# Table of Contents

**Welcome to Attack Path Analysis** ................................................................. 5

Get Started with Attack Path Analysis ......................................................... 7

Key Terms ........................................................................................................... 9

Example Workflow .......................................................................................... 12

Attack Path Analysis Metrics .......................................................................... 14

Data Timing ....................................................................................................... 14

Cyber Exposure Score (CES) ............................................................................ 15

Asset Exposure Score (AES) .............................................................................. 15

Asset Criticality Rating (ACR) .......................................................................... 15

Attack Path Analysis Categories ..................................................................... 16

Attack Path Analysis Scoring Explained .......................................................... 16

Log in to Attack Path Analysis ........................................................................ 17

Navigate Attack Path Analysis ....................................................................... 17

Log out of Attack Path Analysis ...................................................................... 24

**Attack Path Analysis** .................................................................................. 25

Attack Path Analysis Dashboard ..................................................................... 27

Mitre Att&ck Heatmap ...................................................................................... 29

Findings ............................................................................................................. 32

Export a Finding ............................................................................................... 37

Add and View Comments on a Finding ............................................................ 38

Change the Status of a Finding ........................................................................ 39

Archive a Finding ............................................................................................. 40

View Finding Details ......................................................................................... 40
<table>
<thead>
<tr>
<th>Finding Details</th>
<th>44</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Log History</td>
<td>45</td>
</tr>
<tr>
<td>Discover</td>
<td>46</td>
</tr>
<tr>
<td>Generate an Attack Path Query with the Attack Path Query Builder</td>
<td>51</td>
</tr>
<tr>
<td>Generate an Asset Exposure Graph Query</td>
<td>55</td>
</tr>
<tr>
<td>Generate a Blast Radius Query</td>
<td>58</td>
</tr>
<tr>
<td>Interact with Attack Path Query Data</td>
<td>60</td>
</tr>
<tr>
<td>Information Panel</td>
<td>66</td>
</tr>
<tr>
<td>Generate an Asset Query with the Asset Query Builder</td>
<td>68</td>
</tr>
<tr>
<td>Interact with Asset Query Data</td>
<td>71</td>
</tr>
<tr>
<td>Information Panel</td>
<td>76</td>
</tr>
<tr>
<td>Generate an Attack Path with a Built-in Query</td>
<td>78</td>
</tr>
<tr>
<td>Query Types in the Attack Path Query Library</td>
<td>80</td>
</tr>
<tr>
<td>Attack Path Analysis Techniques</td>
<td>84</td>
</tr>
</tbody>
</table>

**Access the Settings Menu** | 85 |
| System Settings | 87 |
| Data Sources | 87 |
| Data Timing | 88 |
| Configure Data Sources for Attack Path Analysis | 88 |
| Plugins Required for Attack Path Analysis | 90 |
| License Information | 92 |
| User Management | 92 |
| Roles | 92 |
| Authentication | 93 |
Activity Logs
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 data set of vulnerability and exposure context.
- Communicate exposure risk to business leaders and stakeholders with clear KPIs, benchmarks, and actionable insights.
- Leverage the broadest vulnerability coverage spanning IT assets, cloud resources, containers, web apps, and identity systems.
- Integrate with third-party data sources and tools for enhanced exposure analysis and remediation.

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

- Tenable One Introduction (Tenable University)

Tenable One is a package that includes the following products:

<table>
<thead>
<tr>
<th>Product</th>
<th>Tenable One Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable Vulnerability Management</td>
<td>Tenable One Standard, Tenable One Enterprise</td>
</tr>
<tr>
<td>Legacy Tenable Cloud Security</td>
<td>Tenable One Standard, Tenable One Enterprise</td>
</tr>
</tbody>
</table>
Use Cases

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

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

Utilize the Asset Inventory to:

- Utilize existing tags or create new tags that can be used to create custom exposure cards.
- View and manage all assets, regardless of their source.

For more information, see Get Started with Attack Path Analysis.

Get Started with Attack Path Analysis

Tenable recommends following these steps to get started with Attack Path Analysis data and functionality.

Tip: For additional information on getting started with Tenable One products, check out the Tenable One Deployment Guide and review the following customer education materials:

- Tenable One Introduction (Tenable University)

Prepare

Before you begin:

Ensure you have the following:

- 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.

