Tenable Inventory User Guide

Last Revised: June 25, 2024

Table of Contents

Welcome to Tenable 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
Legacy 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
Tenable Inventory	Tenable One Standard, Tenable One Enterprise
Tenable 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 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 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 Tenable Inventory to: Utilize Tenable 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. - View and manage weaknesses across all of your vulnerability findings.

For more information, see Get Started with Tenable Inventory.

Get Started with Tenable Inventory

Tenable recommends following these steps to get started with Tenable 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 Tenable Inventory key terms.
- Review the Tenable One Licensing *Quick-Reference Guide*.
- Familiarize yourself with the categories and data metrics within Tenable 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 Tenable Inventory:

Follow the Log in to Tenable Inventory steps.

Configure Tenable Inventory for Use

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

Assess Your Exposure

Review your CES and perform analysis:

- Access **Tenable Inventory**, where you can:
  - Create a comprehensive asset inventory and connect assets with each other to correlate associated cyber risks.
  - View gaps in your security coverage and helps you to validate and enforce a security state among your assets, risks, and more.
  - View and manage all of your Tenable assets, tag these assets with descriptive metadata, and navigate a list of all of the most critical weaknesses associated with each asset.

Key Terms

The following key terms apply to the Tenable 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.

Tenable Inventory Metrics

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

Data Timing

Data within Tenable Inventory refreshes on the following cadence:

- Asset Data — Asset information is updated every time the asset is seen as part of a scan.
- Tag Application — When a tag is first created, it can take several hours to assign the tag to the appropriate asset, depending on the number of assets and the tag's rules.
- Tag Reevaluation — Every 12 hours, Tenable Inventory automatically reevaluates tags to ensure they apply to newly discovered assets, and are removed from any inactive assets.

Cyber Exposure Score (CES)

Tenable 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: Tenable 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)

Tenable 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:** Tenable 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 Criticality Rating (ACR)

Tenable assigns an ACR to each asset on your network to represent the asset's relative criticality as an integer from 1 to 10. A higher ACR indicates higher criticality.

ACR Category	ACR Range
Critical	9 to 10
High	7 to 8
Medium	4 to 6
Low	1 to 3

Because Tenable Vulnerability Management calculates ACR values every 24 hours, you may need to wait up to 24 hours to view the ACR after scanning the asset on your network.

Tenable Inventory Categories

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

Additionally, Tenable Inventory uses specific icons to represent these within the user interface.

Category	Icon
Cloud Resources	

Note: Currently, Tenable One only supports the ingestion of Legacy Tenable Cloud Security data. For more information, contact your Tenable Representative.	
Web Applications	
Identity Exposure	
Computing Resources	

Tenable 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** (Legacy 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 Tenable Inventory

To log in to Tenable 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 Tenable Inventory tile.

   The Tenable Inventory interface appears.

Navigate Tenable Inventory

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

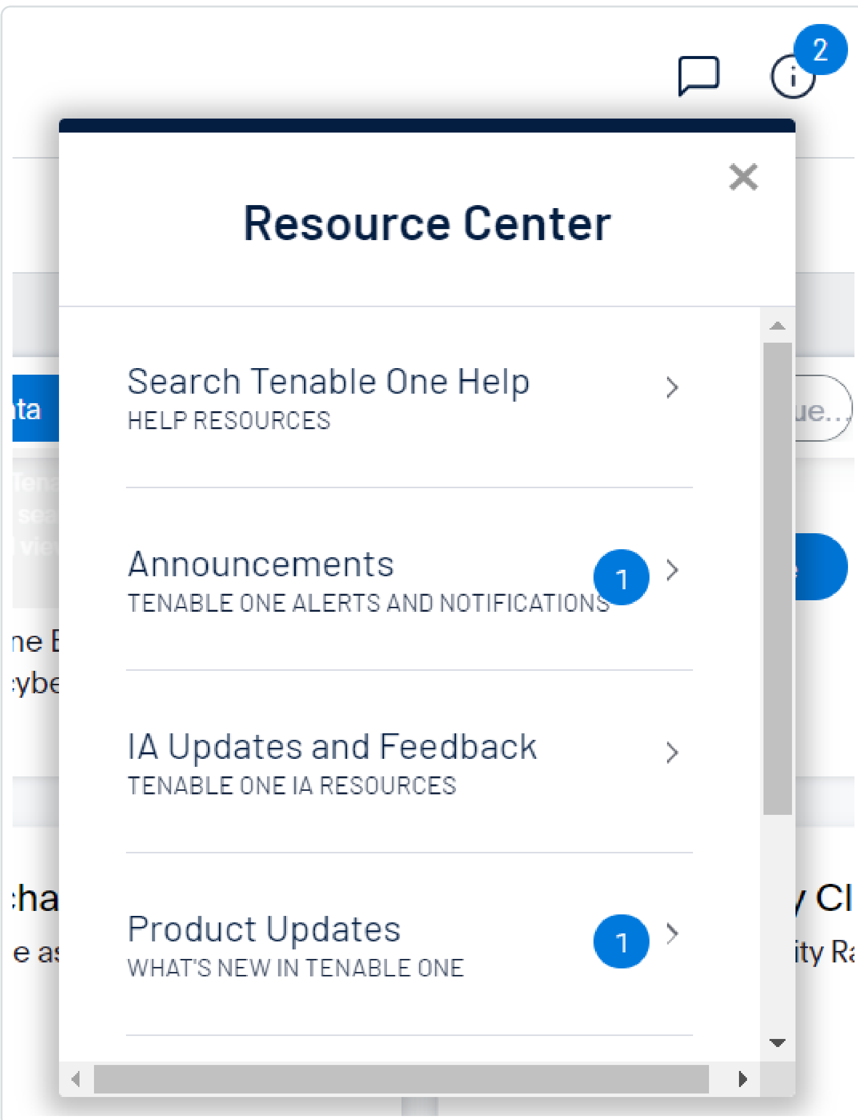
Resource Center

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.

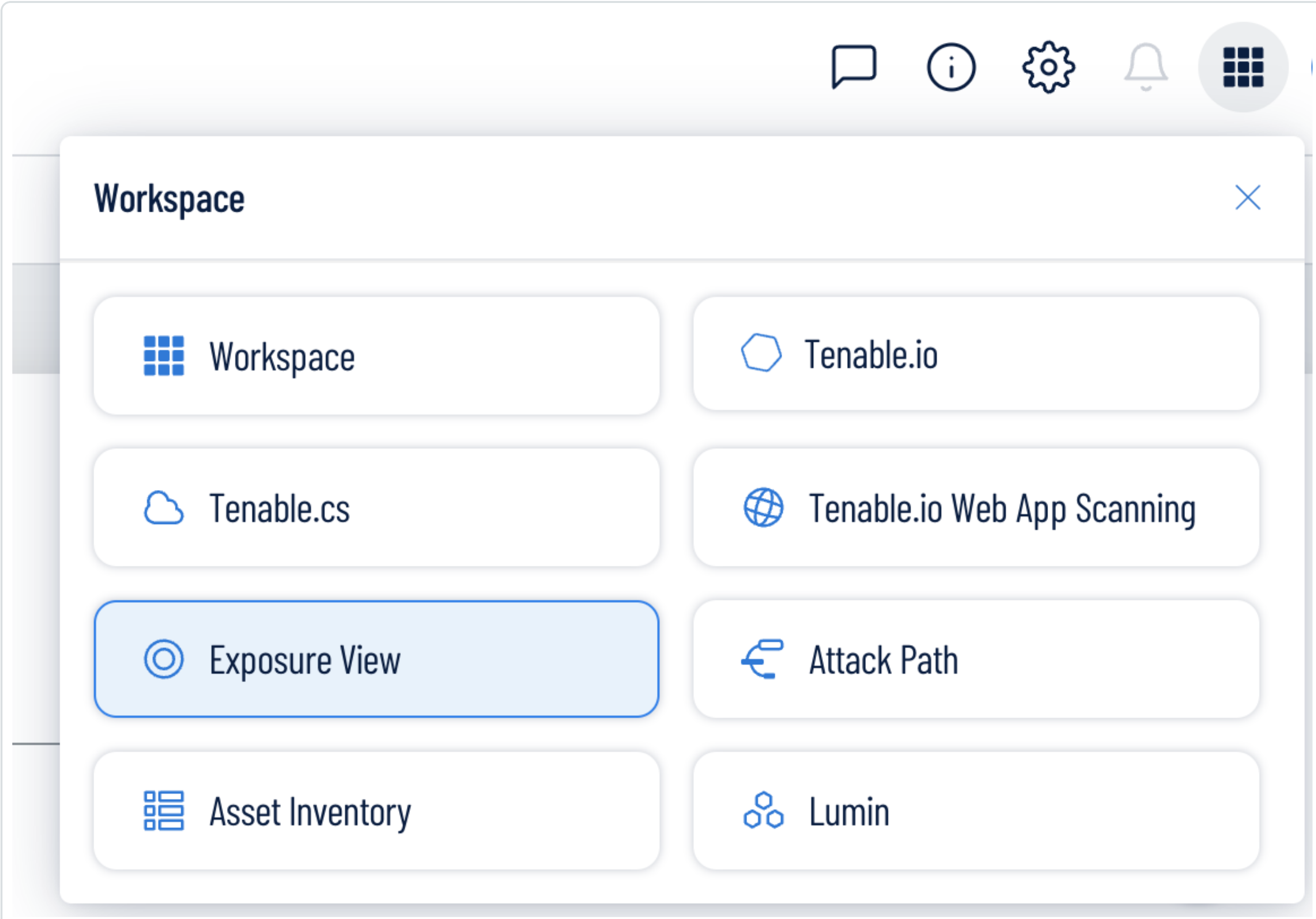
Important: Tenable disables application tiles for expired applications. Tenable removes expired application tiles from the **Workspace** page and menu 30 days after expiration.

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

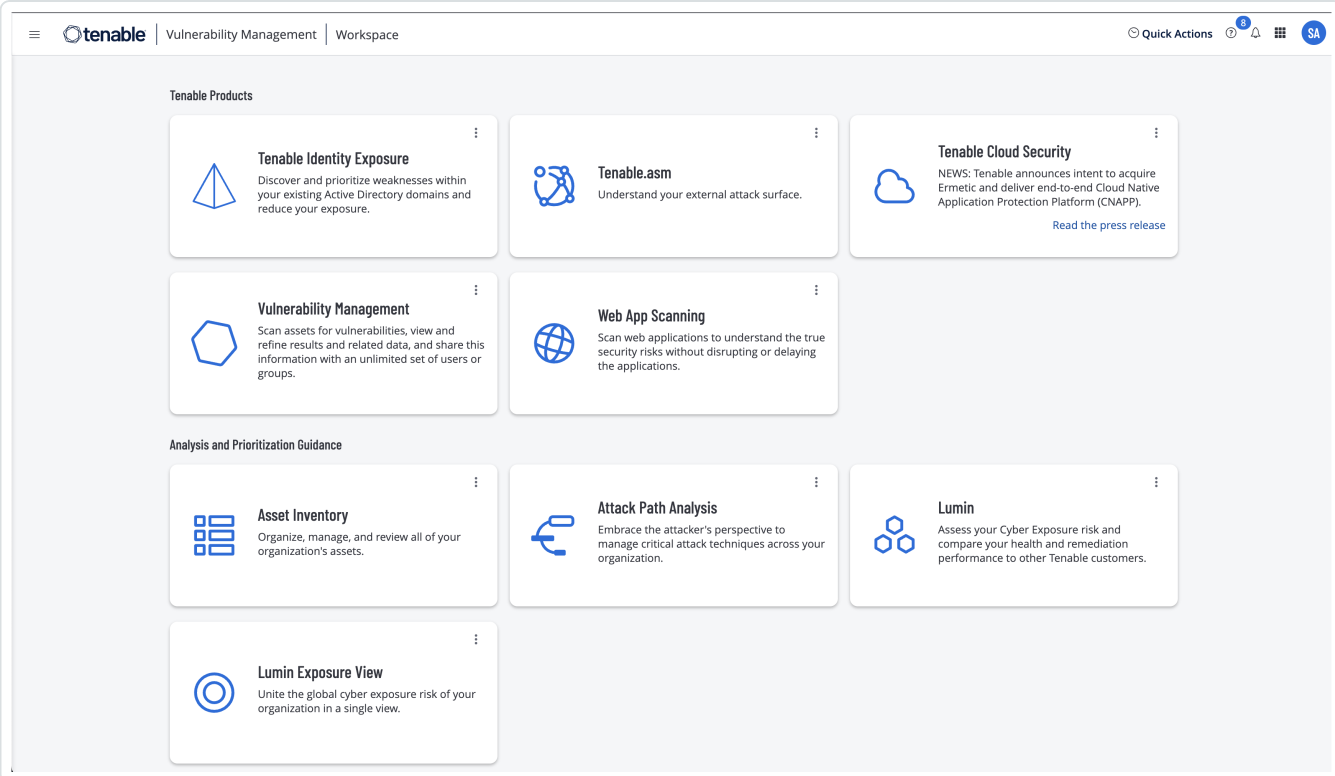
To view the Workspace page:

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.

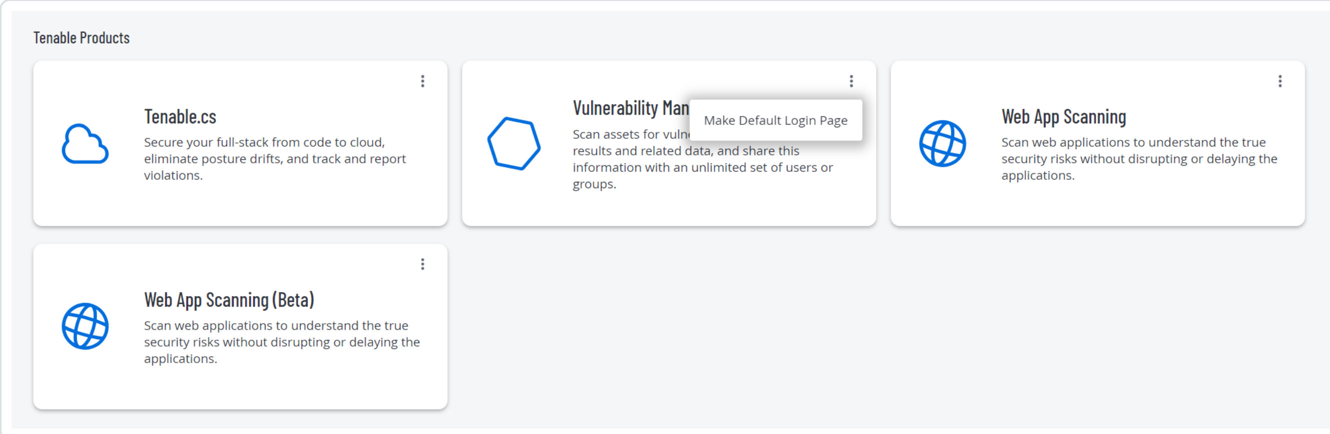
To set a default login application:

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**.

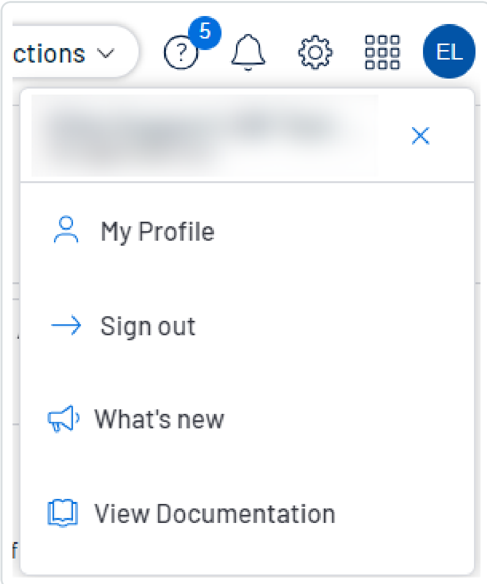
   The **Workspace** page now appears when you log in.

