



Tenable Attack Surface Management User Guide

Last Revised: October 24, 2023



Table of Contents

Welcome to Tenable Attack Surface Management	5
Getting Started with Tenable Attack Surface Management	5
Log in to Tenable Attack Surface Management	7
Create Your First Inventory	8
Add Users to Tenable Attack Surface Management	10
Filter Your Assets	11
Create Subscriptions	14
Set Up Notifications	16
Navigate Tenable Attack Surface Management	18
Access the Workspace	20
Attack Surface Management FAQ	24
Attack Surface Glossary	26
Navigating the Administrator Interface	30
Access the Tenable Attack Surface Management Administrator Interface	31
Adding Users to Tenable Attack Surface Management	32
Edit User Account Details	33
Edit Inventory Details	35
Edit Business Details	38
Inventory	40
Create an Inventory	42
Leave an Inventory	43
Manage Inventory Sources	44
Add a Source	45



Add a Subdomain	49
Move a Domain	50
Update a Source Screenshot	51
Remove a Source	52
Exclusion Rules	53
Create an Exclusion Rule	54
Run Exclusion Rules	55
Automation Rules	56
Create an Automation Rule	57
Automation Rule Settings	58
Asset Filters	62
Asset Details	67
Export an Asset	73
Manage Asset Tags	74
Tagging View	78
Tag Assets Quickly	81
Suggested Domains	81
Add Suggested Domains to an Inventory	84
Archive Suggested Domains	85
Suggestion Blocklist	86
Manage Suggested Domains	86
Manage source-based suggestions	88
Manage brand names	89
Manage registrar emails	90



Manage organization names	91
Manage nameservers	92
Manage backref links	93
Subscriptions	93
Set Up Notifications	95
Add Subscriptions	98
Predefined Subscription Categories	99
Create Custom Subscriptions	100
Share a Subscription	101
Copy a Subscription	102
Delete a Subscription	103
Dashboard	104
TXT Records	105
User Profile	107
Generate API Keys	109



Welcome to 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.

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

Tenable One Exposure Management Platform

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

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

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

Tenable Attack Surface Management exists as a standalone product, or can be purchased as part of the Tenable One Exposure Management platform (Enterprise Edition only).

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

Getting Started with Tenable Attack Surface Management



Use the following steps to get started with Tenable Attack Surface Management:

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 Subscriptions](#)
6. [Set Up Notifications](#)



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.

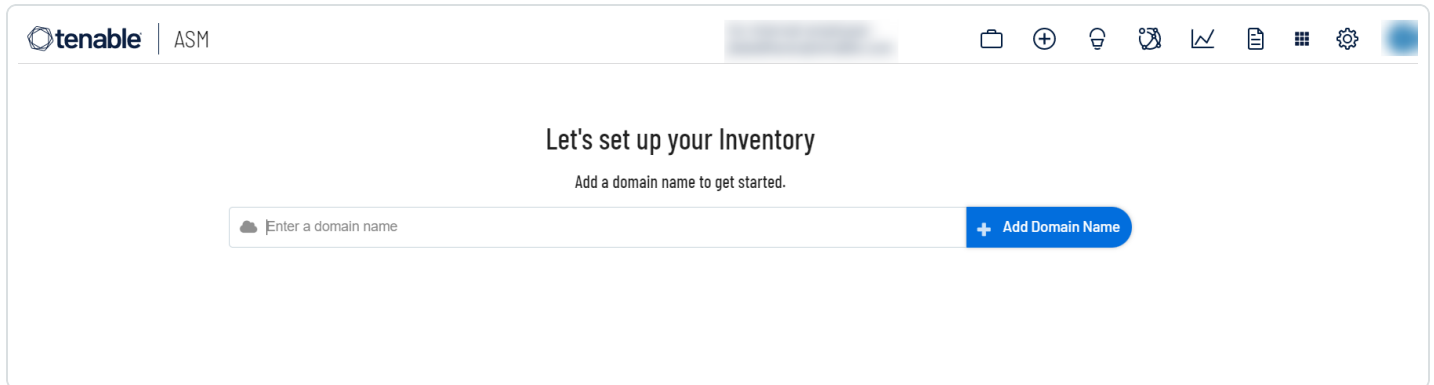
4. Click the Tenable Attack Surface Management tile.

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.



If you entered wikipedia.org as your main domain name, you can see the following inventory:



Your Inventory

Team: Lex

Total Assets
1,058

Domains
1

Subdomains
666

[+ Add filter](#)

1-25 of 1,058



Search

wikipedia.org

Sort by **Asset Count - High to Low** [Select All](#)

<input type="checkbox"/>	Host	Record Type	IP	Ports	Screenshot
<input type="checkbox"/>	bo.wikipedia.org	CNAME	198.35.26.96	80, 443	
<input type="checkbox"/>	to.m.wikipedia.org	CNAME	198.35.26.96	80, 443	
<input type="checkbox"/>	hu.wikipedia.org	CNAME	91.198.174.192	80, 443	
<input type="checkbox"/>	el.wikipedia.org	CNAME	198.35.26.96	80, 443	
<input type="checkbox"/>	ff.wikipedia.org	CNAME	198.35.26.96	80, 443	
<input type="checkbox"/>	pa.m.wikipedia.org	CNAME	198.35.26.96	80, 443	
<input type="checkbox"/>	ltg.wikipedia.org	CNAME	91.198.174.192	80, 443	
<input type="checkbox"/>	pms.m.wikipedia.org	CNAME	198.35.26.96	80, 443	
<input type="checkbox"/>	rue.m.wikipedia.org	CNAME	91.198.174.192	80, 443	
<input type="checkbox"/>	km.m.wikipedia.org	CNAME	198.35.26.96	80, 443	

1.



wikipedia.org
1,058 assets



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](#).

