Asset Inventory User Guide

Last Revised: April 12, 2024

Table of Contents

Welcome to Asset Inventory

The Tenable One Exposure Management Platform helps organizations gain visibility across the modern attack surface, focus efforts to prevent likely attacks, and accurately communicate cyber risk to optimize business performance.

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

The Tenable One platform enables you to:

- Get comprehensive visibility of all assets and vulnerabilities, whether on-premises or in the cloud, and understand where they are exposed to risk.
- Anticipate threats and prioritize efforts to prevent attacks by using generative AI and the industry's largest data set of vulnerability and exposure context.
- Communicate exposure risk to business leaders and stakeholders with clear KPIs, benchmarks, and actionable insights.
- Leverage the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps, and identity systems.
- Integrate with third-party data sources and tools for enhanced exposure analysis and remediation.

Tip: For additional information on getting started with Tenable One products, check out the Tenable One Deployment Guide and review the following customer education materials:

- Tenable One Introduction (Tenable University)

Tenable One is a package that includes the following products:

Product	Tenable One Package
Tenable Vulnerability Management	Tenable One Standard, Tenable One Enterprise
Tenable Cloud Security	Tenable One Standard, Tenable One Enterprise

Tenable Web App Scanning	Tenable One Standard, Tenable One Enterprise
Lumin Exposure View	Tenable One Standard, Tenable One Enterprise
Tenable Identity Exposure	Tenable One Standard, Tenable One Enterprise
Asset Inventory	Tenable One Standard, Tenable One Enterprise
Attack Path Analysis	Tenable One Enterprise
Tenable Attack Surface Management	Tenable One Enterprise

Use Cases

This user guide covers the following interfaces, which can be used alone or in tandem to support these common use cases:

User Type	Use Case
CISO/Executives	Utilize the **Lumin Exposure View** to: • Quickly quantify your overall enterprise risk exposure and identify which areas need further investigation. • Create custom exposure cards to view data based on specific business contexts. • Measure and prioritize risk exposure progress or regression. • Easily communicate important risk information to teams and include in presentations. • Understand how effective your program is via the **Remediation Maturity** metric.
Security Practitioner	Utilize the **Attack Path Analysis** section to: • Evaluate the impact of insecure assets and communicate these insecurities to appropriate parties. • Proactively identify hidden security issues within my

	assets and their relationships.
Both CISO/Executives and Security Practitioners	Utilize the **Asset Inventory** to: • Utilize existing tags or create new tags that can be used to create custom exposure cards. • View and manage all assets, regardless of their source.

For more information, see Get Started with Asset Inventory.

Get Started with Asset Inventory

Tenable recommends following these steps to get started with Asset Inventory data and functionality.

Tip: For additional information on getting started with Tenable One products, check out the Tenable One Deployment Guide and review the following customer education materials:

- Tenable One Introduction (Tenable University)

Prepare

- Familiarize yourself with the Asset Inventory key terms.
- Review the Tenable One Licensing *Quick-Reference Guide*.
- Familiarize yourself with the categories and data metrics within Asset Inventory.
- Review the Tenable One Example Workflow.

License, Access, and Log In

To use Tenable One, you purchase licenses for assets: resources identified by—or managed in—your Tenable products. Each Tenable One product has a different asset type. For more information, see the Tenable One Licensing *Quick-Reference Guide*.

To acquire a license:

1. Determine the interface that best suits your business objectives. For more information, see Use Cases.
2. Contact your Tenable representative to purchase the appropriate package.

To access and log in to Asset Inventory:

Follow the Log in to Asset Inventory steps.

Configure Asset Inventory for Use

- Configure your Asset Inventory settings.
- View your data sources.

Assess Your Exposure

Review your CES and perform analysis:

- Access **Asset Inventory**, where you can:
    - View all of your assets and asset details within Asset Inventory.
    - View all of your tags and tag details within Asset Inventory.
    - Create and manage tags.

Key Terms

The following key terms apply to the Asset Inventory user interface.

Term	Definition
Active Directory (AD)	Attack Path Analysis integrates AD data from Tenable Identity Exposure.
Asset	Any IT or security element in your organization such as user accounts, computers, and software. The **Discover** section represents an asset as a node in the graph.
Asset Exposure Graph	A visualization of an attack path from multiple assets down to one asset.
Asset Exposure Score (AES)	Tenable calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure
Asset Vulnerability Rating (AVR)	An aggregation of all Vulnerability Priority Rating (VPR) scores for vulnerabilities detected on an asset.
Benchmark	A group of scores to which you can compare your scores and assess your performance.
Blast Radius	A visualization of one or more attack paths from one asset to multiple other assets.
CES Trend	A measurement that defines how your CES improves or regresses over time.
Chief Information Security Officer (CISO)	The head of cybersecurity for a company. A CISO can use the Exposure View to quickly quantify the overall enterprise risk exposure, measure its progress or regression over time and easily communicate impact and ROI to key stakeholders.
Choke Point Priority	A choke point is a place where potential attack paths merge together before reaching a critical asset. Attack Path Analysis uses Choke Point

	Priority as a prioritization metric for attack techniques based on the number of attack paths exploiting the attack, the number of critical assets it leads to, and complexity of the attack. Attack Path Analysis categorizes priority levels as **Low**, **Medium**, **High**, and **Critical**.
Cyber Exposure Score (CES)	Your CES quantifies the relative risk of your organization based on the threat exposure and criticality of your licensed assets. CES values range from 0 - 1000, where higher values indicate higher exposure and higher risk.
Data Source	A product that feeds data into Tenable One (for example, Tenable Vulnerability Management).
Evidence	The empirical data from different data sources confirming the feasibility of a Step as part of an attack path.
Exposure Card	An Exposure card represents the incoming data from your configured tags and data sources. It aggregates and normalizes the data to provide a visualization of your Cyber Exposure Score (CES) and other metrics. Users can create custom cards, or use Tenable-provided cards to gain insight and guidance on what areas need their attention most.
Exposure Card View	The section of the Exposure View that includes data about the selected exposure card. This section includes CES, trend, Remediation SLA, and business context information.
Exposure View	A holistic and unified view combining internal and external data sources to provide a complete view of risk in a singular location.
Finding	A feasible implementation of a technique or sub-technique in one or more attack paths that an adversary can leverage. Each finding has a Choke Point Priority that determines its urgency and potential impact.
Industry Benchmark	A benchmark based on members of your Tenable-assigned industry to which you can compare your scores and assess your performance.
MITRE ATT&CK®	MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The MITRE

	ATT&CK® knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
Node Exposure Score (NES)	A metric produce by Tenable One to understand the blast radius exposure of a node. This metric considers the Vulnerability Priority Rating of all vulnerabilities on the asset as well as other relationships such as software installed, sub-networks to which the asset belongs, internet exposure, etc.
Path Priority Rating	A prioritization metric for attack paths based on the exposure of the source, criticality of the target and the number of steps of the attack path.
Population Benchmark	A benchmark based on members of the entire population to which you can compare your scores and assess your performance.
Query Builder	A customizable visualization of one or more attack paths based on configurable source and target assets.
Query Library	Predefined queries that visualize scenarios of potential attack paths based on real-world attacks.
Operational Technology (OT)	Tenable One integrates OT data from OT Security.
Security Practitioner	A Security Practitioner can use the Asset Inventory to evaluate the impact of unsecured assets, proactively identify hidden security issues in assets relationships, and quickly locate areas where a breach or risk is likely to happen.
Service Level Agreement (SLA)	A control by which you can identify whether assets comply with customer security requirements.
Step	A feasible implementation of a technique or sub-technique in an attack path that an adversary can leverage. The **Discover** section illustrates a step as a "bracket" between two or more assets.
Technique / Sub-Technique	Represents "how" an adversary achieves a tactical goal by performing an action. For example, an adversary can dump credentials to achieve

	credential access.
Tags	A way to group assets by business context. For example, you can group assets by product, permissions, business owner, etc.
Vulnerability Management (VM)	Tenable One integrates VM data from Tenable Vulnerability Management and Tenable Security Center.
Web Application Scanning (WAS)	Tenable One integrates web app scanning data from Tenable Web App Scanning.

Example Workflow

The following scenario describes a common use case where the Lumin Exposure View, , and Attack Path Analysis interfaces work in conjunction to assist a company in analyzing and prioritizing their data.

Getting Started

Joe logs in and lands on the **Workspace** landing page, where he can see all of his Tenable products and the Tenable One pages he can access. Since he needs to see his exposure risks globally, he selects **Lumin Exposure View**. Joe then lands on the **Global Lumin Exposure View**, where he can see Vulnerability Management, Tenable Identity Exposure, Tenable Web App Scanning, and Cloud data unified into a single score. He may be wondering, "Which category is driving the score?". For this, in the **CES** section, he can select **Per Category** > **Computing Resources**, and filter all the data on the page.

As Joe reviews the metrics to prepare for his next executive meeting, he can change the date ranges so that he can see what's changed over time and high level indicators of why the changes occurred. Since there was a significant change in the score last week, he decides to comment on the **CES Trend** section to ask his coworker, Rachel, for more details.

Prioritize

Now that Joe has a better understanding of the score and which category is driving it, his next question is "Which business owners (i.e., tags) do we need to chase?". Now, he can look at the **Tag Performance** section to quickly see which tags are the highest contributors to his score. This helps Joe prioritize his focus. Again, If he needs more details or has an action item for Rachel, Joe can comment directly on the **Tag Performance** section in the **Exposure View**. Rachel can then drill down into the **Tag Details** to get further information.

Since there's been a priority in process and products, Joe decides to review how his internal **Remediation SLA** efficiency has improved. By expanding the date range to include the past 6 months, he can report on the positive trend in addressing the crucial risks within the set number of days. Seeing how he missed his target SLA efficiency last week, Joe can look at what's outside of SLA (how many risks, how many days, and which tags) to determine what he needs to follow up on.

He wants to share this **Exposure View** with his entire team, so he exports and emails to the team with a high level summary and action items.

Joe takes note of the businesses he wants to focus on within the **Tag Performance** widget, and then creates a custom exposure card for each one.

Customize

Now, Joe takes a look at his **Exposure Card Library**. At a glance, he can see his **General** and **Custom** exposure cards, where he can also see a high level preview of each card's CES and CES trend.

Should he need to create a **Lumin Exposure View** with a different segment, he may ask Rachel to help create a custom tag within the **Asset Inventory**. Rachel creates a tag that is data agnostic (so he can mix and match assets for a tag) and then a custom card using the new tag. She shares this new **Lumin Exposure View** with Joe. Since Joe needs more details, he clicks on the **Top Affecting tags** link and jumps directly to the where he can see all the assets associated with this tag. Here, he can also view asset details, and can even navigate directly to the data source product for more information. Rachel realizes that the static tag should actually be a dynamic tag, so she edits the tag configuration.

Incidents and Actions

Thomas is on the InfoSec team and is responsible for any incidents. His main focus is the **Attack Path Analysis** section, where he can build a custom query highlighting his most sensitive assets. He can then interact with the attack path data and proactively see potential attack paths and techniques. Here, Thomas can answer the following key questions:

- In my environment, what are all possible attack paths between two assets or asset types?
- In my environment, what are all possible attack paths that leverage a specific technique?
- What assets are in jeopardy if one specific asset is compromised? (Blast Radius)
- How do all assets in my network affect one specific asset in my environment? (Asset Exposure)
- Where is an asset within the attack path?
- How critical is an asset?

Asset Inventory Metrics

The following metrics are used to assess data within Asset Inventory:

Cyber Exposure Score (CES)

Asset Inventory calculates a dynamic CES that represents exposure risk as an integer between 0 and 1000, based on the Asset Exposure Score (AES) values for assets. Higher CES values indicate higher risk.

> **Note:** Asset Inventory does not include assets older than 90 days in your CES.

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

Asset Exposure Score (AES)

Asset Inventory calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.

> **Note:** Asset Inventory does not calculate an AES for unlicensed assets.

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

Asset Inventory Categories

Asset Inventory products refer to data sources as **Categories**. For more information, see Data Sources.

Additionally, Asset Inventory uses specific icons to represent each category within the user interface.

Category	Icon
Cloud Resources	
Web Applications	
Identity Exposure	
Computing Resources	

Asset Inventory Scoring Explained

The building blocks for the Cyber Exposure Score (CES) in the Tenable One Exposure Management Platform are similar to those used for years in Tenable products (e.g., Tenable Vulnerability Management, Tenable Lumin). These mechanisms have to date only been used for vulnerability management data. Tenable One expands these concepts into new realms of the attack surface: **Web Applications** (Tenable Web App Scanning), **Cloud Resources** (Tenable Cloud Security), and **Identity** (Tenable Identity Exposure).