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 Tenable Inventory.
   - Click **What's new** to navigate directly to the Tenable Inventory Release Notes.
   - Click **View Documentation** to navigate directly to the Tenable Inventory User Guide documentation.

Log out of Tenable Inventory

To log out of Tenable Inventory:

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

Tenable Inventory

Tenable Inventory in Tenable One is an application that aggregates all assets and their associated entities to unify and operationalize the data. It focuses on your organization's ability to maintain an accurate inventory or all of your cyber-enabled technologies, while providing data analytics and a comprehensive inventory across various sources. While asset management highlights processes and people that can be affected, Tenable Inventory takes this one step further by digging into the technologies that can be hacked.

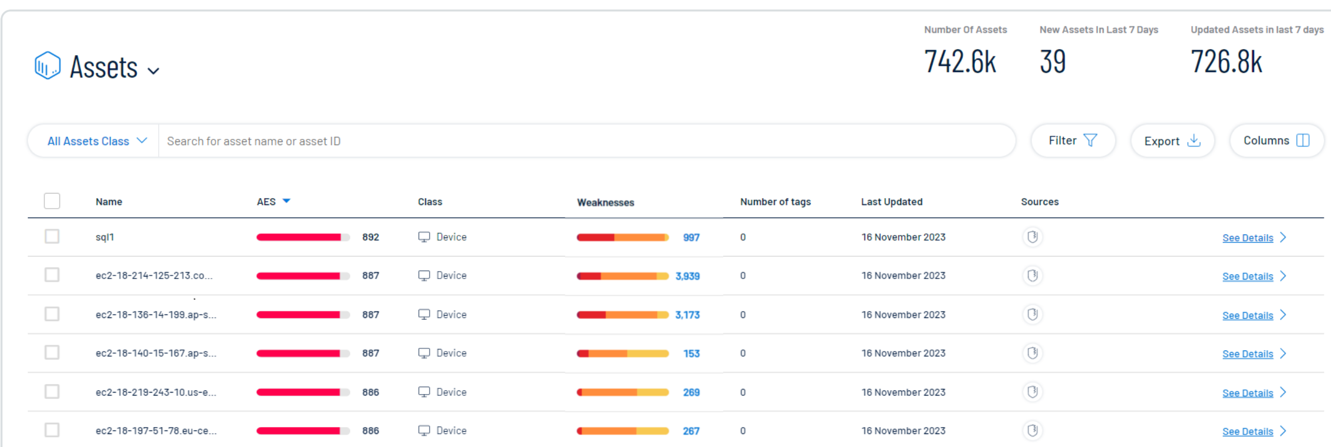
Tenable Inventory aids prioritization by highlighting the following asset data:

- Centralized location
- Asset class breakdown
- Filters
- Related weaknesses

To access the Inventory view:

1. [Log in](#) to Tenable Inventory.
2. At the top of the page, click the **Inventory** tab.

   The **Assets** view appears by default.



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

- View and interact with the data in the Assets view.
- View and interact with the data in the Tags view.
- View and interact with the data in the Weaknesses view.

Assets

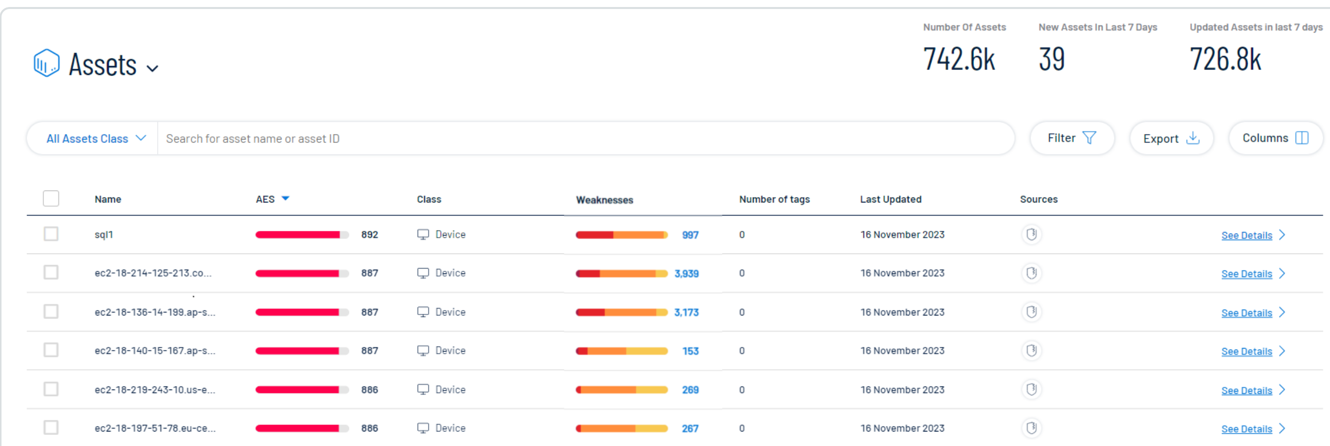
The **Assets** view allows you to view and manage all of your assets. You can quickly see which assets are new or updated, which class the asset belongs to, and other useful asset information.

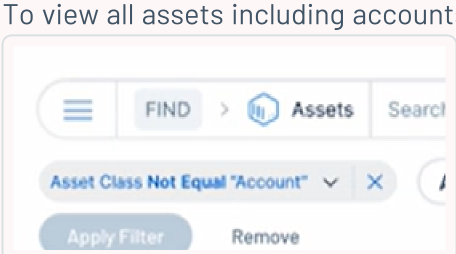
> **Important:** Because they do not include a hardware ID attribute, Microsoft Entra ID devices managed by Microsoft Intune's mobile device management (MDM) are not visible in the Tenable Inventory **Assets** view.

To access the **Assets** view:

1. Access the Tenable Inventory view.

   The **Assets** view appears by default.



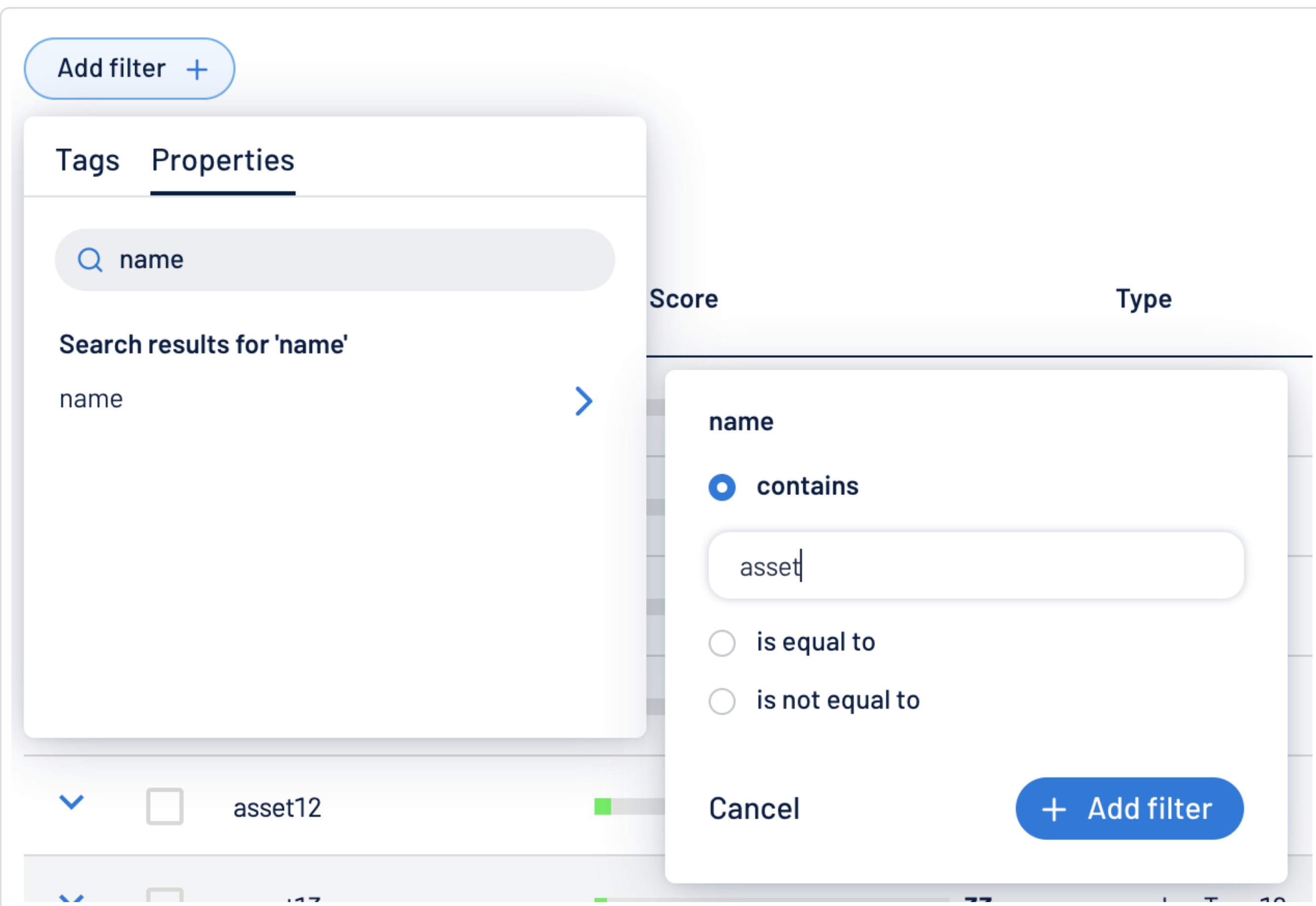
> **Important**: Because a **Person** can have more than one **Account**, Tenable Inventory automatically applies a default filter to hide account class assets from this view. This reduces confusion and avoids the appearance of duplicate assets in your asset list.
> To view all assets including accounts, remove the filter from the top of the list:
>
> 
>
>
> Additionally, when you search or filter the asset list, Tenable Inventory automatically removes the default

filter to ensure your search query results are accurate. For more information about asset classes, see Asset Classes.

In the **Assets** view, you can:

- View the total number of assets within your container.
- View the total number of new assets discovered within the last 7 days.
- View the total number of updated assets within your container in the last 7 days.
- In the class drop-down, filter the asset list by a specific asset class. For more information, see Asset Classes.

  The asset numbers at the top of the page and the asset list update accordingly.
- Use the search box above the asset list to search for a specific asset in the 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.

Tenable 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.

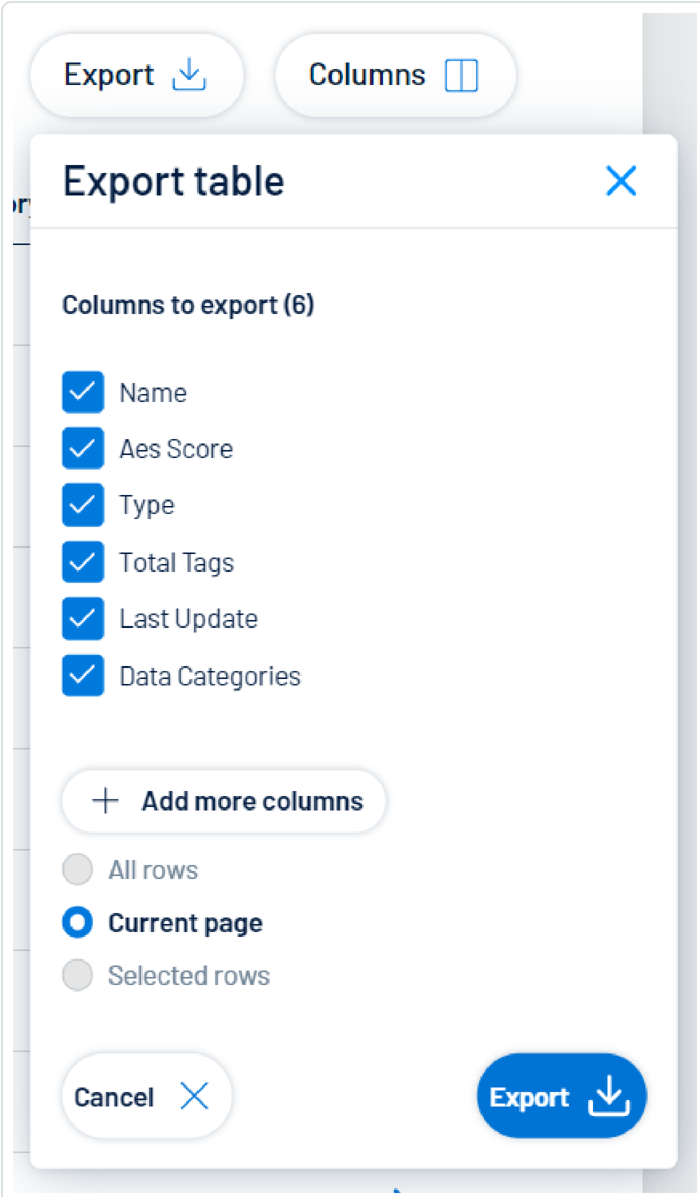
i. Click **Apply filters**.

Tenable 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** .

Tenable 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**.

Tenable Inventory saves your changes to the columns in the table.

- View a list of your assets, including the following information:
  - **Name** — The asset identifier. Tenable 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:** Tenable Inventory does not calculate an AES for unlicensed assets.
  - **Class** — The class type associated with the asset. For more information, see Asset Classes.
  - **Weaknesses** — The weaknesses associated with the asset. For more information, see Weaknesses.

    > **Tip:** Click on a Weakness count to navigate directly to the **Weaknesses** view.
  - **Number of tags** — The number of tags applied to the asset. For more information on tagging an asset, see Tag Assets via the Assets View.
  - **Last updated** — The date and time at which the asset was last updated.
  - **Sources** — The application the asset originated from, for example, Tenable Vulnerability Management.

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

Asset Classes

Classes are how Tenable Inventory groups assets. Because each asset has a different business purpose, classes allow you to easily separate asset data based on its type to get the most out of your analytics.

The asset class types used in Tenable Inventory are as follows:

Class	Description
All Assets	All assets from all sources, including third-party.
Account	The Identity login account for a software resource.
Container	Container image (e.g., Docker images).
Device	Computing devices with a network stack (i.e., IP address) that could, theoretically, be a target of a Nessus scan, including the following: • Traditional VM/Tenable Vulnerability Management hosts • Active Directory "computer" object classes • Cloud runtimes instances, such as EC2 instances • OT devices • ASM
Group	A grouping of persons or other groups.
Infrastructure As Code	Infrastructure as Code (e.g., Terraform, Cloud Formation).
Other Resource	General computing resources. This is a general class for all resources, including cloud runtime resources and non-host, non-identity AD assets.
Person	A person or service with accounts on a software resource.
Resource	An entity that an identity, Group, or Role has permissions to.

Role	Target for permissions that can be granted to persons and groups.
Web Application	Customer applications exposed on the internet .

View Asset Details

In the **Assets** view, you can view additional details for any asset in the assets list.

