



Global Search Quick Reference Guide

Last Revised: August 05, 2025



Table of Contents

Welcome to the Global Search Quick Reference Guide	3
Pre-Defined Queries	4
Custom Queries	7
Query	7
NLP	9
Simple	10
Query Operators, Properties, and Selectors	11



Welcome to the Global Search Quick Reference Guide

Last updated: August 05, 2025

This guide exists to provide complete instructions on using the global search functionality within Tenable Exposure Management. The global search allows you to filter your entire asset inventory using pre-defined queries, Natural Language Processing (NLP), custom queries, and more!

For more information about Tenable Exposure Management, see [Inventory](#) in the *Tenable Exposure Management User Guide*.

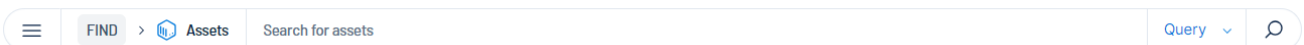
To access the global asset search:

1. Log in to Tenable Exposure Management.
2. At the top of the page, click the **Inventory** tab.

The **Assets** view appears by default.

	Name	AES	Class	Weaknesses	Number of tags	Last Updated	Sources
<input type="checkbox"/>	sql1	892	Device	997	0	16 November 2023	See Details >
<input type="checkbox"/>	ec2-18-214-125-213.co...	887	Device	3,939	0	16 November 2023	See Details >
<input type="checkbox"/>	ec2-18-136-14-199.ap-s...	887	Device	3,173	0	16 November 2023	See Details >
<input type="checkbox"/>	ec2-18-140-15-167.ap-s...	887	Device	153	0	16 November 2023	See Details >
<input type="checkbox"/>	ec2-18-219-243-10.us-e...	886	Device	269	0	16 November 2023	See Details >
<input type="checkbox"/>	ec2-18-197-51-78.eu-ce...	886	Device	267	0	16 November 2023	See Details >

At the top of the page, the global search bar appears.



To get started, see the following topics:


- [Pre-Defined Queries](#)
- [Custom Queries](#)
- [Query Operators, Properties, and Selectors](#)



Pre-Defined Queries

The global search includes three types of pre-defined queries that you can select when searching your asset inventory.

To access the available pre-defined queries:

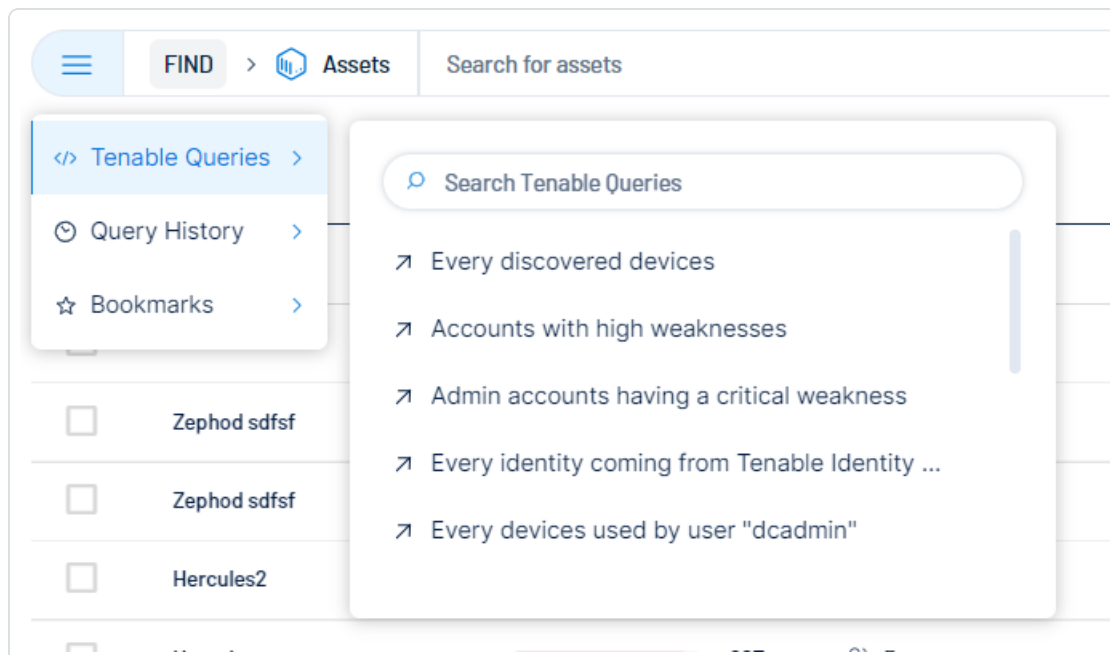
1. In the **Inventory > Assets** view, on the left side of the search bar, click the  button.

The pre-defined queries drop-down appears.

2. Select one of the following options:

Tenable Queries

The **Tenable Queries** option includes a list of Tenable-provided queries that you can use to search your assets.

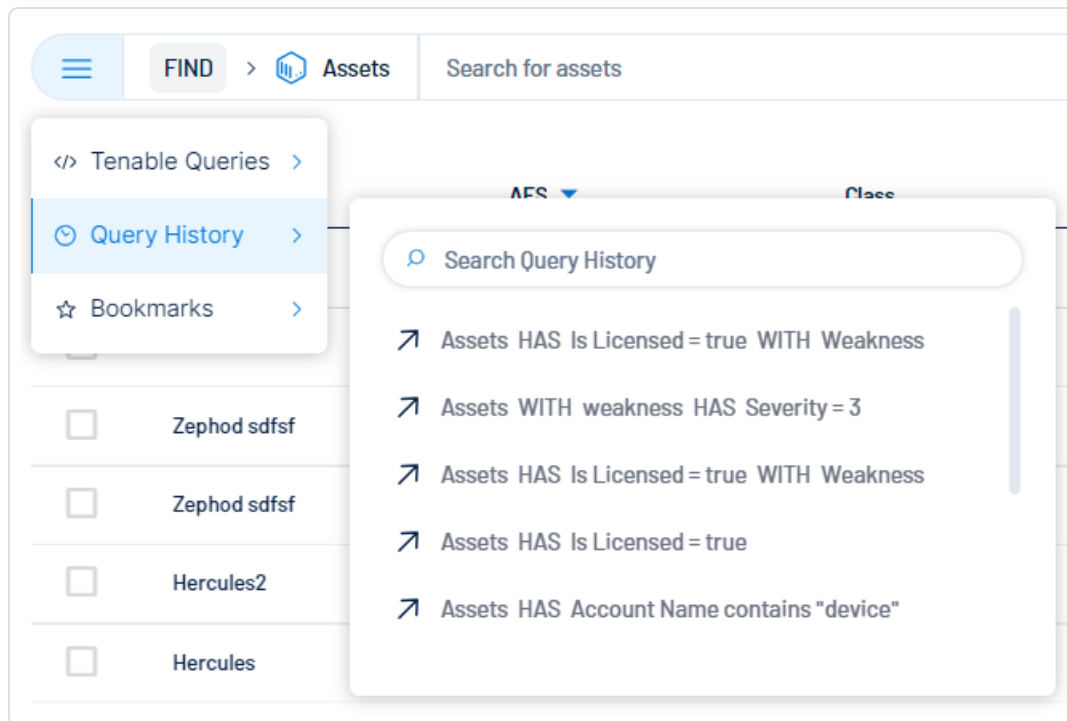


You can use the search bar at the top of the query list to search for a specific Tenable-provided query.

Query History



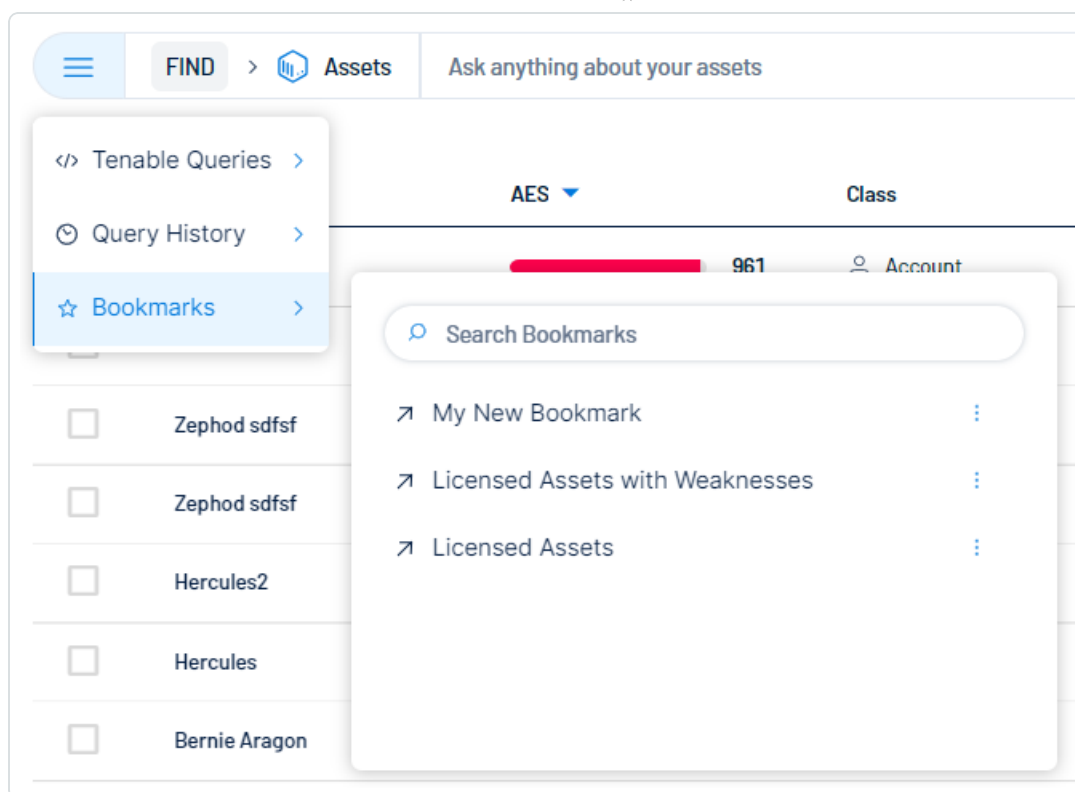
The **Query History** option lists several of the most recently run search queries.