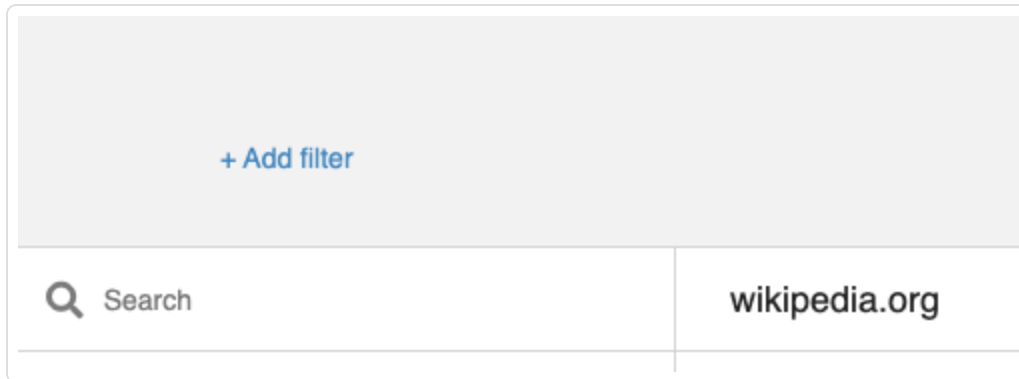


Filter Your Assets

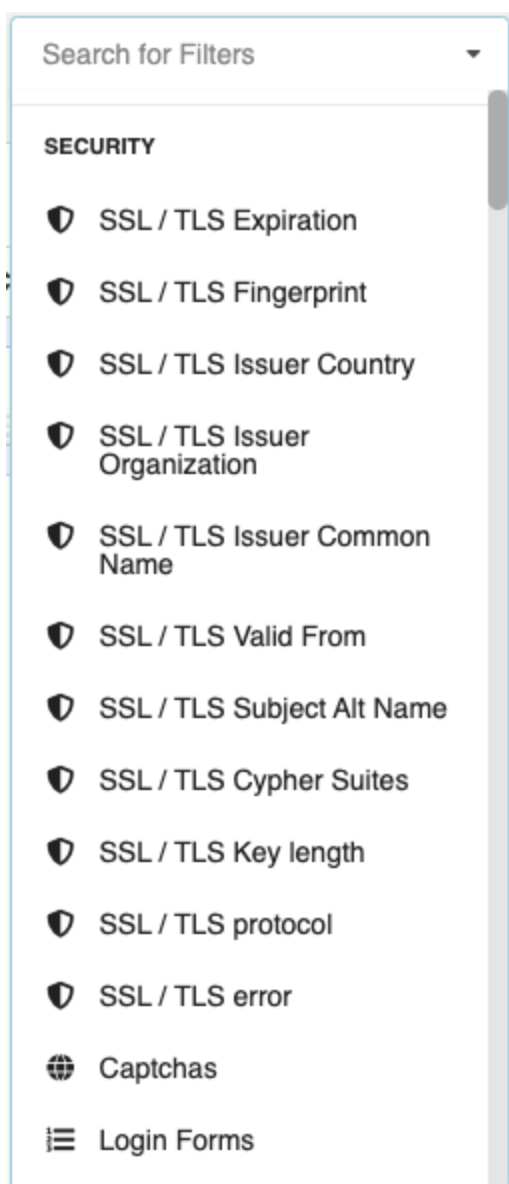
Tenable Attack Surface Management uses filters to provide powerful inventory search capabilities. Filters allow you to view specific subsets of assets in your inventory.

To apply a filter:

1. Above the search box, click **+ Add filter**.



A drop-down menu appears with a list of filters:



2. Select the filter you want to use.

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

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

In this example, Filter = **SSL/TLS Expiration**, Operator = **expires in**, and Value = **30**.

4. Click **Done**.

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.



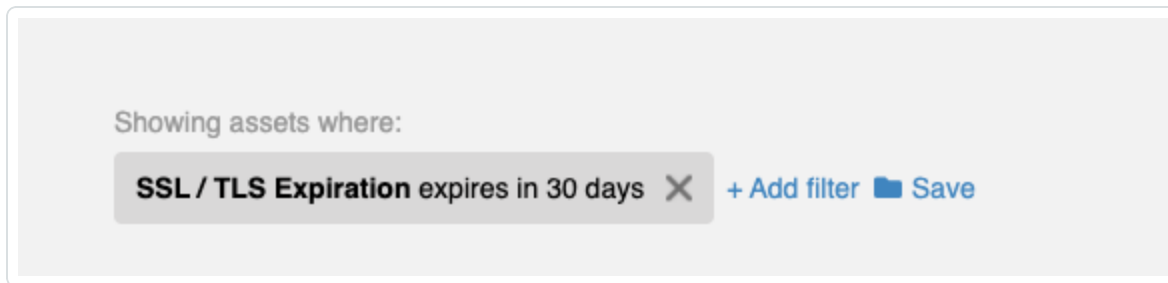
Create Subscriptions

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
	bo.wikipedia.org	CNAME	198.35.26.96	80, 443	Sun Oct 18 2020	
	to.m.wikipedia.org	CNAME	198.35.26.96	80, 443	Sun Oct 18 2020	
	hu.wikipedia.org	CNAME	91.198.174.192	80, 443	Tue Oct 06 2020	
	donate.wikipedia.org	CNAME	91.198.174.192	80, 443	Tue Oct 06 2020	
	ff.wikipedia.org	CNAME	198.35.26.96	80, 443	Sun Oct 18 2020	
▶	pa.m.wikipedia.org	CNAME	198.35.26.96	80, 443	Sun Oct 18 2020	
	ltg.wikipedia.org	CNAME	91.198.174.192	80, 443	Tue Oct 06 2020	
	pms.m.wikipedia.org	CNAME	198.35.26.96	80, 443	Sun Oct 18 2020	
	rue.m.wikipedia.org	CNAME	91.198.174.192	80, 443	Tue Oct 06 2020	
	textbook.wikipedia.org	CNAME	91.198.174.192	80, 443	Tue Oct 06 2020	
▶	ti.m.wikipedia.org	CNAME	198.35.26.96	80, 443	Sun Oct 18 2020	
	fv.m.wikimedia.org	CNAME	91.198.174.192	80, 443	Tue Oct 06 2020	

To see a list of all your subscriptions click the  icon in the top 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.

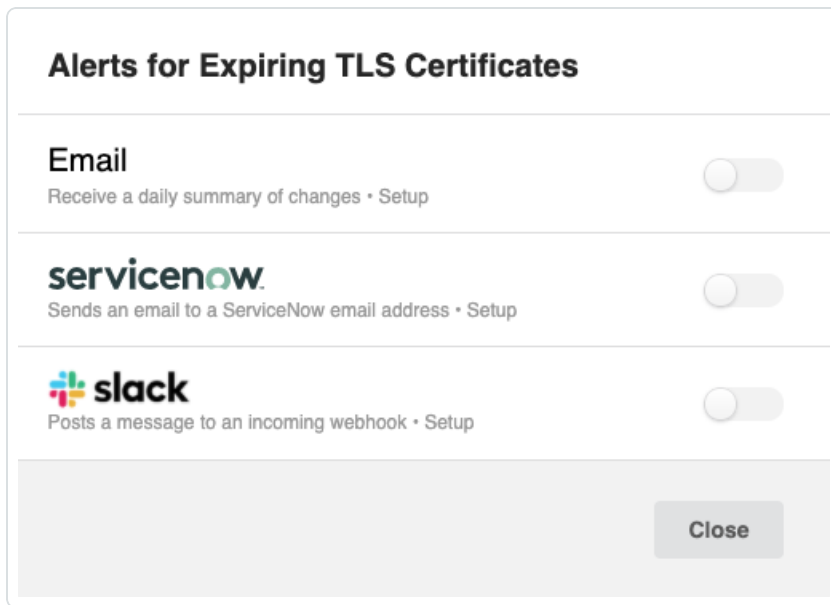
For example, you can receive an email notification when an asset has a TLS certificate that expires soon by using the **Subscription** that you created previously.

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

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:



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.



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.

The screenshot displays the Tenable ASM interface. At the top, there is a navigation bar with the Tenable logo and 'ASM'. Below this, a summary section shows 'Total Assets: 1,406', 'Domains: 3', and 'Subdomains: 558'. A table below the summary lists individual assets with columns for Host, Record Type, IP, ASN, Ports, and Screenshot. The table is sorted by 'Asset Count - High to Low'. Two assets are highlighted in the left sidebar: 'tenable.com' with 863 assets and 'tenabledemo.com' with 14 assets. The table contains 10 rows of data, including records for 'UNK', 'CNAME', and 'SOA' record types, with various IP addresses and ASNs listed.

Host	Record Type	IP	ASN	Ports	Screenshot
[Redacted]	UNK	[Redacted]	AMAZON-AES	80, 443	[Screenshot]
[Redacted]	CNAME	[Redacted]	CLOUDFLARENET	80, 443	[Screenshot]
[Redacted]	SOA	[Redacted]	AMAZON-02	-	-
[Redacted]	CNAME	[Redacted]	AMAZON-02	80, 443	[Screenshot]
[Redacted]	CNAME	[Redacted]	CLOUDFLARENET	80, 443, 2082, 2083, 2086, 2087, 8080, 8443	[Screenshot]
[Redacted]	CNAME	[Redacted]	CLOUDFLARENET	80, 443, 2082, 2083, 2086, 2087, 8080, 8443	[Screenshot]
[Redacted]	CNAME	[Redacted]	-	-	-
[Redacted]	CNAME	[Redacted]	AMAZON-02	80, 443	-
[Redacted]	CNAME	[Redacted]	AMAZON-02	80, 443	[Screenshot]

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.