For more information on Tenable One scoring, see the *Tenable One Scoring Explained Quick Reference Guide*.

Log in to Asset Inventory

To log in to Asset Inventory:

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

   The **Workspace** page appears.
4. Click the Asset Inventory tile.

   The Asset Inventory interface appears.

Navigate Asset Inventory

Asset Inventory includes several helpful shortcuts and tools that highlight important information and help you to navigate the user interface more efficiently:

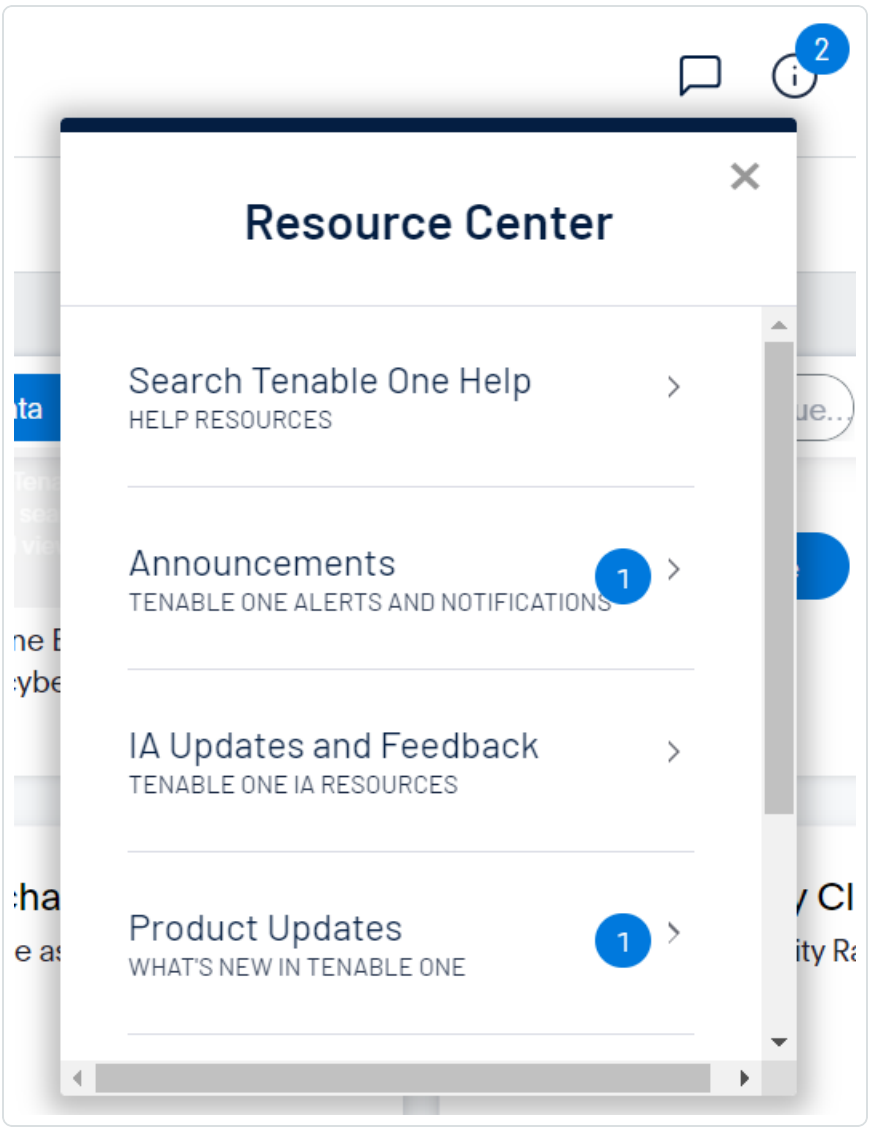
Resource Center

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

To access the Resource Center:

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

   The **Resource Center** menu appears.



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

Settings Icon

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

The **Settings** menu gives you access to user and settings options.

To access the **Settings** menu:

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

   The **Settings** menu appears.

2. Click an item to navigate to that system configuration page.

Workspace

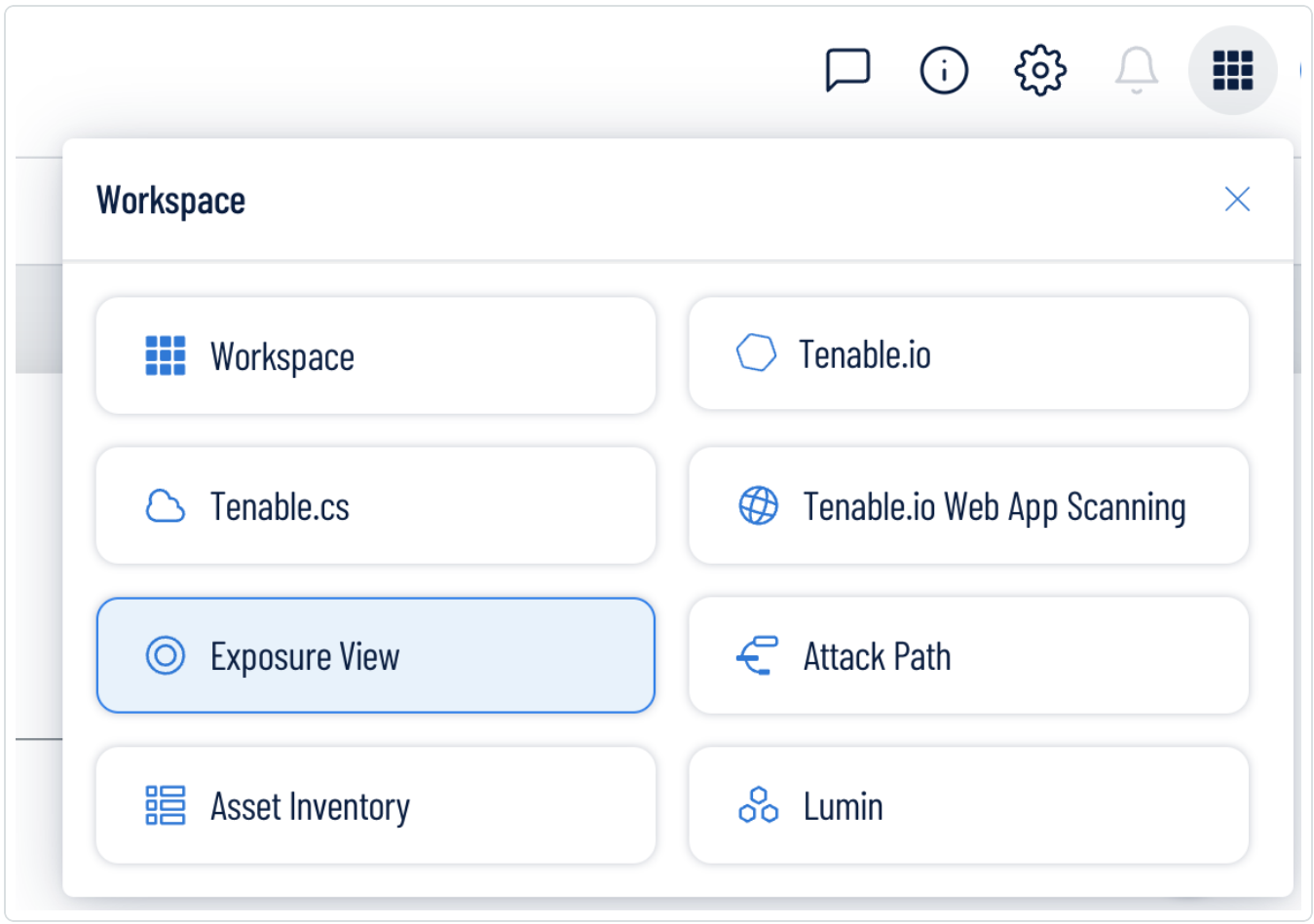
When you log in to Tenable, the **Workspace** page appears by default. On the **Workspace** page, you can switch between your Tenable applications or set a default application to skip the **Workspace** page in the future. You can also switch between your applications from the **Workspace** menu, which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

Open the Workspace Menu

To open the **Workspace** menu:

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

   The **Workspace** menu appears.



2. Click an application tile to open it.

View the Workspace Page

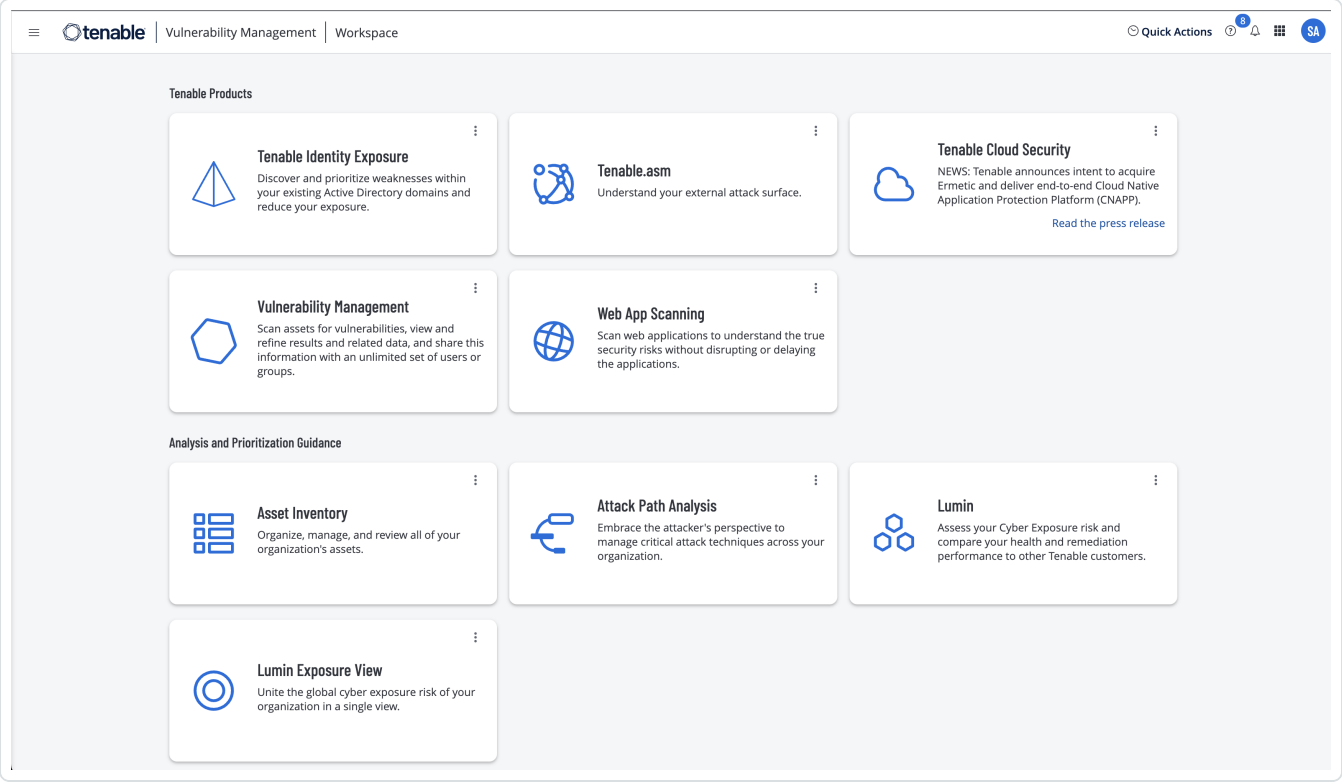
To view the Workspace page:

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

   The **Workspace** menu appears.

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

The **Workspace** page appears.