You can use the search bar at the top of the query list to search for a specific item within your query history.


Bookmarks

The **Bookmarks** option shows a list of your saved query bookmarks. You can save any query-based search as a bookmark for later use.



You can use the search bar at the top of the query list to search for a specific bookmark.

To create a bookmark:

1. Create a [custom query](#) search.
2. On the right side of the search bar, click the  button.

A **Bookmark Added** window appears.

3. In the **Name** text box, type a name for the bookmark.
4. (Optional) In the **Description** text box, type a description for the bookmark.
5. Click **Save**.

A **Bookmark Added** confirmation message appears, and Tenable Exposure Management saves the bookmark to the [Bookmarks](#) list.



Custom Queries

The global search includes three types of custom searches you can perform to filter your asset inventory.

To access the query builder:

1. In the **Inventory > Assets** view, on the right side of the search bar, click the  button.

The custom queries drop-down appears.

Select one of the following options:

Query

The **Query** option allows you to build structured searches using query using blocks of property filters and asset criteria.

Tip: For a full list of possible operators, selectors, properties, and workflows, see [Query Operators, Properties, and Selectors](#).

Start a query

Syntax: AS [object_type][criteria]

1. Start by choosing what you want to find. For example, a device:

Click inside the query box to specify AS, the selector that filters and queries assets based on their type.

2. Select “Device” and press Enter.

The query returns all devices in the inventory.

You can also select other options such as infrastructure as code, accounts, or people.

Examples:

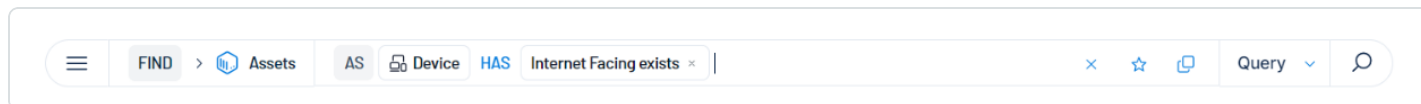
- AS device: Returns all devices in the system
- AS account: Returns all accounts in the system
- AS account device: Returns all accounts and devices



Add Details (Property Filters) to your Query

Property filters enhance the query to include details about your asset type.

Syntax: AS [object_type] HAS [property]:[value]



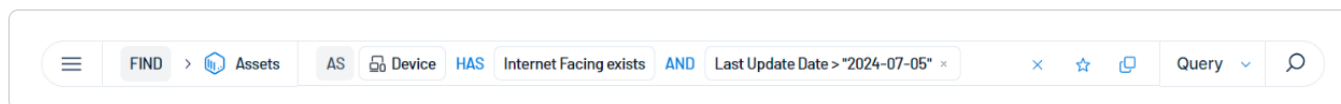
1. After you select your asset type (e.g. devices), choose the selector HAS in the query box.

The selector HAS marks the beginning of a filtering block, allowing you to specify criteria for selecting a subset of assets from the larger inventory, combining multiple filters, and customizing attributes.

2. Select a property filter for the asset. For example: "Internet-facing".
3. Press Enter.

The query returns all devices that are internet-facing in the inventory.

4. Add another property filter using the AND or OR operator. For example, "Last Update Date".
5. Press **Enter**.



The search returns all internet-facing devices last updated on the specified date in the inventory.

6. You can add as many property filters as needed to the query.

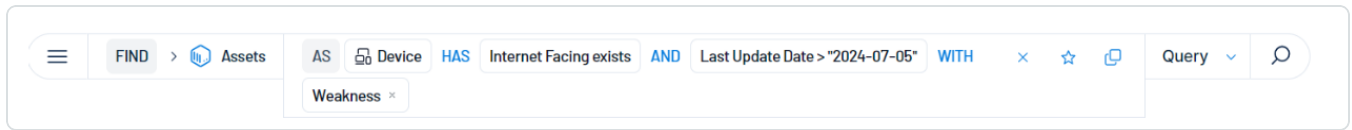
Specify Relationships in your Query

In addition to property filters, you can find asset relationships with other criteria using the WITH selector for more refined and precise results through multiple conditions, nested queries, and customization beyond basic conditions.

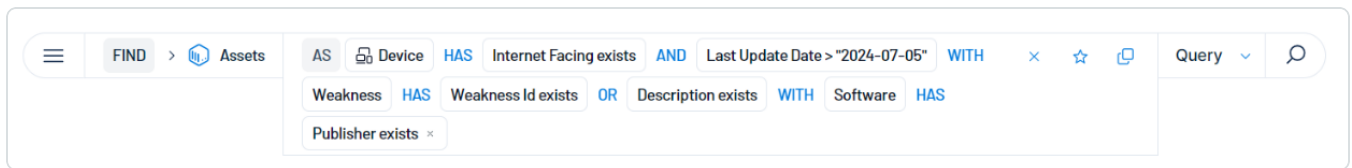
For example, you want to search for a specific weakness type in an asset:



1. In the query box, choose the WITH selector and select "Weakness".
2. Press Enter. The query returns all internet-facing devices last updated on the specified date that contain weaknesses in the inventory.



3. You can also add property filters to the query. For example, a "Weakness ID" type.
4. You can also add other relationships with the WITH selector: Software or Entitlement.



The query takes into account the property filters related to the last used asset type.

Custom Query Examples

AS device HAS weakness:severity:"High" - Finds devices with high-severity vulnerabilities

AS account HAS entitlement:name:"Admin Access" AND software:name:"Microsoft Office" - Finds accounts with admin access and Microsoft Office installed

For a full list of possible operators, selectors, properties, and workflows, see [Query Operators, Properties, and Selectors](#).

NLP

You can use Natural Language Processing (NLP) to ask questions about your assets and receive AI-generated answers.

In the **Ask anything about your assets** text box, type a question you want to ask about your assets. For example, you could ask *"How many critical assets do I have?"*.

This response only includes information related to your asset query. If no data is available, an error message appears indicating no data could be generated for the search criteria you entered.



Tip: For more information on NLP and its use cases, see [NLP Search Use Cases](#) in the *Tenable Exposure Management User Guide*.

Simple


A **Simple** search allows you to filter your asset list by asset name or asset ID.

In the **Search by asset name or asset ID** text box, type the asset name or asset ID by which you want to filter the asset list. *Tenable Inventory* performs the search and filters the asset list based on your query.



Query Operators, Properties, and Selectors

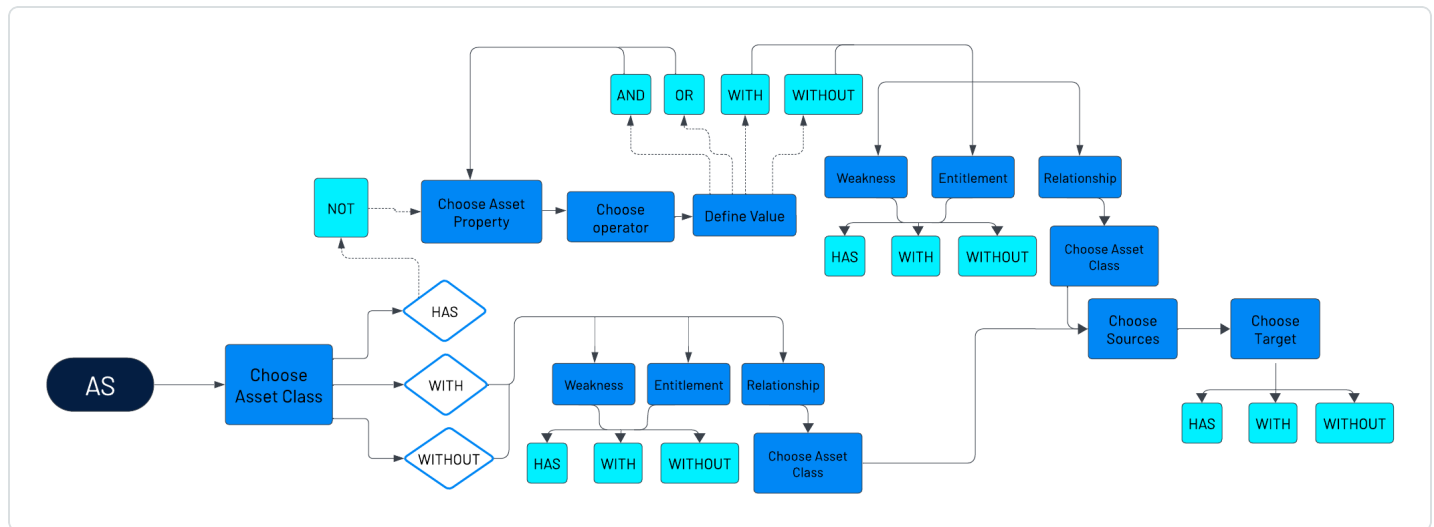
For more information about Tenable Exposure Management, see the [Tenable Exposure Management User Guide](#).

Tip: Follow the  icons to complete each step in the query building process. Additionally, be sure to expand the + buttons to view additional query building steps.

When you begin a query search, you must first select one of the following items. Expand the + next to each item to view full steps to build that query type.

AS

AS is an alias used to reference a specific object class within the Tenable Exposure Management application. It provides a convenient way to filter and query for assets based on their type. By using the AS alias, you can easily target and manipulate objects of a particular class, such as devices, infrastructure as code, accounts, or people.



