Tagging Quick Reference Guide

Last Revised: September 02, 2026

Table of Contents

Tagging in Tenable Products

This guide is a comprehensive reference for how tagging works across the Tenable product portfolio. Whether you are tagging assets in Tenable One Vulnerability Management, creating Asset Tags in Tenable Security Center, managing risk segments in Tenable One, organizing your external attack surface in Tenable One Attack Surface Management, or automating tag workflows via the API, this guide covers the concepts, procedures, and best practices you need.

Applies To

Product	Deployment	Feature Name
Tenable One Vulnerability Management	Cloud (SaaS)	Tags (Category:Value)
Tenable Security Center	On-premises	Asset Tags (typed asset lists)
Tenable Security Center Director	On-premises	Asset Tags (same as Tenable Security Center)
Tenable One	Cloud (SaaS)	Business Context (sourced from Tenable One Vulnerability Management Tags)
Tenable Exposure Management	Cloud (SaaS, part of Tenable One)	Tags (Tenable One, Tenable One Vulnerability Management, and External)
Tenable One Attack Surface Management	Cloud (SaaS)	Tags (name + value type)

Topics in This Guide

- Core Concepts — What a tag is, tag types (static vs. dynamic), re-evaluation timing, and product terminology comparison.
- Tags in Tenable One Vulnerability Management — Tag structure and limits, manual and automatic tags, creating a tag, tag rules, rule filters reference, and management procedures.
- Tag-Based Scanning — The two scan target modes, when to use each, the Empty Targets abort, and the nested tag rule limitation.
- Tags in Tenable Exposure Management — The three tag types in Tenable Exposure Management (Tenable One, Tenable One Vulnerability Management, and External), capability matrix, structure and limits, creating and managing tags, and usage in Exposure View Cards, Dashboards, Inventory, and role-based access control.
- Tags in Tenable One Attack Surface Management — Tenable One Attack Surface Management's name + value type tag model, creating and assigning tags, removing and deleting tags, use cases, and limitations.
- Tags in Tenable Security Center — Tenable Security Center's Asset Tag types (Static, DNS Name List, LDAP Query, Combination, Dynamic, Import), creating and viewing Asset Tags, Tenable One Synchronization, Tenable Security Center Director, and an Asset Tags vs. Tags comparison.
- Tagging via API — API endpoints and example request bodies for Tenable One Vulnerability Management, Tenable One, Tenable One Attack Surface Management, and Tenable Security Center (including Tenable Security Center Director).
- Cross-Product Tag Behavior — How Tenable One Vulnerability Management Tags flow into Tenable One and Exposure Management, Business Context in Tenable One, tag-scoped risk metrics, the Tags (v2) navigation, and the full cross-product capability summary table.
- Best Practices — Naming conventions, tag rule design, cross-product tagging strategy, and governance.
- Examples — Six worked tagging configurations covering common real-world use cases.

- Troubleshoot Tags – Why tags don't apply as expected (including the Excluded Assets list and the recalculation schedule), the Findings-filter and multi-tag-filter limitations, and pointers for scan-related tag issues.
- Frequently Asked Questions – Answers to common conceptual questions about tag behavior, limits, timing, and access control.

Quick Reference – Where to Create Tags

Goal	Create Tags In	Topic
Tag cloud or hybrid assets by business context, environment, or compliance scope	Tenable One Vulnerability Management	Tags in Tenable One Vulnerability Management
Group and target on-premises assets for scanning and reporting	Tenable Security Center	Tags in Tenable Security Center
Scope a scan to a tagged set of assets	Tenable One Vulnerability Management	Tag-Based Scanning
Drive Business Context segments and Cyber Exposure Score in Tenable One	Tenable One Vulnerability Management	Cross-Product Tag Behavior
Scope Exposure View Cards or Dashboards in Tenable Exposure Management	Tenable Exposure Management (Tenable One Tags) or Tenable One Vulnerability Management	Tags in Tenable Exposure Management

Goal	Create Tags In	Topic
Classify external attack surface assets (domains, IPs, web apps)	Tenable One Attack Surface Management	Tags in Tenable One Attack Surface Management
Automate tag creation and assignment at scale	Tenable API (Tenable One Vulnerability Management, Tenable One Attack Surface Management, or Tenable Security Center REST API)	Tagging via API
Diagnose why a tag isn't applying, filtering, or scanning as expected	Tenable One Vulnerability Management	Troubleshoot Tags

Additional Resources

- Tenable One Vulnerability Management – Tags
- Tenable Exposure Management – Tags
- Tenable Security Center – Asset Tags
- Tenable One Attack Surface Management – Asset Tags
- Tenable API – developer.tenable.com/reference/navigate

Core Concepts

What Is a Tag?

A **tag** is a piece of metadata you attach to one or more assets to add business context. Tags are structured as **Category:Value** pairs. The category groups related values under a common theme, and the value identifies the specific attribute within that category.

For example, if you want to group assets by geographic location, you create a **Location** category with a value of **Headquarters**. The resulting tag is `Location:Headquarters`.

A single asset can hold many tags simultaneously, and a single tag can be applied to many assets. This many-to-many relationship makes tags flexible enough to express complex organizational structures without duplicating assets or creating separate scan policies.

> **Note:** If you want to create tags without meaningful category groupings, Tenable recommends using the generic category name **Category**, which you can apply to all your tags.

Tag Types

Tenable supports two modes of applying tags:

Type	How Applied	Stays Current?	Use Case
Manual (Static)	An administrator explicitly adds the tag to selected assets	No – must be maintained manually	Priority flags, exceptions, compliance attestations
Automatic (Dynamic)	Tag Rules define criteria; Tenable One Vulnerability Management evaluates assets continuously	Yes – re-evaluated every 12 hours and on every data import	OS grouping, cloud region, installed software, owner segmentation

Automatic tag rules are available for tags in Tenable One Vulnerability Management, for Tenable One Tags in Tenable Exposure Management, and for Dynamic and Combination Asset Tags in

Tenable Security Center. Tenable One Attack Surface Management tags support manual assignment only and currently offer no rule-based automatic tagging.

Manual tags appear with a static tag icon ( ) in the user interface. Automatic tags appear with a dynamic tag icon ( ). When you manually apply an automatic tag to an asset, it displays the manual icon rather than the dynamic one.

Caution: When you manually apply an automatic tag to an asset, Tenable One Vulnerability Management excludes that asset from future rule evaluation for that tag. The asset keeps the tag until you explicitly remove it, even if it no longer satisfies the rule criteria.

When Tag Membership Is Re-evaluated

For automatic tags, Tenable One Vulnerability Management re-evaluates asset membership against tag rules in the following situations:

- When you create or update a tag
- Tenable One Vulnerability Management imports new scan or connector data
- Every 12 hours (background sweep)

Tenable One Tags in Tenable Exposure Management follow the same re-evaluation cadence: on data import and on a 12-hour background sweep. Tenable Security Center Dynamic Asset Tags refresh using results from Tenable Security Center scans rather than on a fixed interval, and Combination Asset Tags update immediately when a source Asset Tag changes. Tenable One Attack Surface Management tags are always manual, so Tenable One Attack Surface Management has no re-evaluation cycle to consider.

Product Terminology at a Glance

The naming and capabilities of the tagging feature differ across Tenable products, as the following table shows.

Product	Feature Name	Applies To	Supports Rules?	Flows to Tenable One?
Tenable One Vulnerability Management (cloud)	Tags (Category:Value)	Assets	Yes – dynamic/automatic tags	Yes – as Business Context
Tenable Exposure Management	Tags (Tenable One, Tenable One Vulnerability Management, and External)	Assets, Exposure View Cards, Dashboards (varies by tag type)	Inherited from Tenable One Vulnerability Management tags	Not applicable – native
Tenable Security Center (on-premises)	Asset Tags	Assets	Yes – Dynamic and Combination Asset Tags	Partially – via optional Tenable One Synchronization (IPv4 Static/Dynamic Asset Tags only, requires a Tenable Lumin or Tenable One license)
Tenable One Attack Surface Management	Tags (name + value type)	External attack surface assets (domains, IP	No – manual assignment only	No – isolated to the Tenable One Attack Surface Management inventory

Product	Feature Name	Applies To	Supports Rules?	Flows to Tenable One?
		addresses, web applications, cloud services)		

Tags in Tenable One Vulnerability Management

Tag Structure and Limits

Tags are managed under **Settings** → **Tagging**. The Tagging page has two tabs:

- **Categories** – groups of related tag values (maximum 100 categories per instance)
- **Values** – individual tags in *Category:Value* format (maximum 100,000 values per category)

The **Values** tab shows, per tag: the creator, when it was last processed, whether it was applied manually or automatically, the current assessment status, and the number of assets currently carrying that tag.

> **Note:** Tag names cannot contain commas and are limited to 50 characters.

> **Note:** The **# of Assets** column on the **Tags** page may show a higher count than a tag-based search in the Assets inventory. The tag count includes deleted assets that have not yet aged out of the license count. This is expected behavior.

Manual vs. Automatic Tags

When you create a tag, you choose whether it is manual or automatic:

- **Manual tags** have no rules. You explicitly apply them to individual assets. They persist until you remove them and do not respond to changes in asset attributes.
- **Automatic tags** include one or more tag rules. Tenable One Vulnerability Management evaluates assets against those rules continuously and applies or removes the tag as assets change.

Create a Tag

Create a tag when you need to add business context to one or more assets, either by applying it manually or by defining rules that apply it automatically.

Before You Begin

- Confirm your user account has the **Scan Manager** or **Administrator** role.
- Decide whether the tag belongs in an existing **Category** or requires a new one.

To create a tag:

1. In the left navigation bar, click the **Settings** icon.

   The **Settings** page appears.

2. On the Settings page, click the **Tagging** tile.

   The Tagging page appears, showing the **Categories** and **Values** tabs.