- A default Tenable Web App Scanning scan, including injection plugins.
- An AWS connection with a Legacy Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.
- Tenable recommends the following:
  - Have at least 60% of assets scanned via an authenticated scan.
  - Select maximum verbosity in the Basic Network Scan.
  - 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.
- Familiarize yourself with the Attack Path Analysis key terms.
- Review the Tenable One Licensing Quick-Reference Guide.
- Familiarize yourself with the categories and data metrics within Attack Path Analysis.
- Review the Tenable One Example Workflow.

License, Access, and Log In

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

To acquire a license:

1. Determine the interface that best suits your business objectives. For more information, see Use Cases.
2. Contact your Tenable representative to purchase the appropriate package.
To access and log in to Attack Path Analysis:

Follow the [Log in to Attack Path Analysis](#) steps.

### Configure Attack Path Analysis for Use

- Configure your [Attack Path Analysis](#) settings.
- View your [data sources](#).

### Assess Your Exposure

Review your CES and perform analysis:

- Access [Attack Path Analysis](#), where you can:
  - Generate custom, built-in, asset exposure graph, or blast radius queries to view attack path data.
  - Interact with the attack path data.

### Key Terms

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

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory (AD)</td>
<td>Attack Path Analysis integrates AD data from Tenable Identity Exposure.</td>
</tr>
<tr>
<td>Asset</td>
<td>Any IT or security element in your organization such as user accounts,</td>
</tr>
<tr>
<td></td>
<td>computers, and software. The <a href="#">Discover</a> section represents an asset</td>
</tr>
<tr>
<td></td>
<td>as a node in the graph.</td>
</tr>
<tr>
<td>Asset Exposure Graph</td>
<td>A visualization of an attack path from multiple assets down to one asset.</td>
</tr>
<tr>
<td>Asset Exposure Score (AES)</td>
<td>Tenable calculates a dynamic AES for each asset on your network to</td>
</tr>
<tr>
<td></td>
<td>represent the asset's relative exposure as an integer between 0 and</td>
</tr>
<tr>
<td></td>
<td>1000. A higher AES indicates higher exposure.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Asset Vulnerability Rating (AVR)</td>
<td>An aggregation of all Vulnerability Priority Rating (VPR) scores for vulnerabilities detected on an asset.</td>
</tr>
<tr>
<td>Benchmark</td>
<td>A group of scores to which you can compare your scores and assess your performance.</td>
</tr>
<tr>
<td>Blast Radius</td>
<td>A visualization of one or more attack paths from one asset to multiple other assets.</td>
</tr>
<tr>
<td>CES Trend</td>
<td>A measurement that defines how your CES improves or regresses over time.</td>
</tr>
<tr>
<td>Chief Information Security Officer (CISO)</td>
<td>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.</td>
</tr>
<tr>
<td>Choke Point Priority</td>
<td>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 <strong>Low</strong>, <strong>Medium</strong>, <strong>High</strong>, and <strong>Critical</strong>.</td>
</tr>
<tr>
<td>Cyber Exposure Score (CES)</td>
<td>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.</td>
</tr>
<tr>
<td>Data Source</td>
<td>A product that feeds data into Tenable One (for example, Tenable Vulnerability Management).</td>
</tr>
<tr>
<td>Evidence</td>
<td>The empirical data from different data sources confirming the feasibility of a <strong>Step</strong> as part of an attack path.</td>
</tr>
<tr>
<td>Exposure Card</td>
<td>An Exposure card represents the incoming data from your configured tags and data sources. It aggregates and normalizes the data to provide a</td>
</tr>
<tr>
<td><strong>Exposure Card View</strong></td>
<td>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.</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Exposure View</strong></td>
<td>A holistic and unified view combining internal and external data sources to provide a complete view of risk in a singular location.</td>
</tr>
<tr>
<td><strong>Finding</strong></td>
<td>A feasible implementation of a technique or sub-technique in one or more attack paths that an adversary can leverage. Each finding has a Choke Point Priority that determines its urgency and potential impact.</td>
</tr>
<tr>
<td><strong>Industry Benchmark</strong></td>
<td>A benchmark based on members of your Tenable-assigned industry to which you can compare your scores and assess your performance.</td>
</tr>
<tr>
<td><strong>MITRE ATT&amp;CK®</strong></td>
<td>MITRE ATT&amp;CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The MITRE ATT&amp;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.</td>
</tr>
<tr>
<td><strong>Node Exposure Score (NES)</strong></td>
<td>A metric produce by Tenable One to understand the blast radius exposure of a node. This metric considers the Vulnerability Priority Rating of all vulnerabilities on the asset as well as other relationships such as software installed, sub-networks to which the asset belongs, internet exposure, etc.</td>
</tr>
<tr>
<td><strong>Path Priority Rating</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Population Benchmark</strong></td>
<td>A benchmark based on members of the entire population to which you can compare your scores and assess your performance.</td>
</tr>
<tr>
<td><strong>Query Builder</strong></td>
<td>A customizable visualization of one or more attack paths based on configurable source and target assets.</td>
</tr>
<tr>
<td><strong>Query Library</strong></td>
<td>Predefined queries that visualize scenarios of potential attack paths based on...</td>
</tr>
</tbody>
</table>
on real-world attacks.

