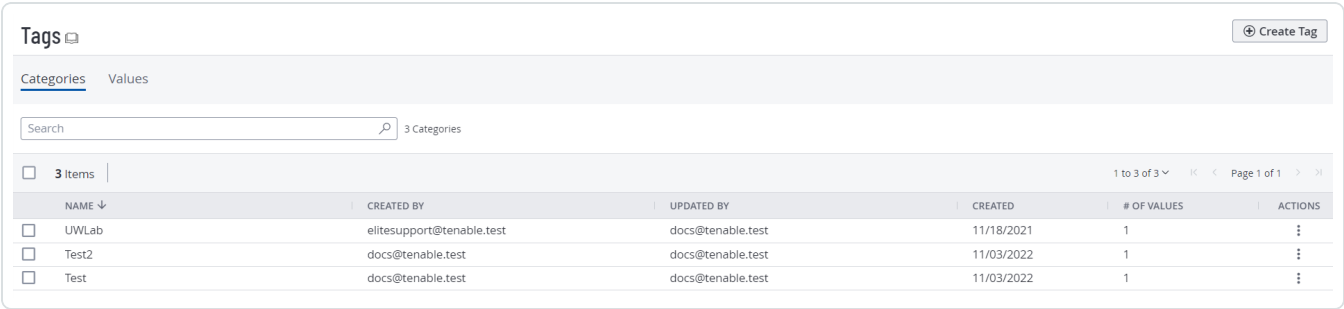
2. In the left navigation plane, click **Settings**.

   The **Settings** page appears.

3. Click the **Tagging** tile.

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

   The **Categories** tab is active.



4. Do one of the following:

To view the categories to which your all the tags on your Tenable Web App Scanning instance are assigned:

a. View your tag categories and relevant data about them in the **Categories** table:

Column	Description
Name	The name of the tag.
Created By	The username of the user who created the tag.
Last Used By	The username of the user who most recently created or edited the tag value or category.
Created	The date on which the tag was created.
# of Values	The number of tag values associated with the tag category.
Actions	The actions you can perform with the tag.

To view all the tags on your Tenable Web App Scanning instance:

a. Click the **Values** tab.

   The **Values** page appears, containing a table of all the tags on your Tenable Web App Scanning instance.

b. View your tags and relevant data about them in the **Values** table:

Column	Description
Name	The name of the tag.
Created By	The username of the user who created the tag.
Updated By	The username of the user who last updated the tag category or value.
Created	The date on which the tag was created.
Applied	Indicates whether the tag is applied **Manually** or **Automatically**.

Last Processed	The date and time when Tenable Web App Scanning last processed the scan and applied it to all relevant assets.
Assessment	Indicates whether Tenable Vulnerability Management has finished identifying and apply the tag to all matching assets.
Actions	The actions you can perform with the tag.

Examples: Asset Tagging

See the following configuration examples to tag assets for common use cases. For general information about tags, see Tags.

- Example: Automatically Tag by Installed Software
- Example: Manually Tag by Priority
- Example: Update ACR Values on Tagged Assets

Example: Automatically Tag by Installed Software

Your company manages assets that run on two software types: Oracle and Wireshark. Your company assigns asset ownership to employees based on the software type. Employees must resolve any vulnerabilities identified on assets with the software type they manage.

As an administrator, you can create an automatic tag for each software type. Then, employees can search for assets by the **Installed Software** tag and filter Tenable Web App Scanning assets by the software type they manage.

> **Note:** For more precise results, set the tag value to the appropriate NVD Common Platform Enumeration (CPE), for example, `cpe:/a:microsoft:office`.

To automatically tag assets by installed software:

1. Create and automatically apply a tag for Oracle assets using the following settings:

Option	Value
Category	*Installed Software*
Value	*Oracle*
Rules	Enabled, with the following rule specified: • **Match All** • **Category**: *Installed Software* • **Operator**: *is equal to* • **Value**: *Oracle*

2. Create and automatically apply a tag for Wireshark assets using the following settings:

Option	Value
Category	*Installed Software*
Value	*Wireshark*
Rules	Enabled, with the following rule specified: • **Match All** • **Category**: *Installed Software* • **Operator**: *is equal to* • **Value**: *Wireshark*

3. Instruct employees to use the new tags to filter assets in the assets table or to search for assets from the tags table.

Example: Manually Tag by Priority

Your company owns sensitive assets and you want employees to prioritize addressing vulnerabilities on these assets first, regardless of the asset's other attributes (for example, the asset's VPR).

To make sure employees view and mediate these sensitive assets first, you can create a **High Priority** tag and manually add it to assets that you want employees to prioritize. Then, employees can search for assets using the **High Priority** tag to filter by the highest priority assets they manage.

To manually tag assets by priority:

1. Create a tag for your highest priority assets using the following settings:

Option	Value
Category	*Priority*
Value	*High Priority*
Value Description	A custom description about the urgency of remediating the vulnerabilities on assets with this tag.

2. Apply the tag manually to your highest priority assets.
3. Instruct employees to use the new tag to filter assets in the assets table or to search for assets from the tags table.

Example: Update ACR Values on Tagged Assets

Your company uses Tenable Lumin to assess your Cyber Exposure. You have groups of assets with common exposure, but the Tenable-assigned ACR values vary within the group of assets.

To customize asset ACR values, you can use attribute settings within any tag to automatically update the ACR value for any asset with that tag.

To update the ACR value for all assets with a tag:

1. Create a tag and apply it manually or automatically.
2. Configure an attribute override for assets with the tag.
    a. Click the **Attribute Override** toggle to enable automatic application of attributes to assets with this tag.

    The criteria boxes appear.

b. In the first box, select an attribute (for example, **Asset Criticality Rating (ACR)**).

c. In the second box, select a value (for example, **9 (Critical)**).

3. Click **Save**.

   Tenable Vulnerability Management updates the attribute for all assets with the tag.

   > **Note:** When you override an asset attribute via tags, Tenable Vulnerability Management may take some time to update the attribute on assets with the tag, depending on the system load and the number of assets.

   > **Tip:** For information about how Tenable Vulnerability Management prioritizes tag-updated ACR values, see Asset Criticality Rating (ACR).

4. Instruct employees to view the updated ACR values in the assets table.

Tag Format and Application

An asset tag is primarily composed of a *Category*:*Value* pair. For example, if you want to group your assets by location, create a *Location* category with the value *Headquarters*.

> **Note:** If you want to create tags without individual categories, Tenable recommends that you add the generic category *Category*, which you can use for all your tags.

Tag membership is reevaluated:

- When you update or create a tag
- When Tenable Web App Scanning imports data
- Every 12 hours

Manual Tags vs. Automatic Tags

When you create a tag, Tenable Web App Scanning automatically applies it to the assets on your instance that match the tags rules. These automatically applied tags are sometimes called *dynamic tags*. When you create an automatic tag, Tenable Web App Scanning applies that tag to all your current assets and any new assets added to your organization's account. Tenable Web App Scanning also regularly reviews your assets for changes to their attributes and adds or removes automatic tags accordingly.

> **Note:** When you create or edit an automatic tag, Tenable Web App Scanning may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

You can also create a tag without rules and then manually apply the tag to individual assets. Alternatively, you can manually apply an automatic tag to additional assets that may not meet the rules criteria for that tag. These manually applied tags are sometimes called *static tags*.

Manual tags appear with the icon, whereas automatic tags appear with the icon.

See the following examples for clarification:

Scenarios	Tag Type	Tag Icon
You create a tag with *Location*:*Headquarters* as the	Manual	

Category:*Value* pair, but you do not add any tag rules. Later, you add the tag to assets located at your headquarters.		
You create a tag with *Location*:*Headquarters* as the *Category*:*Value* pair, and you specify an IP address range in the tag rules. Tenable Web App Scanning then automatically applies the tag to all existing or new assets within that IP address range.	Automatic	

Create a Manual or Automatic Tag

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

Note: When you create a tag from the **Tagging** page, you can select from a list of generic asset filters to create tag rules. If you want to create a tag based on filters that are specific to certain asset types, Tenable recommends that you create a tag from the **Assets** page, where you can select additional filters that are specific to each asset type.

If your tags fail to apply, the tag rules may return too many assets for Tenable Web App Scanning to process. For example, a long list of Fully Qualified Domain Names (FQDNs) with wildcards would cover a large number of assets. When this happens, Tenable recommends reducing the number of assets through stricter tag rules. If needed, you can then use an additional tag to join each list.

