Tenable One Exposure Management Platform Deployment Guide

Quick Reference Guide

Last Revised: April 01, 2024

Table of Contents

Welcome to the Tenable One Exposure Management Platform Deployment Guide

Tenable One is an exposure management platform that helps organizations to gain visibility across the modern attack surface, focus efforts to prevent likely attacks, and accurately communicate exposure risk to support optimal business performance.

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.

Before you begin, review the following customer education materials:

- Tenable One Introduction (Tenable University)

In this document, you'll be guided step-by-step how to:

- Guide you through deploying each product within your Tenable One package.
- Navigate any caveats or limitations between these products.
- Get the most out of your data in the Lumin Exposure View, Asset Inventory, and Attack Path Analysis products.

> **Important:** At the bottom of each page, look for the **What to do Next** steps. Here, you can see which application you should install next based on which Tenable One licensing package you purchased.

The Tenable One package includes the following products:

Product	Tenable One Package

Tenable Vulnerability Management	Tenable One Standard, Tenable One Enterprise
Tenable Web App Scanning	Tenable One Standard, Tenable One Enterprise
Tenable Cloud Security	Tenable One Standard, Tenable One Enterprise
Tenable Identity Exposure	Tenable One Standard, Tenable One Enterprise
Lumin Exposure View	Tenable One Standard, Tenable One Enterprise
Asset Inventory	Tenable One Standard, Tenable One Enterprise
Tenable Attack Surface Management	Tenable One Enterprise
Attack Path Analysis	Tenable One Enterprise

Tenable One Product Architecture

When configuring Tenable One, you must first deploy the "**Point Products**":

- Tenable Vulnerability Management
- Tenable Security Center
- Tenable Web App Scanning
- Tenable Cloud Security
- Tenable Identity Exposure
- Tenable Attack Surface Management (Enterprise Only)

Once you deploy these products, Tenable integrates your data into the Tenable database. From there, the following interfaces pull the data, where you can then interact with and assess the data:

- Lumin Exposure View
- Asset Inventory
- Attack Path Analysis (Enterprise Only)

Things to Consider Before Deploying Tenable One Products

Users and Settings

Most product settings, including user creation, live within the Tenable Vulnerability Management User Interface. This means that managing user roles and permissions for all Tenable One products can be managed directly via the Tenable Vulnerability Management > **Settings** > **Access Control** workflow. For more information, see Access Control in the *Tenable Vulnerability Management User Guide*.

> **Tip:** Looking for information on how to add additional contacts to your Tenable Community portal account? Check out the Tenable Community Guide for Account, Contact, and Product Management.

Tags

- Tags within Tenable Vulnerability Management can include assets from Tenable Vulnerability Management, Tenable Web App Scanning, and Tenable Cloud Security (NOT Tenable Identity Exposure) and sync these assets within Tenable One.
- Tags within Tenable One can include data types from Tenable Vulnerability Management, Tenable Web App Scanning, Tenable Identity Exposure, and Tenable Cloud Security. This means you can break down an application that includes one or more assets from any or all of these data sources. This does not, however, mean that you can bring Tenable Identity Exposure tag data back into Tenable Vulnerability Management.
- The way you tag your data is how you ultimately visualize that data on your Exposure Cards within the Lumin Exposure View. Exposure Cards can include one or more tags. Therefore, the tags you create dictate the custom exposure cards you can create within the Lumin Exposure View.

Tenable One Standard vs. Tenable One Enterprise

Tenable One Enterprise customers must prioritize the deployment of certain products differently than those customers deploying Tenable One Standard. Where applicable, look for a note indicating where deployment prioritization differs for Tenable One Enterprise customers.

Frequently Asked Questions

Q: *Does my organization have SLAs for Tenable Vulnerability Management, Tenable Web App Scanning, Tenable Cloud Security, and/or Tenable Identity Exposure vulnerabilites/misconfigurations?*

A: You can set SLAs to best align with your organization's policy when configuring the Lumin Exposure View. For more information, see Configure the Exposure View in the *Lumin Exposure View User Guide*.

