



Tenable Exposure Management Third-Party Connectors Quick Reference Guide

Last Updated: July 15, 2025



Table of Contents

Welcome to the Tenable Exposure Management Third-Party Connectors Quick Reference Guide	4
Why Integrate	4
What to do next	5
Connectors	6
What is a Connector?	6
Supported Integrations (Connectors)	6
Connectors Guides	7
Ingested Data	7
Interacting with Connector Data in Tenable Exposure Management	7
Resources Within this Guide	8
Supported Third-Party Integrations	8
Security Tools Supported Integrations	8
Asset Inventory Supported Integrations	11
Bug Bounty Supported Integrations	11
Other Integrations	11
Best Practices for Managing and Utilizing Third-Party Integrations	12
Prioritize Endpoint Vulnerabilities	12
Third-Party Data Deduplication in Tenable Exposure Management	19
Why Deduplication Matters	19
How it Works	19
Deduplication Criteria by Asset Class	20
Property Merge Order	21



Deduplication Limitations	22
Additional Resources	22
Asset Retention	22
Configuring Asset Retention	23
Connectors FAQ	24
Integration and Support	24
Sync and Status	24
Deleted Connectors and Tags	25
Asset Deduplication FAQ	27



Welcome to the Tenable Exposure Management Third-Party Connectors Quick Reference Guide

Tenable allows you to ingest data from third-party applications for analyzing with Tenable applications, such as Tenable Exposure Management.

Tenable Exposure Management enables you to:

- Configure and connect third party applications via [Connectors](#).
- Manage these connectors within the Tenable Exposure Management interface.
- View and interact with the data ingested from these connectors including their asset, weakness, and finding data.

This quick-reference guide aims to help you understand how Tenable Exposure Management works with data from third-party connectors, and highlights the best practices to use when managing them.

Important: When using Tenable Exposure Management connectors, Tenable recommends allowlisting the [IP addresses for the region](#) in which the Tenable Vulnerability Management site resides.

Why Integrate

Integrating third-party connectors into Tenable Exposure Management allows you to aggregate and correlate security data across tools and environments – giving your organization a unified, contextualized view of its attack surface. These integrations ingest both asset and vulnerability data from external platforms and combine it with Tenable-native data to support more effective exposure management.

Once the data is ingested, Tenable:

- Aggregates asset and vulnerability data from multiple tools into a single, consolidated inventory.
- Deduplicates and merges data to eliminate noise and ensure each asset is accurately represented.



- Enables cross-platform visibility by linking asset-vulnerability relationships across Tenable and third-party sources.
- Surfaces business context when provided by the source tool. If the third-party platform calculates risk scores or applies business tags, Tenable ingests and displays this information alongside native data to support more informed decision-making.

What to do next

Begin by reading the [Connectors](#) introduction.



Connectors

This quick-reference guide aims to help you understand how Tenable Exposure Management works with data from third-party connectors, and highlights the best practices to use when managing them.

Important: When using Tenable Exposure Management connectors, Tenable recommends allowlisting the [IP addresses for the region](#) in which the Tenable Vulnerability Management site resides.

What is a Connector?

Tenable Exposure Management ingests security and inventory data from existing tools, such as vulnerability scanners, cloud providers, inventory tools, SCA/SAST/DAST, and more.

Connectors are integration modules that allow Tenable Exposure Management to sync with third-party security and inventory tools. They ingest asset and vulnerability data from external platforms and display it alongside Tenable-native data in a single, unified interface.

Supported Integrations (Connectors)

Supported integrations include a variety of asset inventory and security sources from various vendors. These security tools include:

- DAST
- CSPM
- CWPP
- IoT
- Network Scanners
- Endpoint Security
- Bug Bounty
- ASM
- Asset Inventory



Over time, Tenable will continue to add connectors to the **Connectors Library** in Tenable Exposure Management.

For the complete list of supported integrations, see [Connectors and Supported Integrations](#).

Connectors Guides

Each connector has a dedicated guide. These guides are extensive and include all relevant information for configuring a specific connector. The guides are available within the [Exposure Management User Guide](#).

Ingested Data

Tenable Exposure Management ingests assets, weaknesses, and findings from third-party vendors.

- **[Assets](#)**: An asset is any object that represents a part of your organization's attack surface. Assets can be endpoints, apps, cloud resources, code, and more. For the complete list of ingested asset types, see [Asset Classes](#).
- **[Weaknesses](#)**: Weaknesses are vulnerabilities and misconfigurations on your assets. Ingested weaknesses include:
 - Weakness Status
 - Risk Score
- **[Findings](#)**: A finding is a single instance of a vulnerability (weakness or misconfiguration) appearing on an asset, identified uniquely by plugin ID, port, and protocol.