The screenshot shows the Tenable ASM interface with the following elements:

- Header: **tenable | ASM**
- Inventory name field: [Redacted]
- Team: [Redacted] and 1 other
- + Add Filter button
- Search bar
- Sort by: **Asset Count - High to Low** (dropdown), **Select All** (button)
- Table with columns: Host, Record Type
- Table rows:

	Host	Record Type
1. [Redacted]	tenable.com 863 assets	UNK
2. [Redacted]	tenabledemo.com 14 assets	CNAME
	[Redacted]	SOA
	[Redacted]	CNAME
	[Redacted]	CNAME
	[Redacted]	CNAME
	[Redacted]	CNAME
	[Redacted]	CNAME

Top Navigation

Current Inventory
Indicates the currently viewed inventory.

Add Item
Add hostnames, IPs, IP ranges, ASNs, and new inventories.

Domain Suggestions
Indicates when new domain names that you own are discovered.

Subscriptions
Assets organized into subscriptions.

Admin
Access administrator interface to manage users, inventories, and businesses.

Account
Account settings, API key, multi-factor authentication, and logout.

Manage Assets and Sources
Render assets and sources as dashboard, CSV, XLSX, or JSON (assets only).

Dashboard
View insights about your assets.

TXT Records
View text records in your inventory.

Workspace
Access all Tenable products.

The screenshot shows the Tenable ASM top navigation bar with the following elements:

- Header: **tenable | ASM**
- Inventory name field: [Redacted]
- Team: [Redacted] and 1 other
- Summary statistics:

Total Assets	Domains	Subdomains
1,406	3	558
- Navigation icons: Home, Add, Lightbulb, Refresh, Chart, List, Grid, Settings, Profile




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. You can also switch between your applications from the **Workspace** menu, which appears in the top navigation bar.

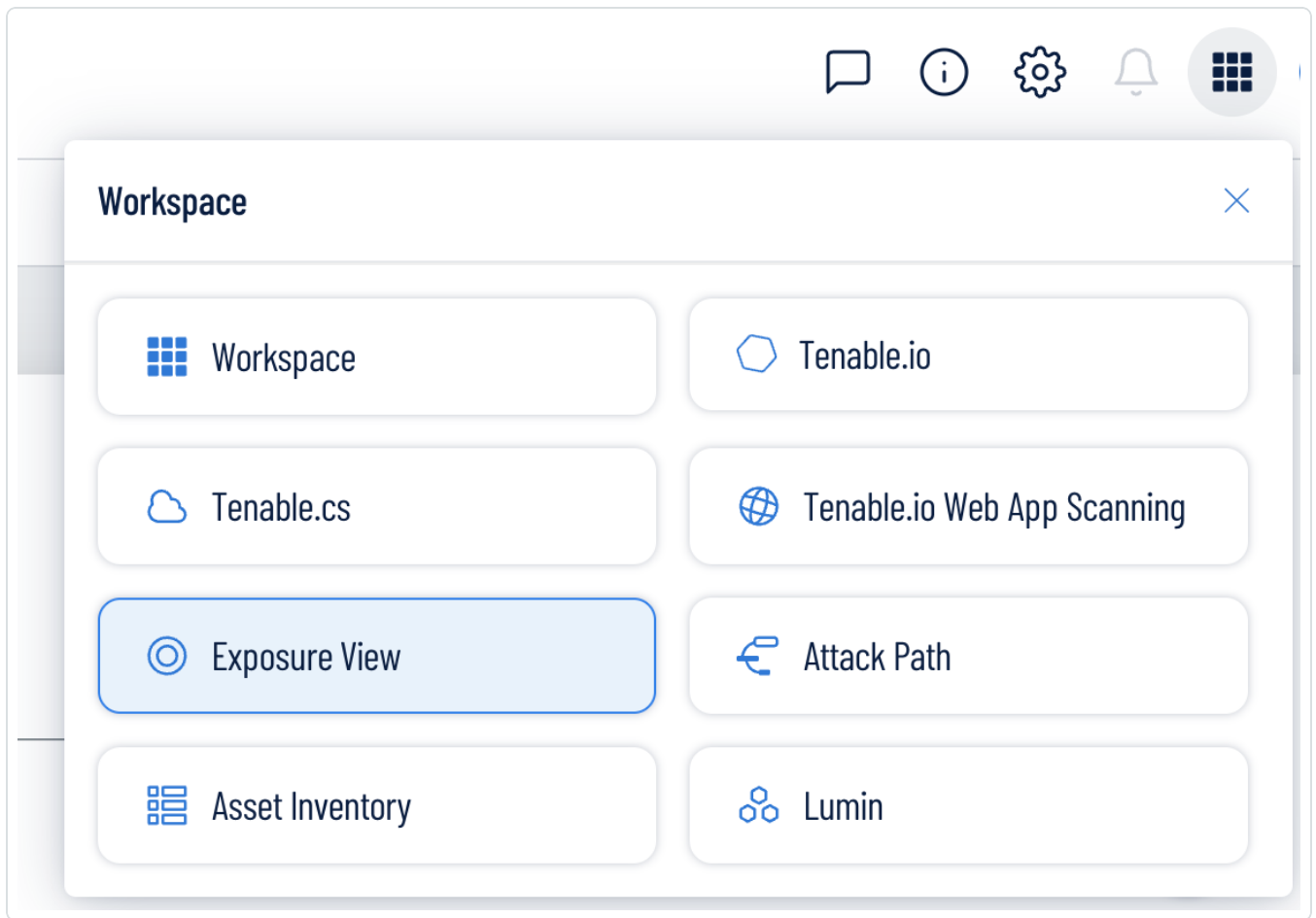
The following feature is not supported in Tenable Vulnerability Management Federal Risk and Authorization Management Program (FedRAMP) environments. For more information, see the [FedRAMP Product Offering](#).

Open the Workspace Menu

To open the **Workspace** menu:

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


The **Workspace** menu appears.