<table>
<thead>
<tr>
<th>Operational Technology (OT)</th>
<th>Tenable One integrates OT data from OT Security.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Practitioner</td>
<td>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.</td>
</tr>
<tr>
<td>Service Level Agreement (SLA)</td>
<td>A control by which you can identify whether assets comply with customer security requirements.</td>
</tr>
<tr>
<td>Step</td>
<td>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 &quot;bracket&quot; between two or more assets.</td>
</tr>
<tr>
<td>Technique / Sub-Technique</td>
<td>Represents &quot;how&quot; an adversary achieves a tactical goal by performing an action. For example, an adversary can dump credentials to achieve credential access.</td>
</tr>
<tr>
<td>Tags</td>
<td>A way to group assets by business context. For example, you can group assets by product, permissions, business owner, etc.</td>
</tr>
<tr>
<td>Vulnerability Management (VM)</td>
<td>Tenable One integrates VM data from Tenable Vulnerability Management and Tenable Security Center.</td>
</tr>
<tr>
<td>Web Application Scanning (WAS)</td>
<td>Tenable One integrates web app scanning data from Tenable Web App Scanning.</td>
</tr>
</tbody>
</table>

**Example Workflow**

The following scenario describes a common use case where the Lumin Exposure View, , 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?

### 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.

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.

<table>
<thead>
<tr>
<th>CES Category</th>
<th>CES Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>650 to 1000</td>
</tr>
<tr>
<td>Medium</td>
<td>350 to 649</td>
</tr>
<tr>
<td>Low</td>
<td>0 to 349</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>AES Category</th>
<th>AES Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>650 to 1000</td>
</tr>
<tr>
<td>Medium</td>
<td>350 to 649</td>
</tr>
<tr>
<td>Low</td>
<td>0 to 349</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>ACR Category</th>
<th>ACR Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>9 to 10</td>
</tr>
<tr>
<td>High</td>
<td>7 to 8</td>
</tr>
<tr>
<td>Medium</td>
<td>4 to 6</td>
</tr>
<tr>
<td>Low</td>
<td>1 to 3</td>
</tr>
</tbody>
</table>

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

**Attack Path Analysis Categories**

Attack Path Analysis products refer to data sources as Categories. For more information, see [Data Sources](#).

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Resources</td>
<td><img src="image" alt="Cloud Icon" /></td>
</tr>
<tr>
<td><strong>Note</strong>: Currently, Tenable One only supports the ingestion of Legacy Tenable Cloud Security data. For more information, contact your Tenable Representative.</td>
<td></td>
</tr>
<tr>
<td>Web Applications</td>
<td><img src="image" alt="Web Icon" /></td>
</tr>
<tr>
<td>Identity Exposure</td>
<td><img src="image" alt="Identity Icon" /></td>
</tr>
<tr>
<td>Computing Resources</td>
<td><img src="image" alt="Computing Icon" /></td>
</tr>
</tbody>
</table>

**Attack Path Analysis Scoring Explained**

The building blocks for the Cyber Exposure Score (CES) in the Tenable One Exposure Management Platform are similar to those used for years in Tenable products (e.g., Tenable Vulnerability Management, Tenable Lumin). These mechanisms have to date only been used for vulnerability
management data. Tenable One expands these concepts into new realms of the attack surface: 

**Web Applications** (Tenable Web App Scanning), **Cloud Resources** (Legacy Tenable Cloud Security), and **Identity** (Tenable Identity Exposure).

