



Tenable Attack Surface Management User Guide

Last Revised: August 28, 2025



Table of Contents

Welcome to Tenable Attack Surface Management	9
Getting Started with Tenable Attack Surface Management	9
Log in to Tenable Attack Surface Management	9
Create Your First Inventory	10
Add Users to Tenable Attack Surface Management	10
Filter Your Assets	11
Create Saved Queries	13
Create Subscriptions	14
Set Up Notifications	15
Expand Tenable Attack Surface Management into Tenable One	16
Tenable Attack Surface Management Licensing	19
Access the Workspace	21
Workspace Menu	22
Workspace Page	22
Attack Surface Management FAQ	25
Key Terms	27
Tenable Attack Surface Management Roles	31
Create a Custom Role	31
Navigating the Administrator Interface	33
Access the Tenable Attack Surface Management Administrator Interface	33
Add Users to Tenable Attack Surface Management	34
Updating User Roles	34
Edit Inventory Details	35



Edit Business Details	37
Explore	40
Cloud Sensors	47
Inventory	50
Create an Inventory	51
Inventory Settings	53
Inventory Columns	55
Asset Prioritization	66
Enable the Severity Column	67
Leave an Inventory	67
Manage Inventory Sources	68
Add Sources	68
Add a Subdomain	84
Move a Domain	85
Update a Source Screenshot	86
Remove a Source	86
Exclusion Rules	87
Create an Exclusion Rule	88
Run Exclusion Rules	90
Delete an Exclusion Rule	91
Automation Rules	92
Create an Automation Rule	92
Automation Rule Settings	94
Modify an Automation Rule	97



Delete an Automation Rule	99
Asset Details	100
View Asset Attribution	103
Export an Asset	105
Manage Asset Tags	106
Move or Copy Assets to another Inventory	110
Archive an Asset	111
Suggested Domains	112
Add Suggested Domains to an Inventory	114
Archive Suggested Domains	115
Suggestion Blocklist	115
Manage Suggested Domains	116
Manage source-based suggestions	117
Manage brand names	117
Manage registrator emails	118
Manage organization names	119
Manage nameservers	120
Manage backref links	121
Subscriptions	121
Set Up Notifications	122
Add Subscriptions	124
Predefined Subscription Categories	124
Create Custom Subscriptions	125
Share a Subscription	126



Copy a Subscription	126
Delete a Subscription	127
Activity Logs	128
Dashboard	131
Manage Dashboards	132
Create a Dashboard	132
View Assets	134
Edit a Dashboard	134
Delete a Dashboard	135
Export a Dashboard	136
Copy a Dashboard	136
Categories of Security Risk	137
TXT Records	139
User Profile	141
Generate API Keys	142
Manage Integrations	142
Add Integrations	144
Filter by Integration Type	145
Edit Integration	145
Delete Integration	146
Integrate with Cloudflare	146
Integrate with AWS	147
Integrate with AWS Using Keyless Authentication	150
Configure AWS for Keyless Authentication	150



Integrate with Microsoft Azure	153
Integrate with Azure Using Keyless Authentication	156
Configure Azure for Keyless Authentication	157
Integrate with Tenable Vulnerability Management	160
Asset Deletion	165
View Deleted Assets	165
Restore Assets	167
Accessing Tenable Attack Surface Management in Tenable Vulnerability Management	168
Integration Characteristics	168
Asset Identification Characteristics	169
Host Asset Conditions	170
Integrate with Tenable Web App Scanning	170
Asset Deletion	174
View Deleted Assets	174
Restore Assets	176
Accessing Tenable Attack Surface Management in Tenable Web App Scanning	176
Integration Characteristics	177
Integrate with Google Cloud Platform	179
Integrate with GCP Using Keyless Authentication	181
Configure GCP for Keyless Authentication	181
Cloud Assets	187
View Cloud Assets	187
View Asset Details for Host and Web Application Assets	189
Automatic Population of Primary Domains of a Container	189



Reports	195
Navigate Tenable Attack Surface Management	198
Triage	200
Inventory	202
Create an Inventory	203
Inventory Settings	204
Inventory Columns	207
Asset Prioritization	218
Enable the Severity Column	219
Leave an Inventory	220
Manage Inventory Sources	222
Add Sources	222
Add a Subdomain	237
Move a Domain	238
Update a Source Screenshot	240
Remove a Source	241
Asset Filters	243
Asset Details	255
View Asset Attribution	262
Export an Asset	266
Manage Asset Tags	268
Tagging View	273
Tag Assets Quickly	276
Move or Copy Assets to another Inventory	276



Archive an Asset	279
Create an Advanced Network Scan	279
Create a Web Application Scan	280



Welcome to Tenable Attack Surface Management

Getting Started with Tenable Attack Surface Management

Tenable Attack Surface Management (formerly known as Tenable.asm) is a web-based inventory tool that you can use to identify internet-accessible assets that may or may not be known to your organization. Tenable Attack Surface Management identifies assets using DNS records, IP addresses, and ASN, and includes more than 180 columns of metadata to help you organize and inventory your assets.

To get started with Tenable Attack Surface Management, complete the following steps:

1. [Log in to Tenable Attack Surface Management](#)
2. [Create Your First Inventory](#)
3. [Add Users to Tenable Attack Surface Management](#)
4. [Filter Your Assets](#)
5. [Create Saved Queries](#)
6. [Set Up Notifications](#)

Tip: For additional information on Tenable Attack Surface Management, review the following customer education materials:

- [Tenable Attack Surface Management Introduction \(Tenable University\)](#)

Log in to Tenable Attack Surface Management

To log in to Tenable Attack Surface Management:

1. In a supported browser, navigate to <https://cloud.tenable.com/>. The login page appears.
2. Type your **Username** and **Password** credentials.
3. Click **Sign In**.

The [Workspace](#) page appears.

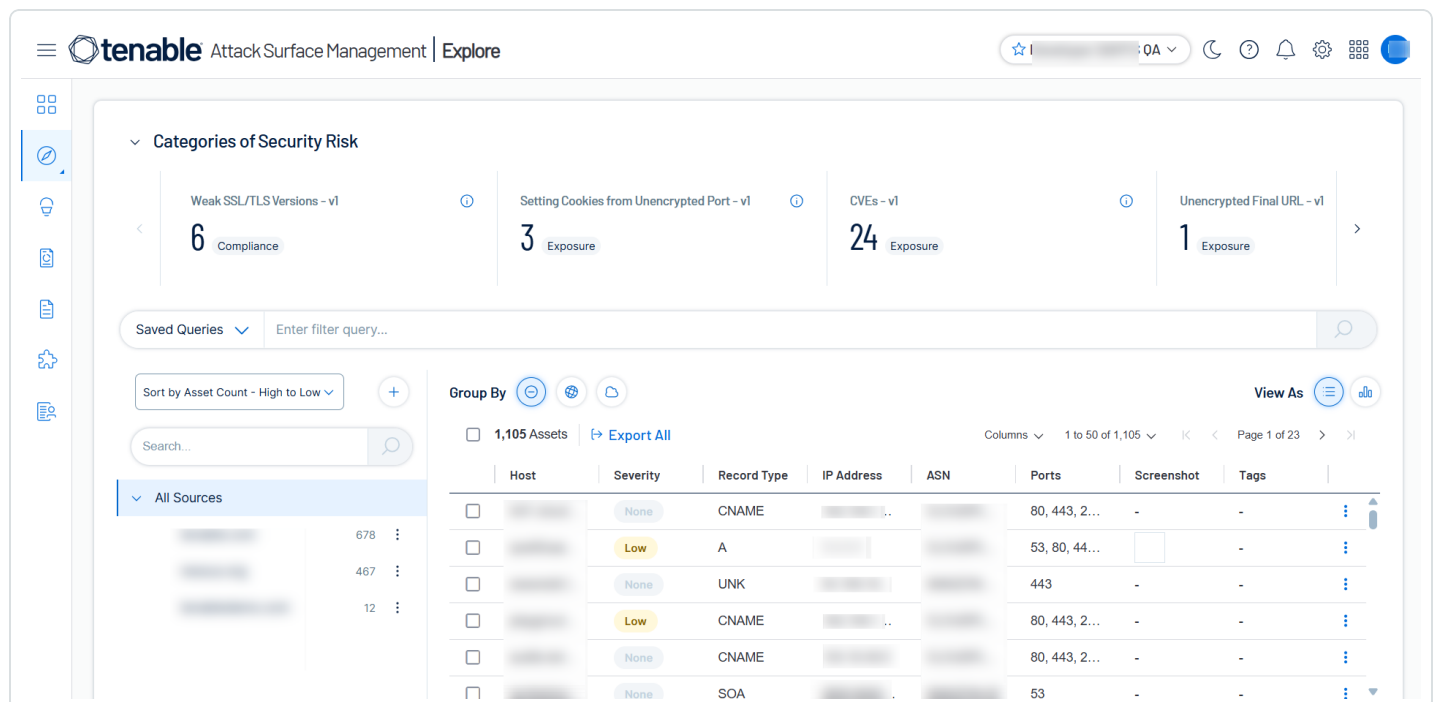
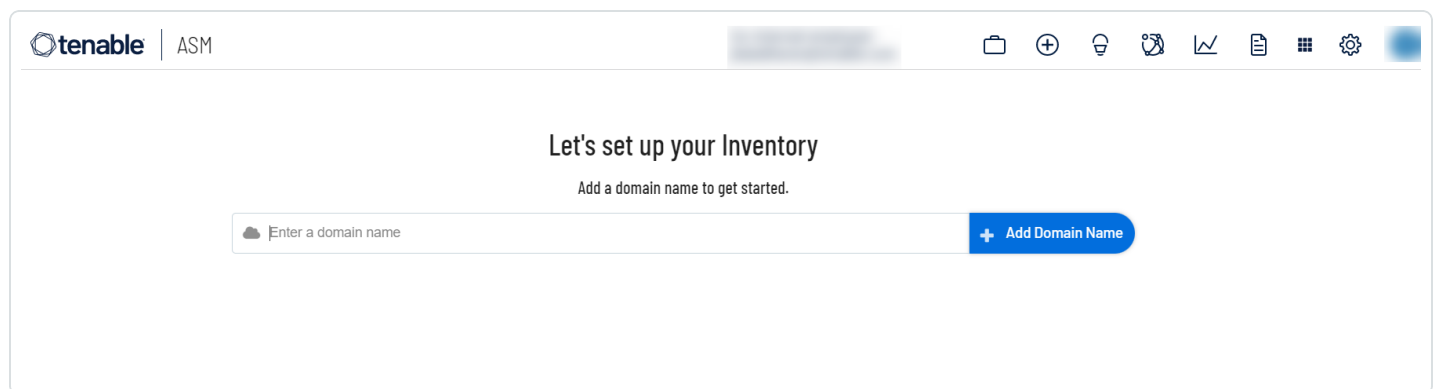


4. Click the Tenable Attack Surface Management tile.

The Tenable Attack Surface Management interface appears, where you can identify internet-accessible assets that may or may not be known to your organization.

Create Your First Inventory

When you log in to Tenable Attack Surface Management for the first time, you can see the **Let's set up your Inventory** page. Type your organization's domain name and click the **+ Add Domain Name** button. Tenable Attack Surface Management starts discovering subdomains and creating your inventory.



Add Users to Tenable Attack Surface Management



To add users to Tenable Attack Surface Management, you must first create users in Tenable Vulnerability Management.

For information about creating users in Tenable Vulnerability Management, follow the instructions in [Create a User Account](#) in the *Tenable Vulnerability Management User Guide*.

(Business Admins only) You can modify user roles and add inventories for users in the Tenable Attack Surface Management [administrator interface](#).

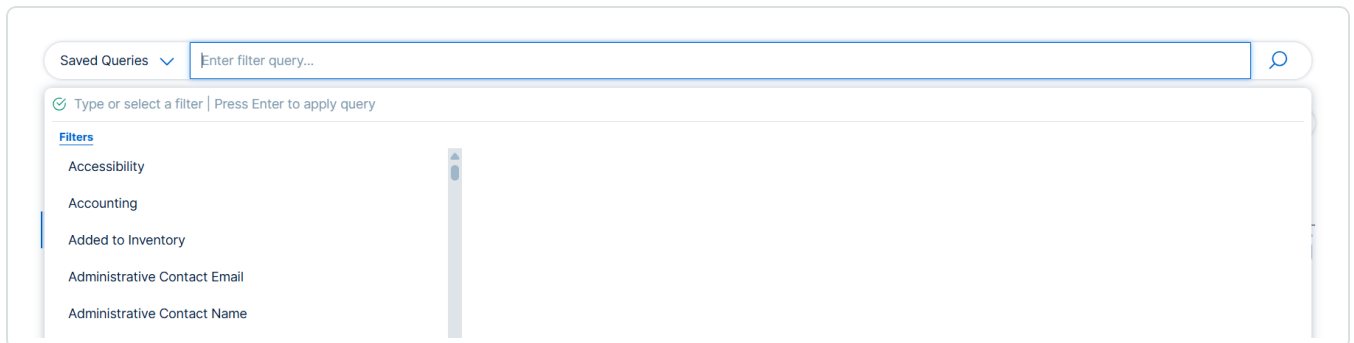
For more information, see [Edit User Account Details](#) and [Edit Inventory Details](#).

Filter Your Assets

Tenable Attack Surface Management uses filters to provide powerful inventory search capabilities. Filters allow you to view specific subsets of assets in your inventory.

To apply a filter:

1. Click inside the **Enter a filter query** box to display the list of available filters.



2. Type or select a filter you want to use.

A list of operators appears. This list varies based on the filter you select.

Saved Queries

Enter filter query...

✓

Type or select a filter

Filters

Accessibility

Accounting

Added to Inventory

Administrative Contact Email

Administrative Contact Name

Administrative Contact Organization

Administrative Contact Telephone

Advertising Networks

Nesting Operators

(

3. If the operator requires a value, type that value in the text box.

Categories of Security Risk

Weak SSL/TLS Versions - v1

Setting Cookies from Unencrypted Port - v1

CVEs - v1

Unencrypted Final URL - v1

6 Compliance

3 Exposure

24 Exposure

1 Exposure

Saved Queries

SSL/TLS Expiration expires in 30 days

✓

Type or select a condition to start adding another filter | Press Enter to apply query

Filters

Social Logins

Social Profiles

SSL/TLS Cypher Suites

SSL/TLS error

SSL/TLS EV Certificate

SSL/TLS Expiration

SSL/TLS Fingerprint

Operators

is expired

is not expired

expires in

within the last

older than

expires on

Values

30

hours

days

months

years

Conditions

AND

OR

- 12 -

4. Add **AND** or **OR** conditions as needed.

5. Press **Enter** to apply the query.

Your inventory displays only assets matching the filter criteria.

In this example, your inventory displays only assets with a TLS certificate that expires within the next 30 days. The SSL/TLS Expiration column also appears.

Create Saved Queries

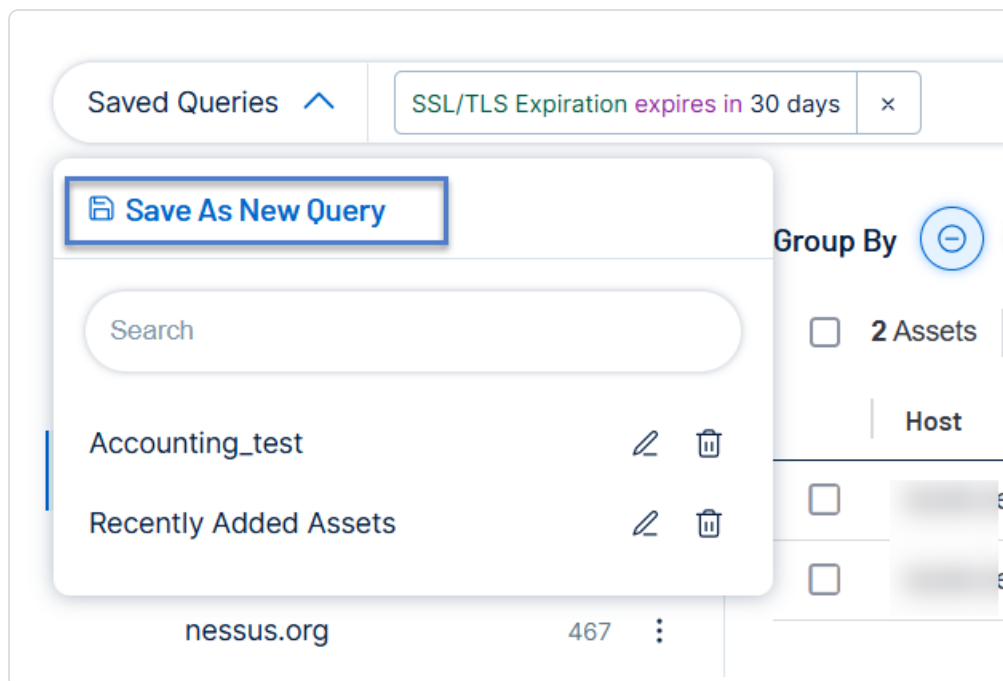
You can save one or more filters as a **Saved Query**. Tenable Attack Surface Management updates saved queries automatically and these contain only the assets that match the applied filters.

For example, if you want to know which assets have TLS certificates that expire within the next 30 days, you can create a Saved Query to refer the filter quickly.

To save a query:

1. [Apply one or more filters](#) to your assets.
2. In the left of the filter box, click the **Saved Queries** drop-down box.

The saved queries list appears.



3. Click **Save as New Query**.



A box for the query name appears.

4. Provide a name for a query.
5. Click ✓ to save the query.

Tenable Attack Surface Management adds the query to the list.

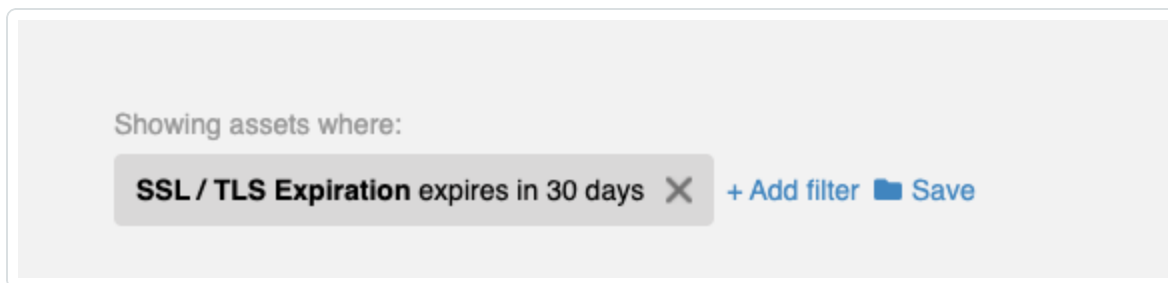
Create Subscriptions

You can save one or more filters as a **Subscription**. Tenable Attack Surface Management updates subscriptions automatically and these contain only the assets that match the applied filters.

For example, if you want to know which assets have TLS certificates that expire within the next 30 days, you can create a **Subscription** to refer the filter quickly.

To create a **Subscription**:

1. [Apply one or more filters](#) to your assets.
2. To the right of the applied filter, click **Save**.



The **Create Subscription** window appears.

3. In the **Subscription name** box, type a name for the subscription.
4. Click **Create Subscription**.

A confirmation window appears with a link to the newly created subscription.

5. Click the link in the confirmation window.

Your subscription appears with a list of assets that match the applied filter.



Expiring TLS Certificates

Total Assets

673

Domains

0

Subdomains

513

Showing assets where:

SSL / TLS Expiration expires in 30 days

1-25 of 673

<input type="checkbox"/>	Host	Record Type	IP	Ports	SSL / TLS Expiration	Screenshot
		CNAME		80, 443	Sun Oct 18 2020	
		CNAME		80, 443	Sun Oct 18 2020	
		CNAME		80, 443	Tue Oct 06 2020	
		CNAME		80, 443	Tue Oct 06 2020	
		CNAME		80, 443	Sun Oct 18 2020	
		CNAME		80, 443	Sun Oct 18 2020	
		CNAME		80, 443	Tue Oct 06 2020	
		CNAME		80, 443	Sun Oct 18 2020	
		CNAME		80, 443	Tue Oct 06 2020	
		CNAME		80, 443	Tue Oct 06 2020	
		CNAME		80, 443	Sun Oct 18 2020	
		CNAME		80, 443	Tue Oct 06 2020	

To see a list of all your subscriptions, click the  icon in the left navigation bar.








Set Up Notifications

If certain aspects of your inventory change, Tenable Attack Surface Management provides a notification system that can email you, send you a Slack message, or communicate through ServiceNow.

For example, you can receive an email notification when an asset has a TLS certificate that expires soon by using the **Subscription** that you created previously.



1. Hover over the row that contains your *Expiring TLS Certificates* subscription, and click the bell icon:

Folders				
Name↓	Updated	Assets		
 Archived Results	a few seconds ago	0		
 Expiring TLS Certificates	a few seconds ago	673	  	
 Recently Added Assets	a few seconds ago	1,058		


The following window appears:

Alerts for Expiring TLS Certificates

Email


Receive a daily summary of changes • Setup

☐

 servicenow.

Sends an email to a ServiceNow email address • Setup

☐

 slack

Posts a message to an incoming webhook • Setup

☐

Close

2. To enable email notifications, click the **Email** toggle.
3. Type your email address and press **Save**.

Tenable Attack Surface Management now sends daily emails that give you a list of assets that have a TLS certificate expiring in 30 days.

Expand Tenable Attack Surface Management into Tenable One



Note: This requires a Tenable One license. For more information about trying Tenable One, see [Tenable One](#).

Integrate Tenable Attack Surface Management with Tenable One and leverage the following features:

- Access the [Exposure View](#) page, where you can gain critical business context by getting business-aligned cyber exposure score for critical business services, processes and functions, and track delivery against SLAs. Track overall risk to understand the risk contribution of assets to your overall Cyber Exposure Score, including by asset class, vendor, or by tags.
 - [View](#) and [manage](#) cyber exposure cards.
 - View [CES](#) and [CES trend](#) data for the Global exposure card.
 - View [Remediation Service Level Agreement](#) (SLA) data.
 - View [Tag Performance](#) data.
- Access the [Exposure Signals](#) page, where you can generate exposure signals that use queries to search for asset *violations*. Simply put, if an asset is impacted by a weakness related to the query, then the asset is considered a *violation*. Using this, you can gain visibility into your most critical risk scenarios.
 - Find top active threats in your environment with up-to-date feeds from Tenable Research.
 - View, generate, and interact with the data from queries and their impacted asset violations.
 - Create custom exposure signals to view business-specific risks and weaknesses
- Access the [Inventory](#) page, where you can enhance asset intelligence by accessing deeper asset insights, including related attack paths, tags, exposure cards, users, relationships, and more. Improve risk scoring by gaining a more complete view of asset exposure, with an asset exposure score that assesses total asset risk and asset criticality.



- View and interact with the data on the [Assets](#) tab:
 - Review your AD assets to understand the strategic nature of the interface. This should help set your expectations on what features to use within Tenable Exposure Management, and when.
 - Familiarize yourself with the [Global Asset Search](#) and its objects and properties. Bookmark custom queries for later use.
 - Find devices, user accounts, software, cloud assets, SaaS applications, networks, and their weaknesses.
 - Drill down into the [Asset Details](#) page to view asset properties and all associated context views.
- View and interact with the data on the [Weaknesses](#) tab:
 - View key context on vulnerability and misconfiguration weaknesses to make the most impactful remediation decisions.
- View and interact with the data on the [Software](#) tab:
 - Gain full visibility of the software deployed across your business and better understand the associated risks.
 - Identify what software may be out of date, and which pieces of software may soon be End of Life (EoL).
- View and interact with the data on the [Findings](#) tab:
 - View instances of weaknesses (vulnerabilities or misconfigurations) appearing on an asset, identified uniquely by plugin ID, port, and protocol.
 - Review insights into those findings, including descriptions, assets affected, criticality, and more to identify potential security risks, visibility on under-utilized resources, and support compliance efforts.
- Access the [Attack Path](#) page, where you can optimize risk prioritization by exposing risky attack paths that traverse the attack surface, including web apps, IT, OT, IoT, identities, ASM, and prevent material impact. Streamline mitigation by identifying choke points to disrupt



attack paths with mitigation guidance, and gain deep expertise with AI insights (**Not supported in [FedRAMP](#) environments**).

- View the [Dashboard](#) tab for a high-level view of your vulnerable assets such as the number of attack paths leading to these critical assets, the number of open attack techniques and their severity, a matrix to view paths with different source node exposure score and ACR target value combinations, and a list of trending attack paths.
 - Review the **Top Attack Path Matrix** and click the **Top Attack Paths** tile to view more information about paths leading to your “Crown Jewels”, or assets with an ACR of 7 or above.

You can adjust these if needed to ensure you’re viewing the most critical attack path data.

- On the [Top Attack Techniques](#) tab, view all attack techniques that exist in one or more attack paths that lead to one or more critical assets by pairing your data with advanced graph analytics and the MITRE ATT&CK® Framework to create attack techniques, which allow you to understand and act on the unknowns that enable and amplify threat impact on your assets and information.
- On the [Top Attack Paths](#) tab, generate attack path queries to view your assets as part of potential attack paths:
 - [Generate an Attack Path with a Built-in Query](#)
 - [Generate an Attack Path Query with the Attack Path Query Builder](#)
 - [Generate an Asset Query with the Asset Query Builder](#)

Then, you can view and interact with the [Attack Path Query](#) and [Asset Query](#) data via the query result list and the [interactive graph](#).

- Interact with the [MITRE ATT&CK Heatmap](#) tab.
- View and interact with the data in the [Tags](#) page:
 - [Create and manage tags](#) to highlight or combine different asset classes.
 - View the [Tag Details](#) page to gain further insight into the tags associated with your assets.

Tenable Attack Surface Management Licensing



This topic breaks down the licensing process for Tenable Attack Surface Management as a standalone product. It also explains how assets are counted and describes what happens during license overages or expirations.

Tenable Attack Surface Management Versions

You can purchase Tenable Attack Surface Management in two versions:

- **Tenable Attack Surface Management Fortnightly Frequency**
- **Tenable Attack Surface Management Daily Frequency**

Licensing Tenable Attack Surface Management

To use any version of Tenable Attack Surface Management, you purchase licenses based on your organizational needs and environmental details. Tenable Attack Surface Management then assigns those licenses to your *assets*: observable objects, which include domain names, subdomains, or IP addresses for internet-connected or internal network devices.

Tip: An observable object is a unique quadruple of DNS record name, DNS record type, DNS record value, and IP address.

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.

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

Note: When you purchase a Tenable Attack Surface Management license, inventory is set to 10% of the purchase limit by default. You can increase this limit on the **Inventory Settings** page. For more information, see [Inventory Settings](#).

How Assets are Counted

All assets in all inventories are counted towards your license, except archived assets.

Reclaiming Licenses



Tenable Attack Surface Management's license count updates daily. The license count updates when you archive individual assets or remove asset sources—and it also updates when assets age out. Removed assets are only counted when restored.

Exceeding the License Limit

In Tenable Attack Surface Management, when your asset count exceeds your license limit, Tenable clearly communicates the overage as follows.

Scenario	Result
You add a source that is greater than your inventory limit.	A message appears in the Source column: <i>"We could not add all of the subdomains for this domain because your inventory is full."</i>
You reach your inventory asset limit.	When you click the inventory, a message appears: <i>"You have reached your limit of # assets. Please contact us to increase your limit."</i>
You reach your business limit, which is related to your licensed asset purchase.	A message appears in Tenable Attack Surface Management: <i>"Business Asset limit reached. Please contact support to increase the Business Asset limit."</i>

Expired Licenses

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

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

Access the 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.




The [Workspace menu](#), which appears in the top navigation bar, allows you to quickly switch between your Tenable applications from any page.

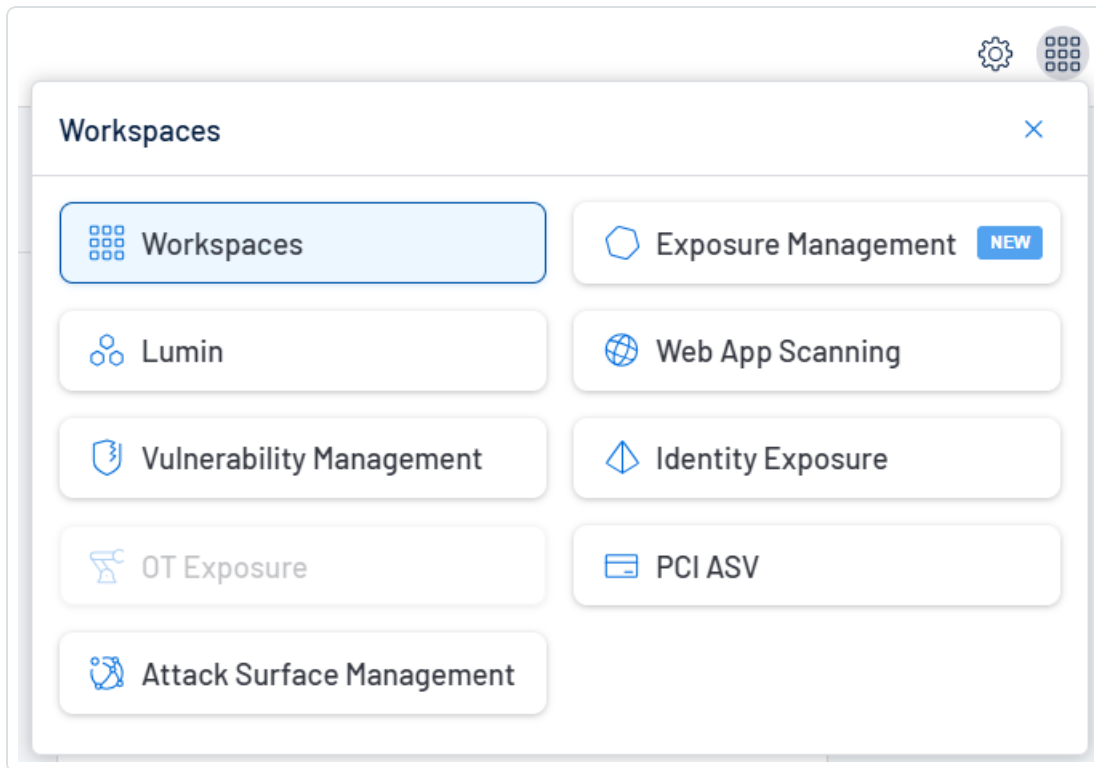
Important: Tenable disables application tiles for expired applications. Tenable removes expired application tiles from the **Workspace** page and menu 30 days after expiration.

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.

Workspace Page

To view the Workspace page:

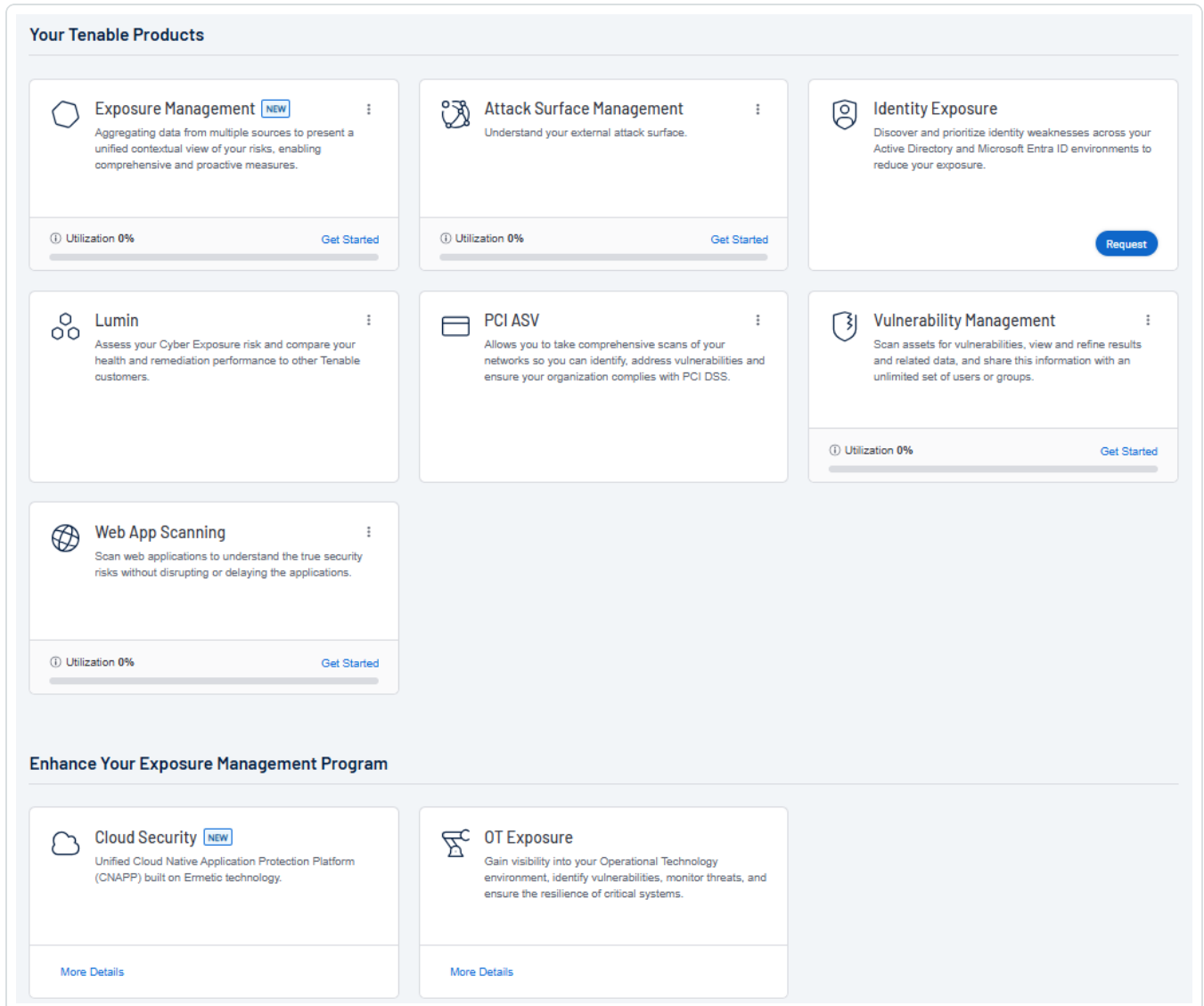


1. From any Tenable application, in the upper-right corner, click the  button.

The **Workspace** menu appears.

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

The **Workspace** page appears.



The screenshot displays the 'Your Tenable Products' section of the Tenable Workspace. It features a grid of product tiles, each with an icon, title, description, and utilization status. The products shown are:

- Exposure Management** (NEW): Aggregating data from multiple sources to present a unified contextual view of your risks, enabling comprehensive and proactive measures. Utilization: 0%. [Get Started](#)
- Attack Surface Management**: Understand your external attack surface. Utilization: 0%. [Get Started](#)
- Identity Exposure**: Discover and prioritize identity weaknesses across your Active Directory and Microsoft Entra ID environments to reduce your exposure. [Request](#)
- Lumin**: Assess your Cyber Exposure risk and compare your health and remediation performance to other Tenable customers.
- PCI ASV**: Allows you to take comprehensive scans of your networks so you can identify, address vulnerabilities and ensure your organization complies with PCI DSS.
- Vulnerability Management**: Scan assets for vulnerabilities, view and refine results and related data, and share this information with an unlimited set of users or groups. Utilization: 0%. [Get Started](#)
- Web App Scanning**: Scan web applications to understand the true security risks without disrupting or delaying the applications. Utilization: 0%. [Get Started](#)

Below the product tiles is the 'Enhance Your Exposure Management Program' section, which includes:

- Cloud Security** (NEW): Unified Cloud Native Application Protection Platform (CNAPP) built on Ermetic technology. [More Details](#)
- OT Exposure**: Gain visibility into your Operational Technology environment, identify vulnerabilities, monitor threats, and ensure the resilience of critical systems. [More Details](#)

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

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



selected application.

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

- **Set a default application:**

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

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

To set a default login application:

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

A menu appears.

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

This application now appears when you log in.

- **Remove a Default Application:**

To remove a default login application:

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

A menu appears.

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

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

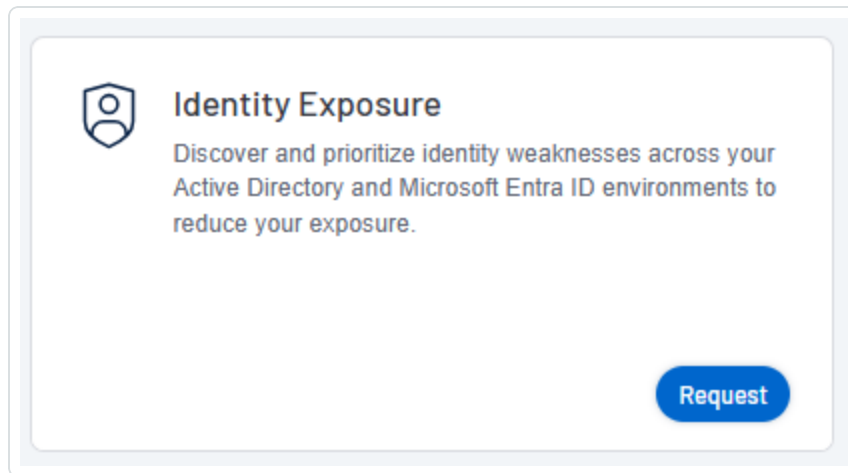
- **Request Access to a Tenable application:**

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



To request access to a Tenable application:

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



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

Attack Surface Management FAQ

What is an attack surface?

An attack surface comes from the network perspective of an adversary, the complete external asset inventory of an organization including all actively listening services (open ports) on each asset.

What is Attack Surface Mapping?

Attack Surface Mapping is the process of discovering and documenting the complete attack surface of an organization. An Attack Surface Map includes the hostnames and IP addresses of each externally facing asset, the listening ports on each, and as much meta-data about each asset as possible. Meta data may include software distribution and version information, IP geolocation, TLS stack information, and so on.

What types of things does Tenable Attack Surface Management help map?

Tenable Attack Surface Management automatically discovers all domain names, hostnames, and IP address for each asset in an organization's attack surface map. Tenable Attack Surface Management may collect over 120 columns of data about each asset. These assets may be located



on-premises, in the cloud, hosted services, and more.

What is considered an asset in Tenable Attack Surface Management?

An asset is a combination of four values: IP address, Fully Qualified Domain Name (FQDN), Record Type, and Record Value. If any of the values differ, it is considered as a separate asset.

What is a record type in Tenable Attack Surface Management?

Record types in Tenable Attack Surface Management are Domain Name System (DNS) records.

How does Attack Surface Mapping help keep organizations secure?

An organization can only secure what they know they own. Most companies have no documented Attack Surface Map at all. For those who do, it is common for the attack surface map to be highly incomplete and out-of-date, possibly leaving thousands of assets unidentified. The security team cannot protect these unidentified assets, often referred to as shadow IT, resulting in lost data and frequent cyber attacks. Tenable Attack Surface Management fills in the gaps in your data and gives you a high-fidelity view of your entire attack surface.

What other features does the Tenable Attack Surface Management service have?

Tenable Attack Surface Management platform sends alerts in real time whenever an inventory changes such as when new servers are brought online, new ports open, and server software needs patching. Tenable Attack Surface Management continually monitors your attack surface and lets you know as it constantly evolves and changes.

Tenable Attack Surface Management also offers advanced technology fingerprinting by identifying CVEs, open ports, running services, thousands of software versions, geolocation, login forms, secret keys, ASNs, programming frameworks, HTML, and much more. Tenable Attack Surface Management can do all of this within minutes as opposed to days with a competitor.

There has been an increased interest in Attack Surface Mapping over the past few years, why do you think that is?

The increased interest in Attack Surface Mapping is easy to explain. The adversary has been targeting an organization's secondary and tertiary assets for exploitation, many unknown to the organization and not just the well-known primary systems. Often these unknown assets are legacy,



long forgotten, and not adequately secured. These assets often connect to other sensitive areas of the network where a breach of highly sensitive data may be achieved.

Key Terms

The following key terms apply to the Tenable Attack Surface Management user interface:

Term	Definition
Asset	<p>An asset is a tuple of a hostname, a record type, an IP address and when applicable a record value. For instance a CNAME may point to another CNAME and so on, so where it points and the IP address it finally resolves to would be a constituent part of the asset. Assets represent Internet connected or internal network connected devices. An asset may include, but not limited to web servers, name servers, IoT devices, network printers, etc. Three examples might be:</p> <p>Asset 1: www.example.com,A,123.123.123</p> <p>Asset 2: www.foo.com,CNAME,www.bar.com,111.111.111.111</p> <p>Asset 3: www.foo.com,CNAME,www.bar.com,222.222.222.222</p> <p>In this way, you may have a single hostname with multiple assets associated with it, to ensure that all of the application virtual hosting code is properly exercised. This is a frequent feature of round robin DNS, and therefore important to find applications that are incorrectly configured within a cluster, or when geographically diverse.</p>
Asset Inventory	<p>A complete collection of an organization's assets and associated metadata of each asset.</p>
Asset Management	<p>Asset management refers to monitoring, configuring, and maintaining of assets.</p>
Attack Surface	<p>From the network perspective of an adversary, the complete asset inventory of an organization including all actively listening services (open ports) on each asset.</p>
Autonomous	<p>An ASN is a unique number that's available globally to identify an</p>



Term	Definition
System Number (ASN)	autonomous system and which enables that system to exchange exterior routing information with other neighboring autonomous systems.
Content Delivery Network (CDN)	A CDN refers to a geographically distributed group of servers which work together to provide fast delivery of Internet content.
Discovery	Discovery refers to the act of identifying assets.
Domain Name	<p>A domain name is a label that identifies a network domain. Domain names are used to identify Internet resources, such as computers, networks, and services, with an easy-to-remember text label that is easier to memorize than the numerical addresses used in the Internet protocols.</p> <p>Example: foo.tld is the domain name of URL http://www.foo.tld/index.html.</p>
External	Refers to the accessibility of an asset that can be connected to from across the Internet.
Host	A device connected to a network that communicates with other hosts on the network.
Hostname	<p>A unique name given to any device that is connected to a specific computer network, typically appended to a domain name, and resolves to an IP-address using the Domain Name System (DNS).</p> <p>Example: 'bar' is the hostname of bar.foo.tld.</p>
Internal	Refers to the accessibility of an asset that cannot be connected to from across the Internet, and generally resides on an internal network (i.e. Intranet).
Orphaned Hostname	<p>A hostname that no longer resolves to an IP-address.</p> <p>Internet-accessible, internet-connected, internet-facing.</p> <p>Refers to an asset that can be connected to over the Internet. While</p>



Term	Definition
	the terms above are often used interchangeably, Internet-accessible is considered the preferred term.
Metadata	A set of data that describes and gives information about an asset. Metadata may include, but not limited to geolocation, operating system, open ports, service banners, TLS certificate details, etc.
Reconnaissance / Recon	The act of finding assets.
Routable / Non-Routable	Refers to a type of IP-address where network traffic can be routed to over the Internet. As defined by RFC-1918, there are certain IP-address ranges where network traffic cannot be routed to over the Internet, which are referred to as 'non-routable' IP-addresses or 'private' IP-space.
Non-Routable IP-Addresses (RFC-1918)	10.0.0.0 – 10.255.255.255 (10/8 prefix) 172.16.0.0 – 172.31.255.255 (172.16/12 prefix) 192.168.0.0 – 192.168.255.255 (192.168/16 prefix)
Open / Listening Service	Short for open ports on a server, or a service on the server that responds to network requests.
Port Scan	Scan that analyzes a server to determine which ports are open.
Subdomain	A subdomain is a domain name with a hostname appended, which is sometimes more accurately described as a fully qualified domain name (FQDN). Example: bar.foo.tld
Top-Level Domain (TLD)	Refers to the last segment of a domain name, the part following immediately after the "dot" symbol. The most common and familiar TLDs are .com, .net, and .org. Example: TLD is the Top-Level Domain name of the domain name bar.foo.tld



Term	Definition
	There are many other TLDs, such as .co.uk and co.jp, which are technically not TLDs because they are not located at the 'top level' of the domain. These types of domains which are referred to as effective TLDs (eTLDs) because they serve a branching point for domain name registrars.
Validity	A configuration option for Apps that establishes how often the app should try to get new data.
Virtual Host	Refers to a method for hosting multiple hostnames or domain names, with separate handling of each name, on a single server.



Tenable Attack Surface Management Roles

You can assign Tenable-provided roles to users at the time of creating them in Tenable Vulnerability Management. Each role in Tenable Vulnerability Management corresponds to an existing role in Tenable Attack Surface Management. For more information about the Tenable-provided roles and privileges, see [Tenable-Provided Roles and Privileges](#).

Note: You can now assign all roles for Tenable Attack Surface Management in Tenable Vulnerability Management.

Tenable-provided Roles	Tenable Attack Surface Management Roles
Administrator	Business Admin
Scan Manager	Active User
Scan Operator	Active User, Cloud Connector Manager
	Note: Assign the Cloud Connector Manager role to the user for integrations.
Standard	View Only
Basic	View Only

To create custom roles for Tenable Attack Surface Management, see [Create a Custom Role](#).


Note: Tenable One users with a custom role allowing access to Tenable Attack Surface Management will have the same permissions as a **View-Only** user in Tenable Attack Surface Management.

Create a Custom Role

In Tenable Attack Surface Management, you can add a role for the Tenable Attack Surface Management user in Tenable Vulnerability Management. For more information about creating a custom role, see [Create a Custom Role](#) in the Tenable Vulnerability Management User Guide.

To create a custom role for Tenable Attack Surface Management:



1. In Tenable Vulnerability Management, click the  icon in the top navigation bar.

Alternatively, in the left navigation bar, click  and go to **Settings > Access Control**.

The **Access Control** page appears.

2. In the **Roles** tab, click **Add Role**.

The **Add Role** page appears.

3. In the left pane, click **Attack Surface Management**.

The parameters relevant to the Attack Surface Management role appear.

4. In the **Name** box, type a name for the role.
5. In the **Description** box, type a description for the role.
6. Click the **Enable Attack Surface Management** toggle to allow the user to access the application from the Workspace.

The **Business** and **Inventory** checkboxes appear. These indicate the level of permission you want to assign to the user.

- Enabling the toggle without selecting any of the checkboxes assigns only **read-only** permission.
- **Business** — Assigns the **Business Admin** role. Selecting this role automatically enables the **Inventory** checkbox.
- **Inventory** — Assigns write access to the inventory.



Navigating the Administrator Interface

User accounts with a **Business Admin** role can access the Tenable Attack Surface Management administrator interface.

The screenshot shows the Tenable Attack Surface Management administrator interface. The top navigation bar includes the Tenable logo, the text 'Attack Surface Management', and a user profile icon. Below the navigation bar, there are three tabs: 'USERS', 'INVENTORIES', and 'BUSINESSES'. The 'USERS' tab is active, and a blue notification badge with the number '1' is visible. The main content area features a 'Find User' search form with fields for 'Email' and 'Inventory', and a 'Search' button. Below the search form, a table displays the search results. The table has columns for ID, Name, Email, Role, Status, Disabled after, Inventory, Created, and an 'Edit' button. One user is listed with ID 54, Role Business Admin, and Created 2 years ago.

ID	Name	Email	Role	Status	Disabled after	Inventory	Created	
54			Business Admin		-		2 years ago	Edit

Business Admins can do the following:

- View and edit the list of users in the business organization.
- Assign or remove inventories to a user account.
- Change the default asset limit for a specific inventory or for all inventories.
- Create new inventories.
- Modify user role.
- Disable a user.

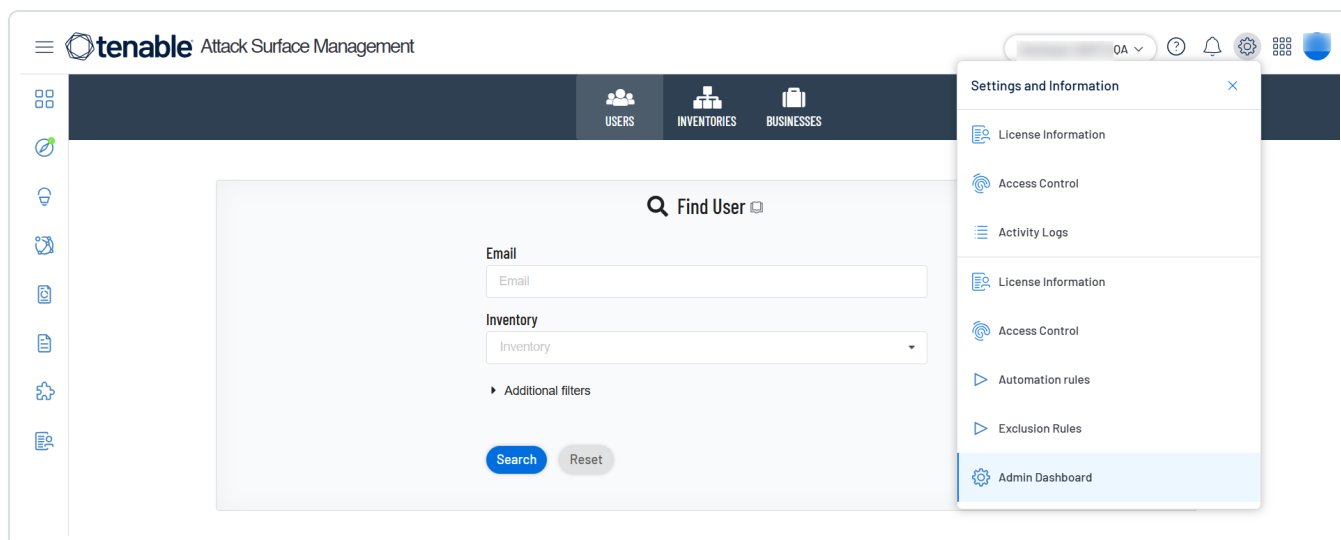
Access the Tenable Attack Surface Management Administrator Interface

To access the administrator interface:



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

The **Settings and Information** drop-down appears.



2. Click **Admin Dashboard**.

The Tenable Attack Surface Management administrator window appears. By default, the **Users** window opens.

There are three tabs available in the administrator interface — **Users**, **Inventories**, and **Businesses**.

Add Users to Tenable Attack Surface Management

To add users to Tenable Attack Surface Management, you must first create users in Tenable Vulnerability Management. For more information, see [Create a User Account](#) in the *Tenable Vulnerability Management User Guide*.

Users appear in the Tenable Attack Surface Management administrator interface after they log in to Tenable Attack Surface Management for the first time.

Updating User Roles

Required User Role: Business Admin




You can update Tenable Attack Surface Management user roles in Tenable Vulnerability Management. After you change the user role, Tenable Attack Surface Management applies the role to the target user the next time they access Tenable Attack Surface Management. For more information about mapping of roles in Tenable Vulnerability Management to roles in Tenable Attack Surface Management, see [Tenable Attack Surface Management Roles](#).

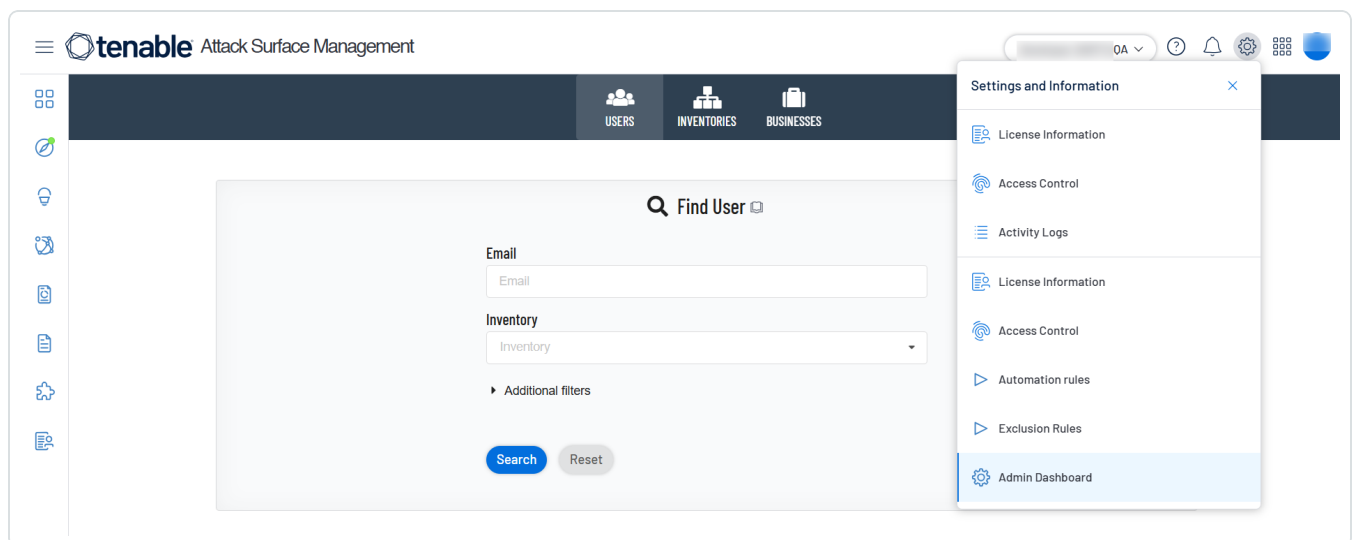
Edit Inventory Details

Required User Role: Business Admin

In the administrator interface, you can modify the default asset limit of an inventory.