Q: *Does my organization understand RBVM/Exposure Management?*

A: At an executive level, reporting within the Lumin Exposure View is different from reporting within the "point products" (i.e., Tenable Vulnerability Management, Tenable Cloud Security). Tenable recommends that you educate leaders in your organization on how these changes can improve your organization's efforts.

> **Tip**: When you recast a finding within the Tenable Vulnerability Management interface, Tenable One updates your Cyber Exposure Score (CES) accordingly.

What to do next

Begin by Provisioning Licenses for your Tenable One Products.

Provisioning Licenses for your Tenable One Products

Before you Begin

Review the Tenable One Licensing *Quick-Reference Guide* to understand how Tenable One assets are licensed.

To provision licenses for your Tenable One products:

Log into http://provisioning.tenable.com to provision Tenable One and its product suite. For a demonstration on using the provisioning portal, see the Provisioning Portal Demo Video.

Once the Tenable One instance has been provisioned, the activation code for each individual product can be found under the **My Products** tab at the top of the Tenable Community toolbar. You must be logged into Tenable Community and have product access to view the products and activation codes.

> **Note:** If Tenable One is your only product suite and it is not provisioned, the **My Products** tab is not visible until provisioning is complete.

If you cannot see the **My Products** tab and believe this is in error, contact the Primary Contact (found in the **My Contacts** tab) on your account. Request access to view or manage permissions for one or all of the products on the account.

If you are the Primary Contact and need help or are no longer able to access your account, contact your Customer Success manager.

What to do next

Deploy Tenable Vulnerability Management.

Tenable Vulnerability Management

The first step when deploying Tenable One is to install and configure Tenable Vulnerability Management.

Deploy Tenable Vulnerability Management

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

Configure Tenable Vulnerability Management for Use in Tenable One

Once you have installed Tenable Vulnerability Management, consider the following best practices for configuring the product for use:

Tags

- Tags you create in Tenable Vulnerability Management are crucial in the Lumin Exposure View. These tags help you visualize your assets within the Lumin Exposure View. For example, you can separate your tags by tier, business unit, physical location, etc.
- Keep in mind: how you tag your assets in Tenable Vulnerability Management dictates how that asset data appears in Tenable One. In Lumin Exposure View, you can create custom exposure cards to assess the exposure of those assets.
- Any tags you create in Tenable Vulnerability Management automatically sync in Tenable One. You can view them in Asset Inventory.

  > **Tip:** You can also create tags directly in Tenable One.

- When you bring more data (for example, from Tenable Web App Scanning and Tenable Cloud Security) into Tenable One, you can tag assets from multiple data sources within a single tag.

Scanning

- (Tenable One Enterprise Only) When considering how data makes its way from Tenable Vulnerability Management into Attack Path Analysis, remember: the more (authenticated) data, the better! When you configure remote Tenable Vulnerability Management scans, be sure to enable the **Override Normal Verbosity** report setting. This ensures the Attack Path Analysis has the most data possible to work with when generating attack paths for your environment.

- The more you scan, the more often your data refreshes in Tenable One. The more frequently your data refreshes, the more relevant the data being presented. If you only scan once a month, be aware that by the end of the month, your data will likely be out of date.
- Review the Asset Criticality Rating of your most critical assets. Most organizations know about their critical assets (ACR = 10). From there, work backwards to identify the next most important assets and validate/adjust their ACR as necessary.

> **Note:** By default, Tenable will not assign an asset an ACR above an 8. You must manually edit an asset's ACR to set it to a 9 or 10.

Onboarding Milestones

Tenable suggests you complete the following milestones to ensure your success before proceeding with your Tenable One deployment process:

- Review and customize your assets' ACR.
- In Lumin Exposure View:
  - Review the **Computing Resources** exposure card.
  - Configure the exposure view settings to set your **Remediation SLA** and **SLA Efficiency** based on your company policy.
  - Create a custom exposure card based on business context (for example, Business units, Operating Systems, Asset Criticality, Physical Location, or Application).
- In Asset Inventory, review your assets to understand the strategic nature of the interface as compared to other cloud products. This should help set your expectations on what features to use within Asset Inventory, and when.

What to do next

Deploy Tenable Security Center.