3. In the upper-right corner, click **Create Tag**.

   The **Create Tag** pane appears.

4. In the **Category** field, select an existing category or create a new one.

5. In the **Value** field, enter a value for the tag.

6. Optionally, in the **Category Description** and **Value Description** fields, enter descriptive text.
7. Do one of the following:
    - To save the tag as a manual tag, click **Save**.
    - To save the tag as an automatic tag, configure at least one tag rule, then click **Save**.

    Tenable One Vulnerability Management adds the tag to the **Values** tab.

Tip: You can also create a dynamic tag directly from the **Assets** page. Filter the asset inventory to the exact set of assets you want, then click **Take Action → Create Dynamic Tag**. Tenable One Vulnerability Management converts your active filters into the tag rule automatically.

What To Do Next

Apply the tag to assets, or, if you created an automatic tag, monitor the **Assessment** column on the **Values** tab until it shows *Completed*. If assets you expect to see are missing, see Troubleshoot Tags.

Tag Rules

Tag rules are the logic that powers automatic tags. Each rule is composed of one or more filter-value conditions combined with **AND** (*Match All*) or **OR** (*Match Any*) logic. When an asset satisfies all the conditions in at least one rule, Tenable One Vulnerability Management applies the tag.

Rule Limits

- **Maximum boolean filter conditions per rule:** 40
- **Maximum values per filter property:** 1,024 (for example, a single IP Address filter can list up to 1,024 addresses)

Note: If your tag fails to apply, the rule may be returning too many assets for Tenable One Vulnerability Management to process. Reduce the scope by adding stricter conditions or splitting the

ule across two tags joined by a nested tag filter. For other common causes of tags not applying, see Troubleshoot Tags.

Tag Rule Filters Reference

The following table lists the most commonly used rule filters. A complete list is available in the Tagging UI under **Settings → Tagging → Create Tag → Rules**.

Filter Category	Example Filters	License Required
Network Identifiers	IPv4 Address (CIDR supported), IPv6 Address, MAC Address, DNS (FQDN), Hostname, NetBIOS Name, Open Ports	Base
Asset Metadata	Operating System, System Type, Installed Software (CPE 2.3), Name, Record Type, Source	Base
Scan Timing	First Seen, Last Seen, Last Authenticated Scan, Last Licensed Scan, Created Date, Updated Date	Base
Cloud – AWS	AWS Region, AWS VPC ID, AWS EC2 Instance ID, AWS Security Group, AWS Owner ID, ARN	Base
Cloud – Azure	Azure Resource Group, Azure VM ID, Azure Subscription ID, Azure Resource Type	Base
Cloud – GCP	Google Cloud Instance ID, Google Cloud Project ID, Google Cloud Zone	Base
Cloud Native Tags	Resource Tags (By Key), Resource Tags (By Value), Cloud Provider, Hosting Provider	Base

Filter Category	Example Filters	License Required
Risk Scores	ACR, ACR Severity, AES, AES Severity	Tenable One
Status Flags	Licensed, Deleted, Terminated, Public, Assessed vs. Discovered, Has Plugin Results	Base
Third-Party	ServiceNow Sys ID, Custom Attribute (key-value pairs)	Base (integration required)
Tags (nested)	Tags – filter assets that already carry a specific tag (case-sensitive; maximum 100 tags per rule)	Base

Tag Rule Operators

Operators define how a filter value is matched against an asset attribute. Available operators depend on the data type of the filter.

Data Type	Available Operators
String	`is equal to`, `is not equal to`, `contains`, `does not contain`, `matches` (wildcards supported), `does not match`, `exists`, `does not exist`
Date / Time	`is equal to`, `is greater than`, `is less than`, `between`, `older than`, `newer than`, `within last`
Numeric / Score	`=`, `!=`, `>`, `>=`, `<`, `<=`

Caution – Wildcard Performance: The asterisk (`*`) wildcard is supported in `matches` and `does not match` operators. Avoid **leading wildcards** (for example, `*linux`). Leading wildcards force a full-index

scan and can cause search timeouts or prevent tags from applying. Use trailing wildcards (for example, `linux*`) or the `contains` operator instead.

Managing Tags — Quick Reference

Task	Required Role	Location
View tags	Read-Only or higher	Settings → Tagging → Categories or Values tab
Create a tag	Scan Manager or Administrator	Settings → Tagging → Create Tag button
Create a dynamic tag from an asset filter	Administrator	Explore → Assets → filter → Take Action → Create Dynamic Tag
Apply a tag to a single asset	Basic User or higher	Asset Details page → Tags section → + button
Apply a tag to multiple assets	Basic User or higher	Explore → Assets → select checkboxes → Add Tags
Remove a tag from assets	Basic User or higher	Explore → Assets → select checkboxes → More → Remove Tags
Edit a tag or category	Scan Manager or Administrator	Settings → Tagging → click the tag or category row
Export tags (CSV or JSON)	Scan Manager or Administrator	Settings → Tagging → select tags → Export
Delete a tag or category	Scan Manager or Administrator	Settings → Tagging → Actions → Delete

Task	Required Role	Location
Search assets by tag	Scan Operator or higher	Settings → Tagging → Values → Actions → Search by Tag

Note: The roles in this table control who can create, edit, or delete tags. They are separate from access group permissions, which use tags to scope which assets a user can view or edit. Access group permissions do not restrict which IP addresses or hostnames a user can manually enter as scan targets. For more information, see Frequently Asked Questions and Tag-Based Scanning.

Caution: Deleting a tag category removes it and all associated tag values from every asset in the system immediately. This action cannot be undone from the UI. Export the tag library before making major changes.

Additional Resources

For complete tagging documentation, see Tags in the Tenable One Vulnerability Management User Guide.

Tag-Based Scanning

You can use tags to define what a scan targets instead of listing individual IP addresses or hostnames. This topic explains the two tag-based target modes, when to use each, and the limitations that most often cause a tag-based scan to fail.

Scan Target Modes

When you use a tag as a scan target source, you choose one of two modes.

Mode	How Targets Are Resolved	Requires IPv4/IPv6?
Targets defined by tags	Resolved dynamically from the tag's current membership each time the scan runs	Yes
Existing tagged assets only	Scans the fixed set of assets that carry the tag at the time you launch the scan	No

Caution – Empty Targets Abort: If a tag resolves to assets that have only an FQDN and no IPv4 or IPv6 address, a scan set to **Targets defined by tags** aborts with an *Empty Targets* error. Switch the scan to **Existing tagged assets only** to scan FQDN-only assets by tag.

Choosing a Target Mode

- Use **Targets defined by tags** when the tagged population is expected to change between scans and every asset in the tag has a resolvable IPv4 or IPv6 address.
- Use **Existing tagged assets only** when the tag includes FQDN-only assets, or when you want the scan to target a stable snapshot of the tag's membership at launch time rather than whatever matches the tag when the scan actually runs.

Configure a Tag-Based Scan Target

Before You Begin

- Confirm which assets the tag currently resolves to and whether they have resolvable IPv4/IPv6 addresses or are FQDN-only.
- Decide whether the scan should track the tag's live membership or a fixed snapshot of it. This determines which target mode you select.

To configure a tag-based scan target:

1. Create a new scan or open an existing scan for editing.
2. In the **Targets** field, select **Tags** as the target source.

   The tag-based targeting options appear.
3. Select **Targets defined by tags** or **Existing tagged assets only**.
4. Select the tag or tags to use as the target source.
5. Save or launch the scan.

   Tenable One Vulnerability Management resolves the scan targets according to the mode you selected.

What To Do Next

If the scan aborts with an Empty Targets error, see the caution above. If you nest a Tags filter inside a rule that also contains IP or FQDN conditions, see the limitation below before troubleshooting further.

Nested Tag Rules and Scan Targeting

> **Caution:** If a dynamic tag's rule nests a **Tags** filter inside a rule that also contains IPv4, IPv6, or FQDN conditions, target resolution for scanning fails silently. When you plan to use a tag as a scan target, keep its rule limited to IP address and FQDN-type conditions only, and build any tag-based grouping logic into a separate, non-nested tag instead.

Tag-Based Scanning and Role-Based Access Control

A user role scoped to a tag controls which assets that user can *view*—it does not prevent the user from manually typing an out-of-scope IP address or hostname into a scan's target field and successfully scanning it. Tag-scoped permissions are a visibility control, not a scan-target control.

If you need to guarantee that users cannot scan outside their assigned tag scope, restrict scan target entry at the scan or scan policy level in addition to configuring tag-scoped roles. For the full clarification, see Frequently Asked Questions.

Tags in Tenable Exposure Management

Overview

Tenable Exposure Management (within Tenable One) presents three distinct tag types, each with different origins, capabilities, and edit permissions. Understanding which type a tag belongs to determines what you can do with it and where you can use it.

Tag Type	Origin	Editable in Tenable Exposure Management?
Tenable One Tags	Created natively in Tenable Exposure Management or Tenable One	Yes – full create/edit/delete
Tenable One Vulnerability Management Tags	Synchronized from Tenable One Vulnerability Management (cloud)	No – read-only; edit in Tenable One Vulnerability Management
External Tags	Imported from Tenable One Cloud Exposure, Tenable One Identity Exposure, or third-party integrations	No – read-only; asset-level only

Tag Type Capabilities

The three tag types differ in which Tenable Exposure Management features they can drive.

Capability	Tenable One Tags	Tenable One Vulnerability Management Tags	External Tags
Filter Inventory (asset search)	Yes	Yes	Yes
Exposure View Cards (scope)	Yes	Yes	No
Dashboard Filters	Yes	No	No
Dynamic Tag Rule Input (filter assets by tag)	Yes	Yes	Yes
Role-based access control	Yes	Yes	No
Cyber Exposure Score per tag	Yes	Yes	No

Tenable One Tags

Tenable One Tags are created and managed directly in Tenable Exposure Management. They follow the same Category:Value pair structure as Tenable One Vulnerability Management Tags. Because they are native to the Tenable One platform, they carry the broadest set of capabilities: Exposure View Card scoping, Dashboard filtering, role-based access control, and a per-tag Cyber Exposure Score.