Interacting with Connector Data in Tenable Exposure Management

As connectors ingest asset, vulnerability, and findings data from third-party platforms, Tenable Exposure Management consolidates this information into its unified data model. Once ingested, the data becomes available across the platform—enabling you to view, analyze, and prioritize it alongside Tenable-native data.

See the following topics in the *Tenable Exposure Management User Guide* for more information:

- [View the Connectors page](#)
- [Manage Connectors](#)



Resources Within this Guide

Review the following resources within this guide to familiarize yourself with connector best practices and frequently asked questions:

- [Best Practices for Managing and Utilizing Third-Party Integrations](#)
 - [Prioritize Endpoint Vulnerabilities](#)
 - [Third-Party Data Deduplication in Tenable Exposure Management](#)
 - [Asset Retention](#)
- [Connectors FAQ](#)
 - [Asset Deduplication FAQ](#)

Supported Third-Party Integrations

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

Tenable Exposure Management offers integration with the security tools listed in the table below.

Each supported integration has:

- Every supported integration has a dedicated **Connector** within Tenable Exposure Management with specific configurations.
- Each connector can belong to one or more security data sources.
- Some connectors support inventory only (ingest only assets data), while others support ingesting assets and vulnerability data.

Tip: To learn more, see [Connectors](#).

Important! On connector creation, it can take up to one hour for connector data to appear within Tenable Exposure Management.

Security Tools Supported Integrations

The following connectors ingest both asset and weakness data.



Supported Integration	Connector Name and Documentation	Security Tool Category	Ingested Asset Classes
Acunetix360	Acunetix360 Connector	DAST	Web Application
Acunetix Premium	Acunetix Premium Connector	DAST	Web Application
Armis	Armis Connector	Operational Technology (OT)	Device
AWS Inspector	AWS Inspector Connector	CSPM	Cloud Resource
BitSight	BitSight Connector	DAST	Device, Web Application
Cortex XDR	Cortex XDR Connector	Endpoint Security	Device, Cloud Resource
CrowdStrike	CrowdStrike Connector	Endpoint Security	Device
Cycognito	Cycognito Connector	DAST, ASM	Device, Cloud Resource
Detectify	Detectify Connector	DAST	Web Application
Microsoft TVM	Microsoft TVM Connector	Endpoint Security	Device
Outpost 24	Outpost 24 Connector	DAST, VM, Endpoint Security	Device, Cloud Resource, Web Application
PrismaCloud CWPP	PrismaCloud CWPP Connector	VM	Device



Supported Integration	Connector Name and Documentation	Security Tool Category	Ingested Asset Classes
Purplemet	Purplemet Connector	DAST	Web Application
Qualys	Qualys Connector	VM	Device
Qualys WAS	Qualys WAS Connector	DAST	Web Application
Rapid7 Insight Appsec	Rapid7 Insight AppSec Connector	DAST	Web Application
Rapid7 Insight VM	Rapid7 Insight VM Connector	DAST	Device
Rapid7 InsightVM Cloud	Rapid7 Insight VM Cloud	VM	Device
Red Hat Insights	Red Hat Insights Connector	VM	Device
RiskRecon	RiskRecon Connector	DAST	Web Application
SecurityScorecard	SecurityScorecard Connector	DAST	Web Application
SentinelOne	SentinelOne Connector	Endpoint Security	Device Other
Tanium	Tanium Connector	Endpoint Security	Device
Veracode	Veracode Connector	DAST	Web Application
WhiteHat	WhiteHat Connector	DAST	Web Application
Wiz	Wiz Connector	VM	Device, Cloud Resource
Wiz Configurations	Wiz Configurations Connector	CSPM	Device, Cloud Resource



Supported Integration	Connector Name and Documentation	Security Tool Category	Ingested Asset Classes
Wiz Issues	Wiz Issues Connector	CSPM	Device, Cloud Resource

Asset Inventory Supported Integrations

The following connectors ingest asset data only.

Supported Integration	Connector Name and Documentation	Ingested Asset Classes
AWS EC2	AWS EC2 Connector	Device
Axonius	Axonius Connector	Device
Microsoft Azure	Azure Connector	Device
Microsoft Intune	Intune Connector	Device
Jamf	Jamf Pro Connector	Device
ServiceNow	ServiceNow Connector	Device

Bug Bounty Supported Integrations

The following connectors ingest bug bounty data.

Supported Integration	Connector Name and Documentation	Category
HackerOne	HackerOne Connector	Bug Bounty

Other Integrations

Supported Integration	Connector Name and Documentation	Category
Tenable On-Prem	Tenable On-Prem Connector	On-Prem



Best Practices for Managing and Utilizing Third-Party Integrations

Tenable Exposure Management enables you to unify, contextualize, and act on security data across your entire environment, including data from assets and vulnerabilities ingested from third-party integrations.

Important: When using Tenable Exposure Management connectors, Tenable recommends allowlisting the [IP addresses for the region](#) in which the Tenable Vulnerability Management site resides.