Tenable Security Center

Activate Tenable Security Center

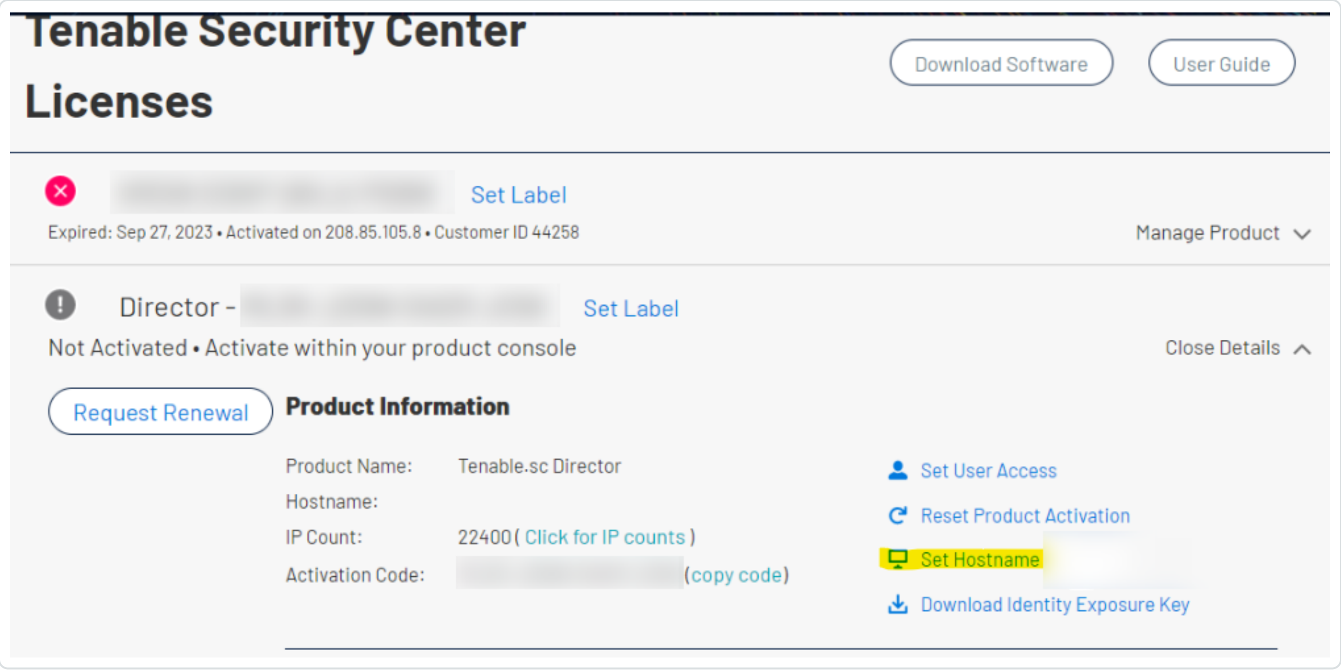
The Tenable One Standard and Enterprise packages include up to 3 Tenable Security Center console (s).

To activate Tenable Security Center for your Tenable One instance:

1. Your primary contact must first log in to the Tenable Provisioning Portal with their Tenable Community credentials and provision the desired number of Tenable Security Center console (s).

   > **Note:** The provisioning process can take up to 15 minutes.

2. Once the console(s) are provisioned, your primary contact can then access the Community Portal, where they must assign a hostname to each console.

   Tenable Security Center Licenses

   ✖ [redacted] Set Label

   Expired: Sep 27, 2023 • Activated on 208.85.105.8 • Customer ID 44258

   ! Director - [redacted] Set Label

   Not Activated • Activate within your product console

   Product Information

   Product Name: Tenable.sc Director
   Hostname:
   IP Count: 22400 (Click for IP counts)
   Activation Code: [redacted] (copy code)

   The Tenable Security Center console(s) appear in Tenable Community after each provisioned console has a hostname.

   > **Tip:** You may need to clear your cache to see the updated console(s) in Tenable Community.