When you create a tag in Tenable Exposure Management, it is stored as a Tenable One Tag. If you want a tag to appear in Tenable One Vulnerability Management as well, create it in Tenable One Vulnerability Management — it will sync into Tenable Exposure Management as a Tenable One Vulnerability Management Tag (read-only in Tenable Exposure Management).

Tenable One Vulnerability Management Tags

Tags created in Tenable One Vulnerability Management sync into Tenable Exposure Management and appear alongside Tenable One Tags. In Tenable Exposure Management they are read-only — to change the tag definition, tag rules, or values, navigate to **Settings → Tagging** in Tenable One Vulnerability Management.

Tenable One Vulnerability Management Tags support all capabilities except Dashboard Filters. They carry a Cyber Exposure Score value, can scope Exposure View Cards, and can define access group membership for role-based access control.

External Tags

External Tags originate from Tenable One Cloud Exposure, Tenable One Identity Exposure, or third-party data integrations. They are applied at the individual asset level and are read-only in Tenable Exposure Management. Their primary use is as search and filter inputs in the Inventory — they cannot scope Exposure View Cards, Dashboards, or role-based access control.

Structure and Limits

- Maximum **100 tag categories** per Tenable One instance
- Maximum **100,000 tag values** per category
- Maximum **1,000 tag rules** per tag value
- Maximum request body size: **1 MB**
- Tag categories **cannot be renamed** after a tag value has been saved under them. Plan category names carefully before creating your first value in a category.

> **Caution:** Unlike Tenable One Vulnerability Management, the category name in Tenable Exposure Management is locked once any value is saved to that category. If you need to rename a category, you must delete all values under it first, then recreate the category with the new name.

Static vs. Dynamic Tags in Tenable Exposure Management

Attribute	Static Tag	Dynamic Tag
Assignment method	Manual	Rule-based, automatic
Re-evaluation	Never (persists until manually removed)	Triggered on data import; background sweep every 12 hours
Manual override	Not applicable	Manually applied tag exempts asset from rule evaluation
Dashboard data lag	Up to 24 hours	Up to 24 hours

The Tags Page

Navigate to **Inventory → Tags** to access the Tags management page. Each row in the tag list displays:

- **Tag Name** – the Category:Value pair
- **Cyber Exposure Score** – the score for assets in that tag (0–1000)
- **Related Assets** – the count of assets carrying the tag
- **Weakness Count** – total weaknesses across tagged assets
- **Last Updated** – when the tag data was last recalculated

Create a Tag

Create a tag in Tenable Exposure Management when you want a tag that is native to Tenable One and fully editable there, rather than one synchronized read-only from Tenable One Vulnerability Management.

Before You Begin

- Choose the **Category** name carefully — category names cannot be changed after a value is saved under them.
- Decide whether the tag should be **Static** (manually applied) or **Dynamic** (rule-based).

From the Tags Page

To create a tag from the Tags page:

1. In the left navigation bar, go to **Inventory → Tags**.

   The Tags page appears.

2. Click **Create Tag**.

   The Create Tag pane appears.

3. Enter a **Category** name (new or existing). If selecting an existing category, note that the name cannot be changed after a value is saved.
4. Enter a **Value** name.
5. Optionally add a description.
6. Choose **Static** (manual) or **Dynamic** (rule-based). For dynamic tags, configure one or more rules.
7. Click **Save**.

   The new tag appears on the Tags page.

From the Assets Page

To create a tag from the Assets page:

1. In the left navigation bar, go to **Inventory** → **Assets**.

   The **Assets** page appears.

2. Select one or more assets.
3. Click the ⋮ **Actions** menu, then click **Tag Assets**.

   The **Tag Assets** dialog appears.

4. Select an existing tag or create a new one inline.
5. Click **Apply**.

   Tenable Exposure Management applies the tag to the selected assets.

What To Do Next

Use the tag to scope an Exposure View Card or Dashboard (see the following sections), or configure a tag-scoped role for role-based access control.

Editing and Deleting Tags

To edit a Tenable One Tag, open the tag from **Inventory** → **Tags** and click the ✎ **Edit** button. You can modify the value name, description, and rules. You cannot change the category name if values already exist under it.

To delete a tag value, click the ⋮ overflow menu on the tag row and select **Delete**. Deleting a value removes it from all assets immediately. Deleting all values in a category removes the category.

Tenable One Vulnerability Management Tags and External Tags display no **Edit** or **Delete** controls in Tenable Exposure Management — those operations must be performed in their respective source products.

Using Tags in Exposure View Cards

Exposure View Cards can be scoped to a specific tag, allowing each card to report Cyber Exposure Score, Asset Exposure Score, and vulnerability counts for a defined segment of your environment. Tenable One Tags and Tenable One Vulnerability Management Tags both support card scoping; External Tags do not.

To scope a card to a tag, open the card configuration and set the **Tag** field to the desired Category:Value pair.

Using Tags in Dashboards

Dashboard-level tag filtering is available for **Tenable One Tags only**. When a dashboard is filtered by a Tenable One Tag, all widgets on the dashboard reflect data scoped to that tag's asset population.

Allow up to **24 hours** for Dashboard data to reflect tag membership changes after a tag rule runs or assets are manually tagged.

Using Tags for Role-Based Access Control

Tenable One Tags and Tenable One Vulnerability Management Tags can define the scope of a user role's permissions in Tenable One. When a role is scoped to a tag, users assigned that role see only assets, findings, and metrics associated with that tag's asset population.

Configure tag-scoped roles under **Settings → Access Control → Roles**.

> **Note – Permission Scope Clarification:** Tag-scoped role permissions control which assets, findings, and metrics a user can *view* in Tenable One and Tenable Exposure Management. They do not restrict what a user can manually type into a scan target field in Tenable One Vulnerability Management. A user whose visibility is scoped to a specific tag can still launch a scan against a manually entered IP address or hostname outside that tag's scope. To prevent out-of-scope scanning, pair tag-scoped roles with scan-level target restrictions rather than relying on tag permissions alone. For more information, see Tag-Based Scanning.

Additional Resources

For complete tagging documentation, see Tags in the Tenable Exposure Management User Guide.

Tags in Tenable One Attack Surface Management

Overview

Tenable One Attack Surface Management uses a tagging model that differs from Tenable One Vulnerability Management and Tenable Exposure Management. Tenable One Attack Surface Management tags have a **name** and a **value type** – they are not structured as Category:Value pairs. Tags are stored in a global tag store for your Tenable One Attack Surface Management inventory, and you assign them to assets individually or in bulk.

Tenable One Attack Surface Management tags help you organize external attack surface assets – domains, IP addresses, web applications, cloud services, and other internet-facing resources – into meaningful groups for tracking, reporting, and prioritization.

> **Note:** Tenable One Attack Surface Management tags are independent from Tenable One Vulnerability Management tags, Tenable One tags, and Tenable Exposure Management tags. They apply only within your Tenable One Attack Surface Management inventory and do not flow into Tenable One Business Context or appear in other Tenable products.

Tag Structure

Each Tenable One Attack Surface Management tag consists of two parts:

- **Name** – a text label that identifies the tag (for example, `Business Unit`, `Priority`, `Owner`).
- **Value Type** – determines what kind of value, if any, the tag carries when assigned to an asset.

Available value types:

Value Type	Description	Example
No Value	A presence/absence flag — the tag either exists on an asset or it doesn't	`Reviewed`, `Accepted Risk`
Keyword	A free-form text string value	`Owner: platform-team`
Number	An integer or decimal value	`Risk Score: 8`
Cost	A monetary value (currency-neutral)	`Annual Cost: 12000`
Percentage	A percentage value (0–100)	`Coverage: 85`
Boolean	True or false	`In Scope: true`

Required Roles

Tag management in Tenable One Attack Surface Management requires one of the following roles:

- **Active User**
- **Cloud Connector Manager**
- **Business Administrator**

Users with read-only roles can view tags assigned to assets but cannot create, edit, or delete tags.

Create a Tag

Create a tag before you can assign it to assets in your inventory.

Before You Begin

Confirm your user account has the **Active User**, **Cloud Connector Manager**, or **Business Administrator** role.

To create a tag:

1. In Tenable One Attack Surface Management, navigate to **Inventory**.

   The inventory appears.

2. In the left panel, click **Tags**.

   The tag store opens.

3. Click **Add Tag**.

   The Add Tag dialog appears.

4. Enter a **Tag Name**.

5. Select a **Value Type** from the drop-down box.

6. Click **Save**.

   Tenable One Attack Surface Management adds the tag to the tag store.

What To Do Next

Assign the tag to one or more assets. See Tags in Tenable One Attack Surface Management below.

Assign Tags to Assets

You can assign tags to assets in two ways.

From the Inventory View (Bulk Assignment)

To assign tags from the Inventory view:

1. Navigate to **Inventory**.

   The inventory appears.

2. Apply filters to isolate the assets you want to tag.
3. Select one or more assets using the checkboxes, or select all filtered results.
4. Click the ⋮ **Actions** menu, then click **Add Tag**.

   The tag selection dialog appears.

5. Select the tag from the list. If the value type requires a value (Keyword, Number, Cost, Percentage, or Boolean), enter the value.
6. Click **Apply**.

   Tenable One Attack Surface Management applies the tag to the selected assets.

From the Asset Details Panel (Individual Asset)

To assign a tag from the asset details panel:

1. In the Inventory, click an asset to open its detail panel.

   The asset detail panel opens.