Once you select **AS**, you can then select one or more **Asset Class**:



Choose an asset class

Account

Container

Device

Group

Infrastructure As Code

Other Resource

Person

Resource

Role

Web Application

Account

Generated by AI

A user account

An account is a record of a user's identity and permissions on a system. It typically includes a username, password, and other information such as the user's name, email address, and role. Accounts are used to control access to system resources and to track user activity.

Here are some key points to understand about accounts in the context of the cyber industry:

- Local Accounts:** These are accounts that are stored on the local system. They are typically used by administrators and other privileged users.
- Domain Accounts:** These are accounts that are stored in a domain. They are typically used by employees and other non-privileged users.
- Service Accounts:** These are accounts that are used by system services. They typically have very high permissions and are often targeted by attackers.
- Group Accounts:** These are accounts that represent a group of users. They can be used to simplify access control and to manage permissions for multiple users at once.

←

→

↑

↓

To navigate

↩

To select

esc

To dismiss

✕

To delete

- **Account** — An account is a record of a user's identity and permissions on a system. It typically includes a username, password, and other information such as the user's name, email address, and role.
- **Container** — A container is a software package that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.
- **Device** — A device is typically defined as a physical or virtual component that can connect to a network, communicate with other devices, and perform specific functions or tasks.
- **Group** — A group is a collection of assets that share common characteristics.
- **Infrastructure as Code** — Infrastructure as code (IaC) is a method of managing and provisioning IT infrastructure using code. IaC treats infrastructure as a set of resources that can be managed and provisioned using code.
- **Other Resource** — Other resources are assets that do not fall into any of the other categories. They can include things like software applications, databases, and websites.



- **Resource** — A resource is a type of asset that can be managed by Tenable Exposure Management. Resources can be physical or virtual, and they can be located on-premises or in the cloud.
- **Role** — A role is a type of asset that represents a specific function or purpose. For example, a web server role might represent a server that is used to host websites. Roles often include Entitlements.
- **Web Application** — A web application is a software application that is accessed via a web browser. It is typically hosted on a web server and can be accessed by anyone with an internet connection.



Then, choose one of the following:

HAS

HAS is used at the beginning of a filtering block to indicate the start of a group of filters that will be applied to the data. It allows users to specify the criteria for selecting a subset of assets from the larger asset inventory.

Choose an item

HAS

WITH

WITHOUT

Choose an asset class

Account

Container

Group

Infrastructure As Code

Other Resource

Person

HAS

Generated by AI

Start of a filtering block

HAS is used at the beginning of a filtering block to indicate the start of a group of filters that will be applied to the data. It allows users to specify the criteria for selecting a subset of assets from the larger asset inventory.

Here are some key points about HAS:

- **Filter Block:** HAS marks the beginning of a filter block, which is a set of criteria used to refine the list of assets based on specific attributes or characteristics.
- **Multiple Filters:** Within a filter block, multiple filters can be combined using logical operators (AND, OR, NOT) to create more complex filtering conditions.
- **Asset Selection:** HAS enables users to select a specific subset of assets that meet the defined criteria. This allows for focused analysis, reporting, and remediation efforts on the assets of interest.
- **Customization:** Filter blocks can be customized to meet the specific needs of an organization. Users can define filters based on various asset attributes such as IP address, operating system, vulnerability status, asset criticality, and more.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



Once you select **HAS**, you can optionally select **NOT** to exclude any items that include your search criteria.



Then, select an asset property to use in your query. See [Key Asset Properties](#) for a list of examples.



Once you have selected an asset property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the asset property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.

WITH

The WITH statement allows you to specify additional filtering criteria for a query. It provides a way to refine the results of a query by applying specific conditions or constraints. The WITH statement is particularly useful when you want to narrow down the scope of your query and focus on specific attributes or relationships of the assets being evaluated.



Choose an item

HAS

WITH

WITHOUT

Choose an asset class

Account

Container

Group

Infrastructure As Code

Other Resource

Person

WITH

Specifies additional filtering criteria for a query

The WITH statement in Tenable.cs allows you to specify additional filtering criteria for a query. It provides a way to refine the results of a query by applying specific conditions or constraints. The WITH statement is particularly useful when you want to narrow down the scope of your query and focus on specific attributes or relationships of the assets being evaluated.

Here are some key points to understand about the WITH statement in Tenable.cs:

- Additional Filtering:** The WITH statement enables you to apply additional filtering criteria beyond the basic conditions specified in the WHERE clause. It allows you to further refine the results of your query and retrieve a more targeted set of assets.
- Multiple Conditions:** You can use the WITH statement to specify multiple conditions or constraints. These conditions can be combined using logical operators (AND, OR, NOT) to create complex filtering criteria.
- Nested Queries:** The WITH statement supports nested queries, which means you can include subqueries within the WITH statement to filter the results further. This allows you to create more granular and sophisticated filtering criteria.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete

Generated by AI

Once you select **WITH**, you can then select one of the following cross-references:

Entitlement

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.

- 15 -



Choose a cross-reference

Generated by AI

Weakness

Entitlement

Relationship

ENTITLEMENT

A right to access a resource

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.

Here are some key points to understand about entitlements in the context of cybersecurity:

- **Access Control:** Entitlements are a fundamental aspect of access control mechanisms, which determine who can access what resources and under what conditions.
- **Role-Based Access Control (RBAC):** RBAC is a common approach to managing entitlements, where users are assigned roles, and each role is associated with a set of permissions or entitlements.
- **Least Privilege Principle:** The principle of least privilege states that users should only be granted the minimum level of entitlements necessary to perform their tasks, reducing the risk of unauthorized access.
- **Identity and Access Management (IAM):** IAM systems manage user identities, authentication, and entitlements, ensuring that only authorized individuals have access to the appropriate resources.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

✕ To delete



After you select **Entitlement**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Entitlement Properties](#) for a list of options.



Once you have selected an entitlement property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the entitlement property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:



- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Finding

A finding is a single instance of a vulnerability (weakness or misconfiguration) appearing on an asset, identified uniquely by plugin ID, port, and protocol.

CROSS-REFERENCES

Generated by AI

Entitlement	<h2>FINDING</h2>
Finding	<h3>A potential security issue detected on an AS.</h3>
Relationship	A finding represents a potential security issue or vulnerability detected on an AS within Cyber Asset Management. These findings are crucial for identifying and addressing weaknesses in your environment.
Software	Here's a breakdown of what findings entail:
Weakness	<ul style="list-style-type: none">• Vulnerability Identification: Findings often highlight specific vulnerabilities present on AS, such as outdated software, misconfigurations, or known security flaws.• Risk Assessment: Each finding is typically associated with a risk level, helping prioritize remediation efforts based on the potential impact and likelihood of exploitation.• Remediation Guidance: Cyber Asset Management may provide recommendations or guidance on how to address or mitigate the identified finding, reducing the overall AES.• Continuous Monitoring: Findings are continuously monitored to track their status and ensure timely remediation, improving the overall security posture.

←

→

↑

↓

To navigate

↩

To select

ESC

To dismiss

✕

To delete



After you select **Finding**, you can select one of the following options:



- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Finding Properties](#) for a list of examples.



Once you have selected a finding property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the finding property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Relationship

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.



Choose a cross-reference

Generated by AI

Weakness

Entitlement

Relationship

RELATIONSHIP

Connection between assets

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.

Here are some key points to understand about relationships in the context of cyber security:

- **Asset Discovery:** Relationships help in identifying and mapping the connections between assets, enabling a comprehensive understanding of the network infrastructure.
- **Vulnerability Assessment:** By understanding the relationships between assets, security teams can identify potential attack paths and assess the impact of vulnerabilities on interconnected systems.
- **Threat Detection and Response:** Relationships provide context to security alerts and incidents, allowing analysts to quickly identify affected assets and prioritize response efforts.
- **Compliance and Risk Management:** Relationships aid in assessing compliance with regulatory requirements and managing risks associated with interconnected assets.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Relationship**, you must select one or more sources. See [Relationship Sources and Targets](#) for a list of options.



Then, you must select a target. See [Relationship Sources and Targets](#) for a list of options.



After you select a target, you can select one of the following options:

- **HAS** – Select **HAS** to select a subset of criteria to include in your query. Optionally, after selecting **HAS**, you can select **NOT** to exclude the criteria from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.



Optionally, repeat the steps to include a [Finding](#), [Weakness](#), [Entitlement](#), [Relationship](#), or [Software](#) application to the target portion of the query.



Once you have selected the operators for any properties you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.

Software

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.

CROSS-REFERENCES

Generated by AI

Entitlement

Finding

Relationship

Software

Weakness

SOFTWARE

A type of keyword

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.

Here are some key points to understand about software:

- **Software Identification:** Automatically discovers and identifies software installed on devices within the organization's network. This information is crucial for understanding the software landscape and potential vulnerabilities associated with specific software versions.
- **Software Inventory:** Maintains an inventory of all software identified on devices, providing a comprehensive view of the software assets within the organization. This inventory helps in tracking software licenses, managing software updates, and ensuring compliance with software policies.
- **Software Vulnerabilities:** Correlates software information with known vulnerabilities, enabling users to identify devices that are potentially vulnerable to specific software exploits. This allows organizations to

← → ↑ ↓ To navigate

↩ To select

ESC To dismiss

✕ To delete



After you select **Software**, you can select one of the following options:



- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain.



Once you have selected a software property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the software property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Weakness

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.



Choose a cross-reference

Weakness

Entitlement

Relationship

Generated by AI

Weakness

Flaw or fault in the system

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.

Here are some key points to understand about weaknesses in the context of cyber security:

- **Vulnerabilities:** Vulnerabilities are specific weaknesses in software, hardware, or system configurations that can be exploited by attackers to gain unauthorized access or compromise the system.
- **Misconfigurations:** These are incorrect or insecure configurations of systems, devices, or software that can introduce weaknesses and make them vulnerable to attacks.
- **Human Errors:** Human mistakes, such as using weak passwords, failing to apply security patches, or mishandling sensitive data, can create weaknesses that can be exploited by attackers.
- **Inadequate Security Measures:** Insufficient security controls, such as lack of encryption, weak authentication mechanisms, or inadequate access controls, can lead to weaknesses in the system.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Weakness**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Weakness Properties](#) for a list of examples.