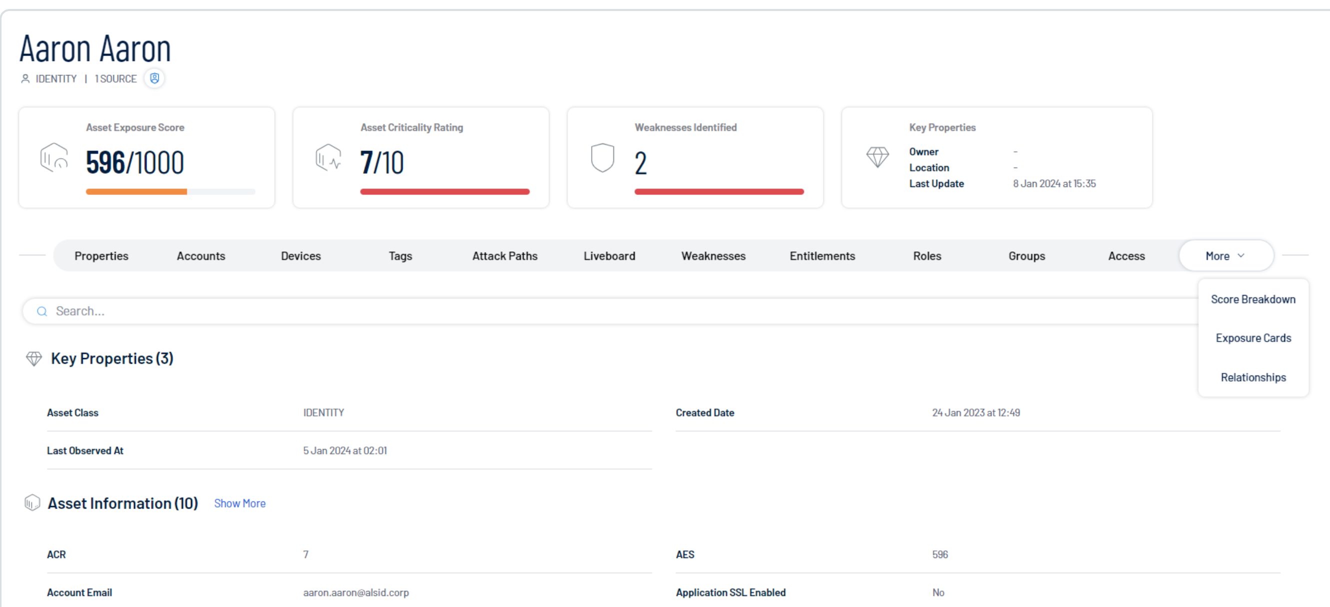
Note: Information on the asset details page varies depending on the class of the asset for which you're viewing details. For example, an **Identity** asset features different tabs and data than a **Device** asset.

Important: Because they do not include a hardware ID attribute, Microsoft Entra ID devices managed by Microsoft Intune's mobile device management (MDM) are not visible in the Tenable Inventory **Assets** view.

To view asset details:

1. Access the **Assets** view.
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:

Note: Some of the following items only appear for specific asset classes.

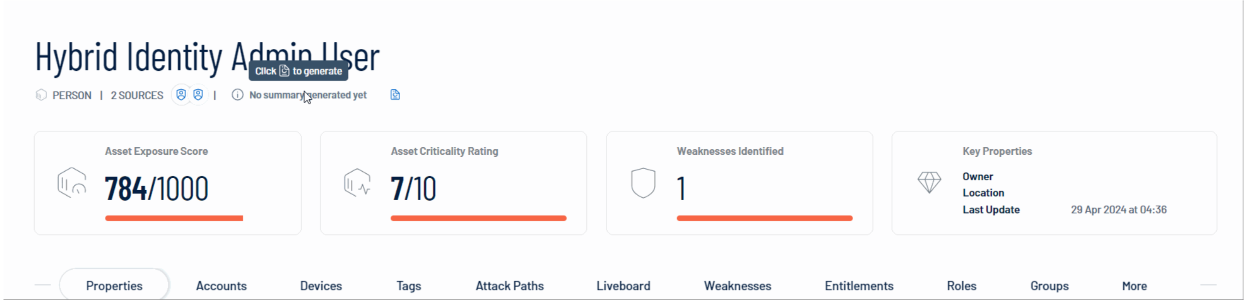
- View the **Asset Name**.
- View the asset class, for example, **Device**.
- View the asset source(s), for example, **T.CS**.
- **Generate and view an AI summary of the asset:**

  Tenable Inventory allows you to generate a summary of your asset using AI. Summaries are generated at the container level, and only apply to licensed assets within your container.

  > **Note:** Tenable Inventory limits the number of summaries you can generate to 100 per hour, with a maximum of 1000 summaries per day.

  Do one of the following:

  - To generate an AI summary for the asset for the first time, next to **No summary generated yet**, click the button.

    Tenable Inventory uses AI to generate a summary of the asset including general details and specifics about the asset's weaknesses.

  - To regenerate an existing AI summary for the asset, click **Show Summary** and, at the bottom of the summary panel, click the button.

    Tenable Inventory regenerates the AI summary for the asset.

  > **Tip:** Click the button to copy the summary directly to your clipboard. You can also rate the helpfulness of the summary by clicking or to help improve the quality of AI-generated content within Tenable Inventory in the future.

- View the **Asset Exposure Score** for the asset.

> **Note:** Tenable Inventory does not calculate an AES for unlicensed assets. For more information, see Tenable Inventory Metrics.

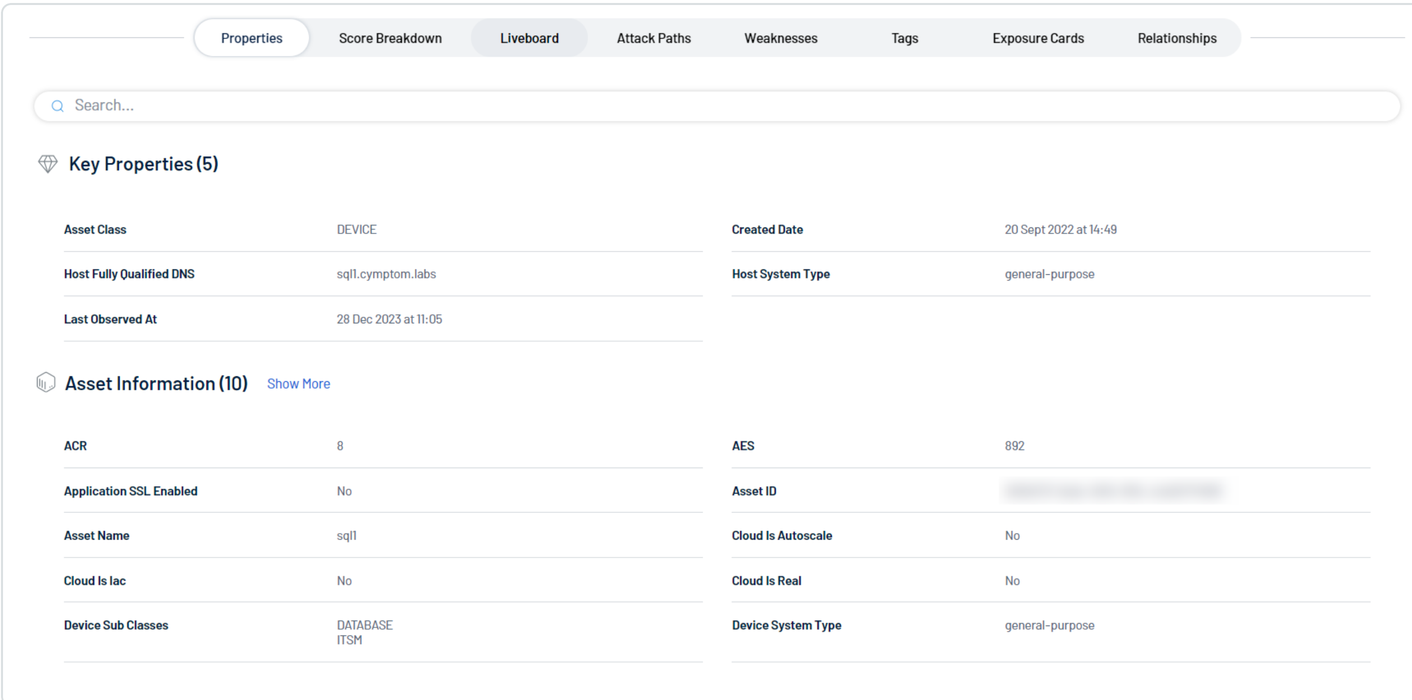
- View the **Asset Criticality Rating** for the asset.
- View the number of **Weaknesses Identified** on the asset. For more information, see Weaknesses.
- View high-level **Key Properties**, including:
  - **Asset Class** — The asset class associated with the asset, for example, **Device**.
  - **Owner** — The owner of the asset.
  - **Drivers** — The key drivers of (that is, plugins that have the biggest effect on) the asset.
  - **Location** — The physical location of the asset.
  - **Last Observed At** — The date and time at which a scan most recently identified the asset.

When viewing the asset details page, you can click on the following tabs to view additional asset information:

> **Tip:** Each tab includes a search box, where you can search for specific items.

Properties

The **Properties** section highlights details about the asset's properties.



Here, you can view asset details including:

Note: The properties listed in the user interface depend on the asset for which you are viewing details.

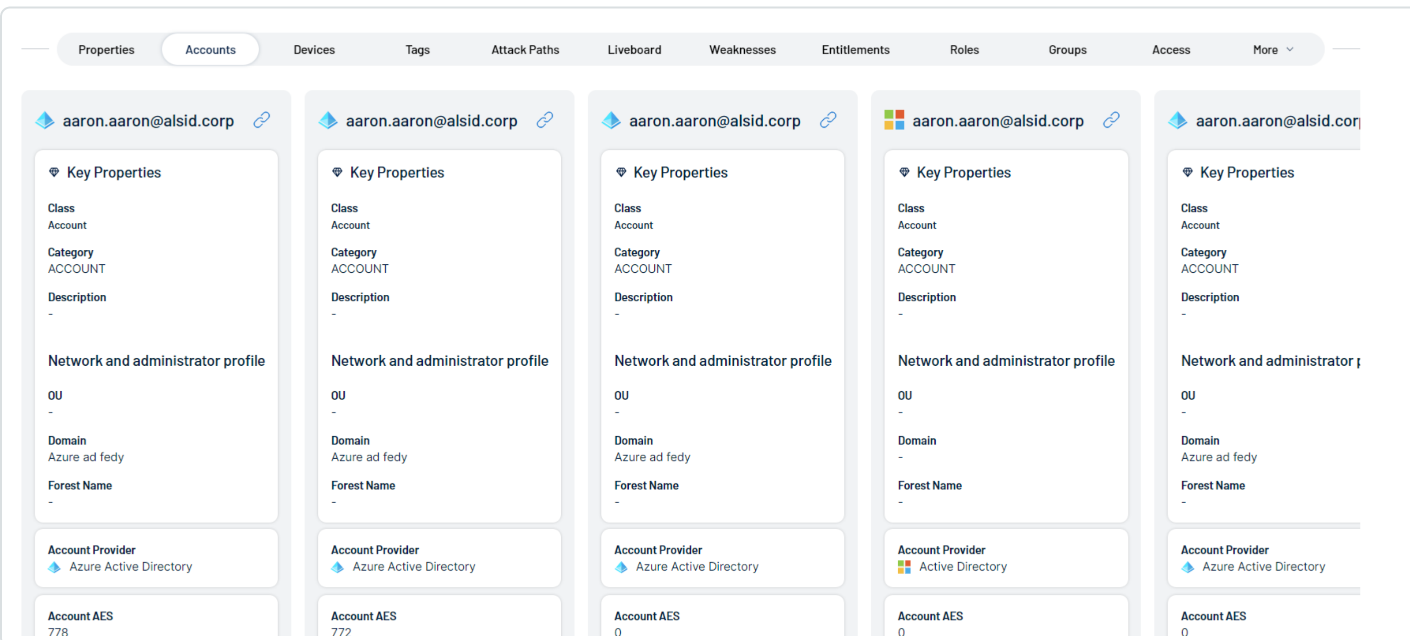
Key Properties	
Item	**Description**
Asset Class	The asset class associated with the asset, for example, **Device**.
Created Date	The date and time at which the asset source first created the asset record.
Host Fully Qualified DNS	The Host Fully Qualified Domain Names, or FQDNs, of the asset host.
Host System Type	The type associated with the asset's host system, for example, **general-purpose**.
Last Observed At	The date and time at which a scan most recently identified the asset.
Asset Information	

Item	Description
ACR	The Asset Criticality Rating associated with the asset. For more information, see Tenable Inventory Metrics.
AES	The Asset Exposure Score associated with the asset. For more information, see Tenable Inventory Metrics.
Application SSL Enabled	Indicates whether or not Application SSL is enabled on the asset.
Asset ID	The asset's UUID.
Asset Name	The asset identifier; assigned based on the presence of certain attributes in the following logical order: 1. Nessus Agent name 2. Hostname 3. WebApp hostname 4. Container Security Image name 5. Container Runtime hostname 6. Cloud Common Resource name 7. Cloud Common Resource identifier 8. Cloud Runtime name 9. Cloud IAC name 10. Active Directory Asset name 11. Domain Record hostname If none of the above attributes are present, then **FQDN** is selected as the name for the asset.
Cloud is Autoscale	Indicates whether or not the asset is part of a cluster that can automatically scale its size.

Cloud is Iac	Indicates whether or not the asset is Infrastructure as Code (IaC).
Cloud is Real	Indicates whether or not the asset is actively running in the cloud.
Device Sub Classes	Where applicable, the subclass associated with the asset device.
Device System Type	Where applicable, the system type associated with the asset device.

Accounts

The **Accounts** section shows a list of tiles with information about accounts associated with the asset.



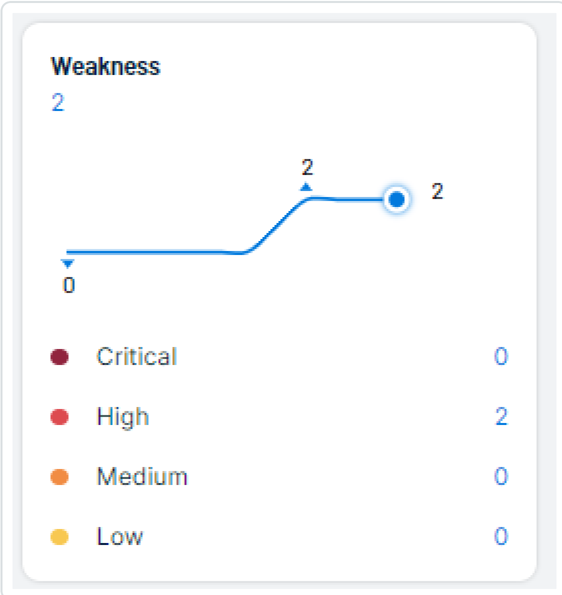
Tip: At the bottom of the page, use the horizontal scroll bar to view all listed accounts.