Set a Default Application

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

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

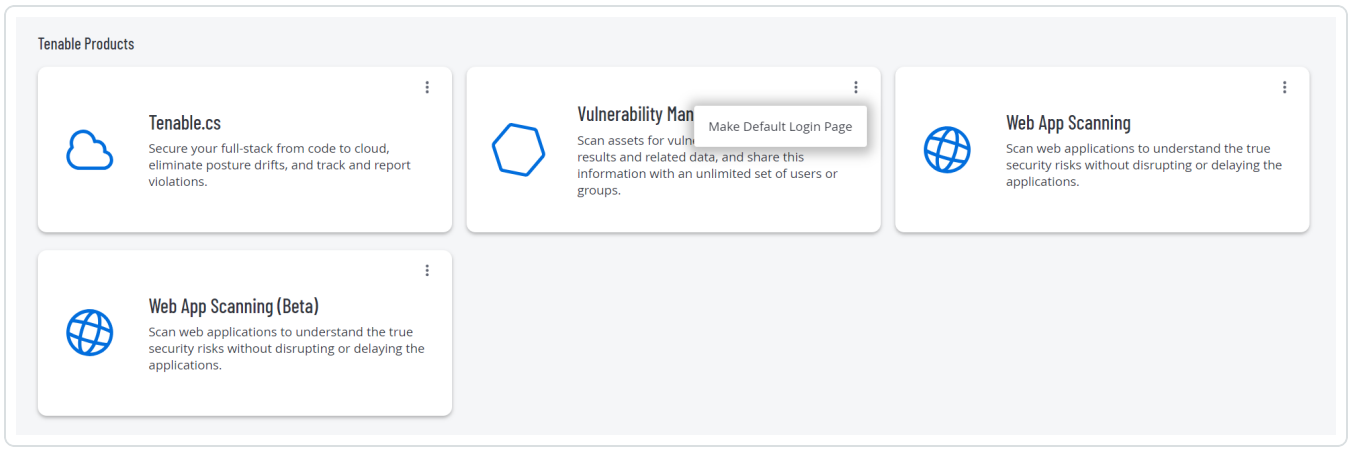
To set a default login application:

1. Log in to Tenable.

   The **Workspace** page appears.

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

   A menu appears.



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

   This application now appears when you log in.

Remove a Default Application

To remove a default login application:

1. Log in to Tenable.

   The **Workspace** page appears.

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

   A menu appears.

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

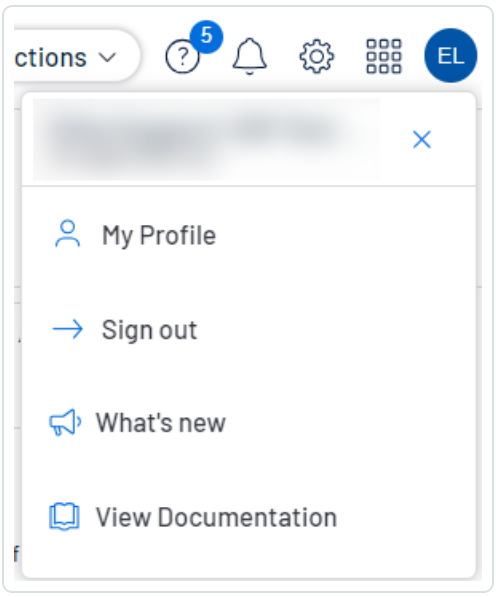
   The **Workspace** page now appears when you log in.

User Account Menu

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

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

   The user account menu appears.



2. Do one of the following:

   - Click **My Profile** to configure your own user account. You navigate directly to the **My Account** settings page. See My Account for more information.
   - Click **Sign out** to sign out of Asset Inventory.
   - Click **What's new** to navigate directly to the Asset Inventory Release Notes.
   - Click **View Documentation** to navigate directly to the Asset Inventory User Guide documentation.

Log out of Asset Inventory

To log out of Asset Inventory:

1. Access the user account menu.
2. Click **Sign Out**.

Access the Asset Inventory

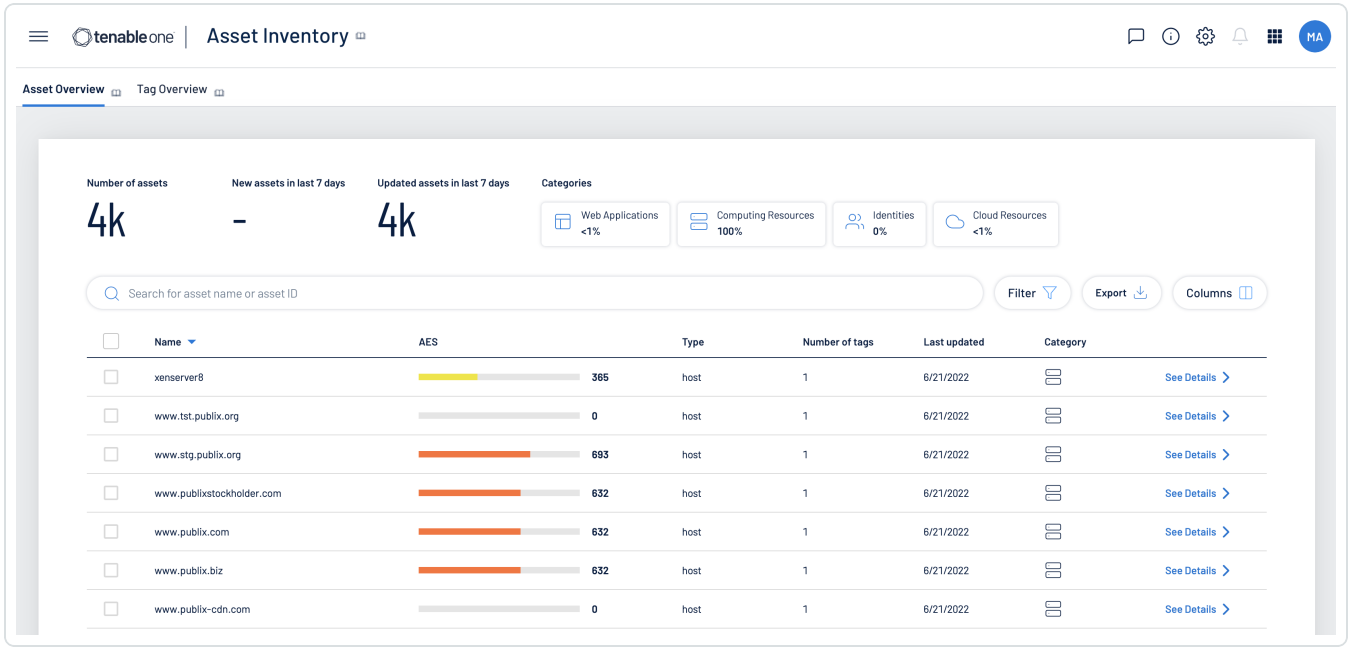
The **Asset Inventory** in Asset Inventory allows you to easily view and manage all of your assets in one location, regardless of their source. You can quickly see which assets are new or updated in the last week, as well as analyze which percentage of assets comes from each individual source. You can also view, manage, and apply tags to assets.

Note: The **Asset Inventory** does not currently support Tenable.asm (Domain Inventory) data.

To access the **Asset Inventory**:

1. In the upper-left corner of the page, click the ☰ button.
2. In the **Analytics** section, click **Asset Inventory**.

   The **Asset Inventory** page appears.

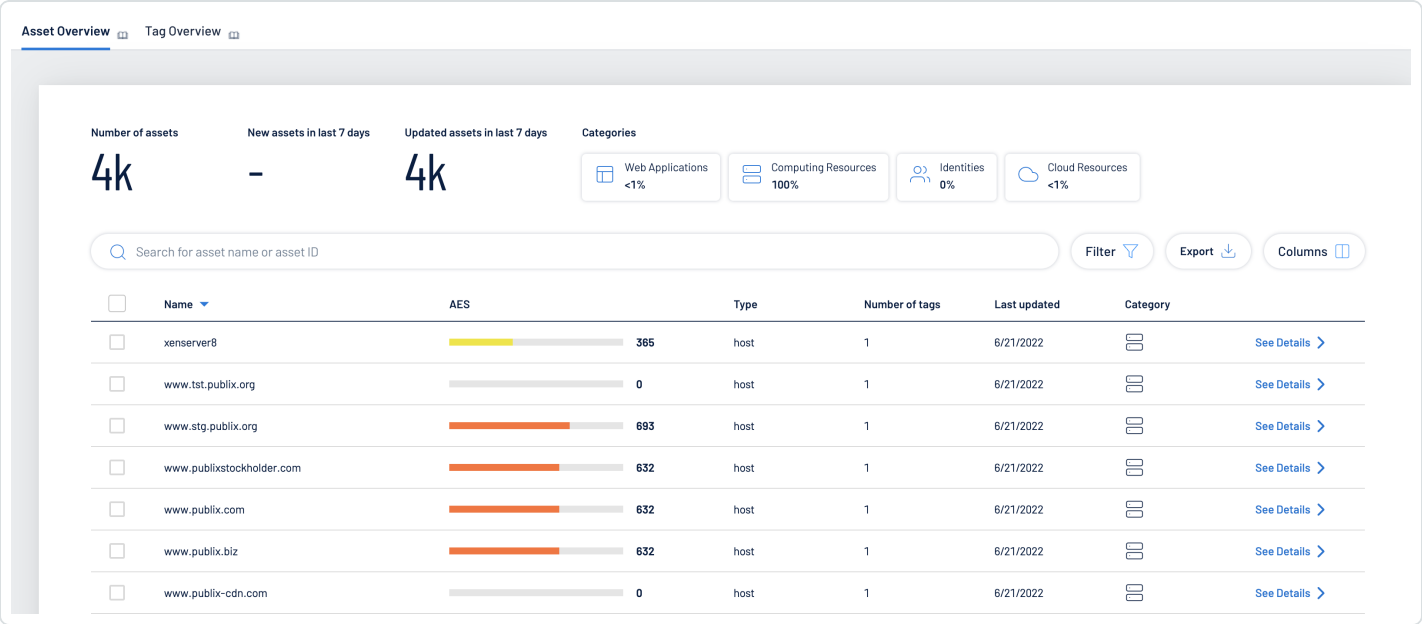


In the **Asset Inventory**, you can:

- View your **Asset Overview**.
- View your **Tag Overview**.

View Your Asset Overview

The **Asset Overview** allows you to view and manage all of your assets. You can quickly see which assets are new or updated in the last week, as well as analyze which percentage of assets come from each individual category.



To view your **Asset Overview**:

1. Access the **Asset Inventory**.
2. At the top of the page, click the **Asset Overview** tab.

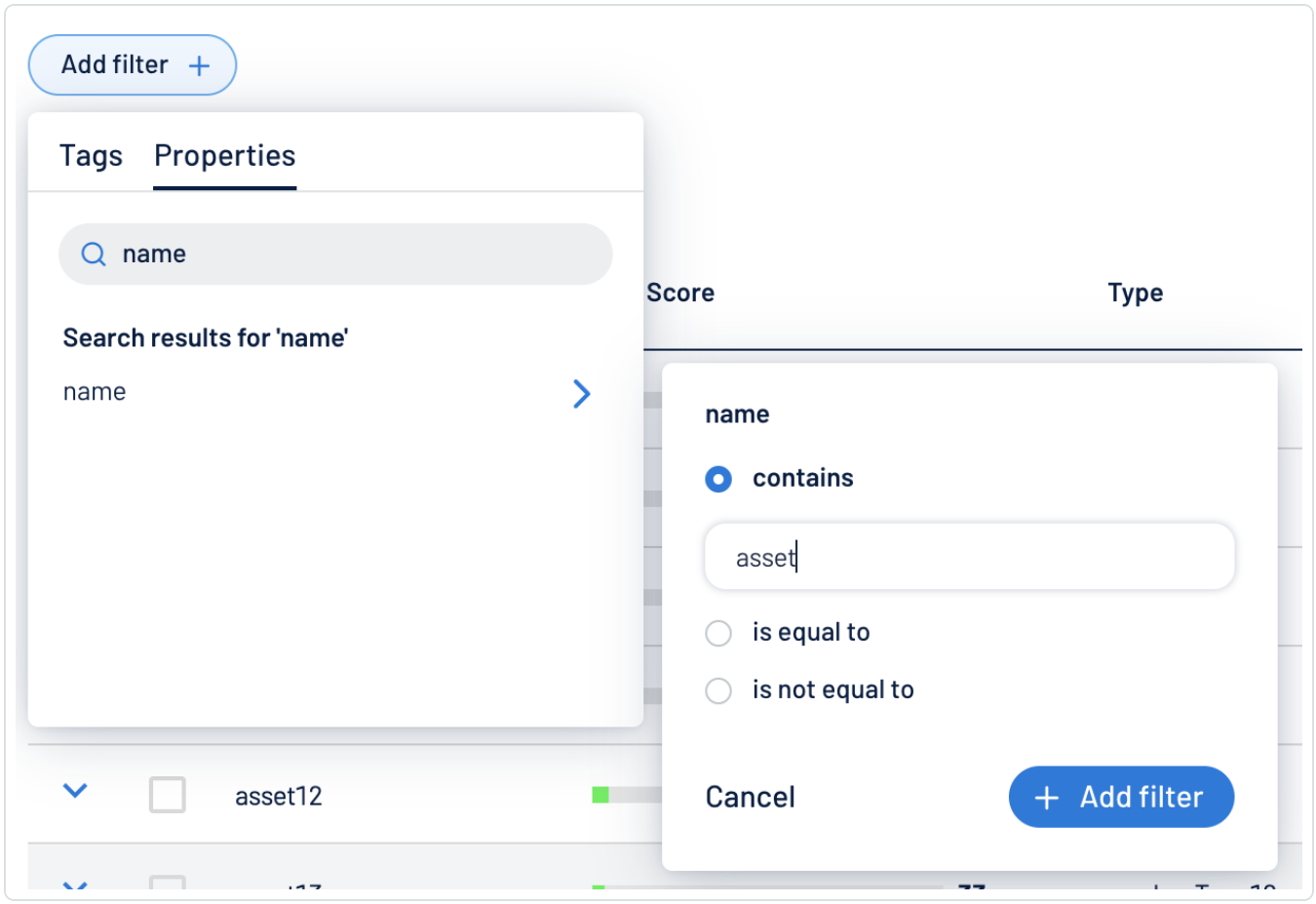
   The **Asset Overview** appears.