Once you have selected a weakness property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the weakness property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:



- **AND** – Combine the criteria defined in the query.
 - **OR** – Return query results that match either of the criteria defined in the query.
 - **WITH** – Select additional criteria to include with the query.
 - **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
 - **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

WITHOUT

The Boolean operator **WITHOUT** is used to exclude specific results from a search query. It allows you to refine your search criteria and narrow down the results by eliminating items that meet certain conditions. By using **WITHOUT**, you can focus on the results that are most relevant to your search and exclude those that are not.

Choose an item

HAS

WITH

WITHOUT

Choose an asset class

Account

Container

Group

Infrastructure As Code

Other Resource

Person

Generated by AI

WITHOUT

Boolean operator to exclude results

The Boolean operator "WITHOUT" is used to exclude specific results from a search query. It allows you to refine your search criteria and narrow down the results by eliminating items that meet certain conditions. By using "WITHOUT," you can focus on the results that are most relevant to your search and exclude those that are not.

Here are some key points to understand about the "WITHOUT" operator in the context of cyber security:

- **Exclusion Criteria:** "WITHOUT" enables you to specify criteria that should not be included in the search results. For example, you can exclude specific IP addresses, domains, or file types from your search query.
- **Refining Results:** By using "WITHOUT," you can refine your search results and make them more precise. This is especially useful when you have a large dataset or when you want to focus on specific aspects of your search.
- **Boolean Logic:** "WITHOUT" is part of Boolean logic, which is a system of logical operators used to combine search terms and refine results. Other Boolean operators include "AND," "OR," and "NOT."
- **Syntax:** The syntax for using "WITHOUT" in a search query is typically "term1 WITHOUT term2." For example, you could search for "vulnerabilities WITHOUT CVE-2023-1234" to exclude vulnerabilities with

To navigate

To select

To dismiss

To delete



Once you select **WITHOUT**, you can then select one of the following cross-references:



Entitlement

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.

Choose a cross-reference

Generated by AI

Weakness

Entitlement

Relationship

ENTITLEMENT

A right to access a resource

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.

Here are some key points to understand about entitlements in the context of cybersecurity:

- **Access Control:** Entitlements are a fundamental aspect of access control mechanisms, which determine who can access what resources and under what conditions.
- **Role-Based Access Control (RBAC):** RBAC is a common approach to managing entitlements, where users are assigned roles, and each role is associated with a set of permissions or entitlements.
- **Least Privilege Principle:** The principle of least privilege states that users should only be granted the minimum level of entitlements necessary to perform their tasks, reducing the risk of unauthorized access.
- **Identity and Access Management (IAM):** IAM systems manage user identities, authentication, and entitlements, ensuring that only authorized individuals have access to the appropriate resources.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Entitlement**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Entitlement Properties](#) for a list of options.



Once you have selected an entitlement property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the entitlement property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Finding

A finding is a single instance of a vulnerability (weakness or misconfiguration) appearing on an asset, identified uniquely by plugin ID, port, and protocol.



CROSS-REFERENCES

Generated by AI

Entitlement

Finding

Relationship

Software

Weakness

FINDING

A potential security issue detected on an AS.

A finding represents a potential security issue or vulnerability detected on an AS within Cyber Asset Management. These findings are crucial for identifying and addressing weaknesses in your environment.

Here's a breakdown of what findings entail:

- **Vulnerability Identification:** Findings often highlight specific vulnerabilities present on AS, such as outdated software, misconfigurations, or known security flaws.
- **Risk Assessment:** Each finding is typically associated with a risk level, helping prioritize remediation efforts based on the potential impact and likelihood of exploitation.
- **Remediation Guidance:** Cyber Asset Management may provide recommendations or guidance on how to address or mitigate the identified finding, reducing the overall AES.
- **Continuous Monitoring:** Findings are continuously monitored to track their status and ensure timely remediation, improving the overall security posture.

← → ↑ ↓ To navigate

↩ To select

ESC To dismiss

ⓧ To delete



After you select **Finding**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Finding Properties](#) for a list of examples.



Once you have selected a finding property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the finding property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:



- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Relationship

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.

Choose a cross-reference

Weakness

Entitlement

Relationship

RELATIONSHIP

Generated by AI

Connection between assets

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.

Here are some key points to understand about relationships in the context of cyber security:

- **Asset Discovery:** Relationships help in identifying and mapping the connections between assets, enabling a comprehensive understanding of the network infrastructure.
- **Vulnerability Assessment:** By understanding the relationships between assets, security teams can identify potential attack paths and assess the impact of vulnerabilities on interconnected systems.
- **Threat Detection and Response:** Relationships provide context to security alerts and incidents, allowing analysts to quickly identify affected assets and prioritize response efforts.
- **Compliance and Risk Management:** Relationships aid in assessing compliance with regulatory requirements and managing risks associated with interconnected assets.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Relationship**, you must select one or more sources. See [Relationship Sources and Targets](#) for a list of options.



Then, you must select a target. See [Relationship Sources and Targets](#) for a list of options.



After you select a target, you can select one of the following options:

- **HAS** – Select **HAS** to select a subset of criteria to include in your query. Optionally, after selecting **HAS**, you can select **NOT** to exclude the criteria from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.



Optionally, repeat the steps to exclude a [Finding](#), [Weakness](#), [Entitlement](#), [Relationship](#), or [Software](#) application to the target portion of the query.



Once you have selected the operators for any properties you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.

Software

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.



CROSS-REFERENCES

Generated by AI

Entitlement

Finding

Relationship

Software

Weakness

SOFTWARE

A type of keyword

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.

Here are some key points to understand about software:

- Software Identification:** Automatically discovers and identifies software installed on devices within the organization's network. This information is crucial for understanding the software landscape and potential vulnerabilities associated with specific software versions.
- Software Inventory:** Maintains an inventory of all software identified on devices, providing a comprehensive view of the software assets within the organization. This inventory helps in tracking software licenses, managing software updates, and ensuring compliance with software policies.
- Software Vulnerabilities:** Correlates software information with known vulnerabilities, enabling users to identify devices that are potentially vulnerable to specific software exploits. This allows organizations to

←

→

↑

↓

To navigate

↩

To select

ESC

To dismiss

✕

To delete



After you select **Software**, you can select one of the following options:

- HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain.



Once you have selected a software property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the software property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:



- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Weakness

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.

Choose a cross-reference

Weakness

Entitlement

Relationship

Weakness

Flaw or fault in the system

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.

Here are some key points to understand about weaknesses in the context of cyber security:

- **Vulnerabilities:** Vulnerabilities are specific weaknesses in software, hardware, or system configurations that can be exploited by attackers to gain unauthorized access or compromise the system.
- **Misconfigurations:** These are incorrect or insecure configurations of systems, devices, or software that can introduce weaknesses and make them vulnerable to attacks.
- **Human Errors:** Human mistakes, such as using weak passwords, failing to apply security patches, or mishandling sensitive data, can create weaknesses that can be exploited by attackers.
- **Inadequate Security Measures:** Insufficient security controls, such as lack of encryption, weak authentication mechanisms, or inadequate access controls, can lead to weaknesses in the system.

← → ↑ ↓ To navigate

↶ To select

esc To dismiss

ⓧ To delete

Generated by AI

After you select **Weakness**, you can select one of the following options:

- 30 -



- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Weakness Properties](#) for a list of examples.



Once you have selected a weakness property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the weakness property that you selected in the previous step.

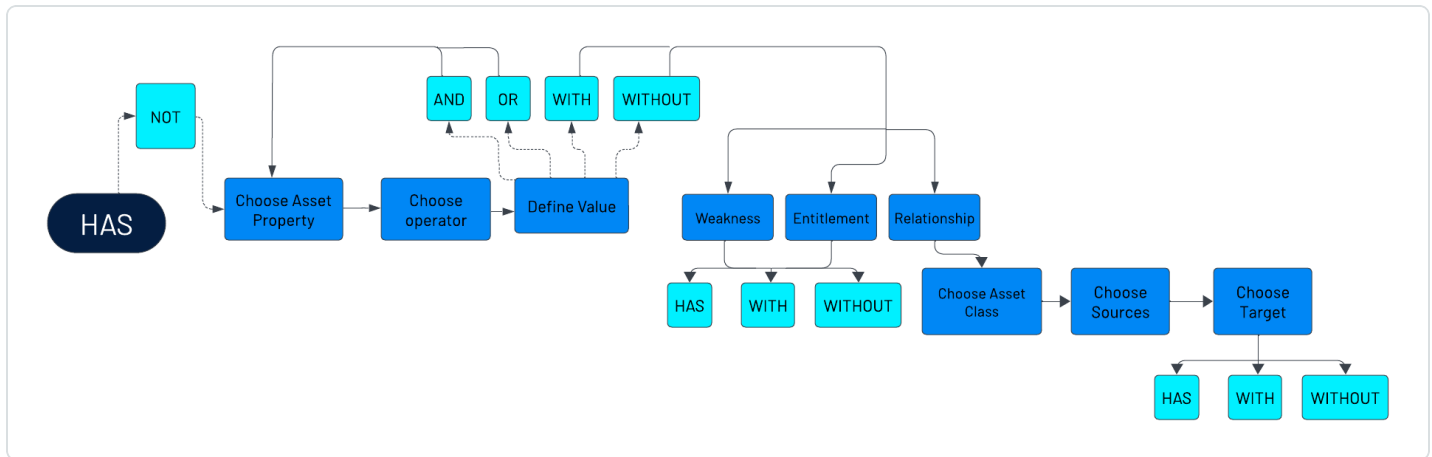


Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

HAS

HAS is used at the beginning of a filtering block to indicate the start of a group of filters that will be applied to the data. It allows users to specify the criteria for selecting a subset of assets from the larger asset inventory.