To modify inventory details:

1. To access the administrator interface, click the  icon in the upper-right corner.



2. Click **Admin Dashboard**.

By default, the **Users** page with the **Find User** section and the table listing all users appears.

3. Click the **Inventories** tab.

The **Inventories** page appears.

4. Do one of the following:



- (Optional) Search for a specific inventory :
 - a. Provide the following details in the **Find inventory** section:

Parameters	Description
Name	The inventory name.
Notes	Add any notes for the inventory.
Status	Indicates whether the inventory is Active or Deleted .

- b. Click **Search**.

The inventories table displays the list of inventories that matches the filters.

Note: If you want to reset the search details, click **Reset**.

- Create a new inventory.
 - a. Click **Create a new inventory**.

The **Create a new inventory** window appears.

- b. Provide the inventory details in the relevant boxes.

Note: The initial inventory size is 10% of your license limit. You can modify the limit in [Step 5](#).

- c. Click the **Source Suggestions** toggle to enable suggestions for the inventories that you want to add.
 - d. In the **Template Inventory** drop-down box, you can select an inventory to use as a template for the new inventory.
 - e. Click **Create**.

Tenable Attack Surface Management displays the list of inventories in a table format.

5. In the row of the inventory you want to edit, click **Edit**.

The **Edit inventory** window appears.

6. Edit the inventory details. Modify the asset limit as needed.



Note: If you click **Access Now**, Tenable Attack Surface Management adds you to the inventory and redirects you to that inventory page.

7. (Optional) Click **Add all users in the Business** to add all users in the inventory's business organization to the inventory.
8. Click **Update**.

Note: To delete the inventory, click **Delete**.

Tenable Attack Surface Management updates the inventory table and displays the latest changes with the following inventory details in a table format:

Column	Description
ID	The inventory ID.
Name	The name of the inventory.
Notes	The notes about the inventory, if any.
Asset count	<div>The number of assets in the inventory. Note: The Total Assets count on the Inventory page shows the most up-to-date data, while the Administrator page updates once every 24 hours. Some actions might refresh the data sooner, but updates to the Administrator page usually follow the 24-hour schedule.</div>
Asset limit	The asset limit of the inventory.
Users	The number of user accounts assigned the inventory.
Pending Invites	The number of invites awaiting for the inventory.
Status	The status of the inventory, whether active or disabled.
Created	Indicates the time of the inventory creation.


Edit Business Details

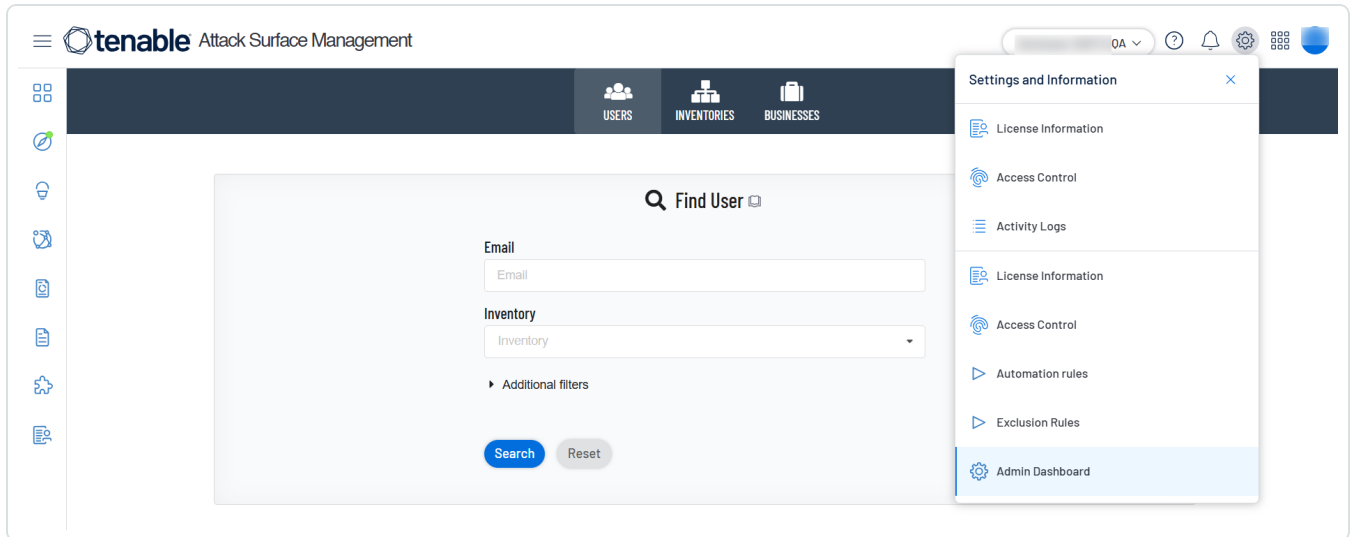
Required User Role: Business Admin



In the administrator interface, you can modify the default asset limit of all inventories in your business organization.

To modify the default asset limit of all inventories in your business:

1. To access the administrator interface, click the  icon in the upper-right corner.



2. Click **Admin Dashboard**.

By default, the **Users** page with the **Find User** section and the table listing all users appears.

3. Click the **Business** tab.

The **Business** page appears.

4. In the row of the business that you want to modify, click **Edit**.

The **Edit business** window appears.

5. To change the default asset limit: in the **Default Asset limit for Inventories** box, modify the value.
6. Click **Save changes**.

Tenable Attack Surface Management saves the changes and displays the following business details in a table format:

Column	Description
--------	-------------



ID	The ID assigned to the business.
Name	The name of the business.
Users	The number of user accounts within the business.
Asset count	The total number of assets across all inventories. Tenable Attack Surface Management refreshes the count daily.
Asset limits	The sum of inventory asset limits currently assigned and the available asset limit for the business.
Inventories	The number of inventories associated the business.




Explore

The **Explore** page in Tenable Attack Surface Management provides central inventory view and allows you to:

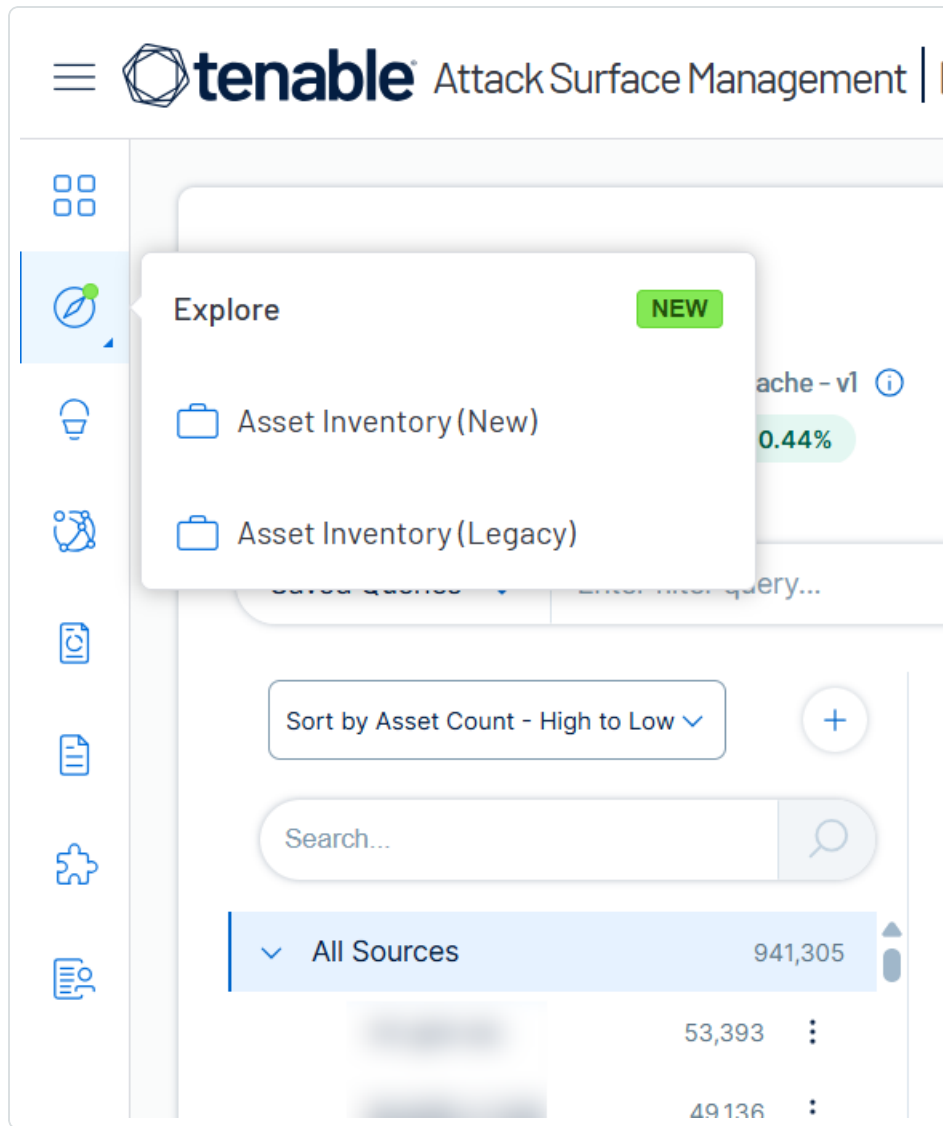
- View security risk categories impacting inventory assets.
- Filter assets using queries and **Saved Queries** to view the security risks.
- Group assets by hostnames or IP addresses.
- Manage sources (add, remove, move).
- Export assets in CSV, XLSX, or JSON.
- Customize asset table columns.
- Manage assets (add, modify, remove).
- View assets in table or chart format.

To access the **Explore** page:

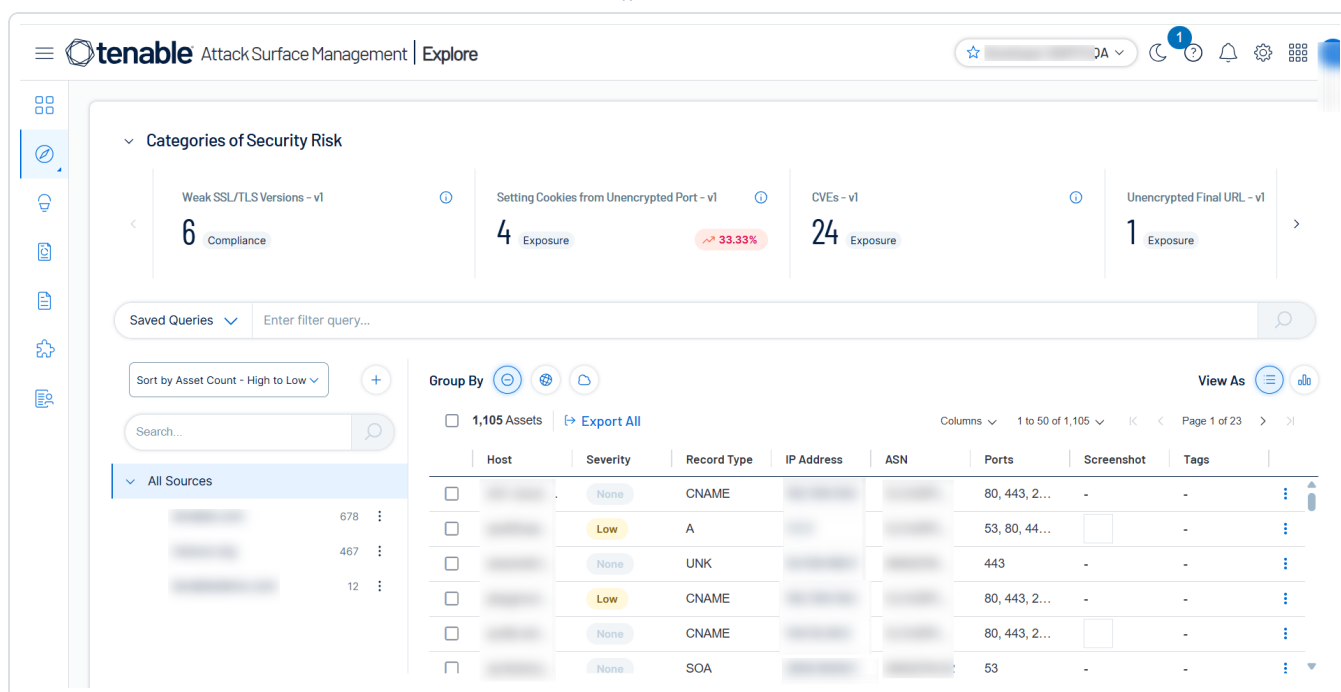
1. In the left navigation bar, click the  button.

The **Explore** menu appears with the options:

- **Asset Inventory (New)**
- **Asset Inventory (Legacy)**



2. Select **Asset Inventory (New)** to open the **Explore** dashboard page. The **Asset Inventory (Legacy)** option opens the legacy user interface.



The **Explore** page in Tenable Attack Surface Management includes the following:

Section	Description
Categories of Security Risk	<p>This panel provides a high-level overview of your assets by listing the critical events in your organization along with the number of your affected assets. Click the > and < arrows to move to the next event.</p> <p>Click a category to view the affected assets in the assets table.</p>
Icons on the left navigation bar	<p>Use the icons to access Suggestions (💡), Reports (📄), TXT Records (📄), Integrations (🔗), Subscriptions (📡), and ASM Activity Logs (📋).</p>
Saved Queries	<p>Save filter queries to track important changes in your environment. Events can include new servers, newly opened or closed ports, and new software. See Asset Filters.</p>
Main panel	<p>The main panel shows the list of assets in a table format. The columns include data such as Host, Severity, IP Address.</p> <ul style="list-style-type: none"> To customize columns, click the Columns drop-down box in the header. In the Customize Columns drop-down box, search for specific columns, add or remove columns, and reset column width.



	<p>See Inventory Columns.</p> <ul style="list-style-type: none">• Use the Group By option to group the assets list by Hostname, IP Address, or None.• Use the Items Per Page drop-down to specify the number of assets on a page: 50,100, 150, or 200.• Use the View As option to view the assets in a table or chart form
Asset Details	Click an asset to view the asset details page. See Asset Details .
Sort by Asset Count	<p>Sort the sources by the asset count: High to Low or Low to High.</p> <p>You can also use the Sort Alphabetically or Sort by Date Added to Inventory to sort the sources.</p>
Search	Use the Search box in the left panel to search for specific sources.
Export All	<ol style="list-style-type: none">1. Click the ➔ Export All button to export the assets table in the following formats:<ul style="list-style-type: none">• CSV• XLSX• JSON2. In the Export window, search for and select the columns to export.3. (Optional) Use the View selected option to view all columns that you selected.4. Click Export. <p>Tenable Attack Surface Management exports all assets in the selected format.</p>
Add Sources	<p>In the Sources panel on the left, click + to add sources to your inventory. Available options:</p> <ul style="list-style-type: none">• Add Hostnames or Domains• Add IP addresses or IP ranges




	<ul style="list-style-type: none">• Add ASN• Add from Cloudflare• Add from AWS• Add from Azure• Add from Google Cloud Platform <p>For more information, see Add Sources</p>
Add Tags or Remove Tags	Add or remove tags for single or multiple assets. See Manage Asset Tags .
Select All Assets	<p>Use the asset count checkbox at the top of the table to select all the assets listed on the page. To select all the assets in the inventory, click the Select all <count> assets link.</p> <p>To clear the selections, click Clear all selections.</p>
Archive	Use the Archive option to archive assets in the inventory. See Archive an Asset .
Create Advanced Network Scan	<ol style="list-style-type: none">1. To create an advanced network scan for a single asset:<ul style="list-style-type: none">• In the row of the asset to scan, click the : button. A menu appears.• Select the checkbox for the asset to create a scan. Tenable Attack Surface Management enables the : More > Create Advanced Network Scan.• Right-click the asset to create a scan. A menu appears.2. Select Create Advanced Network Scan. <p>Tenable Attack Surface Management redirects you to the container to create an advanced network scan.</p>



	<p>To create advanced network scans for multiple assets:</p> <ol style="list-style-type: none">1. Select the checkbox for one or several assets you want to scan. Tenable Attack Surface Management enables the header.2. Click ⋮ More > Create Advanced Network Scan. Tenable Attack Surface Management redirects you to the Advanced Network Scan page in Tenable Vulnerability Management to create an advanced network scan.
Create Web Application Scan	<ol style="list-style-type: none">1. To create an advanced network scan for a single asset:<ul style="list-style-type: none">• In the row of the asset to scan, click the ⋮ button. A menu appears.• Select the checkbox for the asset to create a scan. Tenable Attack Surface Management enables the ⋮ More > Create Web Application Scan.• Right-click the asset to create a scan. A menu appears.2. Select Create Web Application Scan. Tenable Attack Surface Management redirects you to the container to create an advanced network scan. <p>To create advanced network scans for multiple assets:</p> <ol style="list-style-type: none">1. Select the checkbox for one or several assets you want to scan. Tenable Attack Surface Management enables the header.2. Click ⋮ More > Create Web Application Scan. Tenable Attack Surface Management redirects you to Create a Scan - Web App Scan page in Tenable Vulnerability Management to create an advanced network scan.



Copy to Clipboard	To copy the asset hostname, right-click the asset name and select  Copy to Clipboard .
Filter By Value	To filter the assets table by a specific value, right-click any column value and select Filter By Value .
Filter Out Value	To filter out the assets table, right-click and select Filter Out Value .



Cloud Sensors

By default, Tenable provides regional cloud sensors for use in Tenable Attack Surface Management.

The following table identifies each regional cloud sensor and, for allowlist purposes, its IP address ranges. These IP address ranges are exclusive to Tenable.

Tenable Attack Surface Management uses these IP addresses to scan your attack surface, including port scans, webservice scans, and external TLS/SSL certificate checks. Allowing or blocking Tenable Attack Surface Management IP addresses can distort the perceived public attack surface, leading to inaccuracies.

- Example 1 (Allowed IPs): If you have private assets (not publicly visible) and you allow Tenable Attack Surface Management IPs, these assets may appear in Tenable Attack Surface Management as part of your attack surface, even though they are not truly public.
- Example 2 (Blocked IPs): If you have public assets, and you block Tenable Attack Surface Management IPs, these assets, which are legitimately part of your attack surface, may be overlooked and remain vulnerable to exploitation.

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 Vulnerability Management or Tenable Web App Scanning, see [Cloud Sensors](#) in the *Tenable Vulnerability Management User Guide*.

Sensor Group	Region	IPv4 Range	IPv6 Range
US Cloud Scanner, US West Cloud Scanners	us-west-1	3.101.216.64/26 3.101.226.128/26 3.101.230.128/25	2600:1f1c:ba0:dd00::/56
US Cloud Scanner, US East Cloud Scanners	us-east-1	44.210.119.64/27	2600:1f10:48bb:e200::/56
tenable.asm	static	209.126.151.116 209.126.151.117 209.126.151.118	2605:a140:2061:705::1 2605:a140:2061:5217::1 2605:a140:2061:5219::1 2605:a140:2061:5220::1



Sensor Group	Region	IPv4 Range	IPv6 Range
		209.126.151.119	2605:a140:2061:5221::1
		209.126.151.120	2605:a140:2061:5226::1
		209.126.151.121	2605:a140:2061:5228::1
		209.126.151.122	2605:a140:2061:5230::1
		209.126.151.123	2605:a140:2061:5232::1
		209.126.151.124	2605:a140:2060:8106::1
		209.126.151.125	2605:a140:2061:164::1
		207.244.234.126	2605:a140:2061:5215::1
		207.244.251.14	2605:a140:2061:5234::1
		207.244.251.16	2605:a140:2061:5233::1
		209.126.86.45	2605:a140:2060:8101::1
		209.126.86.46	2605:a140:2060:8123::1
		209.126.87.66	2605:a140:2092:2549::1
		209.126.87.68	2a02:c207:2052:4804::1
		209.126.87.70	2605:a140:2092:2546::1
		209.126.87.72	2605:a140:2092:2547::1
		209.145.58.124	2605:a140:2092:2548::1
		207.244.249.143	2605:a140:2092:2546::1
		207.244.251.12	2605:a140:2092:2547::1
		209.126.87.112	2605:a140:2092:2548::1
		209.126.87.73	2605:a140:2092:2549::1
		209.145.53.57	2a02:c207:2052:4804::1
		209.145.59.230	
		154.53.40.98	
		164.68.102.233	
		207.244.235.11	
		207.244.236.30	
		209.126.151.114	
		209.126.151.115	
		66.94.119.243	
		207.244.235.11	
		207.244.236.30	
		66.94.119.243	



Sensor Group	Region	IPv4 Range	IPv6 Range
		154.53.40.98 164.68.102.233	

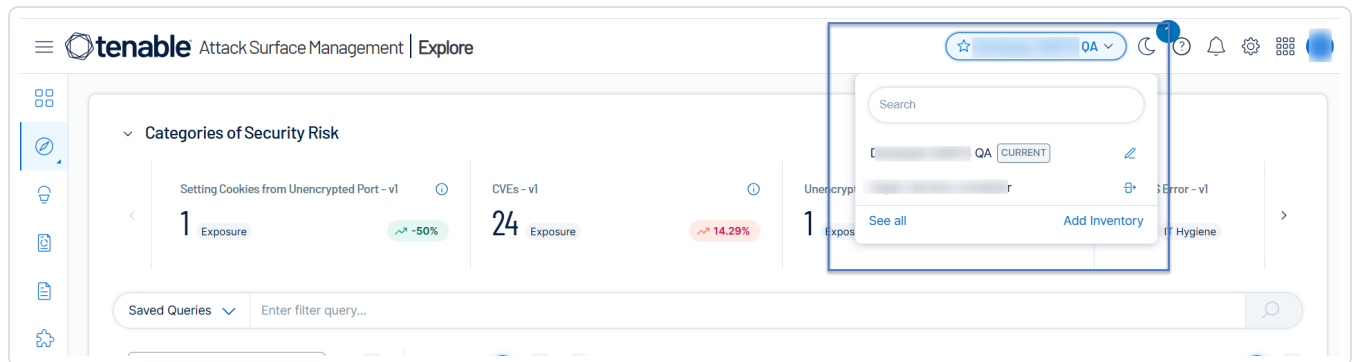


Inventory

In Tenable Attack Surface Management, an inventory is where you view your organization's assets.

To view an existing inventory:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select the inventory you want to view.

Your inventory appears.

Related topics:

[Create an Inventory](#)

[Inventory Settings](#)

[Inventory Columns](#)

[Asset Prioritization](#)

[Leave an Inventory](#)

[Manage Inventory Sources](#)

[Add Sources](#)

[Add a Subdomain](#)

[Move a Domain](#)

[Update a Source Screenshot](#)



[Remove a Source](#)

[Exclusion Rules](#)

[Create an Exclusion Rule](#)

[Run Exclusion Rules](#)

[Delete an Exclusion Rule](#)

[Automation Rules](#)

[Create an Automation Rule](#)

[Automation Rule Settings](#)

[Modify an Automation Rule](#)

[Delete an Automation Rule](#)

[Asset Details](#)

[View Asset Attribution](#)

[Export an Asset](#)

[Manage Asset Tags](#)

[Move or Copy Assets to another Inventory](#)

[Archive an Asset](#)

Create an Inventory

In Tenable Attack Surface Management, you can create an inventory to identify and organize your assets.

To create an inventory and add a domain:

1. In Tenable Attack Surface Management, in the upper-right corner, click the current inventory.

The Inventory drop-down list appears.

Note: Click **See All** to view all your inventories.



2. In the drop-down list, click **Add Inventory**.

The **Create new inventory** window appears.

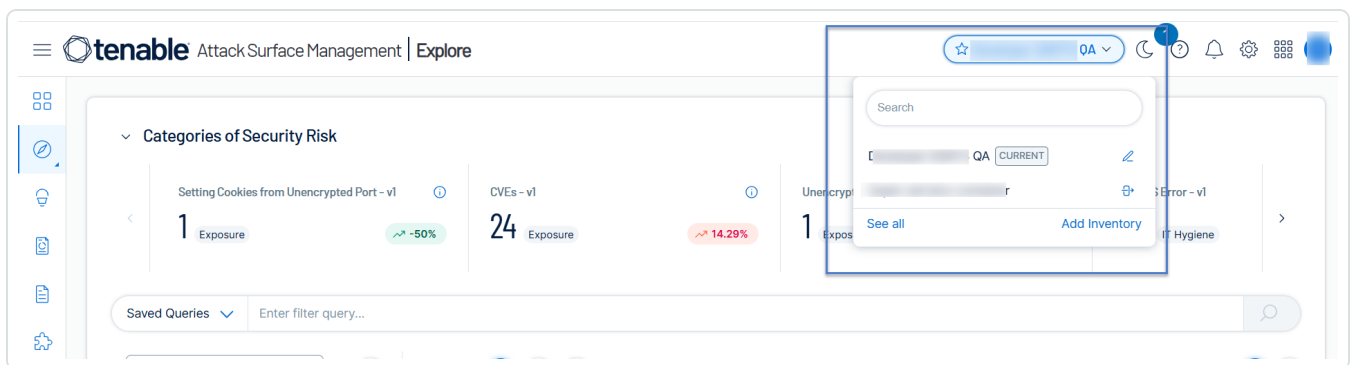
3. In the **New Inventory Name** box, type a name for the inventory.
4. (Optional) In the **Inherit Inventory** box, select an inventory you want to use as a template for the new inventory.

The new inventory inherits the selected inventory's tags, custom columns, subscriptions, and exclusion rules.

5. Click **Save**.

The inventory is created.

6. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

7. In the drop-down list, click the inventory you just created.

The **Set up your Inventory** page appears, prompting you to add a domain to your inventory.

8. In the text box, type your organization's domain.

Note: To add multiple domain names, separate the domain names using space.

9. Click the **+ Add Domain Name** button.

The inventory appears, with the domain added.


10. (Optional) [Add additional sources to your inventory](#).



Inventory Settings




On the Inventory page, you can add or remove columns to the inventory table and also render the assets and sources in your inventory to different formats.

To manage your inventory settings:



1. In Tenable Attack Surface Management, in the left navigation bar, click  **Explore**.

The **Explore** page appears. The main panel of the page is the Assets table. You can perform the following operations on the assets table.

2. Select the required option.

Option	Description
Group By	<ul style="list-style-type: none">• Click the  button to group the assets by hostnames.• Click the  button to group the assets by their IP addresses.• Click the  button to remove the grouping.
Manage Columns	<p>Allows you to add and remove columns from the assets table.</p> <p>To add or remove columns:</p> <ol style="list-style-type: none">1. In the Explore page, in the header of the assets table, click the Columns drop-down list. <p>The Customize Columns window appears.</p> <ol style="list-style-type: none">2. Do the following: <ul style="list-style-type: none">• To add columns, select the checkboxes next to the column names you want to add.• To remove columns, clear the checkboxes next to the column names you want to remove. <ol style="list-style-type: none">3. Click outside the box to close the window. <p>Tenable Attack Surface Management updates the table with the</p>



	selections.
Render Assets as Dashboard	<p>Renders the assets table in the dashboard format.</p> <p>In the assets table, click the View as  button to display each column in the chart format.</p> <div><p>Note: The following columns are not supported for Render Assets as Dashboard:</p><ul style="list-style-type: none">• Asset ID• Screenshot• Added to Inventory• Record Value• Host• IP• Added to this Subscription• HTML• Domain• Canonical URL• SSL / TLS Subject Alt Name• Response Header Value• Response Security Header Value• Banners• Final URL• SSL / TLS Valid From• SSI / TLS Expiration</div> <p>To change the format back to table, click View as  . If you do not change to the table format, Tenable Attack Surface Management shows the dashboard view the next time you log in.</p>
Export All	To export all assets:



	<ol style="list-style-type: none">1. In the assets table, click Export All. The Export window appears.2. Select the format: CSV, XLSX, or JSON.3. Search for and select the columns to export. <div>Note: Use the View selected option to view the selected columns.</div>4. Click Export. Tenable Attack Surface Management exports the assets with the selected columns.
Add Tags Remove Tags	Allows you to tag assets. For more information, see Manage Asset Tags .

Inventory Columns

In Tenable Attack Surface Management, an inventory is where you view your organization's assets. You can view the inventory details in a table format. Add or remove columns to the inventory table to get specific details of an asset in your inventory.

To configure the columns for the inventory table:

1. On the **Explore** page, use the **Columns** drop-down list to **Customize Columns**. See [Explore](#).

The following table shows the available columns that you can choose and their descriptions.

Column Name	Description
Security	
SSL/TLS Expiration	Date until the SSL certificate of the asset is valid.
SSL/TLS Fingerprint	SSL fingerprint of the asset.
SSL/TLS EV	States whether the asset has an Extended Validation (EV)



Certificate	certificate.
SSL/TLS Issuer Country	SSL certificate issuer country.
SSL/TLS Issuer Organization	SSL certificate issuer organization.
SSL/TLS Valid From	The date from which the SSL certificate of the asset is valid.
SSL/TLS Subject Alt Name	SSL subject alternate names of the asset.
SSL/TLS Cypher Suites	Cypher suites available on the asset.
SSL/TLS Key Length	Peer certificate RSA bit size.
SSL/TLS Protocol	SSL protocols used by the asset.
SSL/TLS error	SSL errors produced by the asset.
SSL/TLS Serial Number	SSL serial number of the asset.
Captchas	CAPTCHA software used by the asset.
Cookie Compliance	Cookie compliance used by the asset.
Secret Keys	Secret keys used by the asset. Tenable Attack Surface Management collects this data by executing multiple regular expressions against the rendered HTML of the site.
Login	Whether the asset redirects to or contains a login page.
JARM Hash	A hash that can be used to group assets having similar SSL configurations.



Bug Bounty URL	Bug bounty programs that the asset is part of.
HTTP Response	
Content type	The type of content served by the asset.
Content language	The language of content served by the asset.
Vary	The value of the Vary HTTP header set by the asset.
Response Header Value	HTTP header values returned by the asset.
Response Security Header Value	HTTP security header values returned by the asset.
Sets Cookies	States whether the asset sets cookies or not.
Content Length	The length of the content served by the asset in bytes.
Canonical URL	Canonical URL found in the HTML body returned by the asset.
Response code	The response code returned from the final URL the asset redirects to.
HTML	Raw response body returned by the asset.
Document Title	HTML document title.
Networking	
Host	Hostname of the asset.
Record Type	DNS record type of asset.
Record Value	DNS record value of the asset.
Redirect Chain	The chain of HTTP or client-side redirects that navigated the system to <code>screenshot.finalurl</code> .
IP	IP address of the asset.
Is subdomain	Indicates whether the hostname of the asset is a subdomain or



	not.
Final response code	The response code returned from the final URL the asset redirects to.
ASN	The Autonomous System organization of the asset.
ASN Number	The Autonomous System Number (ASN) of the asset.
Final url	The final URL the asset redirects to.
Domain	Domain name of asset.
Hosting Provider	Cloud provider of the asset.
Cloud Hosted	Whether the Asset is cloud-hosted or not.
Network Devices	Network devices used by the asset.
Mixed Content	Mixed content returned by the asset.
Network Storage	Network storage software used by the asset.
CDN	CDNs used by the asset.
Remote Access	Remote access software used by the asset.
Containers	Container software used by the asset.
SaaS	SaaS solutions used by the asset.
PaaS	PaaS solutions used by the asset.
IaaS	IaaS solutions used by the asset.
Load Balancer	Load Balancers used by the asset.
Reverse Proxy	Reverse proxies used by the asset.
Nameservers	DNS nameservers of the asset based on WHOIS data.
Programming	
Mobile	Mobile frameworks used by the asset.



Frameworks	
Programming Languages	Programming languages used by the asset.
Web Frameworks	Web frameworks used by the asset.
Dev Tools	Development tools used by the asset.
JavaScript Libraries	JavaScript libraries used by the asset.
JavaScript Frameworks	JavaScript frameworks used by the asset.
Landing Page Builders	Landing page builders used by the asset.
Documentation Tools	Documentation tools used by the asset.
Geolocation	
Continent	Location of the asset.
Country	Location of the asset.
City	Location of the asset.
Latitude	Location of the asset.
Longitude	Location of the asset.
Timezone	Location of the asset.
Postal	Postal code of the asset.
In EU	Whether the asset is located in the EU or not.
Subdivisions	Location of the asset.
Registered Country	Country where the asset was registered.



Maps	Maps software used by the asset.
Services	
Ports	Ports open on the asset.
Services	Service running on the asset.
Banners	Banners returned by services running on the asset.
CPE	Services running on the asset in Common Platform Enumeration (CPE) format.
CVE	IDs of CVEs that apply to the asset.
CVSSv3 Scores	Unique CVSS3 scores that apply to the asset.
CVSSv3 Vectors	Unique CVSS3 vector strings that apply to the asset.
Server	Web server running on the asset based on HTTP response headers.
RBL	Realtime Blackhole Lists (RBL) that contain the asset.
Web Servers	Web servers running on the asset.
Email service	Emails used by the asset.
Web applications	
Browser fingerprinting	Browser fingerprinting tools.
Buy now pay later	Buy now pay later tools.
Cart abandonment	Cart abandonment tools.
Content curation	Content curation tools.
Customer data platform	Customer data platform tools.
Digital asset	Digital asset management tools.



management	
Geolocation	Geolocation tools.
Hosting	Hosting information.
Loyalty & rewards	Loyalty and rewards tools.
Performance	Performance tools.
Referral marketing	Referral marketing tools.
Reservations & delivery	Reservations and delivery platforms.
Reviews	
RUM	Real User Monitoring (RUM) tools.
Segmentation	Segmentation tools.
Shipping carriers	Shipping carrier tools.
Translation	Translation tools.
Wordpress plugins	WordPress plugin tools.
Wordpress themes	WordPress theme tools.
Recruitment & staffing	Recruitment and staffing tools.
Returns	Returns technologies.
Livestreaming	Livestreaming tools.
Ticket booking	Ticket booking tools.
Augmented reality	Augmented reality tools.
Cross border ecommerce	Cross-border ecommerce tools.



Message Boards	Message boards used by the asset.
CMS	Content Management Systems (CMS) used by the asset.
Database Managers	Database managers used by the asset.
Wikis	Wiki software used by the asset.
Hosting Panels	Hosting panels used by the asset.
Wordpress Vulnerability IDs	WPScan Vulnerability Database IDs.
Blogs	Bloggng software used by the asset.
Wordpress Core Version	WordPress Core version.
WordPress Scanned Plugins	The WordPress scanned plugins that run on the asset.
Editors	Editor software used by the asset.
Search Engines	Search engines used by the asset.
Web Mail	Web mail used by the asset.
Cryptominer	Cryptomining software used by the asset.
Static Site Generator	Static site generators used by the asset.
User Onboarding	User onboarding software used by the asset.
Document Management Systems	Document management systems used by the asset.
Control Systems	Control systems used by the asset.
Issue Trackers	Control systems used by the asset.



Accessibility	Accessibility libraries used by the asset.
Appointment scheduling	Appointment scheduling libraries used by the asset.
LMS	Learning management systems used by the asset.
Tag Managers	Tag managers used by the asset.
Data	
Analytics	Analytics software used by the asset.
Databases	Databases used by the asset.
Social	
Social Profiles	Social profiles used by the asset.
Live Chat	Live chat software used by the asset.
Comment Systems	Comment systems used by the asset.
Social logins	Social logins used by the asset.
Media	
Photo Galleries	Photo galleries used by the asset.
Media Servers	Media servers used by the asset.
Webcams	Webcam software used by the asset.
Printers	Printer libraries used by the asset.
Font Scripts	Font scripts used by the Asset.
Video Players	Video players used by the asset.
Rich Text Editors	Rich text editors used by the asset.
JavaScript Graphics	JavaScript graphics used by the asset.



Finance	
Shopify apps	Shopify app tools.
Ecommerce	Cross-border ecommerce tools.
Payment Processors	Payment processors used by the asset.
Paywalls	Paywalls used by the asset.
Accounting	Accounting systems used by the asset.
Affiliate programs	Affiliate programs used by the asset.
Marketing	
Google Analytics Keys	Referral marketing tools.
Google Adsense Keys	Google AdSense keys used by the asset.
Advertising Networks	Advertising networks used by the asset.
Marketing Automation	Referral marketing tools.
CRM	Customer relationship management systems used by the asset.
SEO	Search engine optimization software used by the asset.
General	
Widgets	Javascript widgets used by the asset.
Cache Tools	Cache tools used by the asset.
Operating Systems	Operating systems used by the asset.
Web Server Extensions	Web server extensions used by the asset.



Feed Readers	Feed readers used by the asset.
Build CI Systems	Build Continuous Integration systems used by the asset.
Miscellaneous	Miscellaneous software used by the asset.
Tenable.asm	
Asset ID	The unique id of the asset.
Severity	The severity ranking of the asset based on its security risk.
Added to Inventory	Timestamp of date when the asset was added to the current inventory.
Tag	IDs of simple Tags associated with the asset. Corresponds with the Tag column on the user interface.
WHOIS	
Administrative contact email	Administrative contact email of the asset.
Administrative contact name	Administrative contact name of the asset.
Administrative contact organization	Administrative contact organization of the asset.
Billing contact email	Billing contact email of the asset.
Contact email	Contact email of the asset.
Domain name expiration	Age out date of the asset.
Registrant city	Registrant city of the asset.
Registrant country	Registrant country of the asset.



Registrant email	Registrant email of the asset.
Registrant fax	Registrant fax of the asset.
Registrant name	Registrant name of the asset.
Registrant postal code	Registrant postal code of the asset.
Registrant state	Registrant state of the asset.
Registrant street	Registrant street of the asset.

Asset Prioritization

Tenable Attack Surface Management ranks your assets and assigns a severity level to the assets based on their security risk. You can use the severity ranking to prioritize the assets that require immediate attention. The **Severity** column of the asset table shows the severity of an asset as **Low**, **Medium**, **High**, **Critical**, or **None**.

Tenable Attack Surface Management calculates the severity ranking for an asset by matching the asset information with a given set of criteria. Any change or update to the asset changes the severity level of that asset. For example, an asset with a **Critical** severity with a vulnerability issue moves to **Medium** or **Low** severity after you remediate the issue and rescan the asset.

Categories of Security Risk

Setting Cookies from Unencrypted Port - vl

1 Exposure

-50%

CVEs - vl

24 Exposure

14.29%

Unencrypted Final URL - vl

1 Exposure

SSL/TLS Error - vl

164 IT Hygiene

Saved Queries

Enter filter query...

Sort by Asset Count - High to Low

Search...

All Sources

697

380

11

Group By

1,036 Assets

Export All

Columns 1 to 50 of 1,036

Page 1 of 21

Host	Severity	Record Type	IP Address	ASN	Register...	Ports	Screenshot	Tags
	None	CNAME				80, 443, ...	-	tag with
	None	AAAA				80, 443, ...	-	-
	Low	A				53, 80, 4...		-
	None	UNK				443	-	-
	Low	CNAME				80, 443, ...	-	-
	None	A				80, 443, ...	-	-



Tip: To view the factors on which the asset prioritization score is based on, click the asset name to open the asset page. The asset prioritization details are available at the top of the asset details page.

Record Value: .1

Data Sources

Severity
Low

Integration Status
— Host Asset
— Web App Asset

Key Properties
Licensed No
Source Attack Surface Management

Summary HTML Timeline History Integration Status Location Ports Findings

Severity Breakdown

Authentication Asset responds with HTTP status 401 or 403.

Authentication after redirects Asset responds with HTTP status 401 or 403 at the end of the redirect chain.

RFC 1918 and other popular addresses Asset points to a common or private IP address.

Tags +

No Tags Assigned

Enable the Severity Column

You must enable the **Severity** option in Tenable Attack Surface Management for the column to appear in the assets table.

To enable the **Severity** column for your assets:

1. On the **Explore** page, in the assets table header, click **Columns**.

The **Customize Columns** drop-down list appears.

2. Select the **Severity** checkbox.

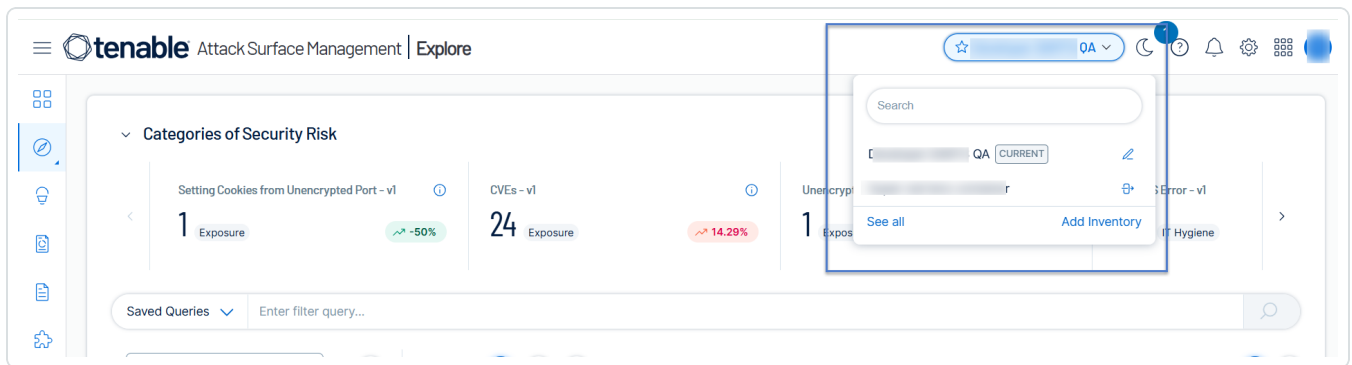
Tenable Attack Surface Management includes the **Severity** column in the assets table.

Leave an Inventory

When you leave an inventory in Tenable Attack Surface Management, other members of the organization can still access the inventory. If you leave an inventory that you own, then ownership will be passed to the next oldest member in the inventory.

To leave an inventory:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.




Tenable Attack Surface Management displays the inventories in the drop-down list.

2. Click **See all**.

The **Your Inventories** page appears.



3. Hover over the inventory that you want to leave.
4. Click the  button.

A dialog box appears, confirming your selection to leave the inventory.

5. Click **Leave**.

Tenable Attack Surface Management removes the inventory from your list of inventories.

Manage Inventory Sources

Add Sources

In Tenable Attack Surface Management, you can add a source to your inventory to identify more assets associated with your organization.



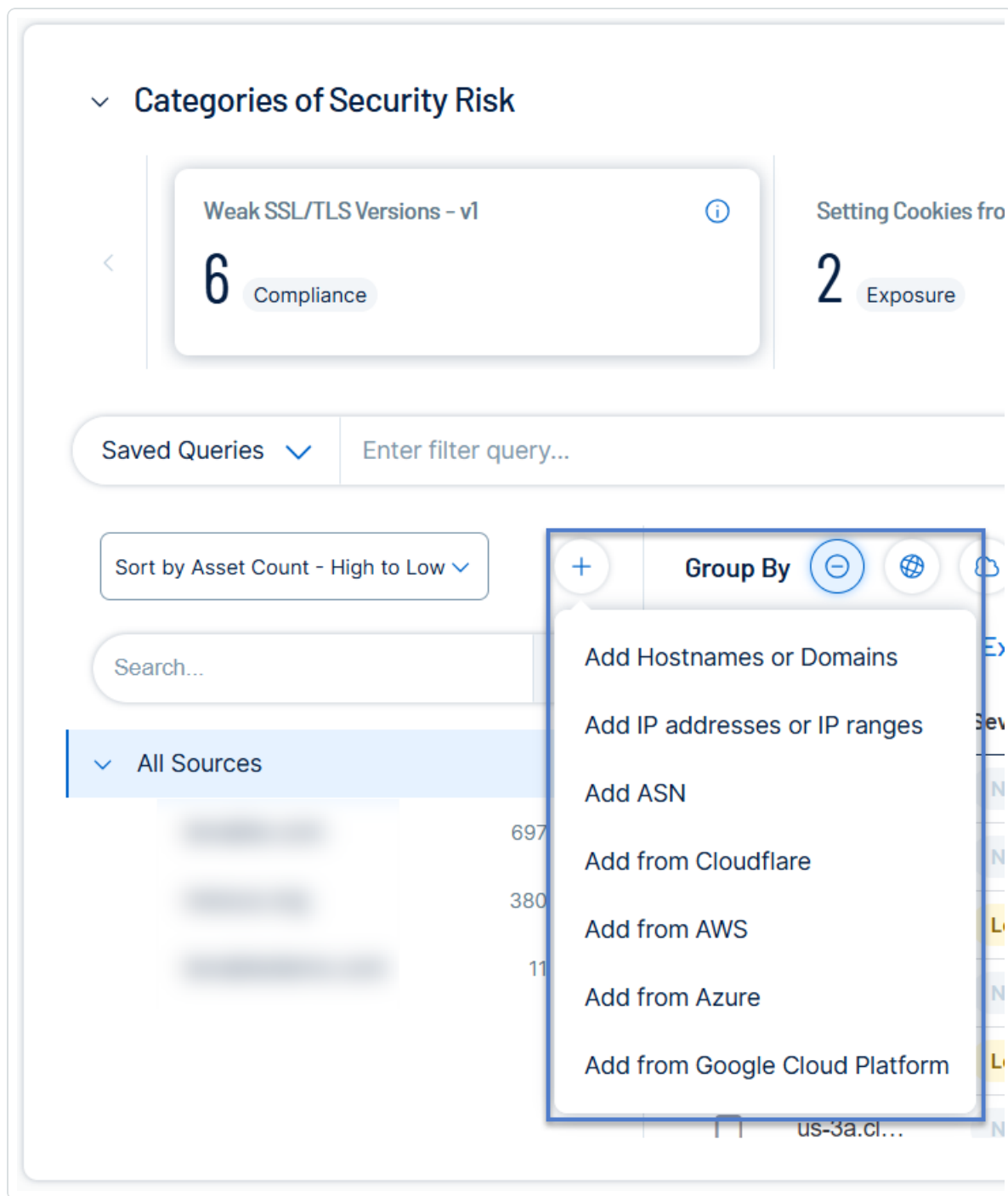
See the following procedures for how to add different types of sources.

- [Add a hostname, domain, or subdomain](#)
- [Add an IP address or IP range](#)
- [Add an Autonomous System Number \(ASN\)](#)
- [Add sources from Cloudflare](#)
- [Add sources from AWS](#)
- [Add sources from Azure](#)
- [Add sources from Google Cloud Platform](#)

Add a hostname, domain, or subdomain



1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In the drop-down list, click **Add Hostname or Domain**.

The **Enter Hostname** window appears.



3. In the **Enter a host to your Inventory** box, type a hostname or domain.

A list of options appears.

Note: You can add a maximum of two domains across your organization. If you already have two domains system-wide, you must delete one before you can add another.

4. Select any applicable options:

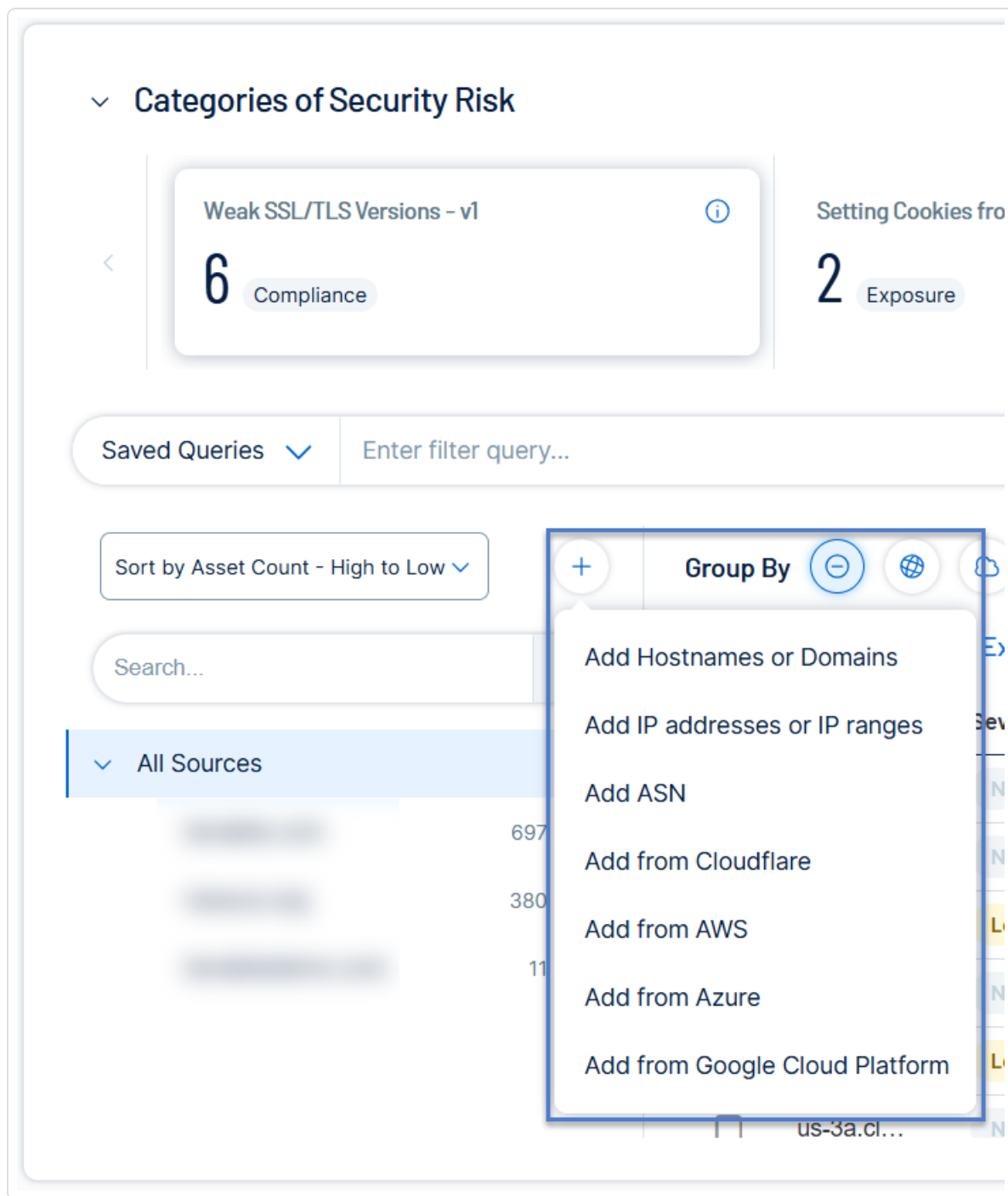
Option	Description
<i>Add subdomains instead of domains</i>	Adds the domain as a subdomain instead of a host or domain.
<i>Don't do subdomain discovery</i>	Prevents Tenable Attack Surface Management from automatically discovering subdomains for the domain.
<i>Elastic source</i>	During asset detection, Tenable Attack Surface Management records both FQDN and IP address of the asset. When you enable the Elastic source option, Tenable Attack Surface Management records only the asset's FQDN. This prevents duplicate asset findings for an asset with frequently changing IP address, such as one hosted by a Cloud service. When extracting data from an asset in an Elastic Source, Tenable Attack Surface Management resolves the FQDN to an IP address right before each scan.

5. Click **Next**.

The hostname, domain, or subdomain appears in your inventory and begins identifying assets.

Add an IP address or IP range

1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In the drop-down list, click **Add IP addresses or IP ranges**.

The **Enter IP address** window appears.