2. Scroll to the **Tags** section.
3. Click **Add Tag**.

   The Add Tag dialog appears.

4. Select the tag and supply a value if required.
5. Click **Save**.

   Tenable One Attack Surface Management applies the tag to the asset.

Removing Tags from Assets

To remove a tag from an asset, open the asset's detail panel, locate the tag in the **Tags** section, and click the remove icon (⌫) next to it.

To remove a tag from multiple assets at once, filter the inventory, select the relevant assets, and choose the ⋮ **Actions** menu, then click **Remove Tag**.

Delete a Tag

To delete a tag:

1. Navigate to **Inventory** → **Tags**.

   The tag store appears.

2. Locate the tag in the list.
3. Click the 🗑 button.
4. Confirm the deletion.

   Tenable One Attack Surface Management removes the tag from the tag store and from every asset that carried it.

> **Caution:** Deleting a tag removes it from *every asset* in the inventory simultaneously. There is no per-asset removal when deleting at the tag store level. This action cannot be undone. If you want to stop using a tag without losing its history, consider leaving it in the store and simply stopping new assignments rather than deleting it.

Common Use Cases

Tenable One Attack Surface Management tags are particularly well suited for classifying external attack surface assets that may not appear in internal vulnerability management programs:

- **Ownership tracking** — Use a Keyword tag (`Owner`) to attribute internet-facing assets to a specific team or business unit for accountability.
- **Scope marking** — Use a Boolean tag (`In Scope`) to mark assets that are part of a scheduled penetration test or Tenable One Attack Surface Management review.
- **Priority tiering** — Use a Number or Keyword tag (`Priority`) to stratify which external assets require immediate remediation attention.
- **Acceptance records** — Use a No Value tag (`Risk Accepted`) as a presence flag on assets where risk has been formally accepted.
- **Cost allocation** — Use a Cost tag (`Annual Cost`) to assign a monetary value to external services for budget reporting.

Limitations and Considerations

- Tenable One Attack Surface Management tags do not support automation rules. All tag assignments are manual or via the API.
- Tenable One Attack Surface Management tags cannot be structured as Category:Value pairs — each tag has a single name and a single value type.
- Tags are scoped to a single Tenable One Attack Surface Management inventory. If you maintain multiple inventories, tags must be created separately in each one.
- Tenable One Attack Surface Management tags do not flow into Tenable One Vulnerability Management, Tenable One, or Tenable Exposure Management.
- There is no bulk export of the Tenable One Attack Surface Management tag library from the UI; use the Tagging via API for programmatic export.

Additional Resources

For complete tag documentation, see Asset Tags in the Tenable One Attack Surface Management User Guide.

Tags in Tenable Security Center

Asset Tag Overview

Tenable Security Center (on-premises) uses **Asset Tags** as its primary mechanism for grouping the assets it monitors — including vulnerability management, OT, and web application scanning data — so you can target them for scanning, filtering, and reporting. Some Asset Tag types are functionally similar to Tenable One Vulnerability Management Tags: **Dynamic Asset Tags** use rule-based condition statements that Tenable Security Center re-evaluates against scan results, and **Combination Asset Tags** build on existing Asset Tags using **AND**, **OR**, and **NOT** operators.

Key differences from Tenable One Vulnerability Management Tags:

- Asset Tags are **typed lists of assets**, not structured Category:Value pairs.
- Asset Tags apply only to **assets**. Other objects, such as scan policies, credentials, and queries, cannot be grouped by an Asset Tag.
- Only **Dynamic** and **Combination** Asset Tags support rule-based or derived membership. The remaining types (Static, DNS Name List, LDAP Query, Import) are membership lists you populate directly.

> **Note:** Tenable Security Center also has a separate, unrelated **Labels** feature — a free-form text descriptor you can attach to an asset, scan policy, credential, or query for lightweight filtering. Labels have no rule engine and are not shared across object types. For details, see Labels in the Tenable Security Center User Guide.

Asset Tag Types

Tenable Security Center supports Template-Based Asset Tags as well as seven custom Asset Tag types:

- **Template-Based** – Pre-configured by Tenable and customizable for your environment. Templates update via the Tenable Security Center feed.
- **Static Asset Tags** – A list of specific IP addresses, CIDR ranges, or IP ranges (up to 50,000 characters). Usable immediately after setup.
- **DNS Name List Asset Tags** – A list of DNS hostnames.
- **LDAP Query Asset Tags** – A dynamic list built from a query against a configured LDAP server, using search base and search string parameters.
- **Combination Asset Tags** – A list built from existing Asset Tags using **AND**, **OR**, and **NOT** operators. Membership updates automatically when a source Asset Tag changes.
- **Dynamic Asset Tags** – A list built from rule-based condition statements. Tenable Security Center refreshes membership using results from Tenable Security Center scans, and requires an initial discovery scan before it can populate.
- **Import Asset Tags** – An Asset Tag reimported from a previously exported file.

> **Caution:** DNS Name List and LDAP Query Asset Tags cannot target agent scans or agent synchronization jobs. If you need agent-based scanning or synchronization, use a Static or Dynamic Asset Tag instead.

Permissions and Sharing

Managing Asset Tags requires an **Organizational User** role with appropriate permissions. The **Assets → Asset Tags** page reflects only the Asset Tags you have permission to view.

Asset Tags can be shared with one or more users based on your organization's local security policy requirements. Asset Tag lists are calculated **per repository** – updating an Asset Tag in one repository does not affect other repositories.

Create an Asset Tag

Create an Asset Tag to group assets so you can target, filter, and report on them as a set.

Before You Begin

- Confirm you have an **Organizational User** role with appropriate permissions.
- Decide which Asset Tag type fits your use case: a Template-Based tag, or a custom Static, DNS Name List, LDAP Query, Combination, Dynamic, or Import tag.
- If you are creating a Dynamic Asset Tag, confirm that Tenable Security Center has already run an initial discovery scan against the target assets.

To create an asset tag:

1. Log in to Tenable Security Center.
2. In the left navigation bar, click **Assets → Asset Tags**.

   The **Asset Tags** page appears.
3. Click the + **Add** button.

   The **Asset Tag Templates** page appears, with Template-Based options grouped under **Common** and custom types grouped under **Other**.
4. Do one of the following:

   - To use a pre-configured template, select a template type in the **Common** section (use the **Search** box if needed), click the template row, review the details on the **Add Asset Tag Template** page, and click **Add**.

- To build a custom Asset Tag, select a type in the **Other** section: **Static**, **DNS Name List**, **LDAP Query**, **Combination**, **Dynamic**, or **Import**.

5. On the **Add Asset Tag** page, type a **Name** and, optionally, a **Description**, then complete the fields specific to the selected type – for example, IP addresses for a Static Asset Tag, or rule-based condition statements for a Dynamic Asset Tag.

6. Click **Submit**.

   Tenable Security Center saves the Asset Tag and adds it to the **Asset Tags** list.

What To Do Next

Use the new Asset Tag as a scan target, or view its details as described in the next section.

View Asset Tag Details

To view asset tag details:

1. On the **Asset Tags** page, right-click the target row, or select its checkbox and choose **View** from the action bar.

2. Click **View**.

   The **View Asset Tag** page appears, showing a **General** section (**Name**, **Description**, **Label**, **IP Addresses per Repository**, **Created**, **Modified**, **Owner**, **Group**, and **ID**) and a **Tenable Synchronization Data** section (synchronization status with Tenable Lumin).

> **Note:** The **label** field shown on the View Asset Tag page is the same free-form Labels feature described earlier in this topic, not part of the Asset Tag's typed definition.

Asset Tags and Tenable One Synchronization

By default, Asset Tags stay local to your Tenable Security Center instance. If your organization holds a Tenable Lumin or Tenable One license, you can optionally enable **Tenable One Synchronization** to send eligible Asset Tag and vulnerability data from Tenable Security Center into Tenable One Vulnerability Management, where it appears as tags — and from there can flow into Tenable One as Business Context using the same mechanism as native Tenable One Vulnerability Management Tags. See Cross-Product Tag Behavior for that downstream flow.

Tenable One Synchronization has the following scope and requirements:

- Only **IPv4 addresses within Static and Dynamic Asset Tags** are eligible. DNS Name List, LDAP Query, Combination, and Import Asset Tags are not synchronized.
- Requires a Tenable Lumin or Tenable One license and Tenable One Vulnerability Management API credentials (an Access Key and Secret Key) with Administrator permissions.
- You cannot synchronize a Tenable Security Center Director instance. Only managed, standalone Tenable Security Center instances are supported.
- Synchronized repositories must have unique names across instances, or the synchronization fails.
- Assets that count toward your Tenable Security Center license also count toward your Tenable One Vulnerability Management license once synchronized.
- Sending data to Tenable One Vulnerability Management does not remove it from Tenable Security Center — your original Asset Tags and scan data remain intact.

> **Note:** The free-form Labels feature never synchronizes, regardless of whether Tenable One Synchronization is configured.

Removing or Deleting an Asset Tag

To delete an asset tag:

1. On the **Asset Tags** page, right-click the target row, or select its checkbox and choose an action from the action bar.
2. Click **Delete**.

   Tenable Security Center prompts you to confirm.
3. Click **Delete** to confirm.

   Tenable Security Center removes the Asset Tag. Scans, policies, or dashboards that targeted the deleted Asset Tag no longer resolve that target.

Caution: Deleting an Asset Tag that is used as a scan target removes that target from any scan configured to use it. Coordinate deletions with scan and dashboard owners before proceeding.