For more information on Tenable One scoring, see the *Tenable One Scoring Explained* Quick Reference Guide.

**Log in to Attack Path Analysis**

To log in to Attack Path Analysis:

1. In a supported browser, navigate to [https://cloud.tenable.com/](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.

**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.

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

To access the Settings menu:
1. In the upper-right corner, click the button.

   The **Settings** menu appears.

2. Click an item to navigate to that system configuration page.

### Workspace

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

### 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**.
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 understanding 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.

Before you begin:

Ensure you have the following:

- 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.

- A default Tenable Web App Scanning scan, including injection plugins.
- An AWS connection with a Legacy Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.

- Tenable recommends the following:
  - Have at least 60% of assets scanned via an authenticated scan.
  - Select maximum verbosity in the Basic Network Scan.
  - 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.

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 AVR 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.

![Attack Path Analysis Dashboard](image)

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

<table>
<thead>
<tr>
<th>Widget</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Compare To</strong></td>
<td>Compare and view the difference between the current data and the data from a specific timeframe. You can select from these options:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Yesterday</td>
</tr>
<tr>
<td></td>
<td>• 7 days</td>
</tr>
<tr>
<td></td>
<td>• 15 days</td>
</tr>
<tr>
<td></td>
<td>• 30 days</td>
</tr>
<tr>
<td>Widget</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>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.</td>
<td></td>
</tr>
<tr>
<td><strong>Critical Assets (reached/total)</strong></td>
<td>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 <strong>Discover</strong> tab.</td>
</tr>
<tr>
<td><strong>Attack Path Leading to Critical Asset</strong></td>
<td>The number of attack paths that lead to critical assets. Click the 🔄 icon to view the attack paths in the <strong>Discover</strong> tab.</td>
</tr>
<tr>
<td><strong>Open Findings</strong></td>
<td>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 <strong>Findings</strong> tab.</td>
</tr>
</tbody>
</table>
| **Attack Path Matrix**                      | Each square in the matrix shows the number of attack paths that corresponds to a range in target Asset Criticality Rating (ACR) and Asset Vulnerability Rating (AVR) values.  
For example, you can quickly view the attack paths that lead to the highest ACR targets and AVR 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, where you can view the matching paths. |
| **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.

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 checkmark 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.

- Filter the techniques based on platforms by selecting one of the options from the left-hand side of the page:
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:

Ensure you have the following:

- 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.

- A default Tenable Web App Scanning scan, including injection plugins.
- An AWS connection with a Legacy Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.

Tenable recommends the following:

- Have at least 60% of assets scanned via an authenticated scan.
- Select maximum verbosity in the Basic Network Scan.
- 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.
- 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.

  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:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Filters by priority: critical, high, medium, or low.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Filters by status: <strong>To Do</strong>, <strong>In Progress</strong>, <strong>In Review</strong>, and <strong>Done</strong>.</td>
</tr>
<tr>
<td>Source</td>
<td>Filters by the attack path source.</td>
</tr>
<tr>
<td>Target</td>
<td>Filters by the attack path target.</td>
</tr>
<tr>
<td>CVE</td>
<td>Filters by specific CVEs.</td>
</tr>
<tr>
<td>Mitigations</td>
<td>Filters by mitigations for the attack techniques.</td>
</tr>
<tr>
<td>Tactic</td>
<td>Filters attack techniques with similar tactics.</td>
</tr>
<tr>
<td>Technique</td>
<td>Filters by attack techniques. For more information about attack techniques, see <a href="#">Attack Path Analysis Techniques</a>.</td>
</tr>
</tbody>
</table>

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 \( \text{.Tile} \) 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.

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](#) **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.

- View **Evidence** related to the finding.

- 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.

i. (Optional) In the upper-right corner, click the Action drop-down and select one of the following actions:

  ○ **Copy to Clipboard** — Copy the mitigation steps to your device's clipboard.

  ○ **Create a Jira Ticket** — Create a Jira ticket from the steps listed in the mitigation guide.

  ○ **Export to CSV** — Export the mitigation steps in CSV format.

  ○ **Export to PDF** — Export the mitigation steps in PDF format.

  ○ **Export to JSON** — Export the mitigation steps in JSON format.

- **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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 🔗 | - 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:**

**Ensure you have the following:**

- 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.