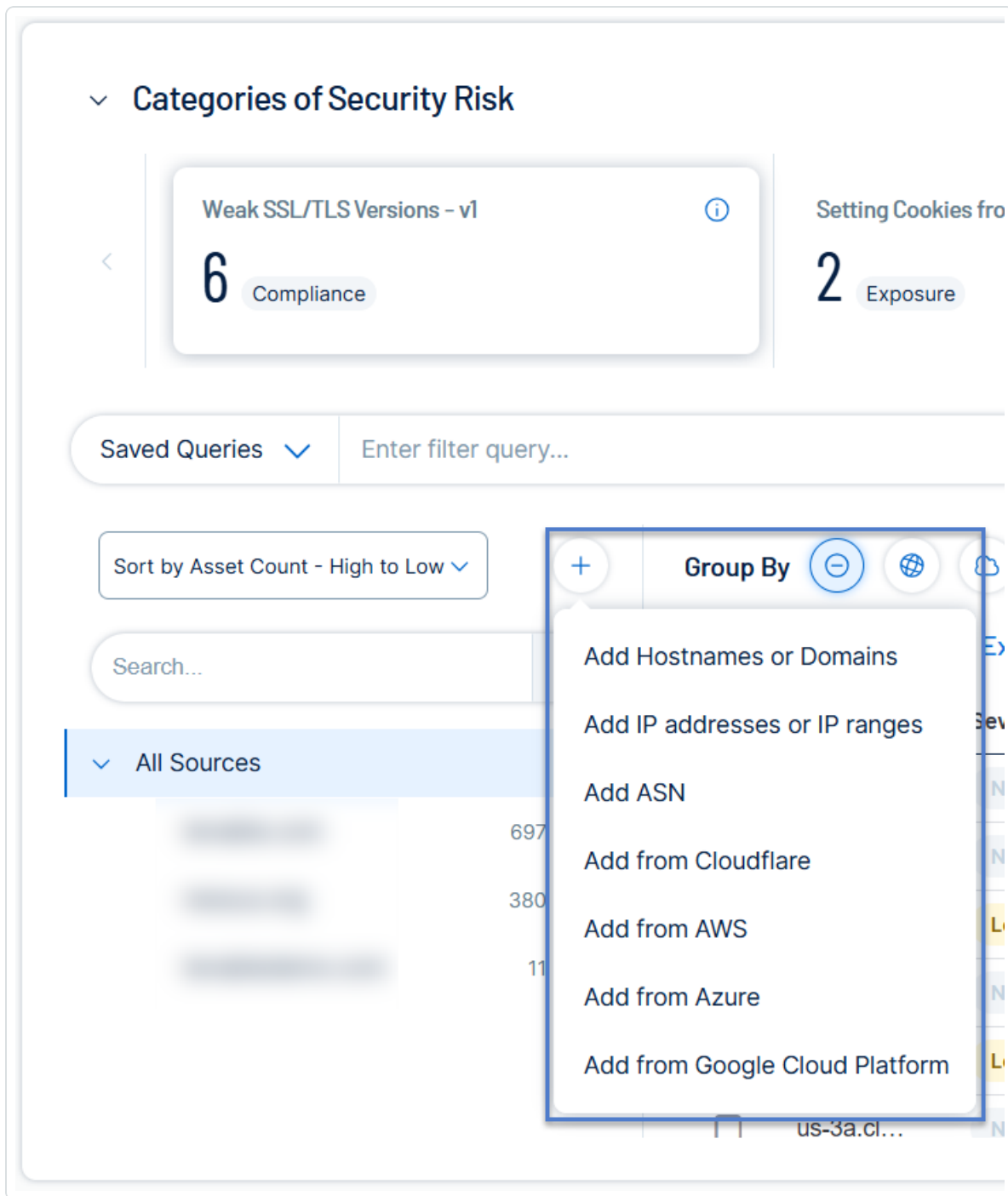


3. In the **Enter an IP range to your Inventory** box, type an IP address, IP range, or a comma-separated list of IP addresses.
4. To select assets, do one of the following:
 - Click **Add IP address** if you want Tenable Attack Surface Management to identify all assets associated with the IP address.
 - Click **Select Assets Manually**. The **Select IP Addresses** window appears: select the IP addresses to add to your inventory, and click **Add to Inventory** to add the assets.

Tenable Attack Surface Management adds the IP addresses to your inventory and begins to identify assets.

Add an Autonomous System Number (ASN)

1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In the drop-down list, click **Add ASN**.

The **Enter ASN** window appears.



3. In the **Enter AS number or organization name** box, type an ASN or search for an organization.
4. Click the **Add ASN** button.

Tenable Attack Surface Management adds the ASN to your inventory and begins to identify assets.

Add sources from Cloudflare

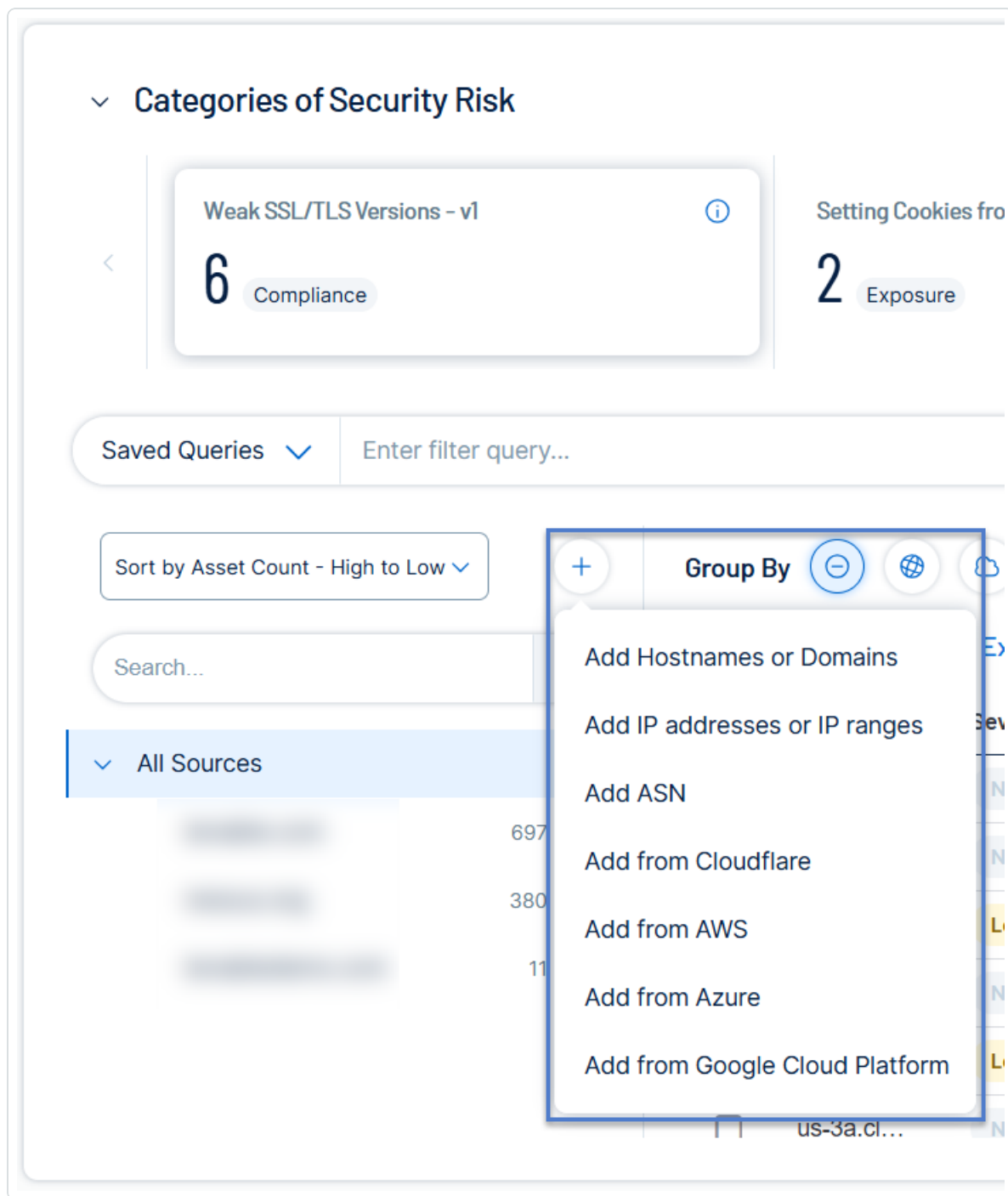
Before you begin

Tenable Attack Surface Management requires the following permissions to add Cloudflare sources:

- **Zone Read** — Grants read access to zone management.
- **DNS Read** — Grants read access to DNS.

To add sources from Cloudflare:

1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In the drop-down list, click **Add from Cloudflare**.

The **Cloudflare keys** window appears with the list of configured API keys.



3. Do one of the following:

- Click an API key to view the list of available zones or domains the API key has access.
- (Optional) If you do not have any configured API keys, add a new API key:

a. Click **Add**.

Tenable Attack Surface Management displays the **Add Cloudflare key** box.

b. In the **Cloudflare account name** box, type a name for the Cloudflare account.

c. In the **API key** box, copy and paste the API key for your Cloudflare account.

d. Click **Add**.

Tenable Attack Surface Management adds the API key and displays the **Available zones** window with the list of Cloudflare zones (domain names) where the API key has access.

Note: Tenable Attack Surface Management supports these types of DNS records: A, AAAA, CNAME, MX, NS, TXT, PTR, and SOA.

4. To add a domain to your inventory, click the **Add to inventory** link next to the domain name to add.

Note: To add all zones to your inventory, click **Add all**.

Tenable Attack Surface Management adds the Cloudflare assets to your inventory and redirects you to the Inventory page showing the newly added sources. The source from Cloudflare has an orange cloud icon under its name.

If there are assets from outside the zone or domain, Tenable Attack Surface Management automatically adds them as elastic assets. Tenable Attack Surface Management extracts data from these elastic assets using the hostname rather than their IP addresses. The **IP** column in the Inventory table shows *Elastic Asset* instead of an IP address for these elastic assets.

To delete a Cloudflare API key:



1. In the **Cloudflare keys** window, click  next to the Cloudflare API key to delete.

Tenable Attack Surface Management deletes the Cloudflare API key. The sources added using this key still show up in the inventory but Tenable Attack Surface Management eventually deletes them across all inventories.

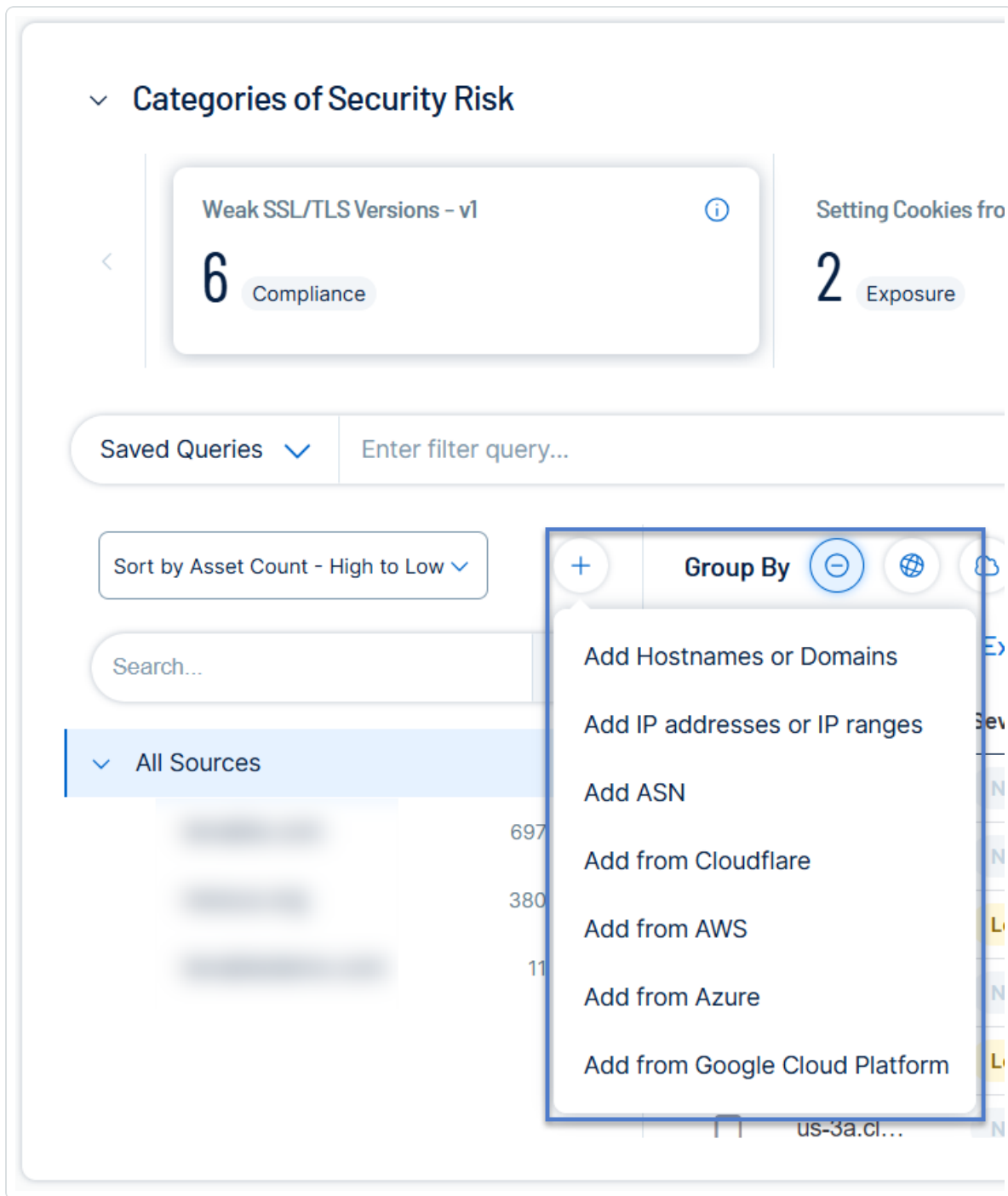
Add sources from AWS

Before you begin

- Make sure that you grant read-only permission for Tenable Attack Surface Management in your AWS account. For more information, see [ReadOnlyAccess](#) in the AWS documentation.
- Add your AWS account to Tenable Attack Surface Management. See [Integrate with AWS](#).

To add sources from AWS:

1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In the drop-down list, click **Add from AWS**.

The **AWS keys** window appears with the list of configured AWS API keys.



3. To add sources from your AWS account, click **Add as a source**.

Tenable Attack Surface Management adds the sources from AWS.

Note: Depending on the number of assets, the process may take some time to complete.

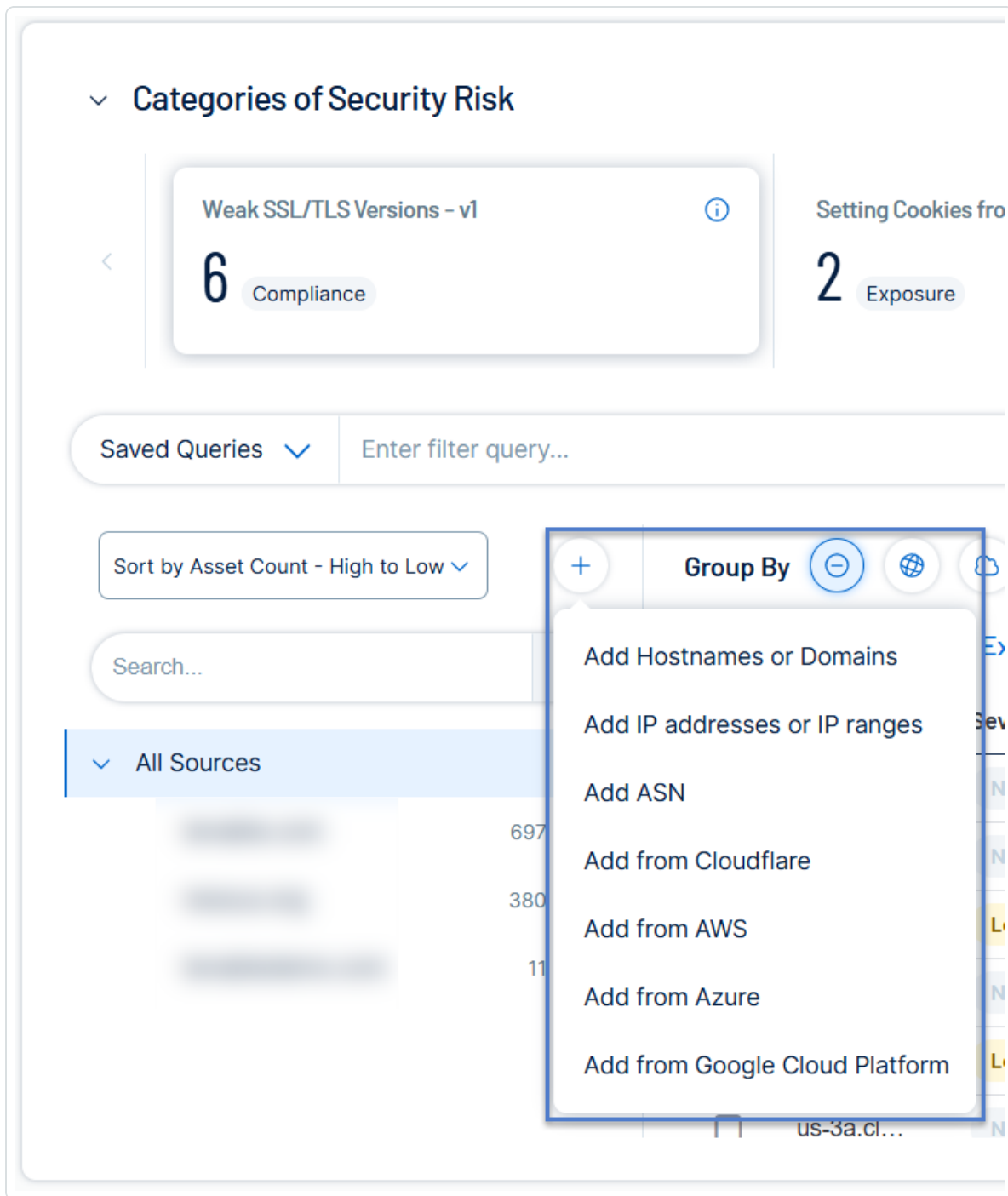
Add sources from Azure

Before you begin

- Make sure that you grant read-only permission (**Reader** role) for Tenable Attack Surface Management in your Azure account. For more information, see [Azure built-in roles for General](#) in the Azure documentation.
- Add your Azure account to Tenable Attack Surface Management. See [Integrate with Microsoft Azure](#).

To add sources from Azure:

1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In the drop-down list, click **Add from Azure**.

The **Azure keys** window appears with the list of configured Azure API keys.



3. To add sources from your Azure account, click **Add as a source**.

Tenable Attack Surface Management adds the sources from Azure.

Note: Depending on the number of assets, the process may take some time to complete.

Add sources from Google Cloud Platform

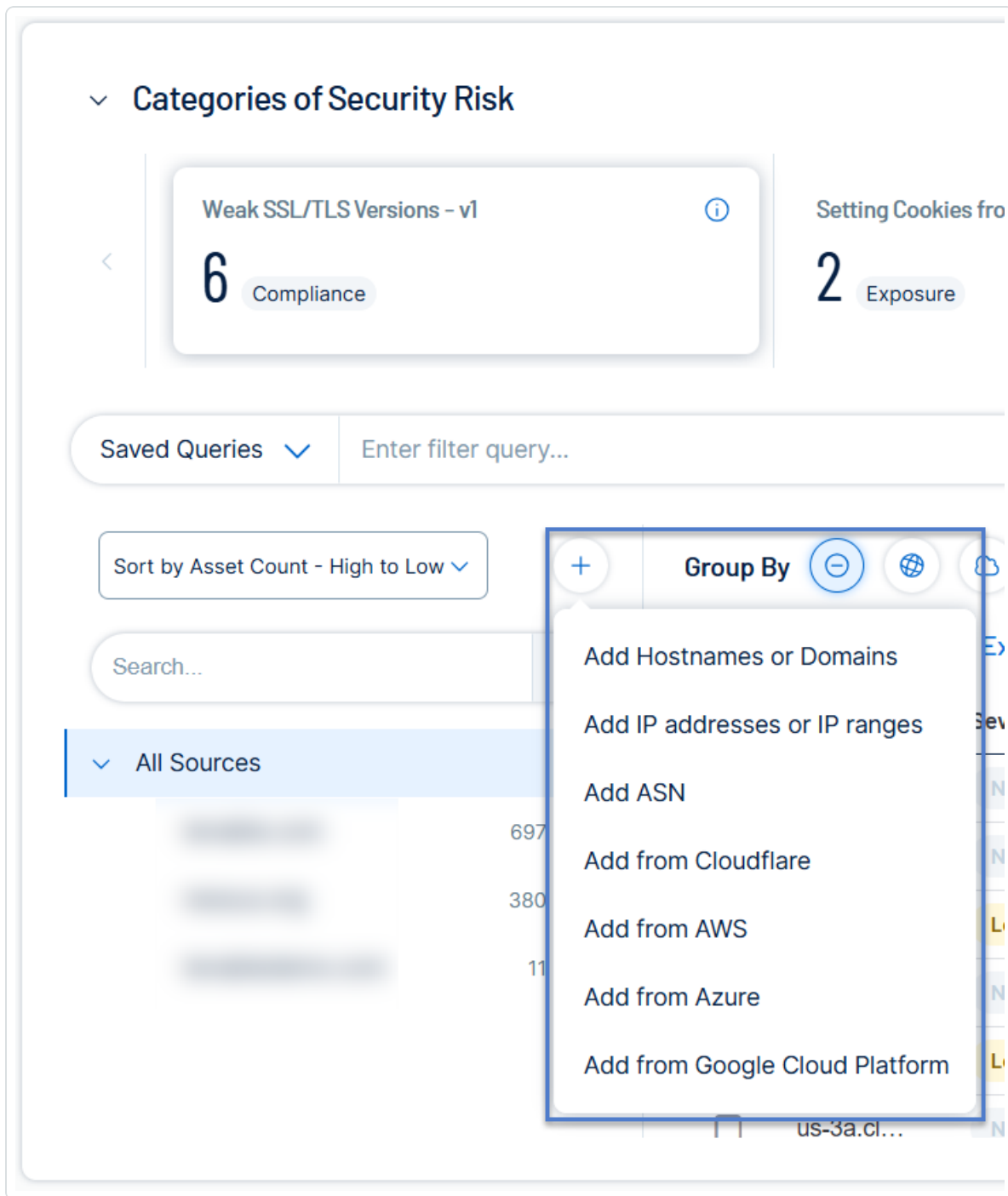
Before you Begin

- Make sure to have a service account with read only permissions. Tenable recommends you use Google's reader role for the service account. To check the service account permissions, click [here](#).
- Add your Google Cloud Platform account to Tenable Attack Surface Management. See [Integrate with Google Cloud Platform](#).

To add sources from Google Cloud Platform:



1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In the drop-down list, click **Add from Google Cloud Platform**.



The **Google Cloud Platform keys** window appears with the list of configured Google Cloud Platform API keys.

3. To add sources from your Google Cloud Platform account, click **Add as a source**.

Tenable Attack Surface Management adds the sources from Google Cloud Platform.

Note: Depending on the number of assets, the process may take some time to complete.

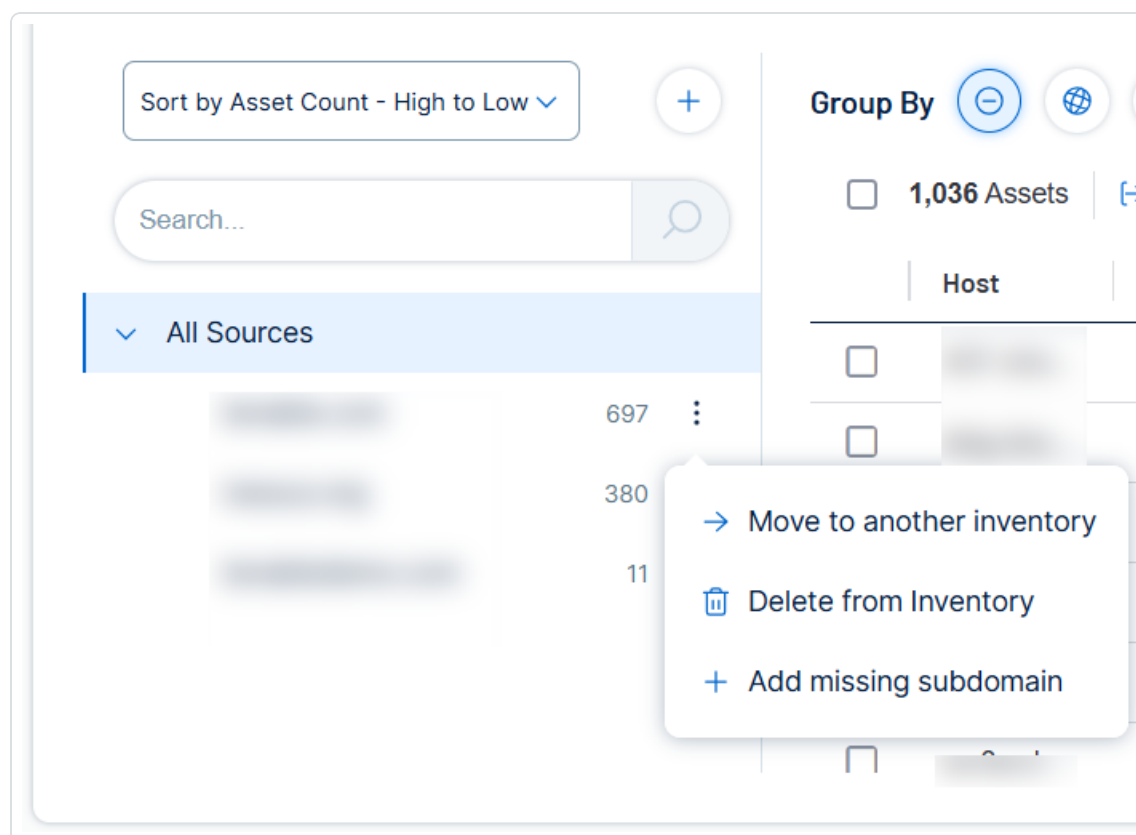
Add a Subdomain

In Tenable Attack Surface Management, you can add a subdomain to an existing domain in your inventory.

To add a subdomain to a domain in your inventory:

1. On the **Explore** page, in the **All Sources** pane, next to the source, click the  button.

A menu appears.



2. In the drop-down list, click **Add subdomain**.



The **Add missing subdomain** window appears.

3. In the text box, type a subdomain or comma-separated list of subdomains.
4. Click **Add subdomains**.

The subdomains are added to your inventory and Tenable Attack Surface Management automatically begins identifying assets in the subdomain.

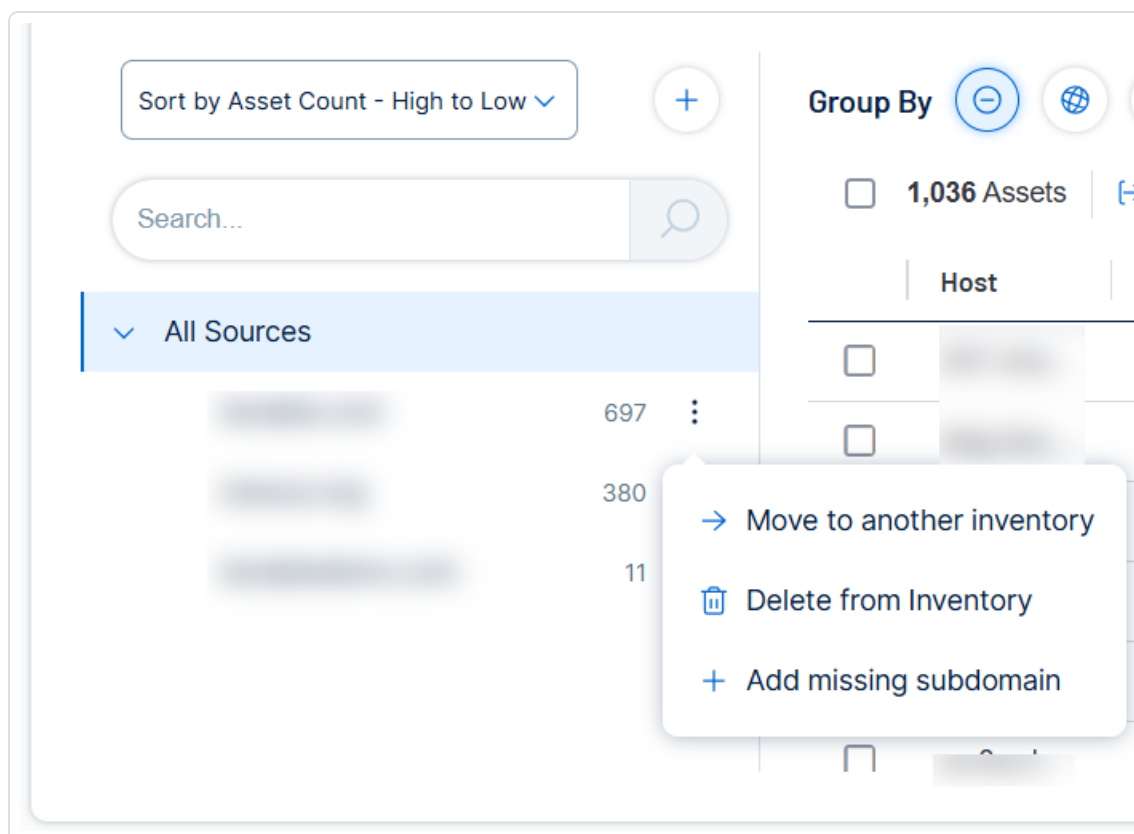
Move a Domain

In Tenable Attack Surface Management, you can move an existing domain to another inventory.

To move a domain to a different inventory:

1. On the **Explore** page, in the **All Sources** pane, next to the source, click the button.

A menu appears.



2. In the drop-down list, click **Move to another inventory**.

The **Move source to another inventory** window appears.



3. In the drop-down box, select the inventory to which you want to move the domain.
4. Click the **Move** button.

The domain is moved to the selected inventory and Tenable Attack Surface Management automatically begins populating the inventory with assets in the domain.

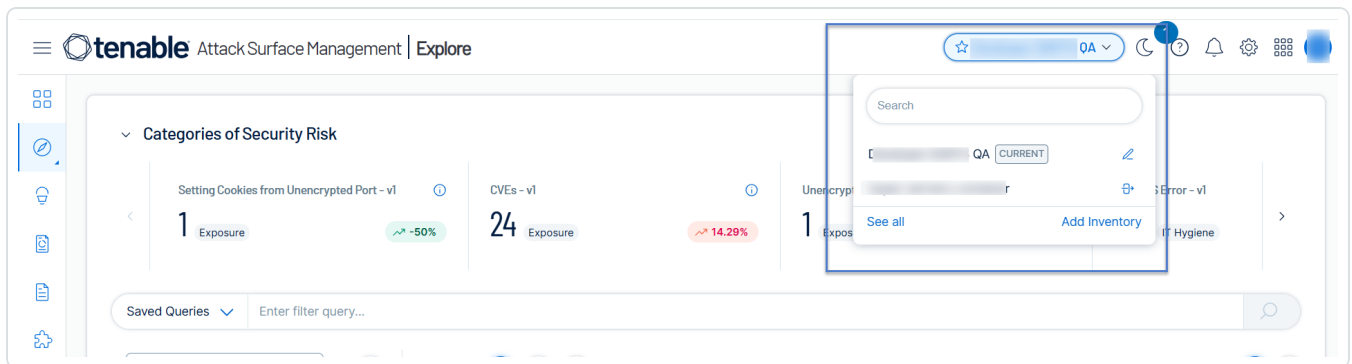
Update a Source Screenshot

In Tenable Attack Surface Management, you can update the screenshot for a source.

Note: You can update a screenshot only in the legacy interface.

To update the screenshot for a source:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select an inventory.
3. In the list of sources, hover over the source for which you want to update the screenshot.

Note: Not every type of source has an available screenshot.

4. Click the  button.
5. In the drop-down list, click **Refresh source screenshot**.

Tenable Attack Surface Management takes a new screenshot of the source.

Remove a Source

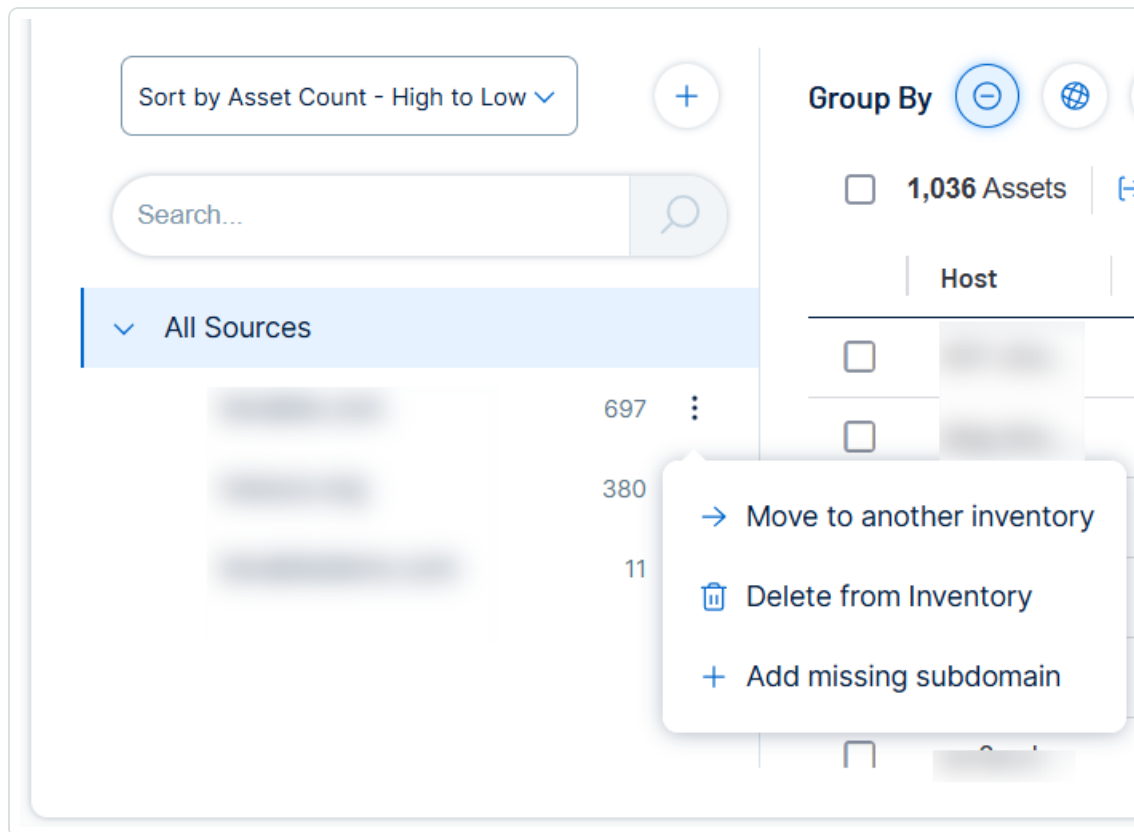


When you remove a source from an inventory, Tenable Attack Surface Management will remove all assets for the source.

To remove a source from an inventory:

1. On the **Explore** page, in the **All Sources** pane, next to the source, click the  button.

A menu appears.



2. In the drop-down list, click **Delete from Inventory**.

Tenable Attack Surface Management deletes the source from the inventory.

Exclusion Rules

In Tenable Attack Surface Management, exclusion rules specify specific assets to include or exclude from your inventory.

The following are the characteristics of exclusion rules:



- Exclusion rules do not support CIDR notation.
- Excluded assets cannot be added to the inventory.
- Excluded assets are archived when you manually add and run an exclusion rule.
- Newly discovered assets that are in the excluded list are not archived. They just do not appear in the inventory.

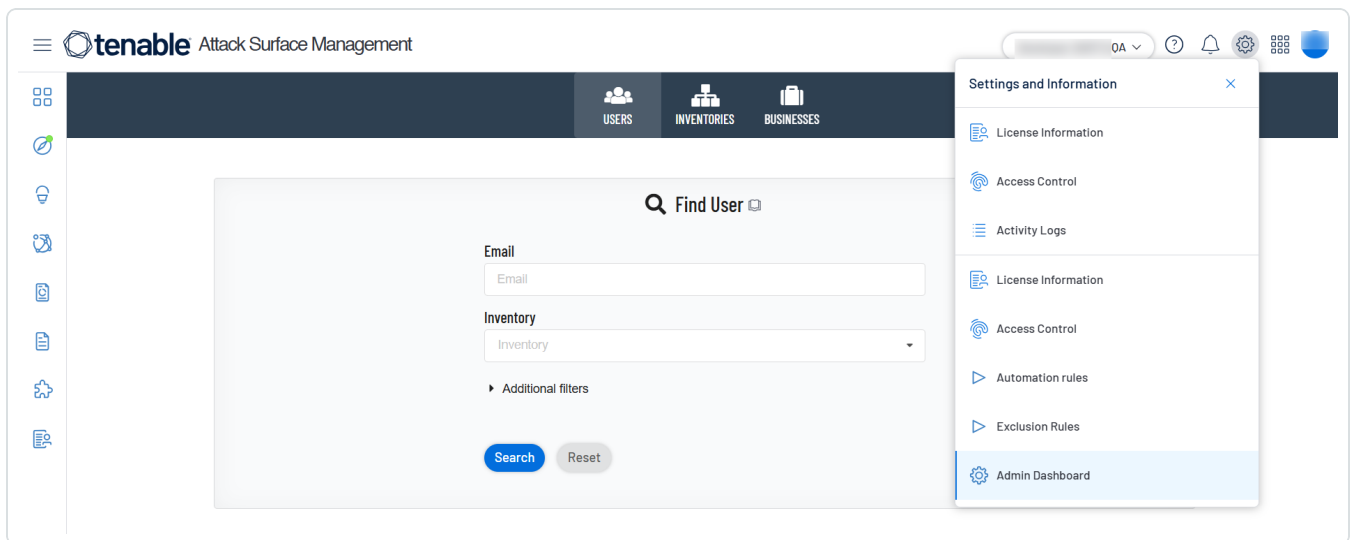
Create an Exclusion Rule

In Tenable Attack Surface Management, you can create an exclusion rule to include or exclude specific assets from your inventory.

To create an exclusion rule:

1. In Tenable Attack Surface Management, click the  icon in the upper-right corner.

The **Settings and Information** drop-down list appears.



2. In the drop-down list, click **Exclusion Rules**.

The **Exclusion Rules** window appears.

3. Click the **Add an exclusion rule** button.

The **Add exclusion rule** window appears.

4. In the first drop-down list, select the type of criteria you want to set for the exclusion rule:



- **Match IP addresses** - The exclusion rule will apply to assets that match specific IP addresses.
 - **Match hostnames** - The exclusion rule will apply to assets that match specific hostnames.
 - **Record type** - The exclusion rule will apply to specific asset types.
5. In the second drop-down list, select whether you want the exclusion rule to include or exclude matches:
 - **Exclude matches** - Tenable Attack Surface Management will exclude any assets that match the exclusion rule criteria.
 - **Include matches** - Tenable Attack Surface Management will include any assets that match the exclusion rule criteria.
 6. In the first text box, type the IP address, hostname, or record type to which you want to apply the exclusion rule.
 7. (Optional) In the second text box, type any relevant notes about the exclusion rule.
 8. Click **Save**.

Tenable Attack Surface Management saves the exclusion rule and it appears on the **Exclusion rules** window. The exclusion rules include a green + sign for rules to include assets and a red - sign for rules to exclude assets that match the criteria.



Exclusion rules

Developer DARTS QA

Exclusion rules proactively stop any assets that meet the set criteria from being added to this inventory. The most common use case is a service provider who hosts their customer's assets such as *.cust.company.com and they do not want to see said assets since they are unmanaged. Exclusion rules are hierarchical, cumulative and work in order from first to last.

⋮ + A

⋮ - PTR

⋮ + NS

Test the rules ▶

Run rules now

Add an exclusion rule

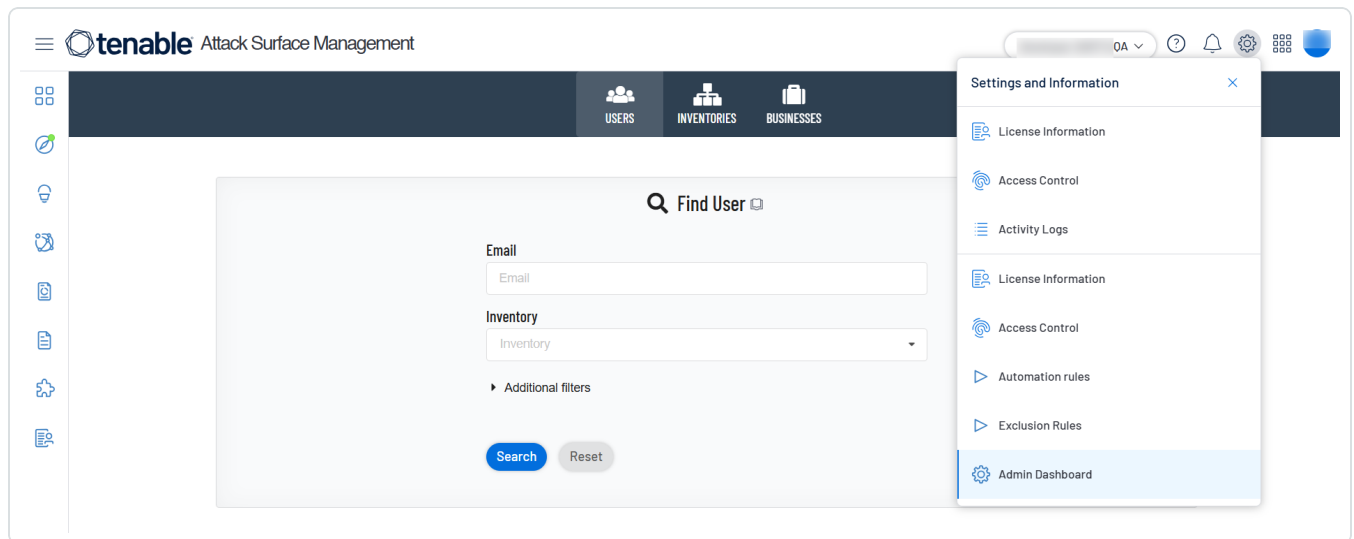
Close

Run Exclusion Rules

To run your exclusion rules:

1. In Tenable Attack Surface Management, click the ⚙ icon in the upper-right corner.

The **Settings and Information** drop-down list appears.



2. In the drop-down list, click **Exclusion Rules**.

The **Exclusion Rules** window appears.

3. Click **Run rules now**.

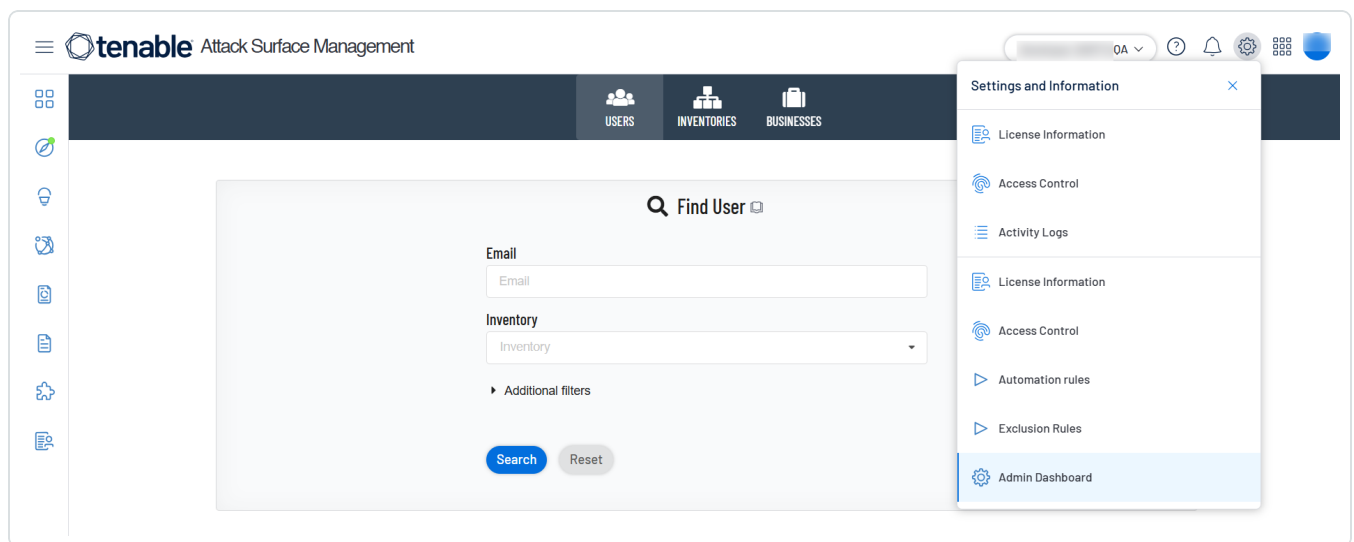
Tenable Attack Surface Management runs the exclusion rules run and updates your inventories to reflect the rules.

Delete an Exclusion Rule

To delete an exclusion rule:

1. In Tenable Attack Surface Management, click the  icon in the upper-right corner.

The **Settings and Information** drop-down list appears.



2. In the drop-down list, click **Exclusion Rules**.

The **Exclusion Rules** window appears.

3. Hover over the exclusion rule you want to delete, then click the  button.

Tenable Attack Surface Management removes the exclusion rule.

Automation Rules

Automation rules perform specific actions automatically when certain events happen in Tenable Attack Surface Management.

Create an Automation Rule

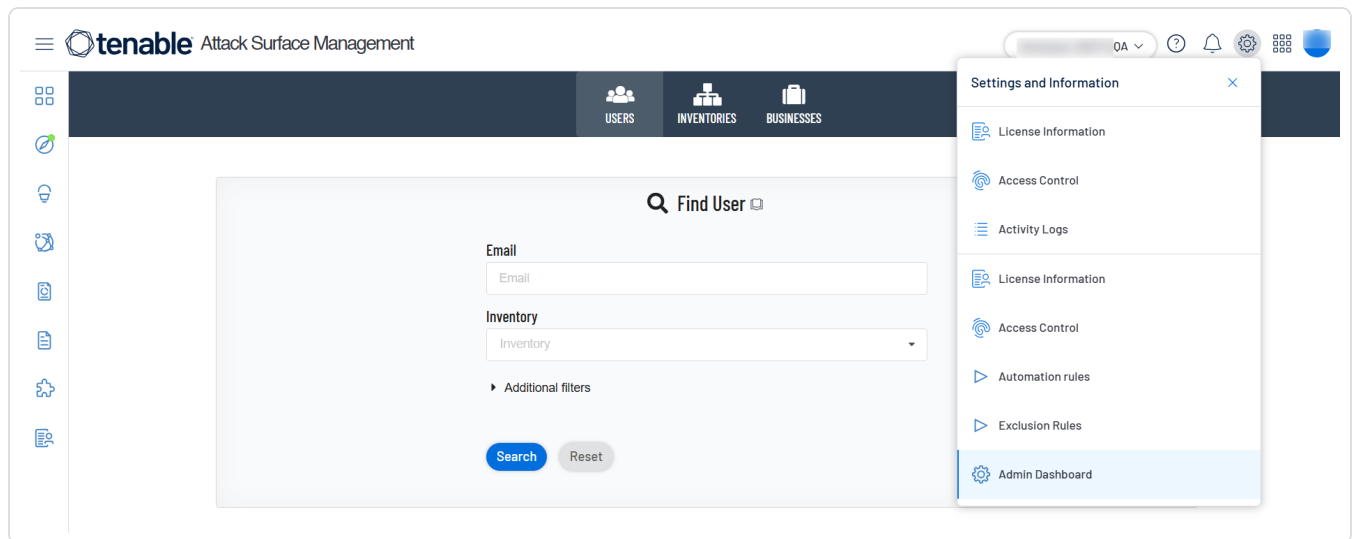
You can create automation rules that run automatically when certain events happen in Tenable Attack Surface Management. For example, you can create an automation rule that adds tags to any assets that fall within a certain subscription.

Automation rules run once a day.

To create an automation rule:

1. In Tenable Attack Surface Management, click the  icon in the upper-right corner.

The **Settings and Information** drop-down list appears.



2. In the drop-down list, click **Automation rules**.

The **Automation Rules** window appears.

3. Click the **Add rule** button.

The **Add Automation Rule** window appears.

4. Select the type of automation rule you want to add and [modify the settings](#).

5. Click **Save**.

Tenable Attack Surface Management creates the automation rule and it appears on the **Automation Rules** window.

To run the automation rule, click the  button.



Automation Rules

Developer DARTS QA

Tenable.asm Automation allows you to write rules which run automatically when certain events happen within Tenable.asm. For instance, you might want an asset to have a particular tag if it falls within a Subscription, without having to tag it yourself. Automation Rules are evaluated on a daily basis.

⋮ #1 **archive assets_autorule**
archive assets_autorule



Close

Add Rule

Automation Rule Settings

The different types of automation rules in Tenable Attack Surface Management have different settings.

Archive Assets

Setting	Description
Rule Name	Type a name for the automation rule.
Rule Description	Type a description for the automation rule.
Archive Asset if it matches	<p>Select when you want the automation rule to archive an asset in your inventory.</p> <ul style="list-style-type: none">• Filters – Archives any assets that match the specified filter. Click +Add Filter to add asset filters.• Subscription – Archives any assets that match the specified subscription. Click the drop-down box to select a subscription.



Modify Tags

Setting	Description
Rule Name	Type a name for the automation rule.
Rule Description	Type a description for the automation rule.
Select what to do	<p>Select whether you want the automation rule to add or remove a tag from assets in your inventory.</p> <ul style="list-style-type: none">• Add – Adds a tag to any asset that matches the automation rule criteria.• Remove – Removes a tag from any asset that matches the automation rule criteria.
Select Tag	Select the tag that you want the automation rule to add or remove.
if Asset matches	<p>Select when you want the automation rule to add or remove a tag from an asset in your inventory.</p> <ul style="list-style-type: none">• Filters – Adds or removes the tag from any assets that match the specified filter. Click +Add Filter to add asset filters.• Subscription – Adds or removes the tag from any assets that match the specified subscription. Click the drop-down box to select a subscription.

Update Custom Columns

Setting	Description
Rule Name	Type a name for the automation rule.
Rule Description	Type a description for the automation rule.
Select what to do	Select whether you want the automation rule to set or remove custom columns from assets in your inventory.



Setting	Description
	<ul style="list-style-type: none">• Set – Adds a custom column to any asset that matches the automation rule criteria.• Remove – Removes a custom column from any asset that matches the automation rule criteria.
Select Custom Column	Select the custom column that you want the automation rule to add or remove.
if Asset matches	Select when you want the automation rule to update custom columns for assets. <ul style="list-style-type: none">• Filters – Updates custom columns for any assets that match the specified filter. Click +Add Filter to add asset filters.• Subscription – Updates custom columns for any assets that match the specified subscription. Click the drop-down box to select a subscription.

Suggestions

Setting	Description
Rule Name	Type a name for the automation rule.
Rule Description	Type a description for the automation rule.
Select what to do	Select whether you want the automation rule to accept or deny suggestions. <ul style="list-style-type: none">• Accept – Accepts all suggestions that match the automation rule criteria.• Deny – Denies all suggestions that match the automation rule criteria.
Suggestion if it matches	Select when you want the automation rule to accept or deny suggestions. <ul style="list-style-type: none">• Filters – Accepts or denies any suggestions that match the specified filter. Click +Add Filter to add domain filters.



Move Assets

Setting	Description
Rule Name	Type a name for the automation rule.
Rule Description	Type a description for the automation rule.
Moves Asset to	Select the inventory to which you want to move assets that meet the automation rule criteria.
if it matches	Select when you want the automation rule to move assets. <ul style="list-style-type: none">• Filters – Moves any assets that match the specified filter. Click +Add Filter to add domain filters.

Run ad-hoc query

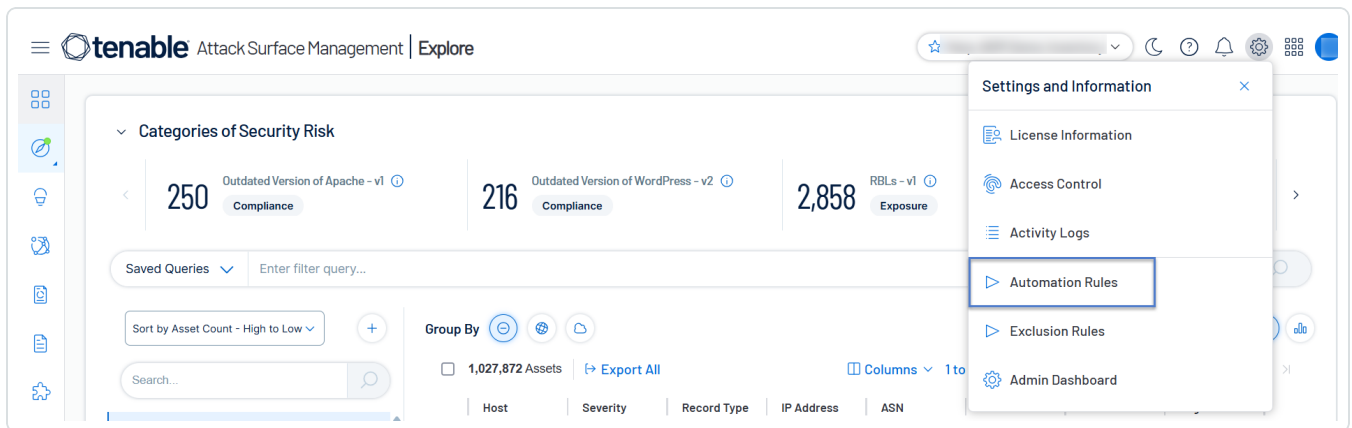
Setting	Description
Rule Name	Type a name for the automation rule.
Rule Description	Type a description for the automation rule.
Run ad-hoc query	Select which query you want the automation rule to run.

Modify an Automation Rule

To modify an automation rule:

1. In Tenable Attack Surface Management, click the  icon in the upper-right corner.

The **Settings and Information** drop-down list appears.