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

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

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

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

   The left navigation plane appears.

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

   The **Settings** page appears.

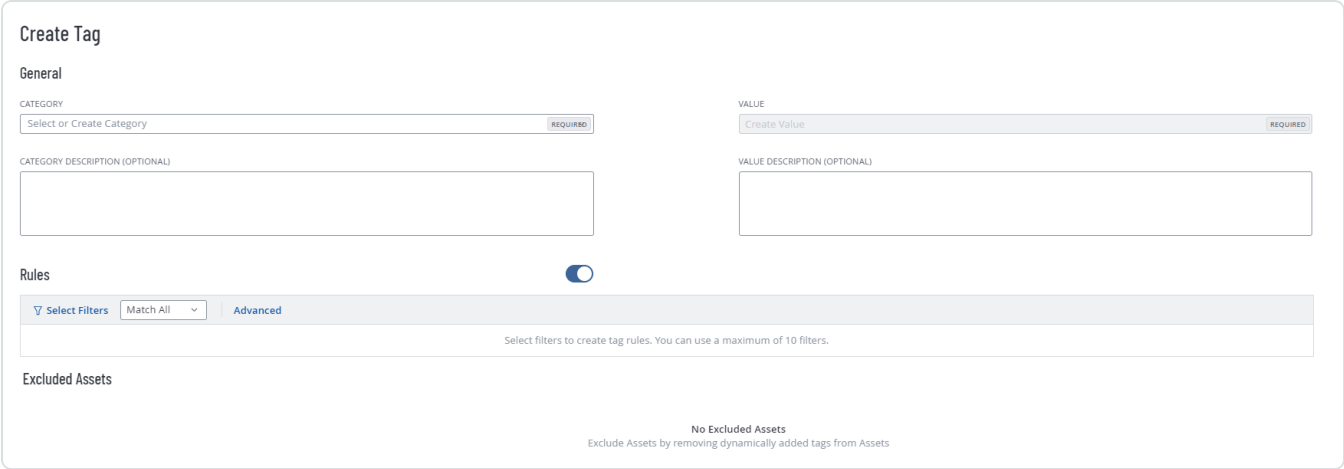
3. Click the **Tagging** tile.

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

   The **Categories** tab is active.

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

   The **Create Tag** page appears.



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

   As you type, the list filters for matches.
7. From the drop-down box, select an existing category, or if the category is new, click **Create "***category name***"**.

   > **Note:** You can create a maximum of 100 categories for your Tenable Web App Scanning instance.
8. (Optional) In the **Category Description** box, type a description of the tag category.
9. In the **Value** box, type a name for the tag.

   > **Note:** Tag names cannot include commas or be more than 50 characters in length.

   > **Tip**: Tenable recommends that you provide a tag name that directly corresponds with the tag category. For example, if the category is *Location*, *Headquarters* would be an appropriate value.
10. (Optional) In the **Value Description** box, type a description for the new tag.
11. Do one of the following:

    ### To save the tag as a manual tag:

    a. Click **Save**.

       Tenable Web App Scanning saves the tag to the tags table.

    b. (Optional) Manually add the tag to one or more assets.

To save and apply the tag automatically:

a. Create a tag rule.

b. Click **Save**.

   Tenable Web App Scanning creates the tag, evaluates existing assets, and automatically applies the tag to assets that match the tag rules.

   > **Note:** When you create an automatic tag, Tenable Web App Scanning may take a few minutes to apply the tag and update any Excluded Assets, depending on the system load and the number of assets.

Considerations for Tags with Rules

Automatic Application

Tenable Web App Scanning evaluates assets against tag rules in the following situations:

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

  > **Note:** When you create or edit a tag rule, Tenable Web App Scanning may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

- When you update an existing asset, Tenable Web App Scanning re-evaluates the asset and removes the tag if the asset's attributes no longer match the tag rules.

Manual Application

If you manually apply a tag that has been configured with rules, Tenable Web App Scanning excludes that asset from any further evaluation against the rules.

Tag Rules

Tag rules allow Tenable Web App Scanning to automatically apply tags you create to the assets on your instance that match the tags rules. These automatically applied tags are called *dynamic* or *automatic* tags.

Tag rules are composed of one or more filter-value pairs based on asset attributes. When you create a rule and add it to a tag, Tenable Web App Scanning applies the tag to all assets on your instance that match the tag rule.

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

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

In the **Tags** section, you can complete the following tasks with tag rules:

- Create a Tag Rule
- Edit a Tag Rule
- Delete A Tag Rule

Create a Tag Rule

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

Required Tenable Vulnerability Management Permission: Can Edit, Can Use permission for applicable asset tags.

When you create or edit a tag to apply automatically, you must create and apply rules to the tag via tag rules filters. You can create a tag rule in either **Basic** or **Advanced** mode.

Caution: If you create a tag rule in **Basic** mode and then switch to **Advanced** mode, the rules you created appear in the **Advanced** mode format. However, if you switch from **Advanced** mode to **Basic** mode, Tenable Web App Scanning removes all rules from the rules section.

Note: When you create a tag from the **Tagging** page, you can select from a list of generic asset filters to create tag rules. If you want to create a tag based on filters that are specific to certain asset types, Tenable recommends that you create a tag from the **Assets** page, where you can select additional filters that are specific to each asset type.

For more information about applying tags automatically, see Considerations for Tags with Rules.

Before you begin:

- Create or edit a tag.

To create and add a rule to a tag:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Tagging** tile.

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

   The **Categories** tab is active.

4. Click the **Values** tab.

The **Values** page appears, containing a table of all the tags on your Tenable Web App Scanning instance.

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

   The **Rules** section appears.

6. For each tag rule you want to create, do one of the following:

   > **Note**: **Basic** mode is active by default.

   ### To create a tag rule in **Basic** mode:

   a. In the **Rules** section, click ▽ **Select Filters**.

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

      > **Note**: Each tag rule filter has different limits on the number of values you can apply to a single filter. For information about those limits, see Tag Rules Filters.

   b. Select a filter.

      The filter you select appears in the **Rules** section.

   c. Click outside the drop-down box.

      The drop-down box closes.

   d. In the filter, click the ⌄ button.

      The filter expands.

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

   f. In the second drop-down box, select or type one or more values for the filter.

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

   h. (Optional) To create another rule:

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

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

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

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

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

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

  Tenable Web App Scanning applies the tag to only assets that meet all of the rules specified in the tag.

To create a tag rule in **Advanced** mode:

a. In the **Rules** section, click **Advanced**.

   A text box appears.

b. Place your cursor in the text box.

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

   > **Note**: Each tag rule filter has different limits on the number of values you can apply to a single filter. For information about those limits, see Tag Rules Filters.

   > **Note:** If there is a typo in the tag rule, an error will appear in the **Rules** box with a description of the issue.

c. Select or type the filter you want to apply.

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

   The filter appears in the text box.

   An operator drop-down box appears to the right of the filter.

d. Select one of the following operators, which are contextual based on the selected filter:

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

Operator	Description
exists	Filters for items for which the selected filter exists.
does not exist	Filters for items for which the selected filter does not exist.
is equal to	Filters for items that match the filter value.
is not equal to	Filters for items that do not include the filter value.
is greater than **is greater than or equal to**	Filters for items with a value greater than the specified filter value. If you want to include the value you specify in the filter, then use the **is greater than or equal to** operator.
is less than **is less than or equal to**	Filters for items with a value less than the specified filter value. If you want to include the value you specify in the filter, then use the **is less than or equal to** operator.
within last	Filters for items with a date within a number of hours, days, months, or years before today. Type a number, then select a unit of time.
after	Filters for items with a date after the specified filter value.
before	Filters for items with a date before the specified filter value.
older than	Filters for items with a date more than a number of hours, days, months, or years before today. Type a number, then select a unit of time.
is on	Filters for items with a specified date.
between	Filters for items with a date between two specified dates.

Operator	Description
contains	Filters for items that contain the specified filter value.
does not contain	Filters for items that do not contain the specified filter value.
wildcard	Filters for items with a wildcard (*****) as follows: • **Begin or end with** – Filters for values that begin or end with text you specify. For example, to find all values that begin with "1", type *1**. To find all values that end in "1", type **1*. • **Contains** –Filters for values that contain text you specify. For example, to find all values with a "1" between the first and last characters, type **1**. • **Turn off case sensitivity** – Filters for values without case sensitivity. For example, to search for findings with a **Plugin Name** of "TLS Version 1.2 Protocol Detection" *or* "tls version 1.2 protocol detection", type **tls version 1.2 protocol detection*.