This series of best practices provides structured guidance for using third-party data effectively within Tenable Exposure Management.

By following these best practices, you can:

- Consolidate asset visibility across multiple data sources.
- Prioritize vulnerabilities with greater accuracy.
- Strengthen your organization's risk insights.
- Accelerate remediation efforts by leveraging integrated context.

Prioritize Endpoint Vulnerabilities

Managing endpoint exposure requires clear, unified visibility across environments and security domains. Within Tenable Exposure Management, you can consolidate asset inventory, vulnerability intelligence, configuration data, and identity signals into a single, actionable risk view.

- This guide shows you how to prioritize endpoint vulnerabilities by following a structured process.
- The examples in this guide use the [CrowdStrike Connector](#), however with minor adjustments this process can be used for any third party connector.
- If you are a Tenable Vulnerability Management customer, your custom asset tags – such as combinations of operating system and device type – automatically synchronize into Tenable Exposure Management.



- For endpoints that only exist in third-party connectors like the [CrowdStrike Connector](#), you can create [custom tags](#) (for example, `Source = CrowdStrike`) and combine them with your existing tags to maintain complete coverage.

By following these best practices — whether using CrowdStrike or any third-party connector — you can unify your asset view, strengthen your risk insights, reduce exposure, and accelerate remediation across your organization.

Step 1: Tenable Exposure Management Identifies and Deduplicates Endpoints

Tenable Exposure Management uses a default merge strategy to identify and combine duplicate assets ingested from multiple sources — including third-party connectors such as CrowdStrike — based on key matching attributes.

Deduplication criteria include:

- Cloud Instance ID
- MAC Addresses
- Hostnames
- External IPs
- Fully Qualified Domain Names (FQDNs)
- IP Addresses

In the CrowdStrike example, the default values for device merging are:

1. `cloud_instance_id`
2. `mac_addresses`
3. `hostname + fqdns + external_ips`
4. `hostname + fqdns`
5. `fqdns + external_ips`






























































6. hostname + external_ips

7. hostname

When Tenable Exposure Management merges assets:

- It automatically applies asset attributes, such as tags, across the merged record.
- You can confirm successful deduplication by checking for multiple icons in the **Sources** column in the [Assets list](#).

Filters	Reset Filters <<		Name	Sources	Class
> Asset classes	1 active	<input type="checkbox"/>	win-vuln-dc	 	 Device
▼ Sources		<input type="checkbox"/>	win-vuln-email	  	 Device
 Tenable Attack Sur... <1%		<input type="checkbox"/>	win-exchange	  	 Device
 Tenable Cloud Secu... 8%		<input type="checkbox"/>	In-demo	 	 Device
 Tenable Container S... 0%		<input type="checkbox"/>	prod-bigfix	 	 Device
 Tenable Identity Ex... 12%		<input type="checkbox"/>	In-dc	  	 Device
 Tenable OT Security 40%		<input type="checkbox"/>	data-dc02	 	 Device
 Tenable Security Ce... 0%		<input type="checkbox"/>	labnetfs	  	 Device
 Tenable Vulnerabili... 53%		<input type="checkbox"/>	ip-172-31-11-196.ec2.inte...	  	 Device
 Tenable Web Applic... 0%		<input type="checkbox"/>	tad-relay	 	 Device
 CrowdStrike Falcon 0%		<input type="checkbox"/>	ex-empire-01	   	 Device
 Microsoft Defender 2%		<input type="checkbox"/>	compnor	 	 Device
 Qualys VMDR 10%		<input type="checkbox"/>	mustafar.tehgeek.local	 	 Device
 SentinelOne Singul... <1%					
 ServiceNow 0%					

Tip: For more information, see [Third Party Data Deduplication](#) in the *Tenable Exposure Management User Guide*.

Step 2: Classify Endpoints Using Pre-Built Tags



Use built-in tagging systems from third-party connectors to classify assets.