- A default Tenable Web App Scanning scan, including injection plugins.

- An AWS connection with a Legacy Tenable Cloud Security scan policy including all vulnerabilities and available AWS resources.

- Tenable recommends the following:
  - Have at least 60% of assets scanned via an authenticated scan.
  - Select maximum verbosity in the Basic Network Scan.
  - 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.

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.

Tip: By default, Attack Path Analysis only loads the first page of top attack paths. Click Find All Attack Paths to load additional paths.

In this list, you can:
- Filter the list:
  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:

<table>
<thead>
<tr>
<th>Filter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Filters by the attack path name.</td>
</tr>
<tr>
<td>Summary</td>
<td>Filters by the attack path summary text.</td>
</tr>
<tr>
<td>Priority</td>
<td>Filters by priority: critical, high, medium, or low.</td>
</tr>
</tbody>
</table>

  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:

- **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 button 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 on 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.

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 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. You can access your saved queries in the **Bookmarks** section of the **Query Library**.

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

13. (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 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 ▼ 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 📜 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.

### Query Result (9 Attack Paths)

<table>
<thead>
<tr>
<th>Name</th>
<th>Path Priority Rating</th>
<th>Nodes</th>
<th>View Graph</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSG Exploits Privilege Escalation for Unauthorized Access</td>
<td>High</td>
<td>n/a</td>
<td><img src="image" alt="View Graph" /></td>
<td><img src="image" alt="Actions" /></td>
</tr>
<tr>
<td>Exploiting Windows Server Privilege Escalation on sqlservr</td>
<td>Critical</td>
<td>n/a</td>
<td><img src="image" alt="View Graph" /></td>
<td><img src="image" alt="Actions" /></td>
</tr>
<tr>
<td>Exploiting Windows Server Privilege Escalation on IIS</td>
<td>N/A</td>
<td>n/a</td>
<td><img src="image" alt="View Graph" /></td>
<td><img src="image" alt="Actions" /></td>
</tr>
<tr>
<td>10.0.110.0/24 Exploits ZeroLogon vulnerability to gain access to sqlservr</td>
<td>N/A</td>
<td>n/a</td>
<td><img src="image" alt="View Graph" /></td>
<td><img src="image" alt="Actions" /></td>
</tr>
<tr>
<td>10.0.120.0/24 Exploits ZeroLogon vulnerability to gain access to IIS</td>
<td>N/A</td>
<td>n/a</td>
<td><img src="image" alt="View Graph" /></td>
<td><img src="image" alt="Actions" /></td>
</tr>
</tbody>
</table>

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:
<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The attack path name.</td>
</tr>
<tr>
<td>Path Priority Rating</td>
<td>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.</td>
</tr>
<tr>
<td>Nodes</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Tip:</strong></td>
<td>Hover your mouse cursor over the icon in this column to view the full name of the node type.</td>
</tr>
<tr>
<td>View Graph</td>
<td>Click the button to view the attack path in a graphical format. For more information, see View the Attack Path Graph.</td>
</tr>
<tr>
<td>Actions</td>
<td>Click the button to view available actions. A menu appears:</td>
</tr>
<tr>
<td></td>
<td>- Click View Findings to navigate directly to the Findings page filtered by the selected attack path.</td>
</tr>
<tr>
<td></td>
<td>- Click Export as CSV to export the attack path information as a .csv file.</td>
</tr>
</tbody>
</table>

- 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.
- 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 Asset Details to navigate directly to Asset Inventory with the node's asset details displayed by default.

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.

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

<table>
<thead>
<tr>
<th>Attack Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tactic: Lateral Movement</td>
</tr>
</tbody>
</table>

**Description**
Adversaries may exploit remote services to gain unauthorized access to internal systems once inside of a network. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system. An adversary may need to determine if the remote system is in a vulnerable state, which may be done through Network Service Discovery or other Discovery methods looking for common vulnerabilities that may be deployed in the network, the lack of certain patches that may indicate vulnerabilities, or security software that

**Evidence**
- Computer “LN-DC” is vulnerable to CVE “CVE-2023-35314”

Click the **Technique ID** to navigate directly to the MITRE definition for that technique.