In the **Asset Overview**, you can:

- View the total number of assets within your **Asset Inventory**.
- View the total number of new assets added to your **Asset Inventory** within the last 7 days.
- View the total number of updated assets within your **Asset Inventory** within the last 7 days.
- In the **Categories** section, click a category tile to see only data for assets that come from that specific category.

  The asset numbers at the top of the page and the asset list update accordingly.

- Use the **Search** box to search for a specific asset in the asset list.
- Filter the asset list:



a. Click **Filter** .

   The **Add filter** button appears.

b. Click **Add filter** .

   A menu appears.

c. Do one of the following:

   - To search the asset list by tag, click **Tags**.
   - To search the asset list by asset property, click **Properties**.

> **Tip:** See Asset Filters for additional information on available filter types.

d. In the search box, type the criteria by which you want to search the asset list.

   The **Asset Inventory** populates a list of options based on your criteria.

e. Click the tag or property by which you want to filter the asset list.

   A menu appears.

f. Select how to apply the filter. For example, if you want to search for an asset whose name is *Asset14*, then select the **contains** radio button and in the text box, type *Asset14*.

g. Click **Add filter** .

   The filter appears above the asset list.

h. Repeat these steps for each additional filter you want to apply.

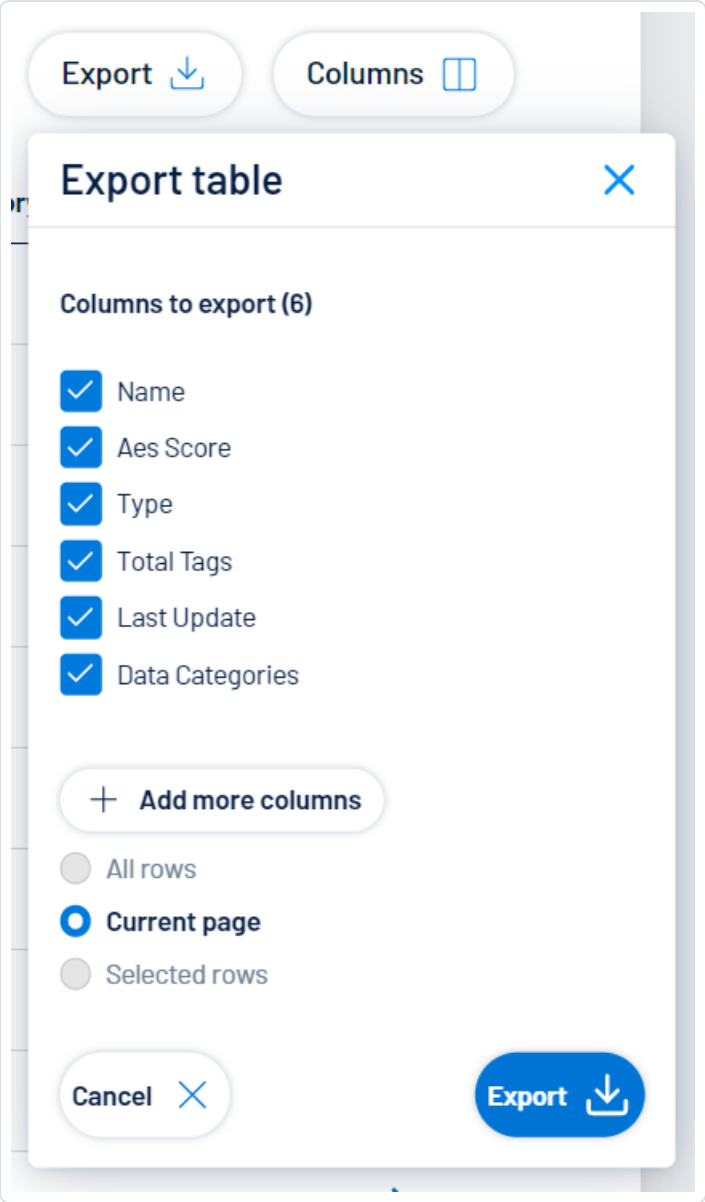
i. Click **Apply filters**.

   The **Asset Inventory** filters the asset list by the designated criteria.

- Export the table:

  a. Click **Export** .

     The **Export table** plane appears.



b. In the **Columns to export** section, select the check box for each column you want to include in the export file.

c. (Optional) To include columns not currently in the table view, click **+ Add more columns**.

   The **Add columns to export** plane appears.

i. Select the check box for each additional column you want to include in the export file.

d. In the rows section, ensure the **Current Page** radio button is selected.

> **Tip:** Currently, you can only export the rows listed on the current page.

e. Click **Export** .

The **Asset Inventory** downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

- Customize the columns in the table:

a. Click **Columns** .

The **Customize columns** window appears.

b. (Optional) In the **Reorder added columns** section, click and drag any column name to reorder the columns.

c. (Optional) In the **Show/Hide** section, select/delesect the check boxes to show or hide columns in the table.

d. (Optional) In the **Remove** section, click the button to permanently remove a column from the table.

e. (Optional) To add columns to the table, click **Add Columns**.

The **Add columns to table** window appears.

i. (Optional) Use the search bar to search for a column property.

The list of column properties updates based on your search query.

ii. Select the check box next to any column or columns you want to add to the table.

iii. Click **Add**.

The column appears in the **Customize columns** window.

f. (Optional) Click **Reset to Defaults** to reset all columns to their defaults.

g. Click **Apply Columns**.

The **Asset Inventory** saves your changes to the columns in the table.

- View a list of your assets. This list includes the following asset information:
  - **Name** — The asset identifier. The **Asset Inventory** assigns this identifier based on the presence of certain asset attributes in the following order:
    1. Agent Name (if agent-scanned)
    2. NetBIOS Name
    3. FQDN
    4. IPv6 address
    5. IPv4 address

    For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the Asset Name.
  - **AES** — The Asset Exposure Score for the asset. The AES represents the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.

    Note: Asset Inventory does not calculate an AES for unlicensed assets.
  - **Type** — The asset type.
  - **Number of tags** — The number of tags applied to the asset. For more information on tagging an asset, see Tag Assets via the Asset Overview.
  - **Last updated** — The date and time at which the **Asset Inventory** last updated the asset.
  - **Category** — The asset category, for example, **Web Applications** or **Computing Resources**.

    Tip: Unsure what the icon in this column means? Check the **Categories** section at the top of the page for information about which category the icon represents. For more information, see Asset Inventory Metrics.

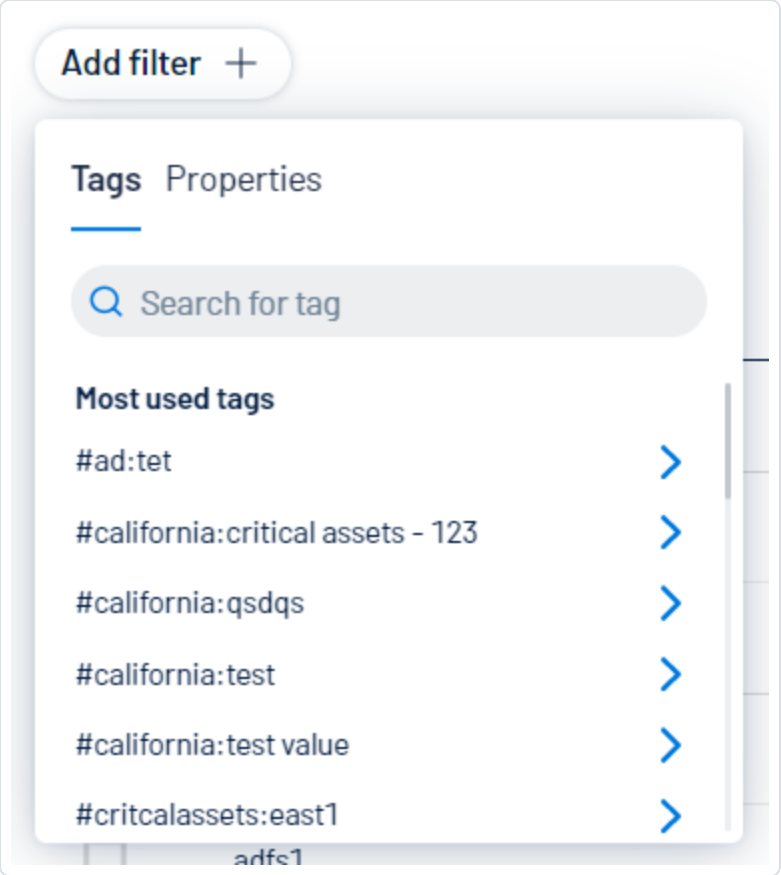
- Click **See details** to view more details about an asset. For more information, see View Asset Details.

Asset Filters

In the **Asset Overview**, you refine the asset list using Tag Filters and Tenable-Provided Filters based on attribute properties.

Tag Filters

Tags allow you to add descriptive metadata to assets that helps you group assets by business context. In the **Asset Overview**, you can use tags to filter the asset list. Under the **Tags** tab, search for or select the tag by which you want to filter the list. For more information, see Tag Assets via the Asset Overview.



Tenable-Provided Filters

Under the **Properties** tab, you can use Tenable-Provided filters to refine the asset list by the following asset properties. The following table lists some, but not all, available filters:

Note: The available Tenable-provided filters in your Asset Inventory instance depend on the data sources you have configured within Asset Inventory. For more information, see Data Sources.

Filter	Description
id	The asset's UUID.
name	The asset identifier. Asset Inventory assigns this identifier based on the presence of certain asset attributes in the following order: 1. Agent Name (if agent-scanned) 2. NetBIOS Name 3. FQDN 4. IPv6 address 5. IPv4 address For example, if scans identify a NetBIOS name and an IPv4 address for an asset, the NetBIOS name appears as the asset name.
aes_score	(Requires Tenable Lumin license) The Asset Exposure Score (AES) calculated for the asset.
last_update	The time and date when the asset record was last updated.
total_tags	The total number of tags associated with the asset.
type	The type of asset.
system_type	The system types as reported by Plugin ID 54615. For more information, see Tenable Plugins.
created	The time and date when Asset Inventory created the asset record.
sources	The source of the scan that identified the asset.
last_licensed_scan_time	The time and date of the last scan that identified the asset as

	licensed.
first_observed	The date and time when a scan first identified the asset.
last_observed	The date and time of the scan that most recently identified the asset.
bios_id	The NetBIOS ID for the asset.
fqdns	The fully qualified domain name of the host that the vulnerability was detected on.
mac_addresses	A MAC address that a scan has associated with the asset record.
host_name	The hostname of the asset. This string is determined by information reported by target plugins, and is dependent on the user's environment and configuration.
netbios_name	The NetBIOS name for the asset.
network_id	The ID of the network object associated with scanners that identified the asset.
operating_systems	The operating systems that a scan identified as installed on the asset.
ssh_fingerprint	The SSH fingerprint associated with the asset.
installed_software	The software that a scan identified as installed on the asset.
acr_score	(Requires Tenable Lumin license) The asset's ACR.
critical_vuln_counts	The number of vulnerabilities that are of critical severity on the asset.
high_vuln_counts	The number of vulnerabilities that are of high severity on the asset.
medium_vuln_counts	The number of vulnerabilities that are of medium severity on the asset.

low_vuln_counts	The number of vulnerabilities that are of low severity on the asset.
has_severity_vulns	Specifies whether the asset has associated severity vulnerabilities.
has_plugin_results	Specifies whether the asset has plugin results.
tenable_id	The UUID of the asset in Tenable Vulnerability Management.
service_now_sys_id	Where applicable, the unique record identifier of the asset in ServiceNow. For more information, see the ServiceNow documentation.
ipv4_addresses	The IPv4 address associated with the asset record. This filter supports multiple asset identifiers as a comma-separated list (for example, hostname_example, example.com, 192.168.0.0). For IP addresses, you can specify individual addresses, CIDR notation (for example, 192.168.0.0/24), or a range (for example, 192.168.0.1-192.168.0.255). **Note:** Ensure the filter value does not end in a period.
ipv6_addresses	An IPv6 address that a scan has associated with the asset record. This filter supports multiple asset identifiers as a comma-separated list. The IPV6 address must be an exact match. (for example, 0:0:0:0:0:ffff:c0a8:0). **Note:** Ensure the filter value does not end in a period.
last_authenticated_scan_time	The date and time of the last authenticated scan run against the asset.
cloud_source	The cloud source of the scan that identified the asset.
is_public	Specifies whether the asset is available on a public network.

