Attack Path Analysis User Guide

Last Revised: March 13, 2025

Table of Contents

Welcome to Attack Path Analysis **5**

Use Cases 6

Get Started with Tenable One 7

Configure your "Point Products" to get Data into Tenable One 8

License, Access, and Log In 9

Configure Tenable One for Use 10

Analyze and Assess 10

System Requirements 13

Key Terms 13

Example Workflow 17

Data Sources 19

Data Timing 21

Plugins Required for Attack Path Analysis 22

Attack Path Analysis Metrics 24

Data Timing 24

Cyber Exposure Score (CES) 24

Asset Exposure Score (AES) 25

Asset Criticality Rating (ACR) 25

Vulnerability Priority Rating (VPR) 25

Attack Path Analysis Exposure Management Classes 26

Scoring Caveats within Tenable One 26

Log in to Attack Path Analysis 27

Navigate Attack Path Analysis 28

Log out of Attack Path Analysis 34
Attack Path Analysis **35**
Attack Path Analysis Dashboard 38
Mitre Att&ck Heatmap 40
Findings 42
Export a Finding 49
Add and View Comments on a Finding 49
Change the Status of a Finding 50
Archive a Finding 51
View Finding Details 52
Share Finding Details 56
View Log History 57
Discover 58
Generate an Attack Path Query with the Attack Path Query Builder 63
(Optional) Save your Query as a Preset/Bookmark 67
Generate an Asset Exposure Graph Query 67
Generate a Blast Radius Query 70
Interact with Attack Path Query Data 72
Information Panel 78
Generate an Asset Query with the Asset Query Builder 81
Interact with Asset Query Data 83
Information Panel 88
Generate an Attack Path with a Built-in Query 91
Query Types in the Attack Path Query Library 93

Attack Path Analysis Techniques 97
Access the Settings Menu 98
System Settings 99
License Information 99
User Management 99
Roles 100
Authentication 101
Activity Logs 101

Welcome to Attack Path Analysis

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

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

The Tenable One platform enables you to:

- Get comprehensive visibility of all assets and vulnerabilities, whether on-premises or in the cloud, and understand where they are exposed to risk.
- Anticipate threats and prioritize efforts to prevent attacks by using generative AI and the industry's largest dataset of vulnerability and exposure context.

  > **Note:** Generative AI is not supported in Tenable FedRAMP Moderate.

- Communicate exposure risk to business leaders and stakeholders with clear KPIs, benchmarks, and actionable insights.
- Leverage the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps, and identity systems.
- Integrate with third-party data sources and tools for enhanced exposure analysis and remediation.

> **Tip:** For additional information on getting started with Tenable One products, check out the Tenable One Deployment Guide and review the following customer education materials:
>
> - Tenable One Introduction (Tenable University)

Tenable One is a package that includes the following products:

- Tenable Vulnerability Management
- Tenable Web App Scanning

- Tenable Cloud Security
- Tenable Identity Exposure
- Tenable Attack Surface Management
- Lumin Exposure View
- Tenable Inventory
- Attack Path Analysis

Use Cases

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

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

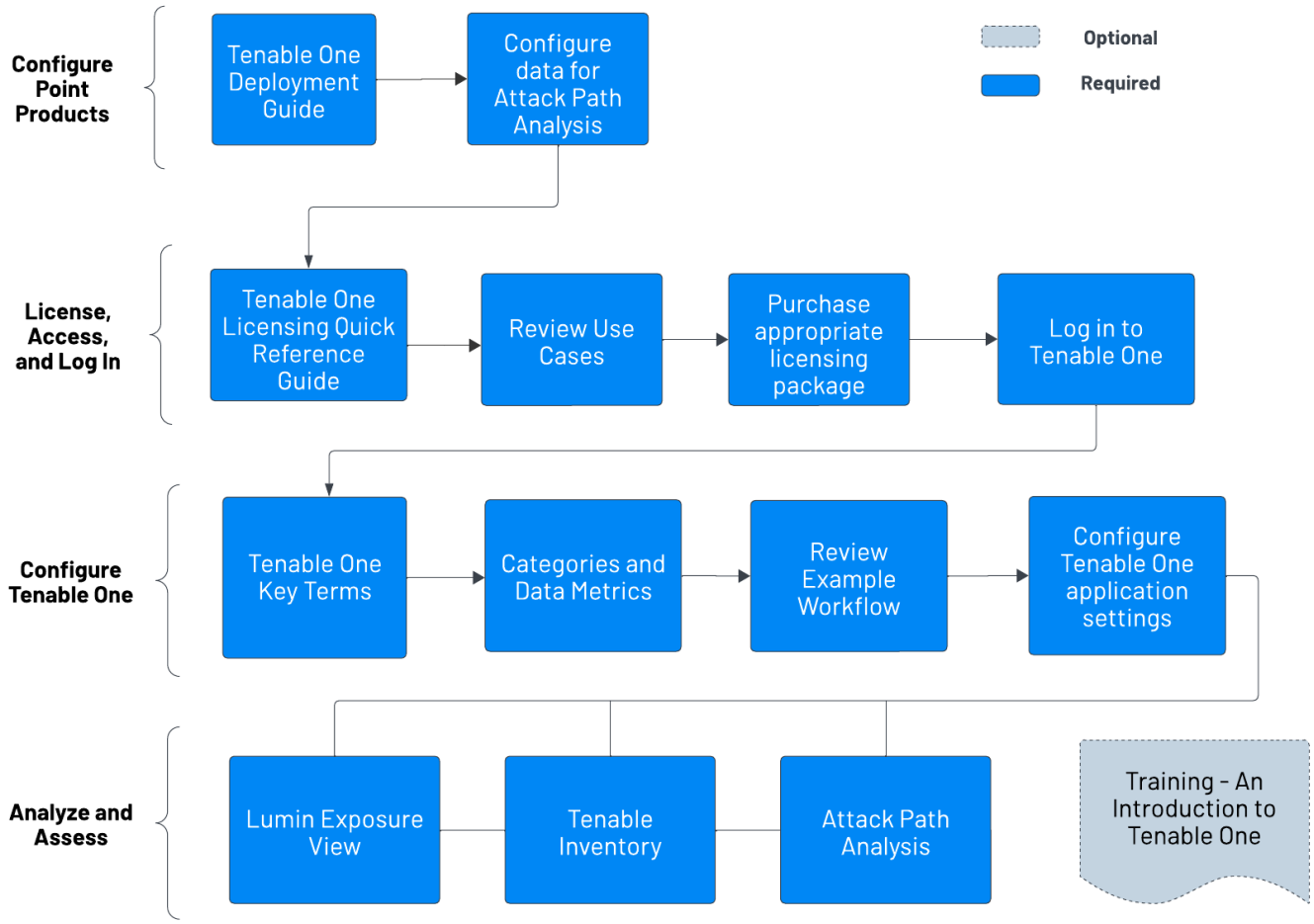
Both CISO/Executives and Security Practitioners	Utilize Tenable Inventory to:
	• In the Exposure Signals section:
	  • Gain visibility into your most critical risk scenarios by viewing risk combinations of that could make any weakness potentially dangerous to your business
	  • Generate exposure signals that use queries to search for asset violations and view business-specific risks and weaknesses.
	• View and manage all assets, regardless of their source.
	• View and manage weaknesses across all of your vulnerability findings.
	• Consolidate data in one location, reducing license and maintenance costs
	• Utilize existing tags or create new tags that can be used to create custom exposure cards.

For more information, see Get Started with Tenable One.

Get Started with Tenable One

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

> **Tip:** Click a box to view the relevant task.



Configure your "Point Products" to get Data into Tenable One

To get data into Tenable One, you must first configure and deploy the Tenable One "point products". Once these are configured, Tenable One can then ingest the data and present it.

Tip: For additional information on getting started with Tenable One products, check out the following resources:

- Tenable One Deployment Guide
- Tenable One Introduction (Tenable University)

For Attack Path Analysis, ensure you have the following:

- A Tenable Vulnerability Management Basic Network Scan with credentials.
- One of the following:
    - A Tenable Vulnerability Management basic scan using the **Active Directory Identity** scan template. This scan type requires fewer permissions, and provides a basic overview of your active directory entities.

      > **Note:** You can run this scan type on its own, or as part of a Basic Network Scan. In a Basic scan, you must ensure the **Collect Identity Data from Active Directory** option is enabled in the **Discovery** section.

    - Tenable Identity Exposure SaaS deployed.

  > **Note:** Because the plugin only supports up to 7,000 identities, the **Active Directory Identity** scan template is not designed for large environments, but is instead intended to help small customers kick start their use of Attack Path Analysis. Tenable recommends that larger customers deploy Tenable Identity Exposure.

- Additionally, for best performance, Tenable recommends the following:
    - Have at least 40% of assets scanned via an authenticated scan.
    - Select maximum verbosity in the Basic Network Scan.
    - A default Tenable Web App Scanning scan, including injection plugins. At least 40% of the web applications should be scanned.
    - An AWS connection with a Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.
    - When using Tenable Identity Exposure, enable privileged analysis. This option highlights key attack vectors used by hackers and gives you a better understanding of your attack surface, including credential auditing and password analysis.
    - A scan frequency of at least once a week.
    - Configure Tenable OT Security.
    - Configure Tenable Attack Surface Management.

License, Access, and Log In

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

To acquire a license:

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

To access and log in to Attack Path Analysis:

- Review the System Requirements.
- Follow the Log in to Attack Path Analysis steps.

Configure Tenable One for Use

- Familiarize yourself with the Tenable One key terms.
- Familiarize yourself with the categories and data metrics within Tenable One.
- Review the Tenable One Example Workflow.
- Configure your Tenable One settings.

Analyze and Assess

Perform analysis on your data within Tenable One:

- Access Lumin Exposure View, where you can gain critical business context by getting business-aligned cyber exposure score for critical business services, processes and functions, and track delivery against SLAs. Track overall VM risk to understand the risk contribution of assets to your overall Cyber Exposure Score, including by asset class, vendor, or by tags.
    - View, create, and manage cyber exposure cards.
    - View CES and CES trend data for any exposure card.

> **Tip:** When viewing exposure cards, you can toggle between **Score** and **Score (Beta)** to compare the differences in your scoring using old and new Tenable data models. For more information, see View Your CES.

    - View Remediation Service Level Agreement (SLA) data.
    - View Tag Performance data.
    - View Tenable blog posts related to vulnerability events via the **News** tab.

- Access Tenable Inventory, where you can enhance asset intelligence by accessing deeper asset insights, including related attack paths, tags, exposure cards, users, relationships, and more. Improve risk scoring by gaining a more complete view of asset exposure, with an asset exposure score that assesses total asset risk and asset criticality.
    - View, generate, and interact with the data from queries and their impacted asset violations via the Exposure Signals page.
        - Find top active threats in your environment with up-to-date feeds from Tenable Research.
    - View and interact with the data in the Assets view:
        - Unify all assets in a single view to simplify analysis, understand relationships, and discover exposures across the attack surface.
        - Familiarize yourself with the Global Search query builder and its objects and properties. Bookmark custom queries for later use.
        - Find devices, user accounts, software, cloud assets, SaaS applications, networks, and their weaknesses.
        - Drill down into the asset details page to view asset properties and all associated context views.
    - View and interact with the data in the Tags view.
        - Create tags to highlight or combine different asset classes.
    - View and interact with the data in the Weaknesses view:

        - View key context on weaknesses to make the most impactful remediation decisions.

- Access Attack Path Analysis, where you can optimize risk prioritization by exposing risky attack paths that traverse the attack surface, including web apps, IT, OT, IoT, identities, ASM, and prevent material impact. Streamline mitigation by identifying choke points to disrupt attack paths with mitigation guidance, and gain deep expertise with AI insights.

  Note: Generative AI is not supported in Tenable FedRAMP Moderate.

  - View the **Attack Path Analysis Dashboard** for a high-level view of your vulnerable assets such as the number of attack paths leading to these critical assets, the number of open findings and their severity, a matrix to view paths with different source node exposure score and ACR target value combinations, and a list of trending attack paths.

    - Review the **Top Attack Path Matrix** and click the **Top Attack Paths** tile to view more information about paths leading to your “Crown Jewels”, or assets with an ACR of 7 or above.

    You can adjust these if needed to ensure you’re viewing the most critical attack path data and findings.

  - On the **Findings** page, view all attack techniques that exist in one or more attack paths that lead to one or more critical assets by pairing your data with advanced graph analytics and the MITRE ATT&CK® Framework to create Findings, which allow you to understand and act on the unknowns that enable and amplify threat impact on your assets and information.

  - On the **Discover** page, generate attack path queries to view your assets as part of potential attack paths:

    - Generate an Attack Path using a Built-in Query
    - Generate an Asset Query using the Asset Query Builder
    - Generate an Attack Path Query using the Attack Path Query Builder

    Then, you can view and interact with the Attack Path Query and Asset Query data via the

query result list and the interactive graph.

- Interact with the MITRE Att&ck Heatmap.

System Requirements

Display Settings

Minimum screen resolution: 1440 x 1024

Supported Browsers

Tenable One supports the latest versions of the following browsers.

Note: Before reporting issues with Tenable One, ensure your browser is up to date.

- Google Chrome
- Apple Safari
- Mozilla Firefox
- Microsoft Edge

Note: Tenable One is not supported on mobile browsers.

Key Terms

The following key terms apply to the Attack Path Analysis user interface.

Term	Definition
Active Directory (AD)	Attack Path Analysis integrates AD data from Tenable Identity Exposure.
Asset	Any IT or security element in your organization such as user accounts, computers, and software. The **Discover** section represents an asset as a node in the graph.
Asset Exposure	A visualization of an attack path from multiple assets down to one asset.

Graph	
Asset Exposure Score (AES)	Tenable calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure
Asset Vulnerability Rating (AVR)	An aggregation of all Vulnerability Priority Rating (VPR) scores for vulnerabilities detected on an asset.
Benchmark	A group of scores to which you can compare your scores and assess your performance.
Blast Radius	A visualization of one or more attack paths from one asset to multiple other assets.
CES Trend	A measurement that defines how your CES improves or regresses over time.
Chief Information Security Officer (CISO)	The head of cybersecurity for a company. A CISO can use the Exposure View to quickly quantify the overall enterprise risk exposure, measure its progress or regression over time and easily communicate impact and ROI to key stakeholders.
Choke Point Priority	A choke point is a place where potential attack paths merge together before reaching a critical asset. Attack Path Analysis uses Choke Point Priority as a prioritization metric for attack techniques based on the number of attack paths exploiting the attack, the number of critical assets it leads to, and complexity of the attack. Attack Path Analysis categorizes priority levels as **Low**, **Medium**, **High**, and **Critical**. Tenable recommends focusing on areas with higher choke points first, as remediating those will negate the largest number of critical items within your organization.
Cyber Exposure Score (CES)	Your CES quantifies the relative risk of your organization based on the threat exposure and criticality of your licensed assets. CES values range from 0 - 1000, where higher values indicate higher exposure and higher risk.

Data Source	A product that feeds data into Tenable One (for example, Tenable Vulnerability Management).
Evidence	The empirical data from different data sources confirming the feasibility of a Step as part of an attack path.
Exposure Card	An Exposure card represents the incoming data from your configured tags and data sources. It aggregates and normalizes the data to provide a visualization of your Cyber Exposure Score (CES) and other metrics. Users can create custom cards, or use Tenable-provided cards to gain insight and guidance on what areas need their attention most.
Exposure Card View	The section of the Exposure View that includes data about the selected exposure card. This section includes CES, trend, Remediation SLA, and business context information.
Exposure View	A holistic and unified view combining internal and external data sources to provide a complete view of risk in a singular location.
Finding	• Within the Lumin Exposure View interface: A single instance of a vulnerability appearing on an asset, uniquely identified by plugin ID, port, and protocol. • Within the Attack Path Analysis interface: A technique or sub-technique in that exists in one or more attack paths that lead to one or more critical assets. Each finding has a Choke Point Priority that determines its urgency and potential impact.
Industry Benchmark	A benchmark based on members of your Tenable-assigned industry to which you can compare your scores and assess your performance.
MITRE ATT&CK®	MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The MITRE ATT&CK® knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.
Node Exposure	A metric produce by Tenable One to understand the blast radius exposure

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

Top Attack Path	An attack path that leads to one or more critical assets.
Vulnerability Management (VM)	Tenable One integrates VM data from Tenable Vulnerability Management and Tenable Security Center.
Web Application Scanning (WAS)	Tenable One integrates web app scanning data from Tenable Web App Scanning.

Example Workflow

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

Getting Started

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

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

Prioritize

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

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

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

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

Customize

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

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

Incidents and Actions

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

- In my environment, what are all possible attack paths between two assets or asset types?
- In my environment, what are all possible attack paths that leverage a specific technique?
- What assets are in jeopardy if one specific asset is compromised? (Blast Radius)

- How do all assets in my network affect one specific asset in my environment? (Asset Exposure)
- Where is an asset within the attack path?
- How critical is an asset?

Data Sources

A data source is any product that feeds data into the Attack Path Analysis interface. Once you have configured a data source for use with Tenable One, the application automatically ingests data from that Tenable One product.

You can configure the following Tenable products as data sources:

- Tenable Vulnerability Management
- Tenable Security Center
- Tenable Web App Scanning
- Tenable Cloud Security
- Tenable Identity Exposure
- Tenable Attack Surface Management
- Tenable OT Security

To configure Tenable Vulnerability Management data sources:

1. Deploy Tenable Vulnerability Management according to the steps outlined in the *Tenable Vulnerability Management User Guide*, or based on guidelines received directly from Tenable Professional Services.
2. Configure Tenable Vulnerability Management for use with Tenable One by:
    - Creating and applying asset tags
    - Creating and launching scans to generate asset data

Tip: For more detailed information on configuring Tenable Vulnerability Management for use with Tenable One, see the Tenable Vulnerability Management topic in the *Tenable One Deployment Guide*.

To configure Tenable Security Center data sources:

1. Deploy Tenable Security Center according to the steps outlined in the *Tenable Security Center User Guide*, or based on guidelines received directly from Tenable Professional Services.
2. Once you have installed Tenable Security Center, follow the Tenable One Synchronization steps outlined in the *Tenable Security Center User Guide*.

Tip: For more detailed information on configuring Tenable Security Center for use with Tenable One, see the Tenable Security Center topic in the *Tenable One Deployment Guide*.

To configure Tenable Web App Scanning data sources:

1. Deploy Tenable Web App Scanning according to the steps outlined in the *Tenable Web App Scanning User Guide*, or based on guidelines received directly from Tenable Professional Services.
2. Create some quick scans to provide a high-level assessment of the target to establish your baseline.

Tip: For more detailed information on configuring Tenable Web App Scanning for use with Tenable One, see the Tenable Web App Scanning topic in the *Tenable One Deployment Guide*.

To configure Tenable Cloud Security data sources:

Deploy Tenable Cloud Security according to the steps outlined in the Tenable Cloud Security *User Guide*, or based on guidelines received directly from Tenable Professional Services.

Tip: For more detailed information on configuring Tenable Cloud Security for use with Tenable One, see the Tenable Cloud Security topic in the *Tenable One Deployment Guide*.

To configure Tenable Identity Exposure data sources:

1. If necessary, activate Tenable Identity Exposure for use within your Tenable One platform.
2. Deploy Tenable Identity Exposure according to the steps outlined in the *Tenable Identity Exposure User Guide*, or based on guidelines received directly from Tenable Professional Services.
3. Configure Tenable Identity Exposure for use with Tenable One by:

- Downloading and configuring the license file
- Downloading and installing the Secure Relay
- Configuring Forests

Tip: For more detailed information on configuring Tenable Identity Exposure for use with Tenable One, see the Tenable Identity Exposure topic in the *Tenable One Deployment Guide*.

To configure Tenable Attack Surface Management data sources:

1. Deploy Tenable Attack Surface Management according to the steps outlined in the *Tenable Attack Surface Management User Guide*, or based on guidelines received directly from Tenable Professional Services.
2. Configure Tenable Attack Surface Management for use with Tenable One by:
    - Configuring domains within Tenable Attack Surface Management
    - Configuring data sets and confirming your entire attack surface is present

Tip: For more detailed information on configuring Tenable Attack Surface Management for use with Tenable One, see the Tenable Attack Surface Management topic in the *Tenable One Deployment Guide*.

To configure Tenable OT Security data sources:

1. Install the Tenable OT Security appliance according to the steps outlined in the *Tenable OT Security User Guide*.
2. (Optional) If you want to pair your sensors with the Industrial Core Platform (ICP), install the OT Security Sensor according to the steps outlined in the *Tenable OT Security User Guide*.
3. Generate a Tenable OT Security**Linking Key** and determine your **Cloud Site** according to the steps outlined in the *Tenable Vulnerability Management User Guide*. Copy and save this information to link the connector to Tenable One.
4. Integrate your Tenable OT Security appliance with Tenable One according to the steps outlined in the *Tenable OT Security User Guide*.

Tip: For more detailed information on configuring Tenable OT Security for use with Tenable One, see the Tenable OT Security topic in the *Tenable One Deployment Guide*.