2. Click an application tile to open it.

View the Workspace Page

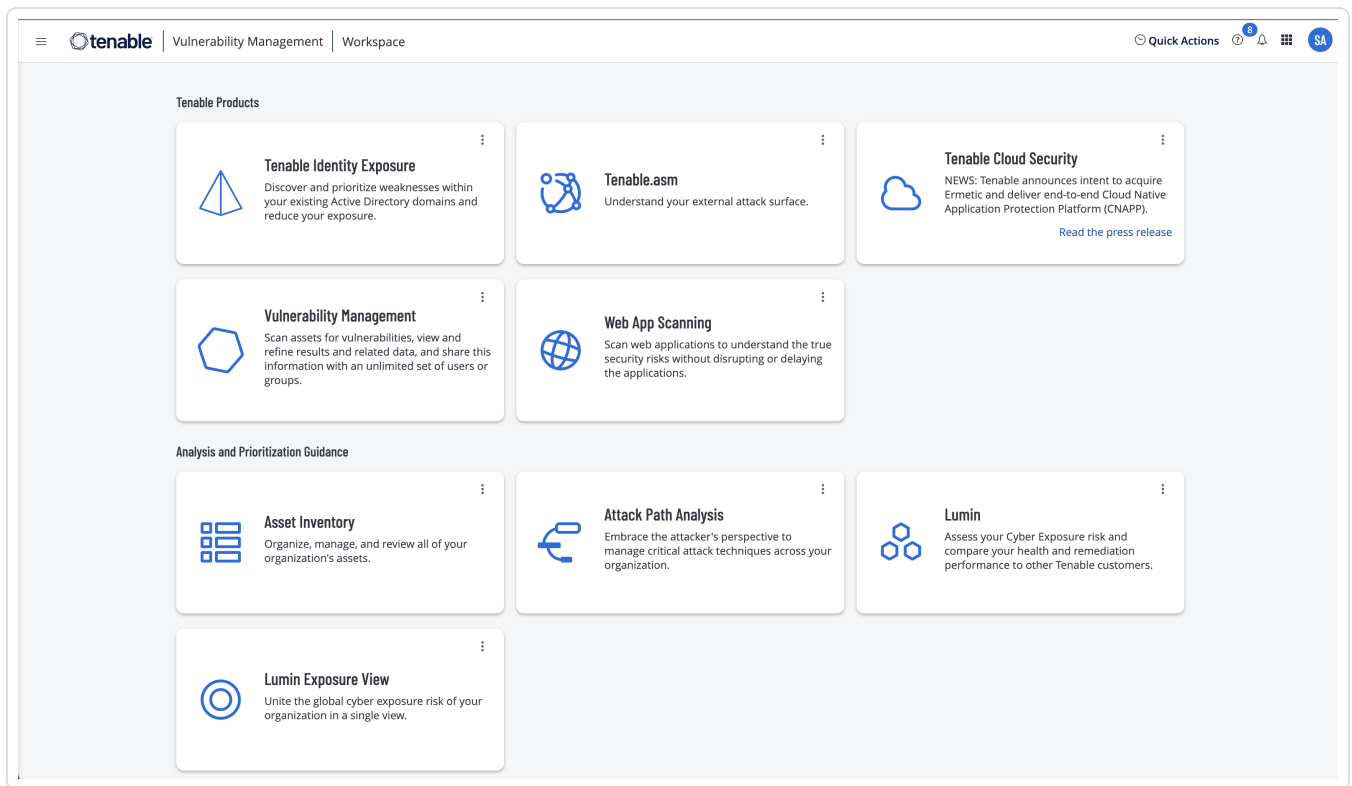
To view the Workspace page:

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

The **Workspace** menu appears.

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

The **Workspace** page appears.



Set a Default Application

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

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

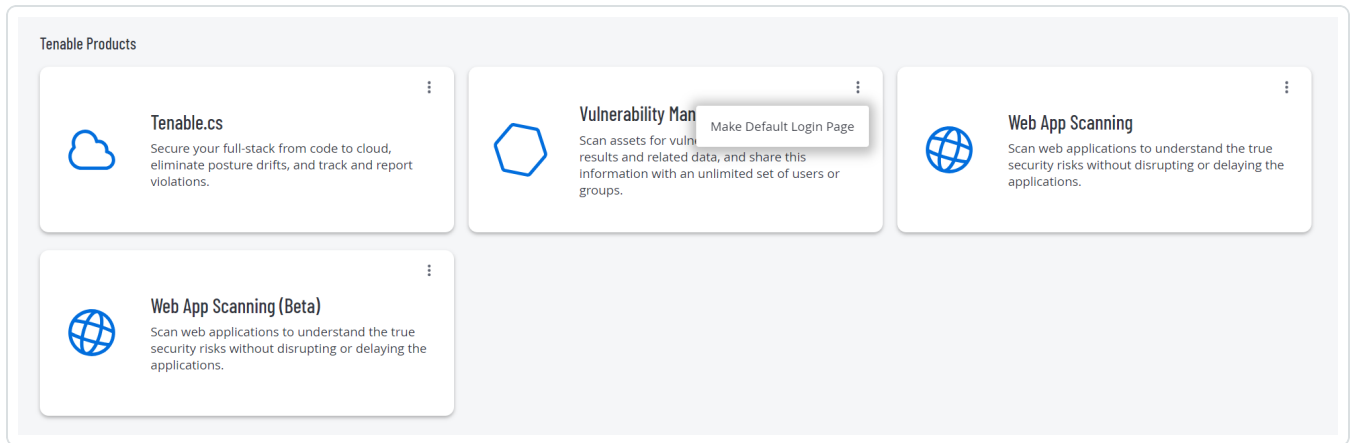
To set a default login application:

1. Log in to Tenable.

The **Workspace** page appears.

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

A menu appears.



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

This application now appears when you log in.

Remove a Default Application

To remove a default login application:

1. Log in to Tenable.

The **Workspace** page appears.

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

A menu appears.

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

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



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.

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.



Attack Surface Glossary

Asset

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:

Asset 1: `www.example.com,A,123.123.123`

Asset 2: `www.foo.com,CNAME,www.bar.com,111.111.111.111`

Asset 3: `www.foo.com,CNAME,www.bar.com,222.222.222.222`

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.

Asset Inventory

A complete collection of an organization's assets and associated metadata of each asset.

Asset Management

Asset management refers to monitoring, configuring, and maintaining of assets.

Attack Surface

From the network perspective of an adversary, the complete asset inventory of an organization including all actively listening services (open ports) on each asset.

Autonomous System Number (ASN)

An ASN is a unique number that's available globally to identify an 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

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.

Example: foo.tld is the domain name of URL <http://www.foo.tld/index.html>.

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

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).

Example: 'bar' is the hostname of bar.foo.tld.

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

A hostname that no longer resolves to an IP-address.

Internet-accessible, internet-connected, internet-facing.

Refers to an asset that can be connected to over the Internet. While the terms above are often used interchangeably, Internet-accessible 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

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.



Navigating the Administrator Interface

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

tenable | ASM

USERS INVENTORIES BUSINESSES

Find User

Email

Inventory

Additional filters

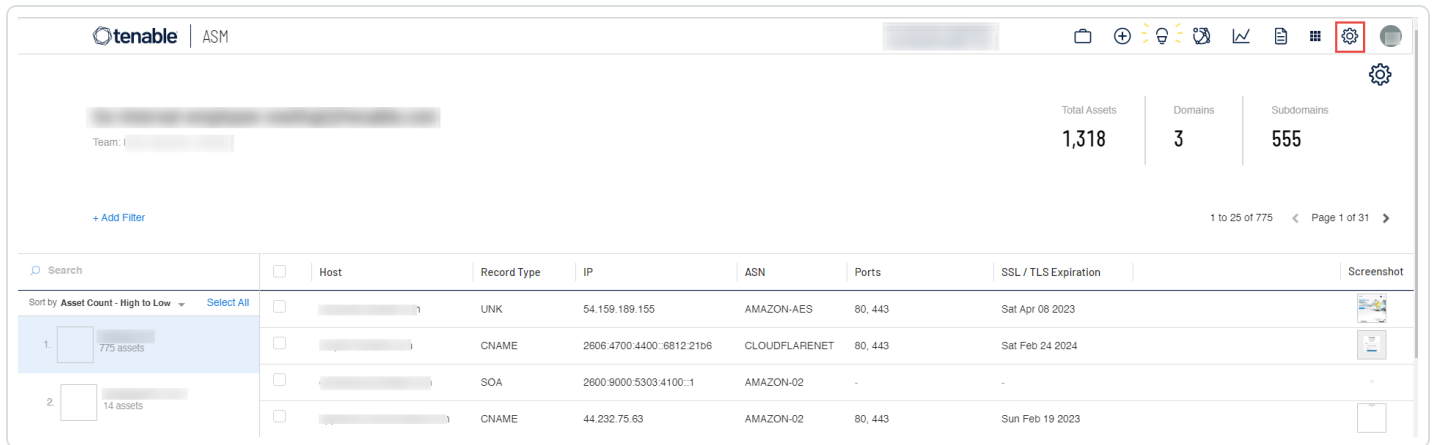
Search Reset

Found 2 items. Filtered by **Role**, Showinvites.