	Note: A public asset is within the public IP space and identified by the `is_public` attribute in the Tenable Vulnerability Management `query` namespace.
is licensed	Specifies whether or not the asset is included in your license count.
aws_ec2_instance_ami_id	The unique identifier of the Linux AMI image in Amazon Elastic Compute Cloud (Amazon EC2). For more information, see the Amazon Elastic Compute Cloud Documentation.
aws_availability_zone	The name of the Availability Zone where AWS hosts the virtual machine instance. For more information, see Regions and Availability Zones in the AWS documentation.
aws_ec2_instance_id	The unique identifier of the Linux instance in Amazon EC2. For more information, see the Amazon Elastic Compute Cloud Documentation.
aws_ec2_instance_type	The type of virtual machine instance in Amazon EC2. Amazon EC2 instance types dictate the specifications of the instance (for example, how much RAM it has). For a list of possible values, see Amazon EC2 Instance Types in the AWS documentation.
aws_ec2_name	The name of the virtual machine instance in Amazon EC2.
aws_owner_id	A UUID for the Amazon Web Service (AWS) account that created the virtual machine instance. For more information, see AWS Account Identifiers in the AWS documentation.
aws_ec2_product_code	The product code associated with the AMI used to launch the virtual machine instance in Amazon EC2.
aws_region	The region where AWS hosts the virtual machine instance, for example, `us-east-1`. For more information, see Regions and Availability Zones in the AWS documentation.
aws_ec2_instance_group_	The group names within the virtual machine instance in

names	Amazon EC2.
aws_ec2_instance_state_name	The state name of the virtual machine instance in AWS at the time of the scan. For possible values, see API Instance State in the Amazon Elastic Compute Cloud Documentation.
aws_subnet_id	The unique identifier of the AWS subnet where the virtual machine instance was running at the time of the scan.
aws_vpc_id	The unique identifier of the public cloud that hosts the AWS virtual machine instance. For more information, see the Amazon Virtual Private Cloud User Guide.
is_managed_by_ssm	Specifies whether the asset is on a system managed by an AWS Systems Manager (SSM).
azure_resource_id	The unique identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
azure_vm_id	The unique identifier of the Microsoft Azure virtual machine instance. For more information, see Accessing and Using Azure VM Unique ID in the Microsoft Azure documentation.
azure_subscription_id	The unique subscription identifier of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
azure_resource_group	The name of the resource group in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
azure_location	The location of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.
azure_type	The type of the resource in the Azure Resource Manager. For more information, see the Azure Resource Manager Documentation.

account_id	The account ID associated with the asset.
resource_name	The resource name for the asset.
resource_id	The resource ID for the asset.
resource_type	The asset's cloud resource type (for example, network, virtual machine).
unique_identifier	The UUID for the cloud resource account associated with the asset.
source	The source of the scan that identified the asset
region	The cloud region where the asset runs.
zone	The zone where the asset runs.
discovery_information	Specific information about how or where a scan discovered the asset.
cloud_tags	Tenable Vulnerability Management tags associated with the asset. For more information, see Tags in the *Tenable Vulnerability Management User Guide*.
gcp_instance_id	The unique identifier of the virtual machine instance in Google Cloud Platform (GCP).
gcp_project_id	The customized name of the project to which the virtual machine instance belongs in GCP. For more information, see Creating and Managing Projects in the GCP documentation.
gcp_zone	The zone where the virtual machine instance runs in GCP. For more information, see Regions and Zones in the GCP documentation.
ssl_tls_enabled	Specifies whether the application on which the asset is hosted uses SSL/TLS public-key encryption.

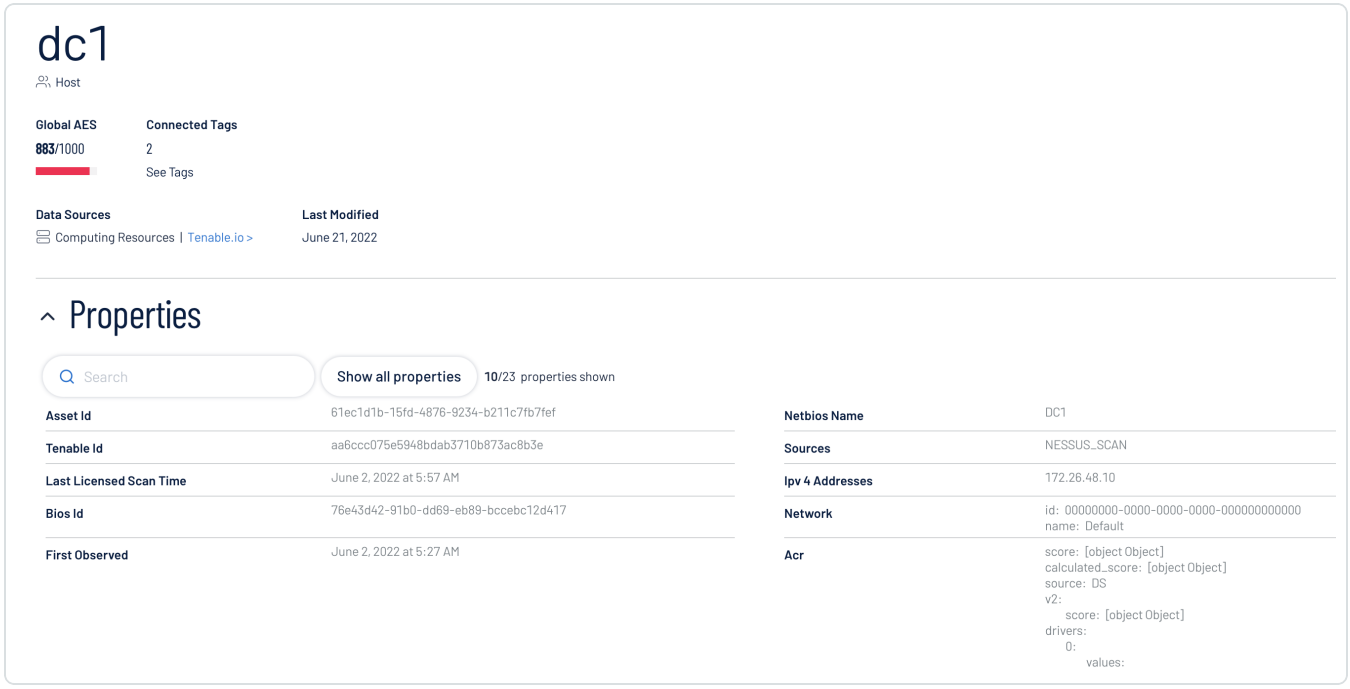
View Asset Details

In the **Asset Inventory**, you can view details for any asset via the **Asset Overview**.

To view asset details:

1. Access the **Asset Overview**.
2. In the row of the asset for which you want to view details, click **See details**.

   The asset details page appears.



On the asset details page, you can:

- View the **Asset Name**.
- View the **Global AES** for the asset.

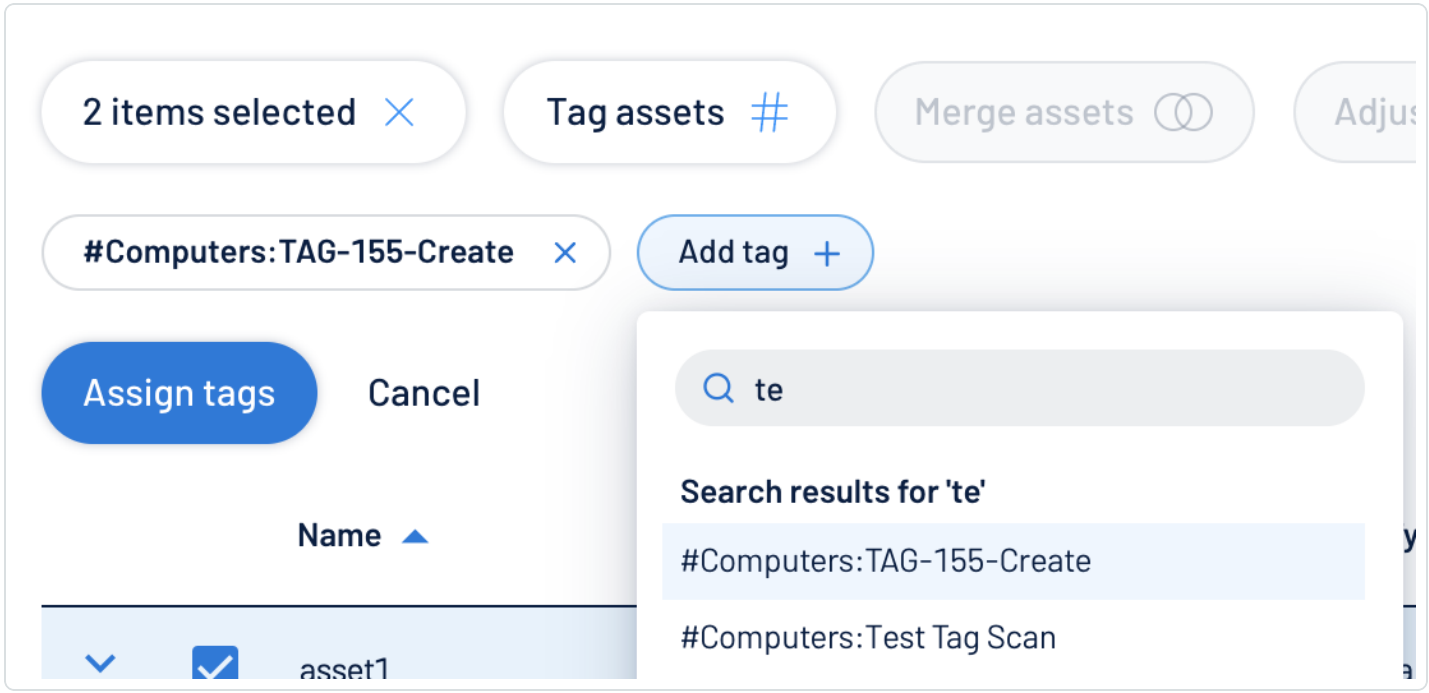
  > **Note:** The **Asset Inventory** does not calculate an AES for unlicensed assets.

- View the number of **Connected Tags** associated with the asset.
  - Click **See Tags** to view the list of connected tags.
- View the **Data Sources** for the asset.

    - Click the name of a data source to navigate to that source.
- View the date at which the asset was **Last Modified**.
- View the **Properties** associated with the asset.
    - Use the search bar to search for a specific asset property.
    - Click **Show all properties** to view all asset properties.
- View the **Related tags** associated with the asset. You can interact with this table the same way you interact with the **Tag Overview** table.

Tag Assets via the Asset Overview

In the **Asset Overview**, you can apply tags directly to an asset in the asset list.



To apply a tag to an asset:

1. Access the **Asset Overview**.
2. In the asset list, select the check box next to any assets to which you want to apply the tag.
3. At the top of the asset list, click **Tag assets** # .

   The **Add tag** + button appears.
4. Click **Add tag** + .

   A **Search** box appears.
5. In the **Search** box, type the name of the tag you want to apply to the asset or assets.

   > **Tip:** To create a new tag, type the [category]:value pair and, at the bottom of the window, click ⊕.
6. Click the name of the tag you want to apply to the asset or assets.