Data Timing

Data within Attack Path Analysis refreshes on the following cadence:

- Asset Data – Asset information is updated every time the asset is seen as part of a scan.
- Tag Application – When a tag is first created, it can take several hours to assign the tag to the appropriate asset, depending on the number of assets and the tag's rules.
- Tag Reevaluation – Every 12 hours, Attack Path Analysis automatically reevaluates tags to ensure they apply to newly discovered assets, and are removed from any inactive assets.
- Tenable Cloud Security data – Attack Path Analysis automatically refreshes Tenable Cloud Security data every 24 hours.

Plugins Required for Attack Path Analysis

Attack Path Analysis requires the following plugins:

Tenable Nessus Plugins:

- 10396
- 20811
- 22869
- 24272
- 25202
- 25203
- 44401
- 48942
- 51187
- 57364
- 60119
- 64582
- 66334
- 71246

- 72387
- 72684
- 86420
- 92364
- 92367
- 92373
- 95928
- 97993
- 100871
- 126527
- 159817
- 159929

Tenable Web App Scanning Plugins:

- 98113
- 98114
- 98115
- 98116
- 98117
- 98118
- 98119
- 98120
- 98121
- 98122
- 98123

- 98124
- 98127
- 98623
- 112614
- 112684
- 113069
- 113162
- 113212

Attack Path Analysis Metrics

The following metrics are used to assess data within Attack Path Analysis:

Data Timing

Data within Attack Path Analysis refreshes on the following cadence:

- Asset Data – Asset information is updated every time the asset is seen as part of a scan.
- Tag Application – When a tag is first created, it can take several hours to assign the tag to the appropriate asset, depending on the number of assets and the tag's rules.
- Tag Reevaluation – Every 12 hours, Attack Path Analysis automatically reevaluates tags to ensure they apply to newly discovered assets, and are removed from any inactive assets.
- Tenable Cloud Security data – Attack Path Analysis automatically refreshes Tenable Cloud Security data every 24 hours.

Cyber Exposure Score (CES)

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

> **Note:** Attack Path Analysis does not include assets older than 90 days in your CES.

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

Asset Exposure Score (AES)

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

Note: Attack Path Analysis does not calculate an AES for unlicensed assets.

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

Asset Criticality Rating (ACR)

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

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

Vulnerability Priority Rating (VPR)

Tenable calculates a dynamic VPR for most vulnerabilities. The VPR is a dynamic companion to the data provided by the vulnerability's CVSS score, since Tenable updates the VPR to reflect the current threat landscape. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploit.

VPR Category	VPR Range
Critical	9.0 to 10.0
High	7.0 to 8.9
Medium	4.0 to 6.9
Low	0.1 to 3.9

Note: Vulnerabilities without CVEs (for example, many vulnerabilities with the **Info** severity) do not receive a VPR. Tenable recommends remediating these vulnerabilities according to their CVSS-based severity.

Attack Path Analysis Exposure Management Classes

Attack Path Analysis products refer to data sources as *Exposure Management classes*. For more information, see Data Sources.

Additionally, Attack Path Analysis uses specific icons to represent these within the user interface.

Exposure Management Class	Icon(s)
Vulnerability Management	
Web Applications	
Identity Exposure	
Operational Technologies	
Cloud Security	

Scoring Caveats within Tenable One

The weakness counts and severities within the Score Breakdown tab and other areas within the Tenable Inventory user interface may not match because each segment counts instances differently:

For Tenable Vulnerability Management assets:

- Weakness counts: Are distinct CVE counts
- Exposure score counts: Distinct (plugin ID, CVE ID) counts to allow for recasted plugins to affect exposure scores

For Tenable Web App Scanning assets:

- Weakness counts: Number of distinct CVEs + distinct plugins where the plugin has no CVEs but has a VPR
- Exposure score counts: Distinct plugin ID counts with VPR > 0. This is to account for plugin ID vulnerabilities with no CVE and to allow for recasted plugins to affect exposure scores

For Tenable Identity Exposure assets:

- Weakness counts: Distinct IoEs observed directly on the asset
- Exposure score counts: Includes IoEs observed directly on the asset plus those inherited from related assets to account for inherited IoEs in exposure scores

For Tenable Cloud Security assets:

- Weakness counts: Cloud Security misconfigurations plus any CVEs found on the asset
- Exposure score counts: Only Cloud Security misconfigurations are counted for exposure scores.

Log in to Attack Path Analysis

To log in to Attack Path Analysis:

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

   The **Workspace** page appears.
4. Click the Attack Path Analysis tile.

   The Attack Path Analysis interface appears.

Tip: Don't see the tile you're looking for? You may need a license for that application. See the *Tenable Licensing Guide* or contact your Tenable representative for more information.

Navigate Attack Path Analysis

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

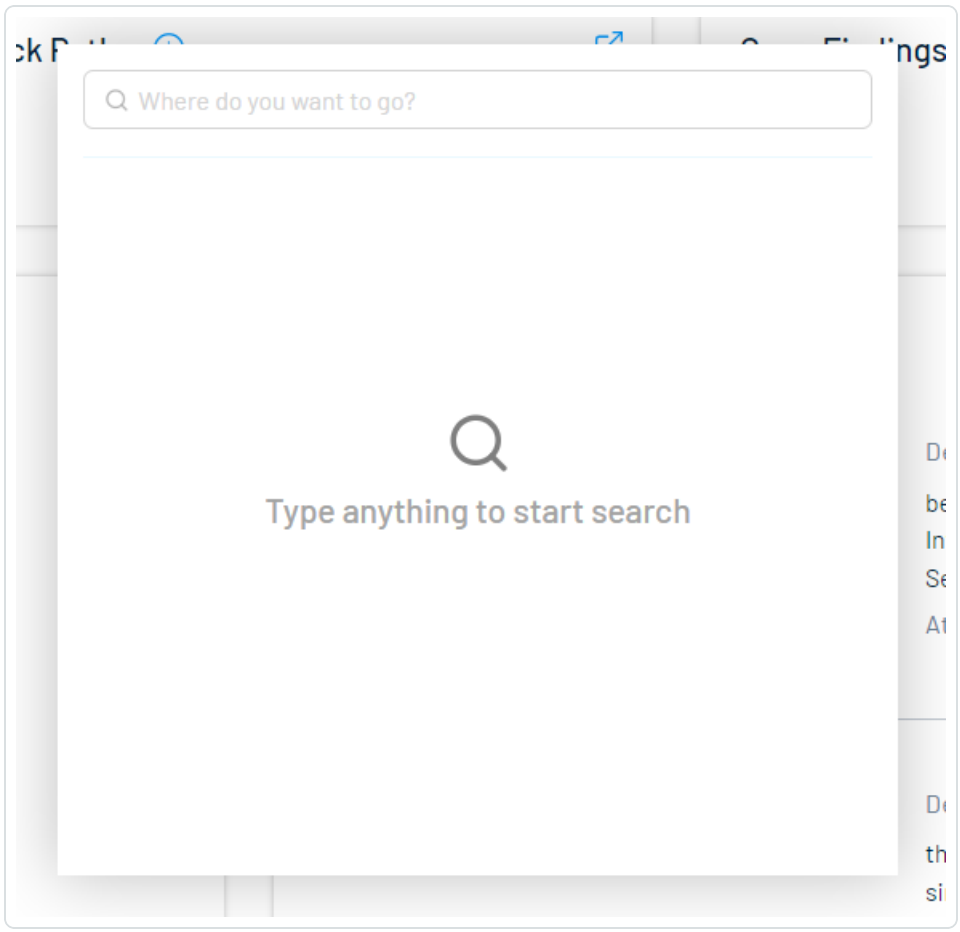
Search Application

Attack Path Analysis includes the ability to search the entire application.

To search the application:

1. Do one of the following:
   - In the upper-right corner, click the button.
   - On your keyboard, press CTRL+Shift+F.

   The search window appears.



2. In the text box, type the criteria by which you want to search the application.

   Your search results appear automatically within the search window.

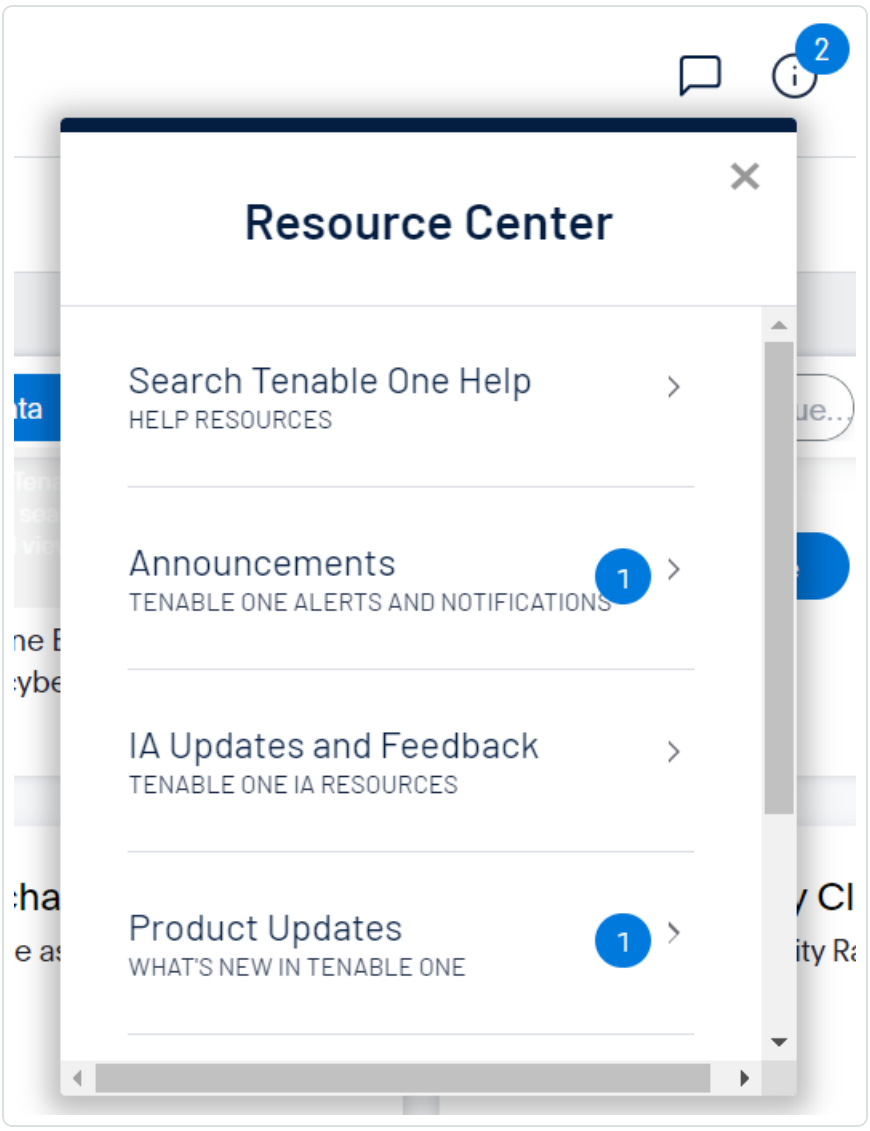
Resource Center

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

To access the Resource Center:

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

   The **Resource Center** menu appears.



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

Settings Icon

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

Workspace

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

appears in the top navigation bar.

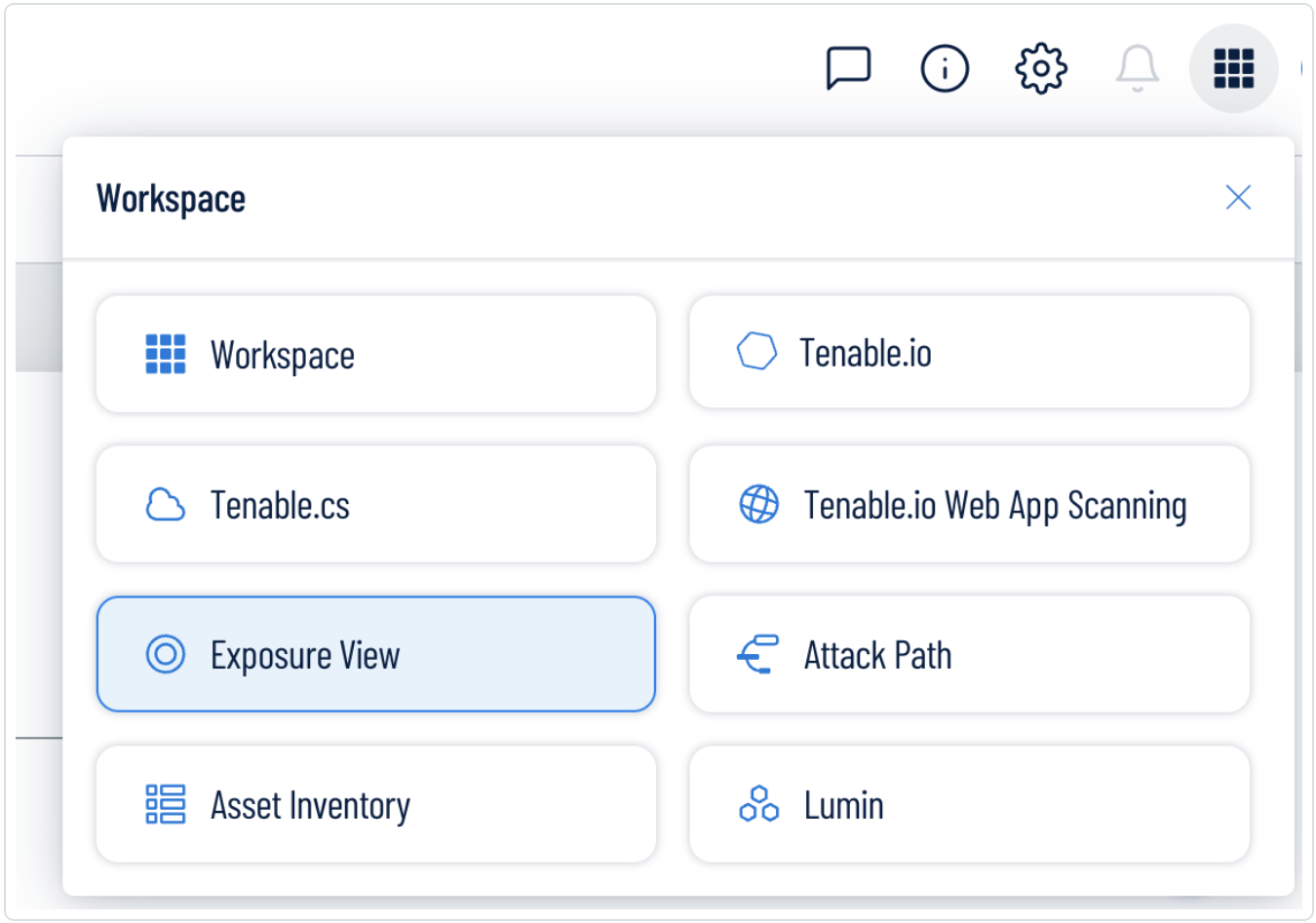
Important: Tenable disables application tiles for expired applications. Tenable removes expired application tiles from the **Workspace** page and menu 30 days after expiration.

Open the Workspace Menu

To open the **Workspace** menu:

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

   The **Workspace** menu appears.



2. Click an application tile to open it.

View the Workspace Page

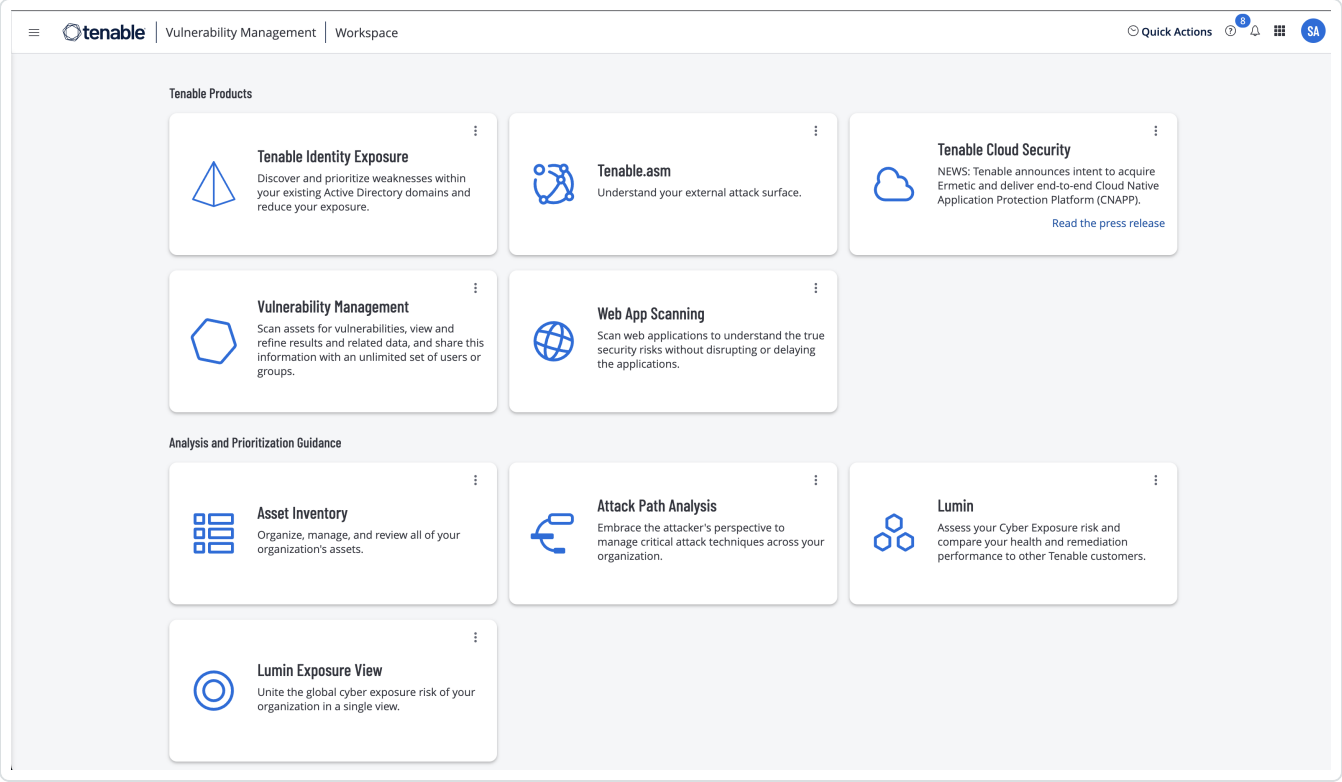
To view the Workspace page:

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

   The **Workspace** menu appears.

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

   The **Workspace** page appears.



Set a Default Application

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

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

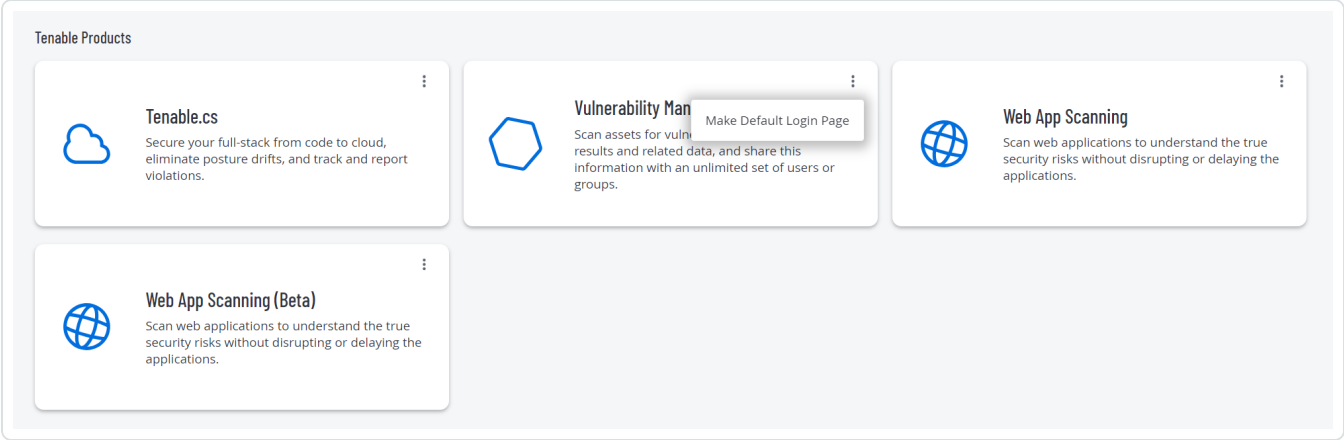
To set a default login application:

1. Log in to Tenable.

   The **Workspace** page appears.

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

   A menu appears.



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

   This application now appears when you log in.

Remove a Default Application

To remove a default login application:

1. Log in to Tenable.

   The **Workspace** page appears.

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

   A menu appears.