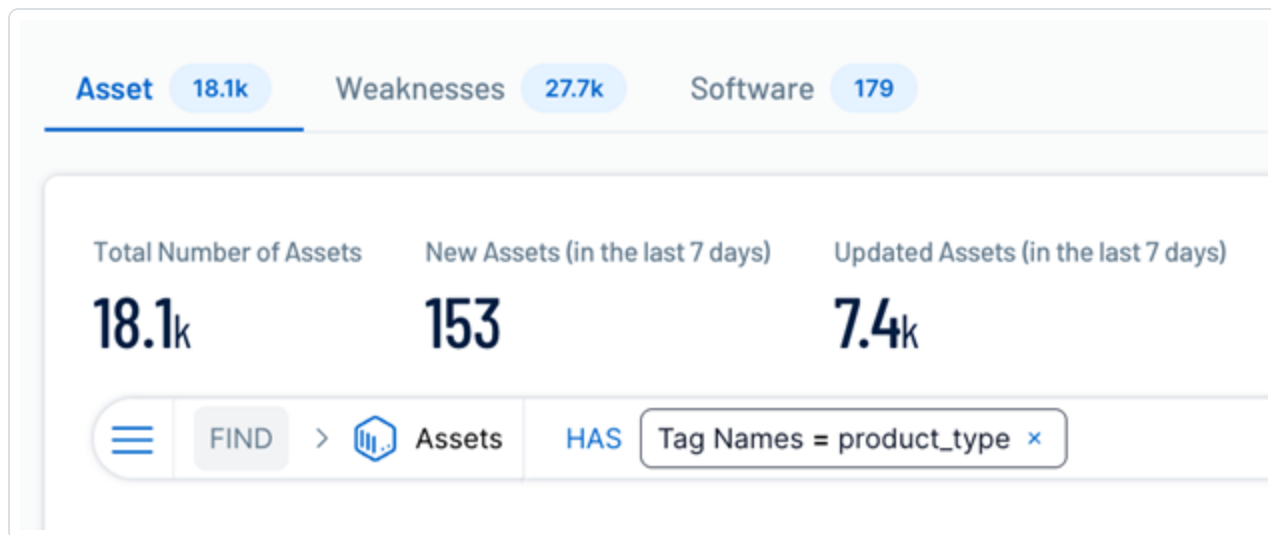
In the CrowdStrike example:

Each asset automatically receives a `product_type` tag, identifying its type (Workstation, Endpoint, or Domain Controller).

To classify your endpoints:

1. Make sure asset deduplication is complete.
2. Filter assets by `product_type:endpoint`.

This gives you a consolidated list of endpoints, regardless of their source.



Important: Many organizations already define asset groups using [Tagging](#). These tags—such as combinations like **Operating System = Windows 10**—synchronize into Tenable Exposure Management automatically. For endpoints detected only through a third-party connector like CrowdStrike, you can create a TenableOne tag (for example, **Source = CrowdStrike**) and combine it with your existing Tenable Vulnerability Management tags to achieve full coverage.

Step 3: Determine Endpoint Owners

Segment your endpoints by ownership or system type using additional tags provided by third-party connectors.

In the CrowdStrike example:

Assets are also tagged with `host_group` to indicate the operating system.



To segment endpoints:

Filter assets using a combination of `product_type:endpoint` and the appropriate `host_group`, such as `host_group:windows`.

This lets you quickly analyze vulnerabilities by platform or asset owner group.

<input type="checkbox"/>	Name	Sources	Class	AES	Weaknesses	Top Attack Techniques	Top Attack Paths	Associated Tags Count	Last Updated
<input type="checkbox"/>	win-smb-01		Device	<div><div></div></div> 987	<div><div></div></div> 4.8%	<div><div></div></div> 1.3%	<div><div></div></div> 1.3%	5	March 15, 2025
<input type="checkbox"/>	win-smb-email		Device	<div><div></div></div> 995	<div><div></div></div> 4.2%	<div><div></div></div> 570	<div><div></div></div> 828	7	March 15, 2025
<input type="checkbox"/>	win-exchange		Device	<div><div></div></div> 989	<div><div></div></div> 1.8%	<div><div></div></div> 478	<div><div></div></div> 648	5	March 15, 2025
<input type="checkbox"/>	in-delta		Device	<div><div></div></div> 984	<div><div></div></div> 1.5%	<div><div></div></div> 824	<div><div></div></div> 347	8	March 15, 2025
<input type="checkbox"/>	prod-logix		Device	<div><div></div></div> 983	<div><div></div></div> 1.8%	<div><div></div></div> 903	<div><div></div></div> 880	8	March 15, 2025

Tip: You can also combine tags from Tenable Vulnerability Management sources for broader coverage.

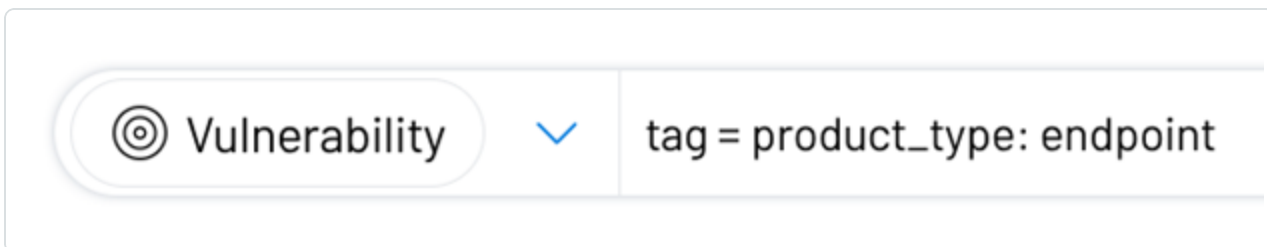
Step 4: Identify Vulnerabilities on Endpoints

Once you have your endpoints identified, you can filter to find associated vulnerabilities.