Asset Tags vs. Tags – Comparison

Aspect	Tenable Security Center Asset Tags	Tenable One Vulnerability Management Tags
Structure	Typed asset list (Static, DNS Name List, LDAP Query, Combination, Dynamic, Import, or Template-Based)	Category:Value pair
Automation	Dynamic and Combination types update automatically; the remaining types are manual lists	Manual or rule-based (dynamic)
Applies to	Assets only	Assets only
Shared across users	Yes – per local security policy	Tag-level Can View / Can Edit permissions
Flows to	Partially – only via optional Tenable One	Yes (as Business

Aspect	Tenable Security Center Asset Tags	Tenable One Vulnerability Management Tags
Tenable One	Synchronization (IPv4 addresses in Static and Dynamic Asset Tags only, requires a Tenable Lumin or Tenable One license)	Context)
Maximum	No documented limit per instance	100 categories; 100,000 values per category
Export	Export and Import Asset Tag files	CSV or JSON from Settings → Tagging
Permissions model	Shared with specific users per local security policy	Tag-level Can View / Can Edit permissions

Asset Tags in Tenable Security Center Director

Tenable Security Center Director is a multi-console management layer that provides a centralized view and control plane across multiple Tenable Security Center instances. Tenable Security Center Director is itself an on-premises deployment and shares the same Asset Tag functionality as a standard Tenable Security Center installation.

- Asset Tags configured within Tenable Security Center Director itself are **local to that Director instance** and are not pushed down to managed Tenable Security Center consoles.
- Asset Tags on individual managed Tenable Security Center consoles remain local to those consoles and do not aggregate up to Tenable Security Center Director.

- You cannot enable Tenable One Synchronization on a Tenable Security Center Director instance itself. Individual managed Tenable Security Center instances can still be synchronized on their own.

If your organization uses Tenable Security Center Director to manage multiple Tenable Security Center deployments, maintain consistent Asset Tag naming and type conventions across all consoles manually. Because Asset Tags are not shared across consoles, a tag created in one managed Tenable Security Center instance is invisible to Tenable Security Center Director and to other managed Tenable Security Center instances.

> **Note:** Tenable Security Center Director API access for Asset Tag management follows the same pattern as the Tenable Security Center REST API, targeting the Director host. See Tagging via API for details.

Additional Resources

- Asset Tags in the Tenable Security Center User Guide
- Manage Asset Tags in the Tenable Security Center User Guide
- Tenable One Synchronization in the Tenable Security Center User Guide
- Labels in the Tenable Security Center User Guide

Tagging via API

Tenable exposes tag management endpoints for Tenable One Vulnerability Management, Tenable One, and Tenable One Attack Surface Management through the Tenable REST API. Automation via the API lets you integrate tag management into CI/CD pipelines, CMDB synchronization workflows, and scripted bulk operations that would be impractical through the UI.

The base URL for all Tenable cloud API calls is `https://cloud.tenable.com`. All requests require an `X-ApiKeys` authentication header.

```
X-ApiKeys: accessKey=<access_key>;secretKey=<secret_key>
```

Generate API keys under **Settings → My Account → API Keys** in Tenable One Vulnerability Management.

Full interactive reference documentation is available at developer.tenable.com/reference.

> **Note:** Tenable Security Center uses a separate on-premises API. Tenable Security Center Asset Tags are managed via the Security Center REST API documented at docs.tenable.com/security-center. Tenable Security Center Director shares the same API surface as Tenable Security Center but targets the Director host.

Tenable One Vulnerability Management – Tags API

The Tenable One Vulnerability Management Tags API uses a two-tier model: **categories** and **values**. Create the category first, then create one or more values within it. Tag rules (for dynamic tags) are defined as part of the tag value.

Required role: Scan Manager [40] or higher for create/update/delete operations. Standard users can read.

Category Endpoints

Operation	Method	Endpoint
Create tag category	`POST`	`/tags/categories`
List tag categories	`GET`	`/tags/categories`
Get category details	`GET`	`/tags/categories/{category_uuid}`
Update tag category	`PUT`	`/tags/categories/{category_uuid}`
Delete tag category	`DELETE`	`/tags/categories/{category_uuid}`

Create category — example request body:

```
{
  "name": "Environment",
  "description": "Deployment environment classification"
}
```

Create category — example response (truncated):

```
{
  "uuid": "a1b2c3d4-...",
  "name": "Environment",
  "description": "Deployment environment classification",
  "created_at": "2026-01-15T10:00:00Z",
  "updated_at": "2026-01-15T10:00:00Z"
}
```

> **Caution:** Deleting a category is irreversible. It removes the category and all associated values from every asset in your instance. The UUID of a deleted category cannot be reused.

Tag Value Endpoints

Operation	Method	Endpoint
Create tag value	`POST`	`/tags/values`
List tag values	`GET`	`/tags/values`
Get tag value details	`GET`	`/tags/values/{value_uuid}`
Update tag value	`PUT`	`/tags/values/{value_uuid}`
Delete tag value	`DELETE`	`/tags/values/{value_uuid}`
Bulk delete tag values	`POST`	`/tags/values/delete`

Create a static (manual) tag value — example request body:

```
{
  "category_uuid": "a1b2c3d4-...",
  "value": "Production",
  "description": "Production environment assets",
  "type": "static"
}
```

Create a dynamic tag value with rules — example request body:

```
{
  "category_uuid": "a1b2c3d4-...",
  "value": "AWS-Production",
  "description": "Auto-tag AWS production assets",
  "type": "dynamic",
  "filters": {
    "asset": {
      "and": [
        {
          "field": "aws_region",
          "operator": "eq",
          "value": "us-east-1"
        },
        {
          "field": "sources",
          "operator": "eq",
          "value": ["AWS"]
        }
      ]
    }
```

```
  }
}
```

Asset Tag Assignment Endpoints

Operation	Method	Endpoint
List tags for an asset	`GET`	`/assets/{asset_uuid}/tags`
Add or remove asset tags	`POST`	`/tags/assets/assignments`
List asset tag filters	`GET`	`/tags/filters/assets`
List tag exclusions	`GET`	`/tags/exclusions`

Add or remove tags from assets — example request body:

```
{
  "action": "add",
  "assets": [
    { "id": "asset-uuid-1" },
    { "id": "asset-uuid-2" }
  ],
  "tags": [
    { "id": "value-uuid-1" }
  ]
}
```

Set `"action"` to `"remove"` to remove the specified tags from the specified assets.

> **Note — API/UI Filter Divergence:** The `GET /tags/filters/assets` endpoint (V1) does not return every filter type available in the Tagging UI, including cloud resource tag filters (**Resource Tags (By Key)** and **Resource Tags (By Value)**). If a filter you rely on in the UI is missing from this endpoint's response, build or verify that rule through the UI rather than assuming API parity.

Recommended API Workflow

To create and assign a tag via the API:

1. Call `GET /tags/categories` to retrieve existing categories and their UUIDs.
2. If the category doesn't exist, call `POST /tags/categories` to create it. Note the returned `uuid`.
3. Call `POST /tags/values` with the category UUID to create the tag value, specifying `type: "static"` or `type: "dynamic"`.
4. For static tags, call `POST /tags/assets/assignments` to assign the tag to specific assets by their UUIDs.
5. For dynamic tags, the rules engine evaluates asset membership automatically – no manual assignment step is required.

Tenable One – Tags API

The Tenable One Inventory API provides endpoints to search and inspect tags within the Tenable One platform. These endpoints work across all tag sources visible in Tenable One – Tenable One Vulnerability Management tags, Tenable One native tags, and External Tags.

Required role: Any authenticated Tenable One user can read. Tag creation and management for Tenable One Tags is done through the Tenable One Vulnerability Management Tags API (above) or the Tenable Exposure Management UI.

Operation	Method	Endpoint
Search tags	`POST`	`/inventory/tag/search`
List tag properties	`GET`	`/inventory/tag/properties`

Search tags – example request body:

```
{
  "query": {
    "field": "tag.category",
    "operator": "eq",
    "value": "Environment"
  },
  "limit": 100,
  "offset": 0
}
```

Use `GET /inventory/tag/properties` to discover the queryable fields and their valid operators before building search queries.

> **Note:** The Tenable One Tags API is read-oriented. To create or modify tags that appear in Tenable One, use the Tenable One Vulnerability Management Tags API or the Tenable Exposure Management UI. External Tags (from Cloud Security, Identity Exposure, or third-party integrations) cannot be created or modified via the Tenable developer API.

Tenable One Attack Surface Management – Tags API

The Tenable One Attack Surface Management Tags API uses a different model from the Tenable One Vulnerability Management Tags API. Tenable One Attack Surface Management tags (referred to internally as "portfolios") have a **name** and a **value type** – they are not structured as Category:Value pairs. Tags are managed globally within an inventory and can be assigned to assets individually or in bulk using filters.

Base URL for Tenable One Attack Surface Management API calls: `https://cloud.tenable.com` (same host, different path prefixes).

Operation	Method	Endpoint
Get all tags from store	GET	/asm/v1/portfolios
Add a new tag	POST	/asm/v1/portfolio/create
Edit tag by ID	POST	/asm/v1/portfolio/edit
Delete tag from store	POST	/asm/v1/portfolio/delete
Search tags by name	POST	/asm/v1/portfolio/search
Add assets to tags	POST	/asm/v1/portfolios/assets/add
Remove assets from tags	POST	/asm/v1/portfolios/assets/remove
Add assets to tags (by filter)	POST	/asm/v1/portfolios/assets/add/filter
Remove assets from tags (by filter)	POST	/asm/v1/portfolios/assets/remove/filter

Create an Tenable One Attack Surface Management tag – example request body:

```
{
  "name": "Business Unit",
  "type": "keyword"
}
```

Valid `type` values are: `no_value`, `keyword`, `number`, `cost`, `percentage`, `boolean`.

Add assets to a tag using a filter – example request body:

```
{
  "portfolio_ids": ["tag-uuid-1"],
  "inventory_id": "your-inventory-uuid",
  "filter": {
```

```
    "field": "domain",
    "type": "contains",
    "value": "example.com"
  }
}
```

Caution: Deleting an Tenable One Attack Surface Management tag via `/asm/v1/portfolio/delete` removes the tag *and all its associations* from every asset across the inventory. This operation cannot be undone.