Each tile includes the following information:

- **Key Properties**:

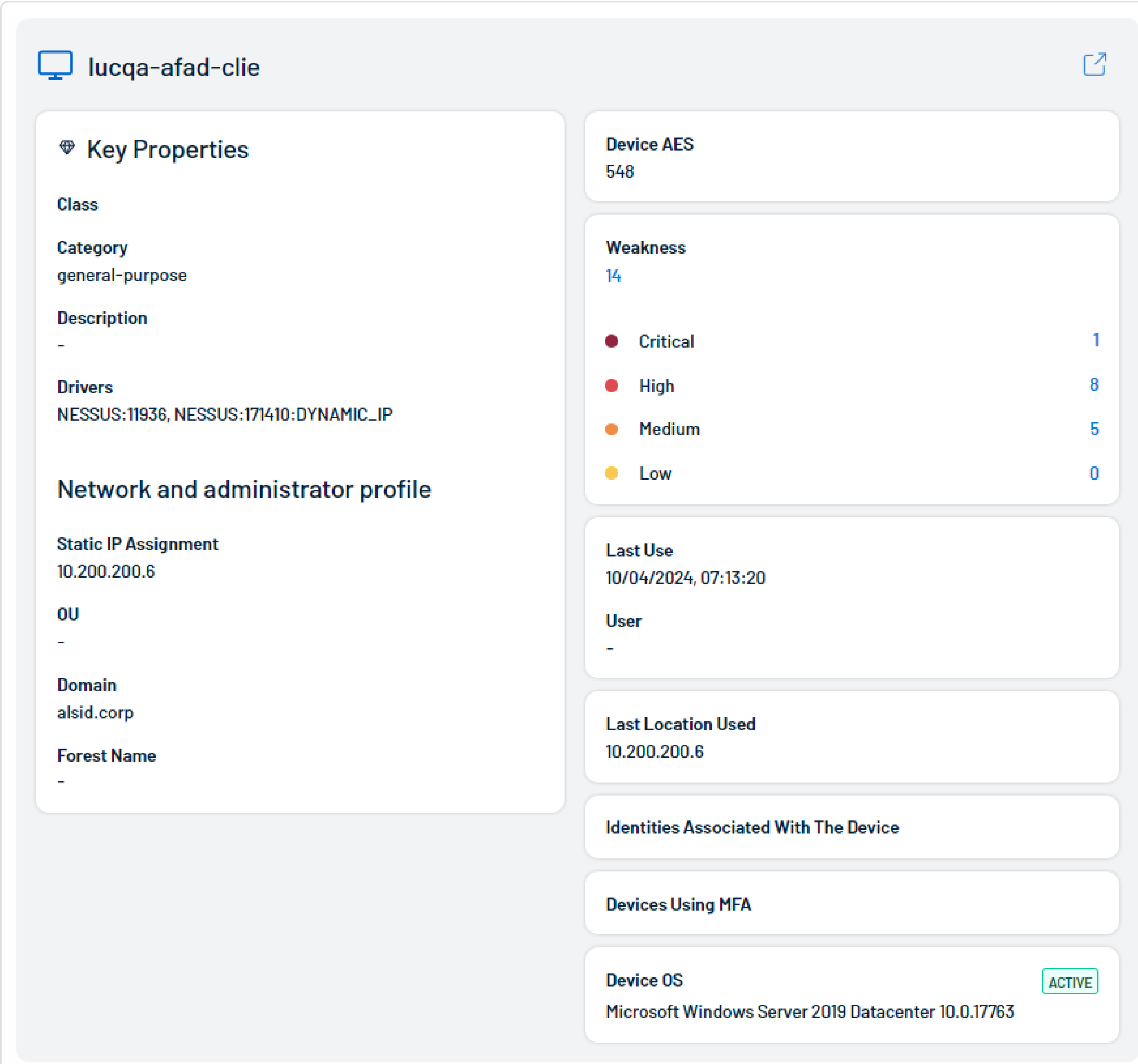
- Class — The asset class associated with the asset, for example, **Account**.
- **Category** — The category associated with the asset, for example, **ACCOUNT**.
- **Description** — Where available, a description of the account.

- **Network and Administrator Profile**:
  - **OU** — The Organizational Unit (OU) associated with the account.
  - **Domain** — The domain associated with the account. For more information, see Domains in the *Tenable Identity Exposure User Guide*
  - **Forest Name** — The forest name associated with the account. For more information, see Forests in the *Tenable Identity Exposure User Guide*.
- **Account Provider** — The provider of the account, for example, **Azure Active Directory**.
- **Account AES** — The overall Asset Exposure Score associated with the account.
- **Last Use** — The date on which the account was most recently accessed by a user.
- **Last Location Used** — The physical location of where the account was most recently used.
- **Account Activity** — The activity status of the account, for example, **Active**.
- **Weakness** — A graphical representation of weaknesses on the account. This section includes a line graph and an individual count of each weakness and its criticality. For more information, see Weaknesses.



Devices

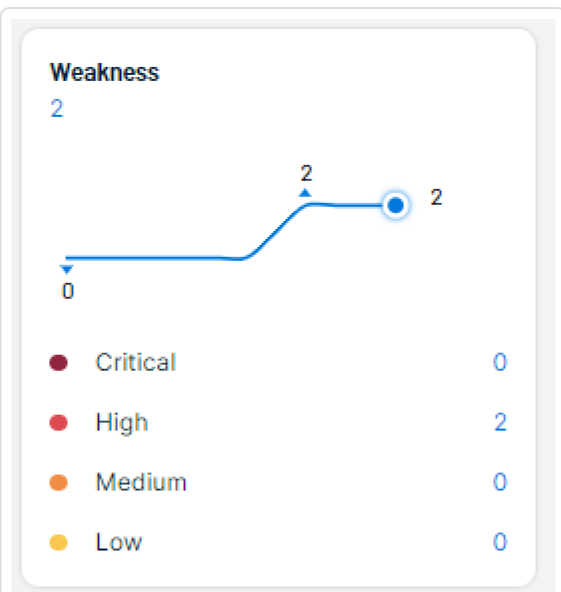
The **Devices** section shows all devices associated with the asset. Each device and its relevant information is listed as a tile on the page.



On each tile, you can view the following device information:

- **Key Properties**:
  - **Class** — The asset class associated with the device.
  - **Category** — The category associated with the device, for example, **general-purpose**.

- Description — Where available, a description of the device.
    - **Drivers** — A list of drivers installed on the device.
- **Network and Administrator Profile**:
    - **Static IP Assignment** — The static IP address associated with the device.
    - **OU** — The Organizational Unit (OU) associated with the device.
    - **Domain** — The domain associated with the device. For more information, see Domains in the *Tenable Identity Exposure User Guide*
    - **Forest Name** — The forest name associated with the device. For more information, see Forests in the *Tenable Identity Exposure User Guide*.
- **Device AES** — The overall Asset Exposure Score associated with the device.
- **Weakness** — A graphical representation of weaknesses on the device. This section includes a line graph and an individual count of each weakness and its criticality. For more information, see Weaknesses.



- **Last Use** — The date on which the device was most recently accessed by a user.
- **Last User** — The last user account to access the device.
- **Last Location Used** — The physical location of where the account was most recently used.

- **Identities associated with the Device** — Where applicable, any Active Directory or Microsoft Entra ID Identities associated with the device.

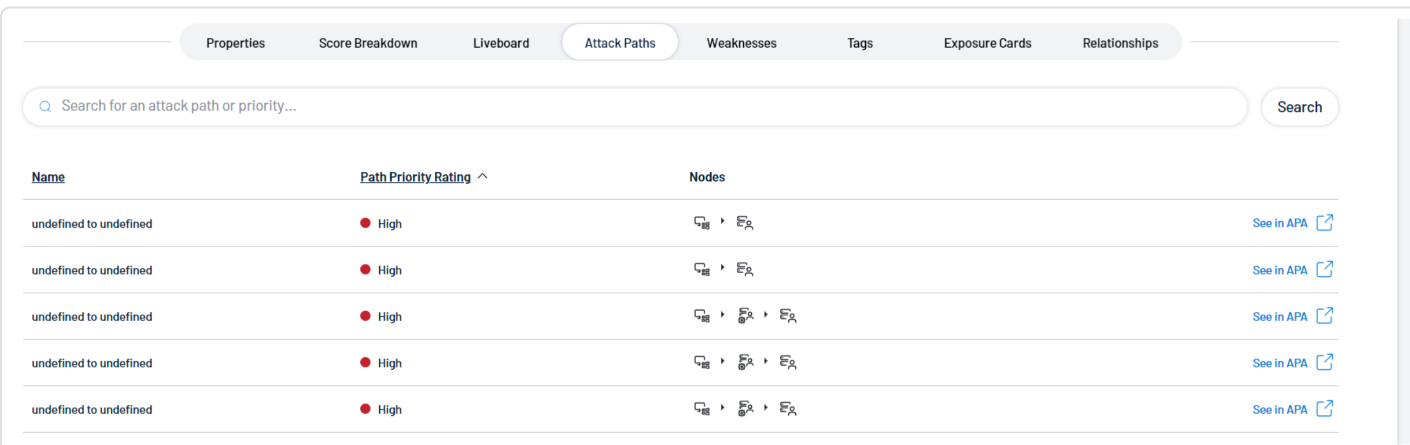
- **Devices Using MFA** — Indicates if the device requires multi-factor authentication (MFA) for user login.

- **Device OS** — The operating system (OS) running on the device. In the upper-right corner of the box, view a color-coded status of the OS, for example, **Active**.

Attack Paths

The **Attack Paths** section shows a table list of the top attack paths in which the asset is present.

> **Tip:** As part of a typical attack, adversaries leverage different tools and techniques to accomplish their objectives. This event is known as Attack Path. An attack path contains one or more Attack Techniques, allowing the hacker to accomplish their objective. To see a full list of supported attack paths within Attack Path Analysis, view the [Tenable Attack Path Techniques]() list.



The attack paths list includes the following information:

- **Name** — The name of the attack path.

- **Path Priority Rating** — The priority of an attack path. Attack Path Analysis calculates the PPR based on the relative number of attack paths to critical assets. Attack Path Analysis categorizes priority levels as **Low**, **Medium**, **High**, and **Critical**.

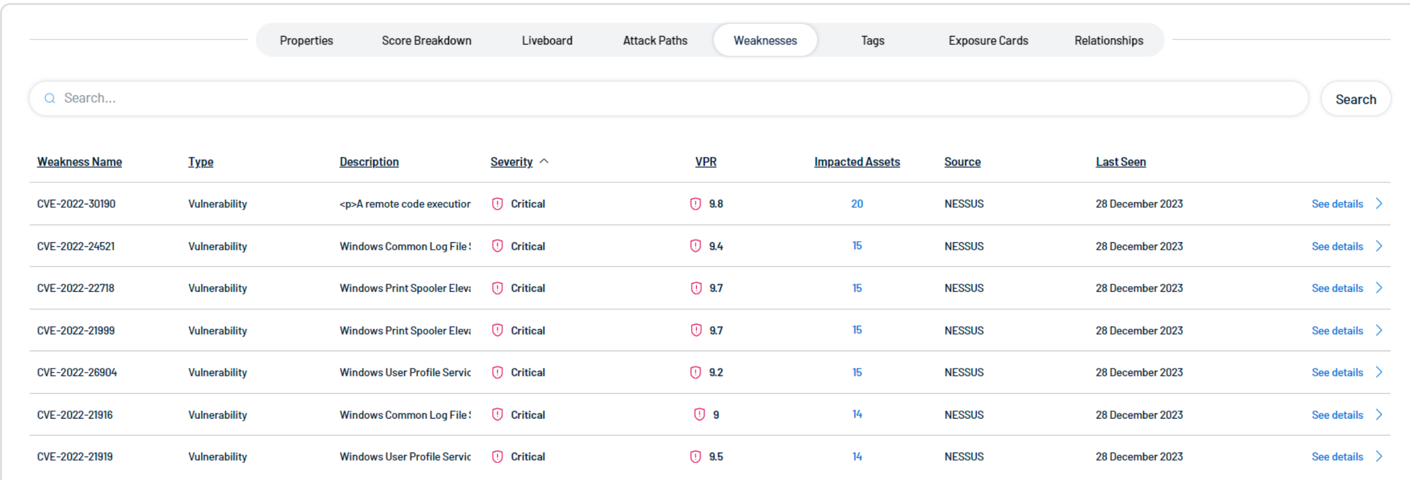
- **Nodes** — A visual representation of the nodes involved in the attack path that indicates the node type and the order in which the nodes might be accessed.

- **See in APA** — Click **See in APA** in the row of any attack path to navigate directly to Attack Path Analysis with the selected attack path displayed by default.

Weaknesses

The **Weaknesses** section shows a table list of all weaknesses associated with the asset.

> **Tip:** For more information, see [**Weaknesses**](#).



The weaknesses table includes the following information:

- **Weakness Name** — The Common Vulnerability Exposure (CVE) ID associated with the weakness.
- **Type** — The type of weaknesses: **Misconfiguration** or **Vulnerability**.
- **Description** — A brief description of the weakness.
- **Severity** — The severity of the weakness, for example, **Critical**.

  > **Note:** At this time, Tenable Inventory does not include information for Info level severity weaknesses.

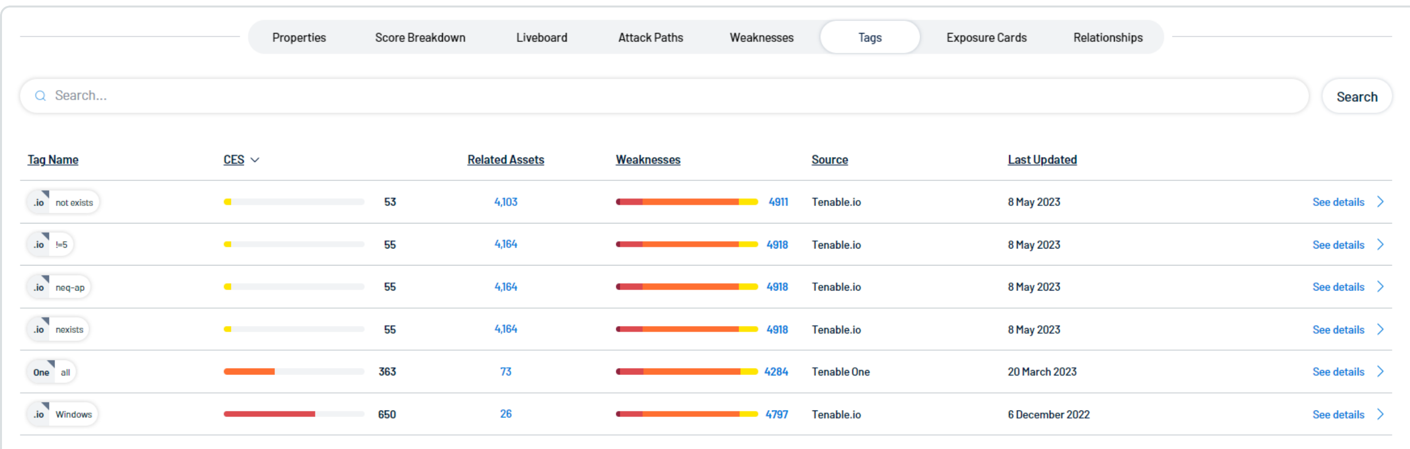
- **VPR** — The [Vulnerability Priority Rating](#) (VPR) of the weakness.
- **Impacted Assets** — The number of assets impacted by the weakness. For more information, see [Assets](#).

- **Source** — The application the weakness' asset originated from, for example, Tenable Vulnerability Management.
- **Last seen** — The date at which the weakness was last seen in a scan on the asset.
- Click **See details** to view more details about a weakness. For more information, see [View Weakness Details]().

Tags

The **Tags** section shows a table list of all tags applied to the asset.

> **Tip:** For more information, see [**Tags**]().