Once you select **HAS**, you can optionally select **NOT** to exclude any items that include your search criteria.



Then, select an asset property to use in your query. See [Key Asset Properties](#) for a list of examples.



Once you have selected an asset property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the asset property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH**

The WITH statement allows you to specify additional filtering criteria for a query. It provides a way to refine the results of a query by applying specific conditions or constraints. The WITH statement is particularly useful when you want to narrow down the scope of your query and focus on specific attributes or relationships of the assets being evaluated.



Choose an item

HAS

WITH

WITHOUT

Choose an asset class

Account

Container

Group

Infrastructure As Code

Other Resource

Person

Generated by **AI**

WITH

Specifies additional filtering criteria for a query

The WITH statement in Tenable.cs allows you to specify additional filtering criteria for a query. It provides a way to refine the results of a query by applying specific conditions or constraints. The WITH statement is particularly useful when you want to narrow down the scope of your query and focus on specific attributes or relationships of the assets being evaluated.

Here are some key points to understand about the WITH statement in Tenable.cs:

- **Additional Filtering:** The WITH statement enables you to apply additional filtering criteria beyond the basic conditions specified in the WHERE clause. It allows you to further refine the results of your query and retrieve a more targeted set of assets.
- **Multiple Conditions:** You can use the WITH statement to specify multiple conditions or constraints. These conditions can be combined using logical operators (AND, OR, NOT) to create complex filtering criteria.
- **Nested Queries:** The WITH statement supports nested queries, which means you can include subqueries within the WITH statement to filter the results further. This allows you to create more granular and sophisticated filtering criteria.

To navigate

To select

To dismiss

To delete



Once you select **WITH**, you can then select one of the following cross-references:

Entitlement

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.



Choose a cross-reference

Generated by AI

Weakness

Entitlement

Relationship

ENTITLEMENT

A right to access a resource

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.

Here are some key points to understand about entitlements in the context of cybersecurity:

- **Access Control:** Entitlements are a fundamental aspect of access control mechanisms, which determine who can access what resources and under what conditions.
- **Role-Based Access Control (RBAC):** RBAC is a common approach to managing entitlements, where users are assigned roles, and each role is associated with a set of permissions or entitlements.
- **Least Privilege Principle:** The principle of least privilege states that users should only be granted the minimum level of entitlements necessary to perform their tasks, reducing the risk of unauthorized access.
- **Identity and Access Management (IAM):** IAM systems manage user identities, authentication, and entitlements, ensuring that only authorized individuals have access to the appropriate resources.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Entitlement**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Entitlement Properties](#) for a list of options.



Once you have selected an entitlement property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the entitlement property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
 - **OR** – Return query results that match either of the criteria defined in the query.
 - **WITH** – Select additional criteria to include with the query.
 - **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
 - **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Finding

A finding is a single instance of a vulnerability (weakness or misconfiguration) appearing on an asset, identified uniquely by plugin ID, port, and protocol.



CROSS-REFERENCES

Generated by AI

Entitlement

FINDING

Finding

A potential security issue detected on an AS.

Relationship

A finding represents a potential security issue or vulnerability detected on an AS within Cyber Asset Management. These findings are crucial for identifying and addressing weaknesses in your environment.

Here's a breakdown of what findings entail:

- **Vulnerability Identification:** Findings often highlight specific vulnerabilities present on AS, such as outdated software, misconfigurations, or known security flaws.
- **Risk Assessment:** Each finding is typically associated with a risk level, helping prioritize remediation efforts based on the potential impact and likelihood of exploitation.
- **Remediation Guidance:** Cyber Asset Management may provide recommendations or guidance on how to address or mitigate the identified finding, reducing the overall AES.
- **Continuous Monitoring:** Findings are continuously monitored to track their status and ensure timely remediation, improving the overall security posture.

Software

Weakness

← → ↑ ↓ To navigate

↩ To select

ESC To dismiss

✕ To delete



After you select **Finding**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Finding Properties](#) for a list of examples.



Once you have selected a finding property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the finding property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
 - **OR** – Return query results that match either of the criteria defined in the query.
 - **WITH** – Select additional criteria to include with the query.
 - **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
 - **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Relationship

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.



Choose a cross-reference

Generated by AI

Weakness

Entitlement

Relationship

RELATIONSHIP

Connection between assets

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.

Here are some key points to understand about relationships in the context of cyber security:

- **Asset Discovery:** Relationships help in identifying and mapping the connections between assets, enabling a comprehensive understanding of the network infrastructure.
- **Vulnerability Assessment:** By understanding the relationships between assets, security teams can identify potential attack paths and assess the impact of vulnerabilities on interconnected systems.
- **Threat Detection and Response:** Relationships provide context to security alerts and incidents, allowing analysts to quickly identify affected assets and prioritize response efforts.
- **Compliance and Risk Management:** Relationships aid in assessing compliance with regulatory requirements and managing risks associated with interconnected assets.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Relationship**, you must select one or more sources. See [Relationship Sources and Targets](#) for a list of options.



Then, you must select a target. See [Relationship Sources and Targets](#) for a list of options.



After you select a target, you can select one of the following options:

- **HAS** – Select **HAS** to select a subset of criteria to include in your query. Optionally, after selecting **HAS**, you can select **NOT** to exclude the criteria from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.



Optionally, repeat the steps to include a [Finding](#), [Weakness](#), [Entitlement](#), [Relationship](#), or [Software](#) application to the target portion of the query.



Once you have selected the operators for any properties you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.

Software

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.



CROSS-REFERENCES

Generated by AI

Entitlement

Finding

Relationship

Software

Weakness

SOFTWARE

A type of keyword

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.

Here are some key points to understand about software:

- **Software Identification:** Automatically discovers and identifies software installed on devices within the organization's network. This information is crucial for understanding the software landscape and potential vulnerabilities associated with specific software versions.
- **Software Inventory:** Maintains an inventory of all software identified on devices, providing a comprehensive view of the software assets within the organization. This inventory helps in tracking software licenses, managing software updates, and ensuring compliance with software policies.
- **Software Vulnerabilities:** Correlates software information with known vulnerabilities, enabling users to identify devices that are potentially vulnerable to specific software exploits. This allows organizations to

← → ↑ ↓ To navigate

↩ To select

ESC To dismiss

ⓧ To delete



After you select **Software**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain.



Once you have selected a software property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the software property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
 - **OR** – Return query results that match either of the criteria defined in the query.
 - **WITH** – Select additional criteria to include with the query.
 - **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
 - **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Weakness

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.



Choose a cross-reference

Weakness

Entitlement

Relationship

Generated by AI

Weakness

Flaw or fault in the system

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.

Here are some key points to understand about weaknesses in the context of cyber security:

- **Vulnerabilities:** Vulnerabilities are specific weaknesses in software, hardware, or system configurations that can be exploited by attackers to gain unauthorized access or compromise the system.
- **Misconfigurations:** These are incorrect or insecure configurations of systems, devices, or software that can introduce weaknesses and make them vulnerable to attacks.
- **Human Errors:** Human mistakes, such as using weak passwords, failing to apply security patches, or mishandling sensitive data, can create weaknesses that can be exploited by attackers.
- **Inadequate Security Measures:** Insufficient security controls, such as lack of encryption, weak authentication mechanisms, or inadequate access controls, can lead to weaknesses in the system.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Weakness**, you can select one of the following options:

- **HAS** – Select **HAS** to select a subset of criteria to include in your query. Optionally, after selecting **HAS**, you can select **NOT** to exclude the criteria from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.



Then, you can select the property that you want the search results to contain. See [Key Weakness Properties](#) for a list of examples.



Once you have selected a weakness property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the weakness property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.

WITHOUT

The Boolean operator **WITHOUT** is used to exclude specific results from a search query. It allows you to refine your search criteria and narrow down the results by eliminating items that meet certain conditions. By using **WITHOUT**, you can focus on the results that are most relevant to your search and exclude those that are not.

Choose an item

HAS

WITH

WITHOUT

Choose an asset class

Account

Container

Group

Infrastructure As Code

Other Resource

Person

WITHOUT

Generated by AI

Boolean operator to exclude results

The Boolean operator "WITHOUT" is used to exclude specific results from a search query. It allows you to refine your search criteria and narrow down the results by eliminating items that meet certain conditions. By using "WITHOUT," you can focus on the results that are most relevant to your search and exclude those that are not.

Here are some key points to understand about the "WITHOUT" operator in the context of cyber security:

- **Exclusion Criteria:** "WITHOUT" enables you to specify criteria that should not be included in the search results. For example, you can exclude specific IP addresses, domains, or file types from your search query.
- **Refining Results:** By using "WITHOUT," you can refine your search results and make them more precise. This is especially useful when you have a large dataset or when you want to focus on specific aspects of your search.
- **Boolean Logic:** "WITHOUT" is part of Boolean logic, which is a system of logical operators used to combine search terms and refine results. Other Boolean operators include "AND," "OR," and "NOT."
- **Syntax:** The syntax for using "WITHOUT" in a search query is typically "term1 WITHOUT term2." For example, you could search for "vulnerability WITHOUT CVE-2023-1234" to exclude vulnerabilities with

To navigate

To select

To dismiss

To delete



Once you select **WITHOUT**, you can then select one of the following cross-references:



Entitlement

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.

Choose a cross-reference

Generated by AI

Weakness

Entitlement

Relationship

ENTITLEMENT

A right to access a resource

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.