---

**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:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The asset name.</td>
</tr>
<tr>
<td>Type</td>
<td>The asset type, for example <strong>Workstation</strong> or <strong>ServiceAccount</strong>.</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> Hover your mouse cursor over the icon in this column to view the full name of the asset type.</td>
</tr>
<tr>
<td>NES</td>
<td>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.</td>
</tr>
<tr>
<td>AES</td>
<td>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.</td>
</tr>
<tr>
<td>ACR</td>
<td>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.</td>
</tr>
<tr>
<td>View Node</td>
<td>Click the 📊 button to view the asset nodes in a graphical format. For more information, see <strong>View Asset Nodes</strong>.</td>
</tr>
<tr>
<td>Actions</td>
<td>Click the 📀 button to view available actions.</td>
</tr>
<tr>
<td></td>
<td>A menu appears:</td>
</tr>
<tr>
<td></td>
<td>- Click <strong>Export as CSV</strong> to export the asset information as a .csv file.</td>
</tr>
</tbody>
</table>

- 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 Asset Details to navigate directly to Asset Inventory with the node's asset details displayed by default.
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.

A panel appears with information about the technique such as a **Description** and **Evidence** of the technique.
Click the Technique ID to navigate directly to the MITRE definition for that technique.

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.
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.

<table>
<thead>
<tr>
<th>Tile</th>
<th>Query Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bookmarks</td>
<td>When a user saves a custom attack path query, Attack Path Analysis</td>
</tr>
</tbody>
</table>
saves the query in the **Bookmarks** section. Here, you can view the query and the user who created it.

For more information, see [Generate an Attack Path Query with the Attack Path Query Builder](#).

| 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 | • **Bluekeep** — Computers that are vulnerable to CVE-2019-0708.
| Vulnerabilities          | • **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** — LLNMR/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.
- **Data Sources** — View all products feeding data into the Attack Path Analysis interface.
- **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*.

**Data Sources**

A data source is any product that feeds data into the Attack Path Analysis interface. By default, Attack Path Analysis automatically ingests data from any Tenable product for which you have a license. On the **Data Sources** tab, you can view details for each data source. For more information, see **Configure Data Sources for Attack Path Analysis**.

To view the **Data Sources** page:

1. **Access** the **Settings** menu.
2. Click **Data Sources**.
The **Data Sources** page appears.

On the **Data Sources** page, you can view the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Source</strong></td>
<td>The product feeding data into the Attack Path Analysis interface.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>A description of the data source.</td>
</tr>
<tr>
<td><strong>Category</strong></td>
<td>The category to which the data source belongs. For more information, see <strong>Attack Path Analysis Metrics</strong>.</td>
</tr>
</tbody>
</table>

### 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.

### Configure Data Sources for Attack Path Analysis

A data source is any product that feeds data into the Attack Path Analysis interface. By default, Attack Path Analysis automatically ingests data from any Tenable product for which you have a license.
You can configure the following Tenable products as data sources for Attack Path Analysis:

- **Tenable Vulnerability Management**
- **Tenable Identity Exposure**

To configure Tenable Vulnerability Management data sources:

1. Access the [Workspace](#).
2. Navigate to Tenable Vulnerability Management.
3. In the left navigation bar, select [Scans](#).
   The [Scans](#) page appears.
4. Click [Create Scan](#).
   The [Select a Scan Template](#) page appears.
5. Select the [Active Directory Identity](#) scan template.
   The [Create a Scan](#) page appears with the Active Directory information.
6. Make sure that you provide the targets and credentials for the scans.
7. Click [Save & Launch](#).
   Tenable Vulnerability Management redirects you to the [Scans](#) page.
8. Click [Create Scan](#).
   The [Create a Scan Template](#) page appears.
9. Click [Basic Network Scan](#).
   The [Create a Scan for Basic Network Scan](#) page appears.
10. Make sure that you provide the targets you want to scan, administrator credentials to allow authenticated scan and the list of [plugins](#) that Attack Path Analysis requires.
11. Click [Save & Launch](#).
   Tenable Vulnerability Management now provides the scan data to Attack Path Analysis.

To configure Tenable Identity Exposure data sources:
• Deploy Tenable Identity Exposure. For more information, see the *Tenable Identity Exposure Administrator Guide*.

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
Tenable Web App Scanning Plugins:

- 98113
- 98114
- 98115
- 98116
- 98117
- 98118
- 98119
- 98120
- 98121
- 98122
- 98123
- 98124
- 98127
- 98623
- 112614
- 112684
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.
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.

**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*.