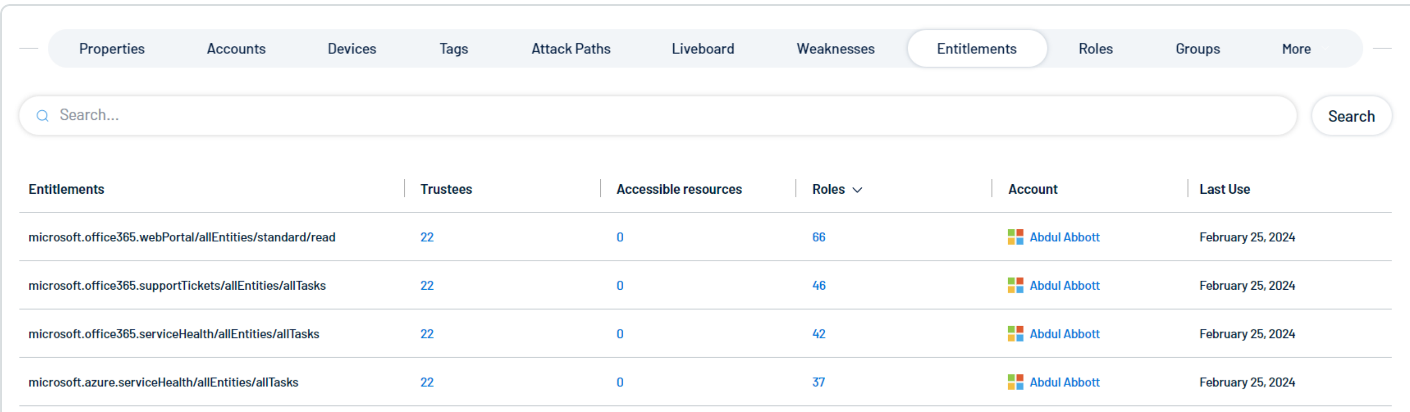
- **Tag name** — The name of the tag value or tag category.
- **CES** — The [Cyber Exposure Score]() for the tag value or tag category. The CES represents Cyber Exposure risk as an integer between 0 and 1000, based on the Asset Exposure Score (AES) values for the assets to which the tag is applied. Higher CES values indicate higher risk.
- **Related Assets** — The number of assets to which the tag is applied.
- **Weaknesses** — The weaknesses associated with the asset. For more information, see [Weaknesses]().
- **Source** — The application the tag originated from, for example, Tenable Vulnerability Management.
- **Last updated** — The date on which a user last updated the tag.

- Click **See details** to view more details about a tag. For more information, see [View Tag Details](#).

Entitlements

The **Entitlements** section shows entitlement information for assets who have roles, either:

- [Assigned in Microsoft Entra ID](#)
- Enabled by [Tenable cloud scanning](#) the Active Directory and [adding the appropriate domain](#).



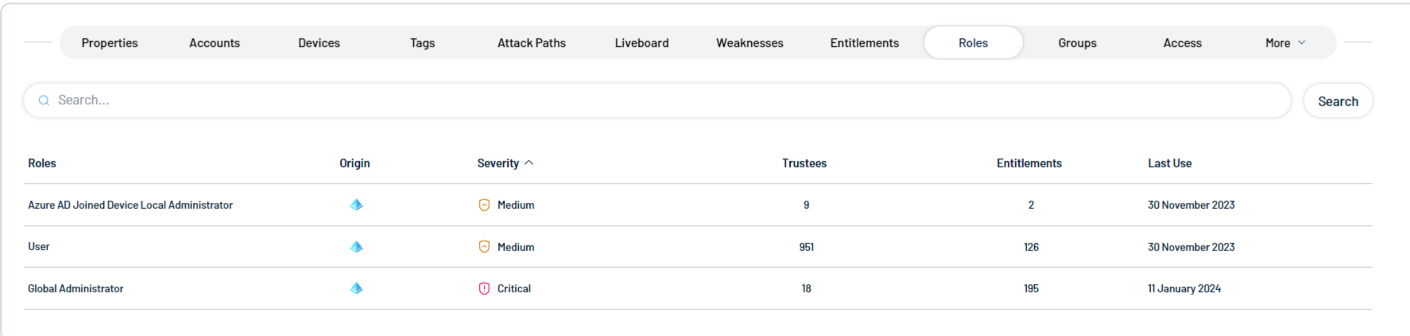
The entitlements section includes the following information:

- **Entitlements** — The name of the asset entitlement.
- **Trustees** — The number of trustees associated with the asset entitlement. Click the number to navigate directly to the [Assets](#) page filtered by all assets to which these trustees have entitlements.
- **Accessible Resources** — The number of accessible resources associated with the asset entitlement. Click the number to navigate directly to the [Access](#) tab for the asset.
- **Roles** — The number of accessible resources associated with the asset entitlement. Click the number to navigate directly to the [Roles](#) tab for the asset.
- **Account** — The name and type of the account asset associated with the entitlement. Click the name to navigate directly to [View Asset Details](#) for that specific asset.
- **Last Use** — The date on which the entitlement was last used by the asset.

Roles

The **Roles** section shows all roles assigned to the asset. For example, if this identity has roles assigned in Microsoft Entra ID, their details appear here.

> **Tip:** For more information, see [Assign Microsoft Entra roles to Users](#).



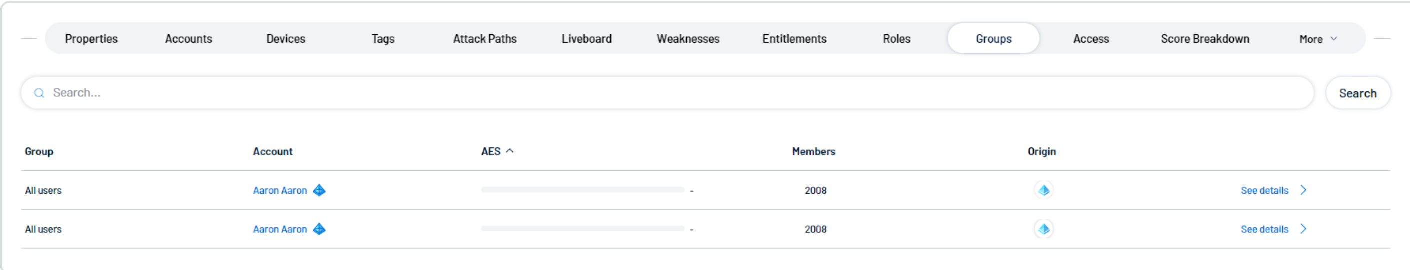
The roles list includes the following information:

- **Roles** — The name of the role assigned to the asset.
- **Origin** — An icon that indicates the origin provider of the account (for example, Azure AD).
- **Severity** — The overall severity of the asset, for example, **Critical**.
- **Trustees** — The number of trustees associated with the asset role.
- **Entitlements** — The number of entitlements to which the role has access.
- **Last Use** — The date on which the role was most recently used on the asset.

Groups

The **Groups** section shows a list of groups to which the asset belongs. For example, if this asset is a member of groups in Microsoft Entra ID or Azure Active Directory, they appear here.

> **Tip:** For more information, see:
>
> - [Assign Identities to Groups in Microsoft Entra](#)
> - [Active Directory Security Groups](#)



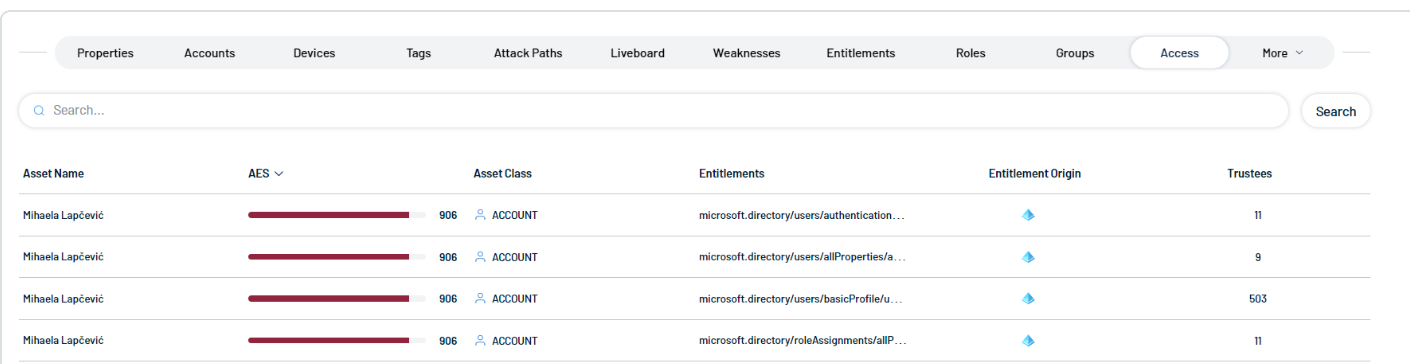
The groups list includes the following information:

- **Group** — The name of the group to which the asset belongs.
- **Account** — The name of the account on the asset that belongs to the group.
- **AES** — The overall Asset Exposure Score associated with the account.
- **Members** — The total number of assets that belong to the group.
- **Origin** — An icon that indicates the origin provider of the group (for example, Azure AD).
- Click **See details** to navigate directly to the asset details page for the selected group.

Access

The **Access** section shows access information for assets who have roles, either:

- Assigned in Microsoft Entra ID
- Enabled by Tenable cloud scanning the Active Directory and adding the appropriate domain.



The access list includes the following information:

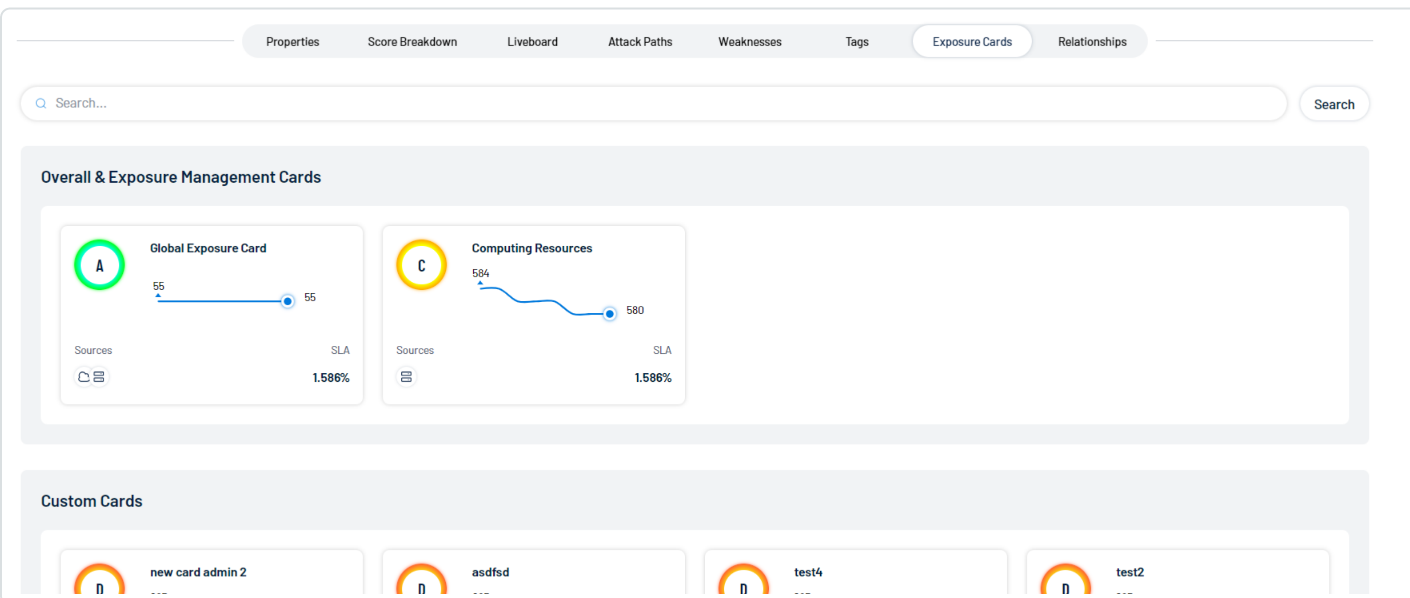
- **Asset Name** — The asset identifier of the asset.
- **AES** — The overall Asset Exposure Score of the asset.

- **Asset Class** — The asset class associated with the asset, for example, **Account**.
- **Entitlements** — The directory path to which the asset has entitlement access.
- **Entitlement Origin** — An icon that indicates the origin provider of the entitlement (for example, Azure AD).
- **Trustees** — The number of trustees associated with the asset.

Exposure Cards

The **Exposure Cards** section shows all Lumin Exposure View exposure cards associated with the asset. Assets can be part of global exposure cards, or custom cards created by users in Lumin Exposure View.

Tip: 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.



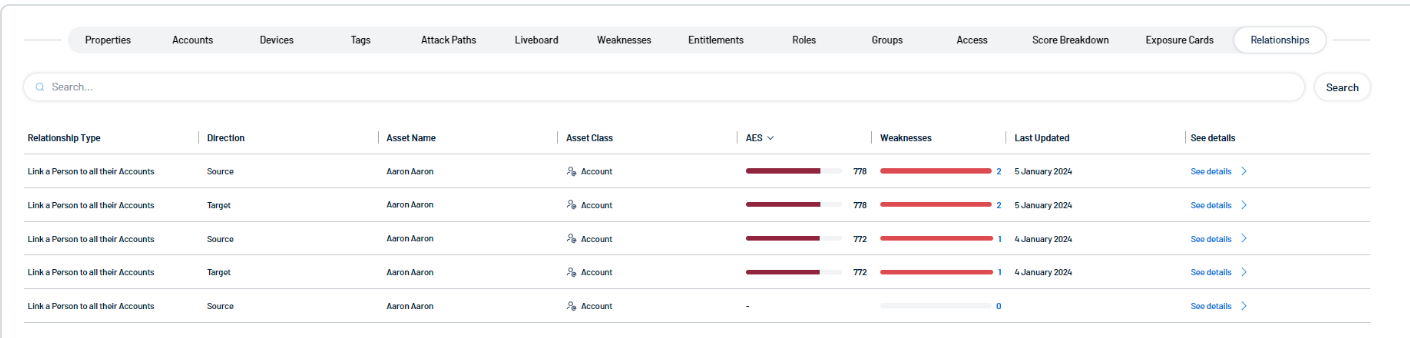
Click on any card to navigate directly to Lumin Exposure View with the selected card data displayed by default.

For more information on exposure cards and how to create them, see the following resources:

- [View the Exposure Cards Library](#) in the *Lumin Exposure View User Guide*
- [Create a Custom Exposure Card](#) in the *Lumin Exposure View User Guide*

Relationships

The **Relationships** section shows a list of all assets with a known relationship to the current asset for which you are viewing details.