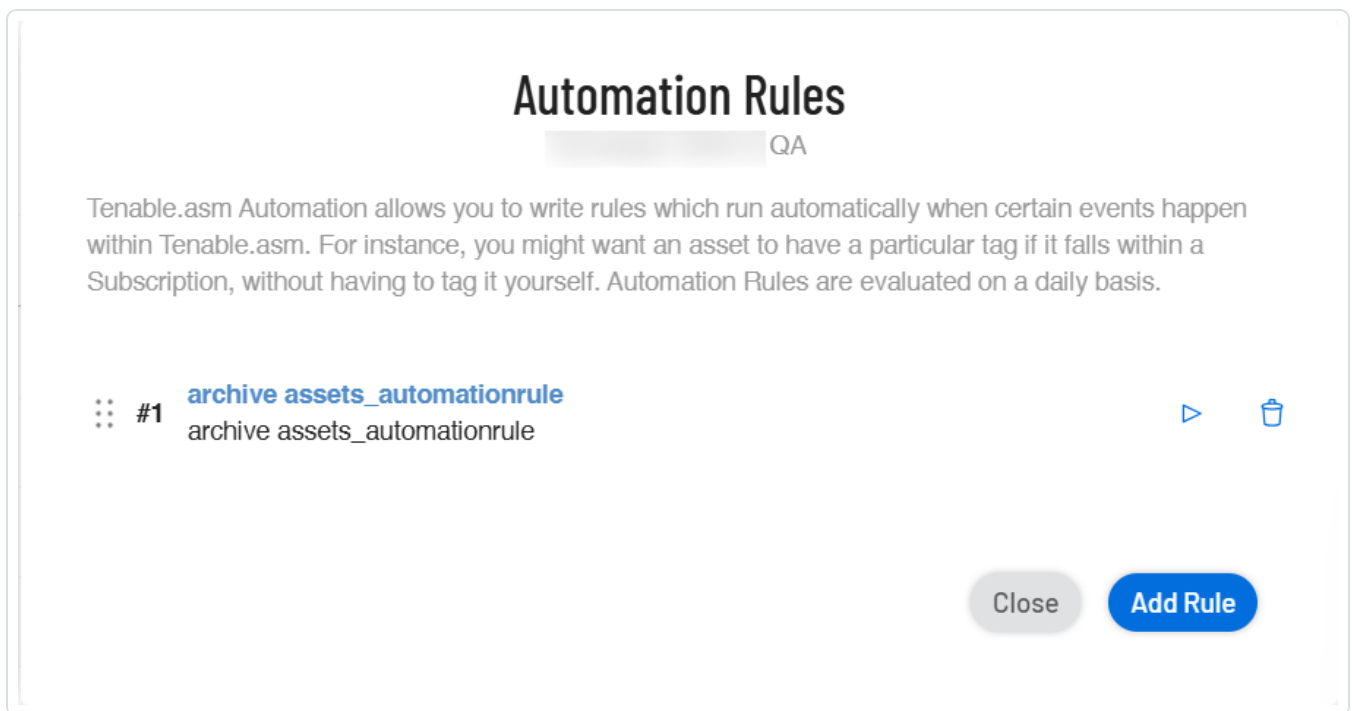


- In the drop-down list, click **Automation rules**.

The **Automation Rules** window appears.

- In the drop-down list, click **Automation rules**.

The **Automation Rules** window appears.



- Click the automation rule you want to modify.

The **Add Automation Rule** window appears.

- Modify the details as needed.



6. Click **Update**.

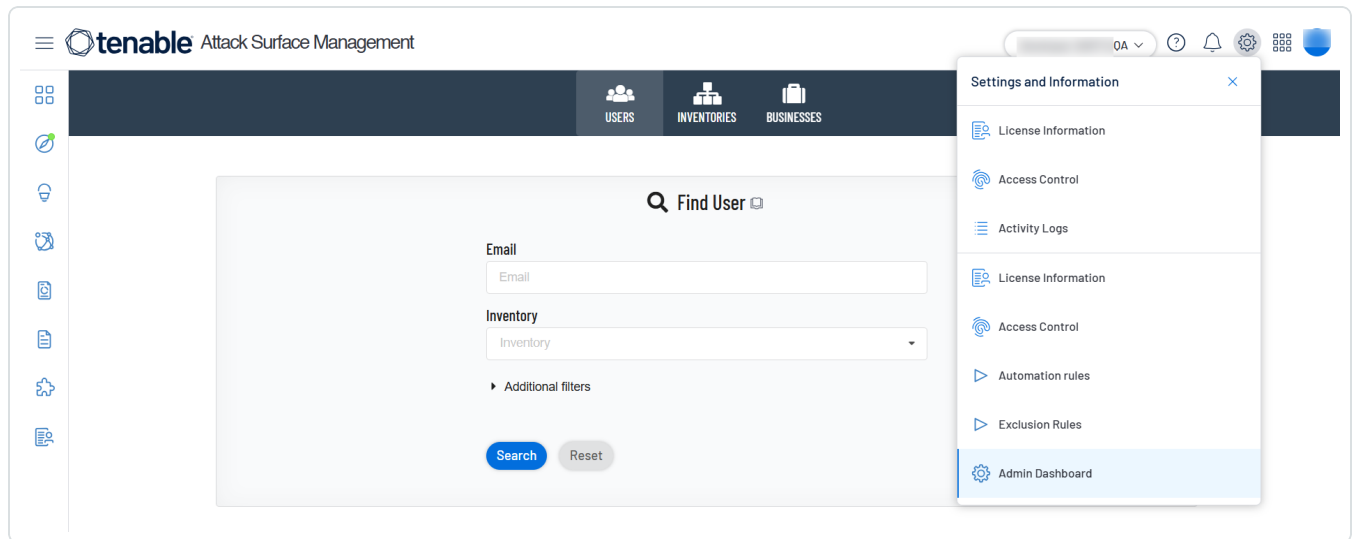
Tenable Attack Surface Management modifies the automation rule.

Delete an Automation Rule

To delete an automation rule:

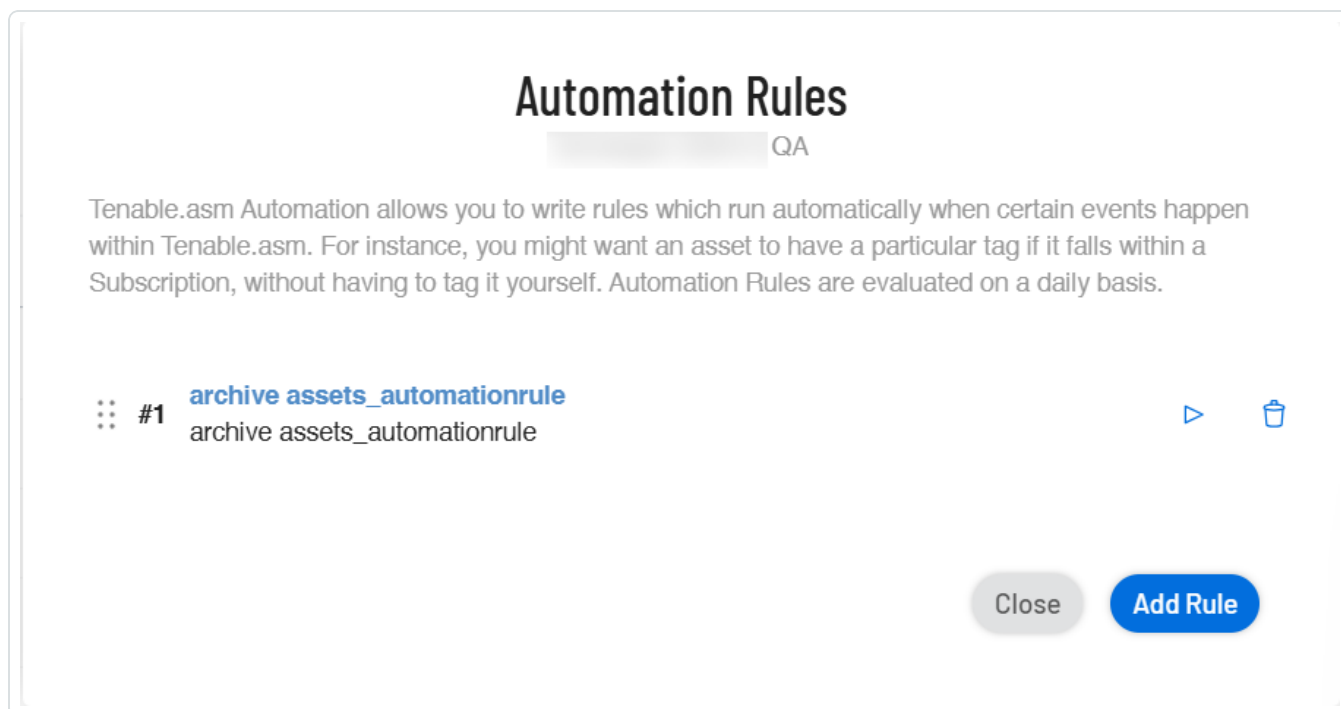
1. In Tenable Attack Surface Management, click the ⚙ icon in the upper-right corner.


The **Settings and Information** drop-down list appears.



2. In the drop-down list, click **Automation rules**.

The **Automation Rules** window appears.



3. In the row of the automation rule you want to delete, click the  button.

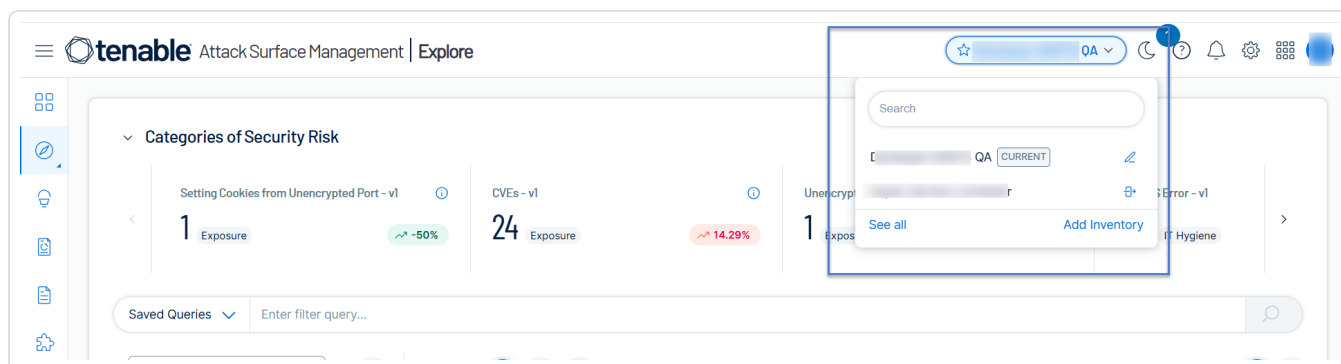
Tenable Attack Surface Management deletes the automation rule.

Asset Details

When you click on an asset in Tenable Attack Surface Management, a page appears that includes all known information about the asset.

To view details for an asset in your inventory:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.





Tenable Attack Surface Management displays the inventories in the drop-down list.

2. Click the inventory you want to view.

The **Explore** page displays the assets for the inventory.

3. In the assets table, click the asset name.

Tenable Attack Surface Management displays the asset details.









The screenshot displays the 'Asset Details' page in Tenable Attack Surface Management. At the top, there's a header with a logo and a record value. Below this, a 'Data Sources' section shows a single source: 'Attack Surface Mana...'. The main content area is divided into three panels: 'Severity' (None), 'Integration Status' (Host Asset, Web App Asset), and 'Key Properties' (Licensed: No, Source: Attack Surface Mana...). Below these panels is a tabbed interface with 'Summary', 'HTML', 'Timeline', 'History', and 'Integration Status'. The 'Summary' tab is selected, showing a 'Tags' section with a tag 'tag without value'. At the bottom, a table lists asset details for 'Tenable.ASM'.

Option	Description
Expand or retract the	In the upper-right corner of the asset details pane:

The **Asset Details** page includes the following details:

Option	Description
Expand or retract the	In the upper-right corner of the asset details pane:



asset details pane	<ul style="list-style-type: none">• Use  option to expand the asset details page.• Use the  option to retract the asset details page.• Click  to close the asset details pane.
Export asset details	<ol style="list-style-type: none">1. In the upper-right corner, click the  button. A menu appears.2. Click  Export to CSV or  Export to XLSX. <p>Tenable Attack Surface Management exports the asset details to the selected format.</p>
Update the asset details	<ol style="list-style-type: none">1. In the upper-right corner, click the  button. A menu appears.2. Click  Update. <p>Tenable Attack Surface Management updates the asset details.</p>
Data Sources	This section shows Severity, Integration Status, and Key Properties of the asset.
Asset details	<p>Click the following tabs to view more details about the asset:</p> <ul style="list-style-type: none">• Summary – A summary of the asset including host details, domain, networking, HTTP headers.• HTML— Asset details in HTML format.• Timeline —Shows a timeline illustrating each stage of the process of adding an asset to the inventory. See View Asset Attribution.• History — The details of change and the time and date when the asset was updated.• Integration Status — The status of Host and Web Application integration. See View Asset Details for Host and Web Application Assets.• Location — The location of the asset. This section includes a pin on a



map, and any known location details for the asset, including continent, country, time zone, and the country where the asset is registered.

- **Ports** – The ports the asset uses for communication.
- **Findings** – The list of vulnerabilities detected on the asset.

Severity Breakdown

Tag

[+ Add tags](#)

Severity Breakdown

LOW

Expired SSL

Asset is using SSL cert passed expiration date.

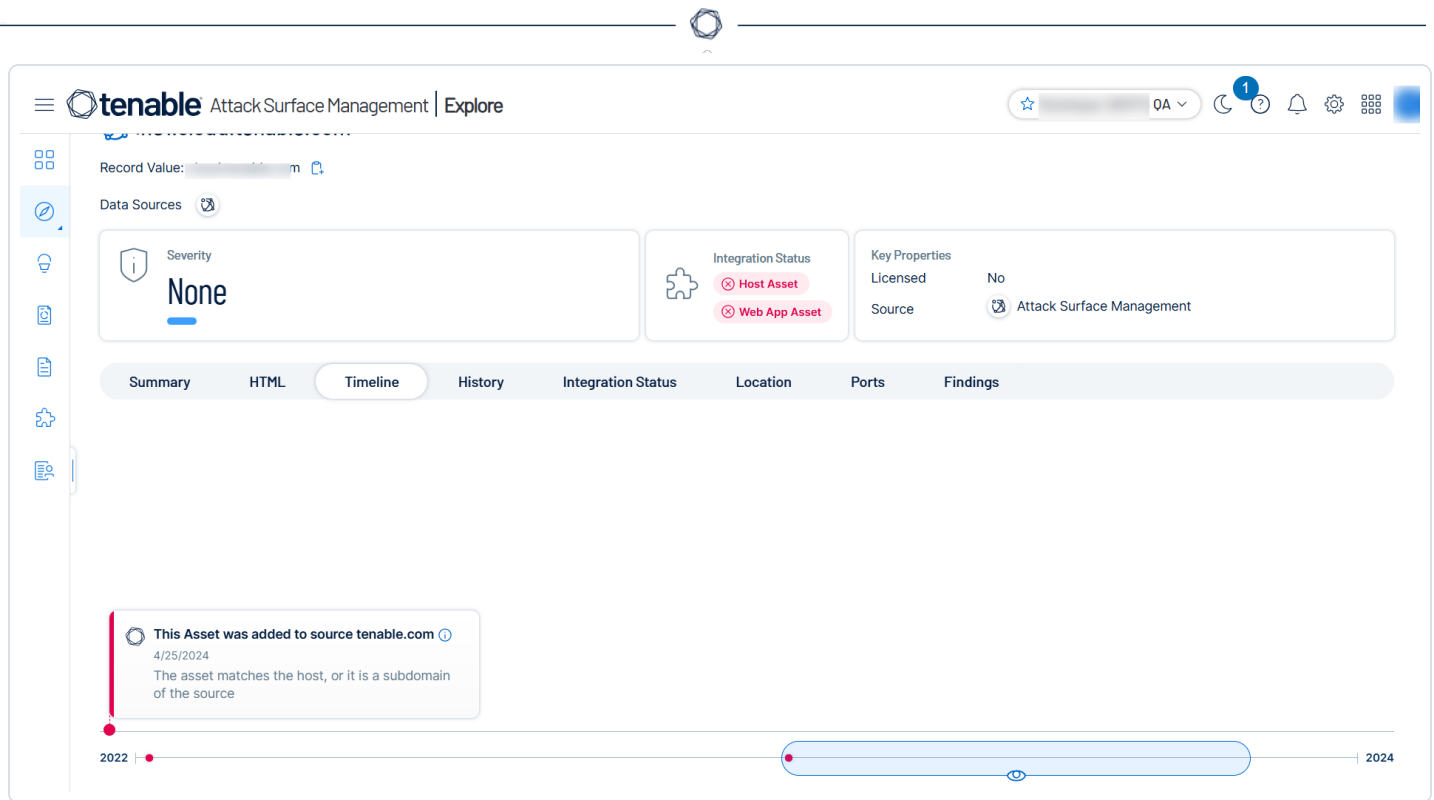
Outdated TLS

Asset supports depreciated TLS versions.

View Asset Attribution

When analyzing exposed assets detected by Tenable Attack Surface Management, it is crucial to understand why each asset appears in the inventory. The asset details page provides origin attributions, offering key insights that enhance analysis by:

- Clarifying asset relevance within the source and inventory context.
- Minimizing manual asset attribution analysis.
- Filtering or searching assets based on attribution events, such as assets linked to an inventory because the WHOIS registrant email of the asset is associated with a specific organization.



The Timeline section on the **Asset Details** page includes a timeline illustrating each stage of the Tenable Attack Surface Management process of adding an asset to the inventory, including:

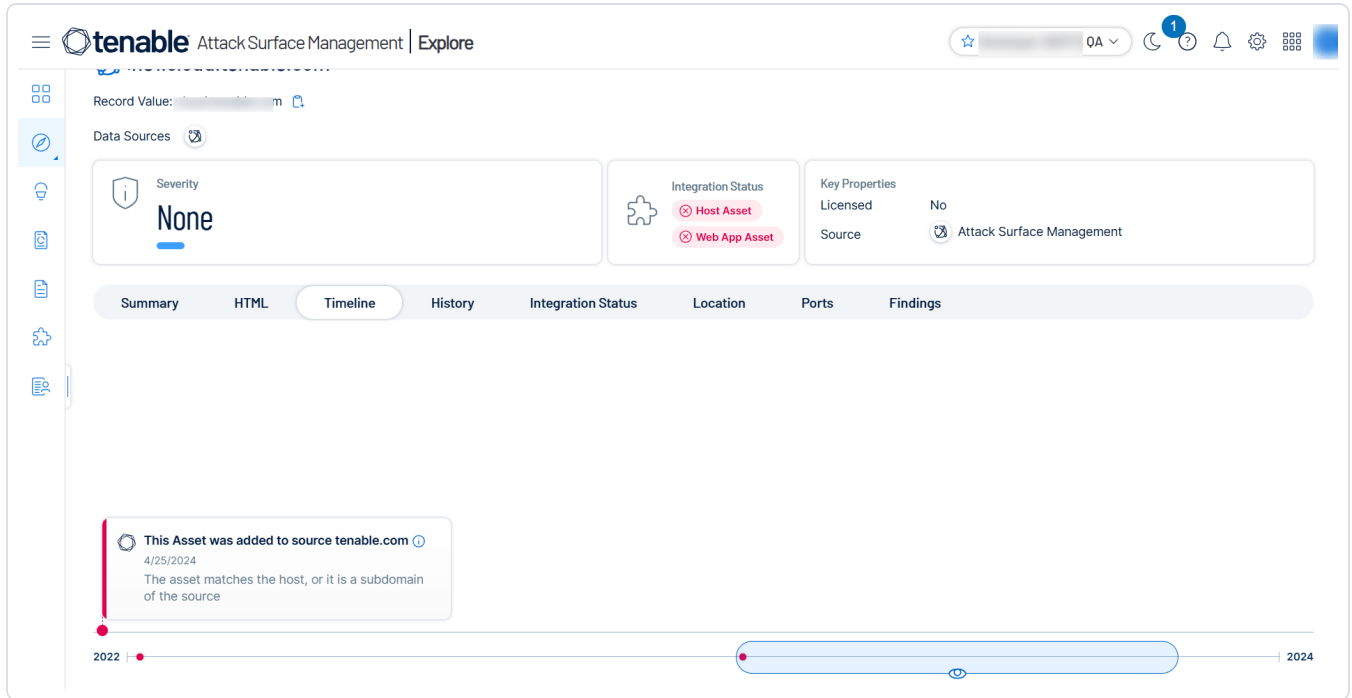
- The ID of the user who initially added the source to the inventory and thereby directly or indirectly added the asset.
- The timestamp when the source was added.
- The timestamp when the asset was added to the source.
- If Tenable Attack Surface Management adds the asset based on an [automation rule](#), then the timeline shows the rule's creation time. For instance, an asset may be added when an automation rule accepts a suggested domain into the inventory. You can click the **View automation rule** link to open the **Add Automation Rule** window to view or modify the automation rule. If the automation rule was updated, you can click the **View logs** link to open the **Activity Logs** page to view the changes.
- The type of source. For example, if the source is IP-based, domain-based, AWS, or Cloudflare.
- If an asset belongs to multiple sources, each source is highlighted in a different color. For example, blue for an IP-based source and dark blue for a domain-based source.
- A **Find similar assets** link to the assets list page that shows assets with similar origin.



To view the origin details for an asset in your inventory:

1. In the **Explore** page, click the asset name in the assets table.

Tenable Attack Surface Management displays the asset details.



Click the **Timeline** tab at the top of the page for the asset attribution details. You can use the slider to navigate the various timelines associated with the asset.

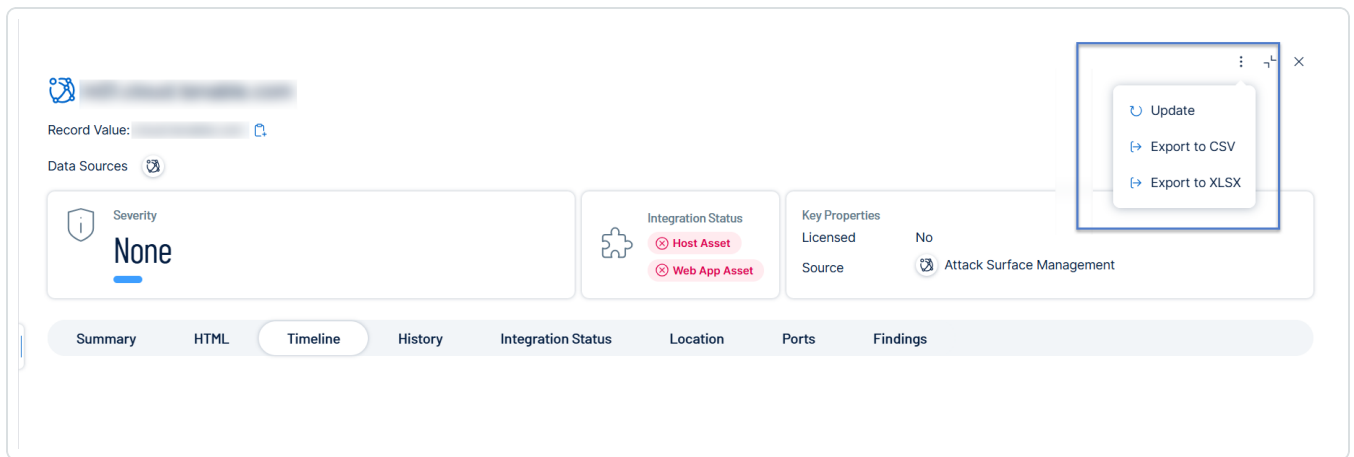
Export an Asset

In Tenable Attack Surface Management, you can export an asset in CSV or XLSX format.

To export an asset:

1. [View the details page for the asset.](#)
2. On the asset details page, in the upper-right corner, click the **⋮** button.

A menu appears.



3. Click [Export to CSV](#) or [Export to XLSX](#).

Tenable Attack Surface Management exports the asset details in the selected format.

Manage Asset Tags

You can add descriptive tags to define and categorize your assets. You can create tags that do not require any values and also which require values such as specific keywords, booleans, cost, and percentage.

Assign Tags to Assets

To assign tags to a single asset or multiple assets:

1. In Tenable Attack Surface Management, in the left navigation bar, click the [Assets](#) button.

The **Explore** page appears.

Scope	Action
Add tags to a single asset	<ol style="list-style-type: none"> 1. To add tags to a single asset: <ul style="list-style-type: none"> • In the row of the asset to add tags, click the ⋮ button A menu appears. • Select the checkbox for the asset to add tags. Tenable Attack Surface Management enables the header.



	<ul style="list-style-type: none">• Right-click the asset you want to add tags. <p>A menu appears.</p> <ol style="list-style-type: none">2. Select Add Tags. <p>The Add Tags window appears.</p> <ol style="list-style-type: none">3. Select or create a new tag. <p>Tenable Attack Surface Management adds the tags to the Tags to be Added box.</p> <ol style="list-style-type: none">4. Click Add Tags. <p>Tenable Attack Surface Management adds the tags to the asset.</p>
Add tags to multiple assets	<p>To add tags to multiple assets:</p> <ol style="list-style-type: none">1. Select the checkbox for one or several assets you want to add tags. <p>Tenable Attack Surface Management enables the header.</p> <ol style="list-style-type: none">2. Select Add Tags. <p>The Add Tags window appears.</p> <ol style="list-style-type: none">3. Select or create a new tag. <p>Tenable Attack Surface Management adds the tags to the Tags to be Added box.</p> <ol style="list-style-type: none">4. Click Add Tags. <p>Tenable Attack Surface Management adds the tags to the assets.</p>

Add Tags from the Asset Details page

To add tags from the Asset Details page:



1. In the **Explore** page, in the assets table, click the asset name.

Tenable Attack Surface Management displays the asset details.

Record Value: [redacted] m

Data Sources

Severity: None

Integration Status: Host Asset, Web App Asset

Key Properties: Licensed: No, Source: Attack Surface Mana...

Summary | HTML | Timeline | History | Integration Status | ...

Tags: tag without value

Tenable.ASM

Host	[redacted]
Severity	None
Record Type	CNAME
Record Value	[redacted]
IP	[redacted]
Last Metadata Change	05/16/2025
Domain	tenable.com

2. In the **Tags** section, click .

The **Add Tags** window appears.

3. Select or create a new tag.

Tenable Attack Surface Management adds the tags to the **Tags to be Added** box.

4. Click **Add Tags**.


Tenable Attack Surface Management adds the tags to the asset.



Remove Tags

Removing tags for an asset removes the tags from Tenable Attack Surface Management and as a result from all the assets that have the specific tag.

To remove tags:

Scope	Action
Remove tags from a single asset	<ol style="list-style-type: none">To remove tags from a single asset:<ul style="list-style-type: none">In the row of the asset to remove tags, click the  button A menu appears.Select the checkbox for the asset to remove tags. Tenable Attack Surface Management enables the header.Right-click the asset for which you want to remove tags. A menu appears.Select Remove Tags. The Remove Tags window appears.Select the tags to remove. Tenable Attack Surface Management adds the tags to the Tags to be Removed box.Click RemoveTags. Tenable Attack Surface Management removes the tags to the asset.
Remove tags from multiple assets	To remove tags from multiple assets:



1. Select the checkbox for one or several assets for which you want to remove tags.

Tenable Attack Surface Management enables the header.

2. Select **Remove Tags**.

The **Remove Tags** window appears.

3. Select the tags to remove.

Tenable Attack Surface Management adds the tags to the **Tags to be Removed** box.

4. Click **Remove Tags**.

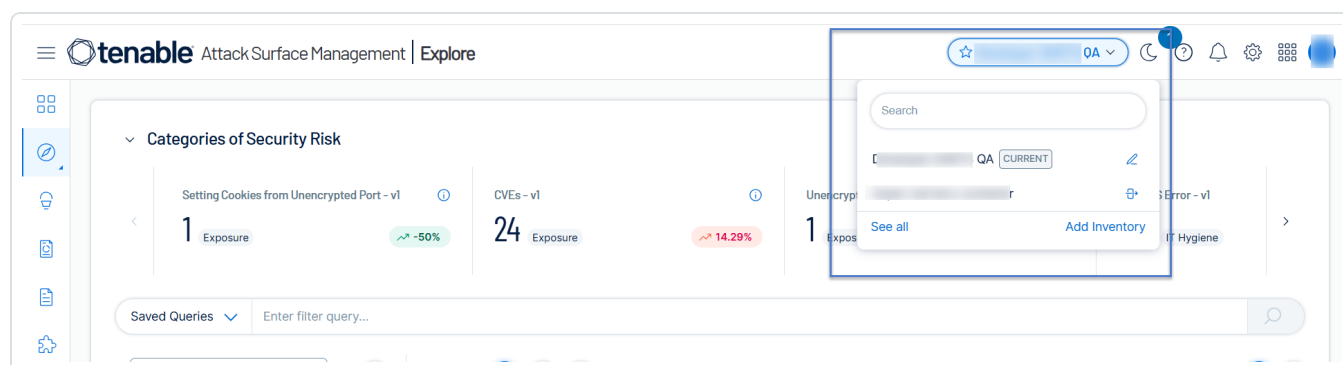
Tenable Attack Surface Management removes the tags from the assets.

Move or Copy Assets to another Inventory

You can move or copy assets from one inventory to another inventory. The target inventory adds these assets to a new source with the name: **From other inventories**. When you move assets, the source inventory archives these assets, whereas copying the assets leaves them in the original inventory.

Move assets from one inventory to another inventory:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.

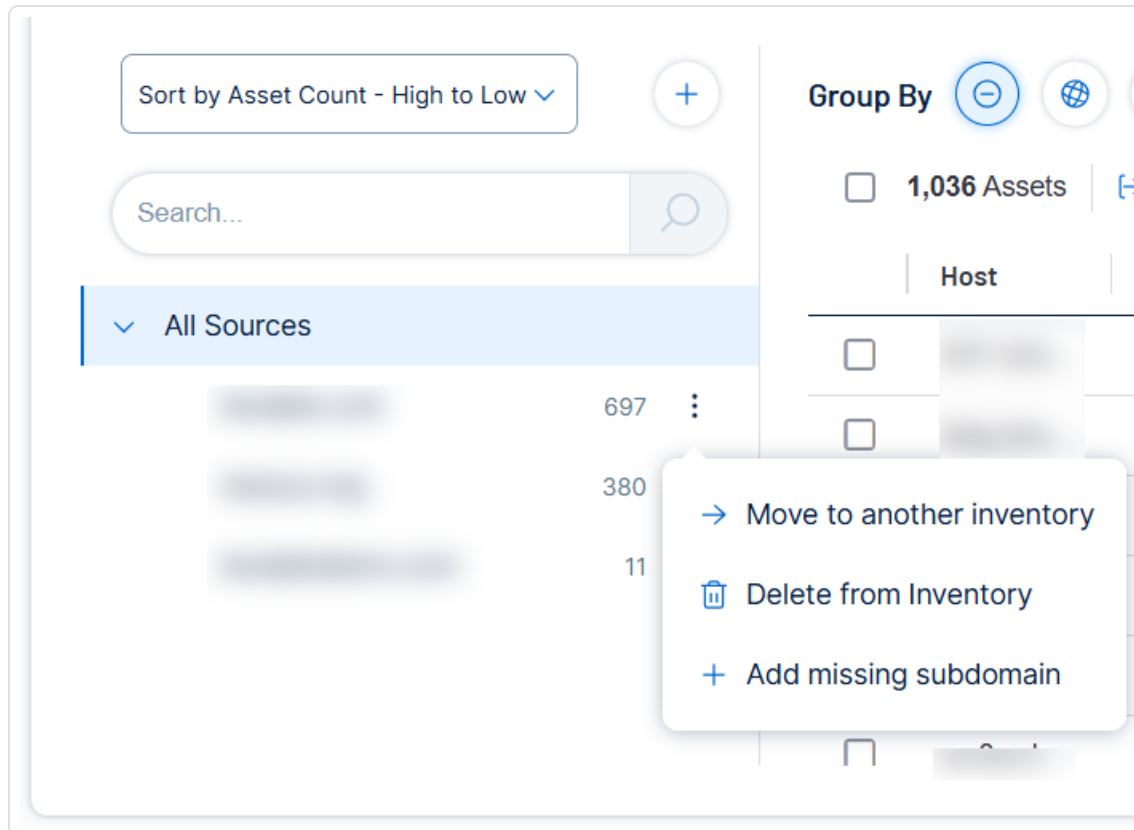




Tenable Attack Surface Management displays the inventories in the drop-down list.

2. On the **Explore** page, in the **All Sources** pane, next to the source, click the  button.

A menu appears.



3. Click **Move to another inventory**.

The **Move source to another inventory** window appears.

Note: The **Move to another inventory** option is available only if the current user has **Archive** permission in the current inventory.

4. Select an inventory from the list to move the assets.
5. Click **Move**.

Tenable Attack Surface Management moves the assets to the target inventory and also archives them in the source inventory.

Archive an Asset

You can archive single or multiple assets from the inventory.



1. To archive a single asset:

- In the row of the asset you want to archive, click the **⋮** button.

A menu appears.

- Select the checkbox for the asset to archive.

Tenable Attack Surface Management enables **⋮ More > Archive**.

- Right-click the row of the asset you want to archive.

A menu appears.

2. Click **Confirm**.

Tenable Attack Surface Management archives the asset.

3. Click **Archive**.

Tenable Attack Surface Management prompts you to confirm.

To archive multiple assets:

1. Select the checkbox for one or several assets you want to archive.

Tenable Attack Surface Management enables the header.

2. Click **⋮ More > Archive**.

Tenable Attack Surface Management prompts you to confirm.

3. Click **Confirm**.

Tenable Attack Surface Management archives the assets.


Suggested Domains

Tenable Attack Surface Management continually analyzes internet data to produce a list of suggested domains that might be related to your organization. You can use the **Suggested domains** page to verify that your organization is aware of every domain it owns. While Tenable Attack Surface Management automatically adds most assets to your inventory, some assets require further verification to confirm ownership.



To view your suggested domains:

1. In the left navigation bar, click the  **Suggestions** button.

The **Suggested domains** page appears. When there are new domain suggestions to review, the  button turns yellow.

The **Suggested domains** page shows the following details:

Columns	Description
Name	Domain names that Tenable Attack Surface Management suggests you may own.
Type	The type of suggestion. Suggestion types can be ASN, brand, domain, IP, IP range, subdomain, or nameserver.
Rules	The logic based on which Tenable Attack Surface Management suggested the domain name. Hover over the column to view the details of the logic. By default, the most recent suggestions are displayed first.
Suggestion Date	The date on which Tenable Attack Surface Management suggested the domain name.

2. On the **Suggested domains** page, you can sort the assets list as follows:

- Filter the table to view specific suggestions.

1. At the top of the table, click  **Add Filter**.

The Add Filter drop-down appears.

2. Use the **Search for Filters** box or select the filter from the list. For example, **Name**.

The list of operators appears.

3. Select the operator. For example, **contains**.

4. Type the value of the filter, if needed.



5. Click **Done**.

6. (Optional) To add another filter, click **+ Add Filter**.

1. Repeat steps from 2 to 5.

Tenable Attack Surface Management adds a new third filter to the list with the following options:

- **that match all filters** – Lists only the assets that match all the filters.
- **that match any filters** – Lists assets that match any one of the filters.

2. Select one of the options and click **Done**.

Tenable Attack Surface Management shows the filtered results.

- Click the column header to sort the table view. For example, sorting the **Rules** column lists the domain names with multiple rules detected.

Prioritizing the Suggested Domains List

Tenable Attack Surface Management can suggest thousands of domain names. To prioritize domain names based on the likelihood of ownership:

- Sort the **Rules** column to view the suggestions with the most matching rules.
- Filter the Suggested domains table to view organization-specific assets.

Add Suggested Domains to an Inventory

Once you confirm that the suggested domains belong to your organization, you can add them to your inventory.

To add suggested domains to your inventory:

1. In the Suggested domains table, select check boxes next to the domain names you want to add to your inventory.

Tenable Attack Surface Management displays a menu bar at the top of the table.

2. Do one of the following:



Description	Action
Add to the current selected inventory	Click the Add to this inventory button.
Add to a different inventory	Click the Add to this inventory drop-down arrow, and select an inventory from the list.

Tenable Attack Surface Management adds the domain name to the selected inventory.

Archive Suggested Domains

You can archive suggested domains to omit them from the Suggested domains list.

To archive suggested domains:

1. In the Suggested domains table, select check boxes next to the domain names to archive.

Tenable Attack Surface Management displays a menu bar at the top of the table.

2. Click **Archive**.


Tenable Attack Surface Management archives the selected domains and removes these domain names from the suggested domains list.

3. (Optional) To view archived suggestions:

- a. Click the  button.

A menu appears.

- b. Select **Archived suggestions**.

The **Archived suggestions** page appears. To go back to the **Suggested domains** page, click the  button.

Suggestion Blocklist

You can add domain names, email addresses, hostname, or CIDR (Classless Inter-Domain Routing) to **Suggestion Blocklist** to exclude them from the suggested domains list.

To add items to blocklist:



1. In the **Suggested domains** page, click the  button.

A menu appears.

2. Select **Blocklisted items**.

The **Suggestion blocklist items** window appears with the following details:

Column	Description
Value	The domain name, email address, CIDR, or hostname for the suggestion.
Type	The type of suggestion – email, domain, hostname, or CIDR.
Extra	Additional information about the suggestion value.

3. (Optional) Use the Search blocklisted items box to search for specific blocklisted items.
4. To add a blocklist item, click **Add an additional blocklist item**.

The **Add an additional blocklist item** window appears.

5. In the **Suggestion type** drop-down box, select one of these suggestion types: domain, email, hostname, or CIDR.
6. In the **Value** box, type a suggestion value.
7. Click **Add**.

Tenable Attack Surface Management adds the entry to the blocklisted items list and displays the **Suggestion blocklist items** window.

8. Click **Close** to exit the window.

Manage Suggested Domains

Tenable Attack Surface Management can suggest domain names based on the assets in your inventory, brand names, email addresses, organization names, nameservers, and backref links.

To refine your suggested domains list by adding domains that belong to a specific category, you can configure the following options:



- **Manage source-based suggestions**
- **Manage brand names**
- **Manage registrator emails**
- **Manage nameservers**
- **Manage backref links**

Manage source-based suggestions

You can configure Tenable Attack Surface Management to suggest domain names based on the assets in your inventory.

To add source-based domains to your suggested domains list:

1. In the **Suggested domains** page, click the  button.

A menu appears.

2. Select **Manage source based suggestions**.

The **Manage source based suggestions** window appears.

3. Click **Add new suggestions based on assets in the inventory** toggle to enable this option.
4. Click **Save**.

Tenable Attack Surface Management starts adding domain names based on the assets in your inventory.

Note: You can disable the **Add new suggestions based on assets in the inventory** option to limit the suggestions to brand names.

Note: When you add an entry, it may take a day for the new suggestions to appear.

Manage brand names

Configure Tenable Attack Surface Management to suggest domain names based on or similar to specific brand names. Tenable Attack Surface Management includes domain names that contain positive modifiers, and excludes those with negative modifiers.



To add suggestions based on brand names:

1. In the **Suggested domains** page, click the  button.

A menu appears.

2. Click **Manage brand names**.

The **Brand names** window appears.

3. Click **Add a new entry**.

The **Add brand name** window appears.

4. Type the brand name without spaces.

5. From the **Modifier** drop-down box, select **Positive** or **Negative**.

Note: If you select a positive modifier, Tenable Attack Surface Management suggests homoglyphs or look-alike domain names based on brand names. If you select a negative modifier, Tenable Attack Surface Management excludes domain names that contain brand names.

6. Click **Save**.

The **Brand names** window appears with the newly added brand entry.

7. (Optional) To add additional entries, click **Add a new entry** or click **Close** to exit the window.

Tenable Attack Surface Management starts adding domain names based on brand names.

Note: When you add a new entry, it may take a day for the new suggestions to appear.

Manage registrator emails

You can add email addresses or domain names for Tenable Attack Surface Management to suggest domain names associated with these email addresses. Tenable Attack Surface Management uses the Whois registration data to uncover domain names linked to specific email addresses.

To add suggestions based on email addresses:



1. In the **Suggested domains** page, click the  button.

A menu appears.

2. Click **Manage registrator emails**.

The **Registrar emails** window appears.

3. Click **Add a new entry**.

The **Add registrator email** window appears.

4. In the **Registrar email** box, type the email address or domain name. For example, *you@yourcompany.com* or *@company.com*.

5. Click **Save**.

The **Registrar emails** window appears with the newly added entry.

6. (Optional) To add additional entries, click **Add a new entry** or click **Close** to exit the window.

Tenable Attack Surface Management starts adding domain names that might be associated with the specified email addresses.

Note: When you add a new entry, it may take a day for the new suggestions to appear.

Manage organization names

Configure Tenable Attack Surface Management to suggest domain names based on organization names.

To add suggestions based on organization names:

1. In the **Suggested domains** page, click the  button.

A menu appears.

2. Click **Manage organization names**.

The **Organization Names** window appears.

3. Click **Add a new entry**.

The **Add organization name** window appears.



4. In the **Organization name** box, type the organization name.
5. Click **Save**.

The **Organization Names** window appears with the newly added entry.

6. (Optional) To add additional entries, click **Add a new entry** or click **Close** to exit the window.

Tenable Attack Surface Management starts adding domain names with the specified organization names.

Note: When you add a new entry, it may take a day for the new suggestions to appear.

Manage nameservers

Configure Tenable Attack Surface Management to suggest domain names based on nameservers.

To add suggestions based on nameservers:

1. In the **Suggested domains** page, click the  button.

A menu appears.

2. Click **Manage nameservers**.

The **Nameservers** window appears.

3. Click **Add a new entry**.

The **Add nameserver** window appears.

4. In the **Nameserver** box, type the nameserver to add. For example, *ns.yourcompany.com*.
5. Click **Save**.

The **Nameservers** window appears with the newly added entry.

6. (Optional) To add more entries, click **Add a new entry** or click **Close** to exit the window.

Tenable Attack Surface Management starts adding domain names associated with the nameservers.

Note: When you add a new entry, it may take a day for the new suggestions to appear.



Manage backref links

Configure Tenable Attack Surface Management to suggest domain names using backref links.

To add suggestions based on organization names:

1. In the **Suggested domains** page, click the  button.

A menu appears.

2. Click **Manage backref links**.

The **Backref links** window appears.

3. Click **Add a new entry**.

The **Add backref link** window appears.

4. In the **Backref link** box, type the backref link. For example, `https://www.yourcompany.com/privacy-policy`.

5. Click **Save**.

The **Backref links** window appears with the newly added entry.

6. (Optional) To add additional entries, click **Add a new entry** or click **Close** to exit the window.

Tenable Attack Surface Management starts adding domain names associated with the backref links.

Note: When you add a new entry, it may take a day for the new suggestions to appear.


Subscriptions

Tenable Attack Surface Management subscriptions notify you about important changes to your attack surface, including new servers, newly opened or closed ports, and new software. You can configure your subscriptions to include the changes that you think are most important.

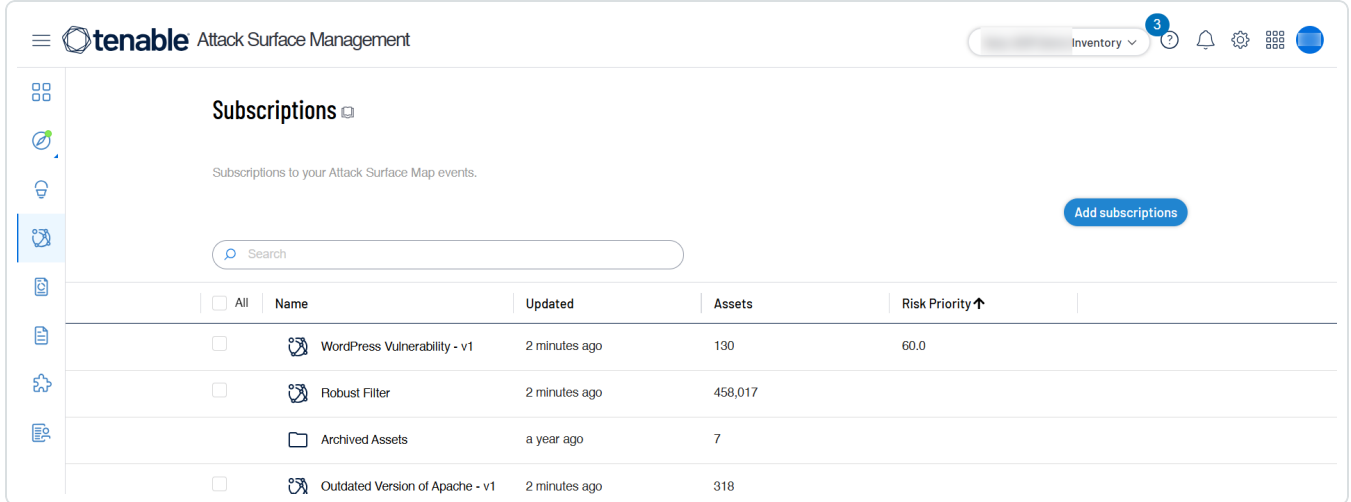
Note: In the **Explore** user interface, you can access subscriptions through **Saved Queries**. For more information, see [Explore](#).



To access **Subscriptions**:

1. In the left navigation bar, click the  button.

The **Subscriptions** page appears.







Subscriptions

Subscriptions to your Attack Surface Map events.

[Add subscriptions](#)

Search

<input type="checkbox"/> All	Name	Updated	Assets	Risk Priority ↑
<input type="checkbox"/>	 WordPress Vulnerability - v1	2 minutes ago	130	60.0
<input type="checkbox"/>	 Robust Filter	2 minutes ago	458,017	
<input type="checkbox"/>	 Archived Assets	a year ago	7	
<input type="checkbox"/>	 Outdated Version of Apache - v1	2 minutes ago	318	


Set Up Notifications

When a particular event occurs on your attack surface, you can receive notifications via email, ServiceNow email, or Slack.

For example: You may want to receive notifications if Tenable Attack Surface Management discovers one of your assets outside of the USA.

To configure notifications:

1. Hover your mouse over the subscription titled **Hosted Outside of US**.



Subscriptions

Subscriptions to your Attack Surface Map events.

[Add subscriptions](#)

<input type="checkbox"/> All	Name	Updated ↑	Assets	Risk Priority
<input type="checkbox"/>	 Hosted Outside of US - v2	a few seconds ago	1,434	  

2. Click the bell icon.




The following options appear:

Alerts for Hosted Outside of US - v2

Email


Sends an email to lex@bitdiscovery.com • Edit

☐

servicenow™

Sends an email to a ServiceNow email address • Setup

☐

slack

Posts a message to an incoming webhook • Setup

☐

Close

- Email:
 - a. Click the toggle to enable the Email option.
 - b. Type the email address in which you want to receive the notifications.
 - c. Click **Save**.

Note: You can click **Send Test Alert** to send a sample email to the specified email address.

- ServiceNow
 - a. Click the toggle to enable the ServiceNow option.
 - b. Type the ServiceNow email address in which you want to receive the notifications.



- c. Click **Save**.

Note: You can click **Send Test Alert** to send a sample email to the specified email address.

- Slack
 - a. Click the toggle to enable the Slack option.
 - b. Type the Slack WebHook URL of the channel in which you want to receive the notifications.
 - c. Click **Save**.

Note: You can click **Send Test Alert** to send a sample message to the specified Slack channel.

Add Subscriptions

Tenable Attack Surface Management provides an ever-growing list of hundreds of events that you can subscribe to.

To add subscriptions:

1. Click the **Add subscriptions** button.

The **Add Subscriptions** window appears.

2. (Optional) Click **All Categories** and select the required category from the list. By default, Tenable Attack Surface Management displays all categories.

Tenable Attack Surface Management lists the subscriptions of the selected category.

3. For the subscriptions that you want to add, in the **Action** column, click **Subscribe**.

Tenable Attack Surface Management adds the subscription.

Predefined Subscription Categories

You can subscribe to the following predefined subscription categories:



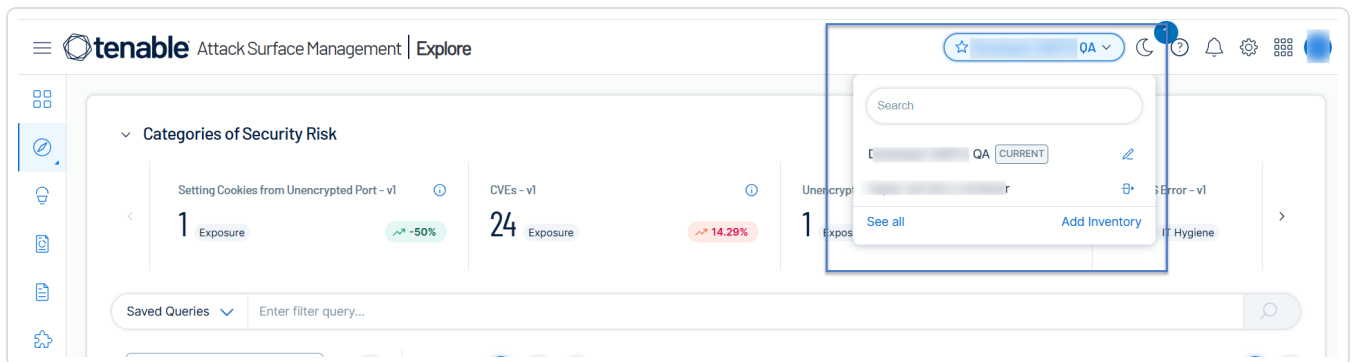
- Compliance – Subscriptions that focus on compliance-related issues, such as GDPR, Copyleft issues, and so on.
- Exposure – Subscriptions that indicate known exposures, such as CVEs, WordPress vulnerabilities, and so on.
- Geography – Geographic subscriptions, such as assets hosted outside the US, and so on.
- IT Hygiene – Subscriptions that highlight applications that are broken or misconfigured, such as SSL/TLS issues, 500 errors, and so on.
- Marketing – Subscriptions that show SEO or marketing issues, such as lack of SEO plugins, disabled caching, and so on.
- Technology – Subscriptions that help identify certain technologies, such as F5, IoT devices, and so on.

Create Custom Subscriptions

You can create custom subscriptions by filtering your inventory and saving the filter as a subscription.

To create custom subscriptions:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select the inventory that you want to view.

Your inventory appears.



3. Click **+ Add Filter** and add the required filter to your inventory.
4. Click Save.

The **Create Subscription** window appears.


5. Type a name for the subscription.
6. Click **Create Subscription**.

Tenable Attack Surface Management saves the subscription and adds it to the list of subscriptions.

Share a Subscription

You can share your subscription with others using a link.

To share a subscription:

1. Hover your mouse over the subscription.
2. Click the  icon.

The **Share Subscription** window appears.

3. Select the number of days after which you want the subscription to age out.

The default number of days is 7. You can set a maximum limit of up to 30 days.

4. Click **Generate Link**.

The Share Subscription window displays a link.

5. Click **Copy Link**.

You can now share this link with others.

Copy a Subscription

In Tenable Attack Surface Management, you can copy a subscription to an inventory.

1. Select the check boxes for the subscriptions you want to copy.
2. Click **Copy Subscriptions**.



The **Copy Subscription to the following Inventories** window appears.

3. Select the inventory to which you want to copy the subscription.
4. Click the **Next** button.

Tenable Attack Surface Management copies the subscription to the inventory.

Delete a Subscription

1. Select the check boxes for the subscriptions you want to delete.
2. Click the **Delete** button.

A dialog box appears, confirming you want to delete the subscription.

3. Click the **Delete** button.

Tenable Attack Surface Management deletes the subscription.



Activity Logs

Tenable Attack Surface Management logs all system events for your account and groups them based on timestamp and actor. You can access the logs using the **Activity Logs** page. You can filter events by timestamp, action, actor, or target.

Activity Logs

System related events committed by users appear here. Log items are grouped based on timestamp and actor.

Set

Created at	Action	Actor	Target	Description
2025-05-20 15:03:26	Added Exclusion Rule	[REDACTED]	none	An exclusion rule was added to the inventory with the mat...
2025-05-20 15:03:09	Deleted Exclusion Rule	[REDACTED]	none	An exclusion rule was deleted from the inventory with the ...
2025-05-20 14:56:13	Added Exclusion Rule	[REDACTED]	none	An exclusion rule was added to the inventory with the mat...
2025-05-20 14:55:54	Added Exclusion Rule	[REDACTED]	none	An exclusion rule was added to the inventory with the mat...
2025-05-20 14:51:41	Added Exclusion Rule	[REDACTED]	none	An exclusion rule was added to the inventory with the mat...

To view all user activity logs:

1. In the left navigation bar, click the button.

The **Activity Logs** page appears with the following details.

Column	Description
Created at	The date and time of the event.
Action	The actual system event.
Actor	<div>The column lists one of the following categories associated with the event.<ul style="list-style-type: none">Automation RuleExclusion RuleDaily Job</div>



	<ul style="list-style-type: none">• Weekly Cleanup Job• User email
Target	The ID of the event target. For example, dashboard ID and asset ID.
Description	A description of the event. For example: An asset was archived.

2. Use the filter query box to filter events.

a. Click inside the filter query box.

A drop-down menu with the column name options appears.

b. Select a column name.

A list of available filter types appear.

c. Select a filter type from the list.