ID	Name	Email	Role	Status	Disabled after	Inventory	Created	
2696			User	Active	-	test-	4 days ago	Edit
2638			Business Admin		-	test-	8 days ago	Edit



Access the Tenable Attack Surface Management Administrator Interface



To access the administrator interface:

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

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**.



Adding 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.



Edit User Account Details

Required User Role: Business Admin

You can have multiple users in a business account and assign all or specific inventories to each user. Tenable Attack Surface Management has two user roles – **Active User** and **Business Admin**. Once the user that you [create](#) in Tenable Vulnerability Management logs in to Tenable Attack Surface Management for the first time, that user appears in the list of users in Tenable Attack Surface Management . By default, the new user's role is **Active User**.

To change the role of a user in Tenable Attack Surface Management:

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

By default, Tenable Attack Surface Management shows the **Users** window with the **Find User** section and the table listing all users.

2. (Optional) Search for a specific user by providing relevant details in the **Find User** section:

Parameters	Description
Email	The email ID of the user.
Inventory	The inventory assigned to the user. The drop-down lists all the inventories in Tenable Attack Surface Management.
Additional filters	In the Additional filters section, provide the following: <ul style="list-style-type: none">• First name• Last name• Role / Status

3. Click **Search**.

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

4. In the row of the user you want to edit, click **Edit**.

The **Edit user** window appears.



Note: You can edit the email ID, first name, and last name in Tenable Vulnerability Management.

5. In the **Role / Status** drop-down box, select the required user role from the options available:
 - **Active User** – Allows users to manage inventories.
 - **Not approved** – Restricts users from accessing Tenable Attack Surface Management until approval.
 - **Disabled** – Restricts access to Tenable Attack Surface Management.
 - **Business Admin** – Allows users to edit user accounts, assign roles, and add inventories to businesses.
 - **View-only User** – Allows users to only view inventories and not modify them. The **View-only** users do not have permissions to create new inventories.
6. In the **Inventories** box, select the inventories you want to assign to the user account.
7. Click **Update**.

Note: If you want to grant access to all inventories for the user account, click **Grant access to all inventories in Business**.

Tenable Attack Surface Management updates the user account and displays the following user details in a table format.

Column	Description
ID	The ID assigned to the user.
Name	The name of the user.
Email	The email ID of the user.
Role	The role assigned to the user.
Status	The status of the account, whether active or disabled.
Inventory	The inventories assigned to the user account.
Created	The date on which the account was created.



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. In the upper right corner, click the  icon.

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

2. Click **Inventories**.

The **Inventories** page appears.

3. 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 default asset limit is 1000.

- 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.

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

The **Edit inventory** window appears.

5. 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.

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

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	The number of assets in the inventory.
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. In the upper right corner, click the  icon.

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

2. Click **Business**.

The **Business** page appears.

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

The **Edit business** window appears.

4. To change the default asset limit: in the **Default Asset limit for Inventories** box, modify the value.

5. 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.



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

Your inventory appears.

Related topics:

[Create an Inventory](#)

[Leave an Inventory](#)

[Manage Inventory Sources](#)

[Add a Source](#)

[Add a Subdomain](#)

[Move a Domain](#)

[Update a Source Screenshot](#)

[Remove a Source](#)

[Exclusion Rules](#)

[Create an Exclusion Rule](#)

[Run Exclusion Rules](#)

[Automation Rules](#)

[Create an Automation Rule](#)

[Automation Rule Settings](#)

[Asset Filters](#)

[Asset Details](#)

[Export an Asset](#)



[Manage Asset Tags](#)

[Tagging View](#)


[Tag Assets Quickly](#)



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  button.
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 will inherit the selected inventory's tags, custom columns, subscriptions, and exclusion rules.

5. Click the **Save** button.

The inventory is created.

6. In Tenable Attack Surface Management, in the upper-right corner, click the  button.
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](#).



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  button.
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.



Manage Inventory Sources



Add a Source

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

1. In Tenable Attack Surface Management, in the upper-right corner, click the **+** button.
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>	Tells Tenable Attack Surface Management to extract data using the IP address that an asset resolves to.

5. Click the **Next** button.

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

Add an IP address or IP range



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

Add an Autonomous System Number (ASN)

1. In Tenable Attack Surface Management, in the upper-right corner, click the **+** button.
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 identifying 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 Tenable Attack Surface Management, in the upper-right corner, click the **+** button.
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) 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 you want 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 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. In Tenable Attack Surface Management, in the upper-right corner, click the  button.
2. In the drop-down list, select an inventory.
3. In the list of domains, hover over the domain to which you want to add a subdomain.
4. Click the  button.
5. In the drop-down list, click **Add subdomain**.

The **Add missing subdomain** window appears.

6. In the text box, type a subdomain or comma-separated list of subdomains.
7. Click the **Add subdomains** button.



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. In Tenable Attack Surface Management, in the upper-right corner, click the  button.
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. In the drop-down list, click **Move to another inventory**.

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

6. In the drop-down box, select the inventory to which you want to move the domain.
7. 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 updated 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  button.
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. In Tenable Attack Surface Management, in the upper-right corner, click the  button.
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. In the drop-down list, click **Delete from Inventory**.

The source is deleted from the inventory.



Exclusion Rules

In Tenable Attack Surface Management, exclusion rules specify specific assets to include or exclude from your 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, in the upper-right corner, click the **+** button.
2. In the drop-down list, click **Add or Modify 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 the **Save** button.

The exclusion rule is created.



Run Exclusion Rules

To run your exclusion rules:

1. In Tenable Attack Surface Management, in the upper-right corner, click the ⊕ button.
2. In the drop-down list, click **Add or Modify Exclusion Rules**.

The **Exclusion Rules** window appears.

3. Click the **Run rules now** button.

The exclusion rules run and your Tenable Attack Surface Management inventories update to reflect the rules.



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, in the upper-right corner, click the **+** button.
2. In the drop-down list, click **Add or Modify 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 the **Save** button.

The automation rule is created.



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	Select when you want the automation rule to archive an asset in your inventory. <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	Select whether you want the automation rule to add or remove a tag from assets in your inventory. <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.



Setting	Description
Select Tag	Select the tag that you want the automation rule to add or remove.
if Asset matches	Select when you want the automation rule to add or remove a tag from an asset in your inventory. <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. <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.



Setting	Description
	<ul style="list-style-type: none">• 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.



Setting	Description
	<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.



Asset Filters

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.

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 expires within 3 days.
 - a. Click **Add Filter**.

A drop-down menu appears.

The screenshot shows the Tenable ASM interface. At the top, the Tenable logo and 'ASM' are visible. Below the header, there is a blurred banner and a 'Team:' label. A search bar is on the left with a magnifying glass icon and the word 'Search'. Below the search bar, there is a 'Sort by Asset C' dropdown menu. A filter dropdown menu is open, displaying a search bar 'Search for Filters' and a list of security filters under the heading 'SECURITY'. The filters are: SSL / TLS Expiration, SSL / TLS Fingerprint, SSL / TLS EV Certificate, SSL / TLS Issuer Country, SSL / TLS Issuer Organization, SSL / TLS Issuer Common Name, SSL / TLS Valid From, SSL / TLS Subject Alt Name, SSL / TLS Cypher Suites, and SSL / TLS Key length. To the right of the filter menu, a table is partially visible with columns 'Host' and 'Record Type'. The table contains several rows of data, some of which are blurred.