The tag appears above the asset list.

7. Repeat these steps for each additional tag you want to apply.
8. Click **Assign Tags**.

   The **Asset Inventory** assigns the designated tags to the asset or assets.

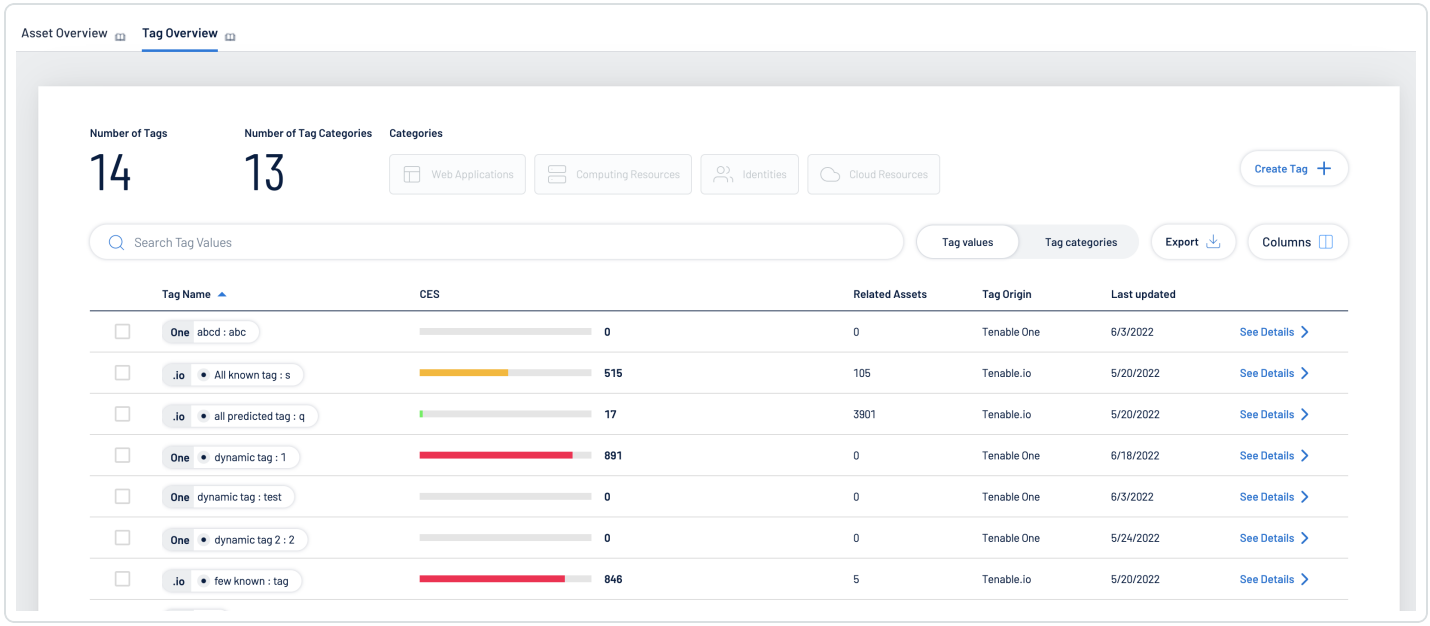
What to do next:

- Create a custom exposure card based on the asset data.

View Your Tag Overview

In the **Asset Inventory**, you can add your own business context to assets by tagging them with descriptive metadata. An asset tag is primarily composed of a *Category:Value* pair. For example, if you want to group your assets by location, create a *Location* category with the value *Headquarters*. For more information about tag structure, see Tag Format and Application.

The **Tag Overview** allows you to view and manage all of your tags. You can quickly identify your number of tags, their related assets, and analyze the origin of each tag.



To view your **Tag Overview**:

1. Access the **Asset Inventory**.
2. At the top of the page, click the **Tag Overview** tab.

   The **Tag Overview** appears.

In the **Tag Overview**, you can:

- View the total number of tags within your Asset Inventory instance.
- Manage your tags:

- Create a Tag
- Edit a Tag
- Delete a Tag

- In the **Categories** section, click a category tile to see only data for tags that come from that specific data source.

  The tag numbers at the top of the page and the tag list update accordingly.

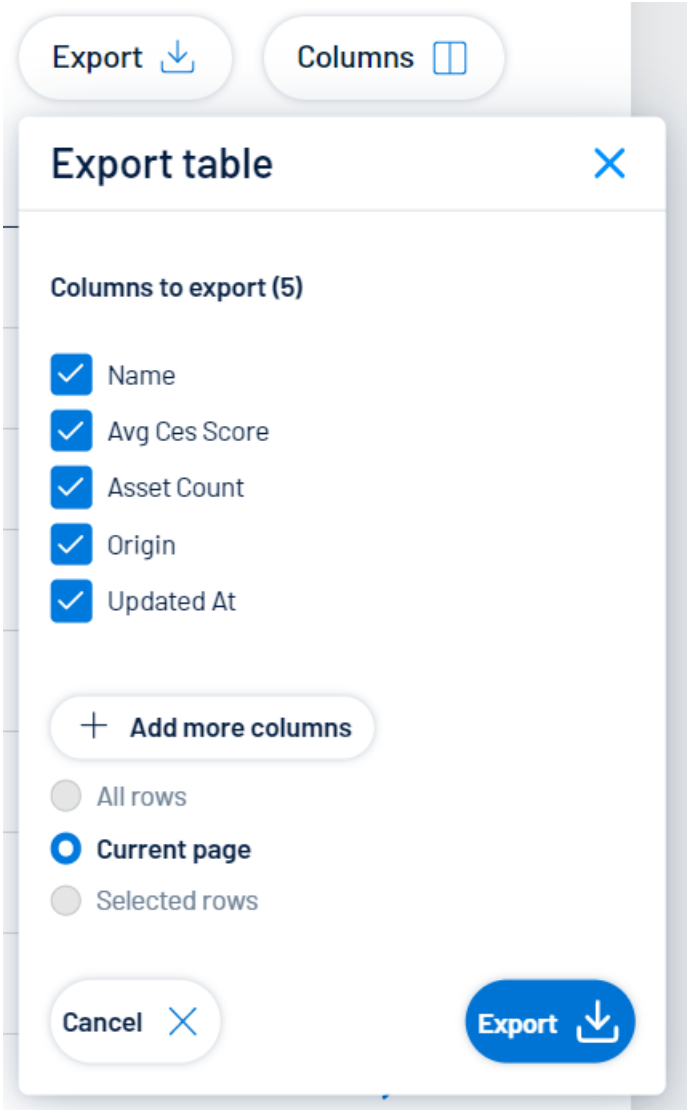
- Use the **Search** box to search for a specific tag in the tag list.
- Filter the tag list by tag type:
  - To view only tag values, next to the **Search** box, click **Tag values**.
  - To view only tag categories, next to the **Search** box, click **Tag categories**.

  The tag list updates based on your selection.

- Export the table:

  a. Click **Export** .

  The **Export table** plane appears.



b. In the **Columns to export** section, select the check box for each column you want to include in the export file.

c. (Optional) To include columns not currently in the table view, click **Add more columns**.

   The **Add columns to export** plane appears.

   i. Select the check box for each additional column you want to include in the export file.

d. In the rows section, ensure the **Current Page** radio button is selected.

> **Tip:** Currently, you can only export the rows listed on the current page.

e. Click **Export** .

The **Asset Inventory** downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

- Customize the columns in the table:

a. Click **Columns** .

The **Customize columns** window appears.

b. (Optional) In the **Reorder added columns** section, click and drag any column name to reorder the columns.

c. (Optional) In the **Show/Hide** section, select/delesect the check boxes to show or hide columns in the table.

d. (Optional) In the **Remove** section, click the button to permanently remove a column from the table.

e. (Optional) To add columns to the table, click **Add Columns**.

The **Add columns to table** window appears.

i. (Optional) Use the search bar to search for a column property.

The list of column properties updates based on your search query.

ii. Select the check box next to any column or columns you want to add to the table.

iii. Click **Add**.

The column appears in the **Customize columns** window.

f. (Optional) Click **Reset to Defaults** to reset all columns to their defaults.

g. Click **Apply Columns**.

The **Asset Inventory** saves your changes to the columns in the table.

- View a list of your tags. This list includes the following tag information:

List Type	Columns
Tag Values	◦ **Tag name** — The name of the tag value. ◦ **CES** — The Cyber Exposure Score for the tag. The CES represents Cyber Exposure risk as an integer between 0 and 1000, based on the Asset Exposure Score (AES) values for the assets to which the tag is applied. Higher CES values indicate higher risk. ◦ **Related Assets** — The number of assets to which the tag is applied. ◦ **Tag Origin** — The origin application for the tag. ◦ **Last updated** — The date on which a user last updated the tag. ◦ Click **See details** to view more details about an asset. For more information, see View Tag Details.
Tag Categories	◦ **Tag category** — The name of the tag category. ◦ **CES** — The Cyber Exposure Score for the tag. The CES represents Cyber Exposure risk as an integer between 0 and 1000, based on the Asset Exposure Score (AES) values for the assets to which the tag is applied. Higher CES values indicate higher risk. ◦ **Related Assets** — The number of assets to which the tag is applied. ◦ **Tag values** — The number of tag values associated with the tag category. ◦ **Tag Origin** — The origin application for the tag. ◦ **Created** — The date on which the tag category was created. ◦ **Last updated** — The date on which a user last updated the tag category. ◦ Click **See details** to view more details about an asset. For more information, see View Tag Details.

Tag Format and Application

An asset tag is primarily composed of a *Category*:*Value* pair. For example, if you want to group your assets by location, create a *Location* category with the value *Headquarters*.

> **Note:** If you want to create tags without individual categories, Tenable recommends that you add the generic category *Category*, which you can use for all your tags.

Static Tags vs. Dynamic Tags

When you create a tag, you can choose between the following tag types:

- **static** — You must manually apply the tag to individual assets. Alternatively, you can manually apply an automatic tag to additional assets that may not meet the rules criteria for that tag.
- **dynamic** — The **Asset Inventory** automatically applies the tag to the assets on your instance that match the tag rules. When you create an automatic tag, the **Asset Inventory** applies that tag to all your current assets and any new assets added to your organization's account. The **Asset Inventory** also regularly reviews your assets for changes to their attributes and adds or removes automatic tags accordingly.

  > **Note:** When you create or edit a dynamic tag, the **Asset Inventory** may take some time to apply the tag to existing assets, depending on the system load and the number of matching assets.

See the following examples for clarification:

Scenarios	Tag Type
You create a tag with *Location*:*Headquarters* as the *Category*:*Value* pair, but you do not add any tag rules. Later, you add the tag to assets located at your headquarters.	static
You create a tag with *Location*:*Headquarters* as the *Category*:*Value* pair, and you specify an IP address range in the tag rules. Tenable Vulnerability Management then automatically applies the tag to all existing or new assets within that IP address range.	dynamic

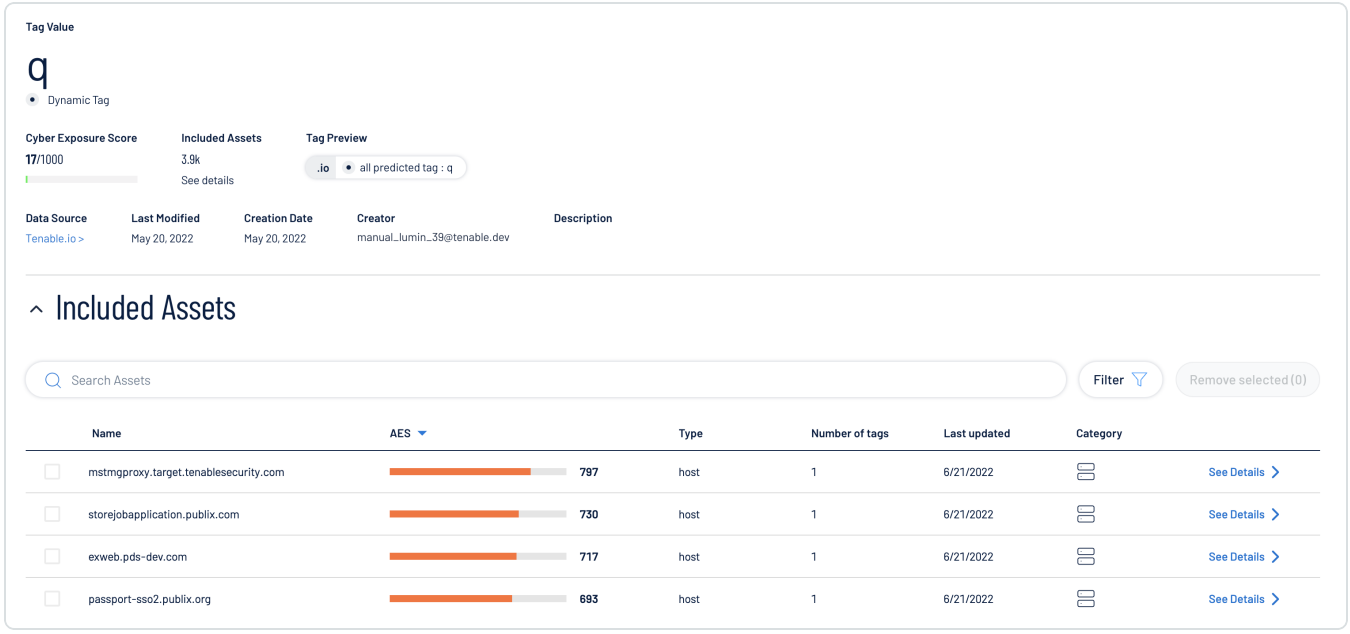
View Tag Details

In Asset Inventory, you can view details for any tag value or category within your **Tag Overview**.