To view vulnerabilities:

1. Within Tenable Exposure Management, navigate to **Weaknesses**.
2. Apply the following filters:
 - Tag = `product_type:endpoint`
 - Weakness Type = Vulnerability

Tenable Exposure Management displays a full view of vulnerabilities affecting your endpoints.



Step 5: Create Exposure Signals

Create custom **Exposure Signals** to track and monitor endpoint vulnerabilities based on your tagging and segmentation/attributes.



To create an exposure signal:

1. Within Tenable Exposure Management, navigate to **Exposure Signals**.
2. Create a new signal using the relevant filters.

Example:

Create a signal that identifies external-facing endpoints affected by CISA KEV vulnerabilities.

New Exposure Signal

Name
Endpoints with Externally Facing Vulnerabilities on the KEV
Max. 60 characters 59/60

Description [Generate using AI](#)
Exposure signal looking for Endpoints with Externally Facing Vulnerabilities on the KEV. These endpoints may be vulnerable to attack, as they are exposed to the internet and have known vulnerabilities listed on the CISA KEV.

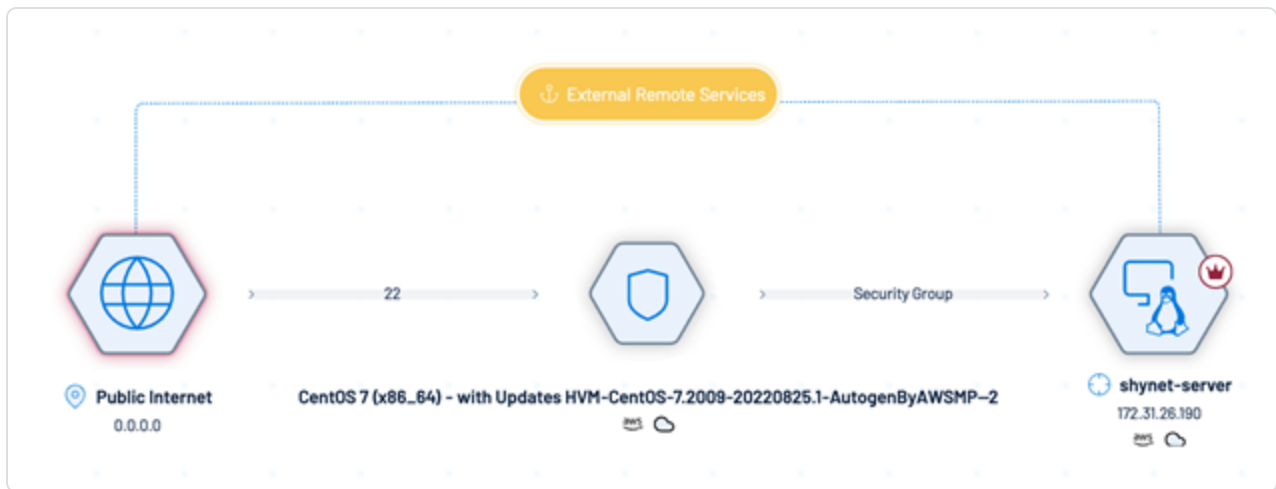
Query builder
Build the query associated to your Exposure Signal and see if it generates any results

FIND > Assets AS Device HAS Tag Names = product_type: endpoints AND Internet Facing = true WITH Weakness HAS CISA KEV Added Date exists

You can also:

- Monitor remediation trends over time.
- Within the **Inventory** view, click **View Graph** to visualize attack paths.

	View Graph	Name	Path Priority Rating	Nodes	Actions
>		An External Asset ec2amaz-64tssl9 Gains Initial Access to win-vuln-dc by Exploiting CVE-2018-8...	Critical		
>		ec2amaz-64tssl9 reaches win-vuln-dc through CVE-2021-3060	Critical		