3. Download the key and access the activation code for Tenable Security Center installation.

Install Tenable Security Center

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

Configure Tenable Security Center for Use in Tenable One

Once you have installed Tenable Security Center, follow the Tenable One Synchronization steps outlined in the *Tenable Security Center User Guide*.

Onboarding Milestones

Tenable suggests you complete the following milestones to ensure your success before proceeding with your Tenable One deployment process:

- Review and customize your assets' ACR.
- In Lumin Exposure View:
  - Review the **Computing Resources** exposure card.
  - Configure the exposure view settings to set your **Remediation SLA** and **SLA Efficiency** based on your company policy.
  - Create a custom exposure card based on business context (for example, Business units, Operating Systems, Asset Criticality, Physical Location, or Application).
- In Asset Inventory, review your assets to understand the strategic nature of the interface as compared to other cloud products. This should help set your expectations on what features to use within Asset Inventory, and when.

What to do next

Deploy Tenable Web App Scanning.

Tenable Web App Scanning

Deploy Tenable Web App Scanning

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

Configure Tenable Web App Scanning for Use in Tenable One

Once you have installed Tenable Web App Scanning, consider the following best practices for configuring the product for use:

Setting Goals

Once you deploy Tenable Web App Scanning, create some quick scans to provide a high-level assessment of the target to establish your baseline. Then, consider setting some goals:

- Identify what qualifies as acceptable for your organization (for example, no critical scan results? All web apps be scanned monthly? All external websites are "clean"?)
- Note that your goals may shift once you interact with this data within the rest of Tenable One as further reporting is likely to outweigh pure numbers.

Known Limitations

Be aware of the following limitations when using Tenable Web App Scanning in Tenable One:

- Vulnerability Priority Rating (VPR) is not exposed in Tenable Web App Scanning.
- Asset Criticality Rating (ACR) is **NOT** exposed or customizable in Tenable Web App Scanning.

  > **Note:** ACR does appear in Asset Inventory, but is not currently customizable in that interface.

- Tenable Web App Scanning data is not currently certified within Attack Path Analysis.

Onboarding Milestones

Tenable suggests you complete the following milestones to ensure your success before proceeding with your Tenable One deployment process:

- In Lumin Exposure View:
  - Review the **Web Applications** exposure card.
  - Configure the exposure view settings to set a customized **Card Target** and configure **Remediation SLA** and **SLA Efficiency** based on your company policy.
  - Create a custom exposure card based on business context (for example, Web App Owner, Asset Criticality, Application, Internal/External Web Servers, or Ecommerce/Supporting Asset).
- In Asset Inventory, review your assets to understand the strategic nature of the interface as compared to other cloud products. This should help set your expectations on what features to use within Asset Inventory, and when.

What to do next

Deploy Tenable Cloud Security.

Tenable Identity Exposure

Important! Tenable One only supports SaaS instances of Tenable Identity Exposure. You cannot use Tenable Identity Exposure On Premises with Tenable One.

Activate Tenable Identity Exposure

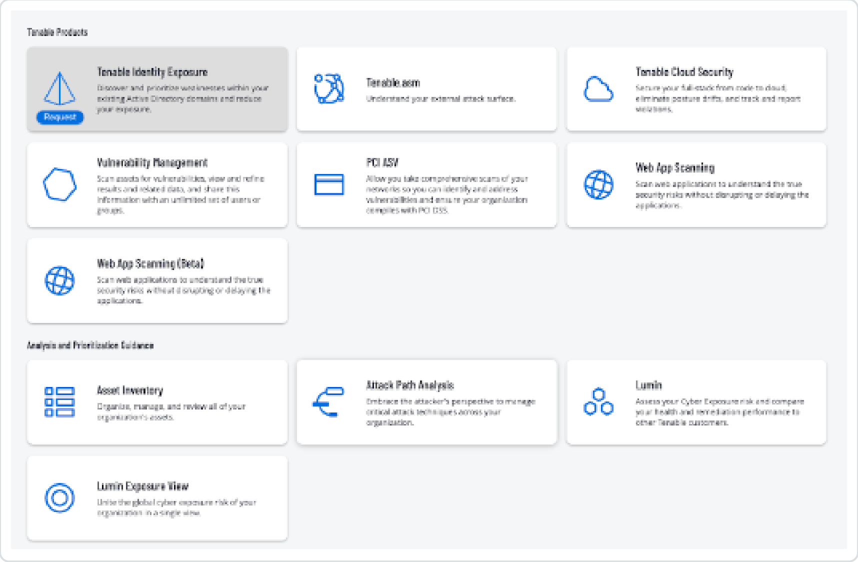
Because there is a significant cost associated with operating each instance of Tenable Identity Exposure, Tenable does not automatically activate the application for all Tenable One customers.