Tenable One Attack Surface Management API Authentication

The Tenable One Attack Surface Management API supports two authentication methods:

- **Tenable API keys** – Use the same `X-ApiKeys` header as the Tenable One Vulnerability Management API, if your Tenable One Attack Surface Management instance is linked to a Tenable cloud account.
- **Bearer token** – Some Tenable One Attack Surface Management API calls use an `Authorization: Bearer <token>` header. Obtain the token via the Tenable One Attack Surface Management login endpoint.

Refer to the Tenable One Attack Surface Management API reference for the authentication method applicable to each endpoint.

Tenable Security Center – Asset Tags API

Tenable Security Center provides a REST API for managing its resources, including Asset Tags. Asset Tags are managed as `asset` resources – the same endpoint family used for the typed asset lists described in Tags in Tenable Security Center.

Host: Your on-premises Tenable Security Center hostname (for example, `https://sc.example.com`).

Authentication: Tenable Security Center uses session-based authentication via `POST /rest/token` or API key authentication (Tenable Security Center 5.13+) via the `X-APIKey` header.

To create a Static Asset Tag, use the following request.

```
POST /rest/asset
{
  "name": "PCI-Scope",
  "type": "static",
  "definedIPs": "10.0.0.0/24"
}
```

To create a Dynamic Asset Tag, supply rule-based condition statements instead of a fixed IP list.

```
POST /rest/asset
{
  "name": "PCI-Scope-Dynamic",
  "type": "dynamic",
  "rules": [
    { "filterName": "ip", "operator": "=", "value": "10.0.0.0/24" }
  ]
}
```

Other supported `type` values include `dnsname`, `ldapquery`, `combination`, and `upload` (Import Asset Tags). Update an existing Asset Tag with `PATCH /rest/asset/{id}`, remove one with `DELETE /rest/asset/{id}`, and recalculate a Dynamic or LDAP Query Asset Tag's membership on demand with `POST /rest/asset/{id}/refresh`.

Full Tenable Security Center REST API documentation is available at docs.tenable.com/security-center.

> **Note:** Tenable Security Center Director uses the same REST API surface as Tenable Security Center, targeting the Director host. Asset Tag management via API against Tenable Security Center Director follows the same pattern described above.

Tenable Security Center – Labels API

Tenable Security Center also has a separate, unrelated Labels feature – a free-form descriptor you can set on an asset, scan policy, credential, or query. Labels are managed through object-level endpoints – you set the label when creating or updating an object, rather than through a dedicated labels endpoint.

Labels are set via the `tags` field on the relevant object. For example, to set a label on an asset, use the following request.

```
PATCH /rest/asset/{id}
{
  "tags": "PCI-Scope"
}
```

And to set a label on a scan policy, use the following request.

```
PATCH /rest/policy/{id}
{
  "tags": "PCI-Scope"
}
```

Labels are stored as plain strings. Each object supports a single label string. To retrieve objects by label, use the `filter` query parameter.

```
GET /rest/asset?filter=tags%3APCI-Scope
```

To retrieve the full list of unique Labels in use, use `GET /rest/asset/tag`.

> **Note:** Label management via API against Tenable Security Center Director follows the same pattern described above, targeting the Director host.

Additional Resources

For the complete API reference, see developer.tenable.com/reference/navigate.

Cross-Product Tag Behavior

Tags created in one Tenable product can influence how assets appear, are scored, and are governed in other Tenable products, but the direction of flow matters. This topic explains how tags move across the Tenable platform, what capabilities they carry at each layer, and where the boundaries are.

How Tenable One Vulnerability Management Tags Flow into Tenable One

Tags created in Tenable One Vulnerability Management (cloud) automatically synchronize into Tenable One and appear as **Business Context** segments in Tenable One dashboards and Tenable Exposure Management.

1. A tag value is created in Tenable One Vulnerability Management (manually or via a dynamic rule).
2. Assets that match the tag are grouped under that Category:Value pair.
3. On the next sync cycle, the tag and its asset membership propagate to Tenable One.
4. In Tenable One, each tag value becomes a Business Context segment with its own Cyber Exposure Score, Asset Exposure Score, Asset Criticality Rating distribution, and remediation maturity score.

Note: Tenable Security Center Asset Tags do not automatically flow into Tenable One, because Tenable Security Center is on-premises and operates independently. If your organization holds a Tenable Lumin or Tenable One license, you can enable Tenable One Synchronization to send IPv4 addresses within Static and Dynamic Asset Tags into Tenable One Vulnerability Management as tags, which then flow into Tenable One as Business Context using the mechanism described above. DNS Name List, LDAP Query, Combination, and Import Asset Tags are not eligible for synchronization, and Tenable Security Center's free-form Labels never sync. See Tags in Tenable

Security Center for details. Without Tenable One Synchronization configured, only the Tenable One Vulnerability Management portion of a hybrid deployment contributes to Business Context in Tenable One.

Business Context in Tenable One

Within Tenable One, each tag value from Tenable One Vulnerability Management becomes a scoped view of your risk posture. For each tag, Tenable One calculates:

- **Cyber Exposure Score** (0–1000) — overall exposure score for assets with that tag
- **Asset Exposure Score** (0–1000) — asset-level risk weighting
- **Asset Criticality Rating** (1–10) — asset criticality within the tag segment
- **Vulnerability Priority Rating** (0.1–10.0) — vulnerability exploitability weighting
- **Assessment Maturity** (grades A–F) — how thoroughly assets in the segment are being scanned
- **Remediation Maturity** (grades A–F) — how effectively vulnerabilities in the segment are being closed

These per-tag scores let security leaders benchmark different business units, environments, or compliance scopes against each other — for example, comparing the Cyber Exposure Score of your production environment tag against your development environment tag.

Tip: Plan your tag taxonomy before creating tags, because each tag value becomes a standalone Business Context segment. Avoid creating one tag per individual team member or ephemeral asset group — focus on durable, reportable segments such as Business Unit, Environment, or Compliance Scope.

Tag-Scoped Risk Metrics

Metric	Range	Meaning
Cyber Exposure Score	0–1000	Overall cyber exposure for the tag segment (lower is better; 0 = no exposure)
Asset Exposure Score	0–1000	Asset exposure weighting — combines Asset Criticality Rating and Vulnerability Priority Rating
Asset Criticality Rating	1–10	Asset criticality based on device type, internet exposure, and other signals (higher = more critical)
Vulnerability Priority Rating	0.1–10.0	Vulnerability exploitability and threat context (higher = more urgent to remediate)
Assessment Maturity	A–F	Scan coverage and frequency for assets in the segment (A = best coverage)
Remediation Maturity	A–F	Speed and thoroughness of remediation activity in the segment (A = fastest remediation)

Tags in Tenable Exposure Management

Tenable Exposure Management presents three tag types: **Tenable One Tags** (native, fully editable), **Tenable One Vulnerability Management Tags** (read-only), and **External Tags** (from Cloud Security, Identity Exposure, or third parties — asset-level only). See Tags in Tenable Exposure Management for the full capability comparison.

The data flow from Tenable One Vulnerability Management into Tenable Exposure Management follows five steps.

1. Tags and asset data are ingested from Tenable One Vulnerability Management into Tenable One.
2. Tag membership is applied to assets in the Tenable One inventory.

3. Risk scores (Cyber Exposure Score, Asset Exposure Score, Asset Criticality Rating) are calculated per tag segment.
4. Tags appear in Tenable Exposure Management Inventory, where they can filter assets and scope Exposure View Cards.
5. Dashboard widgets reflect tag-scoped data within up to 24 hours of membership changes.

Only **Tenable One Tags** support Dashboard filtering in Tenable Exposure Management. Tenable One Vulnerability Management Tags and External Tags cannot be used as Dashboard-level filters.

Using Risk Scores as Tag Rule Filters

When your Tenable One Vulnerability Management instance has an active Tenable One license, Asset Criticality Rating and Asset Exposure Score become available as tag rule filter inputs. This creates a feedback loop: risk scores drive tag membership, and tags drive access control and reporting.

For example, a tag rule built on the Asset Criticality Rating and Asset Exposure Score filters — expressed in the rule builder as `ACR ≥ 8 AND AES ≥ 650` — automatically tags the highest-risk, highest-exposure assets in your environment. As scores change over time — assets become more critical, new vulnerabilities are discovered, patches are applied — tag membership updates automatically on the next rule evaluation cycle.

> **Note:** Asset Criticality Rating values are recalculated every 24 hours. Allow up to 24 hours after an asset's first scan for its Asset Criticality Rating to appear, and then the tag rule evaluates on its next processing cycle.

Cross-Product Behavior Summary

The following table summarizes tag capabilities across products. **Tenable One Tags** refers to tags created natively in Tenable Exposure Management; **Tenable One Vulnerability Management Tags** refers to tags created in Tenable One Vulnerability Management that sync to Tenable One; **Tenable**

Security Center Asset Tags refers to on-premises Tenable Security Center's typed asset-grouping Asset Tags; **External Tags** refers to third-party tags surfaced in Tenable Exposure Management; **Tenable One Attack Surface Management Tags** refers to tags within Tenable One Attack Surface Management.