Filter Type	Description
is	Filters for events that match the selected filter value.
is-not	Filters for events that do not match the filter value.
is-one-of	Filters for events that match one of the filter values. <div>Note: Separate the filter values by commas without any spaces. For example, actor <code>is-one-of x,y,z</code>.</div>
is-not-one-of	Filters for events that do not match any of the filter values. <div>Note: Separate the filter values by commas without any spaces. For example, actor <code>is-not-one-of x,y,z</code>.</div>
starts-with	Filters for events that start with the filter values.
ends-with	Filters for events that end with the filter values.
contains	Filters for events that contain the filter value.



does-not-contain	Filters for events that do not contain the filter value.
is-unknown	Filters for events that have unknown value.
has-any-value	Filters for events that have any value.
more-than	Filters for events that match a value for more than a specific number of days.
exactly	Filters for events that match an exact value.
less-than	Filters for events that match a value less than the specified number.
after	Filters for events that occurred after a specific date.
on	Filters for events that occurred on a specific date.
before	Filters for events that occurred before a specific date.
is-unknown	Filters for events that with an unknown value.
has-any-value	Filters for events that with any value.

- d. Provide the values for the selected type.
- e. To query using multiple criteria, use the **AND** or **OR** operators.
- f. Click **Set**.

Tenable Attack Surface Management displays the filtered events.

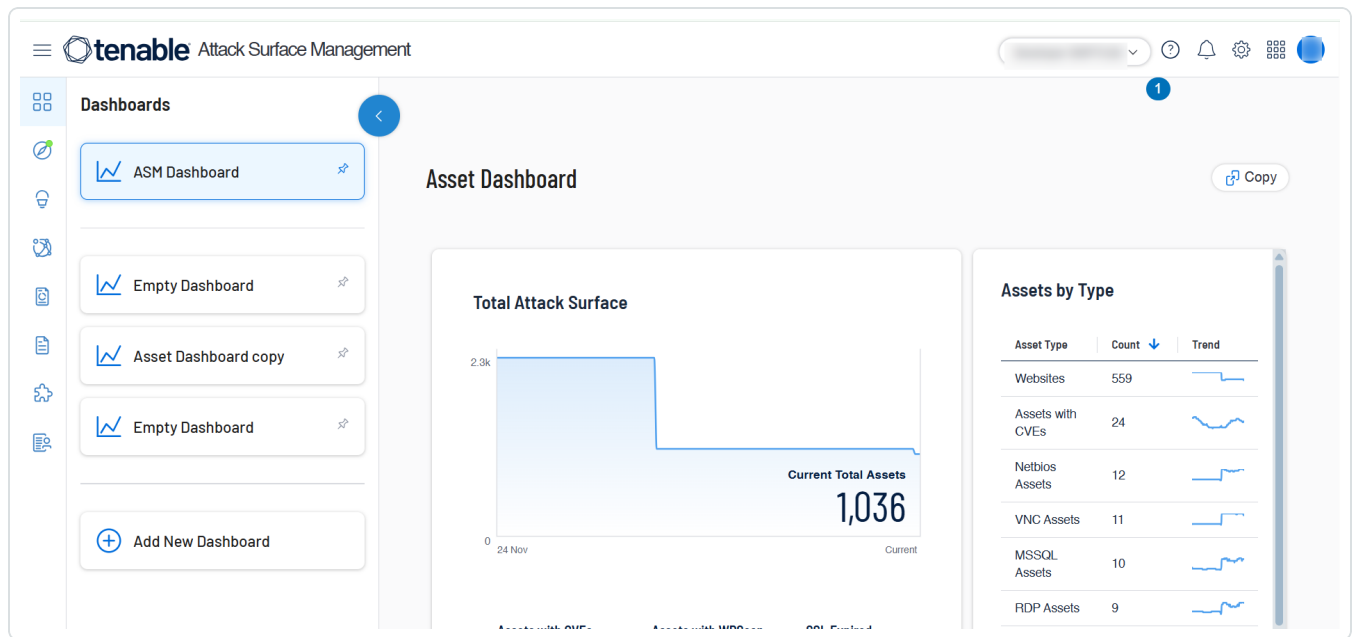
Dashboard

The Tenable Attack Surface Management dashboard provides insights into your organization's assets.

To view your dashboard:

1. In the left navigation bar, click the  **Dashboard** button.

The **Asset Dashboard** page appears.



Click a widget to view a filtered list of assets in your inventory that matches the widget criteria.

Widget	Description
Total Attack Service	The percentage of total assets in the attack surface.
Assets by Type	The number of assets by type.
Attack Surface by Criticality /Severity Ranking over Time	The number of affected assets by their severity. <div>Note: The Current Total Assets number in the chart only includes assets that do not have a ranking None.</div>
Assets by Country	The number of assets by country.
Detected Services	The number of assets by the hosted web servers.




Manage Dashboards

You can create your own dashboards, add new widgets, or customize the default **Asset Dashboard** from the **Dashboards** page.

Create a Dashboard

Add an empty dashboard and add the required widgets to create your own dashboard.

To create a new dashboard:

1. In Tenable Attack Surface Management, in the upper-right corner, click the  button.

The **Dashboards** page appears.

2. In the left panel, click  **Add New Dashboard**.

Tenable Attack Surface Management creates a new **Empty Dashboard**. The new dashboard includes an **Add widget** tile.

3. In the **Empty Dashboard** box, type a name for the new dashboard.
4. To add a new widget to the dashboard, click **Add widget**.

The **Choose a widget** window appears.

5. Choose one of the widget types: Volume Bar and Donut, Asset Count, Line, Periodic, and so on. Click **Choose**.

A panel appears on the right with the parameters relevant for the selected widget.

You can configure the following parameters for a widget:

Note: All parameters may not be applicable for all widgets. Some widgets allow changes only to the panel name.

Parameters	Description
Panel Name	The name for the widget that appears on the dashboard.



System colors	<p>Apply system colors to the widget.</p> <p>To apply a color:</p> <ol style="list-style-type: none">Select a color in the System colors bar for the widget. <p>The selected color appears in the Custom color box.</p>
Data Source type	<p>The data source to populate the widgets in the dashboard.</p> <p>To select a data source type:</p> <ol style="list-style-type: none">From the Data Source type drop-down box, select a data source type. <p>The options relevant for that widget appear. For example, in a Line widget, selecting the "Subscription" data source type displays a list of available subscription-related data sources to populate the chart.</p> <ol style="list-style-type: none">From the drop-down menu, select the required data sources.
Column	<p>The asset column data to populate the widgets in the dashboard. For example, widgets such as the Donut and Bar includes the Column drop-down option.</p> <p>To add a column:</p> <ol style="list-style-type: none">From the Column drop-down box, select a column name. For example, Severity, Record Type, or Country.(Optional) Click +Add Filter to filter the column using Legacy Filtering.

6. Click **Save changes**.

Tenable Attack Surface Management adds the widget to the dashboard.

7. (Optional) Click **Add Row** if you want to add a new row in the same widget.


8. In the upper-right corner, click **Save changes**.



Tenable Attack Surface Management saves the new dashboard, which now appears on the left pane.

View Assets

You can access the assets inventory page from any of the widgets on the dashboard.

1. In Tenable Attack Surface Management, in the upper-right corner, click the  button.

The **Dashboards** page appears.

2. Click the widget for which you want to view the assets.

Tenable Attack Surface Management opens the asset inventory page and displays assets based on the filter applied to the widget. For example, for the **Detected Services** widget, the assets page appears with the filter `WebServices is apache`.

Edit a Dashboard

You can add or modify widgets in a dashboard.

1. In Tenable Attack Surface Management, in the upper-right corner, click the  button.



The **Dashboards** page appears.

2. In the upper-right corner, click  **Edit**.



The dashboard appears in edit mode.

3. Hover over the widget you want to edit.

Tenable Attack Surface Management displays available options.

Option	Description
Hide missing data/ Show missing data	<p>This option is only for specific widgets, such as a Map widget.</p> <p>To show or hide missing data:</p> <ol style="list-style-type: none">a. Click  Hide missing data to hide.b. Click  Show missing data to show.



Edit Widget	<p>To edit a widget:</p> <ol style="list-style-type: none">Click  Edit widget. <p>The Edit widget window appears.</p> <ol style="list-style-type: none">Modify the settings as needed.Click Save changes. <p>Tenable Attack Surface Management saves the changes to the widget and returns to the dashboard.</p>
Delete Widget	<p>To delete a widget:</p> <ol style="list-style-type: none">Click  Delete Widget. <p>Tenable Attack Surface Management asks for confirmation before deleting.</p> <ol style="list-style-type: none">Click Yes, delete to delete the widget. <p>Tenable Attack Surface Management deletes the widget and returns to the dashboard.</p>

- In the upper-right corner, click **Save changes**.

Tenable Attack Surface Management saves the changes to the dashboard.

Delete a Dashboard

You can delete custom dashboards.

To delete a dashboard:

- In Tenable Attack Surface Management, in the upper-right corner, click the  button.

The **Dashboards** page appears.

- In the upper-right corner, click  **Edit**.

The dashboard appears in edit mode.

- In the upper-right corner, click **Delete Dashboard**.



A confirmation message appears.

4. Click **Yes, delete**.

Tenable Attack Surface Management deletes the dashboard and returns to the dashboard page.


5. In the upper-right corner, click **Save changes** to save the changes to the dashboard.

Tenable Attack Surface Management deletes the dashboard.

Export a Dashboard

You can export your customized dashboard to a PDF format and share it with your organization.

To export a dashboard:

1. In Tenable Attack Surface Management, in the upper-right corner, click the  button.

The **Dashboards** page appears.

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

Tenable Attack Surface Management downloads and opens the dashboard in a PDF format.

Copy a Dashboard

You can create a copy of the **ASM Asset Dashboard** or a custom dashboard and modify its settings to create a new dashboard.

To copy a dashboard:

1. In Tenable Attack Surface Management, in the upper-right corner, click the  button.

The **Dashboards** page appears.

2. In the upper-right corner, click  **Copy**.

Tenable Attack Surface Management creates a copy of the dashboard and it appears on the left pane.

Categories of Security Risk

The Categories of Security Risk panel of Tenable Attack Surface Management provides a high-level overview of your assets by listing the critical events in your organization along with the number of your affected assets.

Categories of Security Risk

217 Outdated Version of Apache - v1 Compliance -3.13%

235 Outdated Version of WordPress - v2 Compliance 5.86%

2,832 RBLs - v1 Exposure -0.07%

>=10,000 Weak S... Comp

Search... Enter filter query...

Sort by Asset Count - High to Low

Group By

941,340 Assets Export All Columns 1 to 50 of 941,340 Page 1 of 18,827

Host	Severity	Record Type	IP Address	ASN	Ports	Screenshot	Tags
	Low	A			443	-	-
	None	CNAME			80, 443	-	Test Tag
	None	A			-	-	-
	None	A			80, 443		-
	None	A			80, 443	-	-
	High	A			80, 443		-
	None	A			-	-	-

To view the Categories of Security Risk panel:

1. In the left navigation bar, click the  button.


The **Explore** page appears.

2. View the **Categories of Security Risk** panel.

You can view the following details on the panel:

- List of critical events or triage items in the order of their severity level with the number of affected assets and the category of the event. The events appear in the order of their severity levels – the most important ones appear first. Each triage item also displays the difference in the previous and current number of affected assets as a percentage. Event names are based on the [subscription](#) templates (**Saved Queries** in the **Explore** dashboard).



- Tenable Attack Surface Management automatically refreshes the list daily. To refresh the data, click  > **Refresh**. Once you click **Refresh**, the option gets disabled for an hour accordingly.
- Click an event name to view the assets with the applied filters on the **Inventory** page.



TXT Records

On the **TXT records** page, you can view all text files in your inventory identified by Tenable Attack Surface Management.

To view your text records:

1. In Tenable Attack Surface Management, in the left navigation bar, click the  button.

The **TXT records** page appears. The TXT records table includes the following details:

Column	Description
Host	The hostname of the asset.
Value	The value of the text record.

2. In the left navigation pane, use the **Search** box to search for a specific record or select the required record.

Tenable Attack Surface Management displays the list of hostnames and the associated text records.

3. (Optional) Use the filter to view specific text records.

1. At the top of the table, click  **Add Filter**.

The Add Filter drop-down appears.

2. Use the **Search for Filters** box or select the filter from the list: **Hostname** or **Record Value**.

The list of operators appears.

3. Select the operator. For example, **contains**.

4. Type the value of the filter, if needed.

5. Click **Done**.

6. (Optional) To add another filter, click  **Add Filter**.



1. Repeat steps from 2 to 5.

Tenable Attack Surface Management adds a new third filter to the list with the following options:

- **that match all filters** – Lists only the assets that match all the filters.
- **that match any filters** – Lists assets that match any one of the filters.

2. Select one of the options and click **Done**.

Tenable Attack Surface Management shows the filtered results.



User Profile

Your user profile displays information about your account and your user settings. On this page, you can manage your personal information, set up multi-factor authentication, and manage your API keys.

To view your profile, in the upper right corner, click your profile picture or initials.

Basic Info

In this section, you can upload a profile photo and update your first name, last name, and email address.

Multi-Factor Authentication

In this section, you can enable multi-factor authentication.

To configure multi-factor authentication:

1. In the upper right corner, click your profile picture or initials.

Your user profile appears.

2. In the **MFA** section, click the slider to enable multi-factor authentication.
3. Log out of Tenable Attack Surface Management and log back in.

You will be prompted to select an authenticator app.

4. Select an authenticator app and follow the setup instructions.

Note: Save the provided backup codes in case you lose the device with your authenticator app.

5. Type your multi-factor authentication code from your authenticator app and finish logging in to Tenable Attack Surface Management.

Each time you log in to Tenable Attack Surface Management, you will be prompted to enter the code.

API Keys



In this section, you can manage and copy your API keys. For more information about the Tenable Attack Surface Management API, see the [Tenable Attack Surface Management API documentation](#).

Generate API Keys

The API keys associated with your user account allow you to access the Tenable Attack Surface Management APIs. You can generate two types of API keys:

- API keys that only give access to data in the current inventory, which you can also use to obtain API keys for other inventories.
- API key that can grant access only to the current inventory.

To generate API keys:

1. In the upper right corner, click your profile picture or initials.

Your user profile appears.

2. Do one of the following:

- To generate API keys for all your inventories: In the **API Key for all your inventories** section, click **Copy API Key**.

You can click **Generate new key & invalidate current** to generate a new key, if needed.

- To generate an API key for your inventory: In the **API Key for <your inventory name>** section, click **Copy API Key**.

Note: If you click **Invalidate all old keys**, Tenable Attack Surface Management logs you out and invalidates all your old keys. When you log in again, Tenable Attack Surface Management generates new keys.

You can now use the API keys to pull assets from all your inventories or grant access to your inventory.

For more information about the Tenable Attack Surface Management API, see the [Tenable Attack Surface Management API documentation](#).

Manage Integrations



You can integrate Tenable Attack Surface Management with AWS, Cloudflare, and Azure. This allows you to add the assets data from these sources to your inventory. You can also integrate Tenable Attack Surface Management with Tenable Vulnerability Management allows you to send real-time data into Tenable Vulnerability Management and enhance its existing Host data with external attack surface context.

You can manage all your integrations from the **Integrations** page.

[Add Integrations](#)

[Filter by Integration Type](#)

[Edit Integration](#)

[Delete Integration](#)

[Integrate with Cloudflare](#)

[Integrate with AWS](#)

[Integrate with AWS Using Keyless Authentication](#)

[Configure AWS for Keyless Authentication](#)

[Integrate with Microsoft Azure](#)

[Integrate with Azure Using Keyless Authentication](#)

[Configure Azure for Keyless Authentication](#)

[Integrate with Tenable Vulnerability Management](#)

[Asset Deletion](#)

[Accessing Tenable Attack Surface Management in Tenable Vulnerability Management](#)

[Integrate with Tenable Web App Scanning](#)

[Asset Deletion](#)

[Accessing Tenable Attack Surface Management in Tenable Web App Scanning](#)

[Integrate with Google Cloud Platform](#)

[Integrate with GCP Using Keyless Authentication](#)

[Configure GCP for Keyless Authentication](#)



[Cloud Assets](#)

[View Cloud Assets](#)

[View Asset Details for Host and Web Application Assets](#)

[Automatic Population of Primary Domains of a Container](#)

To access your integrations page:

1. In the left navigation bar, click the  button.



The **All Integrations** page appears.

Add Integrations

Before you begin

- For Cloudflare integration, make sure that you have the API keys generated from your Cloudflare account.
- For AWS integration, make sure that you have the API keys generated from your AWS account.
- For Azure integration, make sure that you have the API keys generated from your Azure account.

To add integrations:

1. Do one of the following:
 - In the upper-right corner, click  **Add**.
 - In the bar above the table, click  **Add**.
 - In the Integrations table, click **Add your first one**, if you are adding the integration for the first time,

A drop-down appears with these options: Tenable, Cloudflare, and AWS.

2. Select the required product for integration.

The **Add Integration** window for the selected product appears.



- [Integrate with Cloudflare](#)
- [Integrate with Tenable Vulnerability Management](#)
- [Integrate with AWS](#)
- [Integrate with AWS Using Keyless Authentication](#)
- [Integrate with Microsoft Azure](#)
- [Integrate with Azure Using Keyless Authentication](#)
- [Integrate with Google Cloud Platform](#)
- [Integrate with GCP Using Keyless Authentication](#)

3. Click **Add**.

Tenable Attack Surface Management saves the integration and lists the integration in the **All Integrations** table.

Filter by Integration Type

To filter by type, in the left navigation pane, click **Tenable**, **Cloudflare**, **AWS**, or **Azure** to view only the integrations for the selected type.

Edit Integration

To edit an integration:

1. In the row of the integration you want to edit, click the  button.

A list of options appears.

2. Select **Edit**.

The Edit window for the respective integration type appears.

3. Modify the values as needed.
4. Click **Save**.





Tenable Attack Surface Management saves the integration.



Delete Integration

To delete an integration:

1. Do one of the following:

Scope	Action
Delete a single integration	<ol style="list-style-type: none">1. Do one of the following:<ul style="list-style-type: none">• In the row of the integration you want to edit, click the  button.A list of options appears.<ul style="list-style-type: none">• Select the checkbox next to the integration you want to delete.Tenable Attack Surface Management enables the action bar at the top of the table.2. Click  Delete.
Delete multiple integrations	<ol style="list-style-type: none">1. Select the checkboxes next to the integrations you want to delete. Tenable Attack Surface Management enables the action bar at the top of the table. <ol style="list-style-type: none">2. Click  Delete.
Delete all integrations	<ol style="list-style-type: none">1. Select the integrations checkbox at the top of the table to select all integrations. Tenable Attack Surface Management enables the action bar at the top of the table. <ol style="list-style-type: none">2. Click  Delete.

Tenable Attack Surface Management deletes the integrations.

Integrate with Cloudflare



You can integrate Tenable Attack Surface Management with your Cloudflare account to add assets data from Cloudflare to your inventories.

Before you begin

- Make sure that you have the API keys generated from your Cloudflare account.

To integrate Cloudflare with Tenable Attack Surface Management:



1. In the left navigation bar, click the  button.

The **All Integrations** page appears.

2. In the left navigation pane, click **Cloudflare**.

The Cloudflare integrations page appears.

3. Do one of the following:

- In the upper-right corner, click  **Add Cloudflare**.
- In the bar above the table, click  **Add Cloudflare**.

The **Add Cloudflare Integration** window appears.

4. In the **Name** box, type a name for the integration.
5. In the **API Key** box, provide the API key for your Cloudflare account.
6. Click **Add**.

Tenable Attack Surface Management saves the integration and lists the integration in the Integrations table. Once the integration is complete, you can add sources from Cloudflare. For more information, see [Add sources from Cloudflare](#).

Integrate with AWS

You can integrate Tenable Attack Surface Management with your AWS account to add sources from AWS to your inventories. Tenable Attack Surface Management pulls data from the following sources:



- Amazon EC2
- Amazon Relational Database Service (RDS)
- Amazon S3
- Amazon Elastic Kubernetes Service (EKS)
- Amazon ElastiCache
- AWS Elastic Beanstalk
- Amazon Route 53
- Amazon OpenSearch / ElasticSearch

Before you begin

- Make sure that you have the Access key and Secret key generated from your AWS account. For more information, see [ReadOnlyAccess](#) in the AWS documentation.

To integrate AWS with Tenable Attack Surface Management:



1. In the left navigation bar, click the  button.

The **All Integrations** page appears.

2. In the left navigation pane, click **AWS**.

The **AWS** integrations page appears.

3. Do one of the following:

- In the upper-right corner, click  **Add AWS**.
- In the bar above the table, click  **Add AWS**.

The **Add AWS Integration** window appears.

4. In the **Name** box, type a name for the integration.
5. In the **Access Key** box, provide the access key for your AWS account.
6. In the **Secret key** box, provide the secret key for your AWS account.
7. Click **Add**.



Tenable Attack Surface Management saves the integration and lists it in the Integrations table. Once the integration is complete, you can add sources from AWS. For more information, see [Add Sources from AWS](#).

Note: You cannot modify the keys after they are added. You can only rename or delete the AWS key.



Integrate with AWS Using Keyless Authentication

You can configure Tenable Attack Surface Management to pull data from AWS using keyless authentication.

Before you begin

- [Configure AWS for Keyless Authentication](#).
- Make sure that your role has the `ReadOnlyAccess` privilege.




Note: Tenable Attack Surface Management does not make any modifications in your AWS account, but you must make sure that the keys have read-only privileges. For example, you can use the AWS-managed policy: `ReadOnlyAccess`.

- Make sure that you have the ARN of the role you created when [configuring](#) AWS for keyless authentication.

To integrate AWS with Tenable Attack Surface Management using keyless authentication:

1. In the left navigation bar, click the  button.

The **All Integrations** page appears.

2. Do one of the following:
 - In the **All Integrations** page, click  **Add > AWS - Keyless**.
 - In the upper-right corner, click  **Add > AWS - Keyless**.
 - In the bar above the table, click  **Add > AWS - Keyless**.

The **Add AWS - Keyless Integration** window appears.

3. In the **Name** box, type a name for the integration.
4. In the **Role ARN** box, provide the ARN value associated with the AWS role you created for this integration. For more information, see [Configure AWS for Keyless Authentication](#).
5. Click **Add**.

Tenable Attack Surface Management adds the integration.

Configure AWS for Keyless Authentication



Before you integrate AWS with keyless authentication, you must first configure AWS.

Before you begin

Make sure that you have the following:

- AWS access to manage IAM.
- Tenable Vulnerability Management Container UUID, which you can copy from the **Integrations** > **Add AWS-Keyless Integration** dialog box. For more information, see [Integrate with AWS Using Keyless Authentication](#).

To configure AWS for keyless authentication:

Via CLI

1. Create the IAM role with the trust relation policy.

```
aws iam create-role --role-name TenableASMCloudConnector --assume-role-policy-document \  
'{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "TenableCloudConnectorAccess",  
      "Effect": "Allow",  
      "Principal": {  
        "AWS": "arn:aws:iam::939095807864:role/tenable-data-aws-connector"  
      },  
      "Action": "sts:AssumeRole",  
      "Condition": {  
        "StringEquals": {  
          "sts:ExternalId": "<CONTAINER_UUID>"  
        }  
      }  
    }  
  ]  
}' \
```

Where:

- 939095807864 is the Tenable's AWS account ID.
- CONTAINER_UUID is the Tenable Vulnerability Management container ID.



- `TenableASMCloudConnector` is the name of the IAM role. Replace it with a name of your choice.
2. Assign read-only permission to the role.

```
aws iam attach-role-policy --role-name TenableASMCloudConnector --policy-arn
arn:aws:iam::aws:policy/ReadOnlyAccess
```

Note: You can use your own read-only access role if you don't want to use the default role.

Where:

- Replace `TenableASMCloudConnector` with the name of the IAM role you created in Step 1.

3. Copy the ARN value.

```
aws iam get-role --role-name TenableASMCloudConnector
```

Where:

- `TenableASMCloudConnector` is the name of the IAM role you created in Step 1.

Via AWS UI

1. On the AWS Management Console, go to **IAM > Roles > Create role**.

The **Create role** page appears.

2. In the **Select trusted entity** page, select **Custom trust policy**.
3. In the **Custom trust policy** box, enter or paste the following policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "TenableCloudConnectorAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::939095807864:role/tenable-data-aws-connector"
      },
      "Action": "sts:AssumeRole",
```




```
    "Condition": {
      "StringEquals": {
        "sts:ExternalId": "<CONTAINER_UUID>"
      }
    }
  ]
}
```

Where:

- 939095807864 is the Tenable AWS account_id.
- CONTAINER_UUID is the Tenable Vulnerability Management container ID.

4. Click **Next**.
5. The **Add Permissions** page appears.
6. Select the **ReadOnlyAccess** permission policy to assign to the role.
7. Click **Next**.

The **Name, review, and create** page appears.

8. In the **Role** name box, type the name of the role. For example: TenableASMCloudConnector.
9. Review the configuration details.
10. Click **Create role**.

AWS creates the IAM role.

11. Copy the ARN value to use in the AWS integration within Tenable Attack Surface Management.

What to do next

[Integrate with AWS Using Keyless Authentication](#)

Integrate with Microsoft Azure

You can integrate Tenable Attack Surface Management with Azure to add sources from Azure to your inventories. Tenable Attack Surface Management pulls data from the following sources:



- Azure App Service
- Azure DNS
- Azure Redis Cache
- Azure Virtual Machines
- MySQL in Azure
- MySQL Flexible in Azure
- PostgreSQL in Azure
- PostgreSQL Flexible in Azure
- MariaDB in Azure
- SQL in Azure

Before you begin

- Make sure that you register a new application in **App registrations** in Azure. For more information, see [Register an application](#) in the Azure documentation.
- Make sure that Azure keys have read-only privileges. For instance, you can use the Azure built-in **Reader** role. For more information, see [Azure built-in roles for General](#) in the Azure documentation.
- Make sure that you have the following Azure information:
 - Name
 - Tenant ID
 - Application ID
 - Client Secret

To integrate Azure with Tenable Attack Surface Management

1. In the left navigation bar, click the  button.

The **All Integrations** page appears.

2. In the left navigation pane, click **Azure**.



The **Azure** integrations page appears with a table that lists the integration name and type.

3. Do one of the following:

- In the upper-right corner, click **+ Add Azure**.
- In the header bar, click **+ Add Azure**.

The **Add Azure Integration** window appears.

4. In the **Name** box, type a name for the integration.
5. In the **Tenant ID** box, provide your tenant ID.
6. In the **Application ID** box, provide the application ID.
7. In the **Client Secret** box, provide the client secret.
8. Click **Add**.

Tenable Attack Surface Management saves the integration and lists it in the Integrations table. Once the integration is complete, you can add sources from Azure. For more information, see [Add Sources from Azure](#).



Integrate with Azure Using Keyless Authentication

You can configure Tenable Attack Surface Management to pull data from Azure using keyless authentication.

Before you begin

- [Configure Azure for Keyless Authentication.](#)




Note: You must add at least one Azure subscription, or the Tenable Attack Surface Management cannot validate the integration.

- Assign read-only permissions for the required subscriptions or resource groups. You can use the Azure-defined **Reader** role.
- Make sure that you have the following:
 - Application ID or the Client ID of the Managed Identity, which you can copy when [configuring](#) Azure for keyless authentication.
 - Tenant ID

To integrate AWS with Tenable Attack Surface Management using keyless authentication:

1. In the left navigation bar, click the  button.

The **All Integrations** page appears.

2. Do one of the following:
 - In the **All Integrations** page, click  **Add > Azure - Keyless.**
 - In the upper-right corner, click  **Add > Azure - Keyless.**
 - In the bar above the table, click  **Add > Azure - Keyless.**

The **Add Azure - Keyless Integration** window appears.

3. Check if the **subject identifier** appears by default. Copy the **Subject identifier** to configure Azure for keyless authentication. For more information, see [Configure Azure for Keyless Authentication.](#)



4. In the **Name** box, type a name for the integration.
5. In the **Tenant ID** box, provide the tenant ID.
6. In the **Application ID** box, provide the application ID or the client ID of the managed identity.
7. Click **Add**.

Tenable Attack Surface Management adds the integration.

Configure Azure for Keyless Authentication

To integrate with Azure, you must first configure Azure for keyless authentication.

Before you begin

Make sure that you have:

- A valid Azure subscription.
- The **Subject identifier** from the **Integrations > Add Azure - Keyless Integration** dialog box in Tenable Attack Surface Management. For more information, see [Integrate with Azure Using Keyless Authentication](#).
- Azure Subscription ID.
- Azure Resource Group Name.

To configure Azure for keyless authentication:

Via CLI

1. Create a managed identity.

```
az identity create -n TenableCloudConnectors --subscription <subscription-name> -g <resource-group-name>
```

Where:



- TenableCloudConnectors is the name of the managed identity.
- subscription-name is the Azure subscription name.
- resource-group-name is the group to which the managed identity belongs.

2. Assign the **Reader** role for the managed identity.

```
az role assignment create --assignee-object-id <managed-identity-id> --role "Reader" --scope  
"/subscriptions/<subscription-id>"
```

Where:

- managed-identity-id is the ID of the managed identity you created in Step 1.
- subscription-id is the Azure subscription ID that has read access.

3. Add Federated credentials for the managed identity.

```
az identity federated-credential create --name TenableASMCloudConnector --identity-name  
TenableCloudConnectors --resource-group <resource-group-name> --audiences us-east-1:96e4d72b-  
7a36-4dc6-a64e-7baae60e027f --issuer https://cognito-identity.amazonaws.com --subject  
<UUIDfromTheASMUI> --subscription <subscriptionID>
```

Where:

- TenableASMCloudConnector is the name of the federated credential.
- TenableCloudConnectors is the name of the managed identity you created in **Step 1**.
- resource-group-name is the resource group to which the managed identity belongs.
- UUIDfromtheASMUI is the **Subject identifier** that you copied from the **Integrations > Add Azure Keyless Integrations** dialog box in Tenable Attack Surface Management.

4. Copy the client ID of the Managed Identity.

```
az identity show -n TenableCloudConnectors --resource-group <resources-group>
```

Where:



- TenableCloudConnectors is the name of the managed identity you created in **Step 1**.
- resource-group-name is the resource group to which the managed identity belongs.

Via Azure UI

To configure Azure for keyless authentication:

1. Sign in to the Azure portal.
2. To create a new managed identity, in the **All Services** page, under **Identity Management**, select **Managed Identities**.
3. Click **Create**.
4. Provide the details and create the managed identity.
5. In the left navigation pane of the managed identity, select **Azure role assignments**.
6. Click **Add role**.
7. Select your subscription and resource group, then select the role as **Reader**.
8. Click **Save**.

Azure saves the role.

9. To add **Federated credentials**, in the left navigation pane, select **Settings > Federated credentials**.

The **Federated credentials** pane appears on the right.

10. Click **Add Credential**.

The **Add Federated Credential** page appears.

11. In the **Federated credential scenario** drop-down box, select **Other Issuer**.

The **Select a managed identity** section appears.

12. In the **Issuer** box, type `https://cognito-identity.amazonaws.com`.
13. In the **Subject identifier** box, copy the subject identifier from the **Add Azure - Keyless Integration** dialog box in Tenable Attack Surface Management.



14. In the **Credential details** section, provide a name, then in the **Audience** box, type `us-east-1:96e4d72b-7a36-4dc6-a64e-7baae60e027f`.
15. Copy the **Client ID** from the **Managed Identity's Overview** page. You need the client ID when integrating the Azure with Tenable Attack Surface Management.

What to do next

[Integrate with Azure Using Keyless Authentication](#)

Integrate with Tenable Vulnerability Management

You can integrate Tenable Attack Surface Management with Tenable Vulnerability Management to provide continuous external attack surface monitoring and deliver real-time data for ingestion into the platform. This integration enhances the Tenable Vulnerability Management Host data with external attack surface context. You can perform deep vulnerability scans against this data, which helps identify the security risk present in exposed vulnerabilities and provides you with a workflow for managing vulnerability findings.

You have complete control of enabling and tailoring the data scope flowing from Tenable Attack Surface Management to Tenable Vulnerability Management. There are several customization options, including complex filters, that you can apply globally or per inventory to ensure assets considered for Tenable Vulnerability Management Host creation fit your team's view of the external world.

Note: If there is no filter added, all data in Tenable Attack Surface Management is ingested into Tenable Vulnerability Management.

Before you begin

- Make sure that your Tenable Vulnerability Management container has a valid Tenable Attack Surface Management license.

To modify filters that control the data that Tenable Attack Surface Management sends to Tenable Vulnerability Management:





1. In the left navigation bar, click the  button.

The **All Integrations** page appears.

2. In the left navigation pane, click **Tenable**.

The **Tenable** integrations page appears with a table that lists the integration name and type.

3. Do one of the following:

- In the upper-right corner, click  **Add Tenable**.
- In the bar above the table, click  **Add Tenable**.

Tenable Attack Surface Management opens the window to update global and inventory settings.



Tenable Vulnerability Management Integration

GLOBAL SETTINGS

Affects all inventories

Custom Network UUID

Default

Asset Identification

Identify assets by IP address

Ingestion Filters

Enter filter query... Set

INVENTORY SETTINGS

☒ Enable Ingestion for Inventory Demo Inventory

Clear Overrides

Custom Network UUID *

Default

Asset Identification

Identify assets by Hostname

Ingestion Filters

Matching all assets Set

* defaulting to global settings

Save Cancel

Note: After the integration with Tenable Vulnerability Management is complete, the **Add Tenable** button is disabled.

4. In the **Global Settings** section, do the following:



Note: **Global Settings** affect all inventories.

- a. In the **Custom Network UUID** drop-down box, select the UUID of your network. The networks created in Tenable Vulnerability Management appear in this list.
- b. To identify assets based on the hostname or the IP address, select one of the following from the **Asset Identification** drop-down box:

- **Identify assets by Hostname**
- **Identify assets by IP address**

For more information, see [Asset Identification Characteristics](#).

- c. In the **Ingestion Filters** box, provide filters and click **Set**. For more information about adding filters, see [Asset Filters](#).
5. (Optional) In the **Inventory Settings** section, click the **Enable Inventory Settings** toggle to enable settings for the current inventory.

Note: **Inventory Settings** affect only the current inventory.

Tenable Attack Surface Management enables the inventory setting parameter fields.

Tip: The * next to the inventory settings indicate that the default values for these parameters are the global configuration settings. Click **Clear Overrides** to reset to the default global setting values.

- a. In the **Custom Network UUID** drop-down box, select the UUID of your network. The networks created in Tenable Vulnerability Management appear in this list.
 - b. To identify assets based on the hostname or the IP address, select one of the following from the **Asset Identification** drop-down box:
 - **Identify assets by Hostname**
 - **Identify assets by IP address**
 - c. In the **Ingestion Filters** box, provide filters and click **Set**. For more information about adding filters, see [Asset Filters](#).
- 6.



Note: When you click the **x** button in the **Ingestion Filters** box, Tenable Attack Surface Management does the following:

- Clears overrides and sets the filters to the default global filter settings.
- Displays a **Match all assets** link. When you click on the link, Tenable Attack Surface Management updates the **Ingestion Filters** option to **Matching all assets**

Tenable Vulnerability Management Integration

GLOBAL SETTINGS

Affects all inventories

Custom Network UUID

Default

Asset Identification

Identify assets by IP address

Ingestion Filters

Enter filter query...

Set

INVENTORY SETTINGS



Enable Ingestion for Inventory: ASM-New-App

Clear Overrides

Custom Network UUID *

Default

Asset Identification

Identify assets by Hostname

Ingestion Filters *

Enter filter query...

Set

Column

Final url

Redirect Chain

Final response code

* defaulting to global settings

Save

Cancel

7. Click **Save**.



Tenable Attack Surface Management saves the integration. Tenable Vulnerability Management now ingests data based on the modified filters and displays the assets that match the filters.

The [example](#) given in the procedure shows that you can divide your assets into different inventories to apply different types of configuration based on your requirements, for instance, in the image:

- Global settings are configured to ingest any asset with any open ports identified by their IP addresses.
- Inventory settings are configured to use an inventory with assets that use elastic IPs identified by their hostnames.


See Also

[Asset Deletion](#)

Asset Deletion

When you delete assets created as part of the Tenable Vulnerability Management integration:

- Tenable Attack Surface Management does not report the asset again.
- You can view and restore the deleted assets list in Tenable Attack Surface Management.

Caution: When you disable or delete the Tenable Vulnerability Management integration from the  > **Integrations** page, Tenable Attack Surface Management removes all assets created during the integration. But if other sensors also detected these assets, Tenable Attack Surface Management does not delete them.

View Deleted Assets

When you delete an asset with the **External Asset** source tag in Tenable Vulnerability Management, Tenable Attack Surface Management does not recreate the deleted asset. You can view the list of previously deleted assets in chronological order, perform sub-string searches across them, and restore them where necessary.

To view deleted assets:

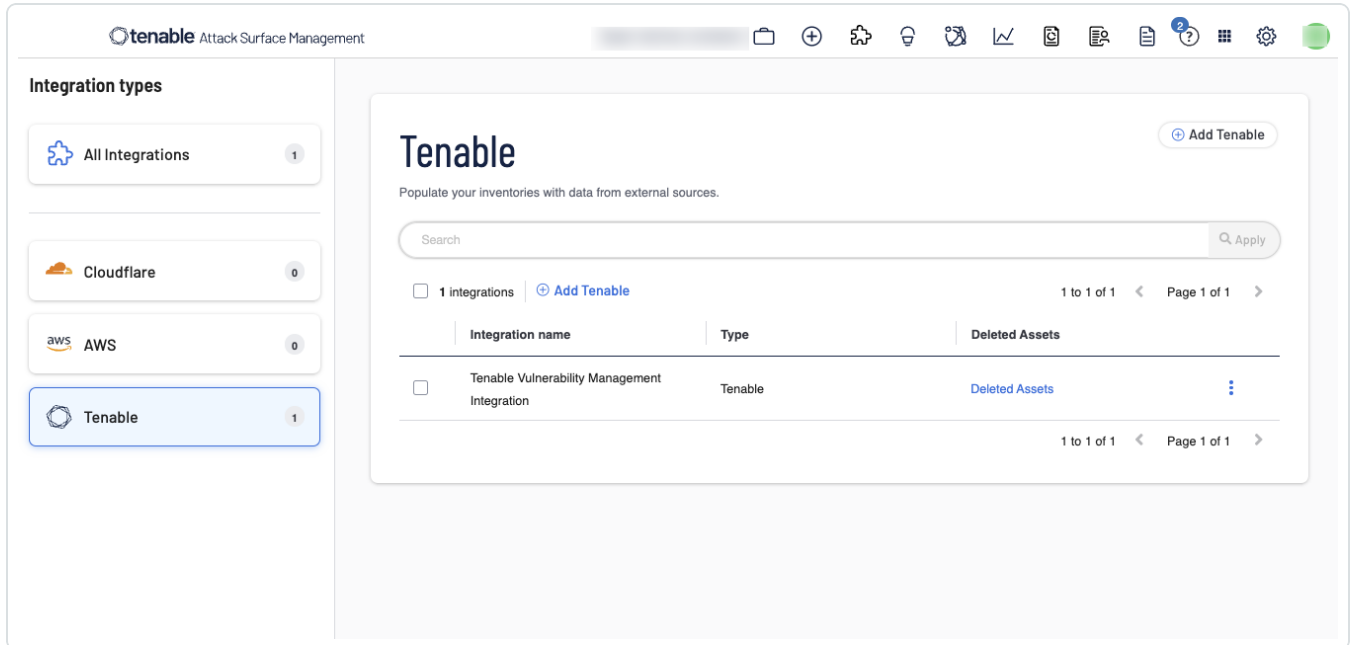


1. In the left navigation bar, click the  button.

The **All Integrations** page appears.

2. In the left navigation pane, click **Tenable**.

The **Tenable** integrations page appears with a table that lists the integration name and type.



The screenshot shows the Tenable Attack Surface Management interface. On the left, the 'Integration types' sidebar lists 'All Integrations' (1), 'Cloudflare' (0), 'AWS' (0), and 'Tenable' (1). The main panel is titled 'Tenable' and includes a search bar and a table of integrations. The table has columns for 'Integration name', 'Type', and 'Deleted Assets'. One integration is listed: 'Tenable Vulnerability Management Integration' with type 'Tenable'. A link 'Deleted Assets' is visible in the 'Deleted Assets' column.

Integration name	Type	Deleted Assets
Tenable Vulnerability Management Integration	Tenable	Deleted Assets

3. In the **Deleted Assets** column, click **Deleted Assets**.

The **Tenable Deleted Assets** page appears with the list of deleted assets in chronological order.



Tenable Deleted Assets

Manually deleted assets from the Vulnerability Management and Web App Scanning sections of the Tenable Web Portal will appear here and won't be recreated if listed by hostname or IP. Restoring them will recreate all associated assets.

[Filter](#)[Refresh](#)[Restore assets](#)**Asset Type****Hostname / IP****Deleted At**

Host

2024-11-25T18:58:37.719Z



Host

2024-11-25T18:58:37.228Z



Host

2024-11-25T18:58:37.203Z



Host

2024-11-25T18:58:36.723Z

[<](#) Page 1 [>](#)

Note: Manually deleted assets from the Tenable Attack Surface Management and Tenable Vulnerability Management integration appear here and they are not recreated if listed by hostname or IP. Restoring them recreates all associated assets.

Restore Assets

You can restore assets manually when you need.

To restore an asset:

- To restore a single asset:
 - In the row of the asset you want to restore, click > **Restore Asset**.
 - Select the checkbox next to an asset. This enables **Restore assets** at the top of the table. Click **Restore assets**.
- To restore multiple assets:
 - Select one or more checkboxes next to assets to restore. This enables **Restore assets** at the top of the table. Click **Restore assets**.

Tip: Use the **Search** box to filter and search for specific assets.



Tenable Deleted Assets

Manually deleted assets from the Vulnerability Management and Web App Scanning sections of the Tenable Web Portal will appear here and won't be recreated if listed by hostname or IP. Restoring them will recreate all associated assets.

Filter Refresh Restore assets

<input checked="" type="checkbox"/>	Asset Type	Hostname / IP	Deleted At	
<input checked="" type="checkbox"/>	Host		2024-11-25T18:58:37.719Z	⋮
<input checked="" type="checkbox"/>	Host		2024-11-25T18:58:37.228Z	⋮
<input checked="" type="checkbox"/>	Host		2024-11-25T18:58:37.203Z	⋮
<input checked="" type="checkbox"/>	Host		2024-11-25T18:58:36.723Z	⋮

< Page 1 >

Tenable Attack Surface Management restores the asset and it appears on the **Inventory** page. Use the **Refresh** button to refresh the page to show the updated assets list.

Accessing Tenable Attack Surface Management in Tenable Vulnerability Management

The data that Tenable Attack Surface Management discovers is ingested into Tenable Vulnerability Management to enrich Host asset data within the platform, which in turn can provide potential assessment targets.

To view the assets data:

- In Tenable Vulnerability Management, go to **Explore > Assets**.

Note: Make sure that you remove the default **Licensed assets** filter.

The **Assets** page appears with all assets in Tenable Vulnerability Management including the ones ingested from Tenable Attack Surface Management.

Integration Characteristics

Tenable Attack Surface Management and Tenable Vulnerability Management integration has the following characteristics:



- Real-time data is ingested into Tenable Vulnerability Management.

Note: Depending on the system load, it may take up to 24 hours for the data to synchronize with Tenable Vulnerability Management.

- You can configure global settings for network, asset identification, and ingestion filters at the time of integration. Optionally, you can enable or disable ingestion for the current inventory.
- Data is filtered based on the **Ingestion Filters** that you provide at the time of integration.
- Tenable Attack Surface Management identifies the assets based on IP address or hostname. This is configured as part of the global settings at the time of integration.
- Host assets are created based on Tenable Attack Surface Management parameters.
- Tenable Attack Surface Management ensures that the Host assets data in Tenable Attack Surface Management and Tenable Vulnerability Management matches completely.
- Tenable Attack Surface Management discovered assets are categorized as unlicensed or unscanned assets that are not counted towards your license.
- The **Source** column in the Assets table shows **External Asset** for the assets discovered by Tenable Attack Surface Management.
- Assets that the Tenable Attack Surface Management discovers via the passive discovery scan can later be scanned by Tenable Nessus.
- The Host assets data is enriched by including CPEs and Ports data.

Asset Identification Characteristics

The following are the characteristics of the asset identification types, IP address and hostname:

- Tenable Vulnerability Management considers the IP or hostname configuration only when an asset has the data to support it.
- If the source includes assets with wildcard DNS, the integration may lack sufficient information to come up with a real hostname. Tenable Attack Surface Management uses a *. notation for wildcard DNS, but it is not a real hostname. In such cases, the asset is identified by the IP address.



- If the source includes assets with elastic IPs, Tenable Attack Surface Management loses the IP information for assets within that source. In such cases, Tenable Attack Surface Management still creates the asset but by using FQDN to identify the asset.
- If the source includes both wildcard DNS and elastic IPs, Tenable Attack Surface Management may lack sufficient information to identify the public asset. In such cases, you can manually add the subdomains to Tenable Attack Surface Management sources by using the [Add Subdomain](#) option.

Host Asset Conditions

The following are the conditions for Tenable Attack Surface Management to create Host Assets:

- Considers only A and AAAA records.
- Filters assets globally by hostnames or IP addresses, and ingestion filters. You can also override the global setting by enabling the inventory settings.

Integrate with Tenable Web App Scanning

You can integrate Tenable Attack Surface Management with Tenable Web App Scanning. to provide continuous external attack surface monitoring and deliver real-time data for ingestion into the platform. This integration enhances the Tenable Web App Scanning. by identifying Web Applications on your perimeter. You can perform deep application scans against new targets, while any application already being scanned is noted as discovered by Tenable Attack Surface Management.

You have complete control of enabling and tailoring the data scope flowing from Tenable Attack Surface Management to Tenable Web App Scanning. There are several customization options, including complex filters, that you can apply globally or per inventory to ensure assets considered for Tenable Web App Scanning creation fit your team's view of the external world.

Note: If there is no filter added, all data in Tenable Attack Surface Management is ingested into Tenable Web App Scanning.

Note: These discovered web applications will also appear in Tenable Vulnerability Management, from which Web Applications Scans can also be launched.

Before you begin



- Make sure that your Tenable Web App Scanning container has a valid Tenable Attack Surface Management license.
- Make sure you are logged in to Tenable Attack Surface Management.



To modify filters that control the data that Tenable Attack Surface Management sends to Tenable Web App Scanning:

1. In the left navigation bar, click the  button.

The **All Integrations** page appears.

2. In the left navigation pane, click **Tenable**.

The **Tenable** integrations page appears with a table that lists the integration name and type.

3. Do one of the following:
 - In the upper-right corner, click  **Add Tenable**.
 - In the bar above the table, click  **Add Tenable**.

Note: After the integration with Tenable Web App Scanning is complete, the **Add Tenable** button is disabled.

A selection window appears:



All Integrations

Populate your inventories with data from external sources.

Search

☐ 0 integrations

Add Tenable Integration

Type

Tenable Web Application Scanning

Tenable Vulnerability Management

Tenable Web Application Scanning

Add

Cancel

4. Select **Tenable Web App Scanning**.

Tenable Web Application Scanning Integration

GLOBAL SETTINGS
Affects all inventories

Ingestion Filters

Enter filter query... Set

INVENTORY SETTINGS

☒ Enable Ingestion for Inventory: ...

Clear Overrides

Ingestion Filters

Domain is .com x Set

* defaulting to global settings

Save Cancel

Tenable Attack Surface Management opens the window to update global and inventory settings.

5. In the **Global Settings** section, do the following:

Note: **Global Settings** affect all inventories.

- a. In the **Ingestion Filters** box, provide filters and click **Set**. For more information about adding filters, see [Asset Filters](#).

6. In the **Inventory Settings** section, click the **Enable Inventory Settings** toggle to enable settings for the current inventory.

Note: **Inventory Settings** affect only the current inventory.



Tenable Attack Surface Management enables the inventory ingestion filter.

Tip: The * next to the inventory settings indicate that the default values for these parameters are the global configuration settings. Click **Clear Overrides** to reset to the default global setting values.

7. Click **Save**.

Tenable Attack Surface Management saves the integration.

Tenable Web App Scanning now creates new web applications based on the filters specified in the integration, which appear in the **Discovered** section of Tenable Web App Scanning. For any application which has already been scanned by Tenable Web App Scanning, a new application is not created. Instead, the application is matched, and a **Source** type of **ASM** (Tenable Attack Surface Management) is added to the application.


See Also:

[Asset Deletion](#)

Asset Deletion

When you delete assets created as part of the Tenable Web App Scanning integration:

- Tenable Attack Surface Management does not report the asset again.
- You can view and restore the deleted assets list in Tenable Attack Surface Management.


Caution: When you disable or delete the Tenable Web App Scanning integration from the  > **Integrations** page, Tenable Attack Surface Management removes all assets created during the integration. But if other sensors also detected these assets, Tenable Attack Surface Management does not delete them.

View Deleted Assets

When you delete an asset with the **ASM** source tag in Tenable Web App Scanning, Tenable Attack Surface Management does not recreate the deleted asset. You can view the list of previously deleted assets in chronological order, perform sub-string searches across them, and restore them where necessary.

To view deleted assets:



1. In the left navigation bar, click the  button.

The **All Integrations** page appears.

2. In the left navigation pane, click **Tenable**.

The **Tenable** integrations page appears with a table that lists the integration name and type.

Tenable

Populate your inventories with data from external sources.

Apply

☐ 1 integrations [Add Tenable](#) 1 to 1 of 1 < Page 1 of 1 >

Integration name	Type	Deleted Assets
<input type="checkbox"/> Tenable Web Application Scanning Integration	Tenable	Deleted Assets ⋮

1 to 1 of 1 < Page 1 of 1 >

3. In the **Deleted Assets** column, click **Deleted Assets**.

The **Tenable Deleted Assets** page appears with the list of deleted assets in chronological order.

Tenable Deleted Assets

Manually deleted assets from the Vulnerability Management and Web App Scanning sections of the Tenable Web Portal will appear here and won't be recreated if listed by hostname or IP. Restoring them will recreate all associated assets.

Filter Refresh

Asset Type	Hostname / IP	Deleted At
<input type="checkbox"/> WebApp	10.10.10.10	2025-03-05T19:55:57.898Z ⋮
<input type="checkbox"/> WebApp	10.10.10.10	2025-03-05T19:55:55.438Z ⋮
<input type="checkbox"/> WebApp	10.10.10.10	2025-03-05T19:55:52.360Z ⋮
<input type="checkbox"/> WebApp	10.10.10.10	2025-03-05T19:55:47.498Z ⋮

< Page 1 >


Note: Manually deleted assets from the Tenable Attack Surface Management and Tenable Web App Scanning integration appear here and they are not recreated if listed by hostname or IP. Restoring them recreates all associated assets.



Restore Assets

You can restore assets manually when you need.

To restore an asset:





- To restore a single asset:
 - In the row of the asset you want to restore, click  > **Restore Asset**.
 - Select the checkbox next to an asset. This enables **Restore assets** at the top of the table. Click **Restore assets**.
- To restore multiple assets:
 - Select one or more checkboxes next to assets to restore. This enables **Restore assets** at the top of the table. Click **Restore assets**.

Tip: Use the **Search** box to filter and search for specific assets.

Tenable Deleted Assets

Manually deleted assets from the Vulnerability Management and Web App Scanning sections of the Tenable Web Portal will appear here and won't be recreated if listed by hostname or IP. Restoring them will recreate all associated assets.

Filter Refresh**Restore assets**

<input checked="" type="checkbox"/>	Asset Type	Hostname / IP	Deleted At	
<input checked="" type="checkbox"/>	WebApp	192.168.1.1	2025-03-05T19:55:57.898Z	
<input checked="" type="checkbox"/>	WebApp	192.168.1.2	2025-03-05T19:55:55.438Z	
<input checked="" type="checkbox"/>	WebApp	192.168.1.3	2025-03-05T19:55:52.360Z	
<input checked="" type="checkbox"/>	WebApp	192.168.1.4	2025-03-05T19:55:47.498Z	

< Page 1 >

Tenable Attack Surface Management restores the asset and it appears on the **Inventory** page. Use the **Refresh** button to refresh the page to show the updated assets list.

Accessing Tenable Attack Surface Management in Tenable Web App Scanning



The data that Tenable Attack Surface Management discovers is ingested into Tenable Web App Scanning to enrich asset data within the platform, which in turn can provide potential assessment targets.

To view the assets data:

- In Tenable Web App Scanning, go to **Applications > Discovered**.

The **Discovered** table shows **Applications** which have been discovered by Tenable Attack Surface Management, but not yet scanned by Tenable Web App Scanning. Once the applications are scanned, they move from **Discovered** to **Scanned**.

Integration Characteristics

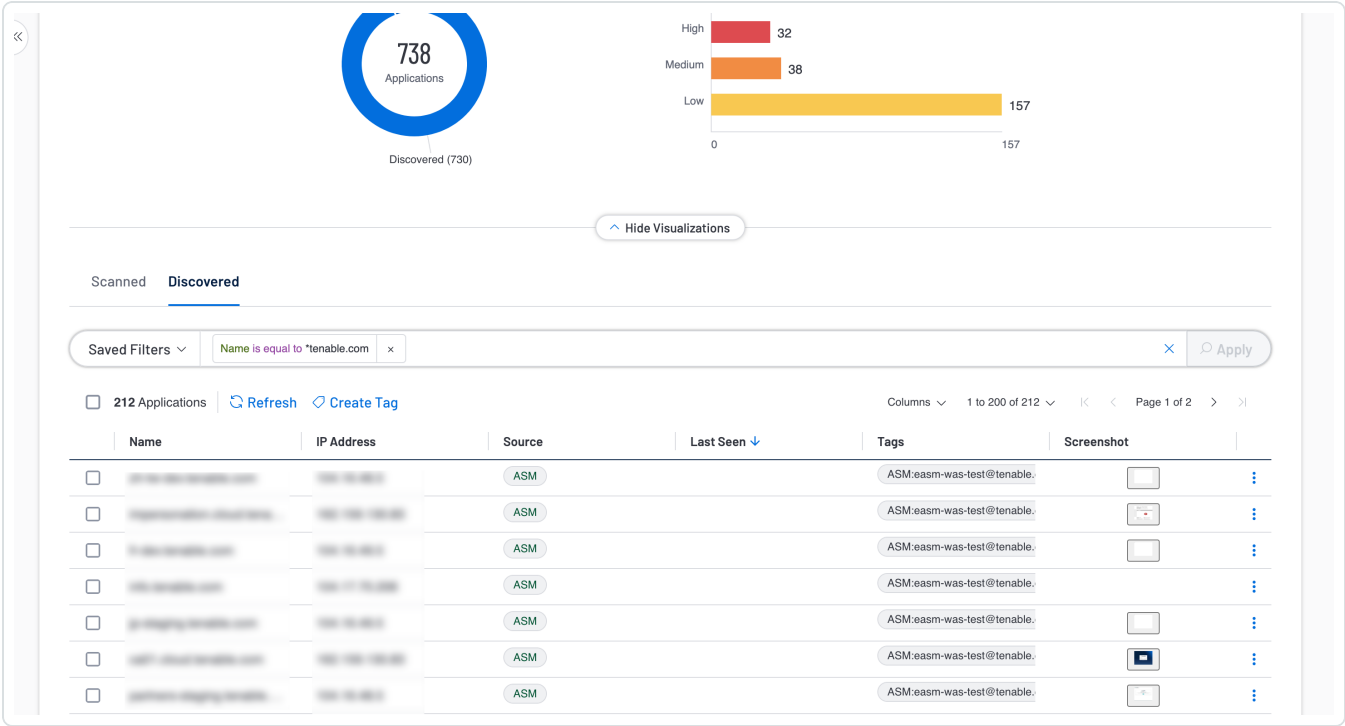
Tenable Attack Surface Management and Tenable Web App Scanning integration has the following characteristics:

- Real-time data is ingested into Tenable Web App Scanning.

Note: Depending on the system load, it may take up to 24 hours for the data to synchronize with Tenable Web App Scanning.

- You can configure global settings for network, asset identification, and ingestion filters at the time of integration. Optionally, you can enable or disable ingestion for the current inventory.
- Data is filtered based on the **Ingestion Filters** that you provide at the time of integration.
- Web application assets are created based on Tenable Attack Surface Management parameters.
- Tenable Attack Surface Management ensures that the web application assets data in Tenable Attack Surface Management and Tenable Web App Scanning matches completely.
- Tenable Attack Surface Management discovered assets are categorized as unlicensed or unscanned assets that are not counted towards your license.
- The **Source** column in any applications table show **ASM** for the assets discovered by Tenable Attack Surface Management.
- Tenable Attack Surface Management adds **Screenshots** for the web application assets that it

discovers:





Integrate with Google Cloud Platform

You can integrate Tenable Attack Surface Management with Google Cloud Platform to add sources from Google Cloud Platform to your inventories. Tenable Attack Surface Management pulls data from the following sources:

- Compute Engine
- Cloud DNS
- Google Kubernetes Engine (GKE)
- Cloud Load Balancers
- Google Cloud SQL
- Cloud Storage

Before you begin

- Make sure to have a service account with read only permissions. Tenable recommends you use Google's reader role for the service account. To check the service account permissions, click [here](#).

To integrate Google Cloud Platform with Tenable Attack Surface Management:

1. In the left navigation bar, click the  button.

The **All Integrations** page appears.

2. In the left navigation pane, click **Google Cloud Platform**.

The **Google Cloud Platform** integrations page appears with a table that lists the integration name and type.

3. Do one of the following:

- In the upper-right corner, click  **Add Google Cloud Platform**.
- In the header bar, click  **Add Google Cloud Platform**.

The **Add Google Cloud Platform Integration** dialog box appears.



4. In the **Name** box, type a name for the integration.
5. To upload the service account JSON file, click **Upload** and browse to the location of the file to upload it.

Tenable Attack Surface Management saves the integration and lists it in the Integrations table. Once the integration is complete, you can add sources from GCP. For more information, see [Add Sources from Google Cloud Platform](#).



Integrate with GCP Using Keyless Authentication

You can configure Tenable Attack Surface Management to pull data Google Cloud Platform using keyless authentication.

Before you begin




- [Configure GCP for Keyless Authentication](#).
- Make sure your account has read-only permissions. You can use the built-in GCP role: **Viewer**.
- Make sure that you [download](#) the configuration file that you obtained when configuring GCP.

Note: Tenable Attack Surface Management does not make any modifications in your Google Cloud Platform account, but you must make sure that the keys have read-only privileges.

To integrate Google Cloud Platform with Tenable Attack Surface Management using keyless authentication:

1. In the left navigation bar, click the  button.

The **All Integrations** page appears.

2. Do one of the following:
 - In the **All Integrations** page, click  **Add > Google Cloud Platform - Keyless**.
 - In the upper-right corner, click  **Add > Google Cloud Platform - Keyless**.
 - In the bar above the table, click  **Add > Google Cloud Platform - Keyless**.

The **Add Google Cloud Platform - Keyless Integration** window appears.

3. In the **Name** box, type a name for the integration.
4. Click **Upload** to upload the Workload Identity Federation file. For information about how to download the configuration file, see [Configure GCP for Keyless Authentication](#).
5. Click **Add**.

Tenable Attack Surface Management adds the integration.

Configure GCP for Keyless Authentication



To integrate Tenable Attack Surface Management with GCP Workload Identity Federation, you must create a workload identity pool in GCP. Then, you must add a provider to the pool, grant access to the provider, and download the credential configuration file. Use this configuration file when integrating Tenable Attack Surface Management with GCP Workload Identity Federation. For more information about pools and how they manage external identities, see the [Google Cloud documentation](#).

To configure GCP for keyless authentication:

Via Google Cloud Platform Console

To create a service account:

1. Log into [Google Cloud Platform](#).
2. In the left navigation bar, select **IAM & Admin**.

The **IAM** page appears.

3. In the left navigation bar, select **Service Accounts**.
 1. In the **Service account name** box, provide a name for the service account. For example: TenableCloudConnector.
 2. In the **Service account ID** box, provide the service account ID. For example: tenablecloudconnector.
 3. Click **Create and continue** to continue to the next section to grant access to the service account.
4. In the **Grant this service account access to project**, select the **Roles** as **Viewer**.
5. Click **Done**.

To create a Workload Identity Pool:

1. In the left navigation pane, select **Workload Identity Federation**.

The **Workload Identity Pools** page appears.

2. Click **Create Pool**.



The **New workload provider and pool** page appears.

3. In the **Create an Identity pool** section, do the following:
 - a. In the **Name** box, type a name for the pool.
 - b. (Optional) In the **Description** box, provide a description for the pool.
 - c. Click **Continue**.
4. In the **Add a provider to pool** section, do the following:
 - a. From the **Select a provider** drop-down box, select AWS from the list.
 - b. In the **Provider details** box, provide the Tenable's AWS account name. For example: TenableCloudConnectorAWS
 - c. In the **AWS account ID** box, provide the Tenable's AWS account ID: 939095807864.
 - d. Click **Continue**.
5. In the **Configure provider attributes** section, add new mapping:
 - a. In the **google subject** box, type the identity as `attribute.aws_role`.
 - b. In the **AWS** box, type `assertion.arn.extract('assumed-role/{role}/')`

For more information, see [Mapping](#) and [Mapping Conditions](#) in Google Cloud Platform documentation.
6. Click **Save**.

GCP creates the pool and opens the newly created pool page.
7. Click **Grant Access**.

The **Grant access to service account** panel appears.
8. Select the **Grant access using Service Account Impersonation** option.

The relevant sections appear.
9. In the **Service** account drop-down box, select the service account that you created in **Step 1**.



10. In the **Select principals** drop-down box, select `aws_role` and provide the value as `tenable-data-gcp-connector`.
11. Click **Save**.

The **Configure your application** dialog box appears.

12. In the **Provider** drop-down box, select the workload identity pool provider, then click **Download Config**.

GCP downloads the configuration file. Use this file in the **Upload File** section when you integrate GCP Workload Identity Federation with Tenable Attack Surface Management.

Via CLI

1. Create a GCP service account.