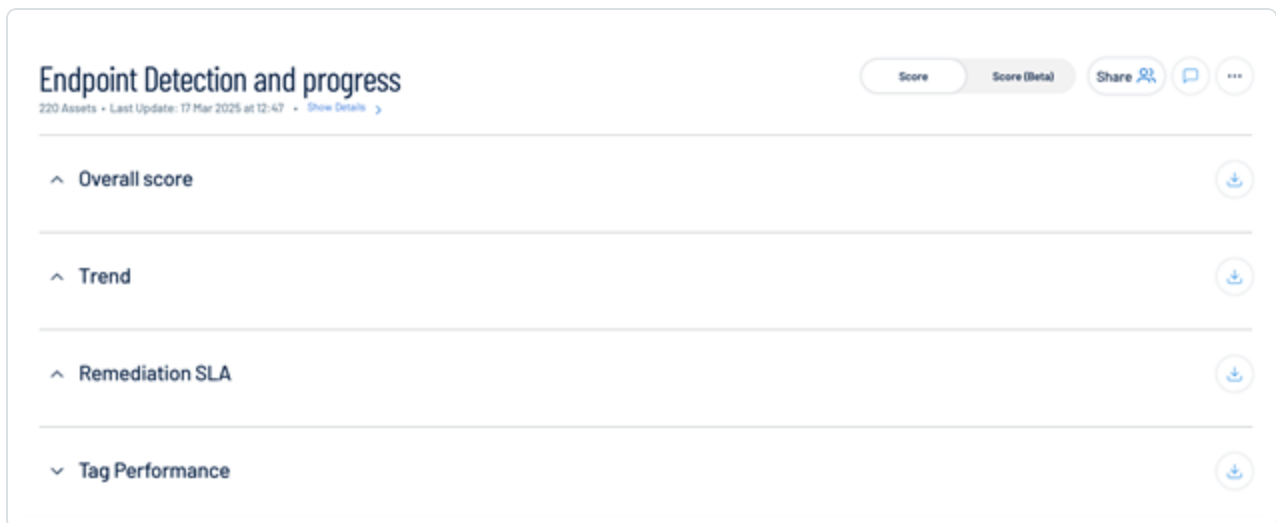
- Filter by **Asset ID** to examine risks such as ransomware exposure, toxic combinations, and compromised credentials.

Step 6: Prioritize Vulnerabilities Using Tenable Scores and Attributes

Use the **Exposure View** to prioritize risk across your assets.

To prioritize endpoint vulnerabilities:

- Segment assets using tags like `product_type:endpoint` and `host_group:windows`.
- Create a custom card, such as **Endpoint Detection and Progress**, to monitor scores, trends, and SLA performance for your endpoint group.



You can adjust targets based on your:



- Business needs
- Team capacity
- Regulatory and compliance requirements

Step 7: Share Insights with Stakeholders

You can monitor progress, generate reports, and share insights using customizable dashboards in Tenable Exposure Management.

- Export dashboards or data for executive reporting.
- Share tailored views with stakeholders to track remediation efforts.

Third-Party Data Deduplication in Tenable Exposure Management

Tenable Exposure Management consolidates asset and vulnerability data from both Tenable products (1st party) and third-party integrations to provide a unified, accurate asset inventory. When duplicate assets are ingested from different sources, Tenable automatically applies deduplication logic to merge records into a single asset view.

This guide explains how deduplication works for third-party data, how the system prioritizes conflicting values, and where users can view this information in the platform.

Why Deduplication Matters

Merging duplicate assets improves clarity, reduces noise, and enables more accurate risk assessment. In Tenable Exposure Management, deduplication happens automatically across sources, giving you:

- A single source of truth for each asset.
- Complete visibility into merged properties from all integrated platforms.

How it Works

Tenable Exposure Management achieves asset deduplication by crossing complex merge criteria and identifying duplications across the data ingested from the different sources.



The merging mechanism is designed to avoid disassembling and reassembling Tenable Exposure Management assets. If the merging criteria are met, new data is added to the existing structure.

Note: At this stage, Tenable Exposure Management uses a predefined merge strategy and property matching logic. Customization of merge rules is not currently available, but enhancements are planned for future releases.

Assets that are deduplicated and merged are considered **Multi Source Assets**. For more information, see [View License Information](#) in the *Tenable Vulnerability Management User Guide*.

Deduplication Criteria by Asset Class

Tenable applies a default merge strategy per asset class, using key properties to match and merge assets. The deduplication logic is case-insensitive and includes parsing of common formats (e.g., MAC addresses, hostnames).

Tip: For more information, see [Asset Classes](#).

Asset Class	Default Merge Properties (in order of priority)
Device	<ol style="list-style-type: none">1. External Identifier2. Mac Addresses3. Name + FQDNs + IP Addresses4. Name + FQDNs5. FQDNs + IP Addresses6. Name + IP Addresses7. Name
Container	<ol style="list-style-type: none">1. sha2562. name
Web Application	<ol style="list-style-type: none">1. Webapp Homepage Screenshot Url2. Name
Cloud	External Identifier



Account	
Role	
Group	
Storage	
Resource	
Other	

Important! The merge criteria listed in this document apply only to third-party data (data ingested from [Connectors](#)).

Tenable-native assets, such as the data that comes from Tenable Vulnerability Management, follow separate internal deduping logic.

Important! Assets with different Tenable UUIDs will never be merged, even if all other third-party matching criteria are met. This safeguards the integrity of Tenable-managed assets and prevents unintended merges.

Property Merge Order

When multiple sources provide different values for the same property (for example, conflicting IP addresses or operating systems), Tenable uses a fixed priority order to determine which value appears in the unified [Assets](#) view.

Default Merge Priority

1. Tenable-native sources (such as Tenable Vulnerability Management) take precedence.
2. Third-party [Connectors](#) are prioritized by the order they were connected. The first connected source is used unless its value is missing, in which case the next available source is used.