Important! If you have not yet purchased or are currently purchasing Tenable One, you can request access to Tenable Identity Exposure during the subscription process. Otherwise, follow the steps below to get set up.

To activate Tenable Identity Exposure for your Tenable One instance:

1. Log in to Tenable One.

   The **Workspace** page appears. The Tenable Identity Exposure tile is disabled by default.

   Tenable Products

   Tenable Identity Exposure
   Discover and prioritize weaknesses within your existing Active Directory domains and reduce your exposure.
   Request

   Tenable.asm
   Understand your external attack surface.

   Tenable Cloud Security
   Secure your full-stack from code to cloud, eliminate posture drifts, and track and report violations.

   Vulnerability Management
   Scan assets for vulnerabilities, view and refine results and related data, and share this information with an unlimited set of users or groups.

   PCI ASV
   Allow you take comprehensive scans of your networks so you can identify and address vulnerabilities and ensure your organization complies with PCI DSS.

   Web App Scanning
   Scan web applications to understand the true security risks without disrupting or delaying the applications.

   Web App Scanning (Beta)
   Scan web applications to understand the true security risks without disrupting or delaying the applications.

   Analysis and Prioritization Guidance

   Asset Inventory
   Organize, manage, and review all of your organization's assets.

   Attack Path Analysis
   Embrace the attacker's perspective to manage critical attack techniques across your organization.

   Lumin
   Assess your Cyber Exposure risk and compare your health and remediation performance to other Tenable customers.

   Lumin Exposure View
   Unite the global cyber exposure risk of your organization in a single view.

2. In the Tenable Identity Exposure tile, click **Request**.

3. Be prepared to provide the estimated number of users in your active directory. If Tenable discovers more assets are required than are available in your Tenable One license, a Tenable representative will reach out directly to discuss license expansion.

This is necessary to ensure that your Tenable One subscription has available assets to apply to assess your organization's active directory. To get an accurate estimate of unique enabled identities, Tenable recommends to running the following PowerShell Command script(s) on your domain controllers:

- AD On-premise Only (Once Per Domain)

  a. In the Active Directory Powershell module, run the following command:

  ```
  (Get-ADuser -ResultSetSize $null -Filter 'enabled -eq
  $true').count
  ```

- Microsoft Entra ID

  a. To install Microsoft Graph, in the Active Directory Powershell module, run the following command:

  ```
  Install-Module Microsoft.Graph -Scope CurrentUser
  ```

  b. Then, to get a count of all Azure AD Identity Users, run the following commands:

  ```
  Connect-MgGraph -Scopes "User.Read.All"
  ```

  ```
  (Get-MgUser -All -Filter "accountEnabled eq true").Count
  ```

  This provides a list of all Microsoft Entra ID users.

  c. Then, to get a count of all Cloud Only Azure AD identities, run the following command:

  ```
  (Get-MgUser -All -Filter "accountEnabled eq true" -Property
  onPremisesSyncEnabled | where { $_.onPremisesSyncEnabled -ne
  $true }).Count
  ```

> **Note:** This excludes any synchronized identities from your on-premises Active Directory "Hybrid Identities".

Once the request is complete, Tenable recommends expecting 2-3 day turnaround time to enable Tenable Identity Exposure access.

Deploy and configure Tenable Identity Exposure in the Cloud

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

Configure Tenable Identity Exposure for Use in Tenable One

- Download and configure the license file:

  1. Navigate to Tenable Community to download the license file required to use Tenable Identity Exposure with Tenable One.

     > **Tip:** If you cannot locate the license file, contact your Tenable Representative.