Capability	Tenable One Vulnerability Management Tags	Tenable One Tags	External Tags (Tenable Exposure Management)	Tenable Security Center Asset Tags	Tenable One Attack Surface Management Tags
Structured Category:Value	Yes	Yes	Varies by source	No (typed asset list)	No (name + value type)
Dynamic rules engine	Yes	Yes	No	Yes – Dynamic and Combination Asset Tags	No
Flows to Tenable One	Yes	Native	Not applicable (already in Tenable Exposure Management)	Partially – via optional Tenable One Synchronization (IPv4 Static/Dynamic Asset Tags only, requires a Tenable Lumin or	No

Capability	Tenable One Vulnerability Management Tags	Tenable One Tags	External Tags (Tenable Exposure Management)	Tenable Security Center Asset Tags	Tenable One Attack Surface Management Tags
				Tenable One license)	
Business Context / Cyber Exposure Score per tag	Yes	Yes	No	No	No
Exposure View Card scoping	Yes	Yes	No	No	No
Dashboard filtering (Tenable Exposure Management)	No	Yes	No	No	No
Inventory search / filter	Yes (Tenable Exposure Management, Tenable One	Yes	Yes (Tenable Exposure Management inventory)	Yes (Tenable Security Center only)	Yes (Tenable One Attack Surface Management only)

Capability	Tenable One Vulnerability Management Tags	Tenable One Tags	External Tags (Tenable Exposure Management)	Tenable Security Center Asset Tags	Tenable One Attack Surface Management Tags
	Vulnerability Management)				
Role-based access control / access group scoping	Yes (Tenable One Vulnerability Management + Tenable Exposure Management)	Yes	No	Shared with specific users per local security policy	No
API management	Yes (REST API)	Yes (via Tenable One Vulnerability Management API)	No (source system)	Yes (Tenable Security Center REST API — `asset` resource)	Yes (Tenable One Attack Surface Management REST API)

Best Practices

Naming Conventions

A consistent naming convention reduces confusion, prevents duplicate categories, and ensures tags render predictably in Tenable One dashboards and asset filters.

- Use **Title Case** for both category and value — for example, `Business Unit:Cloud Platform`, not `business unit:cloud platform`.
- Keep categories **generic and reusable**. One `Location` category with many values is better than dozens of one-off categories.
- Avoid vague category names like `Misc` or `Other`. If you cannot clearly describe what the category means, reconsider the structure.
- Do not repeat the category name inside the value. `Location:East Coast` is correct; `Location:Location-East Coast` is redundant.
- For compliance scopes, prefix the value with the standard — for example, `Compliance:PCI-DSS`, `Compliance:HIPAA`.
- Establish an approved taxonomy document before tagging begins to prevent drift over time.
- Use the **Category Description** and **Value Description** fields when creating tags. These descriptions are visible to all users and improve discoverability.

Tag Rule Design

- Prefer **specific attributes** over broad patterns. Use CIDR ranges, exact OS names, or CPE strings rather than partial-match wildcards wherever possible.
- Use **trailing wildcards** (`Ubuntu*`) rather than leading wildcards (`*Ubuntu`). Leading wildcards force a full-index scan and degrade performance significantly.

- Combine a **restrictive primary filter** (such as an IP range or AWS Region) with secondary qualifiers (such as `Source = Nessus Scan`) to keep rule scope predictable.
- If a rule returns too many assets for the engine to process, it fails silently. Split large rule sets into two or more tags, then join them using a **nested Tags filter**.
- After creating a dynamic tag, monitor the **Assessment** column in the Values tab. Any status other than *Completed* means the engine is still processing or has encountered an error.
- Avoid building rules with more than **20 complex conditions** even though the system limit is 40. Complex rules are harder to troubleshoot and slower to evaluate.
- Use **Resource Tags (By Key)** and **Resource Tags (By Value)** filters to mirror cloud-native tagging from AWS, Azure, or GCP into Tenable One Vulnerability Management automatically — no manual effort required when cloud teams apply tags.

Cross-Product Tagging Strategy

- Define your **Business Context hierarchy** in Tenable One before creating tags. Decide which tag categories (such as `Business Unit`, `Location`, `Compliance`) will appear as Business Context segments in Tenable One dashboards.
- Each Business Context in Tenable One corresponds to one tag value in Tenable One Vulnerability Management. Create **one tag per reportable unit**, not one tag per individual team member or sub-team.
- Tags are native to **Tenable One Vulnerability Management (cloud)**. Tenable Security Center Asset Tags can optionally reach Tenable One through Tenable One Synchronization, but only IPv4 addresses within Static and Dynamic Asset Tags are eligible, and the feature requires a Tenable Lumin or Tenable One license. Account for this in hybrid deployment planning — see Tags in Tenable Security Center.
- When assets migrate between environments (for example, on-premises to AWS), ensure that rule filters using cloud provider attributes will pick them up automatically post-migration.
- For organizations using both Tenable One Vulnerability Management and Tenable Security Center, align Tenable Security Center **Asset Tag names** with your Tenable One Vulnerability

Management tag taxonomy. Static and Dynamic Asset Tags with matching IPv4 scope are the ones eligible for Tenable One Synchronization, so consistent naming makes cross-product Business Context easier to reconcile.

Governance

- Restrict tag **creation permissions** to Scan Managers or Administrators. Basic and Standard users should be able to apply existing tags but should not create new categories without review.
- Review the tag taxonomy **quarterly**. Delete or merge categories that have grown stale or redundant.
- Use the **Export** function (CSV or JSON) to snapshot your tag library before any major structural changes, providing a rollback reference.
- Document the **owner** and **purpose** for each tag category using the Category Description and Value Description fields in the Create Tag UI.
- Coordinate tag **deletions** with report and dashboard owners before proceeding — deleting a category removes it from all assets immediately and can break tag-scoped dashboards or access groups.
- Use the **Permissions** page (*Settings → Access Control → Permissions*) to delegate tag ownership to specific users or groups without granting full Administrator access.
- When a tag is created, Tenable One Vulnerability Management automatically creates *Can Use* and *Can Edit* permissions for the creating user. Administrators can share these permissions with other users or groups as needed.

Examples

The following examples demonstrate common tagging configurations across Tenable One Vulnerability Management and Tenable Security Center.

Example 1 — Auto-Tag by Operating System Family

Tag all Linux assets for separate patch tracking and ownership assignment.

Setting	Value
Category	OS Family
Value	Linux
Tag Type	Automatic

Rule (Match Any):

Filter	Operator	Value
Operating System	contains	Linux

All assets where the detected OS includes the string "Linux" — such as Ubuntu Linux 22.04, Red Hat Enterprise Linux 9, or Debian GNU/Linux — receive the tag automatically. As assets are re-scanned and OS data updates, tag membership updates with them.

Example 2 — Tag AWS Production Assets in a Specific Region

Isolate production assets in the US-East-1 region for compliance reporting and access control.

Setting	Value
Category	Environment
Value	AWS-Prod-US-East

Setting	Value
Tag Type	Automatic

Rule (Match All):

Filter	Operator	Value
AWS Region	is equal to	us-east-1
AWS EC2 Name	contains	prod
Source	is equal to	AWS

This rule catches only EC2 instances in us-east-1 whose name contains "prod," ensuring staging or development instances are excluded from the compliance scope.

Example 3 — Manually Tag Critical Exceptions

Mark assets that are business-critical but exempt from the standard 30-day patch SLA. Because this is a judgment call rather than a rule, a manual tag is appropriate.

Setting	Value
Category	Patch Policy
Value	SLA-Exception
Tag Type	Manual
Value Description	Assets exempt from the standard 30-day patch SLA. Requires CISO approval.

Analysts filter the Assets view by `Patch Policy:SLA-Exception` to see exactly which assets carry the exception. Report owners can use the same tag to build a dedicated dashboard scoped to only those assets.

Example 4 – Mirror Cloud-Native AWS Tags

Your AWS team already tags EC2 instances with an `Owner` key. Bring that context into Tenable One Vulnerability Management automatically without any manual effort.

Setting	Value
Category	Cloud Owner
Value	PlatformTeam
Tag Type	Automatic

Rule (Match All):

Filter	Operator	Value
Resource Tags (By Key)	is equal to	Owner
Resource Tags (By Value)	is equal to	platform-team

Whenever your AWS team assigns `Owner = platform-team` to a new EC2 instance, Tenable One Vulnerability Management picks it up on the next data import and tags the asset automatically.

Example 5 – Tag High-Risk Assets Using Risk Scores

Use Tenable One risk scores as tag rule inputs to automatically identify the highest-risk assets in your environment. **Requires a Tenable One license.**

Setting	Value
Category	Risk
Value	Critical-Tier
Tag Type	Automatic

Rule (Match All):

Filter	Operator	Value
ACR	≥	8
AES	≥	650

Any asset with a high Asset Criticality Rating *and* high Asset Exposure Score receives this tag. Tag membership updates as scores change, making it easy to build dashboards, remediation tickets, or access group restrictions scoped to only the highest-risk assets.

Example 6 — Tenable Security Center Dynamic Asset Tag for PCI Scan Targeting

In Tenable Security Center, create a `PCI-Scope` Dynamic Asset Tag that automatically tracks the assets in scope for quarterly PCI assessments, so scans and reports can target the current PCI population without manual list maintenance.

Before You Begin

- Confirm you have an **Organizational User** role with appropriate permissions.
- Confirm Tenable Security Center has already run an initial discovery scan against the PCI-scope assets.

To create the PCI-Scope dynamic asset tag:

1. Navigate to **Assets** → **Asset Tags**.

   The **Asset Tags** page appears.

2. Click the + **Add** button, then select **Dynamic Asset Tags** in the **Other** section.

   The **Add Asset Tag** page appears.

3. In the **Name** field, type `PCI-Scope`.
4. Define rule-based condition statements that identify the PCI scan population — for example, an IP range filter matching the PCI network segment.
5. Click **Submit**.

   Tenable Security Center saves the `PCI-Scope` Dynamic Asset Tag and begins evaluating matching assets using results from Tenable Security Center scans.

What To Do Next

Target the `PCI-Scope` Asset Tag from a scan policy so quarterly PCI assessments automatically pick up newly added assets. If you also want a lightweight free-text descriptor auditors can search on the scan policy itself, set that policy's separate Label field to `PCI-Scope` as well — see the Tags in Tenable Security Center topic for how Labels and Asset Tags differ.