To the right of the operator, select or type a value for the filter.

> **Tip:** Some text filters support the character (*****) as a wildcard to stand in for a section of text in the filter value. For example, if you want the filter to include all values that end in 1, type **1*. If you want the filter to include all values that begin with 1, *type 1**.
>
> You can also use the wildcard operator to filter for values that contains certain text. For example, if you want the filter to include all values with a 1 somewhere between the first and last characters, type **1**.

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

   i. Press the **Space** key.

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

   ii. Select a modifier.

iii. Press the **Space** key.

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

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

7. Click **Save**.

Tenable Web App Scanning creates the rule and applies it to the tag.

Edit a Tag Rule

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

Required Tenable Vulnerability Management Permission: Can Edit, Can Use permission for applicable asset tags.

Once you create an automatic tag, you can edit the rules that apply to the tag from the **Edit Value** page.

Note: When you edit rules from the **Tagging** page, you can select from a list generic asset filters to create tag rules. However, if you want to add filters that are specific to a certain asset type (e.g., web application assets), Tenable recommends that you edit the tag from the **Assets** page, where you can select filters that are specific to each asset type.

Before you begin:

- Create an automatic tag.

To edit a tag rule:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Tagging** tile.

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

   The **Categories** tab is active.

4. Click the **Values** tab.

   The **Values** page appears, containing a table of all the tags on your Tenable Web App Scanning instance.

5. In the tags table, click the tag for which you want to edit a tag rule.

The **Edit Value** page appears.

> **Tip**: You can also navigate to the **Edit Value** page from the **Edit Category** page by clicking the tag you want to review in the **Values** table.

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

   The **Rules** section appears.

7. In the **Rules** section, in the rule filter you want to edit, click the ⌄ button.

   A drop-down box appears with the lists of rule values previously selected for that filter.

   > **Note:** You can apply up to 10 filters to a tag rule.

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

9. (Optional) In the second box, add or remove a rule value.

   > **Note**: If the rule filter has selectable options (e.g., dates ranges), those options appear below the filter. Otherwise, you must type the value.

10. Click outside the rules drop-down box.

    The drop-down box closes.

11. Click **Save**.

    Tenable Web App Scanning save your changes, evaluates existing assets, and automatically applies the tag to assets that match the updated tag rules.

    > **Note:** Tenable Web App Scanning may take some time to apply the tag to assets and update asset attributes, depending on the system load and the number of assets.

Delete A Tag Rule

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

Required Tenable Vulnerability Management Permission: Can Edit, Can Use permission for applicable asset tags.

When you delete a rule from an automatic tag, Tenable Web App Scanning removes the tag from any assets that match the tag rule. When you delete all rules from an automatic tag, the tag becomes a manual tag.

To delete a tag rule:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Tagging** tile.

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

   The **Categories** tab is active.

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

   The **Values** page appears, containing a table with all the tags on your Tenable Web App Scanning instance.

5. In the tags table, click the tag from which you want to delete a tag rule.

   The **Edit Value** page appears.

   Tip: You can also navigate to the **Edit Value** page from the **Edit Category** page by clicking the tag you want to review in the **Values** table.

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

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

7. Click **Save**.

   Tenable Web App Scanning saves and applies your changes.

Tag Rules Filters

Note: If there is a typo in the tag rule, an error appears in the **Rules** box with a description of the issue.

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

On the **Tags** page, you can select from the following filters to create rules for an automatic tag:

Filter	Description
Account ID	The unique identifier assigned to the asset resource in the cloud service that hosts the asset.
ACR	(Requires Tenable Lumin license) The asset's ACR (Asset Criticality Rating).
ACR Severity	(Requires Tenable Lumin license) The ACR category of the ACR calculated for the asset.
AES	(Requires Tenable Lumin license)The Asset Exposure Score (AES) calculated for the asset.
AES Severity	(Requires Tenable Lumin license) The AES category of the AES calculated for the asset.
Agent Name	The name of the Tenable Nessus agent that scanned and identified the asset.
ARN	The Amazon Resource Name (ARN) for the asset.
ASN	The Autonomous System Number (ASN) for the asset.
Assessed vs. Discovered	Specifies whether Tenable Web App Scanning scanned the asset for vulnerabilities or if Tenable Web App Scanning only discovered the asset via a discovery scan. Possible values are: • **Assessed** • **Discovered Only**

Asset ID	The asset's UUID.
AWS Availability Zone	The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see Regions and Availability Zones in the AWS documentation.
AWS EC2 AMI ID	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Instance ID	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.
AWS EC2 Name	The name of the virtual machine instance in Amazon EC2.
AWS EC2 Product Code	The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2.
AWS Instance State	The state of the virtual machine instance in AWS at the time of the scan. For possible values, see API Instance State in the Amazon Elastic Compute Cloud Documentation.
AWS Instance Type	The type of virtual machine instance in Amazon EC2. Amazon EC2 instance types dictate the specifications of the instance (for example, how much RAM it has). For a list of possible values, see Amazon EC2 Instance Types in the AWS documentation.
AWS Owner ID	A UUID for the Amazon AWS account that created the virtual machine instance. For more information, see AWS Account Identifiers in the AWS documentation. This attribute contains a value for Amazon EC2 instances only. For other asset types, this attribute is empty.
AWS Region	The region where AWS hosts the virtual machine instance, for example, `us-east-1`. For more information, see Regions and Availability Zones in the AWS documentation.
AWS Security Group	The AWS security group (SG) associated with the Amazon EC2 instance.

AWS Subnet ID	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.
AWS VPC ID	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.
Azure Resource Group	The name of the resource group in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure Resource ID	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure Resource Type	The resource type of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure Subscription ID	The unique subscription identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
Azure VM ID	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see Accessing and Using Azure VM Unique ID in the Microsoft Azure documentation.
BIOS ID	The NetBIOS name for the asset.
Cloud Provider	The name of the cloud provider that hosts the asset.
Created Date	The time and date when Tenable Web App Scanning created the asset record.
Custom Attribute	A filter that searches for custom attributes via a category-value pair. For more information about custom attributes, see the Tenable Developer Portal.
Deleted	Specifies whether the asset has been deleted.
Deleted Date	The date when a user deleted the asset record or the number of days since a user deleted the asset. When a user deletes an asset record,

	Tenable Web App Scanning retains the record until the asset ages out of the license count.
DNS (FQDN)	The fully-qualified domain name of the asset host. **Note:** This does not apply to Web Application assets, for which you must use the **Name** filter.
Domain	The domain which has been added as a source or discovered by ASM as belonging to a user.
First Seen	The date and time when a scan first identified the asset.
Google Cloud Instance ID	The unique identifier of the virtual machine instance in Google Cloud Platform (GCP).
Google Cloud Project ID	The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see Creating and Managing Projects in the GCP documentation.
Google Cloud Zone	The zone where the virtual machine instance runs in GCP. For more information, see Regions and Zones in the GCP documentation.
Has Plugin Results	Specifies whether the asset has plugin results associated with it.
Host Name (Domain Inventory)	The host name for assets found during attack surface management scans; only for use with Domain Inventory assets.
Hosting Provider	The hosting provider for the asset.
IaC Resource Type	The Infrastructure as Code (IAC) resource type of the asset.
Installed Software	A list of Common Platform Enumeration (CPE) values that represent software applications a scan identified as present on an asset. This field supports the CPE 2.2 format. For more information, see the Component Syntax section of the CPE Specification documentation, Version 2.2. For assets identified in Tenable scans, this field contains data only if a scan using Tenable Nessus Plugin ID 45590 has evaluated the asset.