Note: The order of connectors influences the merging process. The first connector that completes processing within Tenable Exposure Management determines the identifying criteria.

Example

An asset is discovered by:



- Tenable Vulnerability Management
- CrowdStrike (connected second)
- Microsoft Defender for Endpoint (connected third)

Each source reports different values for IP address and operating system:

Property	Tenable Vulnerability Management	CrowdStrike	Microsoft TVM
IP Address	10.0.0.1	172.16.5.10	192.168.1.100
Operating System	Windows 10 Pro	Windows 11	Windows 10 Enterprise

Result:

- The IP address and OS from Tenable Vulnerability Management are selected and displayed in the UI.
- The values from CrowdStrike and Microsoft TVM are still stored and viewable in the [Asset Details](#) tab but are not shown by default.

Deduplication Limitations

- Assets must belong to the same class to be merged. For example, two assets from different connectors won't merge if one is an Account and the other is a Role.
- For cloud assets, provider IDs may differ by vendor. For example:
 - AWS via one connector might use full ARN
 - Another might use a shortened ID
 - Tenable supports matching multiple keys via a list-based `NATIVE_ID`.

Additional Resources

- [Asset Deduplication FAQ](#)

Asset Retention



Effective risk remediation involves focusing on what matters most to your organization. To keep your lists of assets and weaknesses as fresh and relevant as possible and minimize false positives, Tenable Exposure Management automatically removes assets that are presumed to be retired or inactive and represent no risk to your organization.

Configuring Asset Retention

Tenable Exposure Management provides asset retention settings that let you control when an asset is considered inactive and eligible for removal. This can be configured individually for each connector on its setup page.

To configure asset retention of a specific connector:

1. Within Tenable Exposure Management, navigate to **Connectors**.
2. In the connectors list, click on the connector for which you want to configure asset retention.

The edit connector page appears.

3. In the **Asset Retention** section, configure the retention period for inactive assets based on their last seen date. If an asset has not been detected or updated in a scan within the specified days, Tenable Exposure Management automatically removes it. This ensures your asset inventory stays current and relevant.

Asset Retention

Remove assets when their last seen date is more than days ago

Immediately remove assets when their status is:

Inactive



NoSensorData



Tip: Some connectors allow you also to configure the asset retention based on status change.

How long after the last sync is an asset considered inactive?

Asset inactivity represents the configuration of the number of days Tenable Exposure Management waits before removing an asset once its no longer present in a scan. If your scan cycles are less



frequent and you want to keep assets around for longer periods of time, choose a higher number of days, for example, 90.

If you scan multiple times a day with total coverage and want assets removed as soon as they are missing from a scan, choose a lower value, like 1.

Tenable defines the time an asset was last seen by the *Last Seen* time ingested from the native tool, if available. Otherwise, Tenable pulls from the most recent time the connector synced with Tenable Exposure Management.

Connectors FAQ

The following is not supported in Tenable FedRAMP Moderate environments. For more information, see the [Tenable FedRAMP Product Offering](#).

The following are frequently asked questions regarding connectors in Tenable Exposure Management.

Integration and Support

What integrations does Tenable Exposure Management support?

Tenable Exposure Management supports a wide range of integrations, as detailed in [Supported Third-Party Integrations](#).

Does Tenable Exposure Management support mobilization (ticketing systems) connectors?

Currently, Tenable Exposure Management does not support integrations with ticketing tools.

Sync and Status

How can I identify the status of my connector?

Once a connector is configured, you can monitor its status in the following ways:

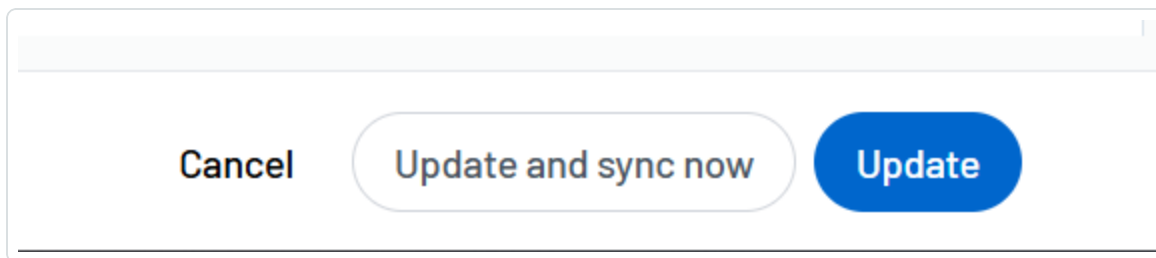


- See [Connector Status](#)
- See [Connector Sync Logs](#)

How can I re-sync a connector on demand?

You can manually trigger a sync for connectors. Sync buttons are available on the connector's setup page:

- **Sync Now:** Triggers a sync without saving changes.
- **Update:** Saves connector settings but waits for the next scheduled sync.
- **Update and Sync Now:** Saves the changes and starts syncing immediately.