1. Access the **Tag Overview**.
2. Filter the tag list by tag type:
   - To view tag value details, next to the **Search** box, click **Tag values**.
   - To view tag category details, next to the **Search** box, click **Tag categories**.

   The tag list updates based on your selection.
3. In the row of the tag value or category for which you want to view details, click **See details**.

   The tag details page appears.



On the tag details page, you can:

- View the name of the **Tag Value** or **Tag Category**.
- View the **Cyber Exposure Score** for the tag value or category.
- View the number of **Included Assets** associated with the tag value or category.
  - Click **See Details** to view the list of included assets.

- (Tag categories only) View the number of **Associated Tag Values** with the tag category.
- View the **Data Source** for the tag value or category.
    - Click the name of a data source to navigate to that source.
- View the date at which the tag value or category was **Last Modified**.
- View the **Creation Date** of the tag value or category.
- View the **Creator** of the tag value or category.
- View a **Description** of the tag value or category.
- (Tag values only) View a list of the **Included Assets** associated with the tag value. You can interact with this table the same way you interact with the **Asset Overview** table.
- (Tag categories only) View a list of the **Associated Tag Values** with the tag category. You can interact with this table the same way you interact with the **Tag Overview** table.

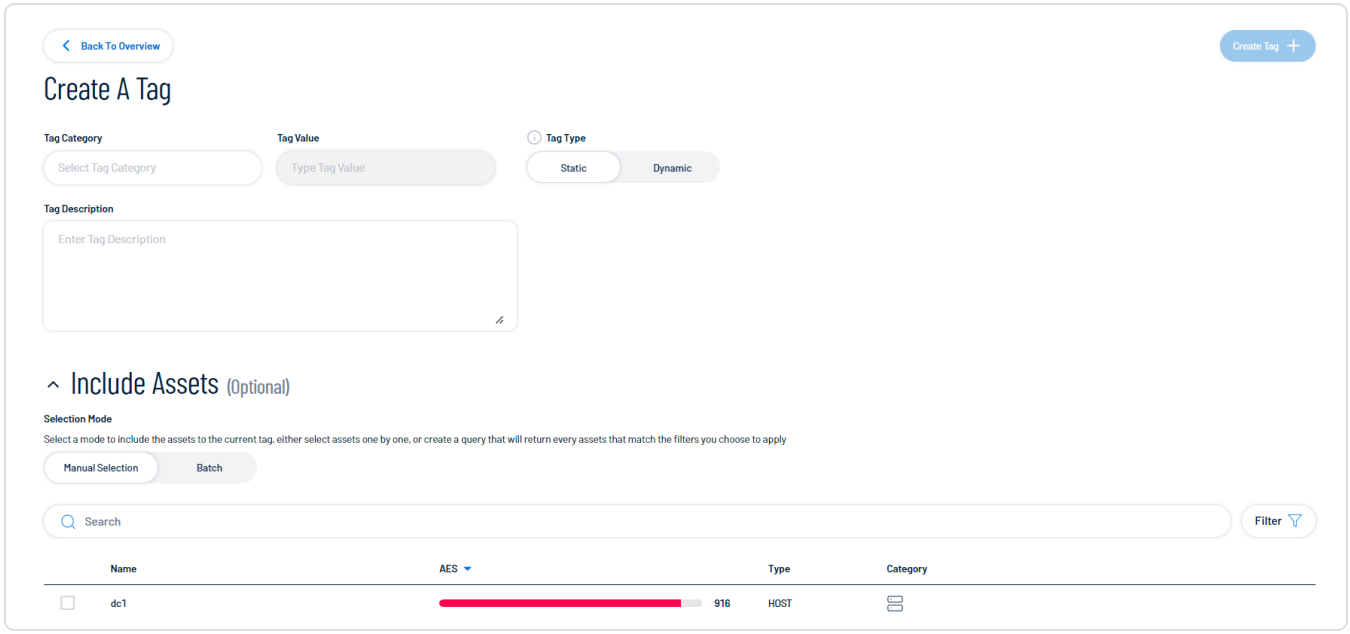
Create a Tag

In the **Tag Overview**, you can create a static tag to apply to assets individually. You can also create an automatic tag by creating tag rules that the **Asset Inventory** uses to identify and tag matching assets.

To create a tag:

1. Access the **Tag Overview**.
2. Click **Create tag** .

   The **Create a Tag** page appears.



3. In the **Tag category** drop-down menu, do one of the following:
   - Select an existing category to which to add the new tag.
   - Add a new tag category:
     a. In the text box, type a name for the new category.
     b. In the **Add new Category** section, click the button.

        The **Asset Inventory** adds the new category.
4. In the **Tag value** text box, type a name for the tag value.

5. In the **Tag type** section, choose the type of tag to create:

> **Tip:** For more information, see Tag Format and Application.

- **Static** — You must manually apply the tag to individual assets.

  The **Include assets** section appears and displays a list of assets:

  a. In the **Selection Mode** section, choose the mode by which you want to apply the tag to assets:

     - **Manual selection** — Manually tag individual assets.
     - **Batch** — Create a query to select the assets to which you want to apply the tag.

  b. (Optional) Filter the asset list:

     i. Click **Filter** .

     The **Add filter** button appears.

     ii. Click **Add filter** .

     A menu appears.

iii. Do one of the following:

- To search the asset list by tag, click **Tags**.
- To search the asset list by asset property, click **Properties**.

iv. In the search box, type the criteria by which you want to search the asset list.

The **Asset Inventory** populates a list of options based on your criteria.

v. Click the tag or property by which you want to filter the asset list.

A menu appears.

vi. Select how to apply the filter. For example, if you want to search for an asset whose name is *Asset14*, then select the **contains** radio button and in the text box, type *Asset14*.

vii. Click **Add filter**.

The filter appears above the asset list.

viii. Repeat these steps for each additional filter you want to apply.

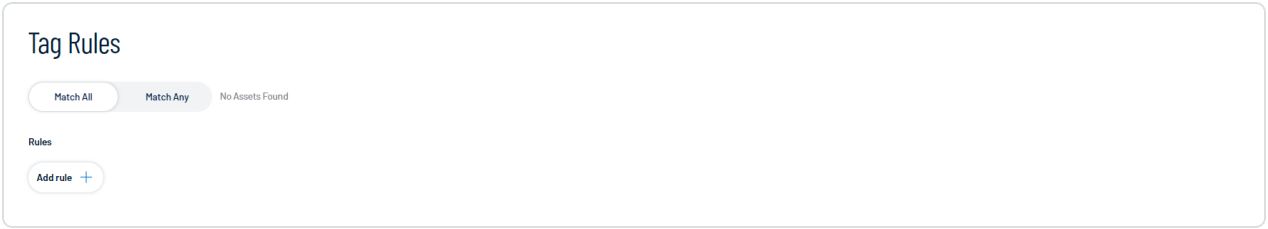
ix. Click **Apply filters**.

The **Asset Inventory** filters the asset list by the designated criteria.

c. Select the check box next to the asset or assets to which you want to apply the tag.

- **Dynamic** — The **Asset Inventory** automatically applies the tag to the assets on your instance that match the tag rules.

The **Tag Rules** section appears:



a. In the **Tag Rules** section, select how to apply the tag rule:

   - **Match All** — Apply the tag to only assets that match all of the rules.
   - **Match Any** — Apply the tag to assets that match any of the rules.

b. In the **Rules** section, click **Add rule** :

   i. Do one of the following:

      - To add a rule based on tags, click **Tags**.
      - To add a rule based on asset property, click **Properties**.

   ii. In the **Tag** or **Properties** list, select the tag or property for which you want to add a rule.

   A logic operator window appears.

   iii. Select one of the following operators:

> **Note:** The available operators depend on your selection from the **Tag** or **Properties** list.

Operator	Description
includes tag	Filters for items that include the selected tag.
excludes tag	Filters for items that exclude the selected tag.
is equal to / includes / include property	Filters for items that include the filter value.
is not equal to / excludes / exclude property	Filters for items that do not include the filter value.
is greater than	Filters for items greater than the

Operator	Description
	filter value.
is less than	Filters for items less than the filter value.
matches	Filters for items that match the filter value.
does not match	Filters for items that do not match the filter value.
contains	Filters for items that contain the filter value.
does not have	Filters for items that do not contain the filter value.
has only	Filters for items that have only the filter value.

iv. In the text box, type the constraint value to use for the filter.

> **Tip:** Some text filters support the character (*****) as a wildcard to stand in for a section of text in the filter value. For example, if you want the filter to include all values that end in 1, type **1*. If you want the filter to include all values that begin with 1, *type 1**.
>
> You can also use the wildcard operator to filter for values that contains certain text. For example, if you want the filter to include all values with a 1 somewhere between the first and last characters, type **1**.

v. Click **Add filter** .

Asset Inventory adds the rule and its filters to the tag.

6. In the upper-right corner of the page, click **Create tag** .

Asset Inventory saves the tag and applies it to the appropriate assets. Asset Inventory may take several minutes to apply the tag to the selected assets and update any associated asset counts.

Edit a Tag

In the **Tag Overview**, you can edit one or more components of a tag, including the category to which the tag belongs as well as the tag's name, description, and any rules applied to the tag.

> **Note:** You can only edit tags created within the **Asset Inventory**. For more information, see Create a Tag.

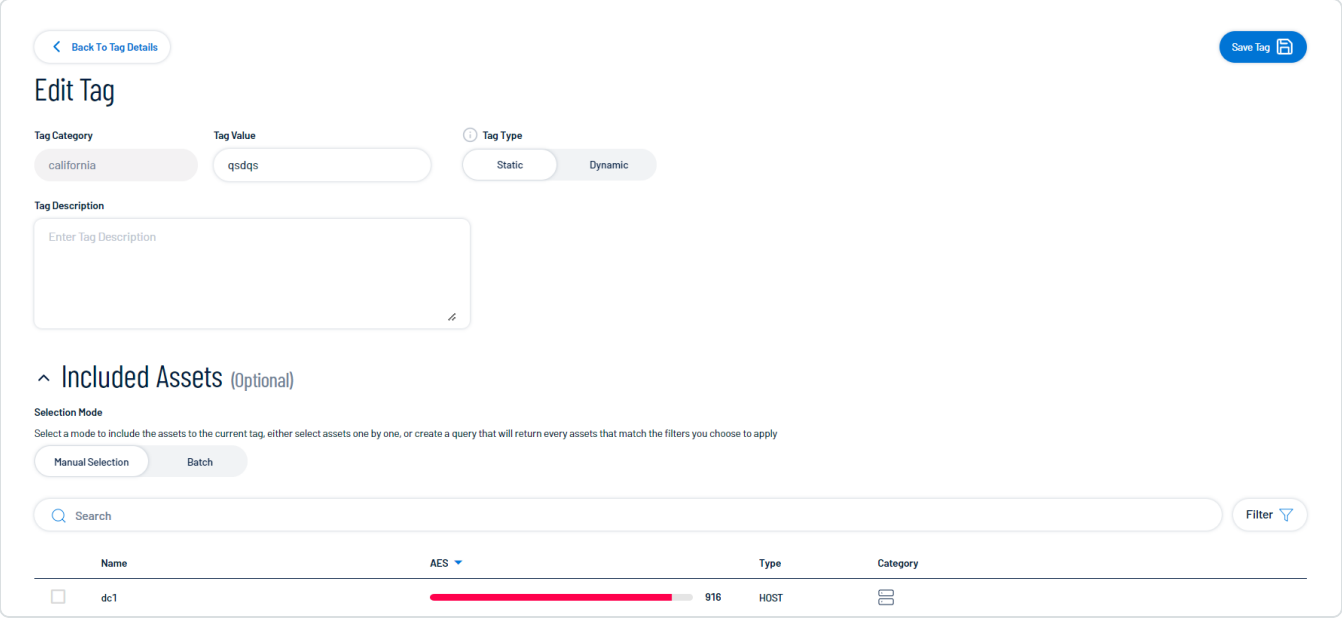
To edit a tag:

1. Access the **Tag Overview**.
2. Filter the tag list by tag type:
   - To edit a tag value, next to the **Search** box, click **Tag values**.
   - To edit a tag category, next to the **Search** box, click **Tag categories**.