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

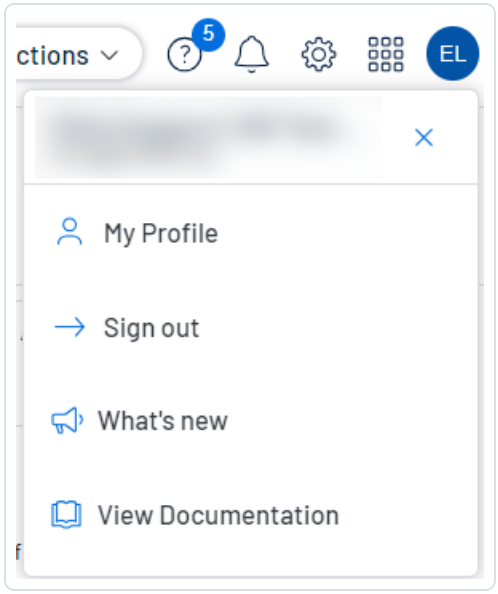
   The **Workspace** page now appears when you log in.

User Account Menu

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

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

   The user account menu appears.



2. Do one of the following:

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

Log out of Attack Path Analysis

To log out of Attack Path Analysis:

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

Attack Path Analysis

As part of a typical attack, adversaries leverage different tools and techniques to accomplish their objectives. Usually, a hacker attains an initial foothold over the network, whether by a phishing attack or exploiting a publicly exposed vulnerability. Hackers may then seem to maintain access over the machine (Persistence), elevate their privileges, and laterally pivot between network devices (Lateral Movement). Last, the hacker tries to complete their objective, for example, a denial of service of critical infrastructure, exfiltration of sensitive information, or distraction of existing services. This event is known as Attack Path. An attack path contains one or more Attack Techniques, allowing the hacker to accomplish his objective.

Attack Path Analysis takes your data and pairs it with advanced graph analytics and the MITRE ATT&CK™ Framework to create **Findings**. These **Findings** allow you to understand and take action on the unknowns that enable and amplify threat impact on your assets and information.

Additionally, you can use the **Discover** tab to dive deeper into the mind of an attacker by interacting directly with attack paths, building custom paths, and manipulating the origins and targets within a path to view exactly how these changes affect your data.

> **Note:** Data ingestion in Attack Path Analysis can take up to 5 hours.

What is Attack Path Analysis?

- *What is a top attack path?*
    - A top attack path is an attack path that leads to one or more critical assets.
- *What is a finding?*
    - A finding is an attack technique that exists in one or more attack paths that lead to one or more critical assets.
- *How does Tenable One map critical assets?*
    - Assets with an Asset Criticality Rating of 7 and above
    - Cloud resource assets marked as Sensitive
    - User account assets within Active Directory with Domain Admin rights
- *How does Tenable One classify the severity of a finding?*

- Likelihood: The number of attack paths
- Impact: The critical assets that could be compromised by the attack
- Method: The tactic associated with the attack (for example, lateral movement or privilege escalation)
- Path: The start and end points of the attack path technique

Before you begin:

For Attack Path Analysis, ensure you have the following:

- A Tenable Vulnerability Management Basic Network Scan with credentials.
- One of the following:
  - A Tenable Vulnerability Management basic scan using the **Active Directory Identity** scan template. This scan type requires fewer permissions, and provides a basic overview of your active directory entities.

    > **Note:** You can run this scan type on its own, or as part of a Basic Network Scan. In a Basic scan, you must ensure the **Collect Identity Data from Active Directory** option is enabled in the **Discovery** section.

  - Tenable Identity Exposure SaaS deployed.

  > **Note:** Because the plugin only supports up to 7,000 identities, the **Active Directory Identity** scan template is not designed for large environments, but is instead intended to help small customers kick start their use of Attack Path Analysis. Tenable recommends that larger customers deploy Tenable Identity Exposure.

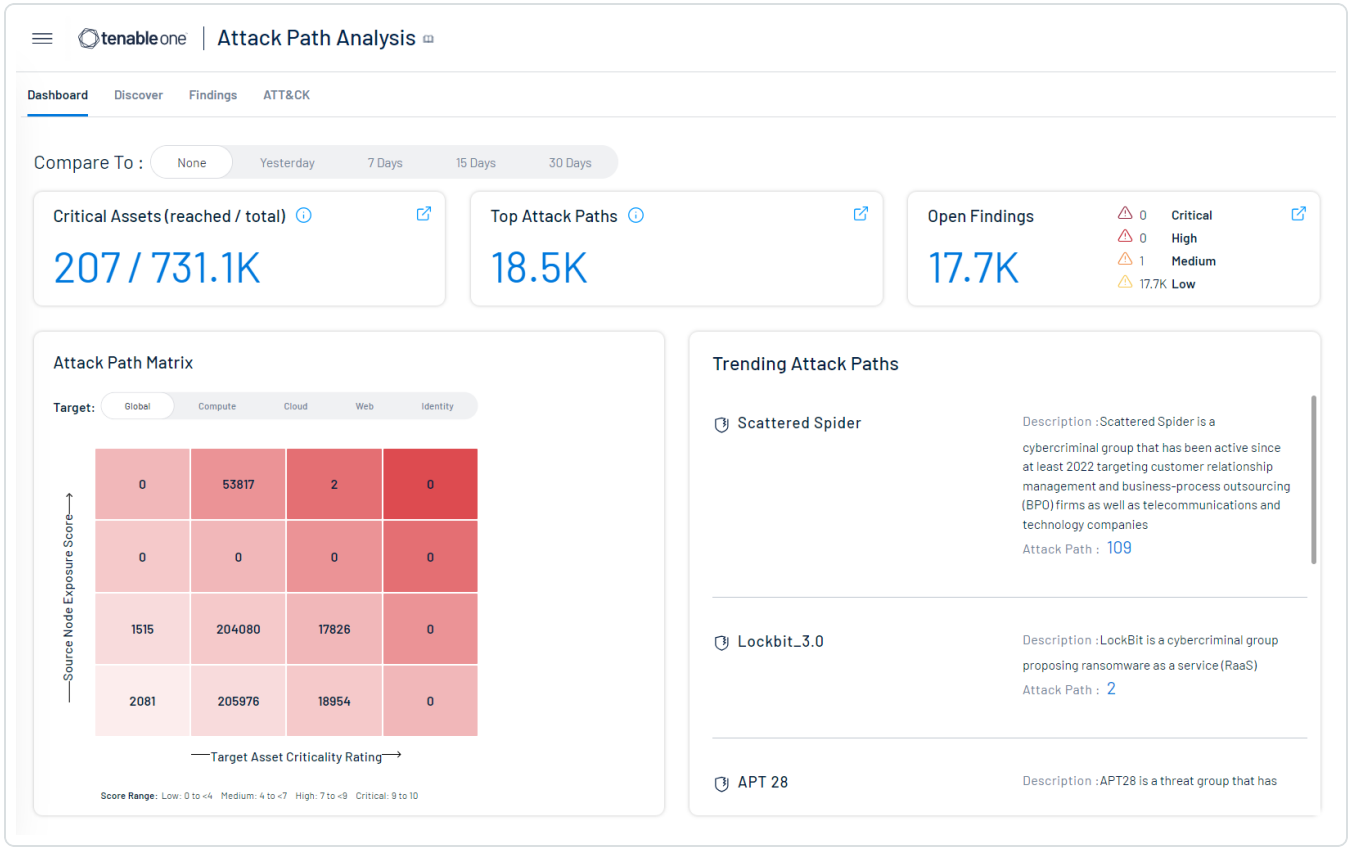
- Additionally, for best performance, Tenable recommends the following:
  - Have at least 40% of assets scanned via an authenticated scan.
  - Select maximum verbosity in the Basic Network Scan.
  - A default Tenable Web App Scanning scan, including injection plugins. At least 40% of the web applications should be scanned.

- An AWS connection with a Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.
- When using Tenable Identity Exposure, enable privileged analysis. This option highlights key attack vectors used by hackers and gives you a better understanding of your attack surface, including credential auditing and password analysis.
- A scan frequency of at least once a week.
- Configure Tenable OT Security.
- Configure Tenable Attack Surface Management.

To access **Attack Path Analysis**:

1. In the upper-left corner of the page, click the ☰ button.
2. In the **Analytics** section, click **Attack Path Analysis**.

   Attack Path Analysis appears. By default, the Attack Path Analysis Dashboard is active.



In **Attack Path Analysis**, you can:

- **Discover** additional attack data and threat possibilities.
- View your Findings.
- Interact with the Mitre Att&ck Heatmap.

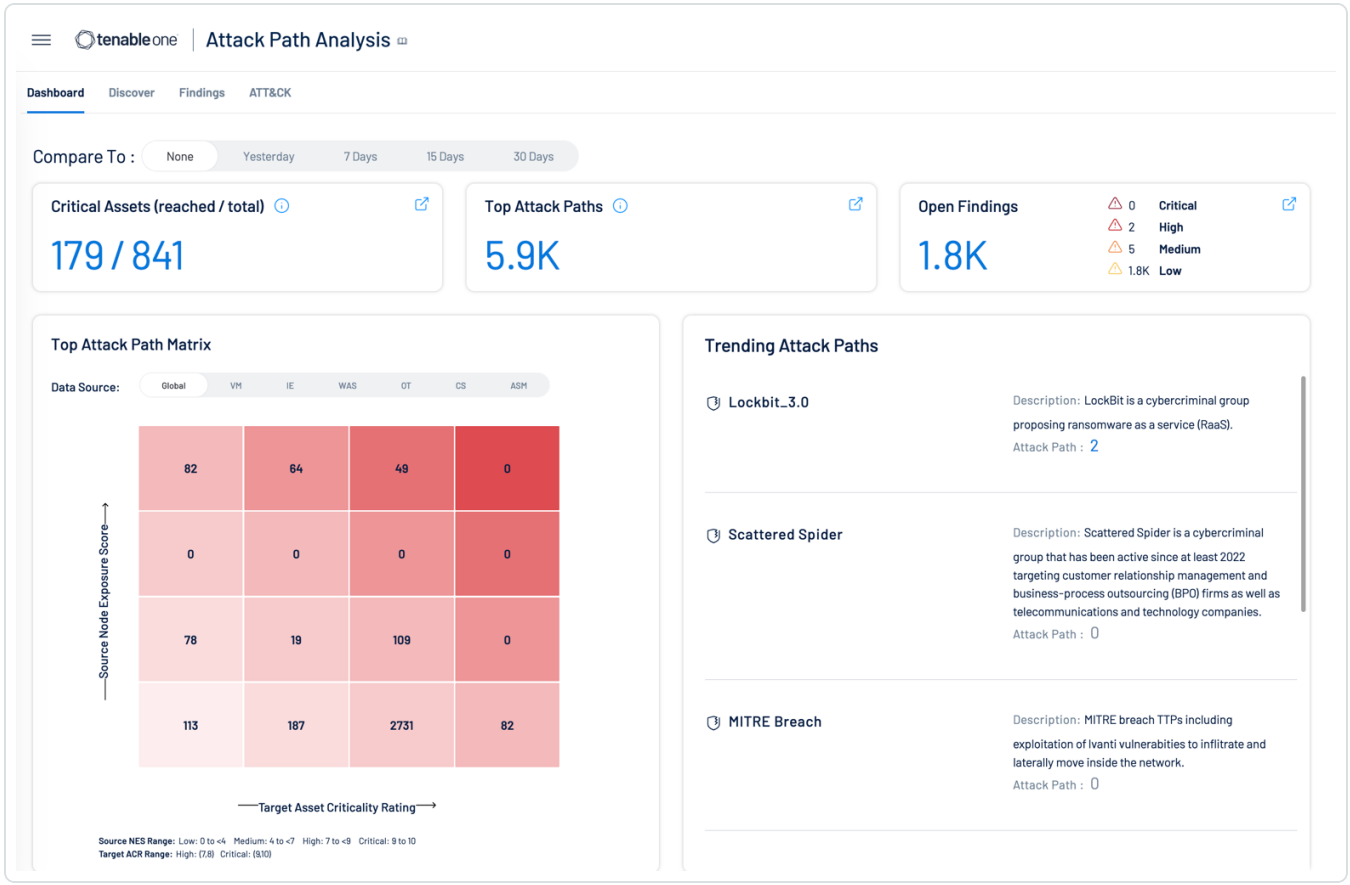
Attack Path Analysis Dashboard

The Attack Path Analysis dashboard gives you a high-level view of your vulnerable assets such as the number of vulnerable critical assets, the number of attack paths leading to these critical assets, the number of open findings and their severity, a matrix to view paths with different source node exposure score and ACR target value combinations, and a list of trending attack paths.

To access the **Dashboard** tab:

1. In the upper-left corner of the page, click the ☰ button.
2. In the **Analytics** section, click **Attack Path Analysis**.

   Attack Path Analysis appears. By default, the **Dashboard** tab is active.



The Attack Path Analysis **Dashboard** shows the following details:

Widget	Description
Compare To	Compare and view the difference between the current data and the data from a specific timeframe. You can select from these options: • **None** • **Yesterday** • **7 days** • **15 days** • **30 days** Based on the option you select, each widget lists the differences between timeframes and shows a colored directional arrow to indicate whether the value has increased or decreased.
Critical Assets (reached/total)	The number of critical assets that attack paths can lead to by the total number of critical assets in your environment. Click the icon to view the reached critical assets in the **Discover** tab.
Attack Path Leading to Critical Asset	The number of attack paths that lead to critical assets. Click the icon to view the attack paths in the **Discover** tab.
Open Findings	The total number of open findings with the number of critical, high, medium, and low severity findings. Click to view the open findings in the **Findings** tab.
Top Attack Path Matrix	Each square in the matrix shows the number of attack paths that corresponds to target Asset Criticality Rating (ACR) and Source Node Exposure Score values. This matrix includes only assets with an ACR of 7 or higher to ensure you can prioritize your most critical assets first. For example, you can quickly view the attack paths that lead to the highest ACR targets and whose source nodes have the highest exposure score source by checking the value in the square in the upper right corner

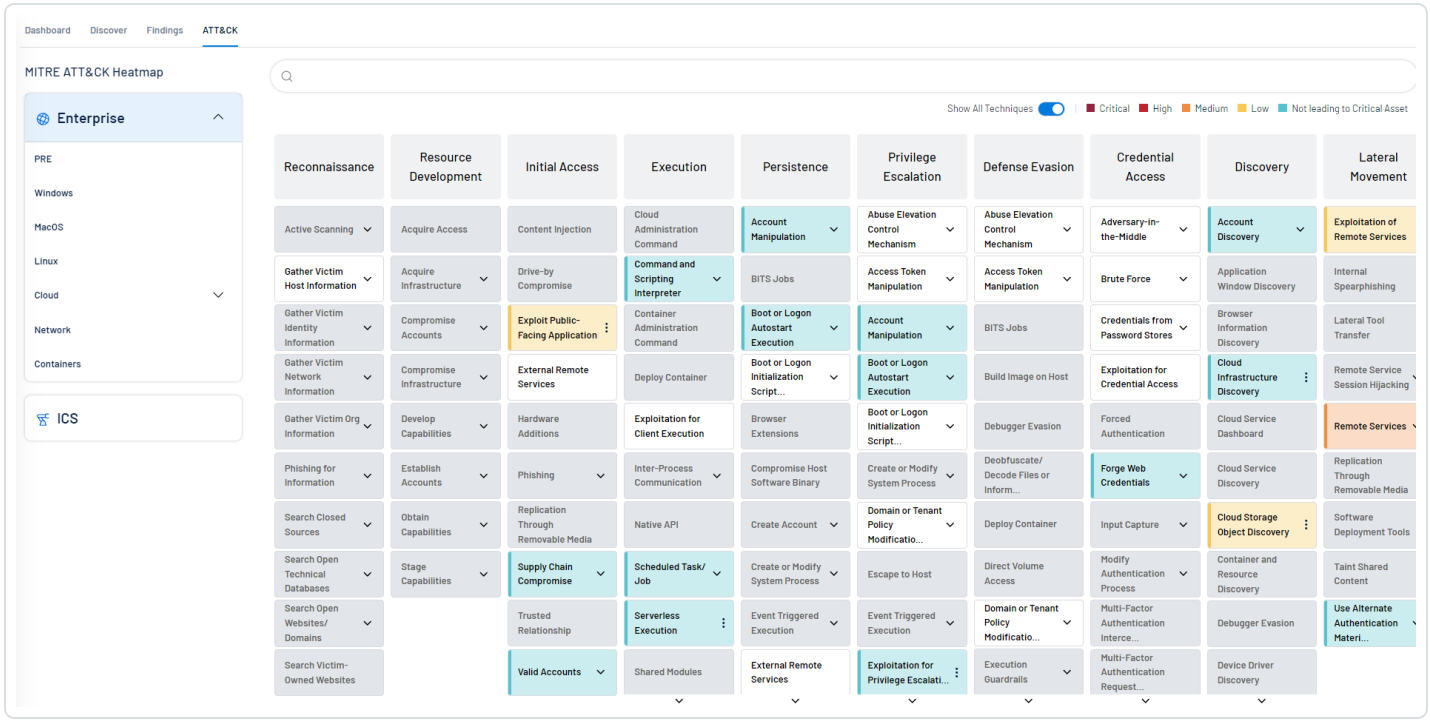
	of the matrix. Click any square to navigate to the Discover tab with the appropriate filter automatically applied. Here you can view paths that match the selected value. **Tip:** At the top of the matrix, click on a **Data Source** to filter the matrix by attack paths from the selected source. If there is no data available for a data source type, the button for that source is disabled.
Trending Attack Paths	A list of all trending attack paths.

Mitre Att&ck Heatmap

The **Mitre Att&ck Heatmap** in Attack Path Analysis provides a holistic view of your data based on tactics and techniques from Mitre Att&ck.

Attack Path Analysis presents the Mitre Att&ck data in a table format that enables you to quickly prioritize and remediate critical vulnerabilities that are most relevant to your organization.

Tip: Check out the full list of Attack Path Techniques to view tactics, techniques, and the Tenable applications that trigger them.



To access **Mitre Att&ck Heatmap**:

1. In Attack Path Analysis, click the **Att&ck** tab.

   The **Mitre Att&ck Heatmap** page appears.

2. Do one of the following:

   - To view data based on Enterprise tactics and techniques, in the left panel, click the **Enterprise** tab.

     a. (Optional) Filter the table by platform type by selecting one of the available filters:

     - **PRE**
     - **Windows**
     - **MacOS**
     - **Linux**
     - **Cloud**
     - **Containers**

   - To view data based on ICS (Industrial Critical Systems) tactics and techniques, in the left panel, click the **ICS** tab.

Attack Path Analysis displays the relevant Mitre Att&ck data in a table format that includes the following details:

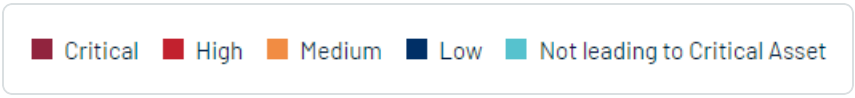
- Each column in the **Mitre Att&ck Heatmap** table represents an enterprise tactic and its techniques. The column header shows the name of the enterprise tactic and the column shows its associated techniques.

  For example, **Gather Victim Host Information**, **Gather Victim Identity Information**, and so on are enterprise techniques related to **Reconnaissance** enterprise tactic.

- Table cells are color-coded to indicate the following information:

  - Gray – Tenable does not currently support these techniques.
  - White – While Tenable supports these techniques and detects them, they are not relevant to your organization.

- The following image shows the colors that represent **Critical**, **High**, **Medium**, and **Low**.



Click on a cell to view findings or attack paths for a technique:

a. Click the ⌄ button.

A list of sub-techniques appears.

> **Note**: If there are no sub-techniques for a technique, only the ⋮ icon is available.

b. Click the ⋮ button:

A menu appears with these options.

- **Findings** – Navigate to the **Findings** page to view findings filtered by the selected technique or sub-technique.
- **Discover** – Navigate to the **Discover** page to view all possible attack paths for the selected technique or sub-technique.

> **Tip**: Each menu option includes the number of findings / attack paths available for the selected technique or sub-technique.

- Teal (**Not leading to Critical Asset**) – These techniques do not lead to critical assets.

When viewing the Mitre ATT&CK page, you can do the following:

- Use the Search bar at the top of the table to search for specific techniques or sub-techniques.
- Click the **Show All Techniques** toggle to view only the cells that are color-coded by severity. This hides the white and gray cells in the heatmap table and shows only the techniques relevant to your organization.
- Click on a severity level to filter the page by severity.

Findings

Every attack path contains one or more attack techniques. Every network includes multiple attack paths. Tenable helps you to focus on the most important paths by highlighting:

- Attack paths that lead to critical assets.
- Assets with an ACR greater than 7.
- Other Tenable defined static identifiers, such as **Domain Admins**.

A **Finding** is an attack technique that exists in one or more attack paths that lead to one or more critical assets. The **Findings** tab in Attack Path Analysis takes your data and pairs it with advanced graph analytics and the MITRE ATT&CK® Framework to create **Findings**, which allow you to understand and act on the unknowns that enable and amplify threat impact on your assets and information.