```
gcloud iam service-accounts create <YOUR_SA> --description="Tenable Cloud Connector export assests to ASM" --display-name="<YOUR_SA>"
```

Where:

- `YOUR_SA` is the service account name. For example: `TenableCloudConnector`.

2. Assign read-only role to your service account.

```
gcloud iam service-accounts add-iam-policy-binding <YOUR_SA_ID> --member=<YOUR_SA> --role=roles/Viewer
```

Where:

- `Your_SA_ID` is the service account ID.
- `Your_SA` is the service account name.

3. Create the Workload Identity Pool.

```
gcloud iam workload-identity-pools create <Workload_Identity> --location="global" --display-name="<YOUR_SA>" --description="Tenable Cloud connectors"
```




Where:

- `Workload_Identity` is the workload identity pool name. For example: `tenable-cloud-connectors`.
- `YOUR_SA` is the service account name. For example: `Tenable Cloud Connectors`.

4. Create Provider.

```
gcloud iam workload-identity-pools providers create-aws TenableAWS --location="global" --  
workload-identity-pool="<YOUR_POOL_ID>" --account-id="939095807864" --attribute-  
mapping="attribute.aws_role=assertion.arn.extract('assumed-role/{role}/')
```

Where:

- `TenableAWS` is the name of the Provider.
- `Your_Pool_ID` is the ID of the pool you created.

5. Add service account impersonation.

```
gcloud iam service-accounts add-iam-policy-binding <SERVICE_ACCOUNT_EMAIL> --  
role=roles/iam.workloadIdentityUser --member="principal://iam.googleapis.com/projects/<PROJECT_<br>NUMBER>/locations/global/workloadIdentityPools/<POOL_ID>/attribute.aws_role/tenable-data-gcp-connector"
```

Where:

- `Service_Account_Email` is the email ID of the service account.
- `PROJECT_NUMBER` is the project where the Workload Identity Pool is created.
- `Your_Pool_ID` is the ID of the pool you created.
- `Provider_ID` is the ID of the Provider.

6. Download the configuration file.