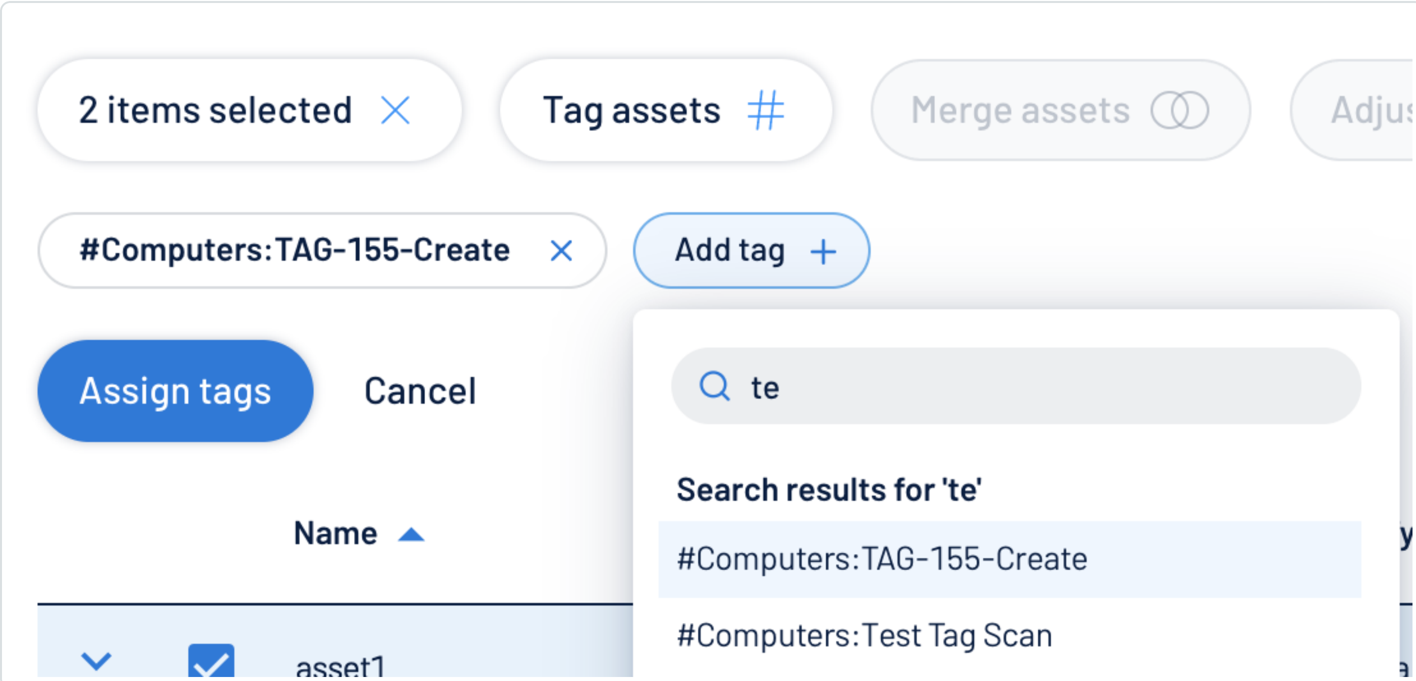


The relationships list includes the following information:

- **Relationship Type** — The type of relationship between the two assets.
- **Direction** — Indicates whether the related asset is the **Source** or the **Target** of the asset relationship.
- **Asset Name** — The asset identifier of the related asset.
- **Asset Class** — The [asset class](#) associated with the asset, for example, **Account**.
- **AES** — The overall [Asset Exposure Score](#) of the related asset.
- **Weaknesses** — The weaknesses associated with the asset. For more information, see [Weaknesses](#).
- **Last Updated** — The date at which a scan most recently identified the asset.
- Click **See details** to navigate directly to the asset details page for the selected asset relationship.

Tag Assets via the Assets View

In the **[Assets](#)** view, you can apply tags directly to an asset in the asset list.



To apply a tag to an asset:

1. Access the **Assets** view.
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**.

   Tenable Inventory assigns the designated tags to the asset or assets.

Tags

In Tenable 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 **Tags** view 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.

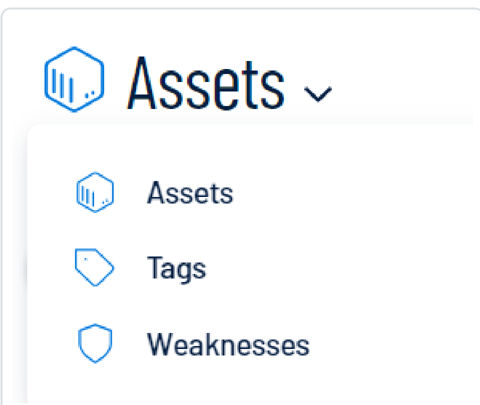
To access the **Tags** view:

1. Access the Tenable Inventory view.

   The **Assets** view appears by default.

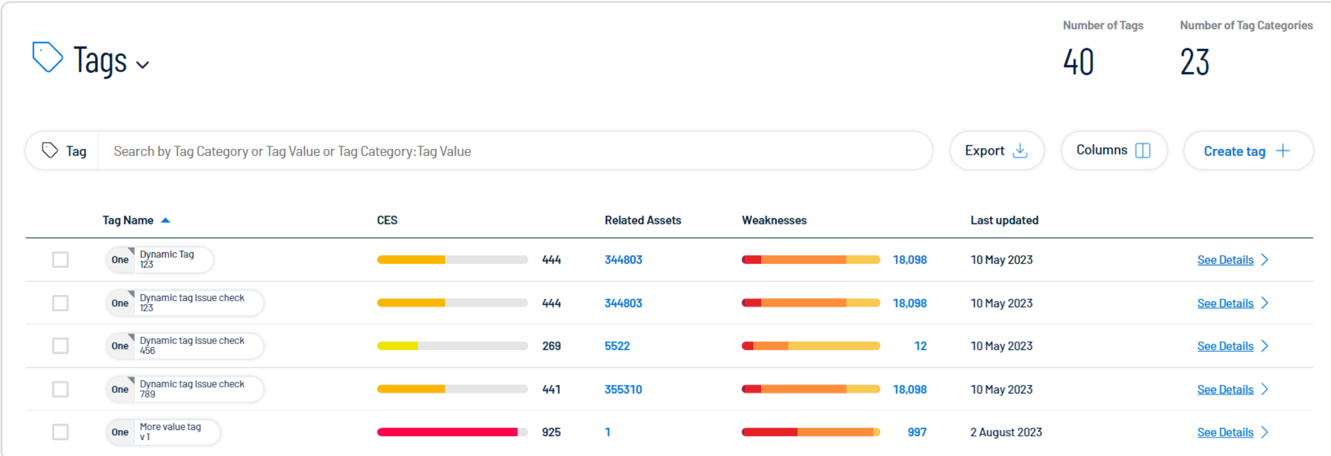
2. Click the **Assets** drop-down.

   A menu appears.

3. Click **Tags**.

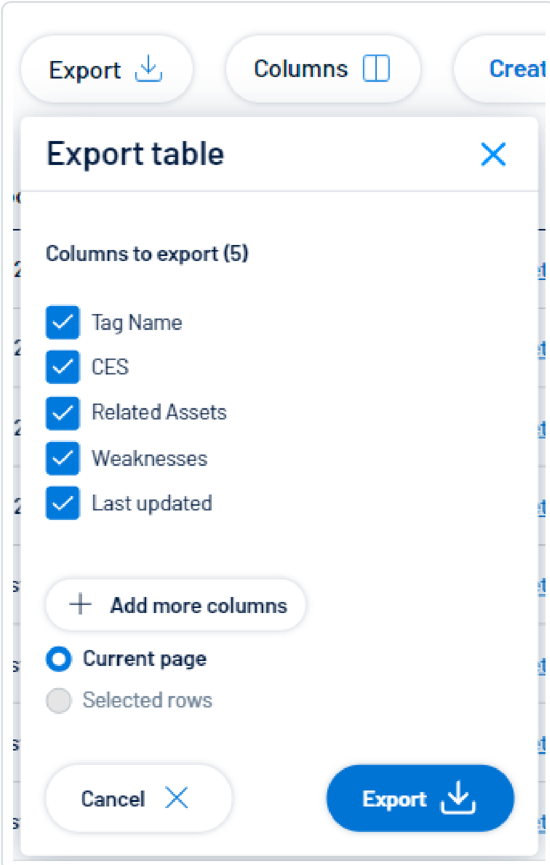
The **Tags** view appears.



In the **Tags** view, you can:

- View the total number of tags within your container.
- View the total number of tag categories within your container.
- Manage your tags:
    - Create a Tag
    - Edit a Tag
    - Delete a Tag
- Use the **Search** box to search for a specific tag value or tag category in the list.
- 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**.

Tenable 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**.

     Tenable Inventory saves your changes to the columns in the table.

- View a list of your tags, including the following information:

  - **Tag name** — The name of the tag value or tag category.

  - **CES** — The Cyber Exposure Score for the tag value or tag category. 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.
- **Weaknesses** — The weaknesses associated with the asset. For more information, see Weaknesses.
- **Last updated** — The date on which a user last updated the tag.
- Click **See details** to view more details about a tag. 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** — Tenable Inventory automatically applies the tag to the assets on your instance that match the tag rules. When you create an automatic tag, Tenable Inventoryapplies that tag to all your current assets and any new assets added to your organization's account. Tenable 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, Tenable 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

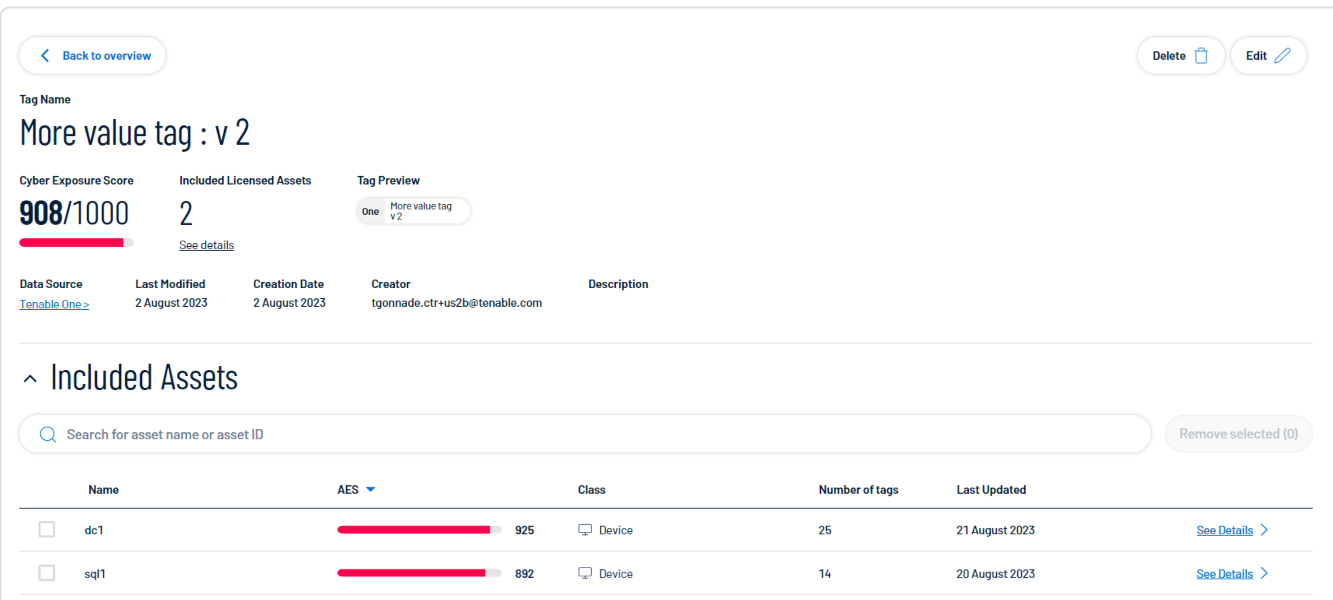
You create a tag with *Location*:*Headquarters* as the *Category*:*Value* pair, but you do not add any tag rules. Later, you add the tag to assets located at your headquarters.	static
You create a tag with *Location*:*Headquarters* as the *Category*:*Value* pair, and you specify an IP address range in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

View Tag Details

In Tenable Inventory, you can view details for any tag value or category within the **Tags** view.

1. Access the **Tag Overview**.
2. 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 **Tag Name**.
- View the **Cyber Exposure Score** for the tag.
- View the number of **Included Licensed Assets** associated with the tag.

- Click **See Details** to view the list of included assets.

- View the **Tag Preview**, where you can visualize the tag *category:value* pair.
- View the **Data Source** application for the tag.
  - Click the name of a data source to navigate to that source application.
- View the date at which the tag value or tag category was **Last Modified**.
- View the **Creation Date** of the tag value or tag category.
- View the **Creator** of the tag value or tag category.
- View a **Description** of the tag value or tag category.
- View a list of the **Included Assets** associated with the tag. You can interact with this table the same way you interact with the **Assets** table.

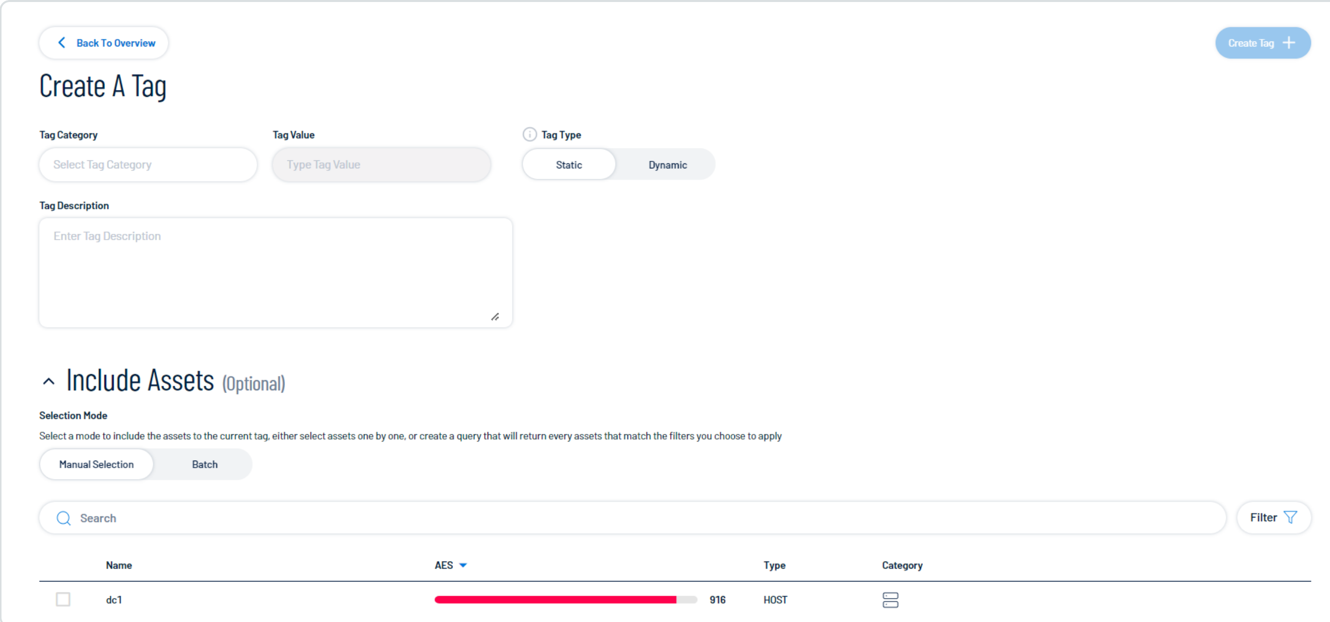
Create a Tag

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

To create a tag:

1. Access the **Tags** view.
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.

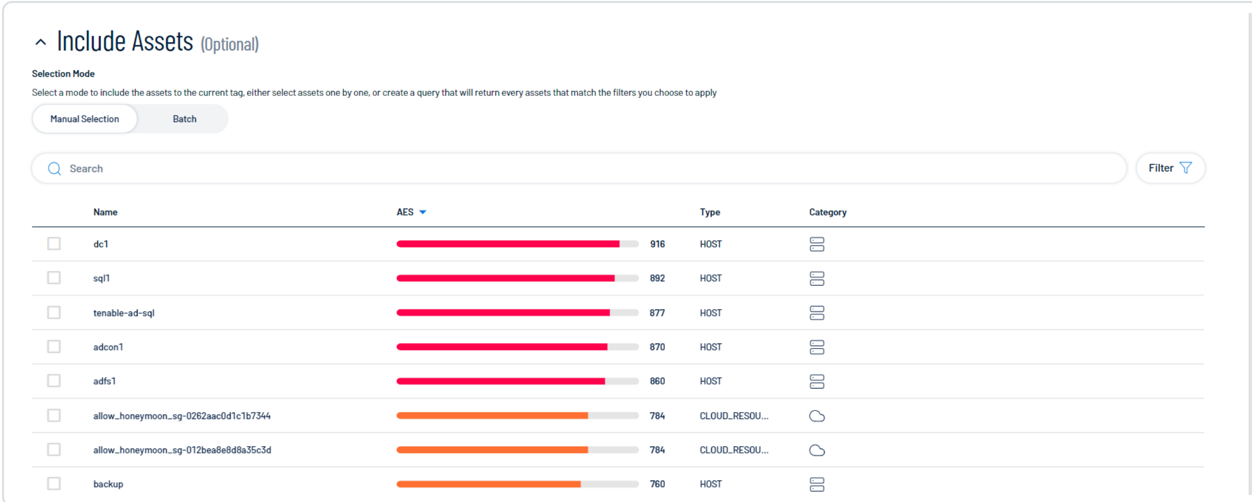
        Tenable Inventory adds the new category.