Before you begin:

For Attack Path Analysis, ensure you have the following:

- A Tenable Vulnerability Management Basic Network Scan with credentials.
- One of the following:
  - A Tenable Vulnerability Management basic scan using the **Active Directory Identity** scan template. This scan type requires fewer permissions, and provides a basic overview of your active directory entities.

    > **Note:** You can run this scan type on its own, or as part of a Basic Network Scan. In a Basic scan, you must ensure the **Collect Identity Data from Active Directory** option is enabled in the **Discovery** section.

  - Tenable Identity Exposure SaaS deployed.

  > **Note:** Because the plugin only supports up to 7,000 identities, the **Active Directory Identity** scan template is not designed for large environments, but is instead intended to help small customers kick start their use of Attack Path Analysis. Tenable recommends that larger customers deploy Tenable Identity Exposure.

- Additionally, for best performance, Tenable recommends the following:
  - Have at least 40% of assets scanned via an authenticated scan.
  - Select maximum verbosity in the Basic Network Scan.

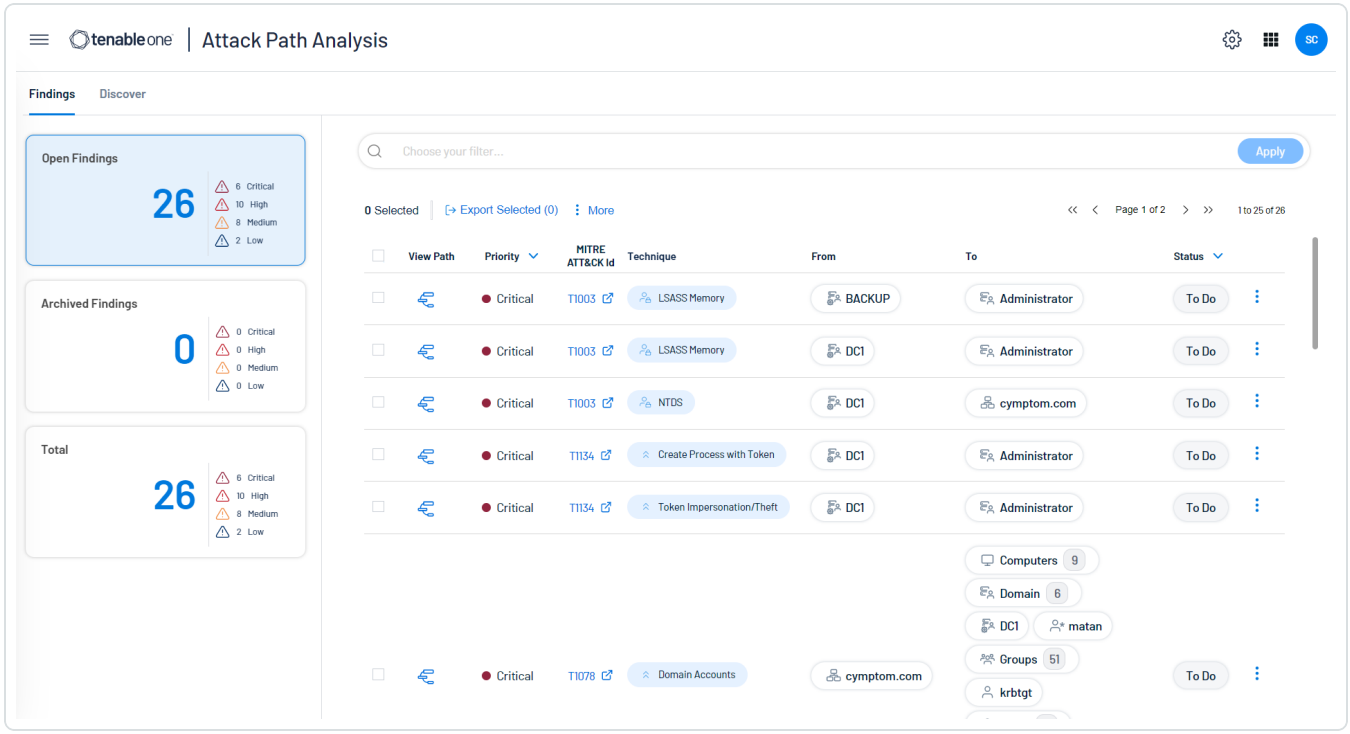
- A default Tenable Web App Scanning scan, including injection plugins. At least 40% of the web applications should be scanned.
- An AWS connection with a Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.
- When using Tenable Identity Exposure, enable privileged analysis. This option highlights key attack vectors used by hackers and gives you a better understanding of your attack surface, including credential auditing and password analysis.
- A scan frequency of at least once a week.
- Configure Tenable OT Security.
- Configure Tenable Attack Surface Management.

- At least one attack technique found within Attack Path Analysis.
- At least one attack path generated within Attack Path Analysis.
- Attack paths that use the previously mentioned attack technique and lead to at least one critical asset.

To access the **Findings** tab:

1. In the upper-left corner of the page, click the ☰ button.
2. In the **Analytics** section, click **Attack Path Analysis**.

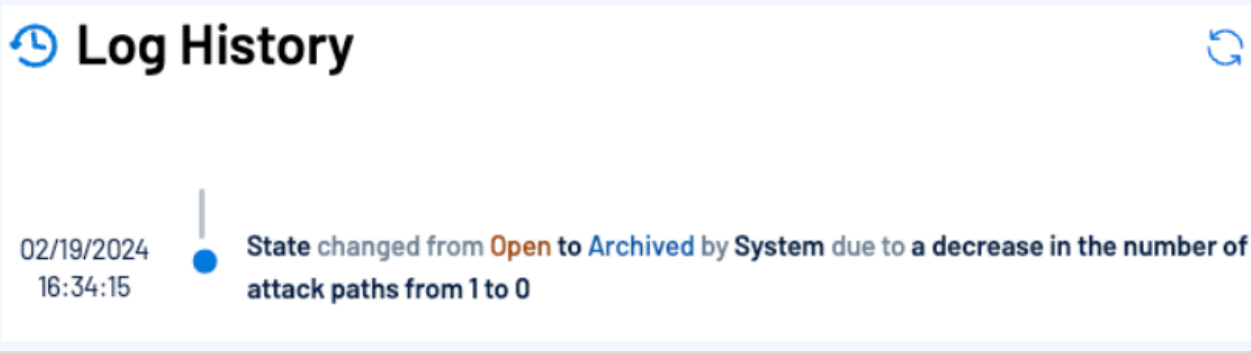
Attack Path Analysis appears. By default, the **Findings** tab is active.



On the **Findings** tab, you can:

- View **Findings** tiles:
  - **Open Findings** – View the total number of open findings within **Attack Path Analysis**. Also, view the number of open findings in each priority level.
  - **Archived Findings** –View the total number of archived findings within **Attack Path Analysis**. Also, view the number of archived findings in each priority level.
  - **Total** – View the total number of findings within **Attack Path Analysis**. Also, view the number of total findings in each priority level.

Deactivated Findings: In cases where attack path data does not exist outside of the **Findings** list, the Attack Path Analysis system automatically updates the Log History of the finding:



- When a finding is not seen as part of any attack path, the system changes the finding **State** to **Archived**.
- When a finding cannot be found within the Attack Path Graph in the **Discover** section, the system changes the finding **State** to **Archived** and the **Status** to **Done**.

If at any point the finding is again seen as part of an attack path, the system automatically reactivates the finding **State** to **Open**.

Click on a tile to filter the **Findings** list by that type of finding.

- View the **Findings** list, where you can:
  - Filter the **Findings** list:
    a. At the top of the **Findings** list, click inside the search box.

    The **Choose your filter** drop-down box appears where you can use the following filters:

Filter	Description
Priority	Filters by priority: critical, high, medium, or low. **Note:** When calculating the priority, Attack Path Analysis considers the following: • The number of attack paths where the finding is present compared to the total number of attack paths. • The number of critical assets to which these attack paths lead compared to the total number of critical assets.

	• The tactic used, for example, **lateral movement** or **privilege escalation**.
Status	Filters by status: **To Do**, **In Progress**, **In Review**, and **Done**.
Source	Filters by the attack path source.
Target	Filters by the attack path target.
CVE	Filters by specific CVEs.
Mitigations	Filters by mitigations for the attack techniques.
Tactic	Filters attack techniques with similar tactics.
Technique	Filters by attack techniques. For more information about attack techniques, see Attack Path Analysis Techniques.

b. Select the filter you want to use to filter the **Findings** list.

   The **Choose operator** drop-down box appears.

c. Select the operator you want to use to filter the **Findings** list.

   The **Choose value** drop-down box appears.

d. Select the value you want to use to filter the **Findings** list.

e. Click **Apply**.

   The **Attack Path Analysis** filters the **Findings** list based on your criteria.

- Show/hide columns in the **Findings** list:

a. In the upper-right corner of the **Findings** list, click the  button.

   A drop-down menu appears.

b. Select or deselect the check box next to the column you want to show or hide in the **Findings** list.

   The **Findings** list updates based on your selection.

- Export a finding.
- Archive a finding.
- Change the status of a finding.

  > **Tip**: See View Log History for more information about finding statuses.

- Click **View Path** to navigate to the **Discover** tab, where you can view a graphical representation of the attack path and interact with more attack path data.
- View the following finding information:
  - **New** – A **New** tag appears whenever Attack Path Analysis detects a new finding. The **Findings** page retains the **New** tag only for findings not older than 5 days or until a user clicks on the finding.
  - **Priority** – The priority, or criticality, of the finding, for example, **Critical**.

    > **Note:** By default, the **Findings** list sorts findings by highest priority first.

    > **Note:** When calculating the priority, Attack Path Analysis considers the following:
    >
    > - The number of attack paths where the finding is present compared to the total number of attack paths.
    > - The number of critical assets to which these attack paths lead compared to the total number of critical assets.
    > - The tactic used, for example, **lateral movement** or **privilege escalation**.

  - **MITRE ATT&CK Id** – The MITRE ATT&CK identification number for the finding. Click an identification number to navigate directly to the MITRE ATT&CK listing for the finding.
  - **Technique** – The MITRE ATT&CK technique associated with the finding.
  - **From** – The origin of the finding.
  - **To** – The target of the finding.

- **Status** – The status to indicate the action taken on the finding, for example, **In Progress**.

- Click on a finding to view additional finding details.

Export a Finding

You can export one or more findings on the **Findings** tab in **Attack Path Analysis**. The export file includes information from the currently visible columns in the **Findings** list. By default, Attack Path Analysis also includes the following items in the export file:

- mitreURL
- state
- vectorCount

To export a finding:

1. Access the **Findings** tab.
2. Do one of the following:
   - In the **Findings** list, next to the finding you want to export, click the ⋮ button.

     A menu appears.

     a. Click **Export as CSV**.
   - In the **Findings** list, select the check box next to each finding you want to export.

     a. At the top of the list, click **Export Selected**.

   Attack Path Analysis downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

Add and View Comments on a Finding

Attack Path Analysis allows you to add comments on any section of the finding details page and share it with other users in your organization. You can address your comment to a specific user and receive replies to your comment. Attack Path Analysis also notifies you whenever someone replies to your comment or when new comments are added.

To comment on a finding:

1. Access the **Findings** tab.
2. Click a finding that you want to comment on.

   The finding details page appears.
3. Do one of the following:

   a. In the upper-right corner of the view, click the button.

   b. Scroll to the section on which you want to comment and click the button.

      The **Comments** pane appears.
4. In the text box, type your comment.

   > **Note**: You can send your comment to another user by prefixing @ before the user's email ID.
5. (Optional) To include a snapshot of the section on which you want to comment, select the **Include snapshot** check box.
6. Click the button.

   Attack Path Analysis posts your comment and notifies other users about your comment.

   ### What to do next

   Whenever someone posts a comment, the icon in the upper-right corner shows a blue dot indicating that you have new comments.

   To view the comments, click the icon to open the **Comments** pane. When you click a comment, Attack Path Analysis directs you to the section including the newly added comment.

Change the Status of a Finding

You can change the status of one, several, or all findings on the **Findings** tab in **Attack Path Analysis**.

To change the status of a finding:

1. Access the **Findings** tab.
2. Do one of the following:
   - In the **Findings** list, next to the finding for which you want to change the status, click the ⋮ button.

     A menu appears.

     a. Click **Change Status**.
   - In the **Findings** list, select the check box next to each finding for which you want to change the status.

     a. At the top of the list, click ⋮ **More**.

     A menu appears.

     b. Click **Change Status**.

   A menu appears.
3. Click the status to which you want to change the finding, for example, **In Progress**.

   Attack Path Analysis updates the status of the finding.

Archive a Finding

You can archive one, several, or all findings on the **Findings** tab in Attack Path Analysis. By archiving a finding, you are effectively accepting the risk of the finding as part of attack paths within Attack Path Analysis.

> **Note:** Attack Path Analysis automatically archives findings that are no longer part of any attack paths. For more information, see Log History.

To archive a finding:

1. Access the **Findings** tab.
2. Do one of the following:

- In the **Findings** list, next to the finding you want to archive, click the ⋮ button.

  A menu appears.

  a. Click **Move to Archived**.

- In the **Findings** list, select the check box next to each finding you want to archive.

  a. At the top of the list, click ⋮ **More**.

  A menu appears.

  b. Click **Move to Archived**.

A confirmation message appears.

3. Click **Move to Archived**.

   Attack Path Analysis moves the finding to the **Archived Findings** section.

Tip: View the Log History to see the movement history of any given finding.

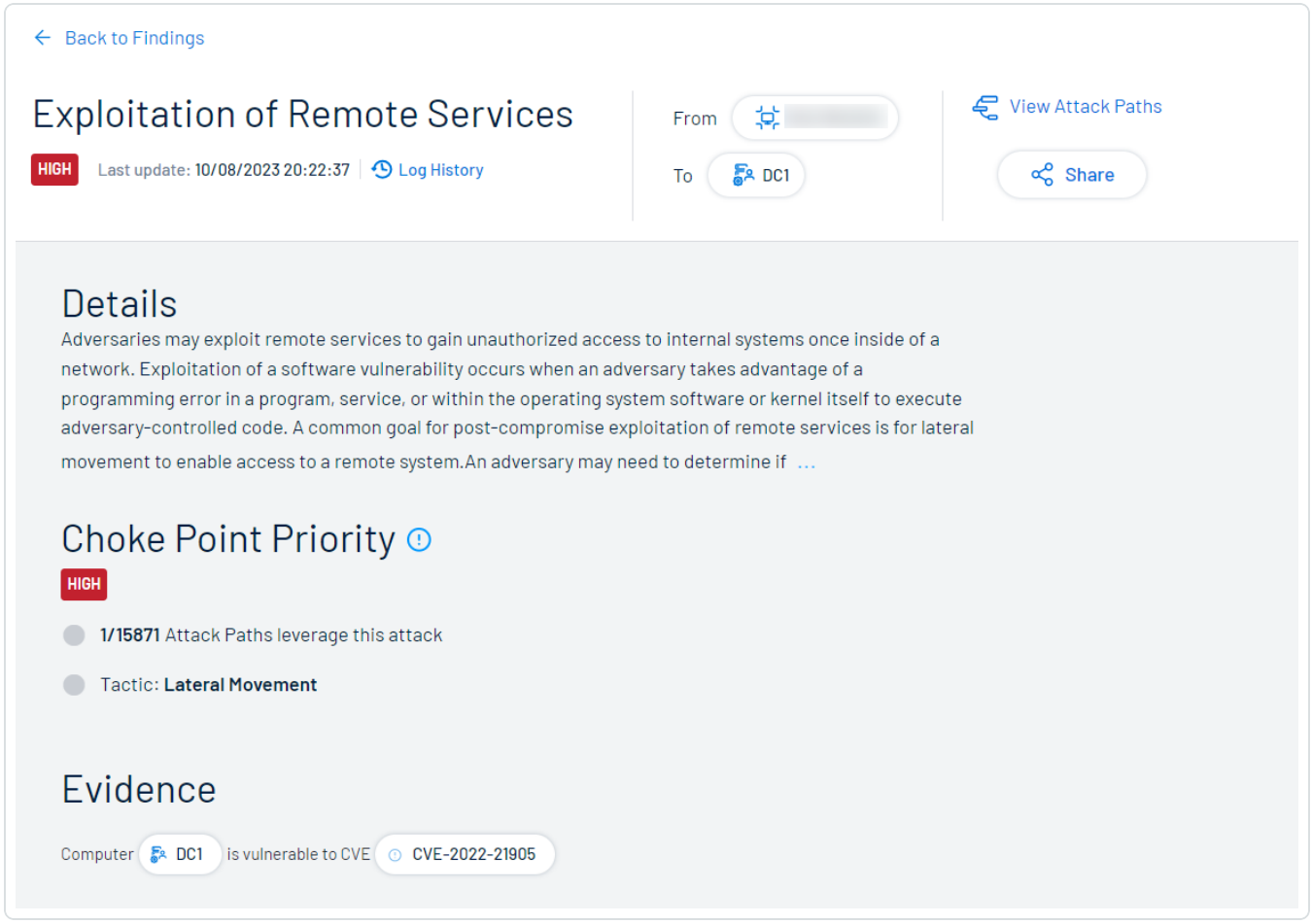
View Finding Details

You can view additional details for any findings on the **Findings** tab within Attack Path Analysis.

To view additional details for a finding:

1. Access the **Findings** tab.
2. In the Findings list, click the finding for which you want to view additional details.

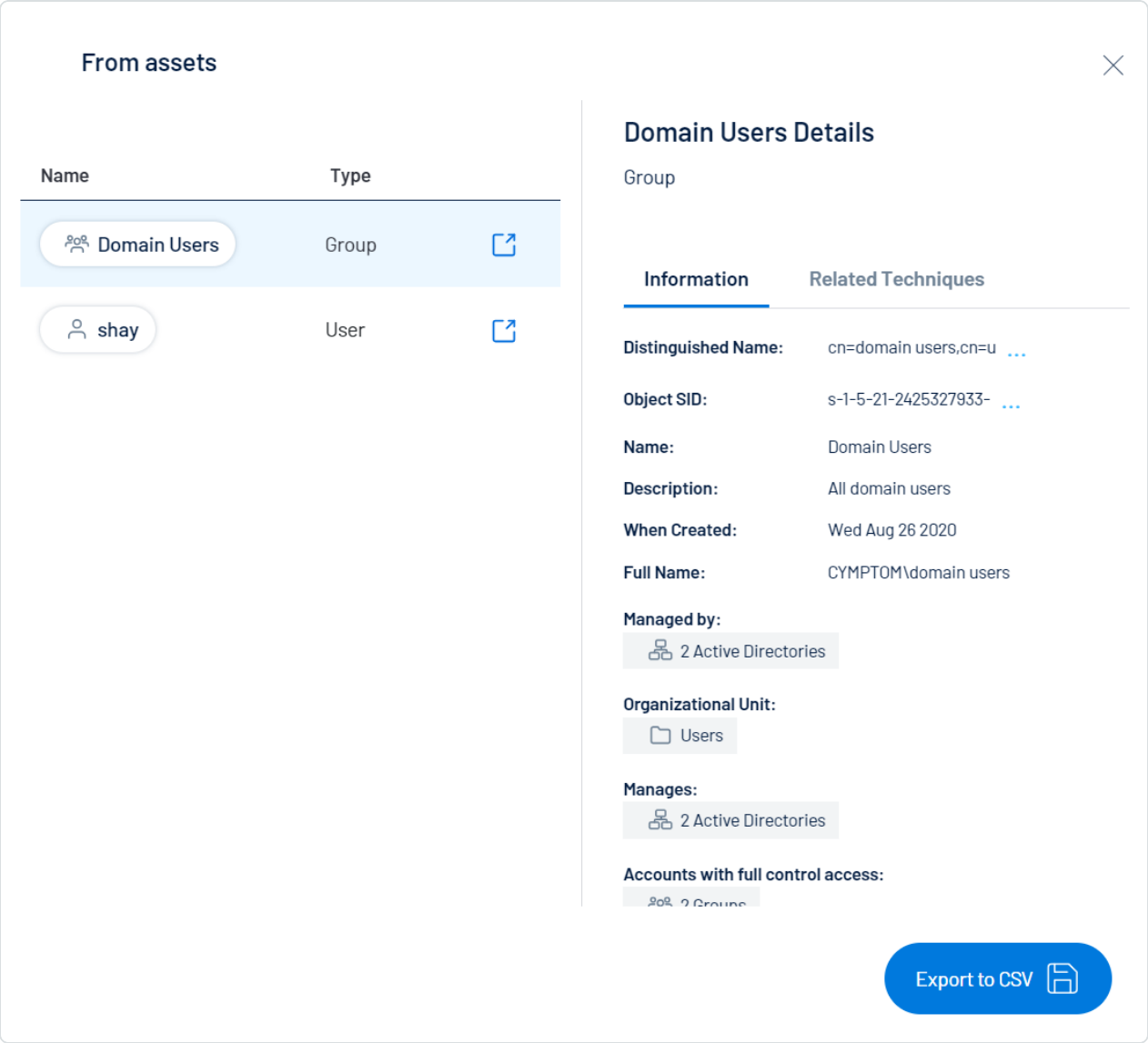
The finding details page appears.