Troubleshoot Tags

This topic covers the most common reasons a tag doesn't behave as expected in Tenable One Vulnerability Management, and how to resolve each one. For general conceptual questions about tag behavior, see Frequently Asked Questions.

Tags Are Not Applying to Expected Assets

If a dynamic tag was created or updated but one or more assets you expect to see are missing, work through the following checks in order.

Check the Excluded Assets List

When you manually remove a rule-based tag from an asset, Tenable One Vulnerability Management adds that asset to the tag's **Excluded Assets** list. From that point on, the asset is silently exempt from every future rule evaluation for that tag — even if the asset matches the rule again later. Nothing in the standard Assets view distinguishes an excluded asset from one that simply doesn't match the rule, which makes this one of the most frequently missed causes of "my dynamic tag isn't picking up an asset it should."

To check whether an asset is excluded:

1. Call `GET /tags/exclusions` (see Tagging via API) to list the assets currently excluded from a given tag, or inspect the tag icon on the asset — a static (non-dynamic) icon (🏷) indicates a manual override.

   The response returns the asset UUIDs currently excluded from rule evaluation for that tag.

2. To let the rules engine re-evaluate the asset, remove the manually applied tag from it.

   Tenable One Vulnerability Management re-enters the asset into rule-based evaluation on the tag's next processing cycle.

Note: Excluding an asset after a manual removal is expected behavior, not a bug — it exists so that an intentional manual change to a rule-based tag isn't immediately overwritten by the next rule evaluation. See Core Concepts for how manual overrides interact with automatic tags.

Check the Recalculation Schedule

Tenable One Vulnerability Management re-evaluates automatic tag membership only when one of the following occurs:

- You create or edit the tag or its rules (and save).
- A scan or connector import completes and new data is available.
- The 12-hour background sweep runs.

An asset from a scan that completed moments ago may not be tagged yet simply because none of these triggers has run for it. Before assuming a rule is broken, check the **Last Processed** and **Assessment** columns on the Values tab, and allow time for the next scheduled trigger.

Check Whether the Rule Is Too Broad

A rule that matches an extremely large number of assets can fail silently instead of returning an error. See Tags in Tenable One Vulnerability Management for rule limits and guidance on splitting an overly broad rule into two tags joined by a nested tag filter, and avoid leading wildcards, which force a full-index scan.

Tags Filter Assets, Not Findings

Note — Known Limitation: Tags filter the **Assets** view. They do not filter the **Findings** view. There is currently no workaround. If you need to correlate findings with a tagged asset population, filter the Assets view by tag to get the asset list, then cross-reference that list against Findings manually or through the API.

Filtering by Multiple Tags Has a Practical Limit

Note – Known Limitation: Filtering assets by several tags at the same time can produce inconsistent results once the number of tags in the filter grows large. This is a known engineering limitation. If a multi-tag filter returns unexpected results, reduce the number of tags in a single filter and combine the results manually, or use a nested Tags rule condition on a dynamic tag instead of a live multi-tag view filter.

Scan Aborts with "Empty Targets"

If a scan configured to use tags as its target source aborts with an **Empty Targets** error, the tag most likely resolves to assets that have no IPv4 or IPv6 address (for example, FQDN-only assets) and the scan is set to the wrong target mode. See Tag-Based Scanning for the two target modes and which one to use.

Nested Tag Rules Fail Silently in Scan Targeting

A tag rule that nests a Tags filter inside a rule that also contains IPv4, IPv6, or FQDN conditions does not work reliably as a scan target source. See Tag-Based Scanning for the supported rule structure.

API Tag Filters Don't Match the UI

If you're building dynamic tag rules through the API and a filter type you use in the UI (such as a cloud resource tag filter) doesn't appear in the API's filter list, this is a known V1 API limitation. See the note in Tagging via API.

Frequently Asked Questions

This topic answers common conceptual questions about how tagging behaves across Tenable products. If a tag isn't applying, filtering, or scanning the way you expect, see Troubleshoot Tags instead.

My dynamic tag was created but no assets are showing up. What's wrong?

Check the **Assessment** column on the Values tab (**Settings → Tagging → Values**). If it shows anything other than *Completed*, the rules engine is still processing or has encountered an error.

This is the most common tagging support issue, and it almost always traces back to one of three causes: an overly broad rule, a recently scanned asset that hasn't been re-evaluated yet, or an asset sitting on the tag's Excluded Assets list. See Troubleshoot Tags for the full diagnostic steps.

The # of Assets on the Tags page is higher than what I see in the Assets view. Why?

The tag count includes **deleted assets that have not yet aged out** of the license count. Tenable One Vulnerability Management retains deleted asset records until they age out, and the tag engine counts them. The Assets inventory filters out deleted records by default. This is expected behavior and not a bug.

I manually applied a tag that has rules. Will the engine remove the tag if the asset no longer matches?

No. When you manually apply a tag to an asset — even one configured with automatic rules — Tenable One Vulnerability Management **excludes that asset from future rule evaluation** for that

tag. The tag persists until you explicitly remove it, regardless of whether the asset would pass or fail the rule criteria.

This is by design: manual overrides are intentional. If you want the asset to re-enter rule-based evaluation, remove the manually applied tag. The engine will then reassess the asset on its next scheduled run. For how this interacts with the Excluded Assets list, see Troubleshoot Tags.

How long does it take for a new tag rule to apply to all assets?

Processing time depends on system load and the number of assets. In small environments, application is typically complete within minutes. In large environments (hundreds of thousands of assets), it can take longer. Monitor the **Last Processed** and **Assessment** columns on the Values tab to track progress. Do not assume the tag has failed simply because it hasn't completed immediately. For the exact triggers that cause tag membership to recalculate, see Troubleshoot Tags.

Can I use tags to restrict what assets a user can see?

Yes. Tenable One Vulnerability Management's Access Control system uses tags to define access groups. You can grant users *Can View* or *Can Edit* permissions scoped to specific tag values, which restricts their asset visibility to only assets carrying that tag. Configure this under **Settings → Access Control → Permissions**.

When a tag is created, Tenable One Vulnerability Management automatically grants the creating user *Can Use* and *Can Edit* permissions for that tag. Administrators can extend those permissions to other users or groups.

> **Note – Permission Scope Clarification:** Tag-scoped access control restricts which assets a user can *view or edit*. It does not restrict what a user can manually type into a scan target field. A user whose access is scoped to a specific tag can still successfully launch a scan against a manually entered IP address or hostname that falls outside that tag's scope. If you need to prevent out-of-scope scanning,

ombine tag-scoped permissions with scan-level target restrictions. See Tag-Based Scanning for more information.

Note: Tenable One Web App Scanning does not handle permissions that rely on a tag. Access group restrictions based on tags do not apply to Tenable One Web App Scanning assets.

Do Tenable Security Center Asset Tags sync to Tenable One?

Partially, and only if configured. Tenable Security Center is on-premises and does not synchronize with Tenable One by default. If your organization holds a Tenable Lumin or Tenable One license, you can enable Tenable One Synchronization to send IPv4 addresses within Static and Dynamic Asset Tags into Tenable One Vulnerability Management as tags, which then appear as Business Context in Tenable One dashboards the same way native tags do. DNS Name List, LDAP Query, Combination, and Import Asset Tags are not eligible, and Tenable Security Center's separate free-form Labels never sync regardless of configuration. See Tags in Tenable Security Center for setup requirements. If your organization runs a hybrid deployment without Tenable One Synchronization enabled, plan separate tagging strategies for each platform.

I deleted a tag category and now some dashboards are broken. Can I recover?

Deleting a category removes it and all associated tag values from every asset in the system — this cannot be undone from the UI.

If you exported the tag library to CSV or JSON before the deletion, you can re-create the categories and values by importing them via the Tenable API or by manually recreating them in the UI and then re-tagging assets either manually or by recreating the rules.

To prevent this situation in the future: always export the tag library before major changes, and communicate planned deletions to dashboard and report owners in advance.

My tag rule includes a CIDR range but assets outside that range are still tagged. What's happening?

Check whether those assets were **manually tagged** at some point, or whether they were previously removed from the tag and are now sitting on its Excluded Assets list. Both cases exempt an asset from rule evaluation. See Troubleshoot Tags for how to identify and clear each case.

Also verify that your CIDR notation is correct and that no IP address value ends with a period. A /0 mask is not supported and will return a 400 Bad Request error.

Can I tag Web Application assets the same way as host assets?

Partially. Tags apply to all asset types in Tenable One Vulnerability Management, including Web Application assets. However, some rule filters behave differently:

- For Web Application assets, use the **Name** filter — not DNS/FQDN — to match by hostname.
- Tenable One Web App Scanning does not honor permissions that rely on tags, so access group restrictions do not apply to Tenable One Web App Scanning assets.

What is the maximum number of tags I can create?

Tenable One Vulnerability Management supports:

- Up to **100 tag categories** per instance
- Up to **100,000 tag values** per category

For most organizations, this far exceeds what's needed. However, it is worth planning your taxonomy carefully so you do not exhaust the 100-category limit as your program matures — categories cannot currently be merged after they are created.

I created a tag rule based on Asset Criticality Rating but assets with a high Asset Criticality Rating are not being tagged. Why?

Asset Criticality Rating values are recalculated every 24 hours. If the assets were recently scanned for the first time, their Asset Criticality Rating may not yet have been calculated. Allow up to 24 hours after scanning for Asset Criticality Rating values to appear, and then the tag rule will evaluate those values on its next processing cycle (either on data import or during the 12-hour background sweep).

Also confirm that your Tenable One Vulnerability Management instance has an active Tenable One license — Asset Criticality Rating and Asset Exposure Score are not available as tag rule filters without this license.