Here are some key points to understand about entitlements in the context of cybersecurity:

- **Access Control:** Entitlements are a fundamental aspect of access control mechanisms, which determine who can access what resources and under what conditions.
- **Role-Based Access Control (RBAC):** RBAC is a common approach to managing entitlements, where users are assigned roles, and each role is associated with a set of permissions or entitlements.
- **Least Privilege Principle:** The principle of least privilege states that users should only be granted the minimum level of entitlements necessary to perform their tasks, reducing the risk of unauthorized access.
- **Identity and Access Management (IAM):** IAM systems manage user identities, authentication, and entitlements, ensuring that only authorized individuals have access to the appropriate resources.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Entitlement**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Entitlement Properties](#) for a list of options.



Once you have selected an entitlement property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the entitlement property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Finding

A finding is a single instance of a vulnerability (weakness or misconfiguration) appearing on an asset, identified uniquely by plugin ID, port, and protocol.



CROSS-REFERENCES

Generated by AI

Entitlement

Finding

Relationship

Software

Weakness

FINDING

A potential security issue detected on an AS.

A finding represents a potential security issue or vulnerability detected on an AS within Cyber Asset Management. These findings are crucial for identifying and addressing weaknesses in your environment.

Here's a breakdown of what findings entail:

- **Vulnerability Identification:** Findings often highlight specific vulnerabilities present on AS, such as outdated software, misconfigurations, or known security flaws.
- **Risk Assessment:** Each finding is typically associated with a risk level, helping prioritize remediation efforts based on the potential impact and likelihood of exploitation.
- **Remediation Guidance:** Cyber Asset Management may provide recommendations or guidance on how to address or mitigate the identified finding, reducing the overall AES.
- **Continuous Monitoring:** Findings are continuously monitored to track their status and ensure timely remediation, improving the overall security posture.

← → ↑ ↓ To navigate

↩ To select

ESC To dismiss

⌫ To delete



After you select **Finding**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Finding Properties](#) for a list of examples.



Once you have selected a finding property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the finding property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
 - **OR** – Return query results that match either of the criteria defined in the query.
 - **WITH** – Select additional criteria to include with the query.
 - **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
 - **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Relationship

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.



Choose a cross-reference

Generated by AI

Weakness

Entitlement

Relationship

RELATIONSHIP

Connection between assets

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.

Here are some key points to understand about relationships in the context of cyber security:

- **Asset Discovery:** Relationships help in identifying and mapping the connections between assets, enabling a comprehensive understanding of the network infrastructure.
- **Vulnerability Assessment:** By understanding the relationships between assets, security teams can identify potential attack paths and assess the impact of vulnerabilities on interconnected systems.
- **Threat Detection and Response:** Relationships provide context to security alerts and incidents, allowing analysts to quickly identify affected assets and prioritize response efforts.
- **Compliance and Risk Management:** Relationships aid in assessing compliance with regulatory requirements and managing risks associated with interconnected assets.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Relationship**, you must select one or more sources. See [Relationship Sources and Targets](#) for a list of options.



Then, you must select a target. See [Relationship Sources and Targets](#) for a list of options.



After you select a target, you can select one of the following options:

- **HAS** — Select **HAS** to select a subset of criteria to include in your query. Optionally, after selecting **HAS**, you can select **NOT** to exclude the criteria from the query.
- **WITH** — Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** — Select **WITHOUT** to specify additional filtering criteria to exclude from the query.



Optionally, repeat the steps to exclude a [Finding](#), [Weakness](#), [Entitlement](#), [Relationship](#), or [Software](#) applicatino to the target portion of the query.



Once you have selected the operators for any properties you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.

Software

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.



CROSS-REFERENCES

Generated by AI

Entitlement

Finding

Relationship

Software

Weakness

SOFTWARE

A type of keyword

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.

Here are some key points to understand about software:

- **Software Identification:** Automatically discovers and identifies software installed on devices within the organization's network. This information is crucial for understanding the software landscape and potential vulnerabilities associated with specific software versions.
- **Software Inventory:** Maintains an inventory of all software identified on devices, providing a comprehensive view of the software assets within the organization. This inventory helps in tracking software licenses, managing software updates, and ensuring compliance with software policies.
- **Software Vulnerabilities:** Correlates software information with known vulnerabilities, enabling users to identify devices that are potentially vulnerable to specific software exploits. This allows organizations to

← → ↑ ↓ To navigate

↩ To select

ESC To dismiss

ⓧ To delete



After you select **Software**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain.



Once you have selected a software property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the software property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
 - **OR** – Return query results that match either of the criteria defined in the query.
 - **WITH** – Select additional criteria to include with the query.
 - **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
 - **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Weakness

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.



Choose a cross-reference

Weakness

Entitlement

Relationship

Generated by AI

Weakness

Flaw or fault in the system

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.

Here are some key points to understand about weaknesses in the context of cyber security:

- **Vulnerabilities:** Vulnerabilities are specific weaknesses in software, hardware, or system configurations that can be exploited by attackers to gain unauthorized access or compromise the system.
- **Misconfigurations:** These are incorrect or insecure configurations of systems, devices, or software that can introduce weaknesses and make them vulnerable to attacks.
- **Human Errors:** Human mistakes, such as using weak passwords, failing to apply security patches, or mishandling sensitive data, can create weaknesses that can be exploited by attackers.
- **Inadequate Security Measures:** Insufficient security controls, such as lack of encryption, weak authentication mechanisms, or inadequate access controls, can lead to weaknesses in the system.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Weakness**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Weakness Properties](#) for a list of examples.



Once you have selected a weakness property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the weakness property that you selected in the previous step.

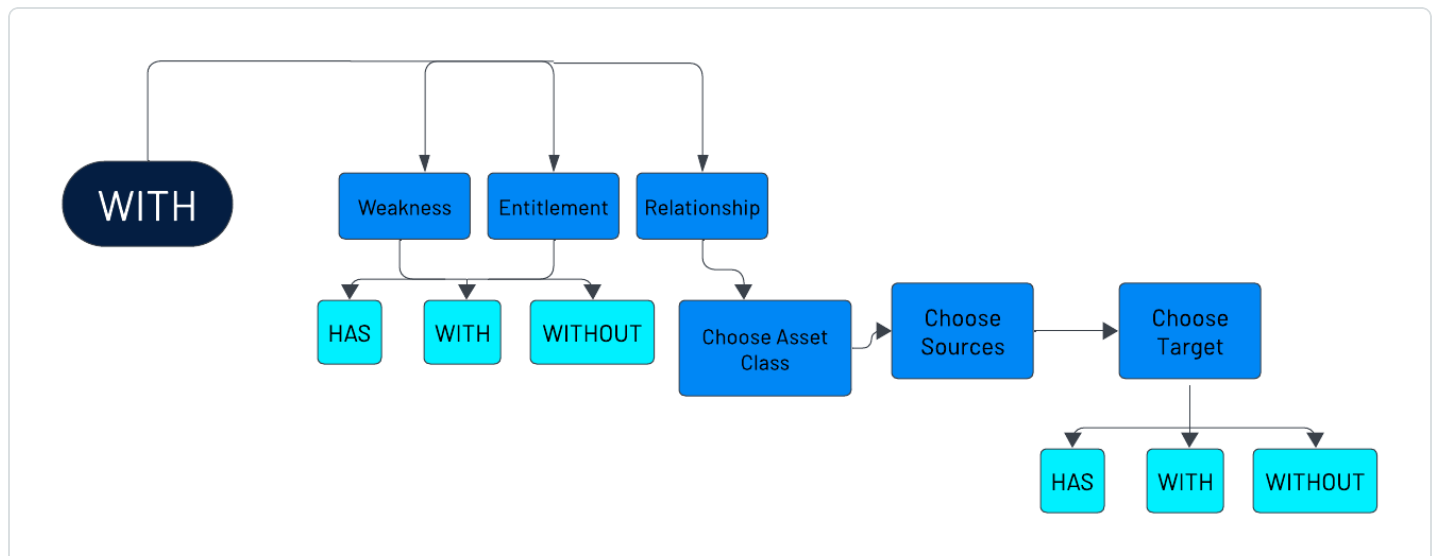


Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
 - **OR** – Return query results that match either of the criteria defined in the query.
 - **WITH** – Select additional criteria to include with the query.
 - **WITHOUT** – Select additional criteria to exclude from the query.
-
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
 - **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

WITH

The WITH statement allows you to specify additional filtering criteria for a query. It provides a way to refine the results of a query by applying specific conditions or constraints. The WITH statement is particularly useful when you want to narrow down the scope of your query and focus on specific attributes or relationships of the assets being evaluated.



Once you select **WITH**, you can then select one of the following cross-references:



Entitlement

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.

Choose a cross-reference

Generated by AI

Weakness

Entitlement

Relationship

ENTITLEMENT

A right to access a resource

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.

Here are some key points to understand about entitlements in the context of cybersecurity:

- **Access Control:** Entitlements are a fundamental aspect of access control mechanisms, which determine who can access what resources and under what conditions.
- **Role-Based Access Control (RBAC):** RBAC is a common approach to managing entitlements, where users are assigned roles, and each role is associated with a set of permissions or entitlements.
- **Least Privilege Principle:** The principle of least privilege states that users should only be granted the minimum level of entitlements necessary to perform their tasks, reducing the risk of unauthorized access.
- **Identity and Access Management (IAM):** IAM systems manage user identities, authentication, and entitlements, ensuring that only authorized individuals have access to the appropriate resources.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Entitlement**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Entitlement Properties](#) for a list of options.



Once you have selected an entitlement property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the entitlement property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Finding

A finding is a single instance of a vulnerability (weakness or misconfiguration) appearing on an asset, identified uniquely by plugin ID, port, and protocol.



CROSS-REFERENCES

Generated by AI

Entitlement

Finding

Relationship

Software

Weakness

FINDING

A potential security issue detected on an AS.

A finding represents a potential security issue or vulnerability detected on an AS within Cyber Asset Management. These findings are crucial for identifying and addressing weaknesses in your environment.