On the finding details page, you can:

- View the name and priority of the finding.
- View the date and time at which the finding was last updated. For example, a change in the status, priority, or state of a finding can change the **Last update** time.
- Click **Log History** to view the changes in the state, status, and priority of a finding. For more information, see View Log History.
- View information about nodes within attack paths that exploit the finding.
    - Click a node name to view additional details:

      The node details panel appears.



In the node details panel, you can:

- On the left side of the panel, select the node for which you want to view additional details.

  The information on the right side of the panel updates accordingly.

  > **Tip:** Click the button to view that node directly in the Attack Path Graph.

- Click the **Information** tab to view further details about the node, including, but not limited to:
  - **NES** – The Node Exposure Score (NES) is a metric produced by Attack Path Analysis to understand the blast radius exposure of a node. This metric considers the Vulnerability Priority Rating of all vulnerabilities on the asset as well as other relationships such as software installed, sub-networks to which the asset belongs, internet exposure, etc.
  - **Logged in Users** – Users currently logged into the node.
  - **Member of** – Lists the number of groups to which the node belongs.
  - **Related Types** – The node type as categorized by Attack Path Analysis.

  The information in this panel varies based on the node type, for example, **Computer** or **User**.
- Click the **Related Techniques** tab to view Attack Path Techniques associated with the node.
- Click **Export to CSV** to export the node details in CSV format.

- Click **View Attack Paths** to navigate to the **Discover** tab, where you can view a graphical representation of the attack path as well as interact with more attack path data.
- Click **Share** to copy, send via email, or print the details of the finding. For more information, see Share Finding Details.
- View a brief description of the **Details** of the finding.
- View the **Choke Point Priority** related to the finding.

  Tip: A choke point is a place where potential attack paths merge together before reaching a critical asset. Attack Path Analysis uses a **Choke Point Priority** metric to determine the criticality of choke points. Tenable recommends focusing on areas with higher choke points first, as remediating those will negate the largest number of critical items within your organization.
- View **Evidence** related to the finding.

- View **Related Products, Assets, and Findings** for the finding. This section displays information about the data sources used or seen within this specific finding.

  Tip: Click on a related finding to open it directly within its source application. Within the source application, the list of findings is filtered by related assets and plugin IDs. However, if there are more than 15 related assets, the list is filtered only by plugin IDs and shows findings for all assets within the source application. Not all applications include plugin information.

  Note: While source information is available for on-premises products such as Tenable Identity Exposure On-Prem and partial products such as Tenable Security Center without Tenable Vulnerability Management, links to the source application are currently unavailable for these.

- View **Mitigation** options for the finding:

  a. Click on an option to view further information steps you can take to mitigate the finding.

  b. To view a step-by-step guide on how to mitigate the finding, click **Step by Step Mitigation Guide**.

  On the right side of the page, the **Step by Step Mitigation Guide** panel appears, which includes a set of instructions you can follow to mitigate the finding and therefore its risk.

- View **Detection** information for the finding.
- View **Related Malware and Tools** associated with the finding.
- View external **References**, where you can learn more about the finding.

  a. Click a reference to navigate to that resource.

Share Finding Details

In Attack Path Analysis, you can share finding details with other users in your organization. You can also print these details or copy and share the URL of a specific finding details page.

To share the finding details:

1. Access the **Findings** tab.
2. In the **Findings** list, click the row of the finding you want to share.

   The finding details page appears.

3. Click **Share**.

   Attack Path Analysis displays the following menu:

Option	Description
	• Click the button. The finding details page opens in your browser and the URL gets copied to your clipboard.
	• Click the button. Attack Path Analysis opens your configured email with the URL to the finding details page.
	• Click the button. Attack Path Analysis opens the **Print** window, where you can print the finding details page.

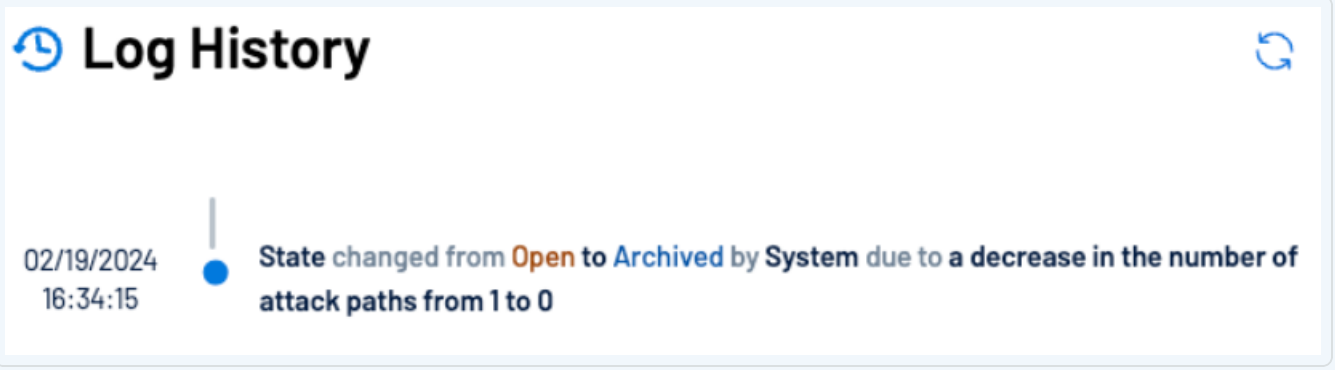
View Log History

You can use the **Log History** page to view the following details for a finding:

- State changes, whether **Open** or **Archived**.
- Any change in the status: **To Do**, **In Progress**, **In Review**, Or **Done**.
- Changes in the priority level: **Critical**, **High**, **Medium**, or **Low**.

The priority of a finding can change for a number of reasons, including a change in the number of targets, sources, attack paths, or critical assets. Priority can also change if the target or source is renamed.

> **Deactivated Findings**: In cases where attack path data does not exist outside of the **Findings** list, the Attack Path Analysis system automatically updates the state and status of the finding:



- When a finding is not seen as part of any attack path, the system changes the finding **State** to **Archived**.
- When a finding cannot be found within the Attack Path Graph in the **Discover** section, the system changes the finding **State** to **Archived** and the **Status** to **Done**.

If at any point the finding is again seen as part of an attack path, the system automatically reactivates the finding **State** to **Open**.

To view the log history of a finding:

1. Access the **Findings** tab.
2. In the **Findings** list, in the row of the finding for which you want to view the log history, click the ⋮ button.

   A menu appears.
3. Click **Log History**.

   The **Log History** page appears, where you can view a reverse chronological list of findings updates. To refresh the details on the page, click the ↻ icon.

Discover

The **Discover** tab of Attack Path Analysis allows you to dive deeper into the mind of an attacker by interacting directly with attack paths and nodes. Here, you can:

- Use the **Attack Path Query Builder** to generate custom paths and manipulate the origins and targets within a path to view exactly how these changes affect your data.

- Use the **Asset Query Builder** to gain insight into your asset nodes and how they connect to one another.
- Create and manage query bookmarks, and use **Built-in Queries** to dive deeper into possible attack paths.

Before you begin:

For Attack Path Analysis, ensure you have the following:

- A Tenable Vulnerability Management Basic Network Scan with credentials.
- One of the following:
    - A Tenable Vulnerability Management basic scan using the **Active Directory Identity** scan template. This scan type requires fewer permissions, and provides a basic overview of your active directory entities.

      > **Note:** You can run this scan type on its own, or as part of a Basic Network Scan. In a Basic scan, you must ensure the **Collect Identity Data from Active Directory** option is enabled in the **Discovery** section.

    - Tenable Identity Exposure SaaS deployed.

  > **Note:** Because the plugin only supports up to 7,000 identities, the **Active Directory Identity** scan template is not designed for large environments, but is instead intended to help small customers kick start their use of Attack Path Analysis. Tenable recommends that larger customers deploy Tenable Identity Exposure.

- Additionally, for best performance, Tenable recommends the following:
    - Have at least 40% of assets scanned via an authenticated scan.
    - Select maximum verbosity in the Basic Network Scan.
    - A default Tenable Web App Scanning scan, including injection plugins. At least 40% of the web applications should be scanned.
    - An AWS connection with a Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.

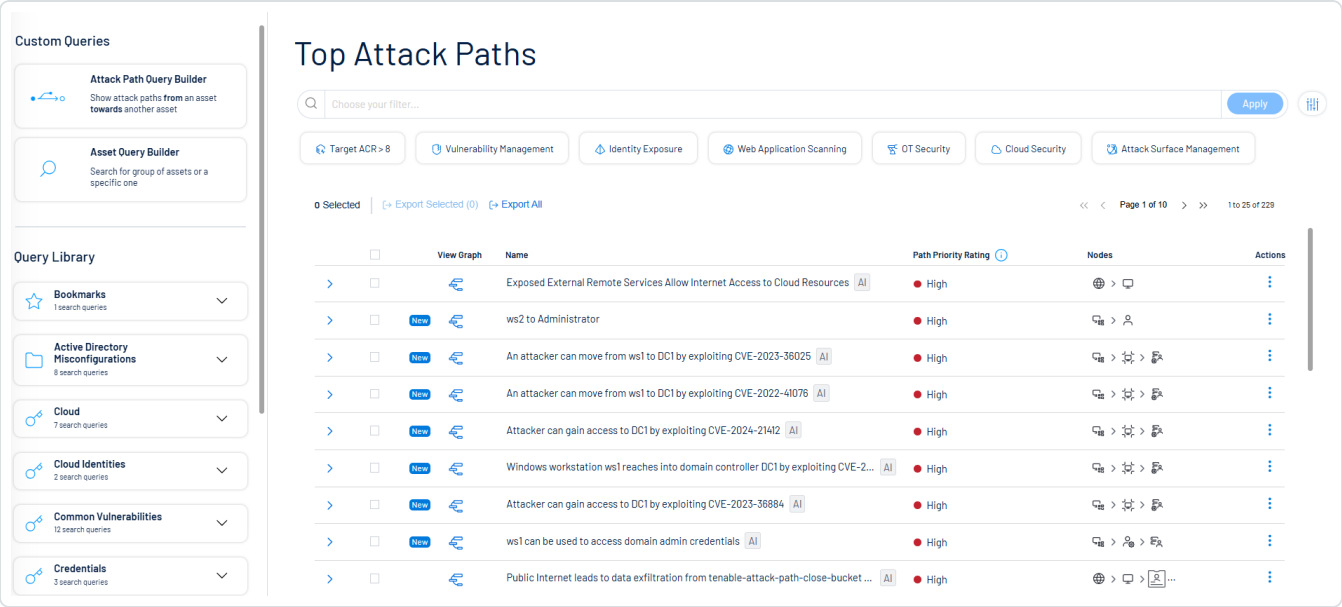
- When using Tenable Identity Exposure, enable privileged analysis. This option highlights key attack vectors used by hackers and gives you a better understanding of your attack surface, including credential auditing and password analysis.
- A scan frequency of at least once a week.
- Configure Tenable OT Security.
- Configure Tenable Attack Surface Management.

To access the Discover tab:

1. In the upper-left corner of the page, click the ☰ button.
2. In the **Analytics** section, click **Attack Path Analysis**.

   Attack Path Analysis appears. By default, the **Dashboard** tab is active.
3. Click the **Discover** tab.

   The **Discover** page appears.



By default, the **Top Attack Paths** list appears, which lists the top attack paths leading to critical assets.

In this list, you can:

- Filter the list:

  Tip: Below the search box, click a quick filter button to automatically filter the list by the selected item.

  a. At the top of the list, click inside the search box.

     The **Choose your filter** drop-down box appears where you can use the following filters:

Filter	Description
Name	Filters by the attack path name.
Summary	Filters by the attack path summary text.
Priority	Filters by priority: critical, high, medium, or low.

  b. Select the filter you want to use to filter the list.

     The **Choose operator** drop-down box appears.

  c. Select the operator you want to use to filter the list.

     The **Choose value** drop-down box appears.

  d. Select the value you want to use to filter the list.

  e. Click **Apply**.

     The **Attack Path Analysis** filters the list based on your criteria.

- Show/hide columns in the list:

  a. In the upper-right corner of the list, click the  button.

     A drop-down menu appears.

  b. Select or deselect the check box next to the column you want to show or hide in the list.

     The list updates based on your selection.

- Export one or more attack paths:

  Do one of the following:

- In the list, next to the attack path you want to export, click the ⋮ button.

  A menu appears.

  a. Click **Export as CSV**.

- In the list, select the check box next to each attack path you want to export.

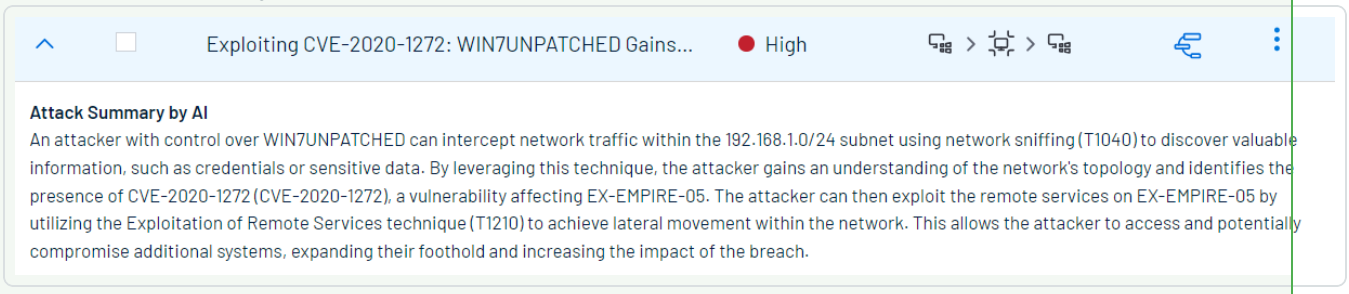
  a. At the top of the list, click **Export Selected**.

- To export all attack paths, at the top of the list, click **Export All**.

Attack Path Analysis downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

- View the following attack path information:

Tip: Click the › button in any row to expand the full attack path summary details, including an AI powered summary of the attack path.



  - **Name** – The name of the attack path.
  - **Path Priority Rating** – The priority of an attack path. Attack Path Analysis calculates the PPR based on the relative number of attack paths to critical assets. Attack Path Analysis categorizes priority levels as **Low**, **Medium**, **High**, and **Critical**.
  - **Nodes** – A visual representation of the nodes involved in the attack path that indicates the node type and the order in which the nodes might be accessed.
  - **View Graph** – Click the button in the row of any attack path for which you want to view a graphical representation the attack path. For more information, see Interact with Attack Path Query Data.
  - **Actions** – Click the ⋮ in the row of any attack path to perform the following actions:

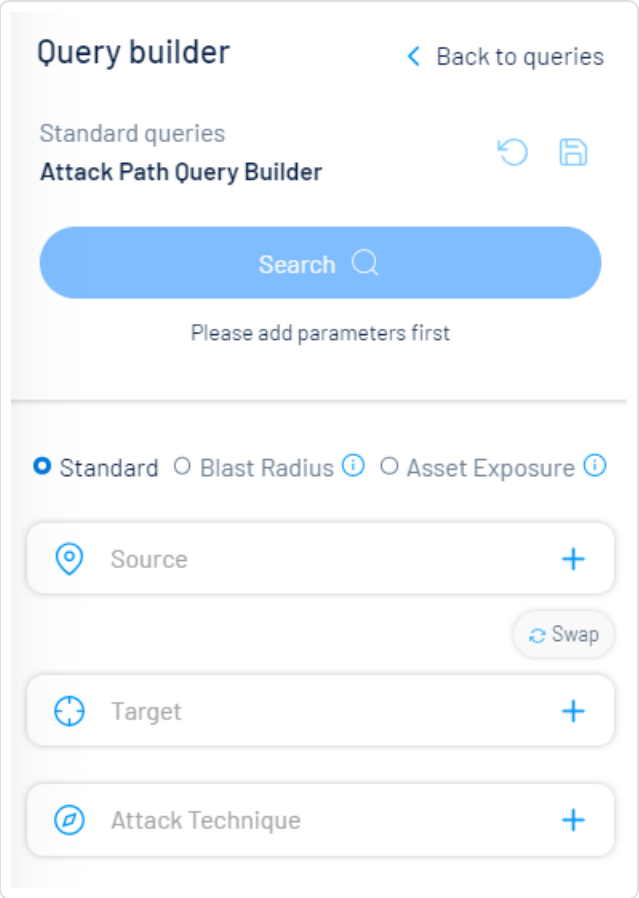
- **View Findings** – Click to navigate directly to the Findings page, filtered by findings related to the selected attack path.
- **Export as CSV** – Click to export the attack path in CSV format. **Attack Path Analysis** downloads the export file to your computer. Depending on your browser settings, your browser may notify you that the download is complete.

On the **Discover** page, you can also:

- Use the **Attack Path Query Builder** to generate a custom attack path query.
- Use the **Asset Query Builder** to generate a custom query for one or more assets or asset groups.
- Use a **Built-in Query** in the **Query Library** to generate a pre-configured query.

Generate an Attack Path Query with the Attack Path Query Builder

You can use the **Attack Path Query Builder** to generate an attack path from one asset to another. You can create a query from a specific node or asset origin, and then specify the target to which you want to compare.



Tip: To generate an attack path using a built-in query, see Generate an Attack Path with a Built-in Query.

To generate a custom attack path query:

1. In Attack Path Analysis, access the **Discover** tab.
2. In the **Custom Queries** section, click **Attack Path Query Builder**.

   The **Query Builder** pane appears.
3. In the **Source** box, click the + button.

   The source options appear.
4. For each source you want to include in the query:

a. Select the radio button next to the type of origin you want to use for the query:

- **Asset type** – Generate a query based on a certain type of asset.
- **Specific asset** – Generate a query based on a specific asset.

b. In the text box, type the asset type or specific node/asset you want to use for the query.

c. (Optional) To apply filters to the origin:

i. Click the  button.

The **Filters** window appears.

ii. In the **Parameter** drop-down, select the parameter by which you want to filter the origin.

iii. In the **Operator** drop-down, select the operator to apply to the parameter.

iv. In the text box, type or select the value or values you want to use for the filter.

> **Note:** The values you can use differ depending on the parameter you selected.

v. Click **Apply and search**.

Attack Path Analysis applies the filter to the origin.

5. In the **Target** section, click the  button.

The target options appear.

6. For each target you want to include in the query:

a. Select the radio button next to the type of target you want to use for the query:

- **Asset type** – Generate a query based on a certain type of asset.
- **Specific asset** – Generate a query based on a specific asset.

b. In the text box, type the asset type or specific node/asset you want to use for the query.

c. (Optional) To apply filters to the target:

i. Click the button.

The **Filters** window appears.

ii. In the **Parameter** drop-down, select the parameter by which you want to filter the target.

iii. In the **Operator** drop-down, select the operator to apply to the parameter.

iv. In the text box, type or select the value or values you want to use for the filter.

> **Note:** The values you can use differ depending on the parameter you selected.

v. Click **Apply and search**.

Attack Path Analysis applies the filter to the target.

7. (Optional) Click Swap to swap between Source and Target assets.

8. In the **Attack Technique** section, click the button.

A text box in which you can search for and select techniques appears.

9. In the **Technique** box, type or select a specific attack technique.

Attack Path Analysis updates the list based on the search criteria. For more information on available techniques, see Attack Path Analysis Techniques.

10. (Optional) Click **Add a Technique** to add additional techniques.

> **Note**: Attack Path Analysis enables **Add a Technique** only after you add an initial technique.

> **Caution:** You must add techniques to your query in the order in which they appear in an attack path. Attack Path Analysis does not provide query results for incorrectly ordered techniques.

11. Click **Search**.

Attack Path Analysis returns any attack paths that match the query you created. For more information on interacting with the data, see Interact With Attack Path Data.

12. (Optional) To reset the query pane, at the top of the pane, click the  button.

    Attack Path Analysis resets the selections within the pane.

(Optional) Save your Query as a Preset/Bookmark

Once you've built your custom query, you can save it as a preset, where you can then access it as a bookmark when creating new built-in attack path queries.

To save your query as a preset:

1. At the top of the pane, click the  button.

   The **Save as preset** window appears.

2. In the **Name of preset** text box, type a name for the query.
3. In the **Description of preset** text box, type a description of the query.
4. Click **Save preset**  .