	Note: If no scan detects an application within 30 days of the scan that originally detected the application, Tenable Web App Scanning considers the detection of that application expired. As a result, the next time a scan evaluates the asset, Tenable Web App Scanning removes the expired application from the **Installed Software** attribute. This activity is logged as a remove type of attribute change in the asset activity log.
IPv4 Address	The IPv4 address associated with the asset record.. This filter supports multiple asset identifiers as a comma-separated list (for example, hostname_example, example.com, 192.168.0.0). For IP addresses, you can specify individual addresses, CIDR notation (for example, 192.168.0.0/24), or a range (for example, 192.168.0.1-192.168.0.255). **Note:** A CIDR mask of /0 is not supported for this parameter, because that value would match all IP addresses. If you submit a /0 value for this parameter, Tenable Web App Scanning returns a 400 Bad Request error message. **Note:** Ensure the tag filter value does not end in a period.
IPv6 Address	An IPv6 address that a scan has associated with the asset record. This filter supports multiple asset identifiers as a comma-separated list. The IPV6 address must be an exact match. (for example, 0:0:0:0:0:ffff:c0a8:0). **Note:** Ensure the tag filter value does not end in a period.
Is Attribute	Specifies whether the asset is an attribute.
Is Auto Scale	Specifies whether the asset scales automatically.
Is Unsupported	Specifies whether the asset is unsupported in Tenable Web App Scanning.
Last Audited	The time and date at which the asset was last audited.
Last Authenticated	The date and time of the last authenticated scan run against the asset.

Scan	An authenticated scan that only uses discovery plugins updates the **Last Authenticated Scan** field, but not the **Last Licensed Scan** field.
Last Licensed Scan	The date and time of the last scan in which the asset was considered "licensed" and counted towards Tenable's license limit. A licensed scan uses non-discovery plugins and can identify vulnerabilities. Unauthenticated scans that run non-discovery plugins update the **Last Licensed Scan** field, but not the **Last Authenticated Scan** field. For more information on licensed assets, see Tenable Vulnerability Management Licenses.
Last Seen	The date and time of the scan that most recently identified the asset.
Licensed	Specifies whether the asset is included in the asset count for the Tenable Web App Scanning instance.
MAC Address	A MAC address that a scan has associated with the asset record.
Mitigation Last Detected	The date and time of the scan that last identified mitigation software on the asset.
Name	The asset identifier that Tenable Web App Scanning assigns based on the presence of certain asset attributes in the following order: 1. Agent Name (if agent-scanned) 2. NetBIOS Name 3. FQDN 4. IPv6 address 5. IPv4 address For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.
NetBIOS Name	The NetBIOS name for the asset.
Network	The name of the network object associated with scanners that identified the asset. The default name is **Default**. For more information,

	see Networks.
Open Ports	Open ports on the asset.
Operating System	The operating system that a scan identified as installed on the asset.
Port	The port associated with the asset.
Public	Specifies whether the asset is available on a public network.
Record Type	The asset type.
Region	The cloud region where the asset runs.
Repositories	Any code repositories associated with the asset.
Resource Category	The name of the category to which the cloud resource type belongs (for example, object storage or virtual network).
Resource Tags (By Key)	Tags synced from a cloud source, such as Amazon Web Services (AWS), matched by the tag key (for example, Name).
Resource Tags (By Value)	Tags synced from a cloud source, such as Amazon Web Services (AWS), matched by the tag value.
Resource Type	The asset's cloud resource type (for example, network, virtual machine).
ServiceNow Sys ID	Where applicable, the unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.
Source	The source of the scan that identified the asset. Possible filter values are: • AWS • AWS FA • Azure • AZURE FA • Cloud Connector

	• Cloud IAC • Cloud Runtime • GCP • Nessus Agent • Nessus Scan • NNM • ServiceNow • WAS
SSL/TLS	Specifies whether the application on which the asset is hosted uses SSL/TLS public-key encryption.
System Type	The system types as reported by Plugin ID 54615. For more information, see Tenable Plugins.
Tags	A unique filter that searches tag (category: value) pairs. When you type a tag value, you must use the *category: value* syntax, including the space after the colon (:). You can use commas (,) to separate values. If there is a comma in the tag name, insert a backslash (\) before the comma. You can add a maximum of 100 tags. For more information, see tags. **Note:** If your tag name includes double quotation marks (" "), you must use the UUID instead.
Target Groups	The target group to which the asset belongs. This attribute is empty if the asset does not belong to a target group. For more information, see Target Groups.
Tenable ID	The UUID of the agent present on the asset.
Terminated	Specifies whether or not the asset is terminated.
Type	The system type on which the asset is managed. Possible filter values

	are: • **Cloud Resource** • **Container** • **Host** • **Cloud**
Updated Date	The time and date when a user last updated the asset.
VPC	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.

Create a Tag via Asset Filters

Required User Role: Administrator

When you filter your assets, you can use the filters as tag rules to create a new automatic tag.

After you create the tag, Tenable Web App Scanning automatically applies the tag to any assets identified through those filters.

You can also create a manual or automatic tag for your assets from the **Tagging** page.

To create a tag using asset filters:

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

   The left navigation plane appears.

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

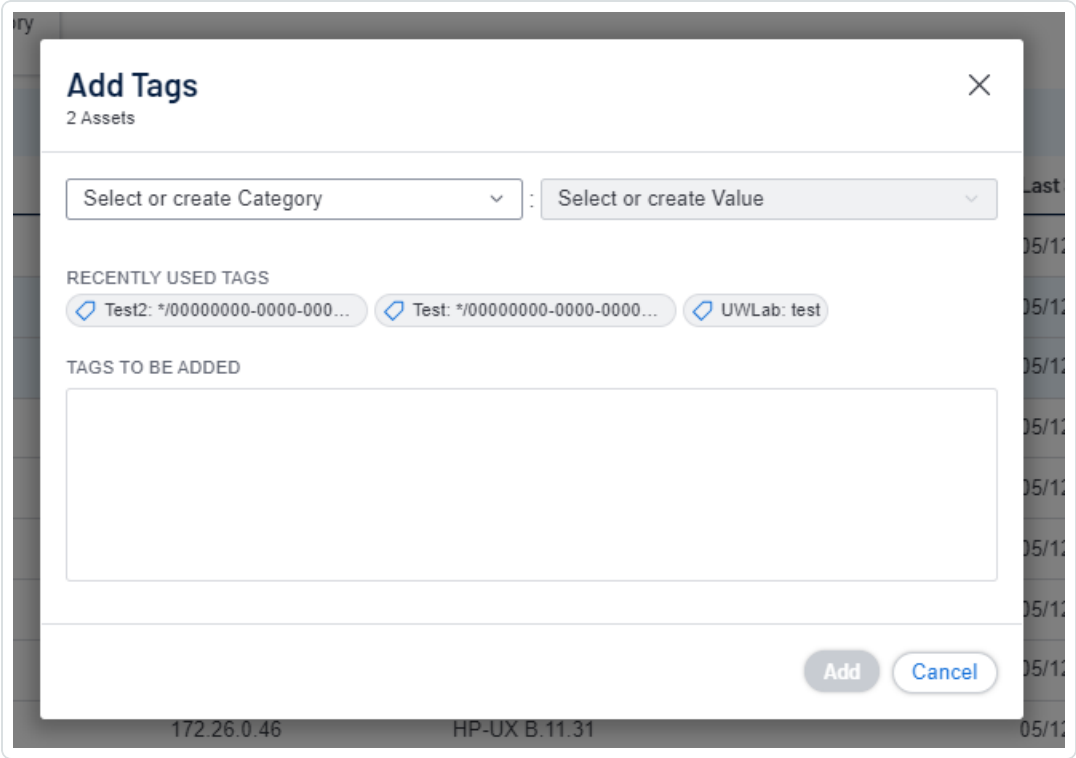
   The **Assets** page appears.

3. Filter the table, selecting and deselecting filters based on the rules you want to add to or remove from your tag.

   The filters you selected appear in the header above the filter plane.

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

   The **Add Tags** window appears.



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

   As you type, the list filters for matches.

6. In the drop-down box, select an existing category, or if the category is new, click **Create "***category* **"**.

   > **Tip**: You can create a generic tag category and apply to different tag values to group your tags. For example, if you create a *Location* category, you can apply it to multiple values such as *Headquarters* or *Offshore* to create a group of location tags.

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

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

9. Click **Save**.

   Tenable Web App Scanning saves the tag and applies it to applicable assets on your account.

   > **Note**: It can take up to several minutes for Tenable Web App Scanning to apply a tag to the applicable assets.

Edit a Tag or Tag Category

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

Required Tenable Vulnerability Management Permission: Can Edit, Can Use permission for applicable asset tags.

In the **Tagging** section, you can edit one or more components of a tag, including the category to which the tag belongs as well as the tag's name and description and any rules applied to the tag.

To edit a tag or tag category:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Tagging** tile.

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

   The **Categories** tab is active.

4. To edit an individual tag:

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

      The **Values** page appears, containing a table with all the tags on your Tenable Web App Scanning instance.

   b. In the **Values** table, click the tag you want to edit.