Here's a breakdown of what findings entail:

- **Vulnerability Identification:** Findings often highlight specific vulnerabilities present on AS, such as outdated software, misconfigurations, or known security flaws.
- **Risk Assessment:** Each finding is typically associated with a risk level, helping prioritize remediation efforts based on the potential impact and likelihood of exploitation.
- **Remediation Guidance:** Cyber Asset Management may provide recommendations or guidance on how to address or mitigate the identified finding, reducing the overall AES.
- **Continuous Monitoring:** Findings are continuously monitored to track their status and ensure timely remediation, improving the overall security posture.

← → ↑ ↓ To navigate

↩ To select

ESC To dismiss

ⓧ To delete



After you select **Finding**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Finding Properties](#) for a list of examples.



Once you have selected a finding property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the finding property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:



- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Relationship

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.

Choose a cross-reference

Weakness

Entitlement

Relationship

RELATIONSHIP

Generated by AI

Connection between assets

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.

Here are some key points to understand about relationships in the context of cyber security:

- **Asset Discovery:** Relationships help in identifying and mapping the connections between assets, enabling a comprehensive understanding of the network infrastructure.
- **Vulnerability Assessment:** By understanding the relationships between assets, security teams can identify potential attack paths and assess the impact of vulnerabilities on interconnected systems.
- **Threat Detection and Response:** Relationships provide context to security alerts and incidents, allowing analysts to quickly identify affected assets and prioritize response efforts.
- **Compliance and Risk Management:** Relationships aid in assessing compliance with regulatory requirements and managing risks associated with interconnected assets.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Relationship**, you must select one or more sources. See [Relationship Sources and Targets](#) for a list of options.



Then, you must select a target. See [Relationship Sources and Targets](#) for a list of options.



After you select a target, you can select one of the following options:

- **HAS** – Select **HAS** to select a subset of criteria to include in your query. Optionally, after selecting **HAS**, you can select **NOT** to exclude the criteria from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.



Optionally, repeat the steps to include a [Finding](#), [Weakness](#), [Entitlement](#), [Relationship](#), or [Software](#) application to the target portion of the query.



Once you have selected the operators for any properties you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.

Software

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.



CROSS-REFERENCES

Generated by AI

Entitlement

Finding

Relationship

Software

Weakness

SOFTWARE

A type of keyword

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.

Here are some key points to understand about software:

- **Software Identification:** Automatically discovers and identifies software installed on devices within the organization's network. This information is crucial for understanding the software landscape and potential vulnerabilities associated with specific software versions.
- **Software Inventory:** Maintains an inventory of all software identified on devices, providing a comprehensive view of the software assets within the organization. This inventory helps in tracking software licenses, managing software updates, and ensuring compliance with software policies.
- **Software Vulnerabilities:** Correlates software information with known vulnerabilities, enabling users to identify devices that are potentially vulnerable to specific software exploits. This allows organizations to

← → ↑ ↓ To navigate

↩ To select

ESC To dismiss

✕ To delete



After you select **Software**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain.



Once you have selected a software property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the software property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:



- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Weakness

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.

Choose a cross-reference

Generated by AI

Weakness

Entitlement

Relationship

Weakness

Flaw or fault in the system

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.

Here are some key points to understand about weaknesses in the context of cyber security:

- **Vulnerabilities:** Vulnerabilities are specific weaknesses in software, hardware, or system configurations that can be exploited by attackers to gain unauthorized access or compromise the system.
- **Misconfigurations:** These are incorrect or insecure configurations of systems, devices, or software that can introduce weaknesses and make them vulnerable to attacks.
- **Human Errors:** Human mistakes, such as using weak passwords, failing to apply security patches, or mishandling sensitive data, can create weaknesses that can be exploited by attackers.
- **Inadequate Security Measures:** Insufficient security controls, such as lack of encryption, weak authentication mechanisms, or inadequate access controls, can lead to weaknesses in the system.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Weakness**, you can select one of the following options:



- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Weakness Properties](#) for a list of examples.



Once you have selected a weakness property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the weakness property that you selected in the previous step.

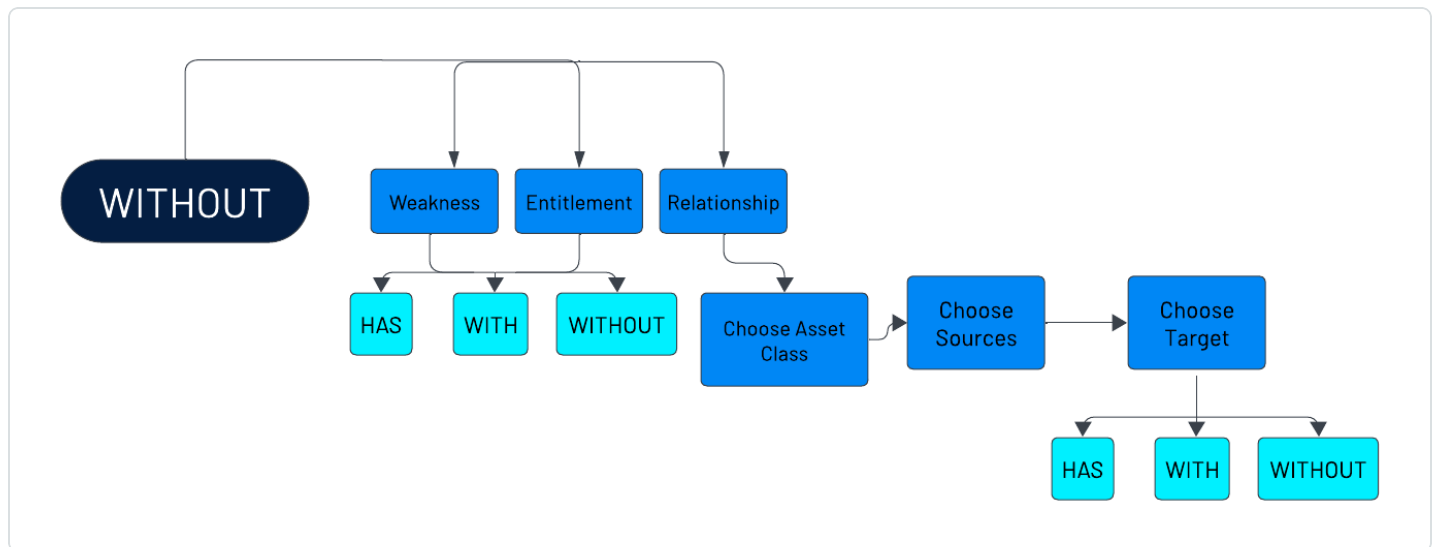


Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

WITHOUT

The Boolean operator **WITHOUT** is used to exclude specific results from a search query. It allows you to refine your search criteria and narrow down the results by eliminating items that meet certain conditions. By using **WITHOUT**, you can focus on the results that are most relevant to your search and exclude those that are not.



Once you select **WITHOUT**, you can then select one of the following cross-references:

Entitlement

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.



Choose a cross-reference

Generated by AI

Weakness

Entitlement

Relationship

ENTITLEMENT

A right to access a resource

An entitlement is a right or permission granted to an individual or entity to access a specific resource, system, or information. It defines the level of access and the specific actions that the individual or entity is authorized to perform. Entitlements are often used in the context of cybersecurity to control and manage access to sensitive data, systems, or applications.

Here are some key points to understand about entitlements in the context of cybersecurity:

- **Access Control:** Entitlements are a fundamental aspect of access control mechanisms, which determine who can access what resources and under what conditions.
- **Role-Based Access Control (RBAC):** RBAC is a common approach to managing entitlements, where users are assigned roles, and each role is associated with a set of permissions or entitlements.
- **Least Privilege Principle:** The principle of least privilege states that users should only be granted the minimum level of entitlements necessary to perform their tasks, reducing the risk of unauthorized access.
- **Identity and Access Management (IAM):** IAM systems manage user identities, authentication, and entitlements, ensuring that only authorized individuals have access to the appropriate resources.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

✕ To delete



After you select **Entitlement**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Entitlement Properties](#) for a list of options.



Once you have selected an entitlement property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the entitlement property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:



- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Finding

A finding is a single instance of a vulnerability (weakness or misconfiguration) appearing on an asset, identified uniquely by plugin ID, port, and protocol.

CROSS-REFERENCES

Generated by AI

Entitlement	<h2>FINDING</h2>
Finding	<h3>A potential security issue detected on an AS.</h3>
Relationship	A finding represents a potential security issue or vulnerability detected on an AS within Cyber Asset Management. These findings are crucial for identifying and addressing weaknesses in your environment.
Software	Here's a breakdown of what findings entail:
Weakness	<ul style="list-style-type: none">• Vulnerability Identification: Findings often highlight specific vulnerabilities present on AS, such as outdated software, misconfigurations, or known security flaws.• Risk Assessment: Each finding is typically associated with a risk level, helping prioritize remediation efforts based on the potential impact and likelihood of exploitation.• Remediation Guidance: Cyber Asset Management may provide recommendations or guidance on how to address or mitigate the identified finding, reducing the overall AES.• Continuous Monitoring: Findings are continuously monitored to track their status and ensure timely remediation, improving the overall security posture.

←

→

↑

↓

To navigate

↩

To select

ESC

To dismiss

✕

To delete



After you select **Finding**, you can select one of the following options:



- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Finding Properties](#) for a list of examples.



Once you have selected a finding property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the finding property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Relationship

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.



Choose a cross-reference

Generated by AI

Weakness

Entitlement

Relationship

RELATIONSHIP

Connection between assets

A relationship is a connection or association between two or more assets in a network. It represents the logical or physical connectivity and dependencies between assets, providing a comprehensive view of the network infrastructure and its components.