Host	Record Type
▶ [blurred]	NS
[blurred]	A
▶ [blurred]	SOA
[blurred] ..	AAAA
[blurred] ..	CNAME
[blurred] ...	A

- b. Select the **SSL/TLS Expiration** filter.

The screenshot shows the Tenable ASM interface. At the top, the Tenable logo and 'ASM' are visible. Below the header, there is a search bar and a 'Team: j' label. A filter dropdown menu is open, showing the following options:

- is expired
- is not expired
- expires in
-
- expired less than
- expired more than
- expires on
- expires after
- expires before
- is unknown
- has any value

At the bottom of the dropdown menu is a 'Done' button. To the right of the dropdown menu, there is a '+ Add Filter' button. Below the dropdown menu, a table is visible with the following columns: 'Host' and 'Record Type'. The table contains several rows of data, including entries for 'NS', 'A', 'SOA', 'AAAA', and 'CNAME' record types.

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 expiring 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:ed1::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** ✕ **Registrar email contains hostmaster** ✕ **Ports is 3306** ✕



Asset Details

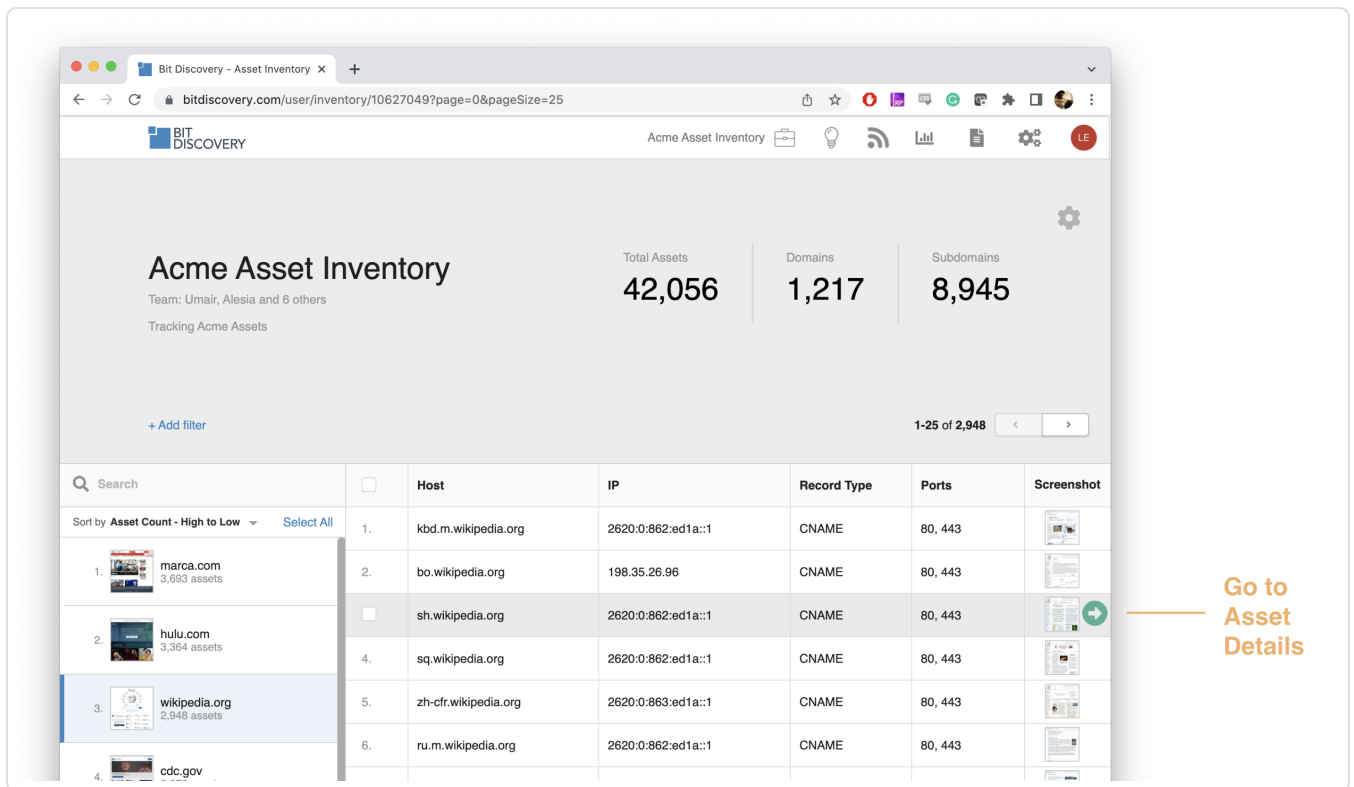
When you click on an asset in Tenable Attack Surface Management, a page appears that includes all known information about the asset.

To view details for an asset in your inventory:

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

In the drop-down list, select an inventory.

2. In the list, hover over the asset for which you want to view more details.



Go to Asset Details

3. Click the green  button.

The details page for the asset appears.

4. (Optional) To refresh details for the asset, at the bottom of the asset details page, click the **Update** button.
5. (Optional) [Export the asset](#).



dyna.wikimedia.org

2620:0:862:ed1a::1

Tag

[+ Add tags](#)

Networking

Domain	wikipedia.org
Record Value	dyna.wikimedia.org
Host	sh.wikipedia.org
Record Type	CNAME
IP	2620:0:862:ed1a::1
ASN	WIKIMEDIA
Final url	https://sh.wikipedia.org/wiki/Glavna_stranica
Cloud Hosted	no
Is subdomain	yes

Services

Port	Service	Last seen	Banner
80	http-proxy	4 days ago	"<!DOCTYPE html>\n<html lang="en">\n<meta charset="utf-8">\n<title>Wikimedia Error</title>\n<style>\n* { margin: 0; padding: 0; }\nbody { background: #fff; font: 15px/1.6 sans-serif; color: #333; }\n.content { margin: 7% auto 0; padding: 2em 4em 4em; width: 80%; }\nfooter { clear: both; margin-top: 40px; border-top: 1px solid #ccc; width: 100%; }\n

Networking Details



Networking

Domain	wikipedia.org
Record Value	dyna.wikimedia.org
Host	sh.wikipedia.org
Record Type	CNAME
IP	2620:0:862:ed1a::1
ASN	WIKIMEDIA
Final url	https://sh.wikipedia.org/wiki/Glavna_stranica
Cloud Hosted	no
Is subdomain	yes

Services Details

Services

Port	Service	Last seen	Banner
80	http-proxy	4 days ago	"<!DOCTYPE html>\n<html lang="en">\n<meta charset="utf-8">\n<title>Wikimedia Error</title>\n<style>\n* { margin: 0; padding: 0; }\nbody { background: #fff; font: 15px/1.6 sans-serif; color: #333; }\n.content { margin: 7% auto 0; padding: 2em 1em 1em; max-width: 640px; }\n.footer { clear: both; margin-top: 14%; border-top: 1px solid #e5e5e5; background: #f9f9f9; padding: 2em 0; font-size: 0.8em; text-align: center; }\nimg { float: left; margin: 0 2em 2em 0; }\na img { border: 0; }\nh1 { margin-top: 1em; font-size: 1.2em; }\n.content-text { overflow: hidden; overflow-wrap: break-word; word-wrap: break-word; -webkit-hyphens: auto; -moz-hyphens: auto; -ms-hyphens: auto; hyphens: auto; }\np { margin: 0.7em 0 1em 0; }\na { color: #0645ad; text-decoration: none; }\na:hover { text-decoration: underline; }\ncode { font-family: sans-serif; }\n.text-muted { color: #777; }\n</style>\n<div class="content" role="main">\n <html lang="en"> <meta charset="utf-8"> <title>Wikimedia Error</title> <style> margin: 0; padding: 0; } body { background: #fff; font: 15px/1.6 sans-serif; color: #333; } .content { margin: 7% auto 0; padding: 2em 1em 1em; max-width: 640px; } .footer { clear: both; margin-top: 14%; border-top: 1px solid #e5e5e5; back