      The **Edit Value** page appears.

      Tip: You can also navigate to the **Edit Value** page from the **Edit Category** page by clicking the tag you want to review in the **Values** table.

   c. (Optional) In the **Value** box, edit the tag name.

   d. (Optional) In the **Value Description (Optional)** box, edit the tag description.

e. (Optional) Configure the tag rules.

5. To edit the tag category:

> **Note**: When you edit a tag category, Tenable Web App Scanning changes the category for all the tags in that category.

a. In the tag categories table, click the category you want to edit.

   The **Edit Category** page appears.

b. In the tag categories table, click the category you want to edit.

   The **Edit Category** page appears.

c. (Optional) To edit the name, in the **Category** box, type a new name.

d. (Optional) To edit the description, in the **Category Description** box, type a new description.

6. Click **Save**.

   Tenable Web App Scanning saves and applies your changes.

Edit a Tag via Asset Filters

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

Required Tenable Vulnerability Management Permission: Can Edit, Can Use permission for applicable asset tags.

On the **Assets** page, you can use asset filters to edit a tag's rules, category, and value.

To edit a tag using asset filters:

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

   The left navigation plane appears.

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

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

3. Filter the table, selecting and deselecting filters based on the rules you want to add to or remove from your tag.

   The filters you applied appear in the header above the filter plane.

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

   The **Tag Matching Assets** window appears.

5. Do one of the following:

   - To edit a recently used tag:

     a. Under **Recently Used Tags**, click the tag you want to edit.

     The tag category appears in the **Select or create Category** drop-down box.

     The tag value appears in the **Select or create Value** drop-down box.

   - To edit any other tag:

a. In the **Select or create Category** drop-down box, type a category name.

   As you type, the list filters for matches.

b. Select the category for the tag you want to edit.

c. In the **Select or create Value** drop-down box, type a value name.

   As you type, the list filters for matches.

d. In the drop-down box, select the value for the tag you want to edit.

6. (Optional) To edit the tag category:

   a. In the **Select or create Category** drop-down box, type a new name for your category.

      Create "*category***"** appears in the drop-down box.

   b. In the drop-down box, select **Create "***category***"**.

      The new category name appears selected in the drop-down box.

7. (Optional) To edit the tag value:

   a. In the **Select or create Value** drop-down box, type a new value for your tag.

      Create "*value***"** appears in the drop-down box.

   b. In the drop-down box, select **Create "***value***"**.

      The new value name appears selected in the drop-down box.

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

9. Click **Save**.

   Tenable Web App Scanning saves your edits.

Add a Tag to an Asset

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

Required Tenable Vulnerability Management Permission: Can Use permission for applicable asset tags.

After you create a tag, you can manually apply it to one or more assets on your Tenable Web App Scanning instance.

To add a tag to an 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 **Hosts** tab is visible.

3. View your assets list.

4. (Optional) Refine the table data. For more information, see Tenable Web App Scanning Workbench Tables.

5. Do one of the following:

   To add a tag to a single asset:

a. Select the page where you want to add the tag:

Location	Action
Assets page	To add a tag from the **Assets** page: a. In the assets table, right-click the row for the asset to which you want to add a tag. The action options appear next to your cursor. -or- In the assets table, in the **Actions** column, click the ⋮ button for the asset to which you want to add a tag. The action buttons appear in the row. b. Click **Add Tags**.
Asset Details page preview plane	To add a tag from the **Asset Details** page: a. In the assets table, click the row for the asset to which you want to add a tag. The preview plan for the asset's **Asset Details** page appears. b. In the left section of the preview plane, next to **Tags**, click the ⊕ button.
Asset Details page	To add a tag from the **Asset Details** page: a. View the **Asset Details** page for the asset from which you want to remove the tag. The **Asset Details** page appears. b. In the upper-right corner, click the **Actions** button.

	The actions menu appears. c. In the actions menu, click **Add Tag**. -or- On the left side of the page, next to **Tags**, click the ⊕ button.

The **Add Tags** window appears.

b. Click **Add**.

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

To add a tag to multiple assets:

a. In the assets table, select the check box for each asset to which you want to add a tag.

The action bar appears at the top of the table.

b. Click **Add Tags**.

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

6. Do one of the following:

To add a recently used tag:

- Under **Recently Used Tags**, select the tag you want to add.

The tag appears in the **Tags to be Added** box.

> **Tip:** To remove a tag from **Tags to be Added**, roll over the tag and click the ✕ button.

To add a new or existing tag:

a. In the **Category** box, type a category.

As you type, the list filters for matches.

b. From the drop-down box, select an existing category, or if the category is new, click **Create "***category name***"**.

> **Tip**: You can create a generic tag category and apply to different tag values to group your tags. For example, if you create a *Location* category, you can apply it to multiple values such as *Headquarters* or *Offshore* to create a group of location tags.

c. In the **Value** box, type a value.

   As you type, the list filters for matches.

d. From the drop-down box, select an existing value, or if the value is new, click **Create "***value***"**.

> **Note:** The system does not save new tags you create by this method until you add the new tags to the asset.

The tag appears in the **Tags to be Added** box.

> **Tip:** To remove a tag from **Tags to be Added**, roll over the tag and click the ✕ button.

7. Click **Add**.

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

Override Asset Attributes via Tag

Required Additional License: Tenable Lumin

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

When editing a tag to apply manually or automatically, you can specify asset attributes you want Tenable Vulnerability Management to override for all assets with the tag.

For example, you can select the ACR attribute to bulk update a specific ACR value to all assets with the tag.

Tip: For information about ACR prioritization, see Override Asset Attributes via Tag.

To override asset attributes via tag in the new interface:

1. Begin creating a tag.
2. To automatically override an asset attribute for all assets with this tag, edit the attributes:
   a. Click the **Attribute Override** toggle to enable automatic application of attributes to assets with this tag.

      The criteria boxes appear.

   b. In the first box, select an attribute (for example, **Asset Criticality Rating (ACR)**).

   c. In the second box, select a value (for example, **9 (Critical)**).
3. Click **Save**.

   Tenable Vulnerability Management updates the attribute for all assets with the tag.

   Note: When you override an asset attribute via tags, Tenable Vulnerability Management may take some time to update the attribute on assets with the tag, depending on the system load and the number of assets.

   Tip: For information about how Tenable Vulnerability Management prioritizes tag-updated ACR values, see Asset Criticality Rating (ACR).

Export Tags

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

On the **Tags** page, you can export tag categories and values in CSV or JSON format.

To export tag categories or values:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Tagging** tile.

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

   The **Categories** tab is active.

4. (Optional) Refine the table data. For more information, see Tenable Web App Scanning Workbench Tables.

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

5. Do one of the following:

   To export tag categories:

a. Select the tag categories that you want to export:

Export Scope	Action
Selected tag categories	To export selected tag categories: a. In the categories table, select the check box for each tag category you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 tag categories, select all the tag categories in the list and then click [→ **Export**.
A single tag category	To export a single tag category: a. In the categories table, right-click the row for the tag category you want you want to export. The action options appear next to your cursor. -or- In the categories table, in the **Actions** column, click the ⋮ button in the row for the tag category you want to export. The action buttons appear in the row. b. Click **Export**.

To export tag values:

a. Click the **Values** tab.

The **Values** tab appears. This tab consists of a table that contains all your tag values.

b. Select the tag values that you want to export:

Export Scope	Action
Selected tag values	To export selected tag values: a. In the values table, select the check box for each tag value you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you want to export more than 200 tag values, select all the tag values in the list and then click [→ **Export**.
A single tag value	To export a single tag value: a. In the categories table, right-click the row for the tag value you want you want to export. The action options appear next to your cursor. -or- In the values table, in the **Actions** column, click the ⋮ button in the row for the tag value you want to export. The action buttons appear in the row. b. Click **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

> **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

6. In the **Name** box, type a name for the export file.
7. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of tag categories or values. **Note:** If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Web App Scanning automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of tag categories or values. Empty fields are not included in the JSON file.

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

   Note: Tenable Vulnerability Management allows you to set a maximum of 30 calendar days for export expiration.

10. (Optional) To set a schedule for your export to repeat:
    - Click the **Schedule** toggle.

      The **Schedule** section appears.
    - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
    - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
    - In the **Repeat** drop-down box, select how often you want the export to repeat.

- In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

  > **Note**: If you select never, the schedule repeats until you modify or delete the export schedule.