   The tag list updates based on your selection.
3. In the tag list, in the row for the tag value or tag category you want to edit, click **See Details**.

   The tag details page appears.
4. In the upper-right corner, click **Edit**.

   The **Edit Tag** page appears.



5. Make any desired changes.
6. Click **Save** .

   The **Asset Inventory** saves your changes to the tag value or tag category.

Delete a Tag

In the **Asset Inventory**, you can delete the following components of a tag:

- Tag value — The **Asset Inventory** removes that specific tag from all assets where you applied the tag.
- Tag category — The **Asset Inventory** deletes any tags created under that category and removes those tags from all assets where you applied the tag.

> **Note:** You can only delete tag values or categories created within the **Asset Inventory**. For more information, see Create a Tag.

To delete a tag:

1. Access the **Tag Overview**.
2. Filter the tag list by tag type:
   - To delete a tag value, next to the **Search** box, click **Tag values**.
   - To delete a tag category, next to the **Search** box, click **Tag categories**.

   The tag list updates based on your selection.
3. Do one of the following:
   - Delete one or more tag values or categories via the tag list:
     a. Select the check box next to the tag value or category that you want to delete.
     b. At the top of the table, click **Remove** .
   - Delete a tag value or category via the tag details page:
     a. In the tag list, in the row for the tag value or tag category you want to delete, click **See Details**.

        The tag details page appears.
     b. In the upper-right corner, click **Delete** .

   A confirmation message appears.

4. Click **Delete tags** .

   The **Asset Inventory** does the following:

   - If you deleted a tag value, the **Asset Inventory** deletes the tag value and removes it from all assets where you applied the tag.
   - If you deleted a tag category, the **Asset Inventory** deletes the category, any tags created under that category, and removes those tags from all assets where you applied the tag.

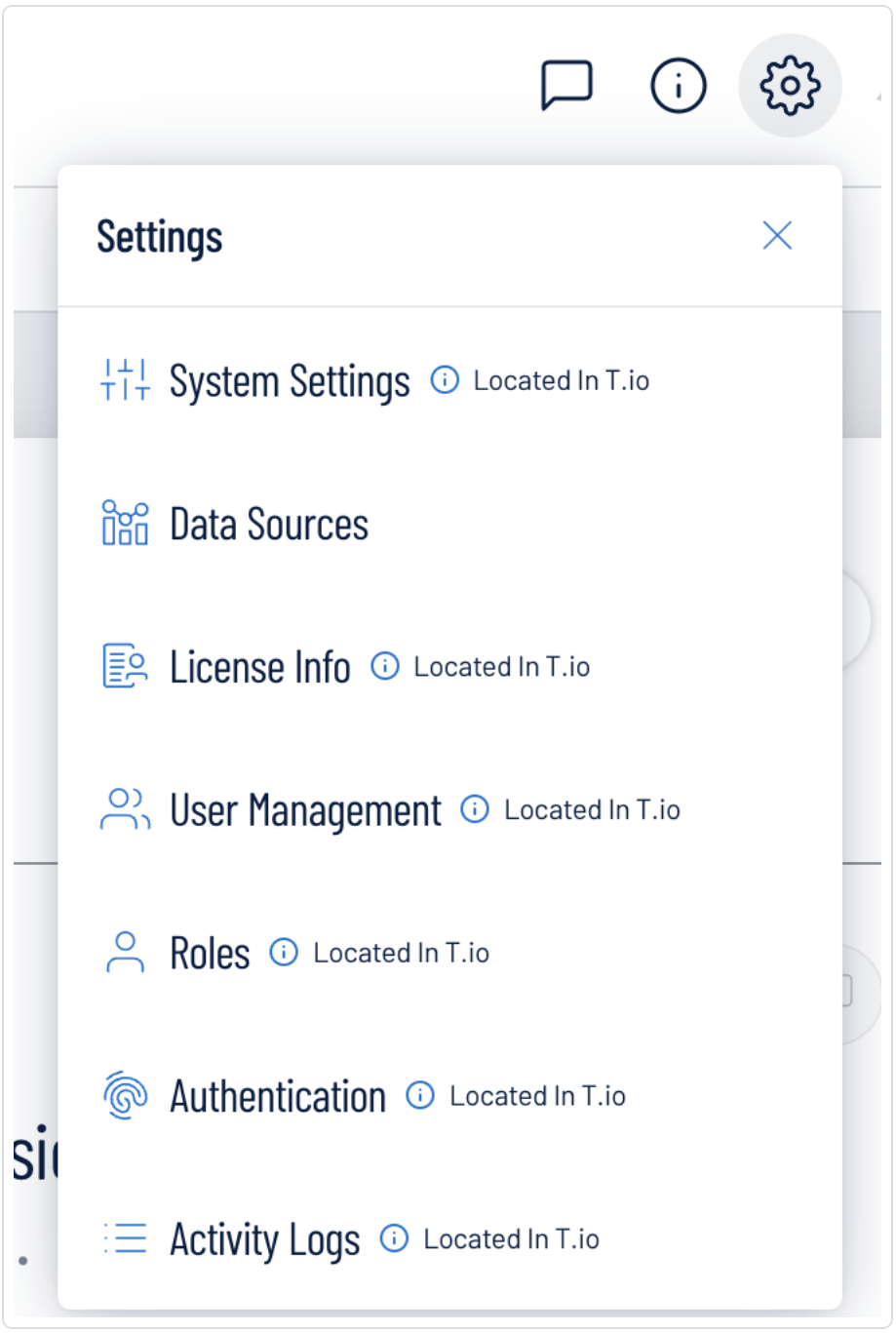
Access the Settings Menu

The **Settings** menu gives you access to user and settings options.

To access the **Settings** menu:

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

   The **Settings** menu appears.



2. Click one of the following options:

    - System Settings — View and manage settings for your container.
    - Data Sources — View all products feeding data into the Asset Inventory interface.
    - License Information — View your license information.

- User Management — View and manage all users, groups, and permissions.
- Roles — View and manage your Asset Inventory roles.
- Authentication — View and manage your user authentication settings.
- Activity Logs — View user activity logs.

System Settings

The **System Settings** option in the **Settings** menu directs you to the **Settings** page, where you can interact with all system settings options.

> **Note:** These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

To access the Settings page:

1. Access the **Settings** menu.
2. Click **System Settings**.

   The **Settings** page appears. For more information, see Settings within the *Tenable Vulnerability Management User Guide* .

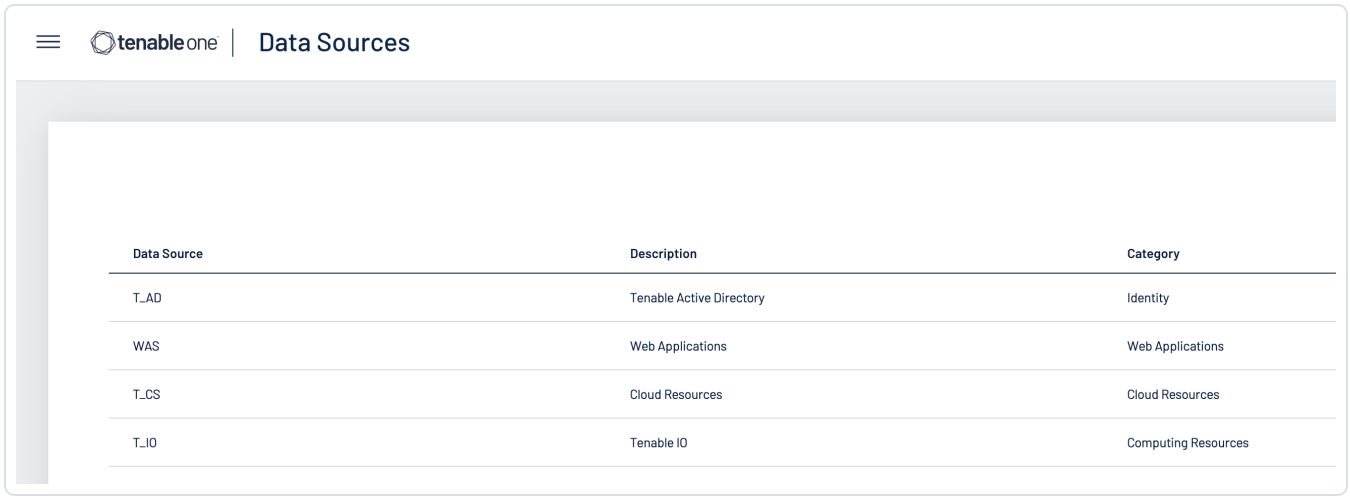
Data Sources

A data source is any product that feeds data into the Asset Inventory interface. By default, Asset Inventory automatically ingests data from any Tenable product for which you have a license. On the **Data Sources** tab, you can view details for each data source.

To view the **Data Sources** page:

1. Access the **Settings** menu.
2. Click **Data Sources**.

   The **Data Sources** page appears.



On the **Data Sources** page, you can view the following information:

Column	Description
Data Source	The product feeding data into the Asset Inventory interface.
Description	A description of the data source.
Category	The category to which the data source belongs. For more information, see Asset Inventory Metrics.

License Information

The **License Info** option in the **Settings** menu directs you to the **License** page, where you can view license information.

Note: These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

To access the License page:

1. Access the **Settings** menu.
2. Click **License Info**.

   The **License** page appears. For more information, see View License Information within the *Tenable Vulnerability Management User Guide* .

User Management

The **User Management** option in the **Settings** menu directs you to the **Users** page, where you can interact with all user management options.

> **Note:** These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

To access the Users page:

1. Access the **Settings** menu.
2. Click **User Management**.

   The **Users** page appears. For more information, see Users within the *Tenable Vulnerability Management User Guide* .

Roles

Roles allow you to manage privileges for major functions and control which Asset Inventory resources users can access.

Note: These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

When you create a user, you must select a role for that user that broadly determines the actions the user can perform. For more information, see Users.

Caution: If you don't have two-factor authentication configured, be sure to disable the **Two-Factor Required** toggle when creating a user. Failure to do so can cause the user interface to display incorrectly for the user.

Note: You can further refine user access to specific resources by assigning permissions to individual users or groups. For more information, see Permissions.

The Asset Inventory interface supports the following role types:

- Administrator — Has all permissions and privileges, is responsible for setting up the account, and knows the organization's architecture. They can create groups to organize different business units, and add and manage users on the account.
- Custom — Has custom applied privileges specific to organizational needs. For more information, see the following documentation in the *Tenable Vulnerability Management User Guide*:
    - Custom Roles
        - Create a Custom Role
        - Duplicate a Role
        - Edit a Custom Role
        - Delete a Custom Role
    - Export Roles

Authentication

The **Authentication** option in the **Settings** menu directs you to the **My Account** page, where you can interact with all authentication options.

> **Note:** These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

To access the My Account page:

1. Access the **Settings** menu.
2. Click **Authentication**.

   The **My Account** page appears. For more information, see My Account within the *Tenable Vulnerability Management User Guide* .

Activity Logs

The **Activity Logs** option in the **Settings** menu directs you to the **Activity Logs** page, where you can view activity log information.

> **Note:** These settings are managed directly within Tenable Vulnerability Management. When you access the this section, you are automatically redirected to the Tenable Vulnerability Management user interface.

To access the System Settings page:

1. Access the **Settings** menu.
2. Click **Activity Logs**.

   The **Activity Logs** page appears. For more information, see Activity Logs within the *Tenable Vulnerability Management User Guide* .