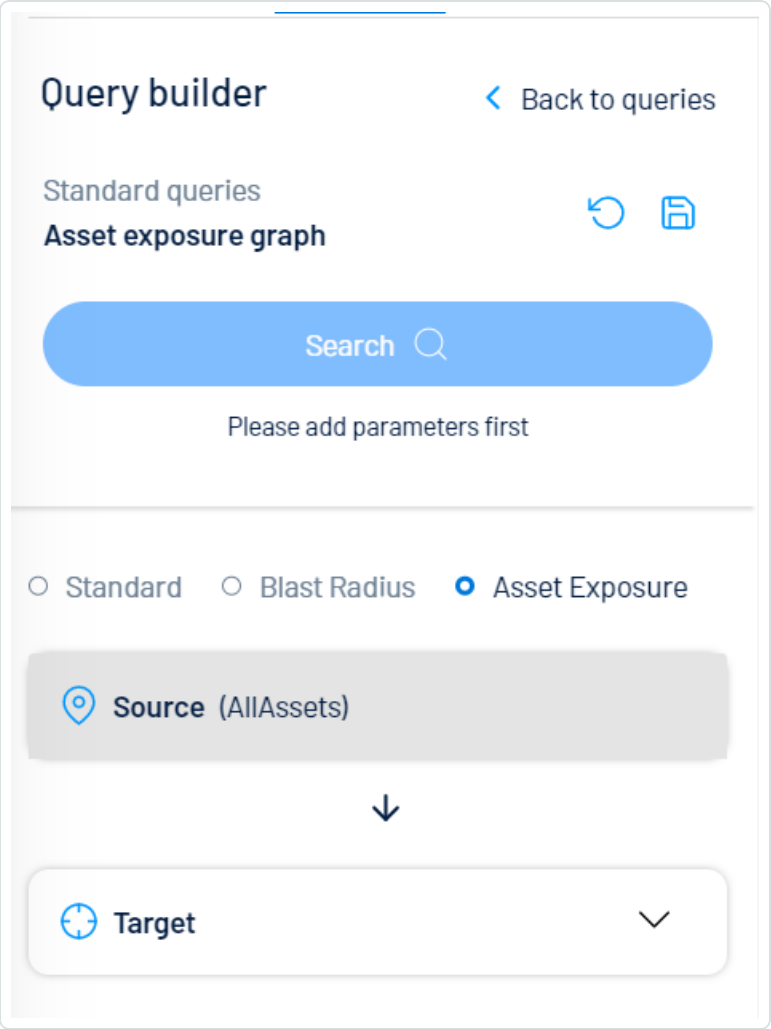
   Attack Path Analysis saves the query as a preset. You can access your saved queries in the **Bookmarks** section of the **Query Library**.

What to do next:

Interact with the attack path data provided by the query.

Generate an Asset Exposure Graph Query

You can generate a query to view an **Asset Exposure Graph**, which helps you to visualize an attack path from multiple assets down to one asset.



To generate an Asset Exposure Graph query:

1. In **Attack Path Analysis**, access the **Discover** tab.
2. Click **Asset Exposure**.

   The **Source** and **Target** sections appear. The **Source** box shows the **All Assets** option by default.

3. In the **Target** section, click the + button.

   The target options appear.

4. For each target you want to include in the query:

a. Select the radio button next to the type of target you want to use for the query:

- **Asset type** – Generate a query based on a certain type of asset.
- **Specific asset** – Generate a query based on a specific asset.

b. In the text box, type the asset type or specific node/asset you want to use for the query.

c. (Optional) To apply filters to the target:

i. Click the button.

The **Filters** window appears.

ii. In the **Parameter** drop-down, select the parameter by which you want to filter the target.

iii. In the **Operator** drop-down, select the operator to apply to the parameter.

iv. In the text box, type or select the value or values you want to use for the filter.

> **Note:** The values you can use differ depending on the parameter you selected.

v. Click **Apply and search**.

Attack Path Analysis applies the filter to the target.

5. Click **Search**.

Attack Path Analysis returns any attack paths that match the query you created. For more information on interacting with the data, see Interact With Attack Path Data.

6. (Optional) To save the query as a preset, at the top of the pane, click the button.

The **Save as preset** window appears:

a. In the **Name of preset** text box, type a name for the query.

b. In the **Description of preset** text box, type a description of the query.

c. Click **Save preset**.

Attack Path Analysis saves the query as a preset.

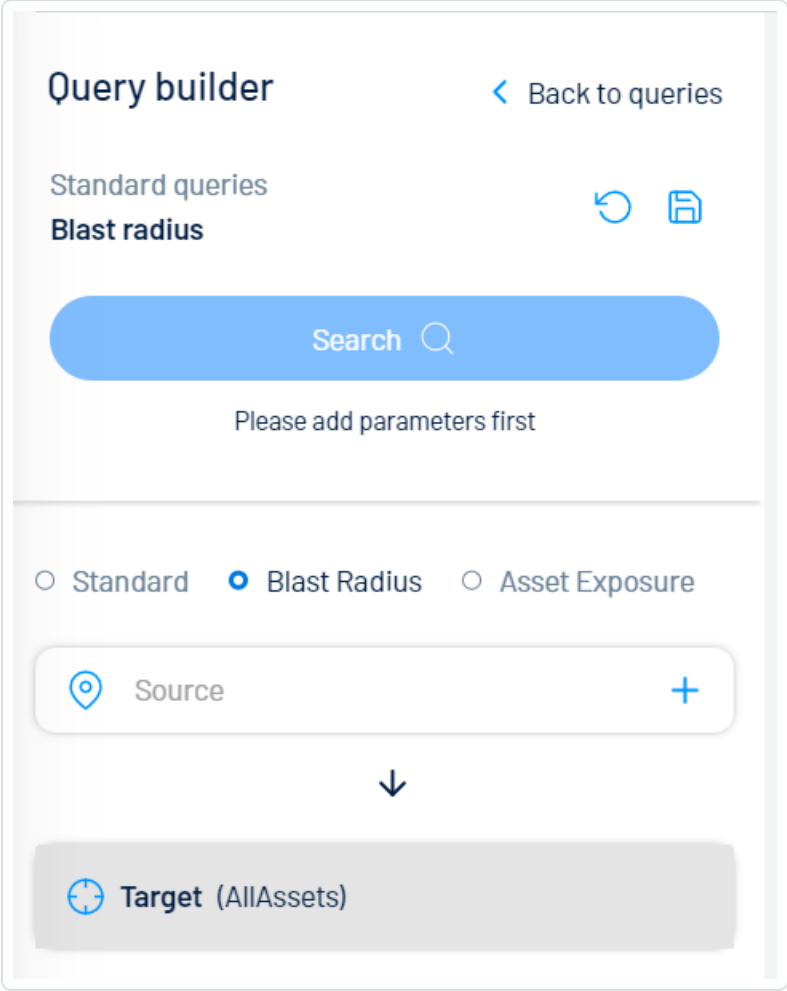
Tip: When you save a query as a preset, you can use it as a filter on the Findings tab.

What to do next:

Interact with the attack path data provided by the query.

Generate a Blast Radius Query

In the **Attack Path** section, you can generate a query to view **Blast Radius**, which helps you to visualize an attack path from one asset to multiple other assets.



To generate a Blast Radius query:

1. In **Attack Path Analysis**, access the Discover tab.
2. Click **Blast Radius**.

The **Source** and **Target** sections appear. The **Target** box shows the **AllAssets** option by default.

3. In the **Source** text box, click the + button.

   The source options appear.

4. For each source you want to include in the query:

   a. Select the radio button next to the type of source you want to use for the query:

      - **Asset type** – Generate a query based on a certain type of asset.
      - **Specific asset** – Generate a query based on a specific asset.

   b. In the text box, type the asset type or specific node/asset you want to use for the query.

   c. (Optional) To apply filters to the origin:

      i. Click the filter button.

      The **Filters** window appears.

      ii. In the **Parameter** drop-down, select the parameter by which you want to filter the origin.

      iii. In the **Operator** drop-down, select the operator to apply to the parameter.

      iv. In the text box, type or select the value or values you want to use for the filter.

      > **Note:** The values you can use differ depending on the parameter you selected.

      v. Click **Apply and search**.

      Attack Path Analysis applies the filter to the origin.

5. Click **Search**.

   Attack Path Analysis returns any attack paths that match the query you created. For more information on interacting with the data, see Interact With Attack Path Data.

6. (Optional) To save the query as a preset, at the top of the pane, click the save button.

   The **Save as preset** window appears:

a. In the **Name of preset** text box, type a name for the query.

b. In the **Description of preset** text box, type a description of the query.

c. Click **Save preset** .

Attack Path Analysis saves the query as a preset.

What to do next:

Interact with the attack path data provided by the query.

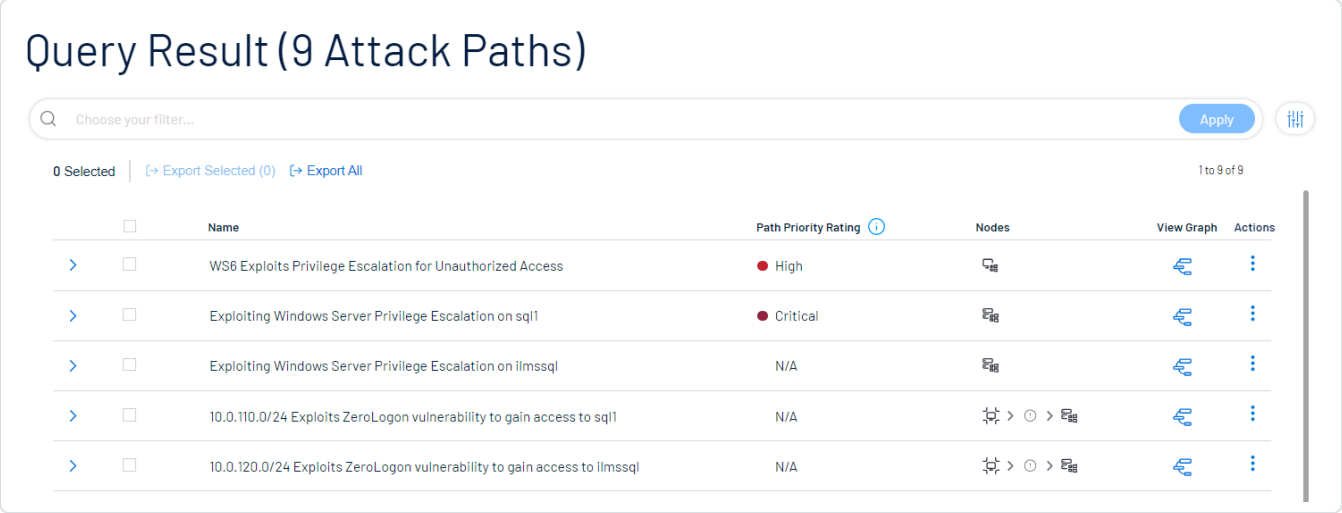
Interact with Attack Path Query Data

After running an Attack Path Query, Attack Path Analysis displays the results associated with your query. From here, you can drill-down and interact with the data to gain further insights.

To view and interact with attack path query data:

1. Create one of the following query types:
   - Use the **Query Builder** to generate a custom query.
     - Generate an **Asset Exposure Graph** query to visualize attack paths from multiple assets down to one asset.
     - Generate a **Blast Radius** query to visualize attack paths from one asset to multiple other assets.
   - Use a **Built-in Query** in the **Query Library** to generate a pre-configured query.

The **Query Result** page appears.



1. On the **Query Result** page, you can:

> **Note:** Because the options and data in this section depend on the type of query you run, some items listed below may not be available for your query.

- Filter the list of attack paths:
    a. At the top of the list, click inside the search box.

       The **Choose your filter** drop-down box appears.

    b. Select the filter you want to use to filter the list.

       The **Choose operator** drop-down box appears.

    c. Select the operator you want to use to filter the list.

       The **Choose value** drop-down box appears.

    d. Select or type the value you want to use to filter the list.

    e. Click **Apply**.

       The **Attack Path Analysis** filters the list based on your criteria.

- View a list of attack paths that match your query. This table includes the following attack path information:

Column	Description
Name	The attack path name.
Path Priority Rating	A prioritization metric for attack paths based on the exposure of the source, criticality of the target and the number of steps of the attack path. Higher PPR indicates higher risk.
Nodes	The asset nodes associated with the attack path. If there are multiple nodes within the attack path, Attack Path Analysis inserts directional arrows to show the direction of the path to and from each node. **Tip:** Hover your mouse cursor over the icon in this column to view the full name of the node type.
View Graph	Click the button to view the attack path in a graphical format. For more information, see View the Attack Path Graph.
Actions	Click the button to view available actions. A menu appears: ◦ Click **View Findings** to navigate directly to the **Findings** page filtered by the selected attack path. ◦ Click **Export as CSV** to export the attack path information as a .csv file.

- Click the button to expand an AI generated summary of the attack path.

- Export one or more attack paths from the list:

  Do one of the following:

  ◦ To export individual attack paths:

  a. In the list, select the check box next to each asset you want to export.

  b. At the top of the list, click **Export Selected**.

- To export all attack paths in the list:

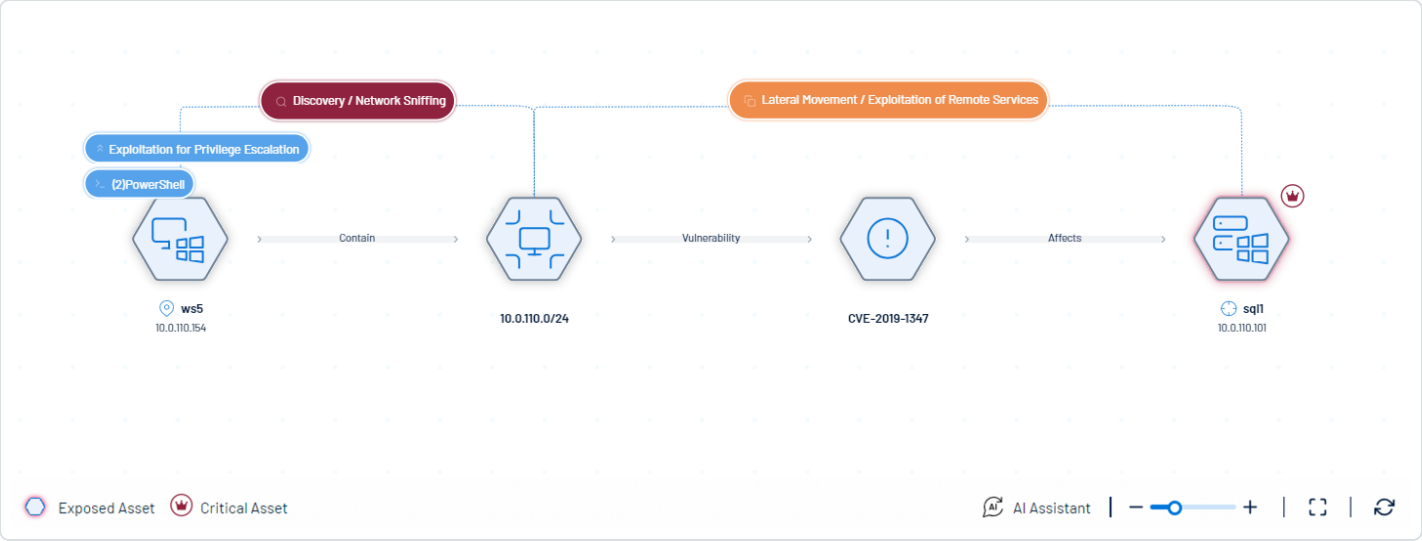
  a. At the top of the list, click **Export All**.

Attack Path Analysis downloads the list of selected attack paths as a .csv file.

View the Attack Path Graph

When you click **View Graph** in the **Query Result** list, Attack Path Analysis shows a graphical representation of the selected attack path.

Note: Because the options and data in this section depend on the type of query you run, some items listed below may not be available for your query.



In this section you can:

- At the top of the graph, click the › button to expand an AI generated summary of the attack path. Here, you can also view a list of **Related Products, Assets, and Findings** for the attack path. This section displays information about the data sources used or seen within this specific attack path.

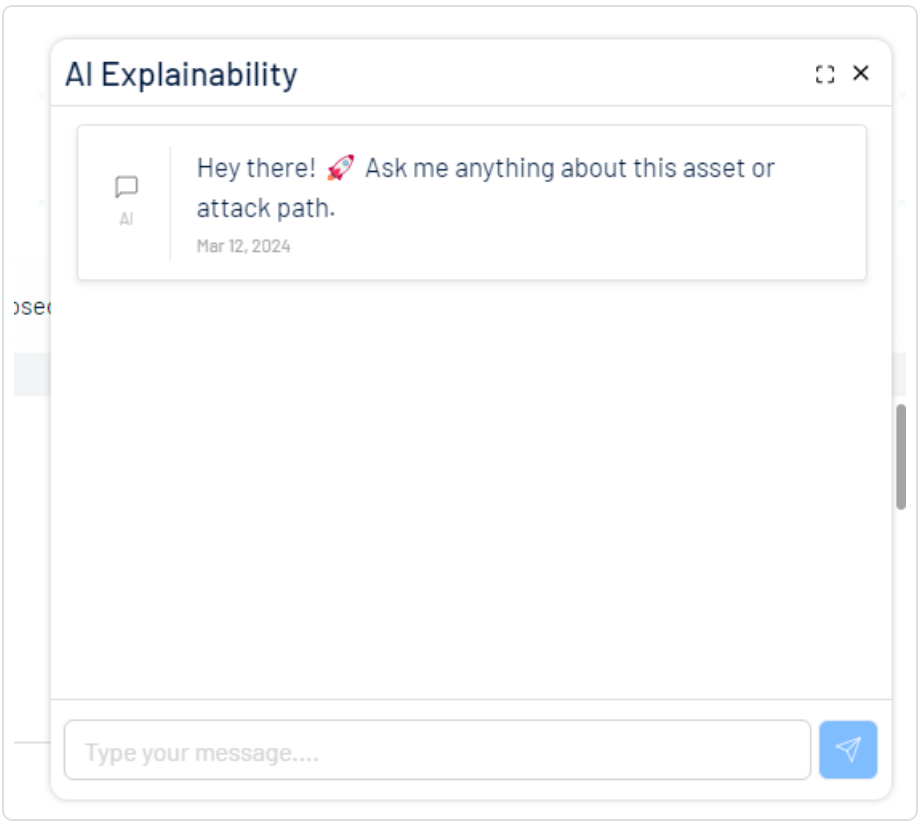
  Tip: Click on a related finding to open it directly within its source application. Within the source application, the list of findings is filtered by related assets and plugin IDs. However, if there are more than 15 related assets, the list is filtered only by plugin IDs and shows findings for all assets within the source application. Not all applications include plugin information.

> **Note:** While source information is available for on-premises products such as Tenable Identity Exposure On-Prem and partial products such as Tenable Security Center without Tenable Vulnerability Management, links to the source application are currently unavailable for these.

- View icons that represent the steps within the attack path, or the assets that match your query parameters.
    - Where applicable, view color coded steps and assets:
        - Technique segments color coded by priority (for example, a technique in red should be prioritized above a technique in orange).

          > **Note:** Informational attack paths, or attack paths without a priority, appear in blue.

        - Exposed assets highlighted in red.
        - Critical assets highlighted by the  icon.
    - Click on a step or an asset to view the information panel for that item.
- Where applicable, view direction arrows and other indicators that show the source, direction, and target of the attack path.
- Click **AI Assistant** to open an AI chat window, where you can ask questions related to the asset node or the attack path to which it belongs.



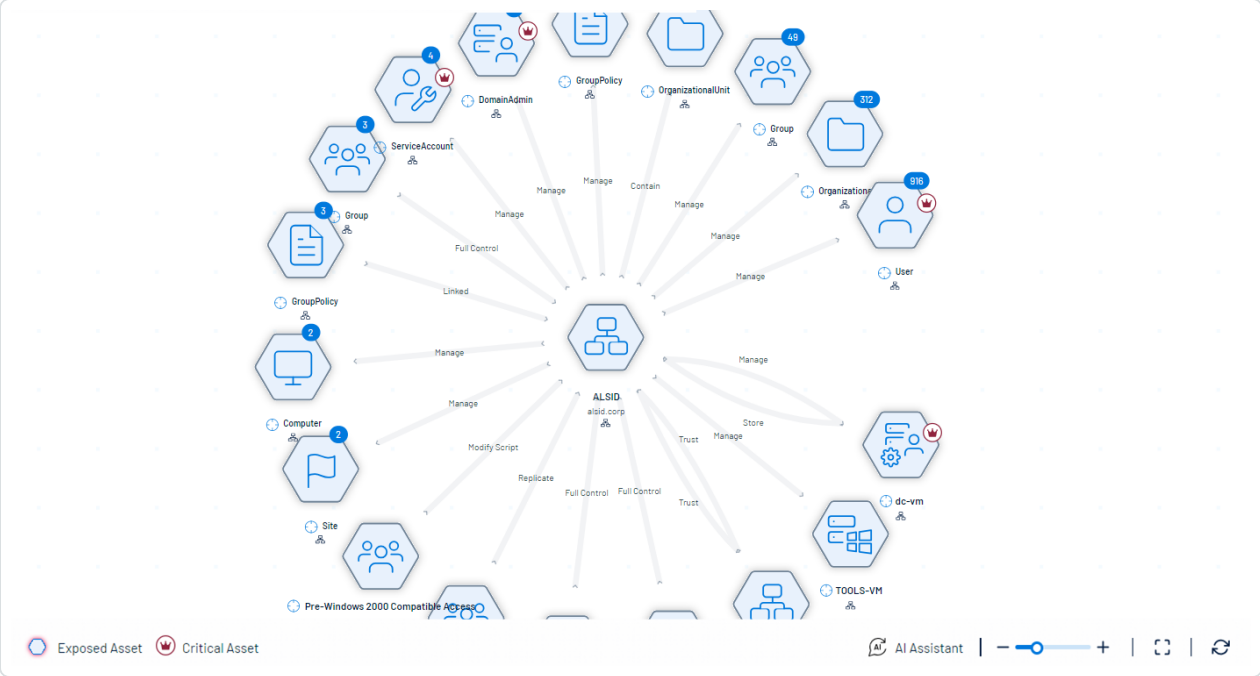
Using this AI, users can better understand the attack path and its associated risk. Here, you can also gain additional insight into the assets affected by the attack path.