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.

      Tenable 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.

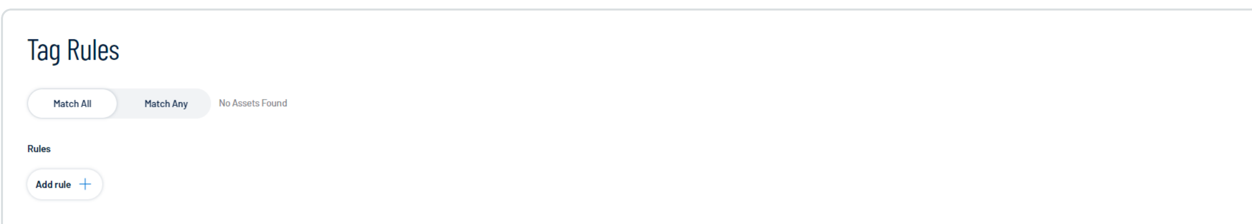
ix. Click **Apply filters**.

   Tenable 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** — Tenable 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** — If an asset matches every individual filter defined within the rule, Tenable Inventory.

  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 filter value.
is less than	Filters for items less than the filter value.
matches	Filters for items that match the filter value.

Operator	Description
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** +.

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

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

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

Edit a Tag

In the **Tags** view, 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.

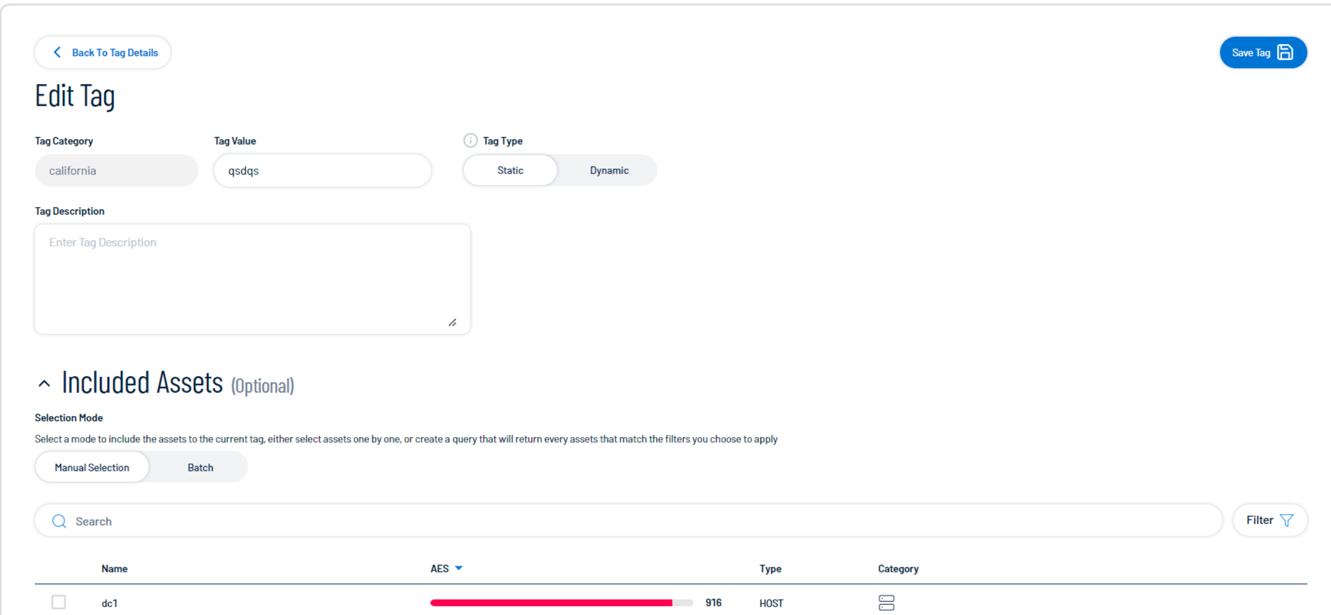
> **Note:** You can only edit tags created within Tenable Inventory. For more information, see Create a Tag.

To edit a tag:

1. Access the **[Tags](#)** view.
2. 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.
3. In the upper-right corner, click **Edit**.

   The **Edit Tag** page appears.

4. Make any desired changes.
5. Click **Save Tag** .

   Tenable Inventory saves your changes to the tag value or tag category.

Delete a Tag

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

- Tag value — Tenable Inventory removes that specific tag from all assets where you applied the tag.
- Tag category — Tenable 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 tag categories created within Tenable Inventory. For more information, see [Create a Tag](#).

To delete a tag:

1. Access the **Tag Overview**.
2. 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 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 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.
3. Click **Delete tags**.

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

Create an Exposure Card via the Tags View

In the **Tags** view, you can select one or more tags with which to create a custom exposure card. Exposure cards are cards within Lumin Exposure View that group specific data sets to more easily navigate the data for that group. For more information, see the *Lumin Exposure View User Guide*.

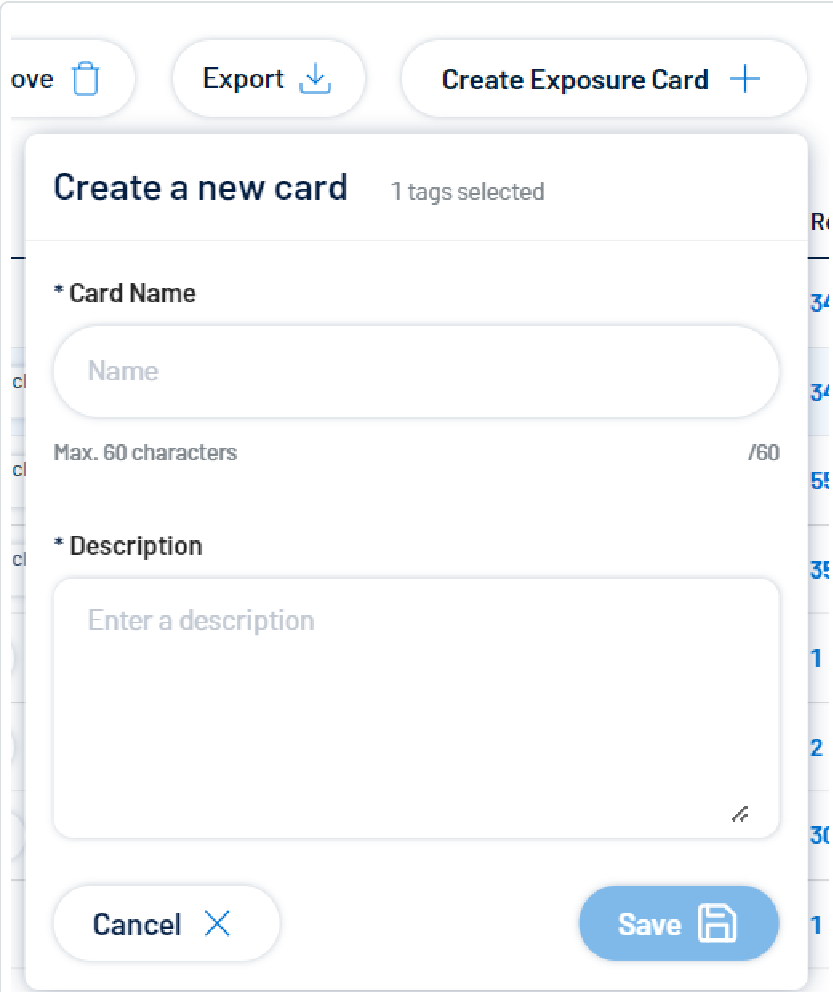
To create an exposure card via the Tags view:

1. Access the **Tags** view.
2. In the tags list, select the tag or tags for which you want to create an exposure card.

Action buttons appear at the top of the list.

3. Click **Create Exposure Card** + .

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



4. In the **Card Name** text box, type a name for the exposure card.

5. In the **Description** text box, type a brief description of the exposure card.

6. Click **Save** .

   Tenable Inventory saves the tag and adds it to the Exposure Card Library in Lumin Exposure View.

Weaknesses

Weaknesses are vulnerabilities and misconfigurations on your assets. The **Weaknesses** view highlights weaknesses on your assets and provides useful insights into those weaknesses, including descriptions, assets affected, criticality, and more.

> **Note:** Only Active and Resurfaced vulnerabilities count towards your weaknesses.

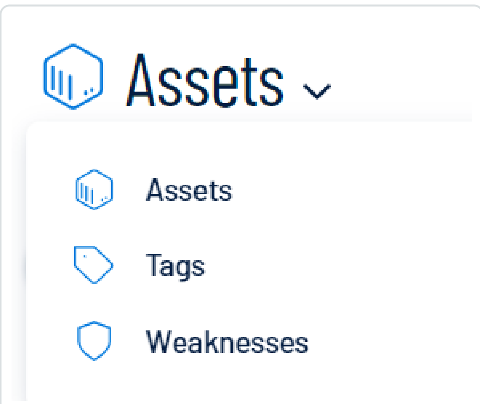
To access the Weaknesses view:

1. Access the Tenable Inventory view.

   The **Assets** view appears by default.

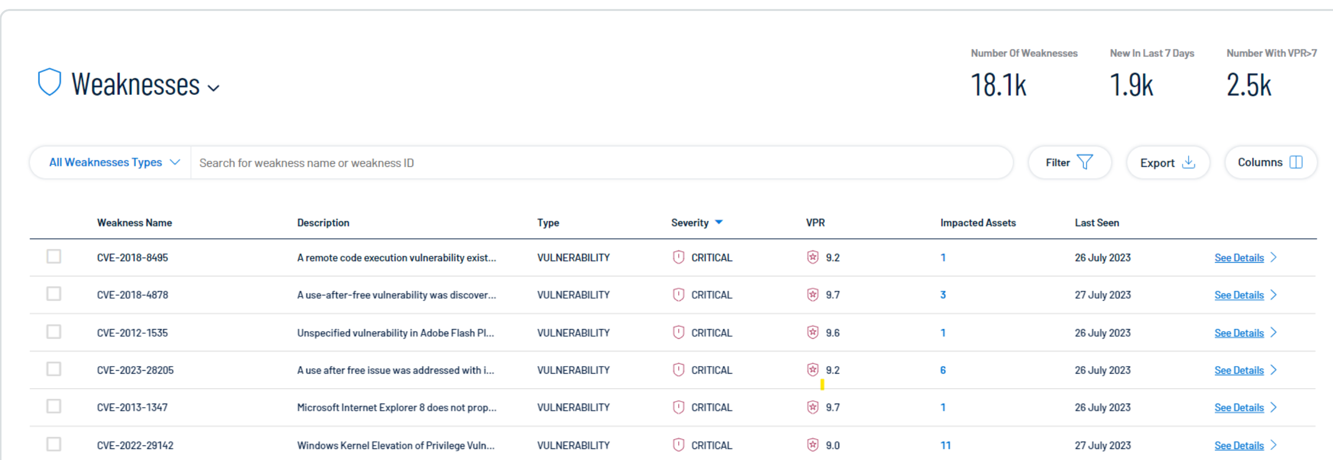
2. Click the **Assets** drop-down.

   A menu appears.

3. Click **Weaknesses**.

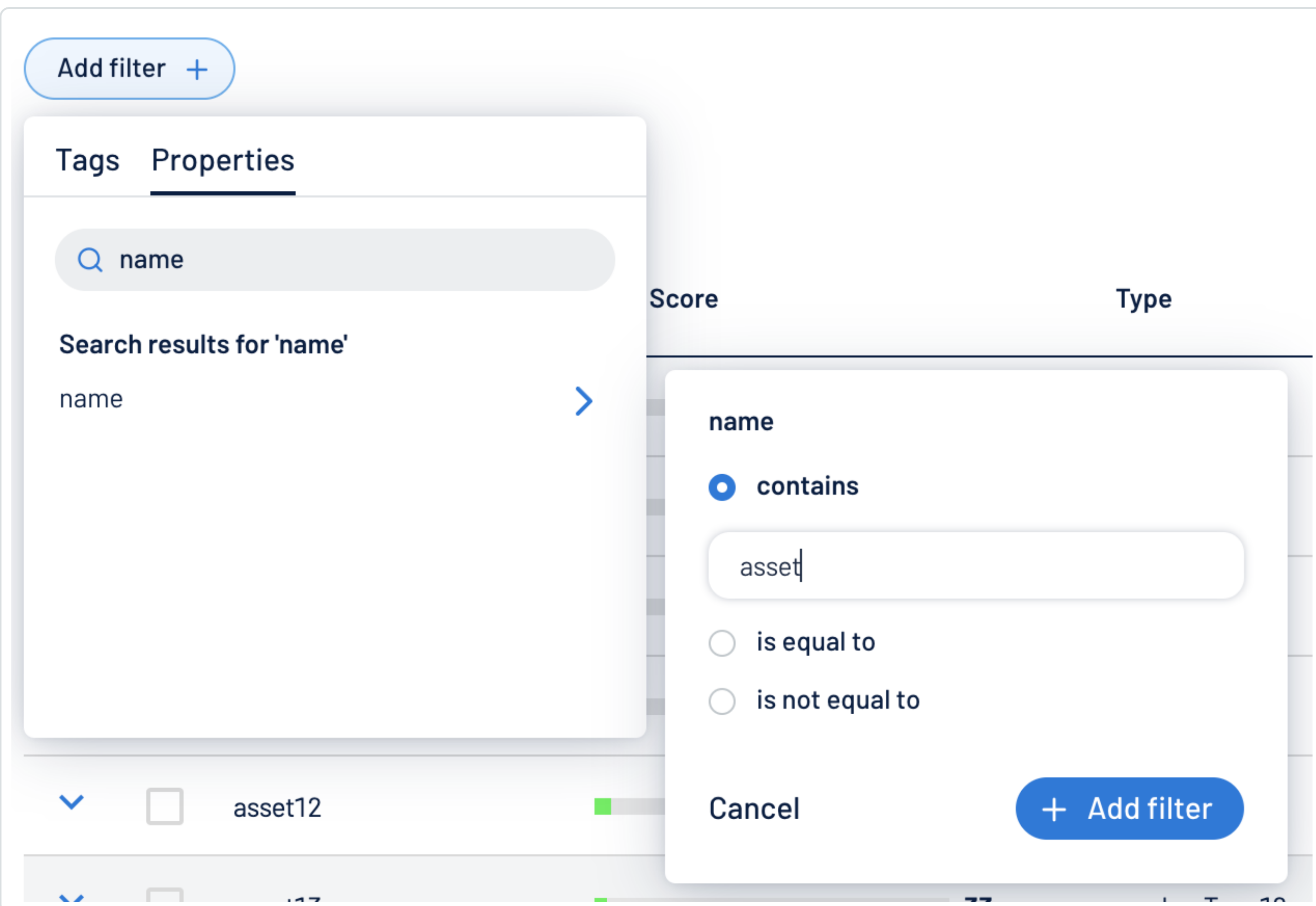
   The **Weaknesses** view appears.