11. (Optional) To send email notifications on completion of the export:

    > **Note**: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

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

    - (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

      > **Note**: Tenable Web App Scanning sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

12. Click **Export**.

    Tenable Web App Scanning begins processing the export. Depending on the size of the exported data, Tenable Web App Scanning may take several minutes to process the export.

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

13. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file in the **Export Management View**.

Delete a Tag Category

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

Required Tenable Vulnerability Management Permission: Can Edit, Can Use permission for applicable asset tags.

When you delete a tag category, Tenable Web App Scanning deletes any tags created under that category and removes those tags from all assets where they were applied.

Caution: When you delete a tag category, all associated values and assignments are also deleted. If you want to remove a specific tag, see Delete a Tag .

To delete a tag category:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Tagging** tile.

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

   The **Categories** tab is active.

4. Click the **Categories** tab.

   The tag categories table appears.

5. To delete one tag category:

   a. In the tags table, in the **Action** column , click the ⋮ button.

      A menu appears.

b. Click the **Delete** button.

A confirmation window appears, asking if you are sure that you want to delete the category and all associated tags and assignments.

To delete multiple tag categories:

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

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

b. In the action bar, click the **Delete** button.

A confirmation window appears, asking if you are sure that you want to delete the category and all associated tags and assignments..

6. Click **Delete**.

Tenable Web App Scanning deletes the tag category and any associated tags, and removes those tags from all assets where you applied them.

Delete a Tag

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

Required Tenable Vulnerability Management Permission: Can Edit, Can Use permission for applicable asset tags.

When you delete a tag, Tenable Web App Scanning removes that specific tag from all assets where you applied the tag.

To delete one or more tags:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Tagging** tile.

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

   The **Categories** tab is active.

4. Delete a one or more tags:

Scope of Deletion	Action
A single tag	To delete a single tag: a. Click the **Values** tab. The **Values** tab appears, displaying a table with all the tags on your Tenable Web App Scanning instance in *Category:Value* format. b. In the tags table, right-click the row for the tag you want to delete. The action options appear next to your cursor.

	-or- In the tags table, in the **Actions** column, click the ⋮ button for the tag you want to delete. The action buttons appear in the row. c. Click **Delete**.
Multiple tags	To delete multiple tags: a. Click the **Values** tab. The **Values** tab appears, displaying a table with all the tags on your Tenable Web App Scanning instance in *Category:Value* format. b. In the tags table, select the check box for each tag you want to delete. The action bar appears at the top of the table. c. In the action bar, click **Delete**. -or- Delete all tags in a category by deleting the tag category.

5. Click the **Values** tab.

6. To delete one tag:

   a. In the tags table, roll over the tag you want to delete.

      The action buttons appear in the row.

   b. Click the **Delete** button.

      A confirmation window appears.

   To delete multiple tags:

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

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

b. In the action bar, click the **Delete** button.

   A confirmation window appears.

7. Click **Confirm**.

   Tenable Web App Scanning deletes the tag and removes it from all assets where you applied the tag.

Search for Assets by Tag from the Tags Table

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

You can see which assets have a specific tag applied by searching for assets by tag.

To search for assets by tag from the tags table:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Tagging** tile.

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

   The **Categories** tab is active.

4. Click the **Values** tab.

5. In the table, click the ⋮ button.

   The actions menu appears.

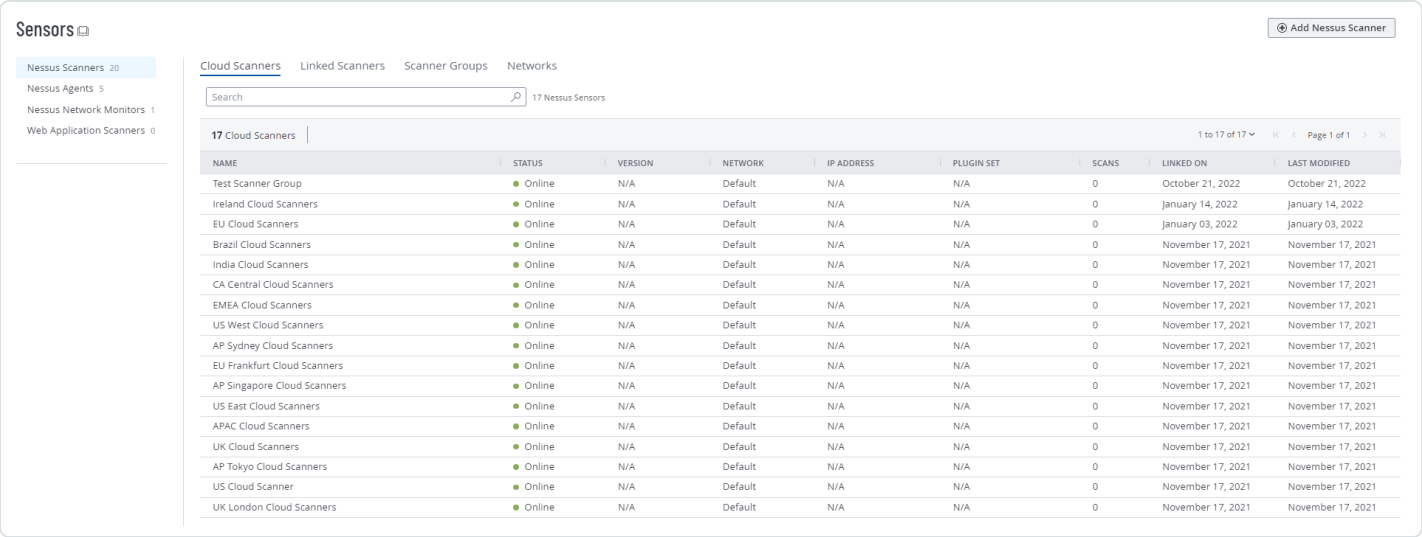
6. Click 🔍 **Search by Tag**.

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

Cloud Sensors

By default, Tenable provides regional cloud sensors for use in Tenable Web App Scanning. You can select these sensors when you create and launch scans.

The following table identifies each regional cloud sensor and, for allow list purposes, its IP address ranges. These IP address ranges are exclusive to Tenable.



Note: If you use cloud connectors, Tenable recommends allowlisting the IP addresses for the region in which the site resides.

Note: While these IP addresses are for outbound requests, they are also used for inbound cloud.tenable.com requests.

Tip: The cloud sensor and IP address information contained in the table below is also provided in JSON format for users that want to parse the data programmatically.

For Cloud IPs associated with Tenable Attack Surface Management, see Cloud Sensors in the *Tenable Attack Surface Management User Guide*.

Sensor Region	IPv4 Range	IPv6 Range
ap-northeast-1	13.115.104.128/25 35.73.219.128/25	2406:da14:e76:5b00::/56
ap-southeast-1	13.213.79.0/24	2406:da18:844:7100::/56

Sensor Region	IPv4 Range	IPv6 Range
	18.139.204.0/25 54.255.254.0/26	
ap-southeast-2	13.210.1.64/26 3.106.118.128/25 3.26.100.0/24	2406:da1c:20f:2f00::/56
ap-south-1	3.108.37.0/24	2406:da1a:5b2:8500::/56
ca-central-1	3.98.92.0/25 35.182.14.64/26	2600:1f11:622:3000::/56
eu-west-1	3.251.224.0/24	2a05:d018:f53:4100::/56
eu-west-2	18.168.180.128/25 18.168.224.128/25 3.9.159.128/25 35.177.219.0/26	2a05:d01c:da5:e800::/56
eu-central-1	18.194.95.64/26 3.124.123.128/25 3.67.7.128/25 54.93.254.128/26	2a05:d014:532:b00::/56
me-central-1	51.112.93.0/24	2406:da17:524:dd00::/56
us-east-1	34.201.223.128/25 44.192.244.0/24 54.175.125.192/26	2600:1f18:614c:8000::/56
us-east-2	13.59.252.0/25 18.116.198.0/24 3.132.217.0/25	2600:1f16:8ca:e900::/56
us-west-1	13.56.21.128/25 3.101.175.0/25 54.219.188.128/26	2600:1f1c:13e:9e00::/56
us-west-2	34.223.64.0/25	2600:1f14:141:7b00::/56

Sensor Region	IPv4 Range	IPv6 Range
	35.82.51.128/25 35.86.126.0/24 44.242.181.128/25 35.93.174.0/24	
sa-east-1	15.228.125.0/24	2600:1f1e:9a:ba00::/56
static	162.159.129.83/32 162.159.130.83/32	2606:4700:7::a29f:8153 2606:4700:7::a29f:8253