For more information about AI explainability, how to use it, and its limitations, see the Attack Path Analysis Generative AI Best Practices Guide.

- Use your mouse cursor, the zoom slider, or the + and - buttons in the lower-right corner of the graph to zoom the graph in and out.
- Click the button to enable or disable full screen view.
- Click the button to reset the graph.
- Right-click on a step or an asset node to open a menu with additional options:
  - **Ask AI About This Node** – Click to open an AI chat window, where you can ask questions related to the asset node or the attack path to which it belongs.
    Using this AI, users can better understand the attack path and its associated risk. Here, you can also gain additional insight into the assets affected by the attack path. For more information about AI explainability, how to use it, and its limitations, see the Attack Path

Analysis Generative AI Best Practices Guide.

- **Expand Node** – Click to expand a full view of all items related to the asset node.



- **Blast Radius** – Click to open a blast radius query, where the selected node is the source of the attack path. For more information, see Generate a Blast Radius Query.
- **Asset Exposure** – Click to open an Asset Exposure query, where the selected node is the target of the attack path. For more information, see Generate an Asset Exposure Graph Query.

Information Panel

The Information panel displays additional information about asset nodes and attack paths on the **Discover** tab.

To view the information panel for a node or technique:

1. Access the **Discover** tab.
2. In the **Standard Queries** section, click **Query Builder**.

   The **Query Builder** pane appears.

3. Create a custom query or use a built-in query from the query library.

   For more information, see:

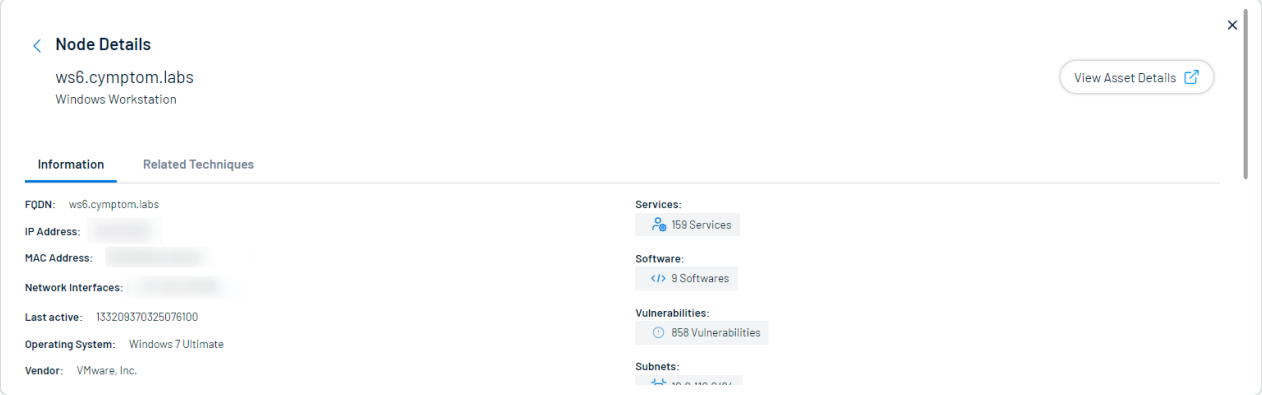
   - Generate an Attack Path Query with the Attack Path Query Builder
   - Generate an Asset Query with the Asset Query Builder

4. Do one of the following:

   - Click a node on the canvas.

     A panel appears at the bottom of the page with information about the node.

     Tip: In the upper-right corner, click **View in ...** to navigate directly to that application with the node's asset details displayed by default. For example. if the node is an asset, you can click **View in Asset Details** and navigate directly to the Tenable Inventory Asset Details page.

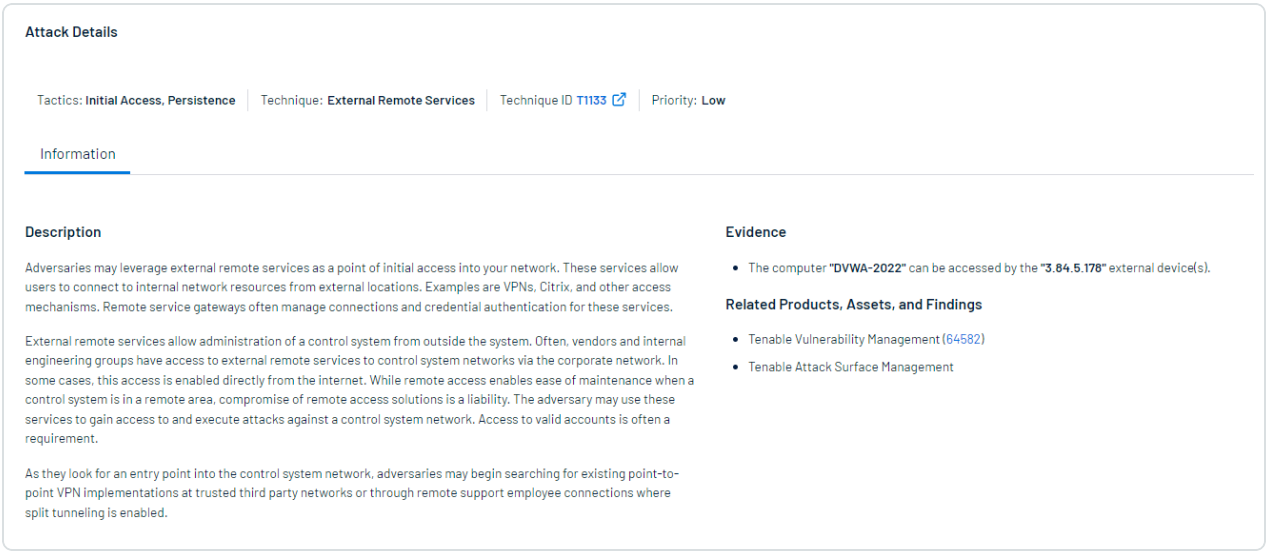
     This information includes, but is not limited to:

     - **Open Ports** – The open ports on the asset.
     - **ACR** – Tenable assigns an ACR to each asset on your network to represent the asset's relative criticality as an integer from 1 to 10. A higher ACR indicates higher criticality.
     - **AES** – Tenable calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.

- **AVR** – The Asset Vulnerability Rating (AVR) is an aggregation of all Vulnerability Priority Rating (VPR) scores for vulnerabilities detected on the asset.
- **NES** – The Node Exposure Score (NES) is a metric produced by Attack Path Analysis to understand the blast radius exposure of a node. This metric considers the Vulnerability Priority Rating of all vulnerabilities on the asset as well as other relationships such as software installed, sub-networks to which the asset belongs, internet exposure, etc.
- **Sensors** – The sensor or sensors that detected the asset.

- Click an attack technique (i.e., step) on the canvas.

  A panel appears with information about the technique such as a **Description** and **Evidence** of the technique.



  Here you can:

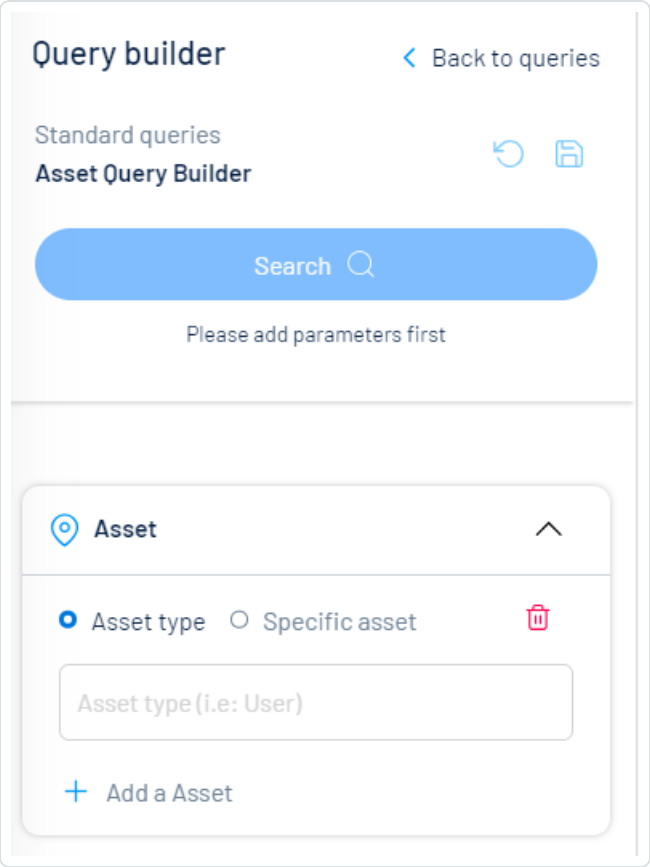
  - Click the **Technique ID** to navigate directly to the MITRE definition for that technique.
  - In the **Related Products, Assets, and Findings** section, click the plugin number to navigate directly to that plugin finding within the source application.

Note: Within the source application, the list of findings is filtered by related assets and plugin IDs. However, if there are more than 15 related assets, the list is filtered only by plugin IDs and shows findings for all assets within the source application.

Note: While source information is available for on-premises products such as Tenable Identity Exposure On-Prem and partial products such as Tenable Security Center without Tenable Vulnerability Management, links to the source application are currently unavailable for these.

Generate an Asset Query with the Asset Query Builder

You can use the **Asset Query Builder** to generate an interactive list of your nodes (assets and asset groups).



To generate a custom asset query:

1. In Attack Path Analysis, access the Discover tab.
2. In the **Custom Queries** section, click **Asset Query Builder**.

The **Query Builder** pane appears and displays the **Asset** configuration options.

3. For each asset you want to include in the query:
   a. Select the radio button next to the type of origin you want to use for the query:
      - **Asset type** – Generate a query based on a certain type of asset.
      - **Specific asset** – Generate a query based on a specific asset.
   b. In the text box, type the asset type or specific node/asset you want to use for the query.
   c. (Optional) To apply filters to the asset query:
      i. Click the button.

      The **Filters** window appears.

      ii. In the **Parameter** drop-down, select the parameter by which you want to filter the origin.

      iii. In the **Operator** drop-down, select the operator to apply to the parameter.

      iv. In the text box, type or select the value or values you want to use for the filter.

      > **Note:** The values you can use differ depending on the parameter you selected.

      v. Click **Apply and search**.

      Attack Path Analysis applies the filter to the asset query.
4. (Optional) Click **Add an Asset** to add additional assets to the query.
5. Click **Search**.

Attack Path Analysis returns any assets and/or asset groups that match the query you created. For more information on interacting with the data, see Interact with Asset Query Data.

6. (Optional) To save the query as a preset, at the top of the pane, click the button.

The **Save as preset** window appears:

a. In the **Name of preset** text box, type a name for the query.

b. In the **Description of preset** text box, type a description of the query.

c. Click **Save preset**.

Attack Path Analysis saves the query as a preset.

> **Tip:** When you save a query as a preset, you can use it as a filter on the **Findings** tab.

7. (Optional) To reset the query pane, at the top of the pane, click the button.

Attack Path Analysis resets the selections within the pane.

What to do next:

Interact with the asset data provided by the query.

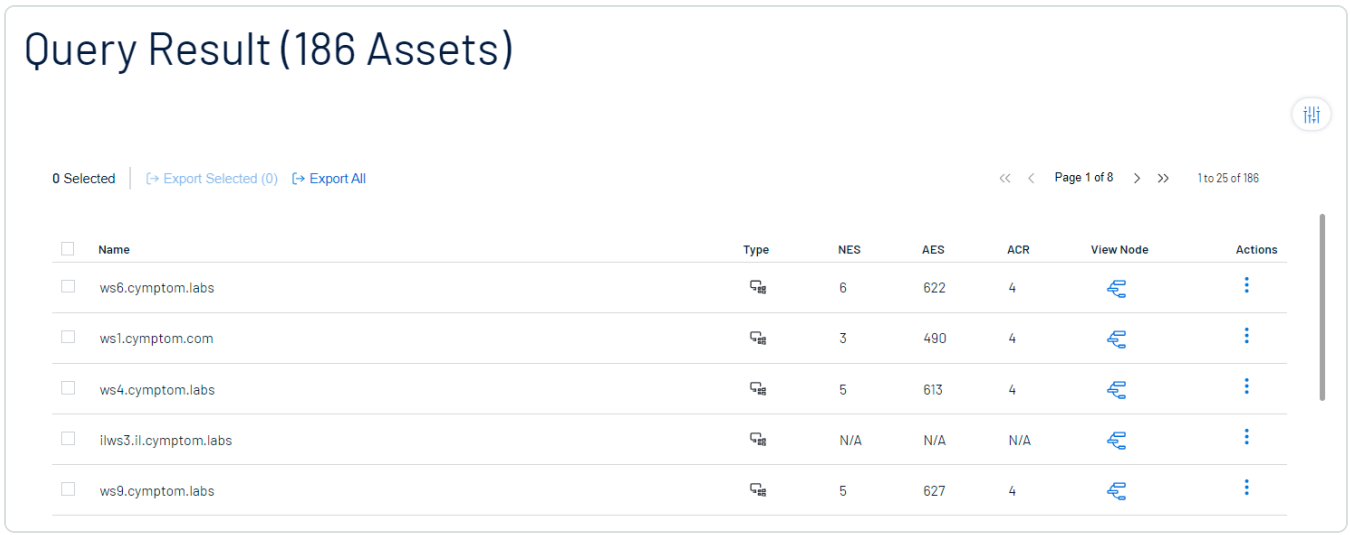
Interact with Asset Query Data

After you run an Asset Query, Attack Path Analysis displays the results associated with your query. From here, you can drill down and interact with the data to gain further insights.

To view and interact with asset query data:

1. Generate an Asset Query with the Asset Query Builder.

The **Query Result** page appears.



2. On the **Query Result** page, you can:

Note: Because the options and data in this section depend on the type of query you run, some of the following items may not be available for your query.

- View a list of assets that match your query. For example, if the query searches for workstations, the list displays all assets that have a *type* of **Workstation**. This table includes the following asset information:

Column	Description
Name	The asset name.
Type	The asset type, for example **Workstation** or **ServiceAccount**. **Tip:** Hover your mouse cursor over the icon in this column to view the full name of the asset type.
NES	The Node Exposure Score (NES) is a metric produced by Attack Path Analysis to understand the blast radius exposure of a node. This metric considers the Vulnerability Priority Rating of all vulnerabilities on the asset as well as other relationships such as software installed, sub-networks to which the asset belongs, internet exposure, etc.
AES	Tenable calculates a dynamic AES for each asset on your network to

	represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.
ACR	Tenable assigns an ACR to each asset on your network to represent the asset's relative criticality as an integer from 1 to 10. A higher ACR indicates higher criticality.
View Node	Click the button to view the asset nodes in a graphical format. For more information, see View Asset Nodes.
Actions	Click the button to view available actions. A menu appears: ◦ Click **Export as CSV** to export the asset information as a .csv file.

- Export one or more assets from the list:

  Do one of the following:

  ◦ To export individual assets:

  a. In the list, select the check box next to each asset you want to export.

  b. At the top of the list, click **Export Selected**.

  ◦ To export all assets in the list:

  a. At the top of the list, click **Export All**.

  Attack Path Analysis downloads the list of selected assets as a .csv file.

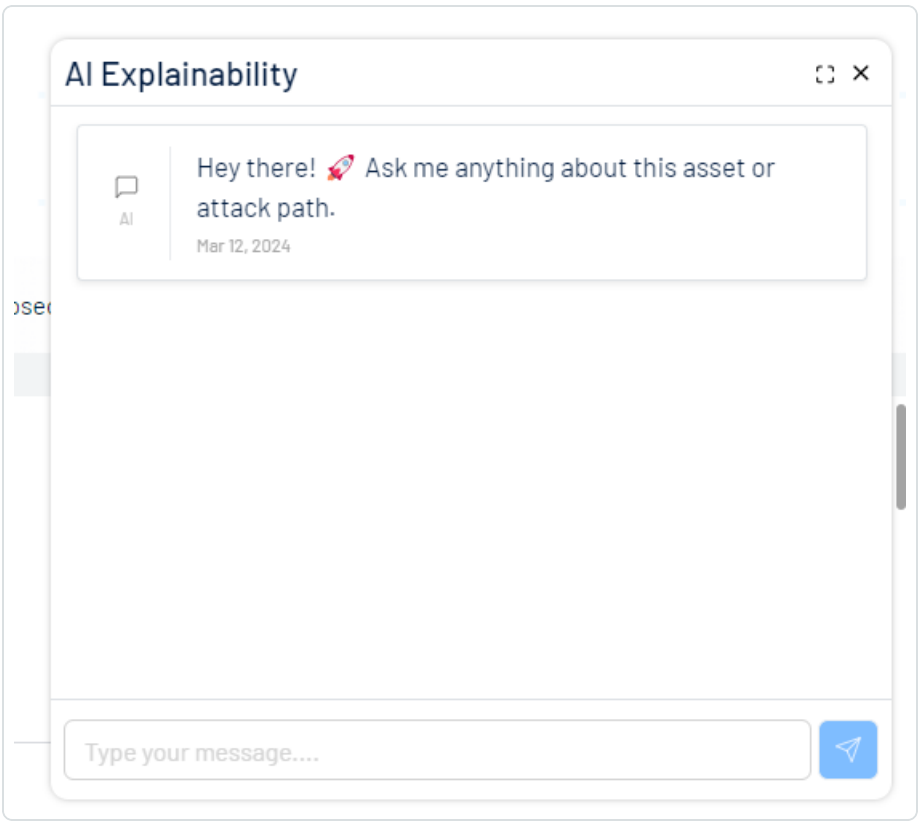
View Asset Nodes

When you click **View Nodes** in the **Query Result** list, Attack Path Analysis shows a graphical representation of the selected asset node.

Note: Because the options and data in this section depend on the type of query you run, some of the following items may not be available for your query.

In this section you can:

- View icons that represent the assets that match your query parameters.
    - Where applicable, view color-coded assets:
        - Exposed assets highlighted in red.
        - Critical assets highlighted by the icon.
- Click on a step or an asset to view the information panel for that item.
- Use your mouse cursor, the zoom slider, or the + and - buttons in the lower-right corner of the graph to zoom the graph in and out.
- Click **AI Assistant** to open an AI chat window, where you can ask questions related to the asset node or the attack path to which it belongs.

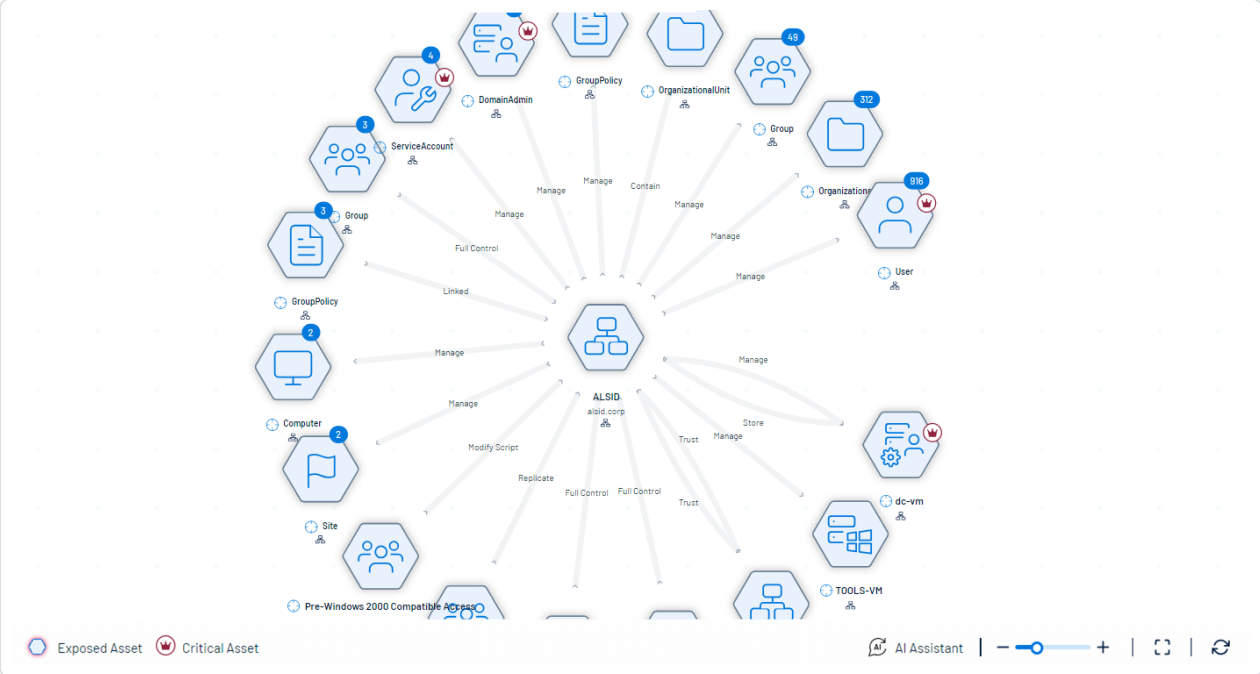


Using this AI, users can better understand the attack path and its associated risk. Here, you can also gain additional insight into the assets affected by the attack path.