```
gcloud iam workload-identity-pools create-cred-config projects/<PROJECT_<br>NUMBER>/locations/global/workloadIdentityPools/<POOL_ID>/providers/<PROVIDER_ID> --service-  
account=<SERVICE_ACCOUNT_EMAIL> --service-account-token-lifetime-seconds=3600 --enable-imdsv2 -  
-aws --output-file=config.json
```



Where:

- `Service_Account_Email` is the email ID of the service account.
- `PROJECT_NUMBER` is the project where the Workload Identity Pool is created.
- `Your_Pool_ID` is the ID of the pool you created.
- `Provider_ID` is the ID of the Provider.

What to do next

[Integrate with GCP Using Keyless Authentication](#)



Cloud Assets

Tenable Attack Surface Management collects data from all integrated sources, enriches it with additional details and sends this data to Tenable Vulnerability Management. After integration with cloud providers, all the cloud assets appear on the **Assets** page in Tenable Vulnerability Management. The unified asset view offers you several benefits, such as:

- Obtain a complete view of the external surface of the cloud assets within Tenable Vulnerability Management.
- Prioritize remediation of high-risk externally exposed assets.
- Leverage existing platform capabilities to enrich asset context with Tenable Attack Surface Management's derived indicators.
- Gain visibility into cloud assets not tracked in internal inventories.
- Gain insight into assets known to the platform versus the assets discovered and publicly exposed by Tenable Attack Surface Management.

View Cloud Assets

View all assets from cloud providers in the **Assets** page of Tenable Vulnerability Management.



Before you begin

- Integrate with Tenable Vulnerability Management and Tenable Web App Scanning.
- Integrate with your AWS, Azure, or Google Cloud Platform account and add the provider as a [source](#).

For more information about integration, see [Manage Integrations](#).

Tip: To ingest only cloud assets, in the **Ingestion filters** box for Tenable Vulnerability Management and Tenable Web App Scanning Integration, provide the filter as **Record Type is Cloud**.

To view cloud assets:

1. Use the  Workspace button to navigate to Tenable Vulnerability Management.
2. In the left navigation bar, click the  Assets icon.

The **Assets** page appears.

tenable

Vulnerability Management

Assets

Quick Actions

?

🔔

⚙️

🗖️

👤

Switch to the new Assets page with smarter search and a streamlined workflow. Your current filters are applied.

Assets

All Time

Advanced

Saved Filters

Search by Agent Name, NetBios Name, DNS (FQDN), or IP address, * for wildcard

Apply

Tags: is equal to ASM: CloudAsset

Clear All

Hosts 9

Cloud Resources 0

Web Applications 4

Domain Inventory 0

External Assets 8

Show Visualization

13 Assets

Only Show Unmanaged Assets

Refresh

Grid: Basic View

Columns

1 to 13 of 13

Page 1 of 1

Name	Type	ACR	Licensed	Last Seen	Source	Tags	Actions
	Host	N/A	No	06/25/2025	External Asset	ASM: CloudAs... +1	
	Host	N/A	No	06/25/2025	External Asset	ASM: CloudAs... +1	
	Host	N/A	No	06/25/2025	External Asset	ASM: CloudAs... +1	
	Host	N/A	No	06/25/2025	External Asset	ASM: CloudAs... +1	
	Host	N/A	No	06/25/2025	External Asset	ASM: CloudAs... +1	
	Host	N/A	No	06/25/2025	External Asset	ASM: CloudAs... +1	
	Host	N/A	No	06/25/2025	External Asset	ASM: CloudAs... +1	
	Host	N/A	No	06/25/2025	External Asset	ASM: CloudAs... +1	
	Host	N/A	No	06/25/2025	External Asset	ASM: CloudAs... +1	

For all assets from Tenable Attack Surface Management, the identifier **External Asset** appears in the **Source** column. Additionally, cloud assets include the **ASM CloudAsset** tag and their corresponding inventory name in the **Tags** column.

Note: The tags for cloud assets may take some time to appear in the Assets table.

You can use the **ASM:CloudAsset** tag to trigger a scan specifically on all the external cloud assets. For more information about creating scans, see [Manage Scans](#) in the Tenable Vulnerability Management User Guide.



View Asset Details for Host and Web Application Assets

After you integrate Tenable Attack Surface Management with Tenable Vulnerability Management, you can view additional context about Host and Web Applications on the **Asset Details** page. The details about Host and Web Application assets include the following:

- Asset merge criteria details.
- Visibility into assets already detected by Tenable Vulnerability Management.
- Security risk information based on ACR and AES scores.

This information helps provide answers to the following questions:

- Has an asset detected by Tenable Attack Surface Management already been scanned by Tenable Vulnerability Management?
- What security risks are my external assets most exposed to?
- Where is my external attack surface lacking coverage the most?

Automatic Population of Primary Domains of a Container

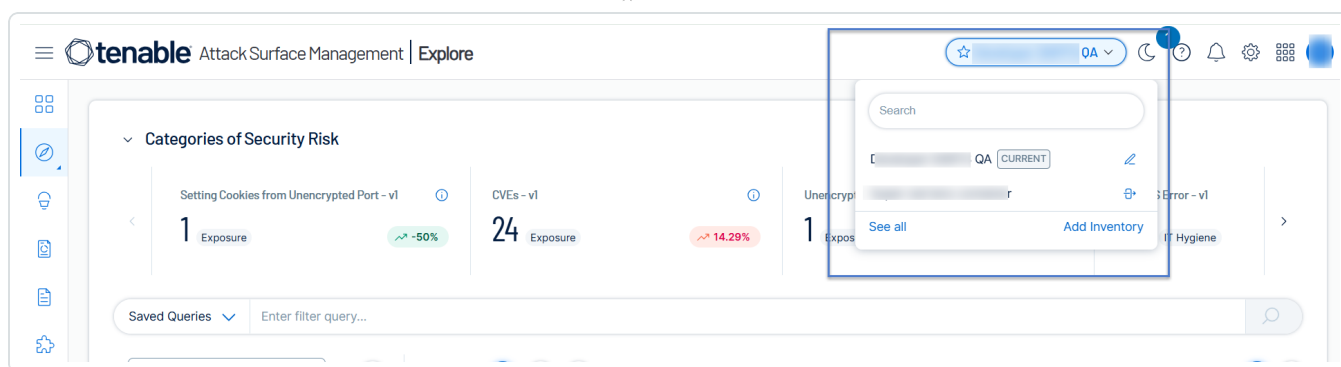
When a container initially acquires a Tenable Attack Surface Management license:

- The container's primary domains are automatically added to the user's initial ASM inventory.
- Host and Web Application integrations are automatically enabled for their initial inventory for which the primary domains are now populated.

To view Host and Web Application Assets details:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.

Tenable Attack Surface Management displays the inventories in the drop-down list.





2. From the drop-down list, select an inventory.


The assets for the inventory appear in a table format.


3. In the list, click the asset for which you want to view more details.

A slider panel appears with the asset details. The **Managed Assets** card indicates whether there are host and web application assets.


 net

Record Value: 


Data Sources 



Severity
Low



Managed Assets
✓ Host Asset
✓ Web App Asset

Key Properties
Licensed No
Source  Attack Surface Management

Summary

Findings


Ports

Attribution



Managed Assets



HTML


Location

 Severity Breakdown

Authentication Asset responds with HTTP status 401 or 403.

 Tags 

 has open ports 

 Tenable.ASM

Host

Severity

Record Type

Record Value

IP

Last Metadata Change

net


Low

A


07/08/2025


4. Click the **Managed Assets** tab to view the integration details.


The **Managed Assets** tab appears with the details about the Host and Web Application assets.



et


Record Value: 

Data Sources 



Severity

Low




Managed Assets

✓ Host Asset

✓ Web App Asset

Key Properties

LicensedNo

SourceAttack Surface Management

Summary

Findings


Ports

Attribution

Managed Assets


HTML

Location

Host Integration

✓ This asset has been identified as a Host asset.

Name	ACR	AES	Last Scanned Date	Last Updated
	4	20	2/11/2025, 11:45 AM	2/26/2025, 7:42 AM

Web Application Integration

✓ This asset has been identified as a Web Application asset.

Name	ACR	AES	Last Scanned Date	Last Updated
	-	-	-	6/1/2025, 8:37 PM

The **Managed Assets** tab displays messages about the assets detected in Host and Web Application integration, explaining why a specific asset is included or excluded. Green messages indicate the reason a host is included, while red messages explain why an asset is excluded.

et

Record Value: !

Data Sources

Severity

None

Managed Assets

✓ Host Asset

✗ Web App Asset

Key Properties

Licensed

No

Source

Attack Surface Management

Summary

Findings

Ports

Attribution

Managed Assets

HTML

Location

Host Integration

✓ This asset has been identified as a Host asset.

Name	ACR	AES	Last Scanned Date	Last Updated
	-	-	-	6/12/2025, 10:52 AM

Web Application Integration

✗ This asset was not integrated due to lack of HTTP response.

The following is the list of messages that appear in the **Managed Assets** tab:

- *This asset has been identified as a <Host | WebApp> asset.*
- *This asset was not integrated due to integration filters in place.*
- *This asset was not integrated due to its record type.*
- *This asset was not integrated because a user has previously deleted a < Host | WebApp > asset of the same name or IP address.*
- *This asset was not integrated because its IP address is non-routable publicly.*
- *This asset was not integrated due to lack of HTTP response.*



- *This asset was not integrated because integration was disabled on inventory or global level.*
- *This asset was not integrated as it represents a DNS wildcard within an Elastic source and lacks a specific identifying IP or hostname.*
- *This asset was not integrated because it is a DNS wildcard, while the integration was configured to identify assets by hostname.*
- *This asset was not integrated because WAS scanner does not currently support IPV6.*
- *This asset was not integrated due to an internal issue. Please contact customer support for more details.*

The Host or Web Application Integration table includes the following information:

Column	Description
Name	The name of the asset.
ACR	The Asset Criticality Rating (ACR) for the asset that indicates how critical the asset is to your organization.
AES	The Asset Exposure Score (AES) that indicates the vulnerability of an asset.
Last Scanned Date	The date and time when Tenable Vulnerability Management last scanned the asset.
Updated at	The date and time when Tenable Attack Surface Management updated the asset details.




Reports

You can create a report that summarizes the details of all your inventories across different indexes such as web servers and ports. You can use the report to measure the size and scope of your organizational attack surface map.

Note: To create reports, you must have the **Manage ad hoc queries** permission. To run the reports, you must have the **Run ad hoc queries** permission.

To access the **Reports** page,

1. In the left navigation bar, click the  button.

The **Reports** page appears with the following details:

Column	Description
Name	Name of the report.
Status	Indicates the status of the report. Available statuses are: Waiting , Running , Done , and Error .
Last Modified	Indicates when the report was last changed.
Last run	Indicates when the report was last generated.

You can do the following actions from the **Reports** page.

Add a report:

1. In the **Reports** page, click **Add Report**.

The **Add Report** page appears.

2. In the **Name** box, type a name for the report.
3. Do one of the following:



- **Add Report** – Click to add the report to the **Reports** page and to run it at a later time. The entries appear in bold on the **Reports** page indicating the reports are new and remain so until you refresh the page.
- **Add and Run Report** – Click to add the report and then run it immediately. If you selected **Add and Run Report**, the **Status** column on the **Reports** page shows **Running**.

Tenable Attack Surface Management adds the report to the **Reports** page.

Run a report:


1. On the **Reports** page, run a report or multiple reports:

Scope	Action
Run a single report	<ol style="list-style-type: none">1. Do one of the following:<ul style="list-style-type: none">• In the row of the report you want to run, click the  button. A menu appears.• Select the check box next to the report you want to run. Tenable Attack Surface Management enables the action bar.2. Click Run Report.
Run multiple reports	<ol style="list-style-type: none">1. Select the check boxes next to the reports you want to run. Tenable Attack Surface Management enables the action bar.2. Click Run Reports.

Tenable Attack Surface Management shows a confirmation message when the report generation is complete.



View Report Details:


1. On the **Reports** page, in the row of the report you want to view the details, click the  button.
2. Click **View Report Details**.

The **Report Details** page appears with the following information:

Section	Description
Download PDF	A link to download the generated report.
Summary	Shows details such as the start time, end time, duration of the report generation and the current status of the report.
Log	Shows any errors that occurred when generating the report. Click Copy to copy the log to share or for further analysis.

3. Click **Done** to close the **Report Details** page.

Edit a Report:

1. On the **Reports** page, in the row of the report you want to edit, click the  button.
2. Click **Edit Report**.

The **Edit Report** page appears.


3. Edit the report details as needed.
4. Click **Save**.

Tenable Attack Surface Management saves the updated report.

Delete Report:



1. On the **Reports** page, to delete a report or multiple reports:

Scope	Action
Delete a single report	<ol style="list-style-type: none">1. Do one of the following:<ul style="list-style-type: none">• In the row of the report you want to delete, click the  button.A menu appears.<ul style="list-style-type: none">• Select the check box next to the report you want to delete.Tenable Attack Surface Management enables the action bar.2. Click Delete Report.
Delete multiple reports	<ol style="list-style-type: none">1. Select the check boxes next to the reports you want to delete. Tenable Attack Surface Management enables the action bar. <ol style="list-style-type: none">2. Click Delete Reports.

Tenable Attack Surface Management shows a confirmation message that the report is permanently deleted.

Navigate Tenable Attack Surface Management

Your inventory page is the top-level view of your assets. The following images give you a closer look at what each of the items in this interface are.

Note: The section describes the legacy interface.

tenable | ASM

Team:

Total Assets

1,406

Domains

3

Subdomains

558

+ Add Filter

1 to 25 of 863 < Page 1 of 35 >

Search	Host	Record Type	IP	ASN	Ports	Screenshot
Sort by Asset Count - High to Low Select All		UNK			80, 443	
1.		CNAME			80, 443	
2.		SOA			-	
		CNAME			80, 443	
		CNAME			80, 443, 2082, 2083, 2086, 2087, 8080, 8443	
		CNAME			80, 443, 2082, 2083, 2086, 2087, 8080, 8443	
		CNAME			-	
		CNAME			80, 443	
		CNAME			80, 443	

Left Navigation

Inventory name

Inventories can be individually named, making it easy to differentiate from others.

Team

Users who have permission to manage the inventory.

Filters

A selection over 100 filters that allow you to see only the assets you want to see.

Search Sources

Search sources by keyword.

Sources

Assets grouped by a common identifier, such as domain name, or IP range.

Assets List

List of assets associated with the source that is selected in the Sources list.

tenable | ASM

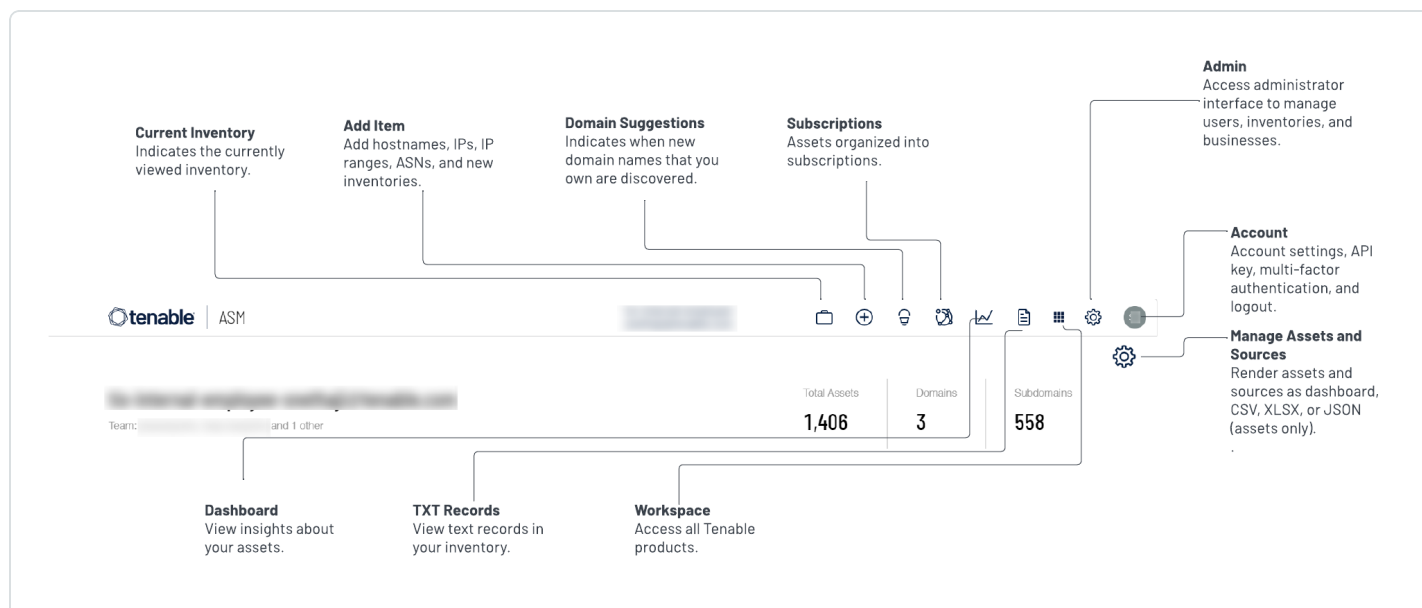
Team: and 1 other

Add a description

+ Add Filter

Search	Host	Record Type
Sort by Asset Count - High to Low Select All		UNK
1.		CNAME
2.		SOA
		CNAME
		CNAME
		CNAME
		CNAME
		CNAME

Top Navigation

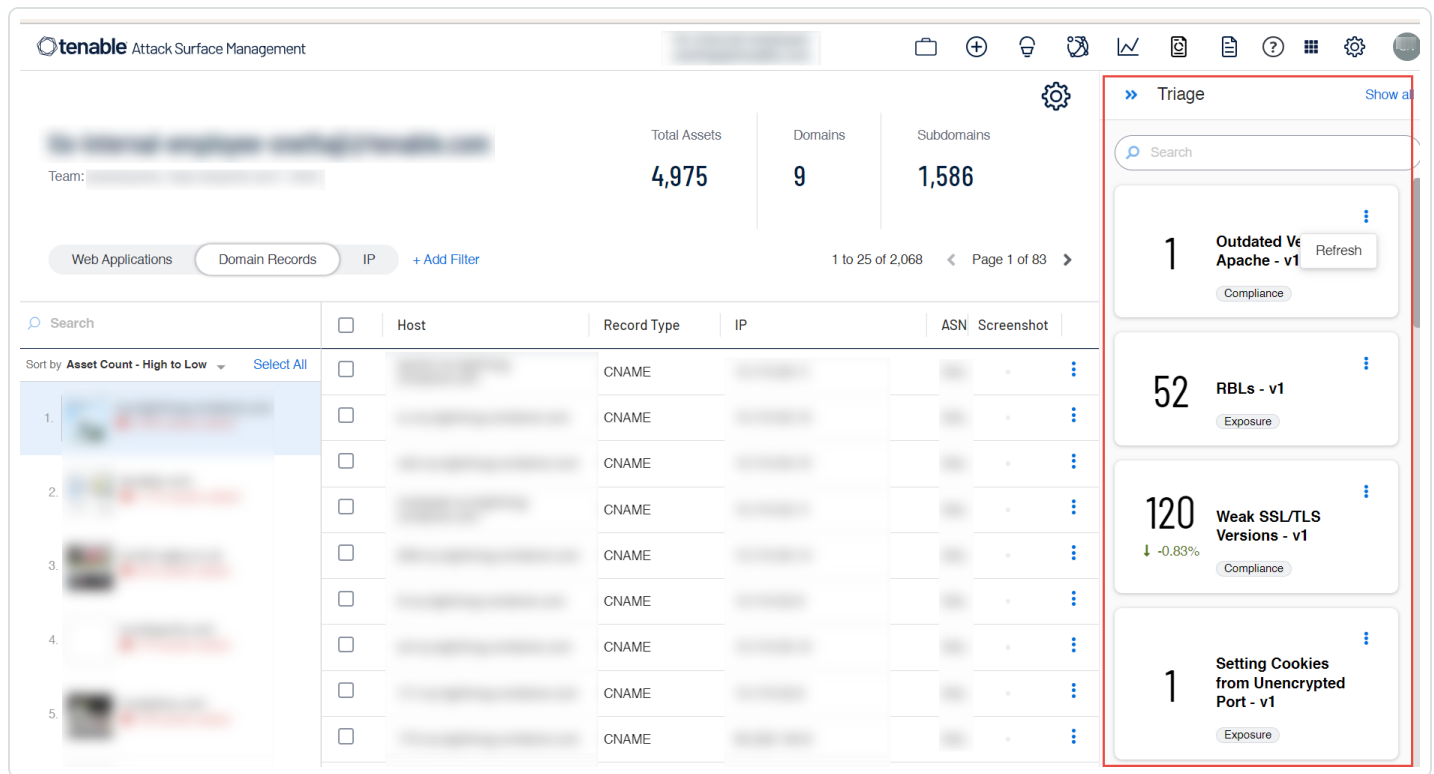


Section	Description
Total Assets	The total number of assets in the inventory. <div>Note: The Total Assets count on the Inventory page shows the most up-to-date data, while the Administrator page updates once every 24 hours. Some actions might refresh the data sooner, but updates to the Administrator page usually follow the 24-hour schedule.</div>
Domains	The number of domains in the inventory.
Subdomains	The number of subdomains in the inventory.

Triage

The **Triage** panel of Tenable Attack Surface Management provides a high-level overview of your assets by listing the critical events in your organization along with the number of your affected assets.

Note: You can access **Triage** categories in the **Categories of Security Risk** panel of the **Explore** dashboard. For more information, see [Explore](#).




To view the **Triage** panel:

1. In the right-hand side bar, click **Triage**.

The **Triage** panel appears.

2. View the **Categories of Security Risk** panel.

You can view the following details on the panel:

- List of critical events or triage items in the order of their severity level with the number of affected assets and the category of the event. The events appear in the order of their severity levels – the most important ones appear first. Each triage item also displays the difference in the previous and current number of affected assets as a percentage. Event names are based on the [subscription](#) templates (**Saved Queries** in the **Explore** dashboard).
- Tenable Attack Surface Management automatically refreshes the list daily. To refresh the data, click  > **Refresh**. Once you click **Refresh**, the option gets disabled for an hour accordingly.
- Click an event name to view the assets with the applied filters on the **Inventory** page.
- Click **Show All** to open **Triage** on a separate page.



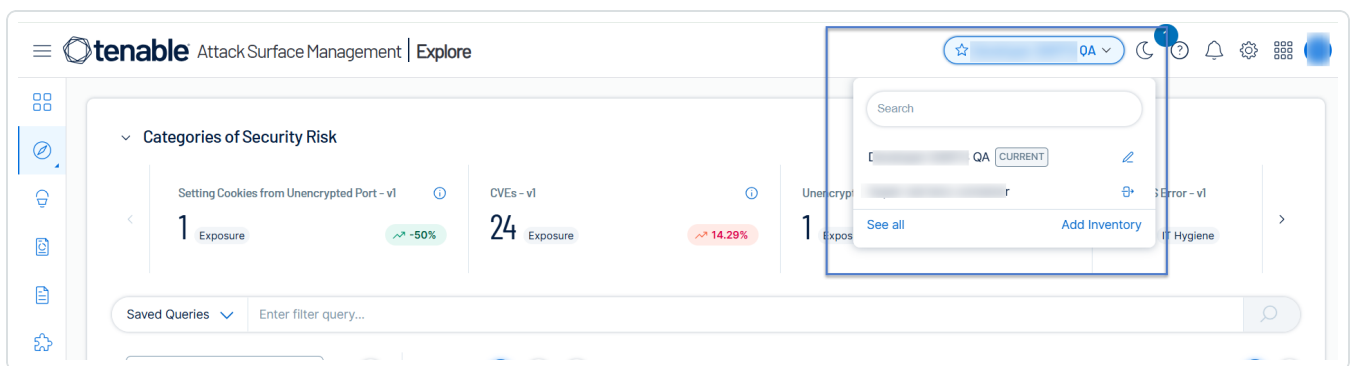
Inventory

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

In Tenable Attack Surface Management, an inventory is where you view your organization's assets.

To view an existing inventory:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select the inventory you want to view.

Your inventory appears.

Related topics:

[Create an Inventory](#)

[Inventory Settings](#)

[Inventory Columns](#)

[Asset Prioritization](#)

[Leave an Inventory](#)

[Manage Inventory Sources](#)

[Asset Filters](#)

[Asset Details](#)



[View Asset Attribution](#)

[Export an Asset](#)

[Manage Asset Tags](#)

[Move or Copy Assets to another Inventory](#)

[Archive an Asset](#)

[Create an Advanced Network Scan](#)

[Create a Web Application Scan](#)

Create an Inventory

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

In Tenable Attack Surface Management, you can create an inventory to identify and organize your assets.

To create an inventory and add a domain:

1. In Tenable Attack Surface Management, in the upper-right corner, click the current inventory.

The Inventory drop-down list appears.

Note: Click **See All** to view all your inventories.

2. In the drop-down list, click **Add Inventory**.

The **Create new inventory** window appears.

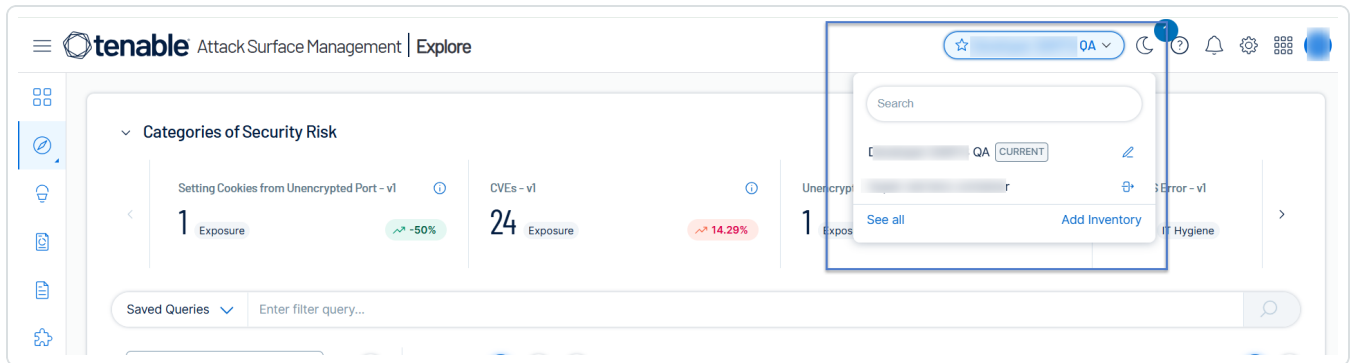
3. In the **New Inventory Name** box, type a name for the inventory.
4. (Optional) In the **Inherit Inventory** box, select an inventory you want to use as a template for the new inventory.

The new inventory inherits the selected inventory's tags, custom columns, subscriptions, and exclusion rules.

5. Click **Save**.

The inventory is created.

6. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

7. In the drop-down list, click the inventory you just created.

The **Set up your Inventory** page appears, prompting you to add a domain to your inventory.

8. In the text box, type your organization's domain.

Note: To add multiple domain names, separate the domain names using space.

9. Click the **+ Add Domain Name** button.

The inventory appears, with the domain added.

10. (Optional) [Add additional sources to your inventory.](#)


Inventory Settings

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

On the Inventory page, you can add or remove columns to the inventory table and also render the assets and sources in your inventory to different formats.


To manage your inventory settings:



1. In the upper-right corner of the Inventory page, click the  icon.

A drop-down menu appears.

2. Select the required option.

Option	Description
Manage Columns	<p>Allows you to add and remove columns from the assets table.</p> <p>To add or remove columns:</p> <ol style="list-style-type: none">1. In the Explore page, in the header of the assets table, click the Columns drop-down list. <p>The Customize Columns window appears.</p> <ol style="list-style-type: none">2. Do the following: <ul style="list-style-type: none">• To add columns, select the checkboxes next to the column names you want to add.• To remove columns, clear the checkboxes next to the column names you want to remove. <ol style="list-style-type: none">3. Click outside the box to close the window. <p>Tenable Attack Surface Management updates the table with the selections.</p>
Render Assets as Dashboard	<p>Renders the assets table in the dashboard format. When you select Render Assets as Dashboard, each column in the assets table appear as widgets in the dashboard.</p> <p>In the assets table, click the View as  button to display each column in the chart format.</p> <div><p>Note: The following columns are not supported for Render Assets as Dashboard:</p><ul style="list-style-type: none">• Asset ID• Screenshot</div>



- Added to Inventory
- Record Value
- Host
- IP
- Added to this Subscription
- HTML
- Domain
- Canonical URL
- SSL / TLS Subject Alt Name
- Response Header Value
- Response Security Header Value
- Banners
- Final URL
- SSL / TLS Valid From
- SSI / TLS Expiration

To change the format back to table, from the drop-down menu, select **Render Assets as Table**. If you do not change to the table format, Tenable Attack Surface Management shows the dashboard view the next time you log in.

Export All

To export all assets:

1. In the assets table, click **Export All**.

The **Export** window appears.

2. Select the format: CSV, XLSX, or JSON.
3. Search for and select the columns to export.

Note: Use the **View selected** option to view the selected columns.

4. Click **Export**.



	Tenable Attack Surface Management exports the assets with the selected columns.
Render Assets as CSV	Exports the assets table to CSV.
Render Assets as XLSX	Exports the assets table to XLSX.
Render Assets as JSON	Exports the assets table to JSON.
Render Sources as CSV	Exports the sources to CSV.
Render Sources as XLSX	Exports the sources to XLSX.
Tag Assets Quickly	Allows you to tag assets. For more information, see Tag Assets Quickly .
Add Tags Remove Tags	Allows you to tag assets. For more information, see Manage Asset Tags .


Inventory Columns

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Explore](#).

In Tenable Attack Surface Management, an inventory is where you view your organization's assets. You can view the inventory details in a table format. Add or remove columns to the inventory table to get specific details of an asset in your inventory.

To configure the columns for the inventory table:



1. In the upper-right corner of the Inventory page, click the  icon.

A drop-down menu appears.

2. Select **Manage Columns**.

The **Select data types to list** page appears with the list of columns that you can enable or disable.

3. On the **Explore** page, use the **Columns** drop-down list to **Customize Columns**. See [Explore](#).

The following table shows the available columns that you can choose and their descriptions.

Column Name	Description
Security	
SSL/TLS Expiration	Date until the SSL certificate of the asset is valid.
SSL/TLS Fingerprint	SSL fingerprint of the asset.
SSL/TLS EV Certificate	States whether the asset has an Extended Validation (EV) certificate.
SSL/TLS Issuer Country	SSL certificate issuer country.
SSL/TLS Issuer Organization	SSL certificate issuer organization.
SSL/TLS Valid From	The date from which the SSL certificate of the asset is valid.
SSL/TLS Subject Alt Name	SSL subject alternate names of the asset.
SSL/TLS Cypher Suites	Cypher suites available on the asset.
SSL/TLS Key	Peer certificate RSA bit size.



Length	
SSL/TLS Protocol	SSL protocols used by the asset.
SSL/TLS error	SSL errors produced by the asset.
SSL/TLS Serial Number	SSL serial number of the asset.
Captchas	CAPTCHA software used by the asset.
Cookie Compliance	Cookie compliance used by the asset.
Secret Keys	Secret keys used by the asset. Tenable Attack Surface Management collects this data by executing multiple regular expressions against the rendered HTML of the site.
Login	Whether the asset redirects to or contains a login page.
JARM Hash	A hash that can be used to group assets having similar SSL configurations.
Bug Bounty URL	Bug bounty programs that the asset is part of.
HTTP Response	
Content type	The type of content served by the asset.
Content language	The language of content served by the asset.
Vary	The value of the Vary HTTP header set by the asset.
Response Header Value	HTTP header values returned by the asset.
Response Security Header Value	HTTP security header values returned by the asset.
Sets Cookies	States whether the asset sets cookies or not.
Content Length	The length of the content served by the asset in bytes.



Canonical URL	Canonical URL found in the HTML body returned by the asset.
Response code	The response code returned from the final URL the asset redirects to.
HTML	Raw response body returned by the asset.
Document Title	HTML document title.
Networking	
Host	Hostname of the asset.
Record Type	DNS record type of asset.
Record Value	DNS record value of the asset.
Redirect Chain	The chain of HTTP or client-side redirects that navigated the system to <code>screenshot.finalurl</code> .
IP	IP address of the asset.
Is subdomain	Indicates whether the hostname of the asset is a subdomain or not.
Final response code	The response code returned from the final URL the asset redirects to.
ASN	The Autonomous System organization of the asset.
ASN Number	The Autonomous System Number (ASN) of the asset.
Final url	The final URL the asset redirects to.
Domain	Domain name of asset.
Hosting Provider	Cloud provider of the asset.
Cloud Hosted	Whether the Asset is cloud-hosted or not.
Network Devices	Network devices used by the asset.
Mixed Content	Mixed content returned by the asset.



Network Storage	Network storage software used by the asset.
CDN	CDNs used by the asset.
Remote Access	Remote access software used by the asset.
Containers	Container software used by the asset.
SaaS	SaaS solutions used by the asset.
PaaS	PaaS solutions used by the asset.
IaaS	IaaS solutions used by the asset.
Load Balancer	Load Balancers used by the asset.
Reverse Proxy	Reverse proxies used by the asset.
Nameservers	DNS nameservers of the asset based on WHOIS data.
Programming	
Mobile Frameworks	Mobile frameworks used by the asset.
Programming Languages	Programming languages used by the asset.
Web Frameworks	Web frameworks used by the asset.
Dev Tools	Development tools used by the asset.
JavaScript Libraries	JavaScript libraries used by the asset.
JavaScript Frameworks	JavaScript frameworks used by the asset.
Landing Page Builders	Landing page builders used by the asset.
Documentation Tools	Documentation tools used by the asset.



Geolocation	
Continent	Location of the asset.
Country	Location of the asset.
City	Location of the asset.
Latitude	Location of the asset.
Longitude	Location of the asset.
Timezone	Location of the asset.
Postal	Postal code of the asset.
In EU	Whether the asset is located in the EU or not.
Subdivisions	Location of the asset.
Registered Country	Country where the asset was registered.
Maps	Maps software used by the asset.
Services	
Ports	Ports open on the asset.
Services	Service running on the asset.
Banners	Banners returned by services running on the asset.
CPE	Services running on the asset in Common Platform Enumeration (CPE) format.
CVE	IDs of CVEs that apply to the asset.
CVSSv3 Scores	Unique CVSS3 scores that apply to the asset.
CVSSv3 Vectors	Unique CVSS3 vector strings that apply to the asset.
Server	Web server running on the asset based on HTTP response headers.



RBL	Realtime Blackhole Lists (RBL) that contain the asset.
Web Servers	Web servers running on the asset.
Email service	Emails used by the asset.
Web applications	
Browser fingerprinting	Browser fingerprinting tools.
Buy now pay later	Buy now pay later tools.
Cart abandonment	Cart abandonment tools.
Content curation	Content curation tools.
Customer data platform	Customer data platform tools.
Digital asset management	Digital asset management tools.
Geolocation	Geolocation tools.
Hosting	Hosting information.
Loyalty & rewards	Loyalty and rewards tools.
Performance	Performance tools.
Referral marketing	Referral marketing tools.
Reservations & delivery	Reservations and delivery platforms.
Reviews	
RUM	Real User Monitoring (RUM) tools.
Segmentation	Segmentation tools.
Shipping carriers	Shipping carrier tools.



Translation	Translation tools.
Wordpress plugins	WordPress plugin tools.
Wordpress themes	WordPress theme tools.
Recruitment & staffing	Recruitment and staffing tools.
Returns	Returns technologies.
Livestreaming	Livestreaming tools.
Ticket booking	Ticket booking tools.
Augmented reality	Augmented reality tools.
Cross border ecommerce	Cross-border ecommerce tools.
Message Boards	Message boards used by the asset.
CMS	Content Management Systems (CMS) used by the asset.
Database Managers	Database managers used by the asset.
Wikis	Wiki software used by the asset.
Hosting Panels	Hosting panels used by the asset.
Wordpress Vulnerability IDs	WPScan Vulnerability Database IDs.
Blogs	Blogging software used by the asset.
Wordpress Core Version	WordPress Core version.
WordPress Scanned Plugins	The WordPress scanned plugins that run on the asset.



Editors	Editor software used by the asset.
Search Engines	Search engines used by the asset.
Web Mail	Web mail used by the asset.
Cryptominer	Cryptomining software used by the asset.
Static Site Generator	Static site generators used by the asset.
User Onboarding	User onboarding software used by the asset.
Document Management Systems	Document management systems used by the asset.
Control Systems	Control systems used by the asset.
Issue Trackers	Control systems used by the asset.
Accessibility	Accessibility libraries used by the asset.
Appointment scheduling	Appointment scheduling libraries used by the asset.
LMS	Learning management systems used by the asset.
Tag Managers	Tag managers used by the asset.
Data	
Analytics	Analytics software used by the asset.
Databases	Databases used by the asset.
Social	
Social Profiles	Social profiles used by the asset.
Live Chat	Live chat software used by the asset.
Comment Systems	Comment systems used by the asset.



Social logins	Social logins used by the asset.
Media	
Photo Galleries	Photo galleries used by the asset.
Media Servers	Media servers used by the asset.
Webcams	Webcam software used by the asset.
Printers	Printer libraries used by the asset.
Font Scripts	Font scripts used by the Asset.
Video Players	Video players used by the asset.
Rich Text Editors	Rich text editors used by the asset.
JavaScript Graphics	JavaScript graphics used by the asset.
Finance	
Shopify apps	Shopify app tools.
Ecommerce	Cross-border ecommerce tools.
Payment Processors	Payment processors used by the asset.
Paywalls	Paywalls used by the asset.
Accounting	Accounting systems used by the asset.
Affiliate programs	Affiliate programs used by the asset.
Marketing	
Google Analytics Keys	Referral marketing tools.
Google Adsense Keys	Google AdSense keys used by the asset.



Advertising Networks	Advertising networks used by the asset.
Marketing Automation	Referral marketing tools.
CRM	Customer relationship management systems used by the asset.
SEO	Search engine optimization software used by the asset.
General	
Widgets	Javascript widgets used by the asset.
Cache Tools	Cache tools used by the asset.
Operating Systems	Operating systems used by the asset.
Web Server Extensions	Web server extensions used by the asset.
Feed Readers	Feed readers used by the asset.
Build CI Systems	Build Continuous Integration systems used by the asset.
Miscellaneous	Miscellaneous software used by the asset.
Tenable.asm	
Asset ID	The unique id of the asset.
Severity	The severity ranking of the asset based on its security risk.
Added to Inventory	Timestamp of date when the asset was added to the current inventory.
Tag	IDs of simple Tags associated with the asset. Corresponds with the Tag column on the user interface.
WHOIS	
Administrative contact email	Administrative contact email of the asset.



Administrative contact name	Administrative contact name of the asset.
Administrative contact organization	Administrative contact organization of the asset.
Billing contact email	Billing contact email of the asset.
Contact email	Contact email of the asset.
Domain name expiration	Age out date of the asset.
Registrant city	Registrant city of the asset.
Registrant country	Registrant country of the asset.
Registrant email	Registrant email of the asset.
Registrant fax	Registrant fax of the asset.
Registrant name	Registrant name of the asset.
Registrant postal code	Registrant postal code of the asset.
Registrant state	Registrant state of the asset.
Registrant street	Registrant street of the asset.

Asset Prioritization

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Asset Prioritization](#).

Tenable Attack Surface Management ranks your assets and assigns a severity level to the assets based on their security risk. You can use the severity ranking to prioritize the assets that require immediate attention. The **Severity** column of the asset table shows the severity of an asset as **Low**, **Medium**, **High**, **Critical**, or **None**.



Tenable Attack Surface Management calculates the severity ranking for an asset by matching the asset information with a given set of criteria. Any change or update to the asset changes the severity level of that asset. For example, an asset with a **Critical** severity with a vulnerability issue moves to **Medium** or **Low** severity after you remediate the issue and rescan the asset.

The screenshot shows the Tenable Attack Surface Management interface. At the top, there are statistics: Total Assets (949), Domains (3), and Subdomains (511). Below this is a search bar and a table of assets. The 'Severity' column is highlighted with a red box, showing values like 'Low' and 'None'. The table has columns for Host, Severity, Record Type, IP, ASN, Ports, and Screenshot.

Host	Severity	Record Type	IP	ASN	Ports	Screenshot
	Low	CNAME				
	None	A				
	None	CNAME				
	None	CNAME				
	None	A				
	None	A				
	None	A				

The screenshot shows the Tenable Attack Surface Management interface with a 'Categories of Security Risk' section. Below this is a search bar and a table of assets. The 'Severity' column is highlighted with a blue box, showing values like 'None' and 'Low'. The table has columns for Host, Severity, Record Type, IP Address, ASN, Register..., Ports, Screenshot, and Tags.

Host	Severity	Record Type	IP Address	ASN	Register...	Ports	Screenshot	Tags
	None	CNAME				80, 443, ...	-	tag with
	None	AAAA				80, 443, ...	-	-
	Low	A				53, 80, 4...		-
	None	UNK				443	-	-
	Low	CNAME				80, 443, ...	-	-
	None	A				80, 443, ...	-	-

Tip: To view the factors on which the asset prioritization score is based on, click the asset name to open the asset page. The asset prioritization details are available at the top of the asset details page.

Enable the Severity Column

You must enable the **Severity** option in Tenable Attack Surface Management for the column to appear in the assets table.

To enable the **Severity** column for your assets:



1. In Tenable Attack Surface Management, click the  button.

A menu appears.

2. In the drop-down list, click **Manage Columns**.

The **Select data types to list** page appears.

3. In the **Tenable.asm** section, select the **Severity** checkbox.

4. Click **Show**.

Tenable Attack Surface Management includes the **Severity** column in the assets table.

5. On the **Explore** page, in the assets table header, click **Columns**.

The **Customize Columns** drop-down list appears.

6. Select the **Severity** checkbox.

Tenable Attack Surface Management includes the **Severity** column in the assets table.

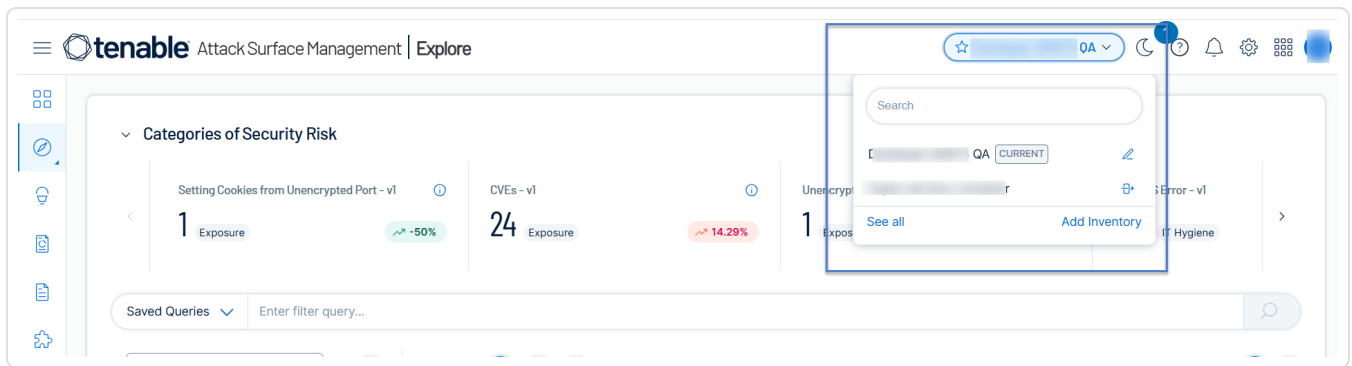
Leave an Inventory

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).


When you leave an inventory in Tenable Attack Surface Management, other members of the organization can still access the inventory. If you leave an inventory that you own, then ownership will be passed to the next oldest member in the inventory.

To leave an inventory:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

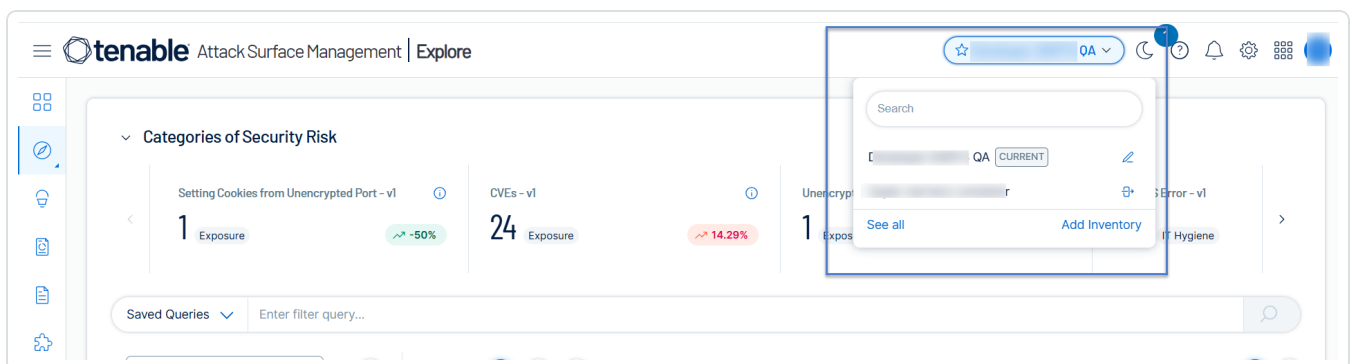
2. In the drop-down list, hover over the inventory that you want to leave.
3. Click the  button.

A dialog box appears, confirming your selection to leave the inventory.

4. Click the **Leave** button.

The inventory is removed from your list of inventories.

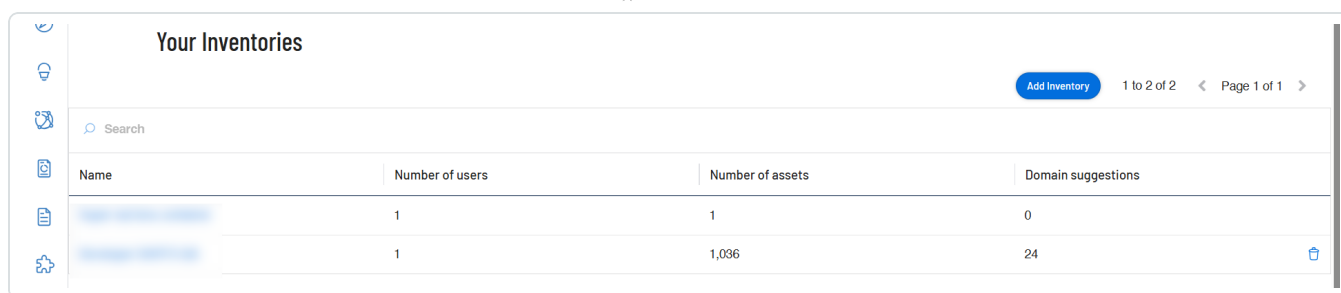
1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. Click **See all**.

The **Your Inventories** page appears.



Name	Number of users	Number of assets	Domain suggestions
[Redacted]	1	1	0
[Redacted]	1	1,036	24

3. Hover over the inventory that you want to leave.

4. Click the  button.

A dialog box appears, confirming your selection to leave the inventory.

5. Click **Leave**.

Tenable Attack Surface Management removes the inventory from your list of inventories.

Manage Inventory Sources

Add Sources

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

In Tenable Attack Surface Management, you can add a source to your inventory to identify more assets associated with your organization.

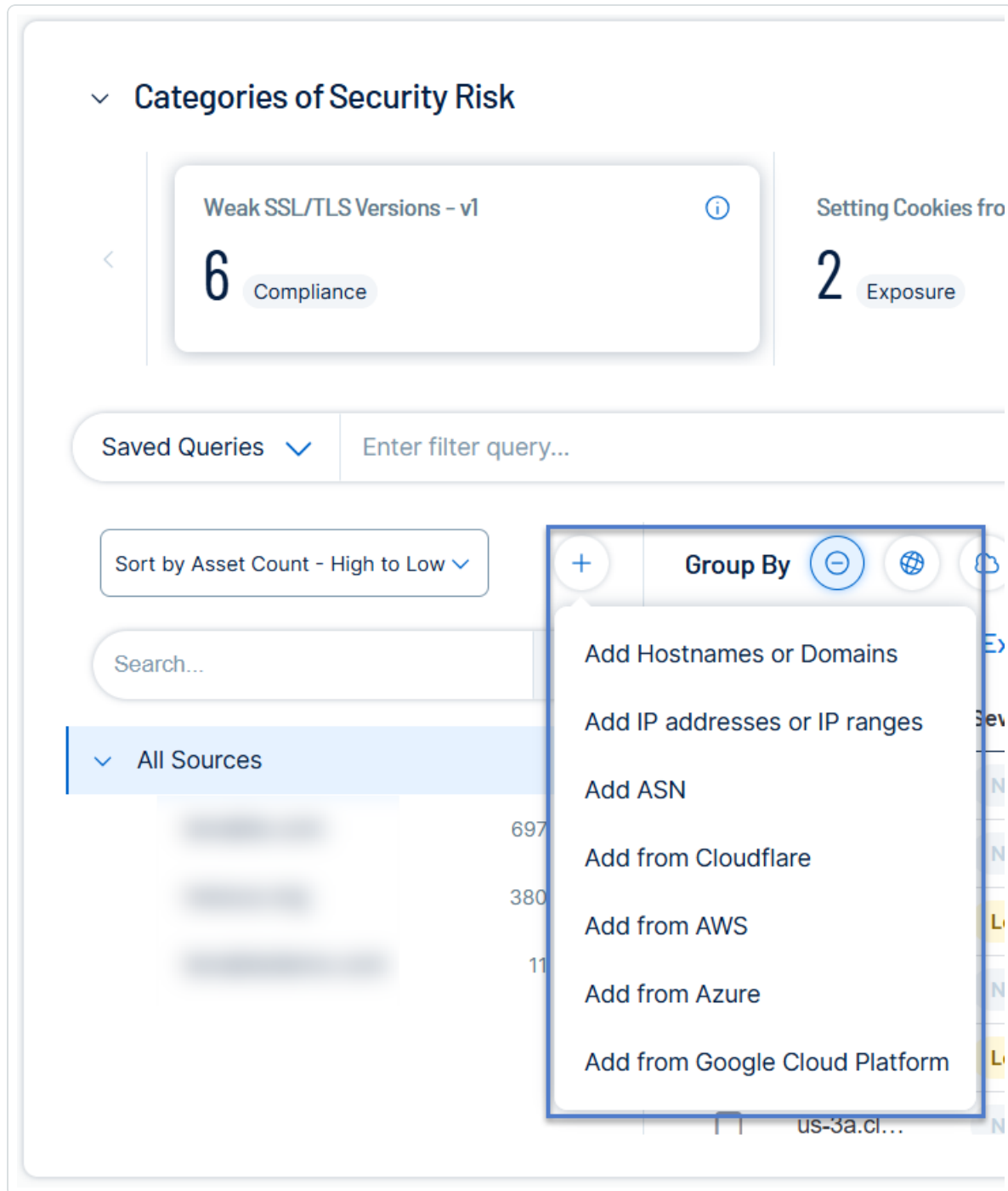
See the following procedures for how to add different types of sources.

- [Add a hostname, domain, or subdomain](#)
- [Add an IP address or IP range](#)
- [Add an Autonomous System Number \(ASN\)](#)
- [Add sources from Cloudflare](#)
- [Add sources from AWS](#)
- [Add sources from Azure](#)
- [Add sources from Google Cloud Platform](#)



Add a hostname, domain, or subdomain

1. In Tenable Attack Surface Management, in the left pane, click the **+** button.
2. In the left pane of the **Explore** page, click the **+** button.





Tenable Attack Surface Management displays the sources that you can add.

3. In the drop-down list, click **Add Hostnames or Domains**.

The **Enter Hostname** window appears.

4. In the **Enter a host to your Inventory** box, type a hostname or domain.

A list of options appears.

Note: You can add a maximum of two domains across your organization. If you already have two domains system-wide, you must delete one before you can add another.

5. Select any applicable options:

Option	Description
<i>Add subdomains instead of domains</i>	Adds the domain as a subdomain instead of a host or domain.
<i>Don't do subdomain discovery</i>	Prevents Tenable Attack Surface Management from automatically discovering subdomains for the domain.
<i>Elastic source</i>	During asset detection, Tenable Attack Surface Management records both FQDN and IP address of the asset. When you enable the Elastic source option, Tenable Attack Surface Management records only the asset's FQDN. This prevents duplicate asset findings for an asset with frequently changing IP address, such as one hosted by a Cloud service. When extracting data from an asset in an Elastic Source, Tenable Attack Surface Management resolves the FQDN to an IP address right before each scan.

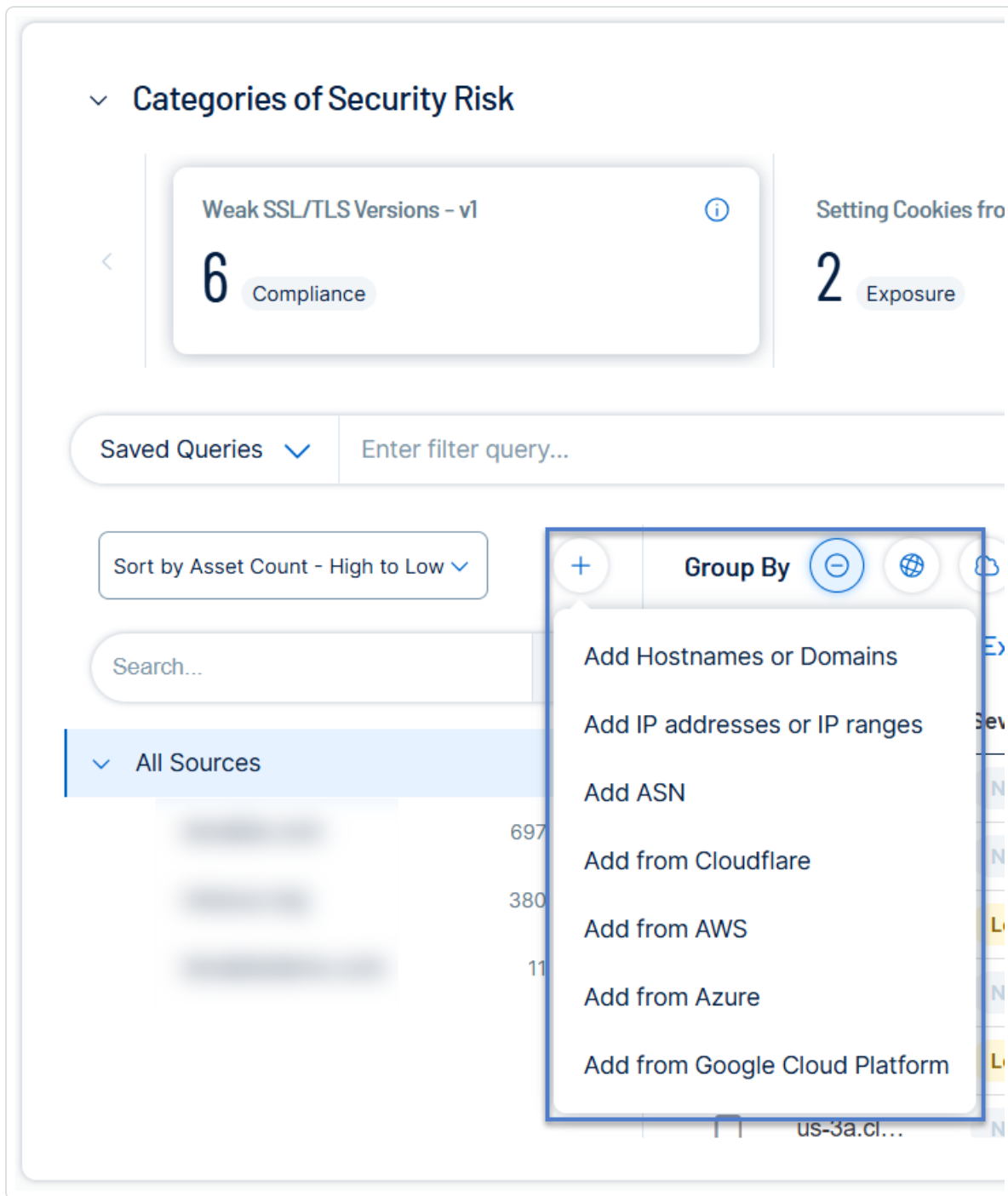
6. Click **Next**.

The hostname, domain, or subdomain appears in your inventory and begins identifying assets.

Add an IP address or IP range



1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In Tenable Attack Surface Management, in the left pane, click the **⊕** button.
3. In the drop-down list, click **Add IP addresses or IP ranges**.



The **Enter IP address** window appears.

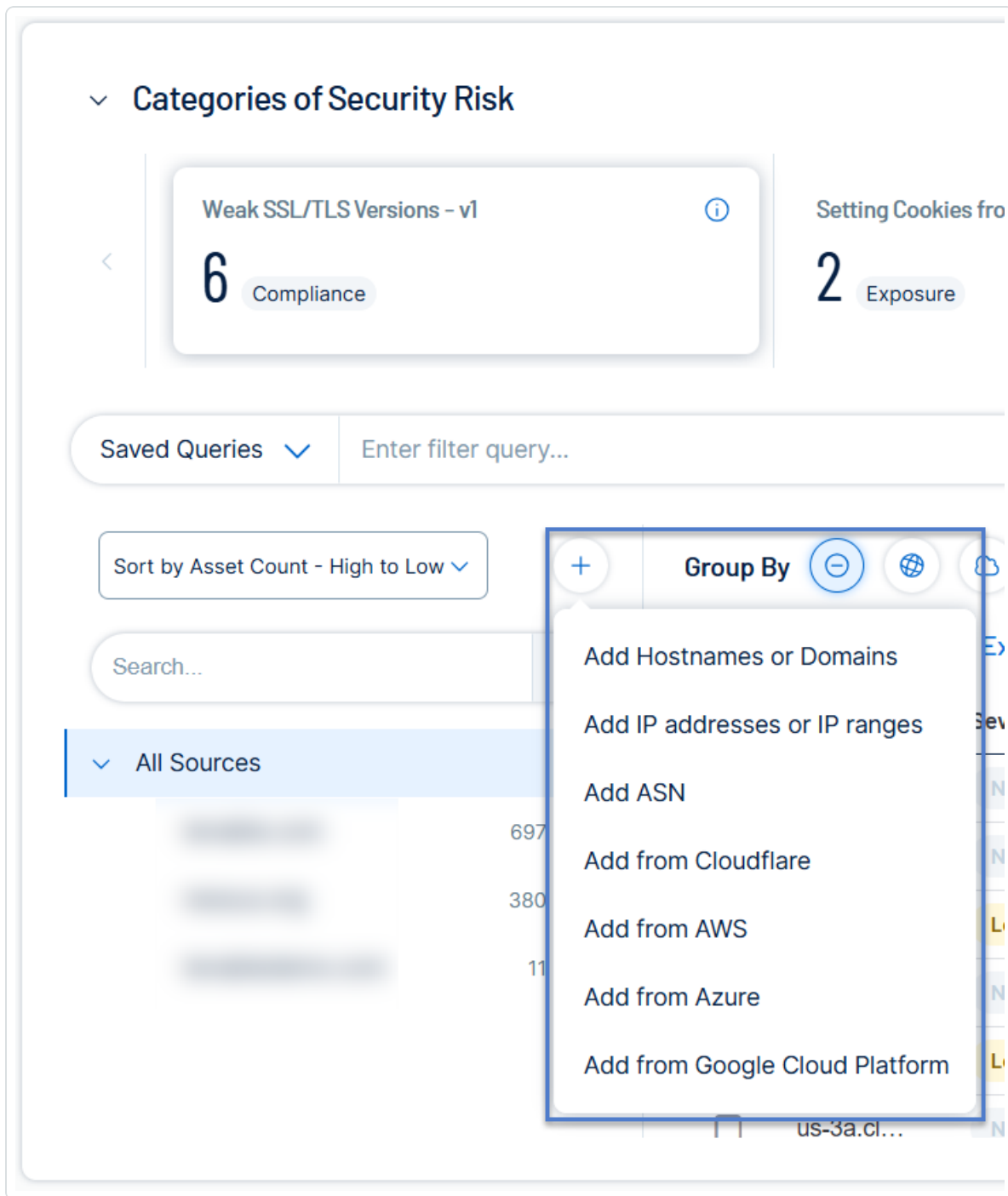
4. In the **Enter an IP range to your Inventory** box, type an IP address, IP range, or a comma-separated list of IP addresses.
5. To select assets, do one of the following:
 - Click **Add IP address** if you want Tenable Attack Surface Management to identify all assets associated with the IP address.
 - Click **Select Assets Manually**. The **Select IP Addresses** window appears: select the IP addresses to add to your inventory, and click **Add to Inventory** to add the assets.

Tenable Attack Surface Management adds the IP addresses to your inventory and begins to identify assets.

Add an Autonomous System Number (ASN)



1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In Tenable Attack Surface Management, in the left pane, click the **⊕** button.
3. In the drop-down list, click **Add ASN**.



The **Enter ASN** window appears.

4. In the **Enter AS number or organization name** box, type an ASN or search for an organization.
5. Click the **Add ASN** button.

Tenable Attack Surface Management adds the ASN to your inventory and begins to identify assets.

Add sources from Cloudflare

Before you begin

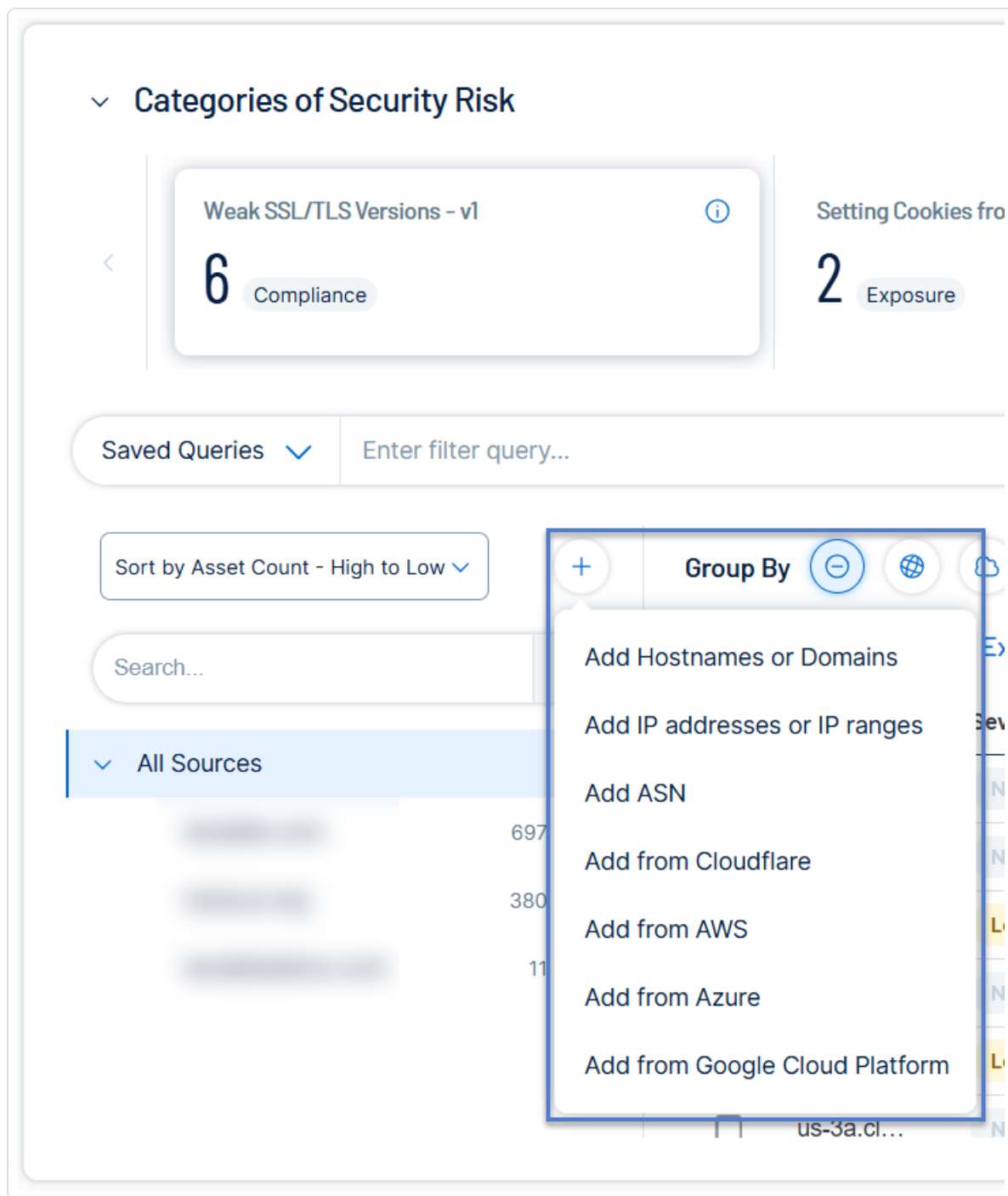
Tenable Attack Surface Management requires the following permissions to add Cloudflare sources:

- **Zone Read** — Grants read access to zone management.
- **DNS Read** — Grants read access to DNS.

To add sources from Cloudflare:



1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In Tenable Attack Surface Management, in the left pane, click the **⊕** button.
3. In the drop-down list, click **Add from Cloudflare**.



The **Cloudflare keys** window appears with the list of configured API keys.

4. Do one of the following:

- Click an API key to view the list of available zones or domains the API key has access.
- (Optional) If you do not have any configured API keys, add a new API key:
 - a. Click **Add**.

Tenable Attack Surface Management displays the **Add Cloudflare key** box.

- b. In the **Cloudflare account name** box, type a name for the Cloudflare account.