SSL/TLS Details

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	D60682CE7DBA8A1ABD8E83D238D54423D9D554ED
SSL / TLS Subject Alt Name	*.wikipedia.org wikimedia.org mediawiki.org wikibooks.org wikidata.org wikinews.org wikiquote.org wikisource.org wikiversity.org wikivoyage.org wiktionary.org wikimediafoundation.org w.wiki wmfusercontent.org *.m.wikipedia.org *.wikimedia.org *.m.wikimedia.org *.planet.wikimedia.org *.mediawiki.org *.m.mediawiki.org *.wikibooks.org *.m.wikibooks.org *.wikidata.org *.m.wikidata.org *.wikinews.org *.m.wikinews.org *.wikiquote.org *.m.wikiquote.org *.wikisource.org *.m.wikisource.org *.wikiversity.org *.m.wikiversity.org *.wikivoyage.org *.m.wikivoyage.org *.wiktionary.org *.m.wiktionary.org *.wikimediafoundation.org *.wmfusercontent.org wikipedia.org
SSL / TLS Cypher Suites	ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-CHACHA20-POLY1305 ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-CHACHA20-POLY1305 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384
JARM Hash	28d28d28d2ad28d00042d42d0000002754d7386e47d3f44bdc269e2eaff0ff
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	mw1430.eqiad.wmnet
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	mw1430.eqiad.wmnet
x-content-type-options	nosniff
p3p	CP="See https://sh.wikipedia.org/wiki/Special:CentralAutoLogin/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://sh.wikipedia.org/wiki/Glavna_stranica
content-length	0
content-type	text/html; charset=UTF-8
age	1419
x-cache	cp3062 hit, cp3064 hit/2
x-cache-status	hit-front
server-timing	cache;desc="hit-front", host;desc="cp3064"
strict-transport-security	max-age=106384710: includeSubDomains: preload



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. At the bottom of the page, click the **Export to CSV** or **Export to XLSX** button.

The CSV or XLSX file immediately begins downloading.




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.

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 check box 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.



1. Assign tags to a single asset or multiple assets:

Scope	Action
Assign tags to a single asset	<ol style="list-style-type: none"><li data-bbox="480 317 1455 527">1. In the assets table, select the check box 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.<li data-bbox="480 558 987 667">2. Click Actions > Add Tags. The list of available tags appears.<li data-bbox="480 699 1279 741">3. Select the check box next to the tags that you require.<li data-bbox="480 772 1430 982">4. Click Add. 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.<li data-bbox="480 1014 1430 1171">5. Provide the values for the tags, if applicable and click Save. Tenable Attack Surface Management applies the selected tags to the asset. <div data-bbox="526 1203 1479 1360" style="border: 1px solid green; padding: 5px;"><p>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.</p></div>
Assign tags to multiple assets	<ol style="list-style-type: none"><li data-bbox="480 1394 1446 1604">1. In the assets table, select the check boxes next to the assets to which you want to assign a tag. Tenable Attack Surface Management enables the action bar at the top of the table.<li data-bbox="480 1635 1471 1719">2. (Optional) To select all assets, select the check box at the top of the table. 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.

3. Click **Actions > Add Tags**.

The list of available tags appears.

4. Select the check box next to the tags that you require.

5. Click **Add**.

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.

6. Provide the values for the tags, if applicable and click **Save**.

Tenable Attack Surface Management assigns the selected tags to the selected 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 check box 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 check box next to the tags you want to remove.

4. Click **Remove**.

Tenable Attack Surface Management removes the tag.



Tagging View

The **Tagging View** page is similar to the asset details page and shows all available data for an asset.

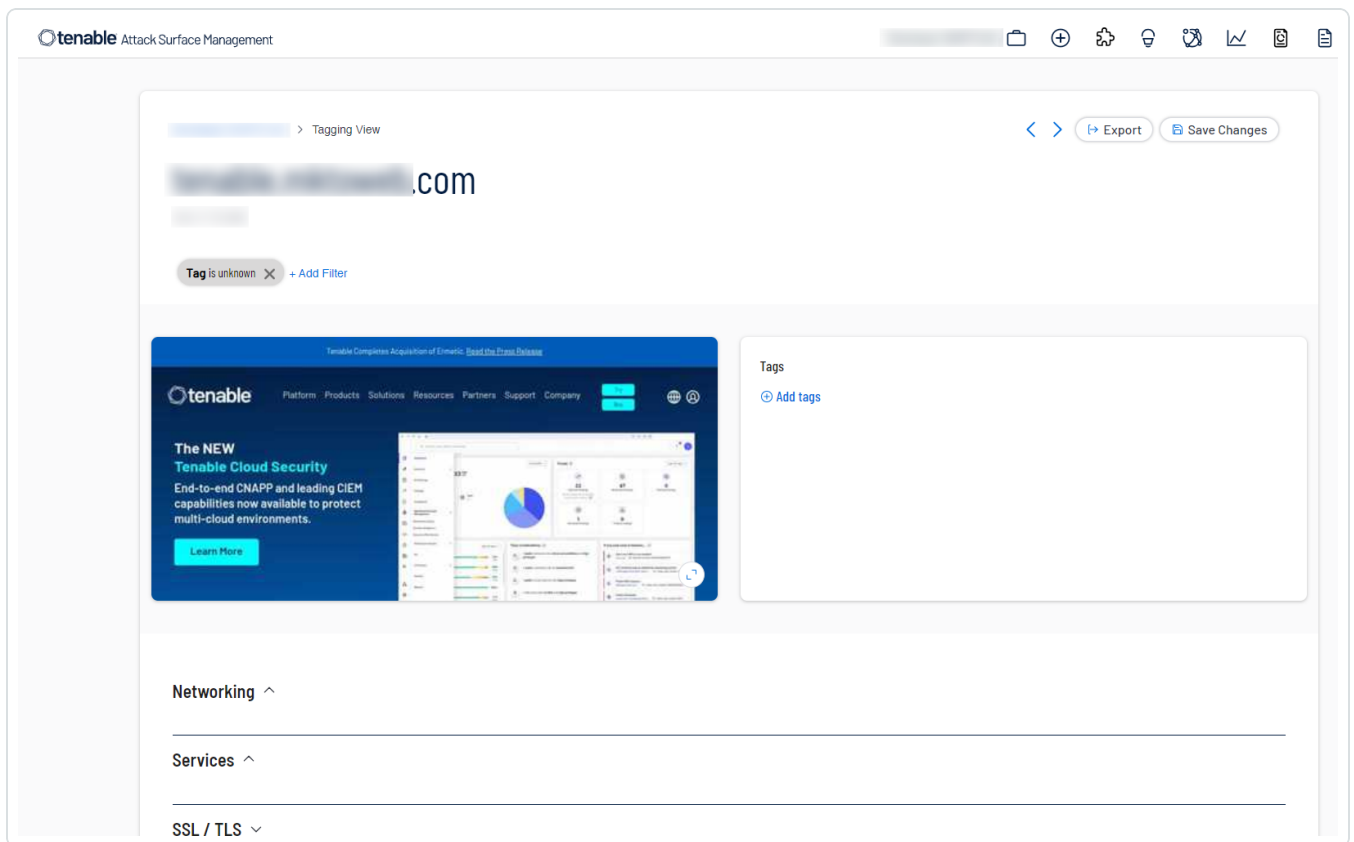
Access the Tagging View Page

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

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.