For more information about AI explainability, how to use it, and its limitations, see the Attack Path Analysis Generative AI Best Practices Guide.

- Click the button to enable or disable full-screen view.
- Click the button to reset the graph.
- Right-click on a step or an asset node to open a menu with additional options:
  - **Ask AI About This Node** – Click to open an AI chat window, where you can ask questions related to the asset node or the attack path to which it belongs.
    Using this AI, users can better understand the attack path and its associated risk. Here, you can also gain additional insight into the assets affected by the attack path. For more information about AI explainability, how to use it, and its limitations, see the Attack Path Analysis Generative AI Best Practices Guide.

- **Expand Node** – Click to expand a full view of all items related to the asset node.



- **Blast Radius** – Click to open a blast radius query, where the selected node is the source of the attack path. For more information, see Generate a Blast Radius Query.
- **Asset Exposure** – Click to open an Asset Exposure query, where the selected node is the target of the attack path. For more information, see Generate an Asset Exposure Graph Query.

Information Panel

The Information panel displays additional information about asset nodes and attack paths on the **Discover** tab.

To view the information panel for a node or technique:

1. Access the **Discover** tab.
2. In the **Standard Queries** section, click **Query Builder**.

   The **Query Builder** pane appears.
3. Create a custom query or use a built-in query from the query library.

For more information, see:

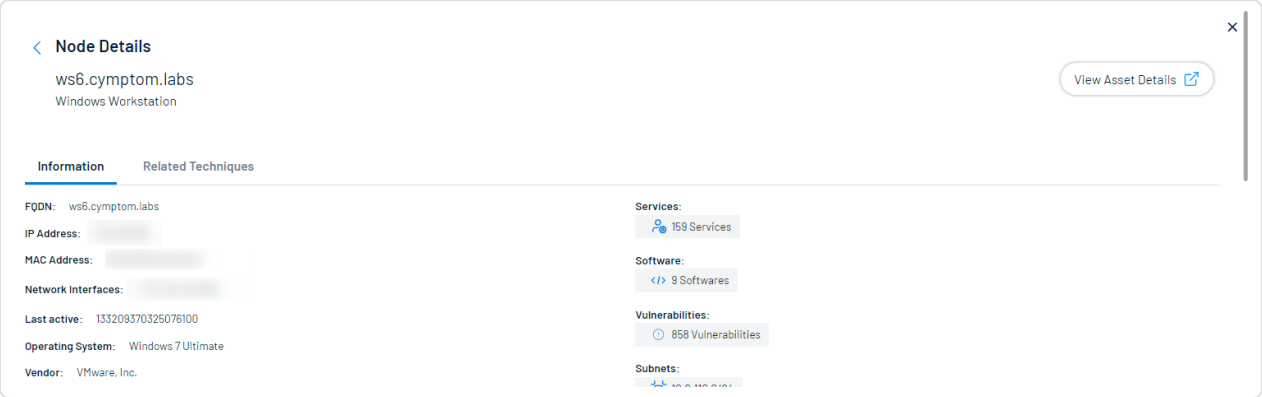
- Generate an Attack Path Query with the Attack Path Query Builder
- Generate an Asset Query with the Asset Query Builder

4. Do one of the following:

   - Click a node on the canvas.

     A panel appears at the bottom of the page with information about the node.

     Tip: In the upper-right corner, click **View in ...** to navigate directly to that application with the node's asset details displayed by default. For example. if the node is an asset, you can click **View in Asset Details** and navigate directly to the Tenable Inventory Asset Details page.

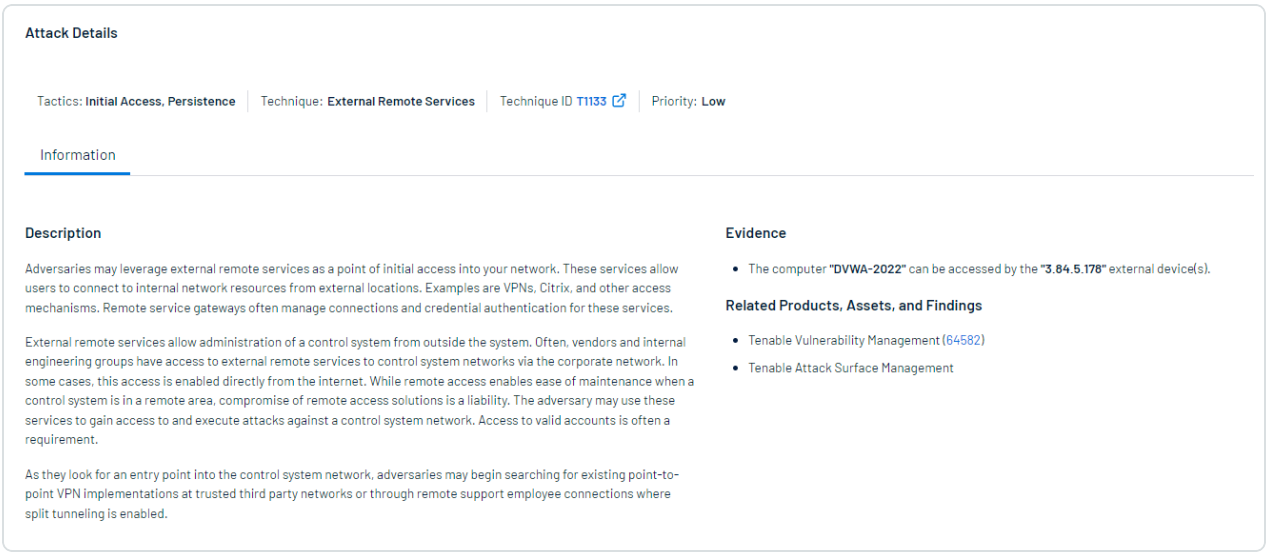
     This information includes, but is not limited to:

     - **Open Ports** – The open ports on the asset.
     - **ACR** – Tenable assigns an ACR to each asset on your network to represent the asset's relative criticality as an integer from 1 to 10. A higher ACR indicates higher criticality.
     - **AES** – Tenable calculates a dynamic AES for each asset on your network to represent the asset's relative exposure as an integer between 0 and 1000. A higher AES indicates higher exposure.
     - **AVR** – The Asset Vulnerability Rating (AVR) is an aggregation of all Vulnerability Priority Rating (VPR) scores for vulnerabilities detected on the asset.

- **NES** – The Node Exposure Score (NES) is a metric produced by Attack Path Analysis to understand the blast radius exposure of a node. This metric considers the Vulnerability Priority Rating of all vulnerabilities on the asset as well as other relationships such as software installed, sub-networks to which the asset belongs, internet exposure, etc.
- **Sensors** – The sensor or sensors that detected the asset.

- Click an attack technique (i.e., step) on the canvas.

  A panel appears with information about the technique such as a **Description** and **Evidence** of the technique.



  Here you can:

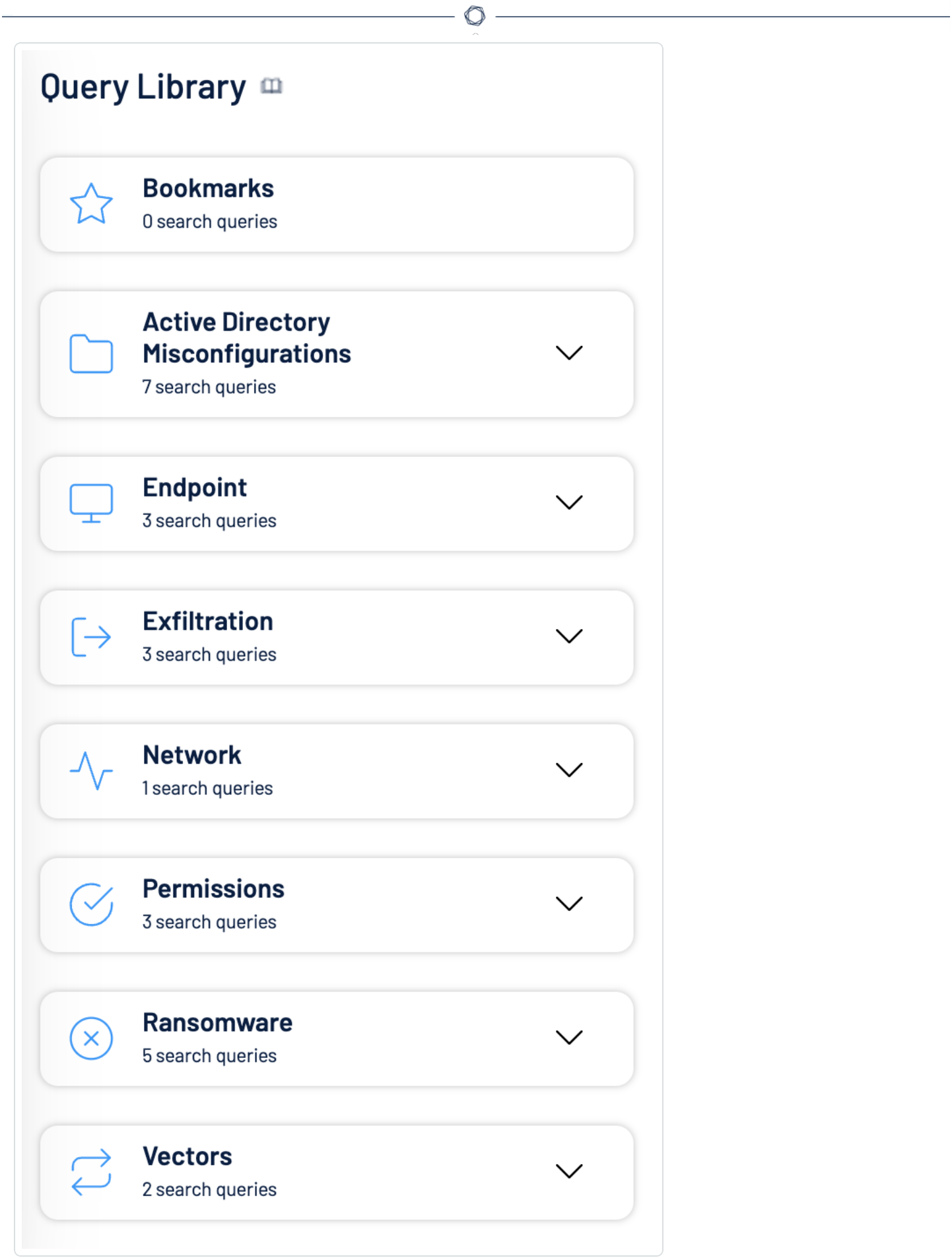
  - Click the **Technique ID** to navigate directly to the MITRE definition for that technique.
  - In the **Related Products, Assets, and Findings** section, click the plugin number to navigate directly to that plugin finding within the source application.

    Note: Within the source application, the list of findings is filtered by related assets and plugin IDs. However, if there are more than 15 related assets, the list is filtered only by plugin IDs and shows findings for all assets within the source application.

Note: While source information is available for on-premises products such as Tenable Identity Exposure On-Prem and partial products such as Tenable Security Center without Tenable Vulnerability Management, links to the source application are currently unavailable for these.

Generate an Attack Path with a Built-in Query

You can use Tenable-provided built-in queries to generate an attack path from one asset to another.


Query Library
Bookmarks
0 search queries
Active Directory Misconfigurations
7 search queries
Endpoint
3 search queries
Exfiltration
3 search queries
Network
1 search queries
Permissions
3 search queries
Ransomware
5 search queries
Vectors
2 search queries

Tip: To generate your own custom query, see Generate an Attack Path Query with the Attack Path Query Builder.

To generate a built-in query:

1. In Attack Path Analysis, access the **Discover** tab.
2. In the **Query Library** section, click the tile that contains the search query you want to use. For more information, see Query Types in the Attack Path Query Library.
3. Click **Search for attack paths**.

   Attack Path Analysis returns any attack paths that match the query you selected and the **Query Builder** appears. For more information on interacting with the data, see Interact With Attack Path Data.

   Note: If there are no matching attack paths, Attack Path Analysis does not return any results for the query.
4. (Optional) Use the **Query Builder** to edit the built-in query you selected. For more information, see Generate an Attack Path Query with the Attack Path Query Builder.

   Note: If you edit a built-in query, your changes do not affect the query within the query library. Instead, you can save the new query as a preset, which appears in the **Bookmarks** tile in the **Query Library**.

What to do next:

Interact with the attack path data provided by the query.

Query Types in the Attack Path Query Library

When generating an attack path from a **Built-in Query**, you can use the following queries within the **Query Library**.

Note: Some query types may not be available for all users.

Tile	Query Types
Bookmarks	When a user saves a custom attack path query, Attack Path Analysis

	saves the query in the **Bookmarks** section. Here, you can view the query, the user who created it, and select the bookmark to use to generate an attack path query. For more information, see (Optional) Save your Query as a Preset/Bookmark.
Active Directory Misconfigurations	• **LAPS Password** – Users with permissions to read LAPS Passwords. • **AdminSDHolder** – Users with write/full control access to AdminSDHolder objects. • **Kerberos Delegation** – Users with permissions to perform Kerberos delegation. • **Domain Admins vulnerable to Kerberos Delegation** – Domain Admins that are not part of Protected Users or has not delegated flag. • **DNS Admins** – Users that are members of the DNS Admins group. • **Reversible Password Hash** – Users whose password is stored in the Active Directory in reversible encryption format. • **Password Not Expired** – Users whose password never expires. • **Password Not Required** – Users who do not require a password for authentication.
Cloud	• **Exposed cloud storage** – Cloud storage that is exposed to the internet. • **Computers vulnerable from cloud** – Computers that have management ports open from the Internet. • **Publicly exposed workload leads to exfiltration** – A publicly exposed web application that leads to compromise of EC2 workload and access to data in S3 bucket.

Common Vulnerabilities	• **Bluekeep** – Computers that are vulnerable to CVE-2019-0708. • **EternalBlue** – Computers that are vulnerable to CVE-2017-0144. • **log4shell** – Computers that are vulnerable to CVE-2021-44228. • **PrintNightmare** – Computers that are vulnerable to CVE-2021-44228. • **ProxyLogon** – Computers that are vulnerable to CVE-2021-26855. • **Zerologon** – Computers that are vulnerable to CVE-2020-1472.
Credentials	• **Domain Admins password reuse** – Domain admin users whose passwords are shared by other users. • **Cracked Passwords** – Passwords that could be cracked by an attacker. • **Kerberoasting** – Users vulnerable to the Kerberoasting attack.
Endpoint	• **Computers that Cache Domain Admins** – Computers that are not Domain Controllers and cache the credentials of domain admin users. • **Bitlocker** – Computers configured without Bitlocker. • **Vulnerable registry service** – Computer services that can be altered by unprivileged Domain Users from the Registry. • **Vulnerable service binaries** – Computer services that can be altered by unprivileged Domain Users from a binary file. • **Services that Cache Domain Admins User** – Services that run under the context of domain admin users.
Network	• **Computers with SMBv1** – Computers with SMB version 1 enabled. • **NBT-NS Poisoning** – LLMNR/NBT-NS Poisoning and SMB

	Relay techniques compromising domain admin users.
Permissions	• **Domain Admin Password Reset** – Users who have permissions to reset a domain admin user password. • **Critical Asset Policy Modification** – Users that have permissions to modify a Group Policy Object (GPO) that affects a Critical Asset. • **Group Membership Modification** – Users that have permissions to modify group membership. • **Network Shares Access** – Network shares accessible by the Everyone user group.
Ransomware	**Note:** The simulations used in these queries do not pose any risk of impact on your system. • **WannaCry Ransomware Attack** – Search an attack with WannaCry TTPs, such as EternalBlue exploit. • **Fancy Bear APT 28** – Search for an attack vector that mimics APT 28. • **Maze Ransomware Attack** – Search an attack with Maze TTPs, such as unique WMI capabilities. • **Ryuk Ransomware Attack** – Search an attack with Ryuk TTPs, such as unique encryption capabilities. • **REvil Ransomware Attack** – Search an attack with REvil TTPs, such as unique evasion capabilities. • **Lazarus Group** – Search for an attack vector that mimics Lazarus Group. • **Petya Ransomware** – Search an attack vector where Petya Group used.
Top Searches	• **Computers with Domain Admin and Log4Shell** – Search for assets that are vulnerable to CVE-2021-44228 and cache the

	credentials of Domain Admin account • **Network Shares that Can Be Accessed by Non-administrators** – Search for network shares with read/write access for a non-administrative account • **Services that Run As Domain Admin** – Search for system services that runs in the context of a Domain Admin account • **Computers exposed to the internet via SMBv1** – Search for computers that were found with SMBv1 exposed to the internet.
Vectors	• **Domain Users to Domain Admins** – Users in the Domain Users group-escalating privileges to the Domain Admins group. • **Workstations to Critical Assets** – An attack path from Workstations to Critical Assets.

Attack Path Analysis Techniques

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

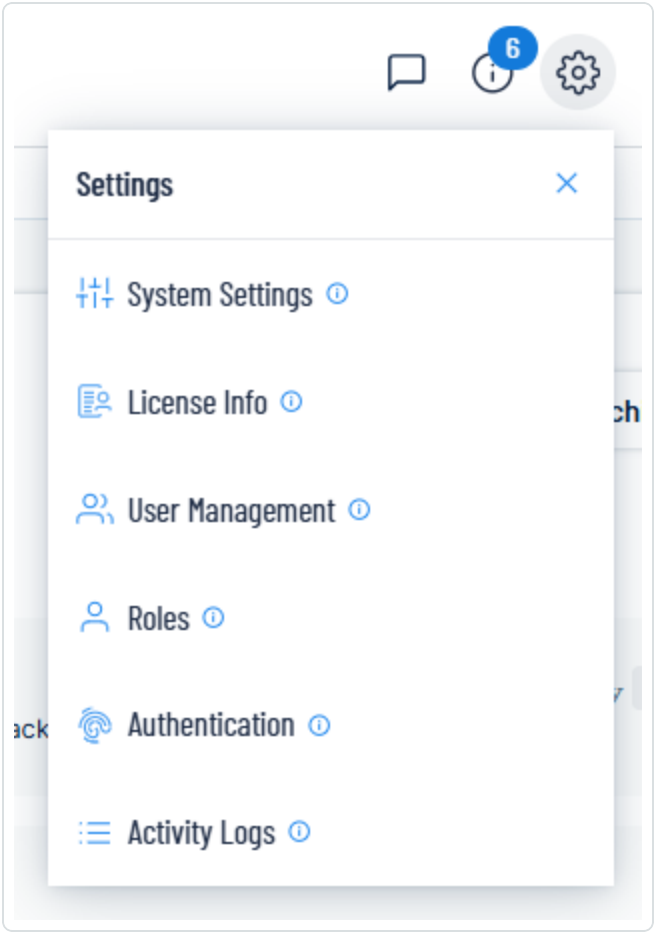
Access the Settings Menu

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

To access the **Settings** menu:

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

   The **Settings** menu appears.



2. Click one of the following options:

   - System Settings – View and manage settings for your container.
   - License Information – View your license information.
   - User Management – View and manage all users, groups, and permissions.
   - Roles – View and manage your Attack Path Analysis roles.

- Authentication – View and manage your user authentication settings.
- Activity Logs – View user activity logs.

System Settings

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

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

To access the Settings page:

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

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

License Information

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

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

To access the License page:

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

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

User Management

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

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

To access the Users page:

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

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

Roles

Roles allow you to manage privileges for major functions and control which Attack Path Analysis resources users can access.

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

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

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

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

The Attack Path Analysis interface supports the following role types:

- Administrator – Has all permissions and privileges, is responsible for setting up the account, and knows the organization's architecture. They can create groups to organize different business units, and add and manage users on the account.

- Custom – Has custom applied privileges specific to organizational needs. For more information, see the following documentation in the *Tenable Vulnerability Management User Guide*:
  - Custom Roles
    - Create a Custom Role
    - Duplicate a Role
    - Edit a Custom Role
    - Delete a Custom Role
  - Export Roles

Authentication

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

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

To access the My Account page:

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

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

Activity Logs

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

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

To access the System Settings page:

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

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