Note: For troubleshooting Tenable Web App Scanning issues with Tenable Support, you may be asked to add the following IP range to your allow list:

- 13.59.250.76/32

Regional cloud sensors appear in the following groups:

- **US East Cloud Scanners**: A group of scanners from the us-east-1 (Virginia) or the us-east-2 (Ohio) ranges.
- **US West Cloud Scanners**: A group of scanners from the us-west-1 (California) or the us-west-2 (Oregon) ranges.
- **AP Singapore Cloud Scanners**: A group of scanners from the ap-southeast-1 (Singapore) range.
- **AP Sydney Cloud Scanners**: A group of scanners from the ap-southeast-2 (Sydney) range.
- **AP Tokyo Cloud Scanners**: A group of scanners from the ap-northeast-1 (Tokyo) range.
- **CA Central Cloud Scanners**: A group of scanners from the ca-central-1 (Canada) range.
- **EU Frankfurt Cloud Scanners**: A group of scanners from the eu-central-1 (Frankfurt) range.
- **UK Cloud Scanners**: A group of scanners from the eu-west-2 (London) range.
- **Brazil Cloud Scanners:** A group of scanners from the sa-east-1 (São Paulo) range.
- **India Cloud Scanners:** A group of scanners from the ap-south-1 (Mumbai) range.

- **Amazon GOV-CLOUD**: A group of scanners available for Federal Risk and Authorization Management Program (FedRAMP) environments.
- **US Cloud Scanner**: A group of scanners from the following AWS ranges:
  - us-east-1 (Virginia)
  - us-east-2 (Ohio)
  - us-west-1 (California)
  - us-west-2 (Oregon)
- **APAC Cloud Scanners**: A group of scanners from the following AWS ranges:
  - ap-northeast-1 (Tokyo)
  - ap-southeast-1 (Singapore)
  - ap-southeast-2 (Sydney)
  - ap-south-1 (Mumbai)
- **EMEA Cloud Scanners**: A group of scanners from the following AWS ranges:
  - eu-west-1 (Ireland)
  - eu-west-2 (London)
  - eu-central-1 (Frankfurt)

Note: If you are connecting to Tenable Vulnerability Management through Tenable Nessus scanners, Tenable Nessus Agents, Tenable Web App Scanning scanners, or Tenable Nessus Network Monitors (NNM) located in mainland China, you must connect through sensor.cloud.tenablecloud.cn instead of sensor.cloud.tenable.com.

Tenable FedRAMP Moderate Cloud Sensors

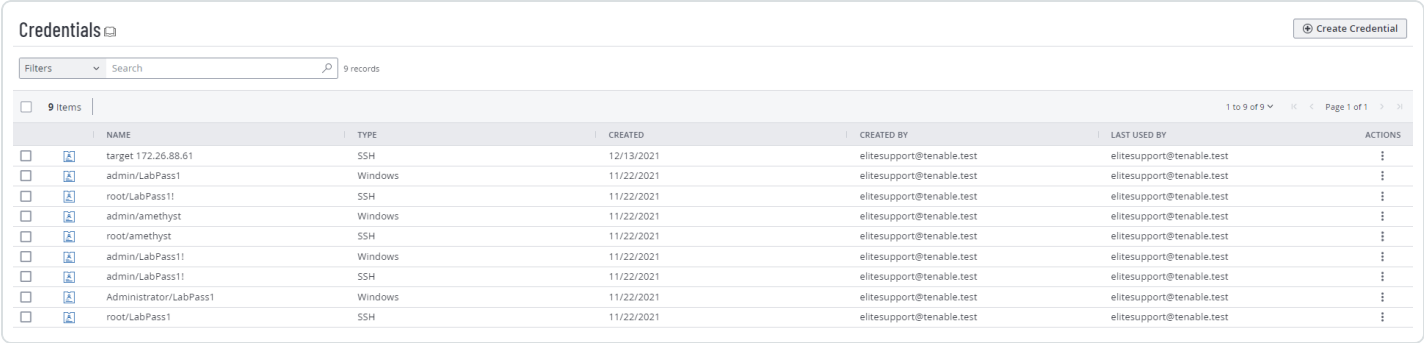
- For cloud based network scans, add the following IP ranges to your allow list:
  - 3.32.43.0 - 3.32.43.31 (3.32.43.0/27)
  - 3.31.100.0/24
- For internal scanner or agent communications, add the following IP ranges to your allow list:
  - 52.61.37.84
  - 15.200.117.191
  - 162.159.140.154
  - 172.66.0.152
  - 2606:4700:7::98
  - 2a06:98c1:58::98
  - 162.159.140.155
  - 172.66.0.153
  - 2606:4700:7::99
  - 2a06:98c1:58::99

Credentials

Note: This section describes creating and maintaining managed credentials. For more information about scan-specific or policy-specific credentials, see Credentials in Tenable Vulnerability Management Scans or Credentials in Tenable Web App Scanning Scans.

Managed credentials allow you to store credential settings centrally in a credential manager. You can then add those credential settings to multiple scan configurations instead of configuring credential settings for each individual scan.

You and users to whom you grant permissions can use managed credentials in scans. Credential user permissions control which users can use and edit managed credentials.



Create a Managed Credential

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

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

This topic describes creating a managed credential in the Tenable Web App Scanning credential manager.

You can also create a managed credential during scan configuration, as well as convert a scan-specific credential to a managed credential. For more information, see Add a Credential to a Scan (Tenable Vulnerability Management) or Configure Credentials Settings in Tenable Web App Scanning.

To create a managed credential:

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

   The left navigation plane appears.

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

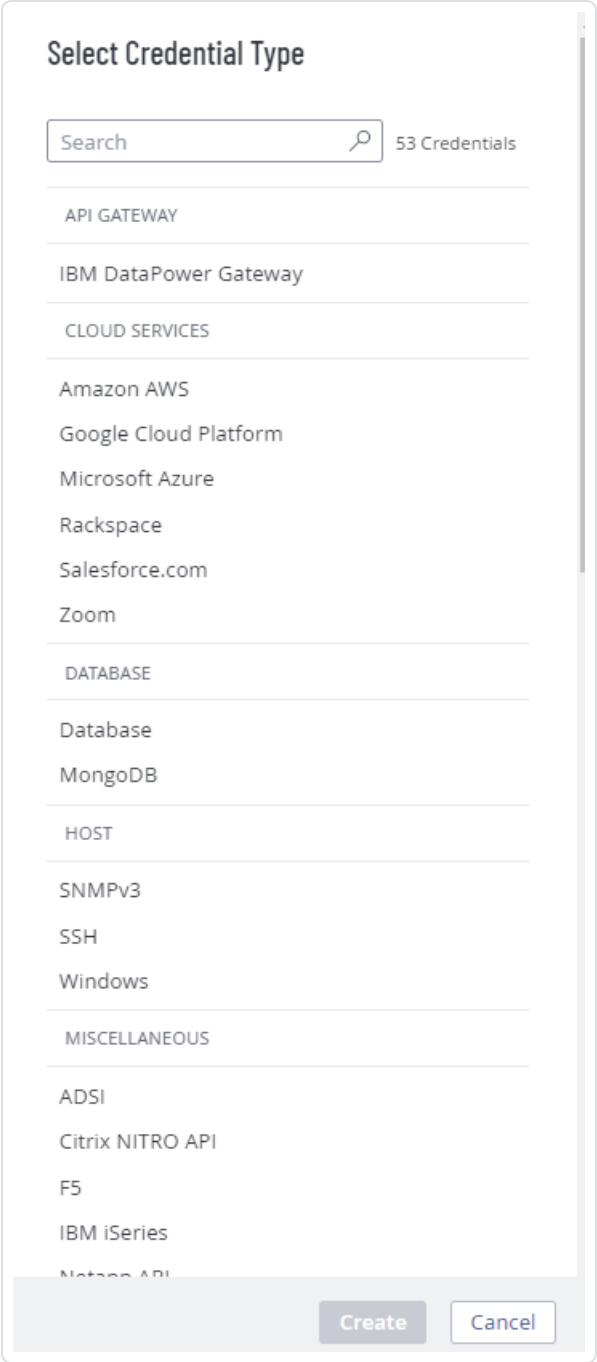
   The **Settings** page appears.

3. Click the **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

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

   The **Select Credential Type** plane appears.