- c. In the **API key** box, copy and paste the API key for your Cloudflare account.
- d. Click **Add**.

Tenable Attack Surface Management adds the API key and displays the **Available zones** window with the list of Cloudflare zones (domain names) where the API key has access.

Note: Tenable Attack Surface Management supports these types of DNS records: A, AAAA, CNAME, MX, NS, TXT, PTR, and SOA.

5. To add a domain to your inventory, click the **Add to inventory** link next to the domain name to add.

Note: To add all zones to your inventory, click **Add all**.

Tenable Attack Surface Management adds the Cloudflare assets to your inventory and redirects you to the Inventory page showing the newly added sources. The source from Cloudflare has an orange cloud icon under its name.

If there are assets from outside the zone or domain, Tenable Attack Surface Management automatically adds them as elastic assets. Tenable Attack Surface Management extracts data from these elastic assets using the hostname rather than their IP addresses. The **IP** column in the Inventory table shows *Elastic Asset* instead of an IP address for these elastic assets.

To delete a Cloudflare API key:



1. In the **Cloudflare keys** window, click  next to the Cloudflare API key to delete.

Tenable Attack Surface Management deletes the Cloudflare API key. The sources added using this key still show up in the inventory but Tenable Attack Surface Management eventually deletes them across all inventories.

Add sources from AWS

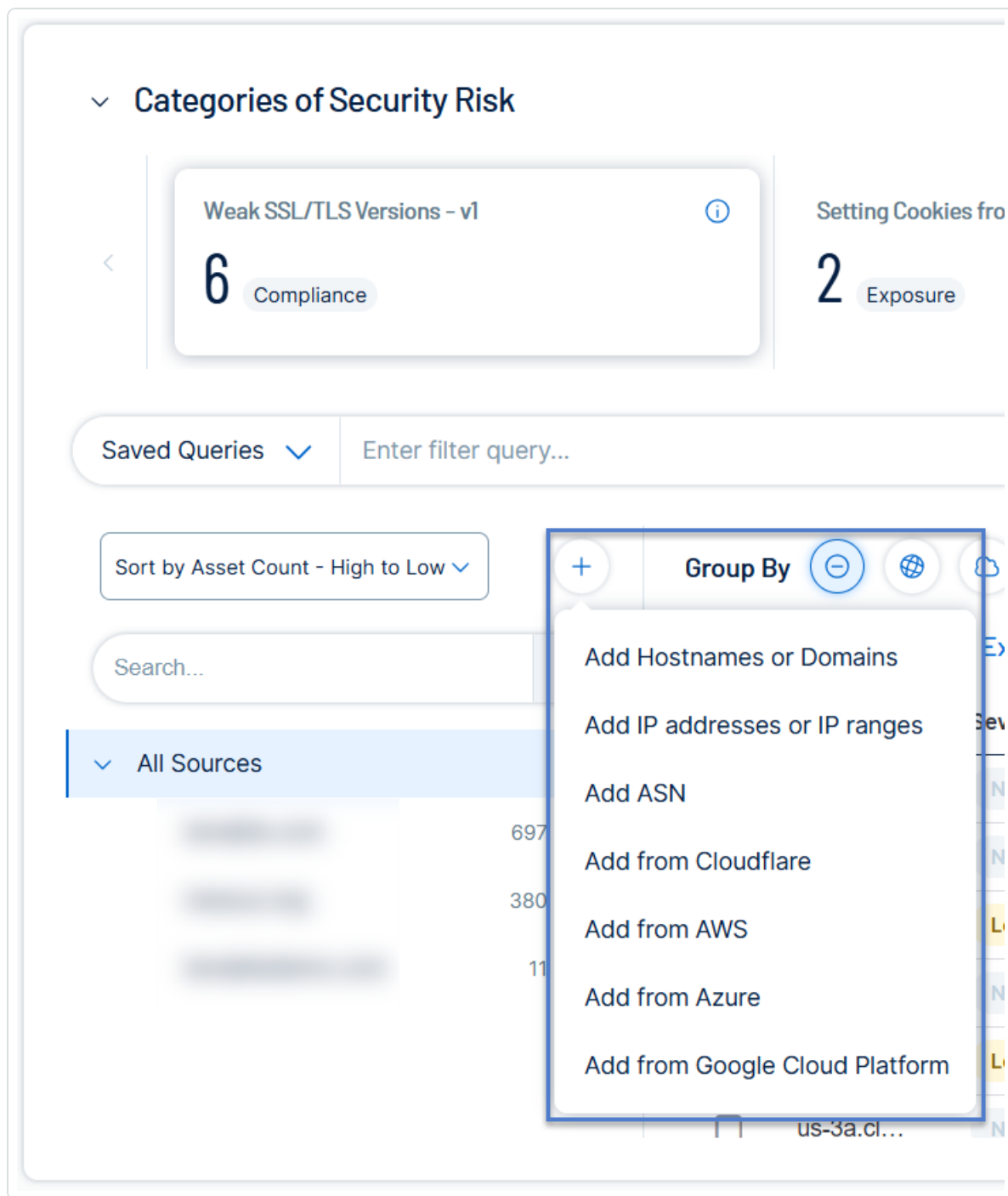
Before you begin

- Make sure that you grant read-only permission for Tenable Attack Surface Management in your AWS account. For more information, see [ReadOnlyAccess](#) in the AWS documentation.
- Add your AWS account to Tenable Attack Surface Management. See [Integrate with AWS](#).

To add sources from AWS:



1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In Tenable Attack Surface Management, in the left pane, click the **⊕** button.
3. In the drop-down list, click **Add from AWS**.



The **AWS keys** window appears with the list of configured AWS API keys.

4. To add sources from your AWS account, click **Add as a source**.

Tenable Attack Surface Management adds the sources from AWS.

Note: Depending on the number of assets, the process may take some time to complete.

Add sources from Azure

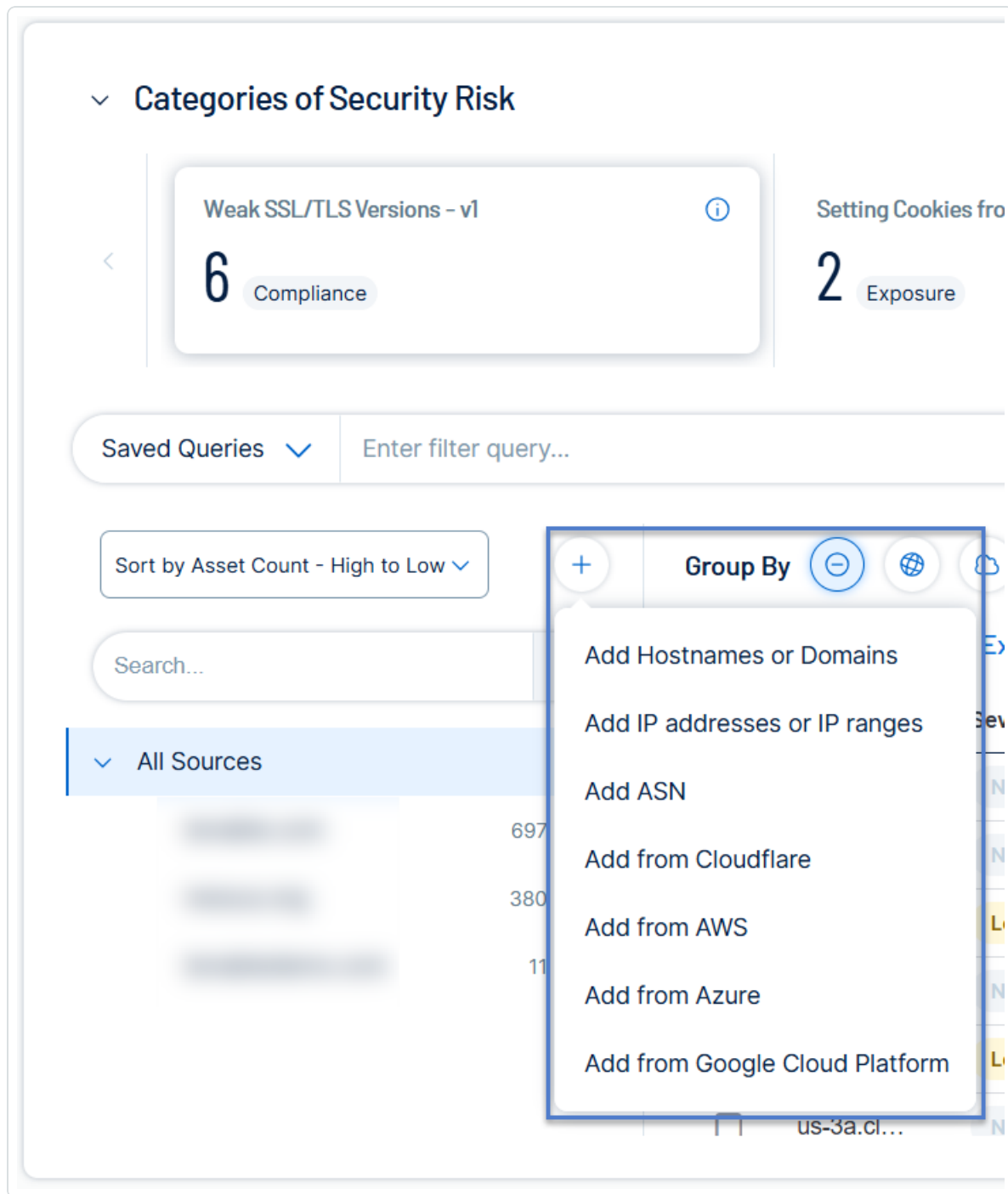
Before you begin

- Make sure that you grant read-only permission (**Reader** role) for Tenable Attack Surface Management in your Azure account. For more information, see [Azure built-in roles for General](#) in the Azure documentation.
- Add your Azure account to Tenable Attack Surface Management. See [Integrate with Microsoft Azure](#) .

To add sources from Azure:



1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In Tenable Attack Surface Management, in the left pane, click the **+** button.
3. In the drop-down list, click **Add from Azure**.



The **Azure keys** window appears with the list of configured Azure API keys.

4. To add sources from your Azure account, click **Add as a source**.

Tenable Attack Surface Management adds the sources from Azure.

Note: Depending on the number of assets, the process may take some time to complete.

Add sources from Google Cloud Platform

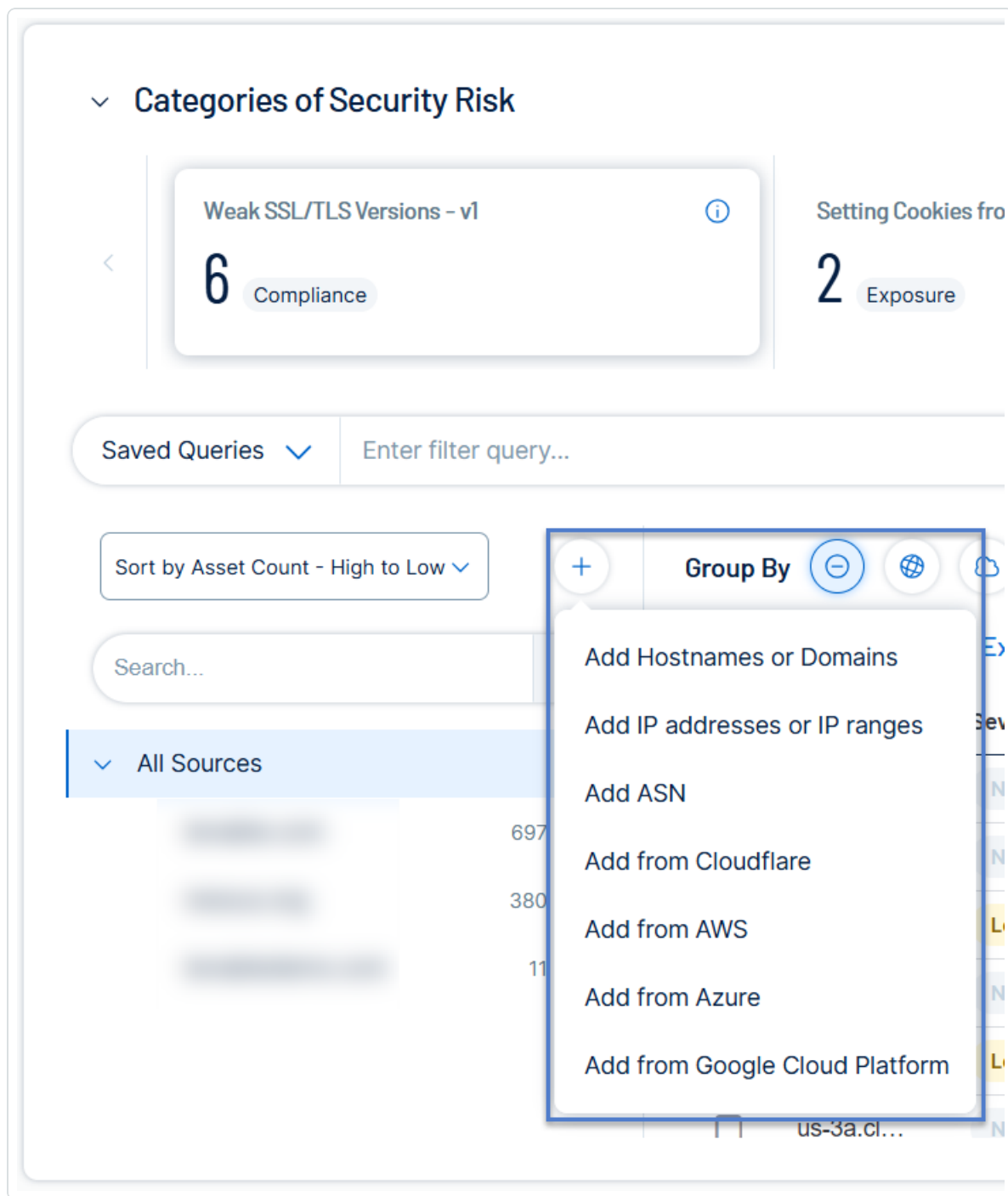
Before you Begin

- Make sure to have a service account with read only permissions. Tenable recommends you use Google's reader role for the service account. To check the service account permissions, click [here](#).
- Add your Google Cloud Platform account to Tenable Attack Surface Management. See [Integrate with Google Cloud Platform](#).

To add sources from Google Cloud Platform:



1. In the left pane of the **Explore** page, click the **+** button.



Tenable Attack Surface Management displays the sources that you can add.

2. In Tenable Attack Surface Management, in the left pane, click the **+** button.
3. In the drop-down list, click **Add from Google Cloud Platform**.



The **Google Cloud Platform keys** window appears with the list of configured Google Cloud Platform API keys.

4. To add sources from your Google Cloud Platform account, click **Add as a source**.

Tenable Attack Surface Management adds the sources from Google Cloud Platform.

Note: Depending on the number of assets, the process may take some time to complete.

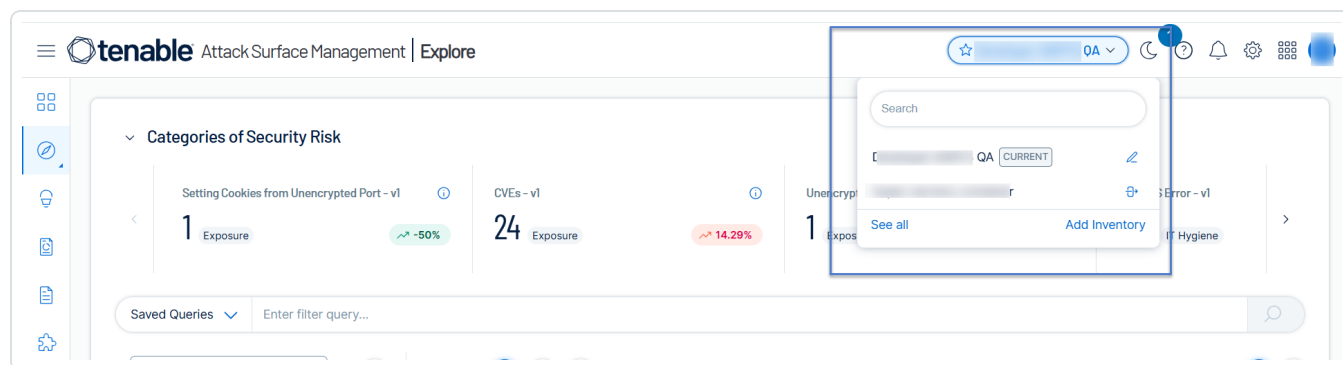
Add a Subdomain

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).


In Tenable Attack Surface Management, you can add a subdomain to an existing domain in your inventory.

To add a subdomain to a domain in your inventory:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.

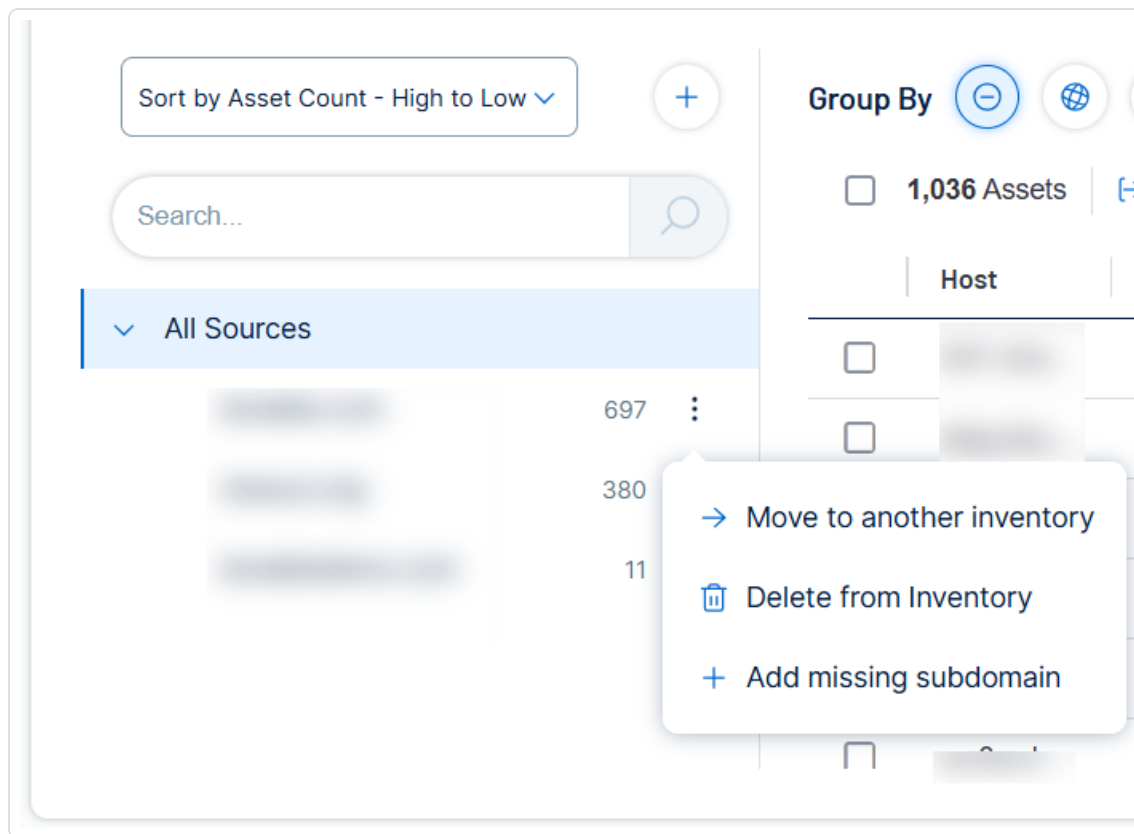


Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select an inventory.
3. In the left pane, from the list of domains, hover over the domain to which you want to add a subdomain.
4. Click the  button.

-
5. On the **Explore** page, in the **All Sources** pane, next to the source, click the  button.

A menu appears.



6. In the drop-down list, click **Add subdomain**.

The **Add missing subdomain** window appears.

7. In the text box, type a subdomain or comma-separated list of subdomains.
8. Click **Add subdomains**.

The subdomains are added to your inventory and Tenable Attack Surface Management automatically begins identifying assets in the subdomain.

Move a Domain

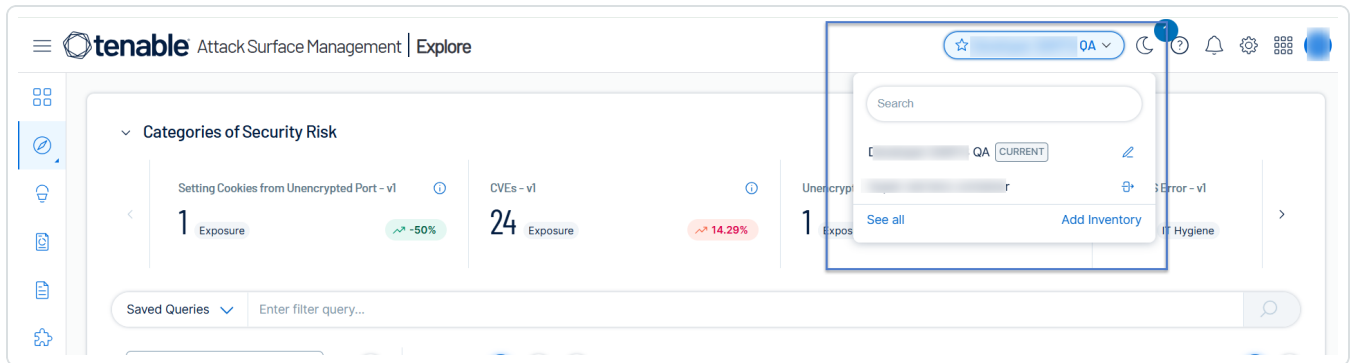
Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

In Tenable Attack Surface Management, you can move an existing domain to another inventory.



To move a domain to a different inventory:



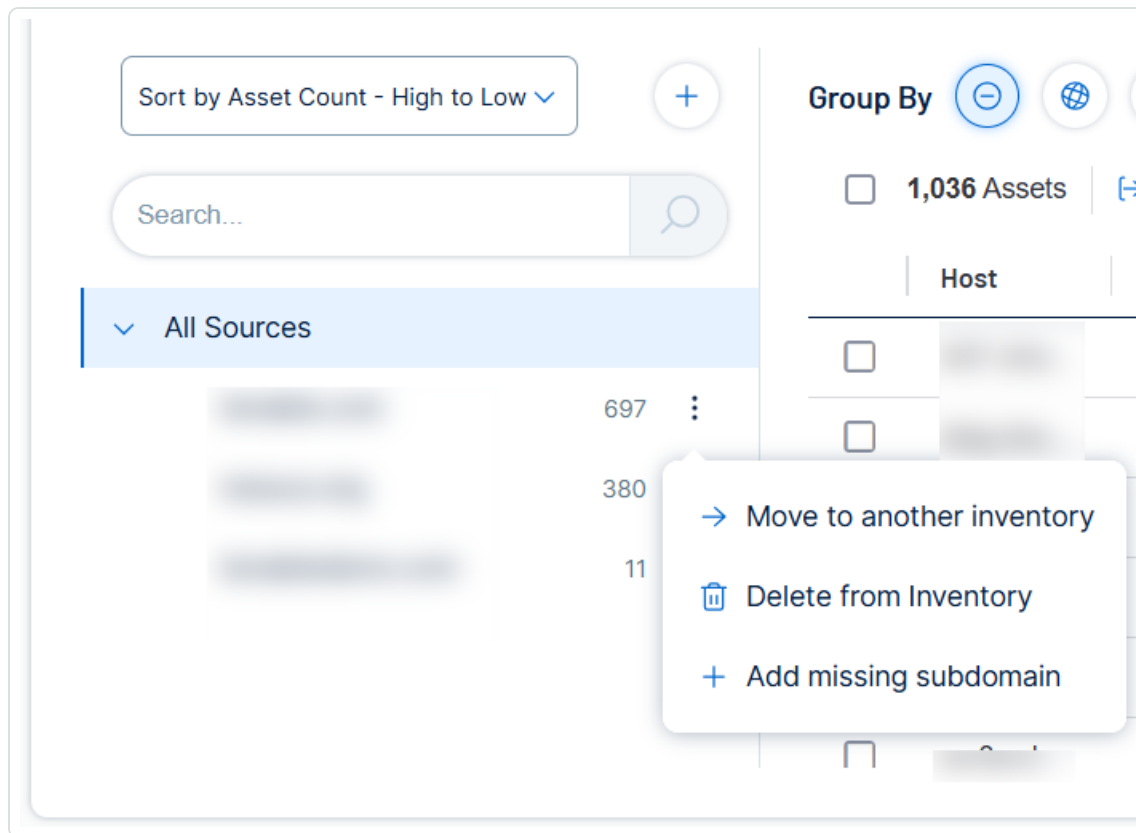
1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select an inventory.
3. In the list of domains, hover over the domain you want to move.
4. Click the  button.
5. On the **Explore** page, in the **All Sources** pane, next to the source, click the  button.

A menu appears.



6. In the drop-down list, click **Move to another inventory**.

The **Move source to another inventory** window appears.

7. In the drop-down box, select the inventory to which you want to move the domain.
8. Click the **Move** button.

The domain is moved to the selected inventory and Tenable Attack Surface Management automatically begins populating the inventory with assets in the domain.

Update a Source Screenshot

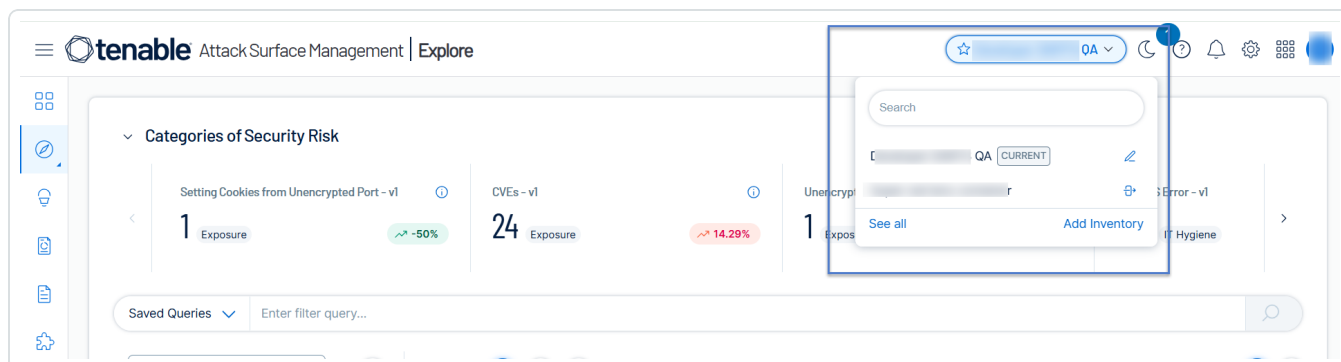
Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

In Tenable Attack Surface Management, you can update the screenshot for a source.

To update the screenshot for a source:



1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select an inventory.
3. In the list of sources, hover over the source for which you want to update the screenshot.

Note: Not every type of source has an available screenshot.

4. Click the  button.
5. In the drop-down list, click **Refresh source screenshot**.

Tenable Attack Surface Management takes a new screenshot of the source.

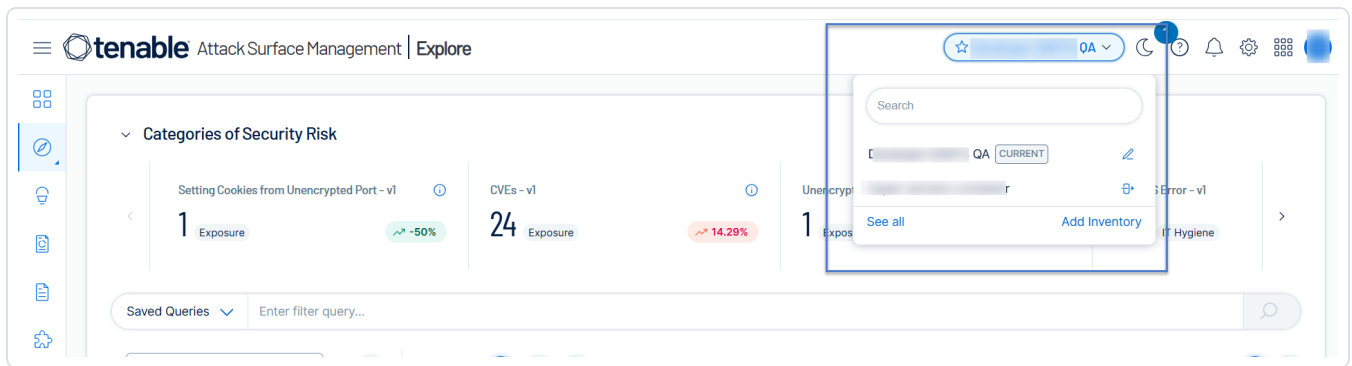
Remove a Source

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).



When you remove a source from an inventory, Tenable Attack Surface Management will remove all assets for the source.

To remove a source from an inventory:

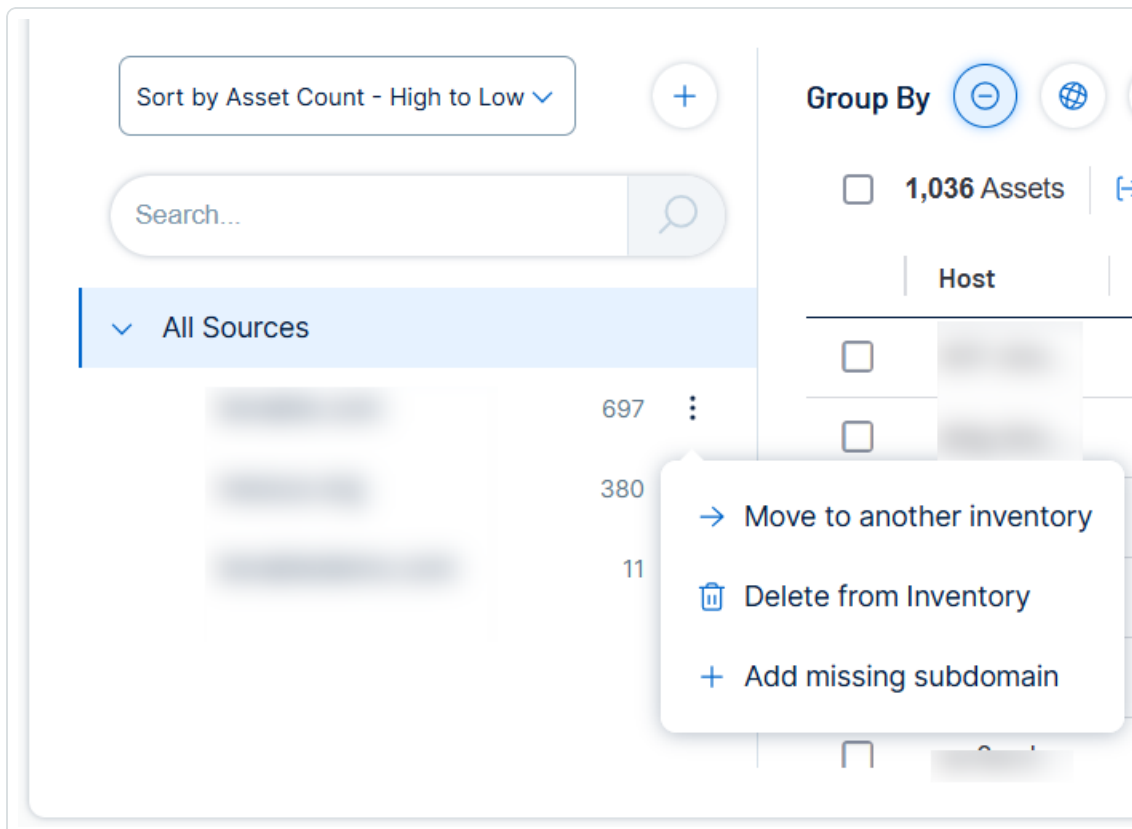
1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select an inventory.
3. In the list of sources, hover over the source you want to remove from the inventory.
4. Click the  button.
5. On the **Explore** page, in the **All Sources** pane, next to the source, click the  button.

A menu appears.





6. In the drop-down list, click **Delete from Inventory**.

Tenable Attack Surface Management deletes the source from the inventory.

Asset Filters

Note: This section describes the filters in the legacy user interface (**Explore > Asset Inventory (Legacy)**).

You can add filters to your inventory to view assets by their importance. Each asset has 130+ properties that can be filtered using one or more filters.

You can filter your assets in two ways:

- **Legacy Filtering** – Allows you to select from available filters to match assets.
- **Robust Filtering** – Allows you to filter by matching column names using strings with AND/OR operators. You can also use two levels of nesting.

Legacy Filtering

To filter your assets:

1. At the top of the table, click **+ Add Filter**.

The Add Filter drop-down appears.

2. Use the **Search for Filters** box or select the filter from the list. For example, **Name**.

The list of operators appears.

3. Select the operator. For example, **contains**.

4. Type the value of the filter, if needed.

5. Click **Done**.

6. (Optional) To add another filter, click **+ Add Filter**.

1. Repeat steps from 2 to 5.

Tenable Attack Surface Management adds a new third filter to the list with the following options:



- **that match all filters** – Lists only the assets that match all the filters.
- **that match any filters** – Lists assets that match any one of the filters.


2. Select one of the options and click **Done**.

Tenable Attack Surface Management shows the filtered results.

Examples

- Filter assets that have a TLS certificate that ages out within 3 days.
 - a. Click **Add Filter**.

A drop-down menu appears.



ASM

Team: j

SSL / TLS Expiration expires in

+ Add Filter

Search

Sort by Asset C

1.

2.

3.

4.

5.

☐ is expired
☐ is not expired
☒ expires in

☐ expired less than
☐ expired more than
☐ expires on
☐ expires after
☐ expires before
☐ is unknown
☐ has any value

Done

<input type="checkbox"/>	Host	Record Type
<input type="checkbox"/>	▶	NS
<input type="checkbox"/>		A
<input type="checkbox"/>	▶	SOA
<input type="checkbox"/>		AAAA
<input type="checkbox"/>		CNAME
<input type="checkbox"/>		A

c. In the **expires in** box, type 3.

d. Click **Done**.

Tenable Attack Surface Management limits your list of assets to only those that have an SSL/TLS certificate aging out within 3 days.



When applying a filter, a column corresponding to the filter is also included in the results. In this case, because the **SSL/TLS Expiration** filter is used, Tenable Attack Surface Management adds an **SSL/TLS Expiration** column.

Using Multiple Filters

Multiple filters can be used at the same time to add incredible granularity. When using multiple filters, you have an option of matching "all" or "any" filters.

Showing assets:

that match all filters

Host is not United States ✕

Sets Cookies yes ✕

[+ Add filter](#)

☒ all filters
☐ any filters

[Done](#)

Host	IP	Record Type	Ports
www	172.67.136.155	A	80, 443, 2082087, 8080,
lhd.m.wikipedia.org	2620:0:862:ed1c::1	CNAME	80, 443

The following are examples of using multiple filters:

- Assets not hosted in the United States

Showing assets where:

Host is not United States

[+ Add filter](#)



- Assets not hosted in the USA that sets cookies

Showing assets:

that match all filters Host is not United States ✕ Sets Cookies yes ✕

- Assets not hosted in the USA that sets cookies, whose registrar email address contains the word "hostmaster, and has port 3306 open.

Showing assets:

that match all filters Host is not United States ✕ Sets Cookies yes ✕ Registrator email contains hostmaster ✕ Ports is 3306 ✕

Robust Filtering

To filter your assets using **Robust filtering**:

- At the top of the table, click **Robust Filtering**.

The **Robust filtering** box appears.

Robust filtering + Add Filter

- Click inside the box.

A drop-down appears with the list of **Column** names.

The screenshot shows the Tenable Attack Surface Management interface. At the top, there's a header with the Tenable logo and 'Attack Surface Management'. Below the header, there's a search bar and a 'Legacy filtering' button. A 'Save filters' dropdown menu is open, showing a list of column names: 'Hosting Provider', 'Hosting Panels', 'Type (partial match)', and 'is-not'. The 'Hosting Provider' column is selected, and its dropdown menu is also open, showing a list of severity levels: 'Low', 'None', and 'High'. The main table displays asset information with columns: Severity, Record Type, IP, ASN, Ports, Tag, and Screenshot. The table shows 1,420 total assets, 3 domains, and 569 subdomains. The page is 1 of 37.



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

3. Filter the assets:

Note: A single query can have only a maximum of 15 filters.

- a. Type the column name or select the column name from the list of matching suggestions.
- b. Select or type the filter type.

c.

Filter Type	Description
contains	Filters for items that contain the filter value.
does not contain	Filters for items that do not contain the filter value.
ends with	Filters for items that end with the filter values.
expired less than	Filters for items that aged out within a specific number of days. This value requires an input for the number of days. For example, SSL / TLS Expiration.
expired more than	Filters for items that aged out more than a specific number of days. This value requires an input for the number of days. For example, SSL / TLS Expiration.
expires after	Filters for items that age out after a specific date. The value requires a date input. For example, SSL / TLS Expiration.
expires before	Filters for items that age out before a specific date. The value requires a date input. For example, SSL / TLS Expiration.
expires in	Filters for items that age out within a specific number of days. This value requires an input for the number of days. For example, SSL / TLS Expiration.
expires on	Filters for items that age out on a specific date. The value requires



	a date input. For example, SSL / TLS Expiration.
has any value	Filters for items that have any associated value.
is	Filters for items that match the selected filter value.
is expired	Filters for items that have aged out. For example, SSL / TLS Expiration.
is not	Filters for items that do not match the filter value.
is not expired	Filters for items that have not aged out. For example, SSL / TLS Expiration.
is not one of	<div>Filters for items that do not match any of the filter values. Note: The filter values must be separated by commas without any spaces. For example, Host <code>is-not-one-of x,y,z</code>.</div>
is one of	<div>Filters for items that match one of the filter values. Note: The filter values must be separated by commas without any spaces. For example, Host <code>is-one-of x,y,z</code>.</div>
is unknown	Filters for items that have unknown value.
not scanned	Filters for items that are not scanned.
scanned	Filters for items that are scanned.
starts with	Filters for items that start with the filter values.
yes	Filters for items that match the "Yes" input. For example, Cloud Hosted .
no	Filters for items that match the "No" input. For example, Cloud Hosted .
greater than	Filters for items that match a value greater than the specified



	number.
less than	Filters for items that match a value less than the specified number.

d. Provide the values for the selected type.

Note: For special filters such as tags and dates, the filter displays the relevant menu to select the values.

- **Tag filter** – Displays a drop-down with the list of available tags.
- **Date filter** – Displays a date picker where you can input the date.

e. Type the **End label**, if prompted.

f. For multiple querying, type **AND** or **OR** operators in the box and select one of the operators.

Note: AND and OR operators are not allowed on the same level.

Note: If you want to filter on a value that has quotation marks (") or spaces, then you must wrap the value in quotation marks (").
If there are quotation marks within the value, then you must use the escape character (\) for the quotation marks ("). For example, to filter the value `<div id="filter_value"`, do this:
`"<div id=\"filter_value\""`

g. (Optional) Use parentheses to add nested filters.

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

4. (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 clear the filters, click the **X** button in the right corner of the text box.

5. Click **Apply**.

Tenable Attack Surface Management filters your data.

6. (Optional) Save the filters to access later or share.



Filter Examples

Filter 1: Host contains example.com

Where:

- Host is the column.
- contains is the filter type.
- example.com is the value.

Filter 2: SSL / TLS Valid From less-than 3 days ago

Where:

- SSL / TLS Valid From is the column name.
- less-than is the filter type.
- 3 is the value.
- days ago is the end label. This is not optional and Tenable Attack Surface Management prompts you to type the text when the filter requires it.

Convert Legacy Filtering to Robust Filtering

If you are using Legacy filtering to filter your assets, you can change your filtering method to Robust filtering by clicking **Robust Filtering**. This converts your selected filters to the Robust filtering mode. You can also convert your saved filters to Robust filtering.

Note: You cannot convert the filtering method from **Robust filtering** to **Legacy filtering**.

Filtering on Tags

When adding an asset filter from the asset inventory page, selecting the **Tag** filter provides these options: **is** and **is not** - filtering for assets that do have a particular tag or do not have a particular tag, respectively. Choosing an operator displays a drop-down list of tags to filter on.

However, not all tags are available to select in this list. The following are the conditions based on which the tags are listed in the tag filter drop-down list.



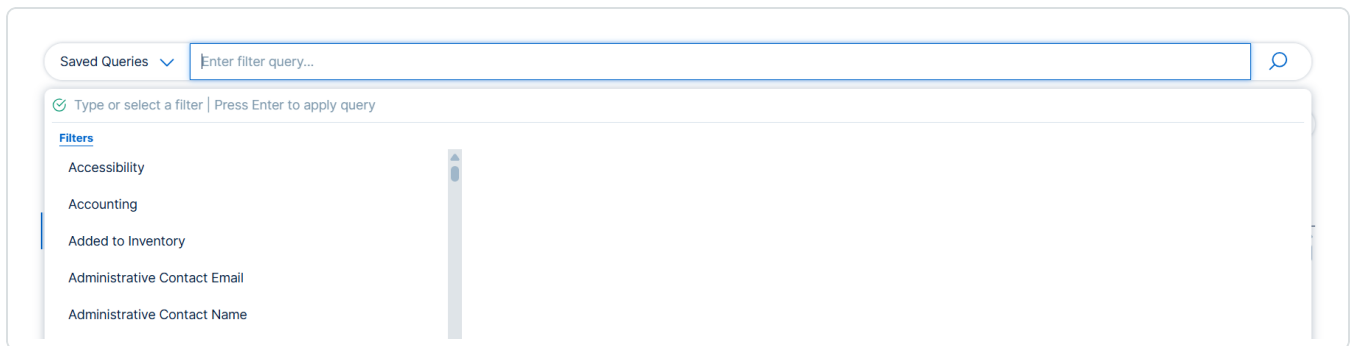
- Tags with a specific custom value type are not listed.
- Only tags with the **I don't want to assign values with this Tag** value are listed.
- Tags with the value type, such as **Keyword**, **Date**, or **Boolean**, are listed as individual filters in the list of filters in the **Generic** section in the **Manage Columns** page.

Filter Your Assets in the Explore Dashboard

Tenable Attack Surface Management uses filters to provide powerful inventory search capabilities. Filters allow you to view specific subsets of assets in your inventory.

To apply a filter:

1. Click inside the **Enter a filter query** box to display the list of available filters.



2. Type or select a filter you want to use.

A list of operators appears. This list varies based on the filter you select.

Saved Queries
Enter filter query...

Type or select a filter

Filters

Accessibility
Accounting
Added to Inventory
Administrative Contact Email
Administrative Contact Name
Administrative Contact Organization
Administrative Contact Telephone
Advertising Networks

Nesting Operators

(

3. If the operator requires a value, type that value in the text box.

Categories of Security Risk

Weak SSL/TLS Versions - v1

Setting Cookies from Unencrypted Port - v1

CVEs - v1

Unencrypted Final URL - v1

6 Compliance

3 Exposure

24 Exposure

1 Exposure

Saved Queries
SSL/TLS Expiration expires in 30 days

Type or select a condition to start adding another filter | Press Enter to apply query

Filters

Social Logins
Social Profiles
SSL/TLS Cypher Suites
SSL/TLS error
SSL/TLS EV Certificate
SSL/TLS Expiration
SSL/TLS Fingerprint

Operators

is expired
is not expired
expires in
within the last
older than
expires on

Values

30
hours
days
months
years

Conditions

AND
OR

- 254 -

4. Add **AND** or **OR** conditions as needed.

5. Press **Enter** to apply the query.

Your inventory displays only assets matching the filter criteria.

In this example, your inventory displays only assets with a TLS certificate that expires within the next 30 days. The SSL/TLS Expiration column also appears.

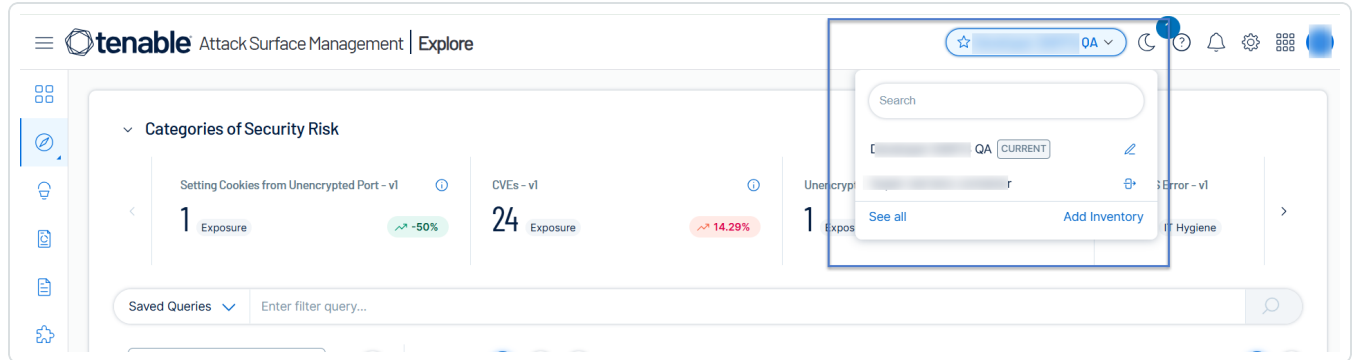
Asset Details

Note: This section describes how to access asset details in the legacy user interface. To view the new interface documentation, see [Asset Filters](#).

When you click on an asset in Tenable Attack Surface Management, a page appears that includes all known information about the asset.

To view details for an asset in your inventory:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the list, hover over the asset for which you want to view more details.



<

3. Click the button.

The details page for the asset appears.

4. Click the inventory you want to view.

The **Explore** page displays the assets for the inventory.

5. In the assets table, click the asset name.

Tenable Attack Surface Management displays the asset details.



Tag

+ Add tags

Severity Breakdown LOW

Expired SSL	Asset is using SSL cert passed expiration date.
Outdated TLS	Asset supports depreciated TLS versions.

For more information, see [View Asset Attribution](#).

Networking Details

Networking

Domain	██████████.██
Record Value	██████████.██████████.██
Host	██.██████████.██
Record Type	CNAME
IP	██████████.██████████.██████████.██████████
ASN	WIKIMEDIA
Final url	https://██████████.██████████.██████████.██████████.██████████
Cloud Hosted	no
Is subdomain	yes

Services Details

Port	Service	Last seen	Banner
80	http-proxy	4 days ago	"HTTP/1.1 200 OK" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36"
443	https	8 days ago	"HTTP/1.1 200 OK" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36"



SSL / TLS

SSL / TLS Issuer Country	US
SSL / TLS Issuer Organization	DigiCert Inc
SSL / TLS Issuer Common Name	DigiCert TLS Hybrid ECC SHA384 2020 CA1
SSL / TLS protocol	TLSv1.2
SSL / TLS Fingerprint	I [REDACTED]
SSL / TLS Subject Alt Name	[REDACTED]
SSL / TLS Cypher Suites	[REDACTED]
JARM Hash	[REDACTED]
SSL / TLS EV Certificate	no



Location Details

This section includes a pin on a map, and any known location details for the asset, including continent, country, time zone, and the country where the asset is registered.

Location



Continent	North America
Country	United States
Time zone	America/Chicago
Registered Country	United States

HTTP Details

HTTP Response

Content type	text/html; charset=UTF-8
Response code	301
Server	mysql400.sjiedu.com.net
Vary	Accept-Encoding,X-Forwarded-Proto,Cookie,Authorization
Document Title	Wikipedia, slobodna enciklopedija
Sets Cookies	yes
Login Forms	no
Login	no

HTTP Headers

Header name	Header value
server	cloudflare
x-content-type-options	nosniff
p3p	CP="5000 ut us no opt optorg optloc" P3P for more info."
vary	Accept-Encoding,X-Forwarded-Proto,Cookie,Authorization
cache-control	s-maxage=1200, must-revalidate, max-age=0
last-modified	Mon, 14 Feb 2022 06:19:51 GMT
location	https://www.cloudflare.com/robots.txt
content-length	0
content-type	text/html; charset=UTF-8
age	1419
x-cache	MISS from cache
x-cache-status	hit-front
server-timing	cache-ttl: 1200, cache-status: hit-front, cache-variant: none
strict-transport-security	max-age=106384710; includeSubDomains; preload

View Asset Attribution



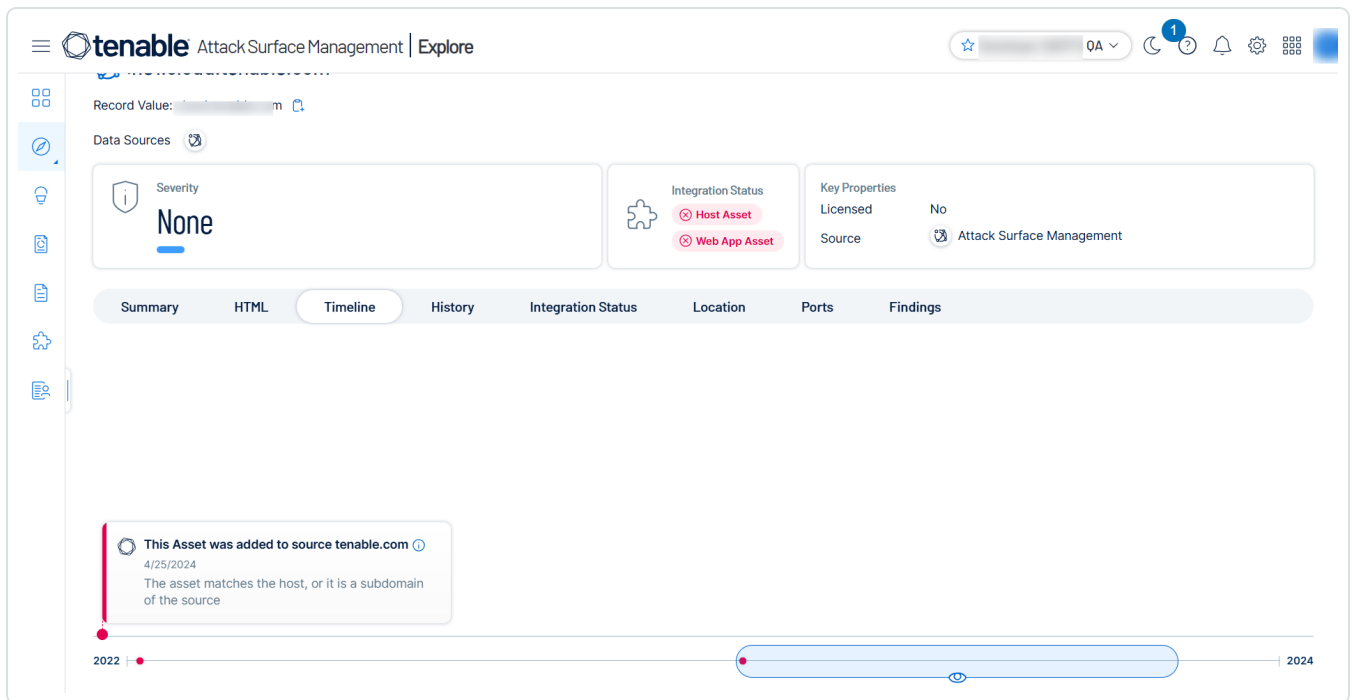
The **Origin** section on the **Asset Details** page includes a timeline illustrating each stage of the Tenable Attack Surface Management process of adding an asset to the inventory, including:

- The ID of the user who initially added the source to the inventory and thereby directly or indirectly added the asset.
- The timestamp when the source was added.
- The timestamp when the asset was added to the source.
- If Tenable Attack Surface Management adds the asset based on an [automation rule](#), then the timeline shows the rule's creation time. For instance, an asset may be added when an automation rule accepts a suggested domain into the inventory. You can click the **View automation rule** link to open the **Add Automation Rule** window to view or modify the automation rule. If the automation rule was updated, you can click the **View logs** link to open the **Activity Logs** page to view the changes.
- The type of source. For example, if the source is IP-based, domain-based, AWS, or Cloudflare.
- If an asset belongs to multiple sources, each source is highlighted in a different color. For example, blue for an IP-based source and dark blue for a domain-based source.
- A **Find similar assets** link to the assets list page that shows assets with similar origin.

To view the origin details for an asset in your inventory:

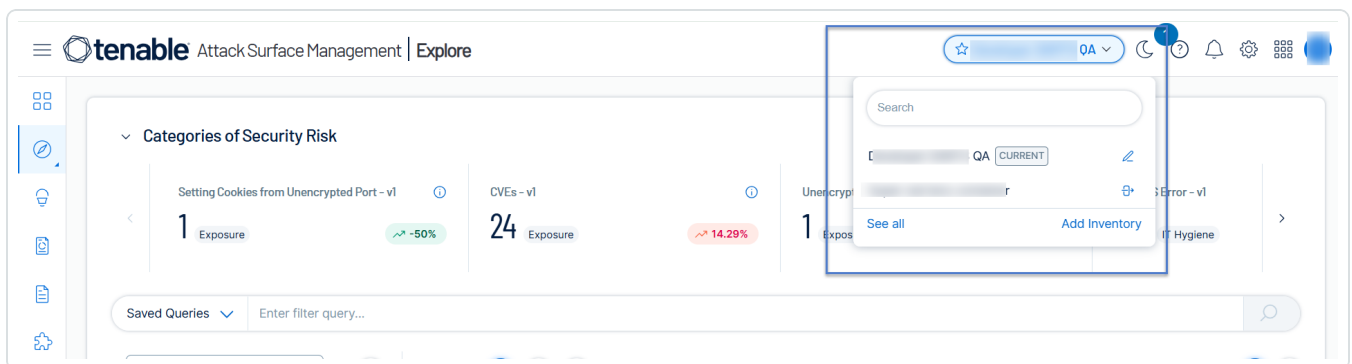
1. In the **Explore** page, click the asset name in the assets table.

Tenable Attack Surface Management displays the asset details.



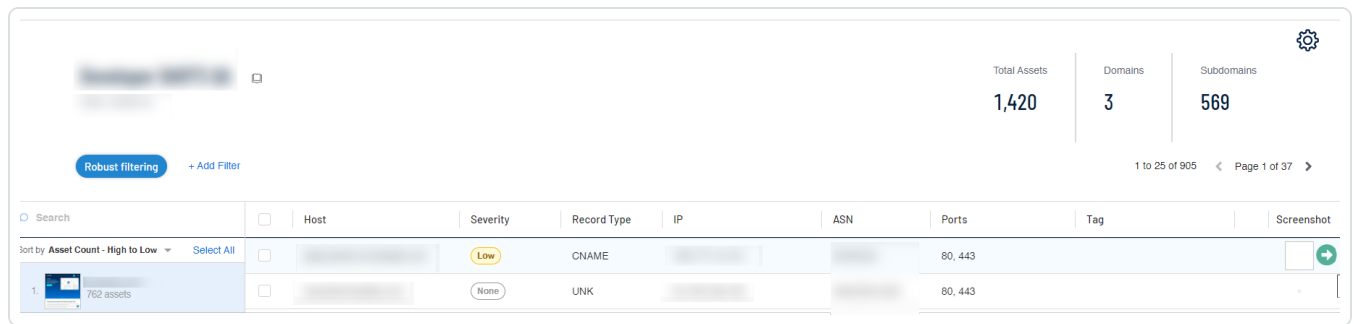
Click the **Timeline** tab at the top of the page for the asset attribution details. You can use the slider to navigate the various timelines associated with the asset.

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select an inventory.
The inventory page appears with the list of assets.
3. In the list, hover over an asset to see its details.



The screenshot shows the Tenable Attack Surface Management interface. At the top right, there are three summary cards: 'Total Assets' with a value of 1,420, 'Domains' with a value of 3, and 'Subdomains' with a value of 569. Below these is a pagination bar showing '1 to 25 of 905' and 'Page 1 of 37'. The main table has columns: Search, Host, Severity, Record Type, IP, ASN, Ports, Tag, and Screenshot. The table is sorted by 'Asset Count - High to Low'. The first row shows a host with a 'Low' severity and a 'CNAME' record type. The second row shows a host with a 'None' severity and an 'UNK' record type. A green arrow button is visible at the end of the first row.

Search	Host	Severity	Record Type	IP	ASN	Ports	Tag	Screenshot
Sort by Asset Count - High to Low		Low	CNAME			80, 443		
		None	UNK			80, 443		

4. Click the  button.

The asset details page appears. See the **Origin** section at the top of the page for the asset attribution details. You can use the slider to navigate the various timelines associated with the asset.

Export an Asset

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

In Tenable Attack Surface Management, you can export an asset in CSV or XLSX format.

To export an asset:

1. [View the details page for the asset.](#)
2. At the bottom of the page, click the **Export to CSV** or **Export to XLSX** button.



Asset history

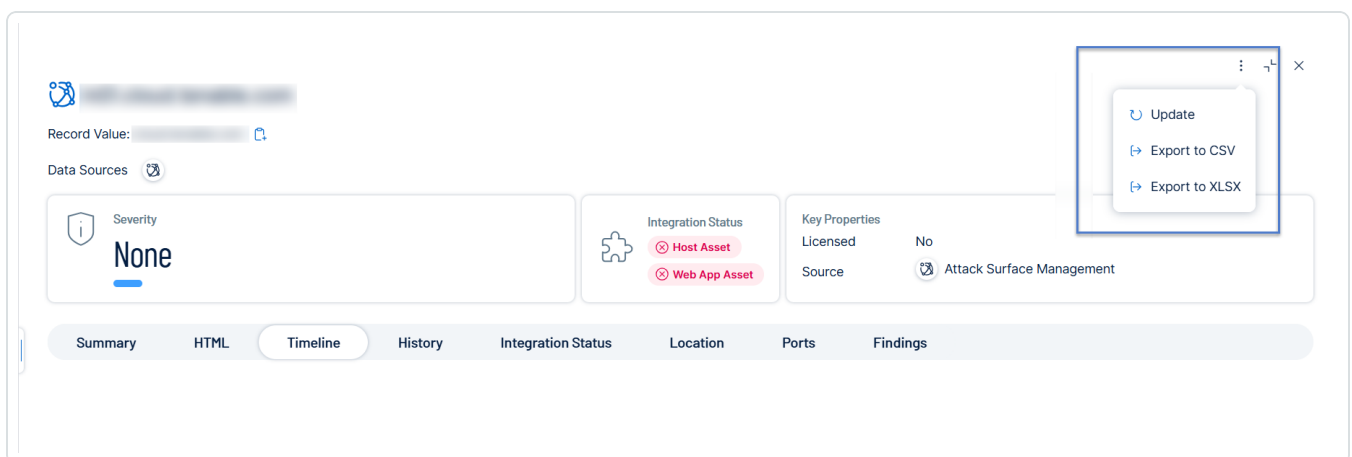
Date	Event
2022-11-08 19:07:13	Asset was added to source [REDACTED]
2024-08-14 13:26:05	Asset was tagged with asd tag
2025-02-06 22:02:22	Asset data for Body was last updated
2025-02-06 22:24:46	Asset data for Port(s) was last updated
2025-02-06 22:50:07	Asset data for IpGeo was last updated
2025-02-06 22:50:33	Asset data for SSL was last updated
2025-02-06 22:51:16	Asset data for Header was last updated
2025-02-06 22:54:10	Asset data for Advanced Details was last updated
2025-02-06 22:58:09	Asset data for WPScan was last updated
2025-02-06 23:04:16	Asset data for RBL was last updated
2025-02-06 23:09:06	Asset data for Domain Info was last updated
2025-02-06 23:44:18	Asset data for Screenshot was last updated

[Update](#)[Export to CSV](#)[Export to XLSX](#)

Tenable Attack Surface Management downloads the CSV or XLSX file.

3. On the asset details page, in the upper-right corner, click the  button.

A menu appears.



The screenshot shows the Tenable Attack Surface Management interface. At the top, there's a header with the Tenable logo and a record value. Below this, there's a section for 'Data Sources' and a 'Severity' indicator showing 'None'. The 'Integration Status' section shows 'Host Asset' and 'Web App Asset' with red status indicators. The 'Key Properties' section shows 'Licensed' as 'No' and 'Source' as 'Attack Surface Management'. A menu is open in the upper-right corner, displaying options: 'Update', 'Export to CSV', and 'Export to XLSX'. The bottom of the page has a navigation bar with tabs: 'Summary', 'HTML', 'Timeline', 'History', 'Integration Status', 'Location', 'Ports', and 'Findings'.

4. Click  **Export to CSV** or  **Export to XLSX**.

Tenable Attack Surface Management exports the asset details in the selected format.



Manage Asset Tags

Note: This section describes asset tags in the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

You can add descriptive tags to define and categorize your assets. You can create tags that do not require any values and also which require values such as specific keywords, booleans, cost, and percentage.

Create a Tag

To create an asset tag:

1. In the assets list, do one of the following:

- In any asset row, click the  button.

A menu appears.

- Select the checkbox next to any asset.

Tenable Attack Surface Management enables the header bar.

2. Click  **Add Tags**.

A drop-down menu appears.

3. Click **Create new tag**.

The **Create new tag** window appears.

4. In the **Tag name** box, type a name for the tag.

In the **Value type** drop-down box, select one of the following:

- **I don't want to assign values with this tag**
- **Keyword**
- **Number**
- **Cost**



- **Percentage**
- **Boolean**

5. Click **Save**.

Tenable Attack Surface Management saves the tag, which you can then apply to assets.

When you create a tag with a value type, a column gets added to the assets table where you can edit the value for that tag. To add or edit the value, click the cell for that tag. For example, if you create a **Boolean** tag, you can select the required values **Yes** or **No** in the specific column for that tag.

Assign Tags to Assets

Before you begin

- Make sure you create the tags you require.

To assign tags to a single asset or multiple assets:

1. In Tenable Attack Surface Management, in the left navigation bar, click the  button.

The **Explore** page appears.

Scope	Action
Assign tags to a single asset	<ol style="list-style-type: none">1. In the assets table, select the checkbox next to the asset to which you want to assign a tag. Tenable Attack Surface Management enables the action bar at the top of the table.2. Click Actions > Add Tags. The list of available tags appears.3. Select the checkbox next to the tags that you require.4. Click Add. Tenable Attack Surface Management applies the tags that do not require




	<p>any values. For tags that require a value, the Enter Tag values window appears.</p> <p>5. Provide the values for the tags, if applicable and click Save.</p> <p>Tenable Attack Surface Management applies the selected tags to the asset.</p> <div>Tip: To assign tags that require a value, in the row of the asset for which you want to assign a tag, click the cell to add or edit the value for that tag.</div>
Assign tags to multiple assets	<p>1. In the assets table, select the checkboxes next to the assets to which you want to assign a tag.</p> <p>Tenable Attack Surface Management enables the action bar at the top of the table.</p> <p>2. (Optional) To select all assets, select the checkbox at the top of the table.</p> <p>A message appears at the top of the table that all 25 assets on the page are selected along with a link with the total number of available assets that you can select.</p> <p>3. Click Actions > Add Tags.</p> <p>The list of available tags appears.</p> <p>4. Select the checkbox next to the tags that you require.</p> <p>5. Click Add.</p> <p>Tenable Attack Surface Management applies the tags that do not require any values. For tags that require a value, the Enter Tag values window appears.</p> <p>6. Provide the values for the tags, if applicable and click Save.</p> <p>Tenable Attack Surface Management assigns the selected tags to the selected assets.</p>

Scope

Action



<p>Add tags to a single asset</p>	<ol style="list-style-type: none">1. To add tags to a single asset:<ul style="list-style-type: none">• In the row of the asset to add tags, click the  button<p>A menu appears.</p><ul style="list-style-type: none">• Select the checkbox for the asset to add tags.<p>Tenable Attack Surface Management enables the header.</p><ul style="list-style-type: none">• Right-click the asset you want to add tags.<p>A menu appears.</p>2. Select Add Tags. <p>The Add Tags window appears.</p> <ol style="list-style-type: none">3. Select or create a new tag. <p>Tenable Attack Surface Management adds the tags to the Tags to be Added box.</p> <ol style="list-style-type: none">4. Click Add Tags. <p>Tenable Attack Surface Management adds the tags to the asset.</p>
<p>Add tags to multiple assets</p>	<p>To add tags to multiple assets:</p> <ol style="list-style-type: none">1. Select the checkbox for one or several assets you want to add tags. <p>Tenable Attack Surface Management enables the header.</p> <ol style="list-style-type: none">2. Select Add Tags. <p>The Add Tags window appears.</p> <ol style="list-style-type: none">3. Select or create a new tag. <p>Tenable Attack Surface Management adds the tags to the Tags to be Added box.</p>



4. Click **Add Tags**.

Tenable Attack Surface Management adds the tags to the assets.

Remove Tags

Removing tags for an asset removes the tags from Tenable Attack Surface Management and as a result from all the assets that have the specific tag.

To remove tags:

1. In the assets table, select the checkbox next to an asset that has the tag applied.

Tenable Attack Surface Management enables the action bar at the top of the table.


2. Click **Actions > Remove Tags**.

The list of available tags appears.

3. Select the checkbox next to the tags you want to remove.

4. Click **Remove**.

Tenable Attack Surface Management removes the tag.

Scope	Action
Remove tags from a single asset	<ol style="list-style-type: none">1. To remove tags from a single asset:<ul style="list-style-type: none">• In the row of the asset to remove tags, click the  buttonA menu appears.• Select the checkbox for the asset to remove tags.Tenable Attack Surface Management enables the header.• Right-click the asset for which you want to remove tags.



	<p>A menu appears.</p> <ol style="list-style-type: none">2. Select Remove Tags. <p>The Remove Tags window appears.</p> <ol style="list-style-type: none">3. Select the tags to remove. <p>Tenable Attack Surface Management adds the tags to the Tags to be Removed box.</p> <ol style="list-style-type: none">4. Click RemoveTags. <p>Tenable Attack Surface Management removes the tags to the asset.</p>
Remove tags from multiple assets	<p>To remove tags from multiple assets:</p> <ol style="list-style-type: none">1. Select the checkbox for one or several assets for which you want to remove tags. <p>Tenable Attack Surface Management enables the header.</p> <ol style="list-style-type: none">2. Select Remove Tags. <p>The Remove Tags window appears.</p> <ol style="list-style-type: none">3. Select the tags to remove. <p>Tenable Attack Surface Management adds the tags to the Tags to be Removed box.</p> <ol style="list-style-type: none">4. Click Remove Tags. <p>Tenable Attack Surface Management removes the tags from the assets.</p>

Tagging View

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

The **Tagging View** page is similar to the asset details page and shows all available data for an asset.



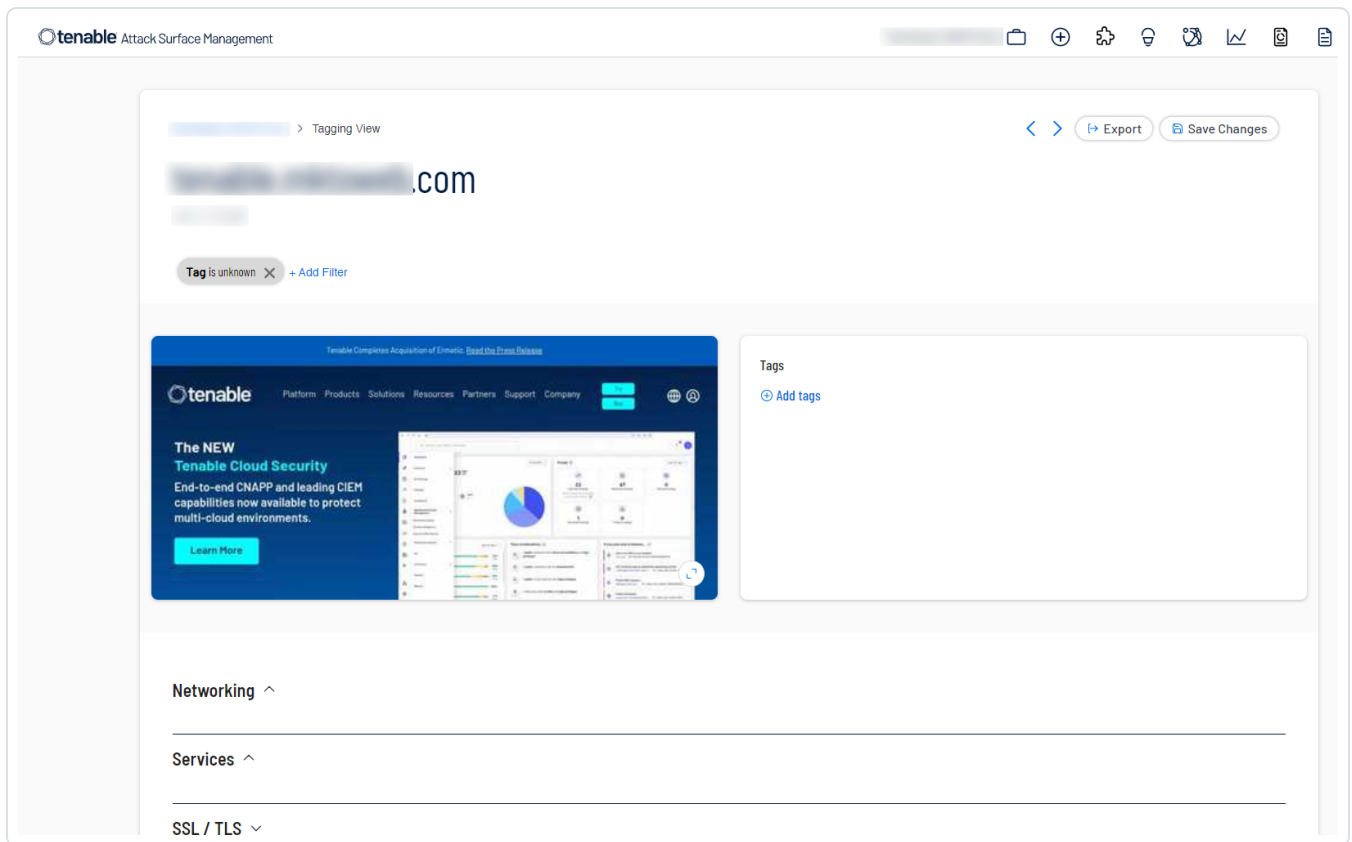
Access the Tagging View Page

1. On the Inventory page, in the upper-right corner, click the  button.

A drop-down menu appears.

2. Select **Tag Assets Quickly**.

The **Tagging View** page appears with details of an asset that matches the filter criteria **Tag is unknown**.



The **Tagging View** page shows the following details about an asset:

- Screenshot of the asset
- Tags
- Networking
- Services



- SSL/TLS
- RBL
- Location
- General
- Web applications
- Programming
- Data
- Social
- Finance
- Marketing
- HTTP response
- HTTP headers
- HTTP Security headers
- Domain info

Note: If the data for any section is not available or applicable for an asset, that section is not displayed.

Tip: The shortcuts to navigate or select tags are provided at the bottom of the page.

Export the Asset Details

1. On the **Tagging View** page, in the upper- right corner, click  **Export**.

A drop-down menu appears with these options:

- Export to CSV
- Export to XLSX

2. Select a format to export the asset details.



Tenable Attack Surface Management exports the details to the selected format and downloads it to your local system.

Tag Assets Quickly

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

You can use the **Tagging View** page to filter out assets that do not have any tags associated and quickly add tags to them.

To add assets:

1. On the Inventory page, in the upper-right corner, click the  button.

A drop-down menu appears.

2. Select **Tag Assets Quickly**.

The **Tagging View** page appears with details of an asset that matches the filter criteria **Tag is unknown**. For more information, see [Tagging View](#).

3. (Optional) Click  **Add Filter** to add additional or new filters.

Tenable Attack Surface Management displays an asset that matches the new filter.

4. (Optional) Click the  button or the  button to move to the next asset or the previous asset.

5. To tag the asset, in the **Tags** section, click  **Add tags** to add a new tag or click an already existing tag.

The new tag appears in the **Tags** section.

6. Click the tag to assign them to the asset.

The tag appears in blue indicating that the tags are selected.

7. Click **Save Changes**.

Tenable Attack Surface Management assigns the tags to the asset.

Move or Copy Assets to another Inventory

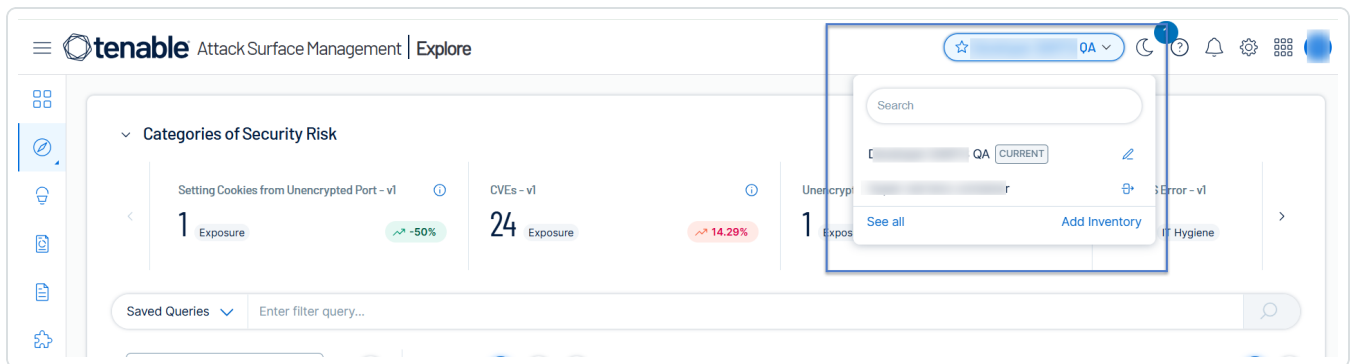


Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

You can move or copy assets from one inventory to another inventory. The target inventory adds these assets to a new source with the name: **From other inventories**. When you move assets, the source inventory archives these assets, whereas copying the assets leaves them in the original inventory.

Move assets from one inventory to another inventory:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select an inventory.

The assets list appears.

3. Select the assets you want to move to another inventory.

Tenable Attack Surface Management enables the **Actions** menu in the upper-right corner.

4. Click **Move to another inventory**.

The **Move source to another inventory** window appears.

Note: The **Move to another inventory** option is available only if the current user has **Archive** permission in the current inventory.

5. Select an inventory from the list to move the assets.



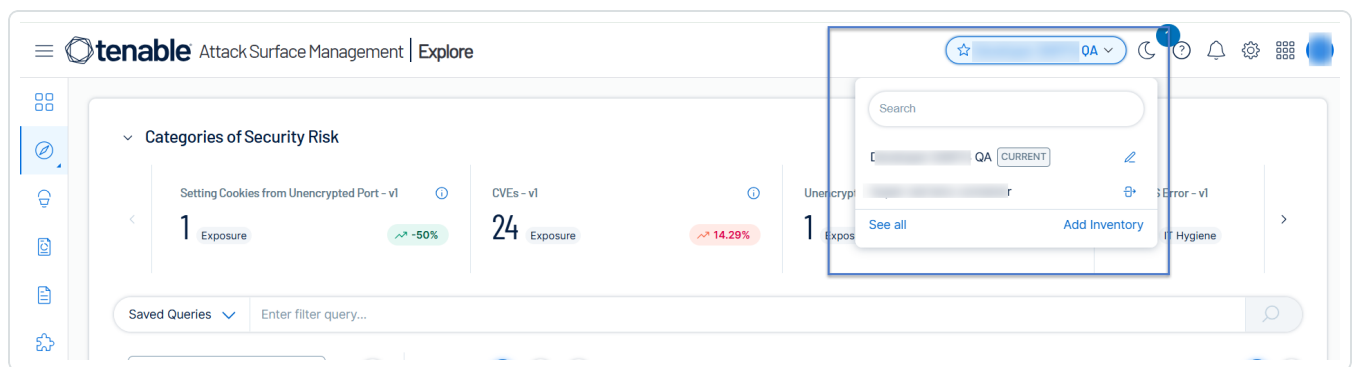
Note: Use the **Search** box to search for a specific inventory.

6. Click **Move**.

Tenable Attack Surface Management moves the assets to the target inventory and also archives them in the source inventory.

Copy assets from one inventory to another inventory:

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select an inventory.

The assets list appears.

3. Select the assets you want to copy to another inventory.

Tenable Attack Surface Management enables the **Actions** menu in the upper-right corner.

4. Click **Copy to another inventory**.

The **Copy Assets to another inventory** window appears.

5. Select an inventory to which you want to move the assets.

Note: Use the **Search** box to search for a specific inventory.

6. Click **Copy**.

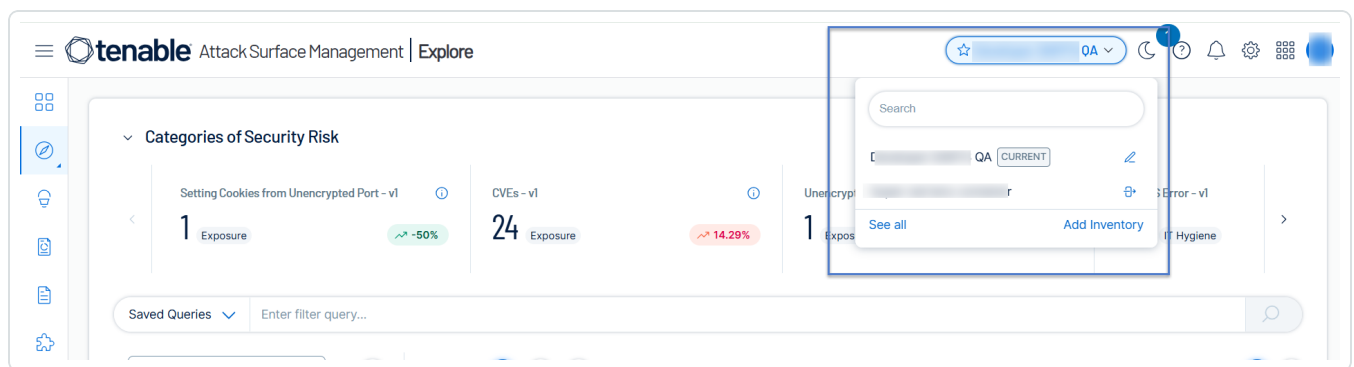
Tenable Attack Surface Management copies the assets to the target inventory and also retains them in the source inventory.

Archive an Asset

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

You can archive single or multiple assets from the inventory.

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select an inventory.

The assets list appears.

3. Select the assets you want to archive.

Tenable Attack Surface Management enables the **Actions** menu in the upper-right corner.

4. Click **Archive**.

Tenable Attack Surface Management archives the assets.

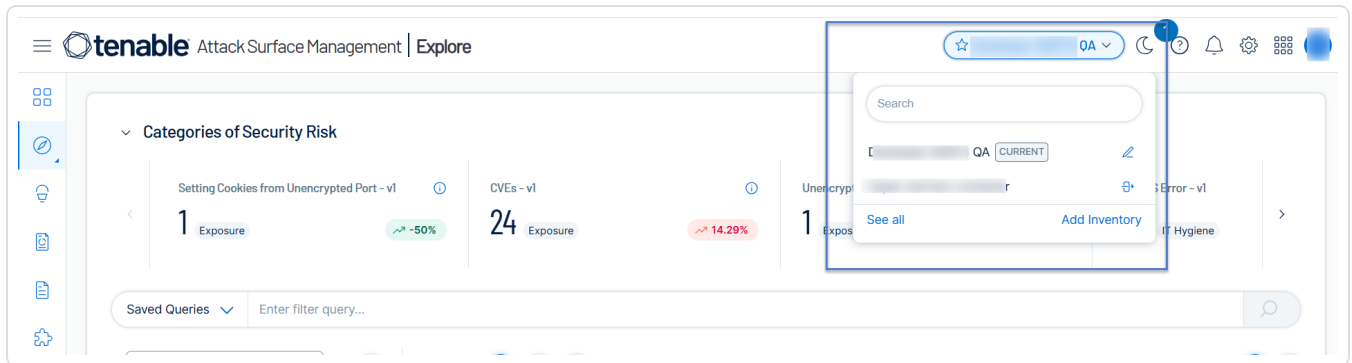
Create an Advanced Network Scan

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

You can create an advanced network scan for assets.



1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select an inventory.

The assets list appears.

3. Select the assets you want to scan.

Tenable Attack Surface Management enables the **Actions** menu in the upper-right corner.

4. Click **Create Advanced Network Scan**.

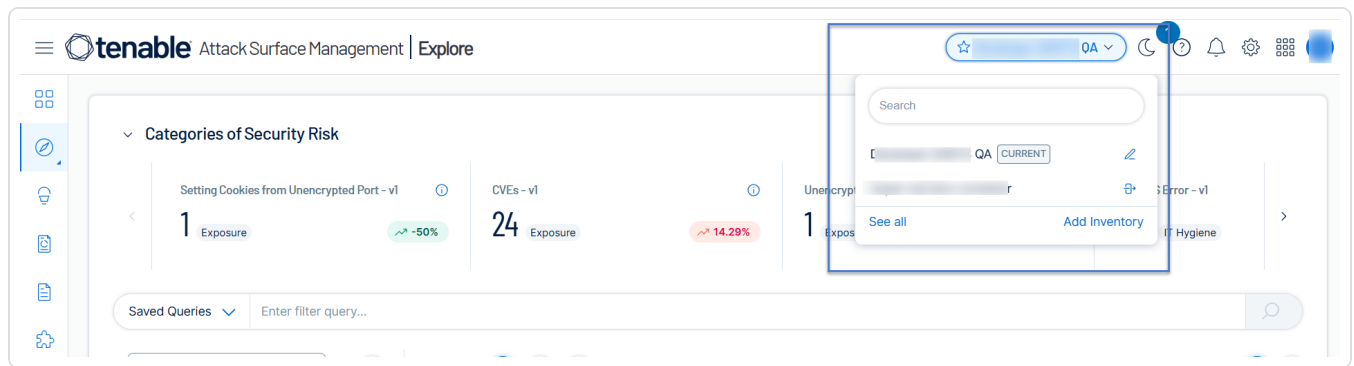
Tenable Attack Surface Management redirects to the **Create a Scan - Advanced Network Scan** page in Tenable Vulnerability Management.

Create a Web Application Scan

Note: This section describes the legacy user interface (**Explore > Asset Inventory (Legacy)**). To view the new interface documentation, see [Inventory](#).

You can create a Web Application scan for assets.

1. In Tenable Attack Surface Management, in the upper-right corner, click the Inventory drop-down list.



Tenable Attack Surface Management displays the inventories in the drop-down list.

2. In the drop-down list, select an inventory.

The assets list appears.

3. Select the assets you want to scan.

Tenable Attack Surface Management enables the **Actions** menu in the upper-right corner.

4. Click **Create Web Application Scan**.

Tenable Attack Surface Management redirects to the **Create a Scan - Web App Scan** page in Tenable Vulnerability Management.