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 upper right corner, click the  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

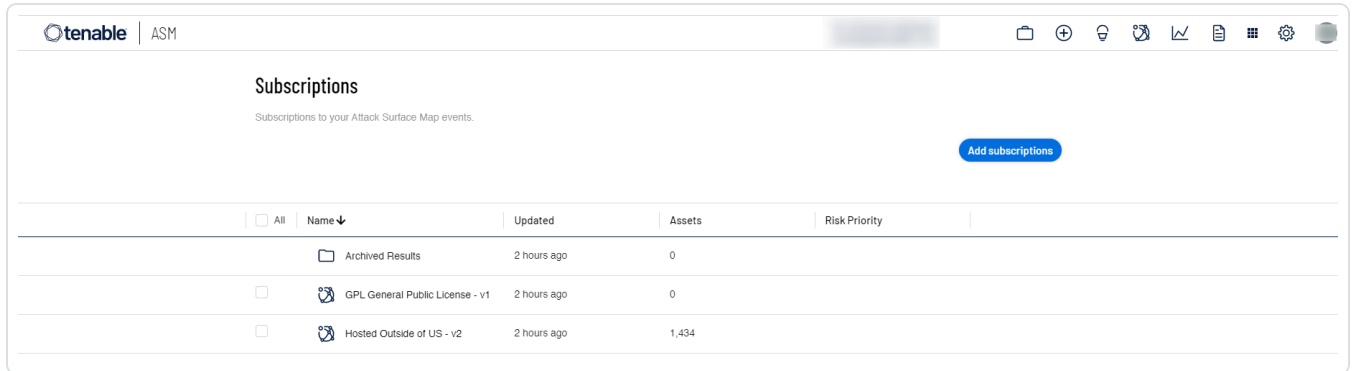
Tenable Attack Surface Management subscriptions notify you about important changes to your attack surface, including new servers, newly opened or closed ports, and new software. You can configure your subscriptions to include the changes that you think are most important.



To access **Subscriptions**:

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

The **Subscriptions** page appears.



The screenshot shows the Tenable ASM interface. At the top left, the Tenable logo and 'ASM' are visible. The main heading is 'Subscriptions' with a subtitle 'Subscriptions to your Attack Surface Map events.' A blue button labeled 'Add subscriptions' is positioned on the right. Below this is a table with columns for selection, Name, Updated, Assets, and Risk Priority. The table contains three rows of subscription data.

<input type="checkbox"/>	Name	Updated	Assets	Risk Priority
<input type="checkbox"/>	Archived Results	2 hours ago	0	
<input type="checkbox"/>	GPL General Public License - v1	2 hours ago	0	
<input type="checkbox"/>	Hosted Outside of US - v2	2 hours ago	1,434	



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



Posts a message to an incoming webhook • Setup



Close

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

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

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



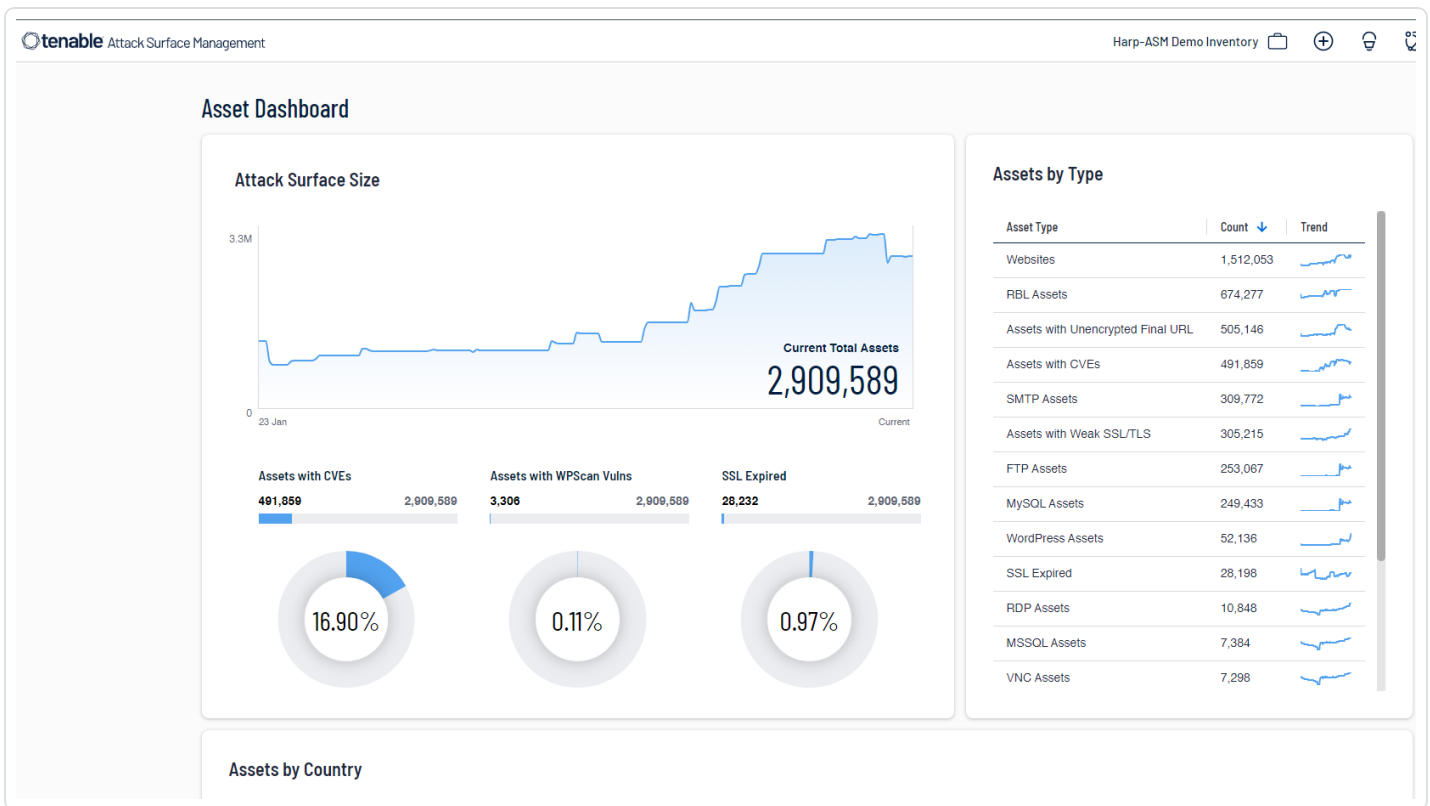
Dashboard

The Tenable Attack Surface Management dashboard provides insights into the assets in your organization.

To view your dashboard:

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

The **Asset Dashboard** page appears.



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

TXT Records

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

The screenshot shows the Tenable ASM interface for viewing TXT records. At the top, there is a navigation bar with the Tenable logo, 'ASM', and several utility icons. Below the navigation bar, the page title 'TXT records' is displayed, along with a '+ Add Filter' button and pagination information '1 to 2 of 2' and 'Page 1 of 1'. A search bar is located on the left side of the table. The table has two columns: 'Host' and 'Value'. The table is sorted by 'Record Count - High to Low'. Two records are visible: 1. [Host] 130 records, 2. [Host] 12 records.

To view your text records:

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

- a. 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](#).