5. Do one of the following:

    - Select one of the available credential types.
    - Click on a credential type in the category sections.

    The credential settings appear.

6. In the **Title** box, type a name for the credential.

7. (Optional) In the **Description** box, type a description for the credential.
8. Configure the settings for the credential type you selected.

   For more information about credential settings, see Credentials (Tenable Vulnerability Management) or Credentials (Tenable Web App Scanning).
9. Add user permissions.
10. Click **Save**.

    Tenable Web App Scanning adds the credential to the credentials table in the **Credentials** page.

Edit a Managed Credential

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, Scan Operator, Standard, Scan Manager, or Administrator

This topic describes editing a credential in the Tenable Vulnerability Management credential manager.

You can also edit managed credentials during scan configuration. For more information, see Add a Credential to a Scan for Tenable Vulnerability Management or Configure Credentials Settings in a Tenable Web App Scanning Scan for Tenable Web App Scanning.

You can edit any credentials where you have **Can Edit** permission.

To edit managed credentials:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

4. Filter or search the credentials table for the credential you want to edit. For more information, see Tenable Web App Scanning Tables.

5. In the credentials table, click the name of the credential you want to edit.

   The credential settings plane appears.

6. Do one of the following:

   - Edit the credential name or description.

     a. Roll over the name or description box.

     b. Click the button that appears next to the box.

     c. Make your changes.

     d. Click the button at the lower right corner of the box to save your changes.

   - Edit the settings for the credential type. For more information about these settings, see Credentials (Tenable Vulnerability Management) or Credentials (Tenable Web App Scanning).

   - Configure user permissions for the credential.

7. Click **Save**.

Configure User Permissions for a Managed Credential

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

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

You configure user permissions for a managed credential separately from the permissions you configure for the scans where you use the credential.

You can configure credential permissions for individual users or a user group. If you configure credential permissions for a group, you assign all users in that group the same permissions. You may want to create the equivalent of a credential manager role by creating a group for the users you want to manage credentials. For more information, see User Groups.

If you create a managed credential, Tenable Web App Scanning automatically assigns you **Can Edit** permissions.

To configure user permissions for a managed credential:

1. Create or edit a managed credential:

Location	Action
In the credential manager	create or edit
In a scan configuration	create or edit

2. Do one of the following:

   - Add permissions for a user or user group.

     Tip: Tenable recommends assigning permissions to user groups, rather than individual users, to minimize maintenance as individual users leave or join your organization.

     a. In the credential settings plane, click the ⊕ button next to the **User Permissions** title.

     The **Add User Permission** settings appear.

b. In the search box, type the name of a user or group.

   As you type, a filtered list of users and groups appears.

c. Select a user or group from the search results.

d. Click the ⌄ button next to the permission drop-down for the user or group.

e. Select a permission level:

   - **Can Use** — The user can view the credential in the managed credentials table and use the credential in scans.
   - **Can Edit** — The user can view and edit credential settings, delete the credential, and use the credential in scans.

f. Click **Add**.

g. Click **Save**.

- Edit permissions for a user or user group.

  a. In the **User Permissions** section of the credential settings plane, click the ⌄ button next to the permission drop-down for the user or group.

  b. Select a permission level:

     - **Can Use** — The user can view the credential in the managed credentials table and use the credential in scans.
     - **Can Edit** — The user can view and edit credential settings, delete the credential, and use the credential in scans.

  c. Click **Save**.

- Delete permissions for a user or user group.

  a. In the **User Permissions** section of the credential settings plane, roll over the user or group you want to delete.

  b. Click the ✕ button next to the user or user group.

     The user or group is removed from the **User Permissions** list.

c. Click **Save**.

Export Credentials

Required User Role: Administrator

On the **Credentials** page, you can export the data for one or more managed credentials.

Note: When you export credential data, authentication details such as usernames, passwords, or keys are not included in the export.

To export credential data:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

4. (Optional) Refine the table data. For more information, see Tenable Web App Scanning Workbench Tables.

5. Select the credentials that you want to export:

Export Scope	Action
Selected credentials	To export selected credentials: a. In the credentials table, select the check box for each credential you want to export. The action bar appears at the top of the table. b. In the action bar, click [→ **Export**. **Note:** The [→ **Export** link is available for up to 200 selections. If you

	want to export more than 200 credentials, select all the credentials in the list and then click [→ **Export**.
A single credential	To export a single credential: a. In the credentials table, right-click the row for the credential you want to export. The action options appear next to your cursor. -or- In the credentials table, in the **Actions** column, click the ⋮ button in the row for the credential you want to export. The action buttons appear in the row. b. Click [→ **Export**.

The **Export** plane appears. This plane contains:

- A text box to configure the export file name.
- A list of available export formats.
- A table of configuration options for fields to include in the exported file.

  > **Note**: By default, all fields are selected.

- A text box to set the number of days before the export expires.
- A toggle to configure the export schedule.
- A toggle to configure the email notification.

6. In the **Name** box, type a name for the export file.
7. Click the export format you want to use:

Format	Description
CSV	A CSV text file that contains a list of credentials.

	Note: If your .csv export file includes a cell that begins with any of the following characters (=, +, -, @), Tenable Web App Scanning automatically inputs a single quote (') at the beginning of the cell. For more information, see the related knowledge base article.
JSON	A JSON file that contains a nested list of credentials. Empty fields are not included in the JSON file.

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

   Note: Tenable Web App Scanning allows you to set a maximum of 30 calendar days for export expiration.

10. (Optional) To set a schedule for your export to repeat:

    - Click the **Schedule** toggle.

      The **Schedule** section appears.

    - In the **Start Date and Time** section, select the date and time on which you want the export schedule to start.
    - In the **Time Zone** drop-down box, select the time zone to which you want the schedule to adhere.
    - In the **Repeat** drop-down box, select how often you want the export to repeat.
    - In the **Repeat Ends** drop-down, select the date on which you want the schedule to end.

      Note: If you select never, the schedule repeats until you modify or delete the export schedule.

11. (Optional) To send email notifications on completion of the export:

    Note: You can enable email notifications with or without scheduling exports.

    - Click the **Email Notification** toggle.

      The **Email Notification** section appears.

- In the **Add Recipients** box, type the email addresses to which you want to send the export notification.
- (Required) In the **Password** box, type a password for the export file. You must share this password with the recipients to allow them to download the file.

> **Note**: Tenable Web App Scanning sends an email to the recipients and from the link in the email, the recipients can download the file by providing the correct password.

12. Click **Export**.

    Tenable Web App Scanning begins processing the export. Depending on the size of the exported data, Tenable Web App Scanning may take several minutes to process the export.

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

13. Access the export file via your browser's downloads directory. If you close the export plane before the download finishes, then you can access your export file from the Exports page.

Delete a Managed Credential

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

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

You can delete any credentials where you have **Can Edit** permission.

To delete a managed credential:

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

   The left navigation plane appears.

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

   The **Settings** page appears.

3. Click the **Credentials** tile.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.

4. Filter or search the credentials table for the credential you want to delete. For more information, see Tenable Web App Scanning Tables.

5. In the table, roll over the credential you want to delete.

   The action buttons appear in the row.

6. Click the 🗑 button.

   The **Confirm Deletion** window appears.

7. Do one of the following:

   - If no scans use the credential, click **Delete**.
   - If any scans use the credential:

a. Click **View Scans**.

   The **Scans** plane appears.

b. Filter or search for scans that use the credential.

c. Do one of the following:

   - Click **Cancel** to cancel the deletion.
   - Click **Delete** to confirm the deletion.

File and Process Allowlist

Tenable suggests permitting the use of the following Tenable Web App Scanning (WAS) files and processes in both first-party and third-party endpoint security software, including anti-virus programs and host-based intrusion and prevention systems.

Allowlist
Files
/opt/ruby/lib/ruby/*/bundler/templates/newgem/bin/*.tt
/opt/ruby/lib/ruby/gems/*/gems/bundler-*/lib/bundler/templates/newgem/bin/*.tt
Processes
/opt/nessus-was-scanner-*/bin/*
/opt/nessus-was-scanner-*/bundle/ruby/*/bin/*
/opt/nessus-was-scanner-*/bundle/ruby/*/gems/*/bin/*
/opt/openssl/bin/*
/opt/ruby/bin/*
/opt/ruby/lib/ruby/*/bundler/templates/newgem/bin/*
/opt/ruby/lib/ruby/gems/*/gems/*/bin/*