Can I sync or process more than one connector at a time?

Yes. Tenable Exposure Management allows you to run syncs for multiple connectors at the same time.

The platform supports parallel sync execution, meaning you can trigger multiple connector syncs—manually or through scheduled jobs—without waiting for one to finish before starting another. View the [Connector Logs](#) to track each sync's progress.

What can I expect during a sync?

Sync duration varies by vendor and data volume. The [Connector Logs](#) tab is the most reliable way to confirm sync completion or investigate errors.

Deleted Connectors and Tags

Important! Full syncs can take up to 24 hours, at which point all connector data is fully removed from Tenable Exposure Management and its user interface.



What happens to asset and vulnerability data when I delete a connector?

When you delete a connector, Tenable Exposure Management removes all native data ingested through that specific integration.

This includes assets, weaknesses/findings, and data metadata fields associated with the connector:

- Only the data unique to that connector is removed.
- If another active connector provides the same asset or finding, that data remains visible and valid in the platform.

When is the data actually deleted?

Tenable Exposure Management removes the data in two stages:

- **Immediately after deletion:** The connector is removed from the UI, and its data is marked for deletion.
- **Next day:** The data is purged during the next scheduled backend cleanup, in line with the Tenable data retention process.

What happens to historical dashboards and reports?

Data previously included in [dashboards](#) or reports may still appear until Tenable Exposure Management refreshes the dataset or clears cached data.

Keep in mind:

- These records are not live.
- You won't see the deleted connector listed in current queries or filters.

Does the deleted data still show up in the Inventory view?

No. Once the connector is deleted and the data is purged, the associated assets and vulnerabilities will no longer appear in:

- [Inventory](#)
- [Exposure View](#)



- [Exposure Signals](#)
- [Dashboards](#) (after data refresh)

Can I recover a deleted connector or its data?

No. Once a connector is deleted and the data retention period has passed, the data is permanently removed. To restore access to the data, you must:

1. Reconfigure the connector.
2. Allow the sync to complete to reingest the data into Tenable Exposure Management.

Note: Some data (such as historical risk scores or past exceptions) may not fully reappear depending on the connector's design and sync behavior.

How do I confirm that a connector has been deleted?

After deletion:

- The connector disappears from the **Connectors** page.
- Its source tag or icon is removed from the **Inventory** and **Asset Details** views.
- The connector no longer appears as a **Source** for any active assets.

Is the data deletion process the same for all connectors?

Yes. The same deletion logic applies to both first-party and third-party connectors. Only data that was originally ingested by the deleted connector is be removed from Tenable Exposure Management.

How long does Tenable Exposure Management keep my connector data in my Dashboards?

By default, Tenable Exposure Management retains dashboard data within the user interface for 90 days. To access this data after this point, contact your Tenable representative.

Asset Deduplication FAQ



The following are frequently asked questions regarding asset deduplication in Tenable Exposure Management.

Do Tenable-native assets follow the same merge criteria as third-party data?

No. Tenable-native assets use a separate, internal merging logic that is not configurable or visible in the platform. The merge criteria [documented in this guide](#) apply only to assets ingested from third-party connectors.

Additionally, assets with different Tenable UUIDs are never merged, even if all other matching fields (such as hostname or IP address) align. This ensures accurate separation of Tenable-managed data and prevents unintended merging between unrelated records.

What happens when I add additional connectors with asset data?

If the deduplication criteria are met, the data merges from multiple connectors into a single asset. These are considered **Multi Source Assets**. For more information, see [View License Information](#) in the *Tenable Vulnerability Management User Guide*.

If the criteria aren't met, the platform treats the asset as unique and creates a new record in the inventory.

How does the system decide whether to merge asset data?

Tenable Exposure Management uses fixed matching criteria per asset class (e.g., device, website). If at least one combination of matching fields meets the merge conditions, the platform merges the data into a single asset.

Example for devices: If two connectors report the same hostname + IP + FQDN, the assets may be merged.

Can I customize the merge criteria?

No. The merge logic and field combinations are currently predefined and not configurable. Custom merge strategies may be introduced in future releases.

Can I choose which connector takes priority for conflicting data?

No. Tenable uses a fixed information order:



1. Tenable-native sources take priority.
2. Third-party connectors are prioritized by the order they were added to the system.

You can review the source of each field on the **Connector Details** tab of the [Asset Details](#) page.

What happens if multiple connectors sync at the same time?

The platform doesn't queue syncs but processes them concurrently. The first successfully processed connector becomes the primary source for merge decisions if Tenable-native data is not available.

Why do I still see data from a removed connector?

If an asset was merged and the connector is deleted, Tenable Exposure Management retains the merged data if other sources still report matching values. Only data exclusively ingested by the deleted connector is removed during connector deletion.