In the **Weaknesses** view, you can:

- View the total number of weaknesses on assets within your container.
- View the total number of new weaknesses discovered within the last 7 days.
- View the total number of new weaknesses with a [Vulnerability Priority Rating](VPR) (VPR) greater than 7.
- In the weakness type drop-down, filter the list by the following weakness types:
    - **Misconfigurations**
    - **Vulnerabilities**

  The weakness numbers at the top of the page and the weakness list update accordingly.
- Use the **Search** box to search for a specific weakness in the list.
- Filter the weaknesses 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 weakness list by tag, click **Tags**.
  - To search the weakness list by asset property, click **Properties**.

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

Tenable Inventory populates a list of options based on your criteria.

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

A menu appears.

f. Select how to apply the filter. For example, if you want to search for a weakness whose name is *CVE-0000-0000*, then select the **contains** radio button and in the text box, type *CVE-0000-0000*.

g. Click **Add filter**.

The filter appears above the asset list.

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

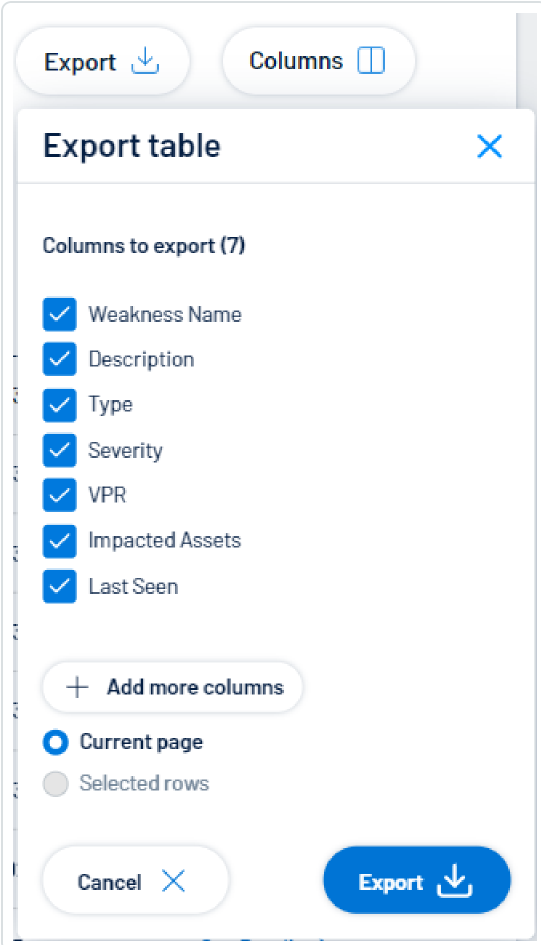
i. Click **Apply filters**.

Tenable Inventory filters the 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 checkbox 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 checkbox 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**.

Tenable 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 checkboxes 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 checkbox 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**.

     Tenable Inventory saves your changes to the columns in the table.

- View a list of your weaknesses, including the following information:

  - **Weakness Name** — The Common Vulnerability Exposure (CVE) ID associated with the weakness.

  - **Description** — A brief description of the weakness.

- **Type** — The type of weaknesses: **Misconfiguration** or **Vulnerability**.
- **Severity** — The severity of the weakness, for example, **Critical**.

  > **Note:** At this time, Tenable Inventory does not include information for Info level severity weaknesses.

- **VPR** — The Vulnerability Priority Rating (VPR) of the weakness.
- **Impacted Assets** — The number of assets impacted by the weakness. For more information, see Assets.
- **Last seen** — The date at which the weakness was last seen in a scan on the asset.
- **Sources** — The application the weakness' asset originated from, for example, Tenable Vulnerability Management.
- Click **See details** to view more details about a weakness. For more information, see View Weakness Details.

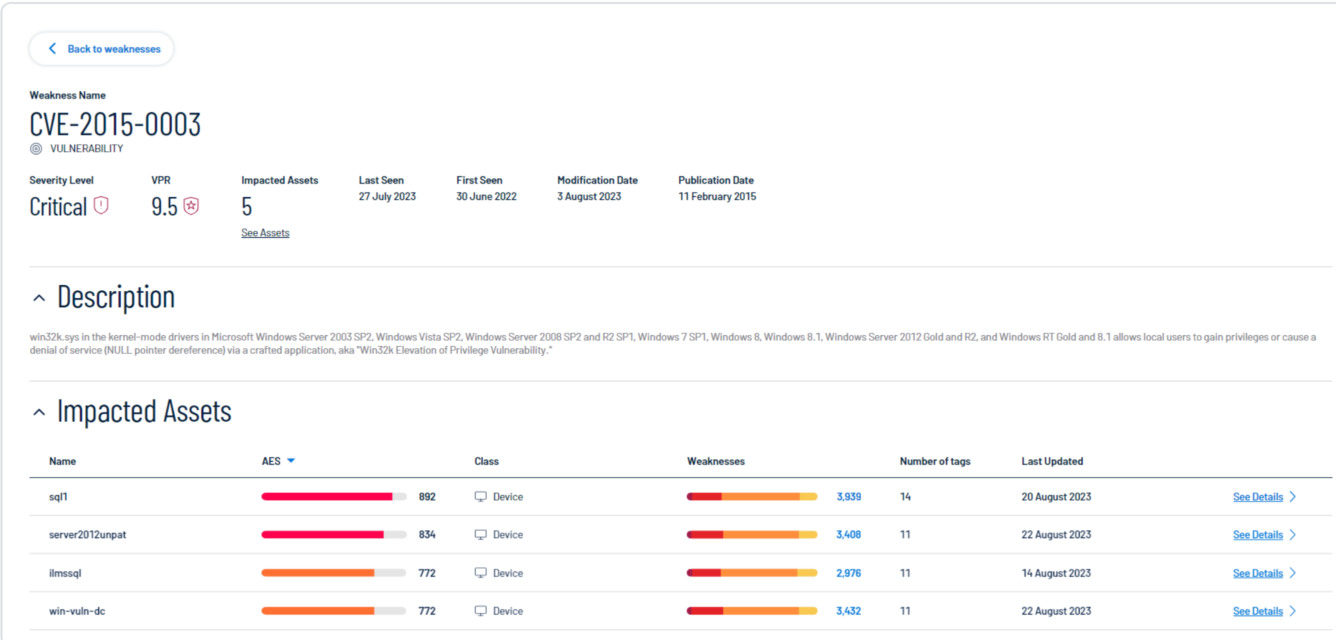
View Weakness Details

In the **Weaknesses** view, you can view details for any weakness in the list.

To view weakness details:

1. Access the **Weaknesses** view.
2. In the row of the weakness for which you want to view details, click **See details**.

The weakness details page appears.



On the weakness details page, you can:

- View the **Weakness Name**.
- View the **Severity** of the weakness, for example, **Critical**.
- View the [Vulnerability Priority Rating](#) (VPR) of the weakness.
- View the number of **Impacted Assets** associated with the weakness.
  - Click **See Details** to view the list of included assets.
- View the date at which the weakness was **Last Seen** in a scan on the asset.
- View the date at which the weakness was **First Seen** in a scan on the asset.
- View the date at which the weakness was **Last Modified**.
- View the weakness' **Publication Date**.
- View a **Description** of the weakness.
- View a table list of the **Impacted Assets** associated with the weakness.

  This list includes the following information:

- **Name** — The asset identifier. Tenable 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:** Tenable Inventory does not calculate an AES for unlicensed assets.

- **Class** — The class type associated with the asset. For more information, see Asset Classes.

- **Weaknesses** — The weaknesses associated with the asset. For more information, see Weaknesses.

  > **Tip:** Click on a Weakness count to navigate directly to the **Weaknesses** view.

- **Number of tags** — The number of tags applied to the asset. For more information on tagging an asset, see Tag Assets via the Assets View.

- **Last updated** — The date and time at which the asset was last updated.

- **Sources** — The application the asset originated from, for example, Tenable Vulnerability Management.

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

- At the bottom of the page, view any **Plugin Output** associated with the weakness.

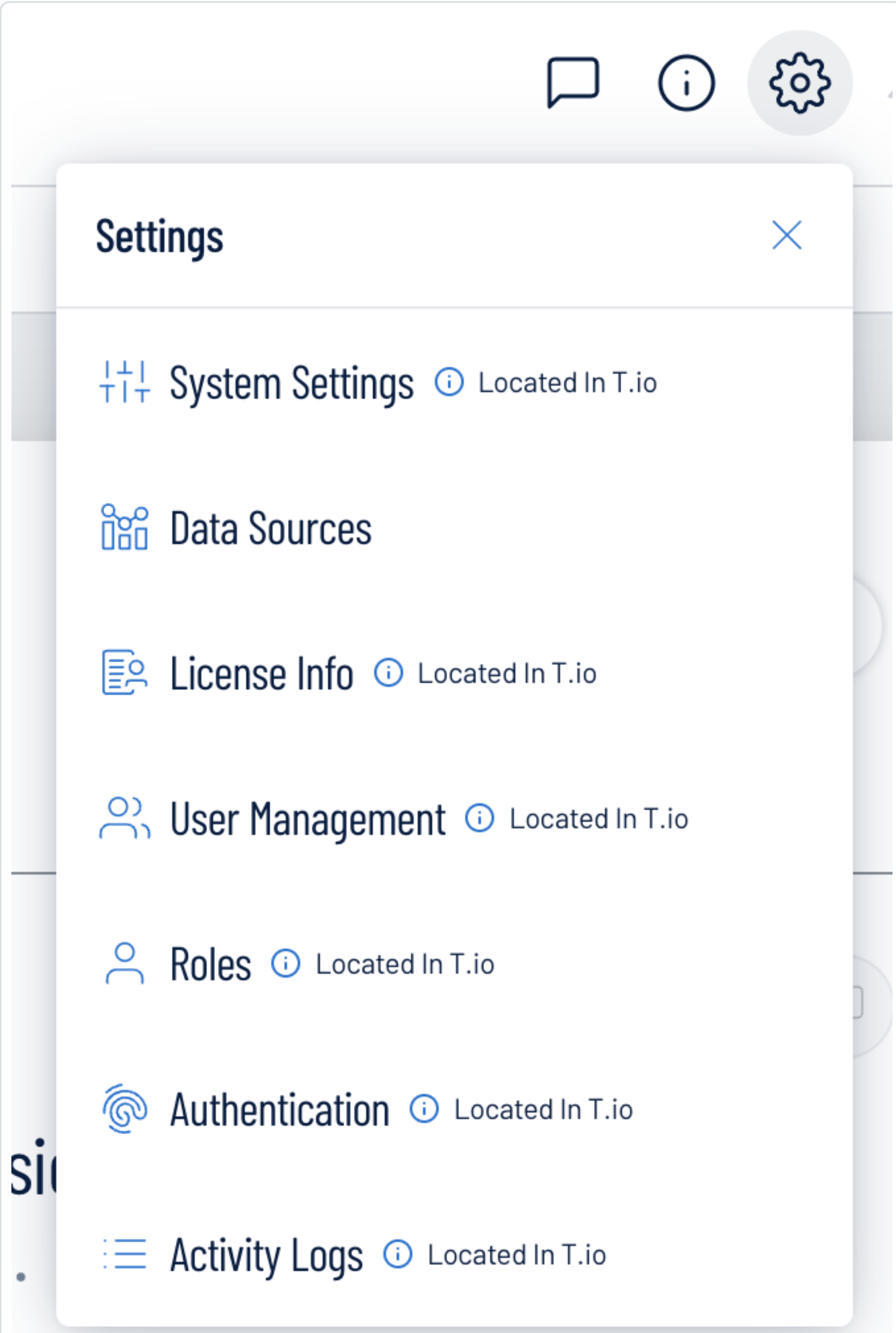
Access the Settings Menu

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 Tenable Inventory interface.
    - License Information — View your license information.

- User Management — View and manage all users, groups, and permissions.
- Roles — View and manage your Tenable 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* .

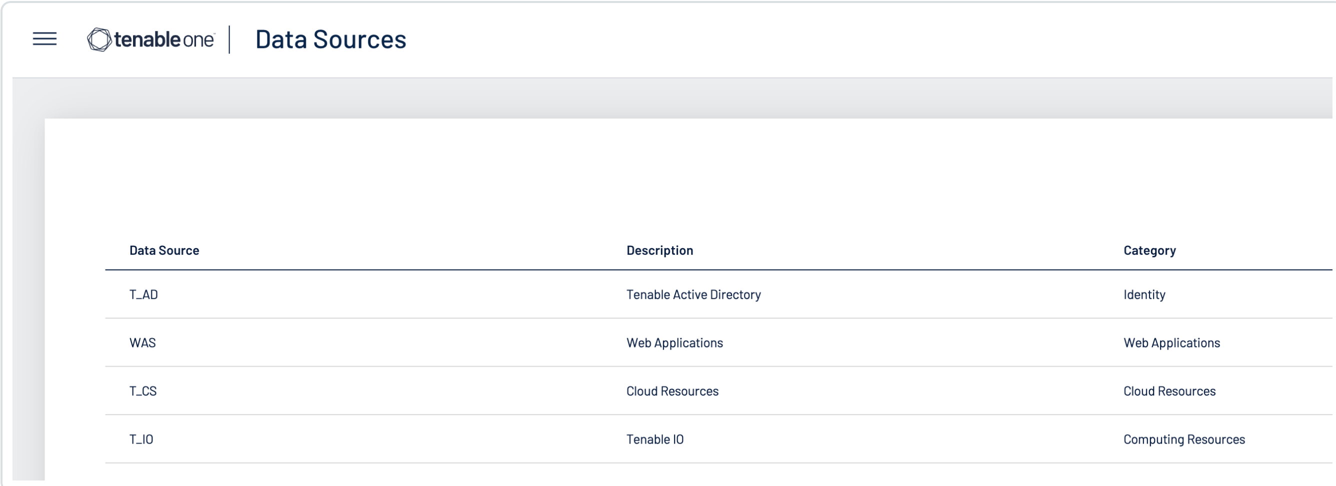
Data Sources

A data source is any product that feeds data into the Tenable Inventory interface. By default, Tenable 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 Tenable Inventory interface.
Description	A description of the data source.
Category	The category to which the data source belongs. For more information, see Tenable Inventory Metrics.

Data Timing

Data within Tenable Inventory refreshes on the following cadence:

- Asset Data — Asset information is updated every time the asset is seen as part of a scan.
- Tag Application — When a tag is first created, it can take several hours to assign the tag to the appropriate asset, depending on the number of assets and the tag's rules.
- Tag Reevaluation — Every 12 hours, Tenable Inventory automatically reevaluates tags to ensure they apply to newly discovered assets, and are removed from any inactive assets.

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 Tenable 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 Tenable 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* .