Here are some key points to understand about relationships in the context of cyber security:

- **Asset Discovery:** Relationships help in identifying and mapping the connections between assets, enabling a comprehensive understanding of the network infrastructure.
- **Vulnerability Assessment:** By understanding the relationships between assets, security teams can identify potential attack paths and assess the impact of vulnerabilities on interconnected systems.
- **Threat Detection and Response:** Relationships provide context to security alerts and incidents, allowing analysts to quickly identify affected assets and prioritize response efforts.
- **Compliance and Risk Management:** Relationships aid in assessing compliance with regulatory requirements and managing risks associated with interconnected assets.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Relationship**, you must select one or more sources. See [Relationship Sources and Targets](#) for a list of options.



Then, you must select a target. See [Relationship Sources and Targets](#) for a list of options.



After you select a target, you can select one of the following options:

- **HAS** – Select **HAS** to select a subset of criteria to include in your query. Optionally, after selecting **HAS**, you can select **NOT** to exclude the criteria from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.



Optionally, repeat the steps to exclude a [Finding](#), [Weakness](#), [Entitlement](#), [Query Operators](#), [Properties, and Selectors](#), or [Software](#) application to the target portion of the query.



Once you have selected the operators for any properties you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.

Software

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.

CROSS-REFERENCES

Generated by AI

Entitlement

Finding

Relationship

Software

Weakness

SOFTWARE

A type of keyword

Software is a type of keyword used in inventory application to identify and classify assets based on their software components. It allows users to gain insights into the software installed on their devices, including operating systems, applications, and other software packages.

Here are some key points to understand about software:

- **Software Identification:** Automatically discovers and identifies software installed on devices within the organization's network. This information is crucial for understanding the software landscape and potential vulnerabilities associated with specific software versions.
- **Software Inventory:** Maintains an inventory of all software identified on devices, providing a comprehensive view of the software assets within the organization. This inventory helps in tracking software licenses, managing software updates, and ensuring compliance with software policies.
- **Software Vulnerabilities:** Correlates software information with known vulnerabilities, enabling users to identify devices that are potentially vulnerable to specific software exploits. This allows organizations to

← → ↑ ↓ To navigate

↩ To select

ESC To dismiss

✕ To delete



After you select **Software**, you can select one of the following options:



- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain.



Once you have selected a software property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the software property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:

- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Weakness

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.



Choose a cross-reference

Weakness

Entitlement

Relationship

Weakness

Flaw or fault in the system

A weakness is a flaw or fault in the system that makes it susceptible to attack, compromise, or unauthorized access. Weaknesses can exist in various forms, such as software vulnerabilities, misconfigurations, or human errors. They can be caused by design flaws, implementation mistakes, or inadequate security measures.

Here are some key points to understand about weaknesses in the context of cyber security:

- **Vulnerabilities:** Vulnerabilities are specific weaknesses in software, hardware, or system configurations that can be exploited by attackers to gain unauthorized access or compromise the system.
- **Misconfigurations:** These are incorrect or insecure configurations of systems, devices, or software that can introduce weaknesses and make them vulnerable to attacks.
- **Human Errors:** Human mistakes, such as using weak passwords, failing to apply security patches, or mishandling sensitive data, can create weaknesses that can be exploited by attackers.
- **Inadequate Security Measures:** Insufficient security controls, such as lack of encryption, weak authentication mechanisms, or inadequate access controls, can lead to weaknesses in the system.

← → ↑ ↓ To navigate

↩ To select

esc To dismiss

⌫ To delete



After you select **Weakness**, you can select one of the following options:

- **HAS – Select HAS to select a subset of criteria to include in your query. Optionally, after selecting HAS, you can select NOT to exclude the criteria from the query.**



If you select **HAS**, you can select the property that you want the search results to contain. See [Key Weakness Properties](#) for a list of examples.:



Once you have selected a weakness property, you can further refine your query using the [Available Operators](#).

Note: Some operators depend on the weakness property that you selected in the previous step.



Once you have selected your operator for the property you included, you can begin your search based on the defined criteria, or you can select more items to add to the query:



- **AND** – Combine the criteria defined in the query.
- **OR** – Return query results that match either of the criteria defined in the query.
- **WITH** – Select additional criteria to include with the query.
- **WITHOUT** – Select additional criteria to exclude from the query.
- **WITH** – Select **WITH** to specify additional filtering criteria to include within the query.
- **WITHOUT** – Select **WITHOUT** to specify additional filtering criteria to exclude from the query.

Key Asset Properties

Asset Property	Definition
Asset ID	An asset ID is a unique identifier that is assigned to each asset in a cyber asset management system. This identifier can be used to track the asset, its associated vulnerabilities, and its security posture.
Asset Class	An asset class is a group of assets that share common characteristics. Asset classes can be used to group assets together for reporting, analysis, and other purposes.
Group Name	The group name is a string that identifies the group to which an asset belongs. Groups can be used to organize assets and to apply policies to groups of assets.
Provider Names	The provider name is the name of the cloud provider that owns the asset.
Provider Identifier	A provider identifier is a unique identifier for an asset that is assigned by the asset's provider. This identifier can be used to track the asset and its associated data.
Created Date	The created date is the date and time an asset was first created in the system.
Last Observed At	The last observed at property indicates the date and time an asset was last seen by a Tenable scanner.



Cloud Name	The cloud name is a property that identifies the cloud provider for an asset. It is typically a string value that is unique to each cloud provider.
Host Name	The host name is a unique name that is assigned to a device. It is used to identify the device on the network and to access its resources.

Key Finding Properties

Finding Property	Definition
Finding Name	The specific identifier or label given to a security finding or alert generated by a vulnerability scan or other security monitoring tools. It helps to distinguish and categorize different types of security events based on their characteristics and potential impact.
Severity	Indicates the level of potential risk posed by a security vulnerability. It helps prioritize remediation efforts by highlighting the most critical vulnerabilities that require immediate attention.
State	The current status of the finding, for example Active or Fixed . This status helps you track the progress of remediation efforts and provides insights into the overall security posture.
First Seen (observed)	The date on which Tenable Exposure Management first identified and added an asset to its inventory.
Last Seen	The most recent date and time when a specific asset or resource was detected as active or online within your monitored environment.
VPR Score	The Vulnerability Priority Rating (VPR) of the finding.
Product Code	A unique identifier assigned to a specific vulnerability or security issue within a software product or system. These codes help in tracking, categorizing, and managing vulnerabilities effectively.
Detection Family	A classification or grouping of security findings based on the underlying techniques or methods used to identify potential vulnerabilities or security risks.



Key Weakness Properties

Weakness Property	Definition
Weakness ID	A weakness is a vulnerability that can be exploited by an attacker to compromise a system or asset. The Weakness Id is a unique identifier that is assigned to each weakness.
Provider Code	A provider code is a unique identifier that is used to identify the provider of a weakness.
Product Code	A product code is a unique identifier for a product. It is typically used to track the product throughout its lifecycle, from development to manufacturing to distribution to sale.
Detection Code	A detection code is a string of characters that can be used to identify a specific weakness.
Weakness Type	A weakness type is a category of weakness. It is used to group weaknesses together based on their common characteristics.
Last Updated	The last updated date and time for a weakness is the date and time when the weakness was last modified or updated.
Severity	The severity of a weakness is a measure of the potential impact that an exploit of the weakness could have on an organization.

Key Entitlement Properties

Entitlement Property	Definition
Name	The name of an object is a unique identifier that is used to refer to the object. It can be a string, number, or other type of data.
Type	The type of an entitlement is a string that indicates the type of resource that the entitlement grants access to.
Provider Type	The provider type is the type of entity that provides the asset. For example,



	a cloud provider, an on-premises provider, or a SaaS provider.
Target Asset ID	The Target Asset ID is a unique identifier for an asset. It is used to track and manage entitlements, and to ensure that the correct permissions are granted to the correct users.

Relationship Sources and Targets

Source / Target	Definition
Account	An account is a record of a user's identity and permissions on a system. It typically includes a username, password, and other information such as the user's name, email address, and role.
Container	A container is a software package that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.
Device	A device is typically defined as a physical or virtual component that can connect to a network, communicate with other devices, and perform specific functions or tasks.
Group	A group is a collection of assets that share common characteristics.
Infrastructure as Code	Infrastructure as code (IaC) is a method of managing and provisioning IT infrastructure using code. IaC treats infrastructure as a set of resources that can be managed and provisioned using code.
Other Resource	Other resources are assets that do not fall into any of the other categories. They can include things like software applications, databases, and websites.
Resource	A resource is a type of asset that can be managed by Tenable Inventory. Resources can be physical or virtual, and they can be located on-premises or in the cloud.
Role	A role is a type of asset that represents a specific function or purpose. For example, a web server role might represent a server that is used to host websites.
Web Application	A web application is a software application that is accessed via a web



browser. It is typically hosted on a web server and can be accessed by anyone with an internet connection.

Available Operators

Operator	Definition
Exists	The Exists operator is used to check if a field is not null. It can be used in queries to filter out results that do not have a value for a particular field.
Does not Exist	The Does not Exist operator is used to check if a field is null. This can be used to filter out objects that do not have a value for a particular field.
Contains	The Contains operator is used to check if a string contains a specific value.
Not Contains	The Not Contains operator is used to exclude a value from a list. It is typically used in queries to filter out specific objects or values.
After/Greater Than	The After/Greater Than operator is used to compare two values and return true if the first value is greater than the second value.
Before/Less Than	The Before/Less Than operator is used to compare two values and return true if the first value is less than the second value.
Between	The Between operator is used to compare a value to a range of values.
Equal To	The Equal To operator is used to compare two values and returns true if they are equal.
Not Equal	The Not Equal operator is used to compare two values and return true if they are not equal.
Older Than	The Older Than operator is used to compare date property to a given period from now.
Newer Than	The Newer Than operator is used to compare a date property to a given period from now.
Within Last	The Within Last operator is used to specify a time range.