  2. In Tenable Identity Exposure, navigate to **System** > **About** > **Edit License File**.

  3. Upload the license file required to use Tenable Identity Exposure with Tenable One.

- Download and install the Secure Relay:

  1. On the Tenable Identity Exposure Downloads site, download the Secure Relay for your Tenable Identity Exposure instance.

  2. Install the Secure Relay on your local network by following the steps outlined in the *Tenable Identity Exposure User Guide*.

  3. Navigate to **Settings** > **Relay Management** to view and manage the Secure Relay.

- Configure Forests:

  1. In Tenable Identity Exposure, navigate to **Settings** > **Forest Management** > **Add Forest**.

  2. On the **Add Forest** page, type the **Login** and **Password** associated with the connected service account.

  3. Click **Add**.

Onboarding Milestones

Tenable suggests you complete the following milestones to ensure your success before proceeding with your Tenable One deployment process:

- In Lumin Exposure View:
    - Review the **Active Directory** exposure card.
    - Configure the exposure view settings to set a customized **Card Target** and configure **Remediation SLA** and **SLA Efficiency** based on your company policy.
    - Create a custom exposure card based on business context (for example, Domains, Domain Admins, Asset Criticality, Critical Users/Critical Assets, or Service Accounts).
- In Asset Inventory, review your assets to understand the strategic nature of the interface as compared to other cloud products. This helps set your expectations on what features to use within Asset Inventory, and when.
- (Tenable One Enterprise Only) Once your Identity scan completes:
    - Review the findings within Attack Path Analysis.
    - Select a critical asset and generate a Blast Radius or Asset Exposure Graph query.
    - Ensure you understand how assets from Tenable Vulnerability Management and Tenable Identity Exposure can create a path into and through your environment that may have previously been hidden.

What to do next

- (Tenable One Standard Only) Review how to best Realize the Value of Your Data.
- (Tenable One Enterprise Only) Deploy Tenable Attack Surface Management (Tenable One Enterprise Only).

Tenable Cloud Security

Deploy Tenable Cloud Security

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

> **Note**: You must have Tenable Cloud Security login credentials to access the *Tenable Cloud Security User Guide*.

Configure Tenable Cloud Security for Use in Tenable One

There are no specific steps to take in order to configure Tenable Cloud Security for use with Tenable One outside of the normal Tenable Cloud Security configuration steps. For more information, see the *Tenable Cloud Security User Guide*.

What to do next

Deploy Tenable Identity Exposure.

Tenable OT Security

Deploy and License Tenable OT Security

To deploy Tenable OT Security:

> **Note**: You must install, at minimum, version 3.18.

1. Install the Tenable OT Security appliance according to the steps outlined in the *Tenable OT Security User Guide*.
2. (Optional) If you want to pair your sensors with the Industrial Core Platform (ICP), install the OT Security Sensor according to the steps outlined in the *Tenable OT Security User Guide*.

To license Tenable OT Security:

Follow the OT Security License Workflow outlined in the *Tenable OT Security User Guide*.

Link Tenable OT Security to Tenable One

Once you have downloaded and licensed Tenable OT Security, you can link the application to Tenable One.

1. Generate a Tenable OT Security **Linking Key** and determine your **Cloud Site** according to the steps outlined in the *Tenable Vulnerability Management User Guide*. Copy and save this information to link the connector to Tenable One.
2. Integrate your Tenable OT Security appliance with Tenable One according to the steps outlined in the *Tenable OT Security User Guide*.

You can expect to see your Tenable OT Security data in Tenable One within the following timeframes:

- It can take up to 2 hours to see your OT data in Asset Inventory.
- It can take up to 4 hours to see your OT data in Lumin Exposure View.

Once the initial sync completes, Tenable OT Security automatically syncs OT data with Tenable One every hour.

Onboarding Milestones

Tenable suggests you complete the following milestones to ensure your success before proceeding with your Tenable One deployment process:

- In Asset Inventory:
    - Review your OT assets to understand the strategic nature of the interface as compared to other cloud products. This should help set your expectations on what features to use within Asset Inventory, and when.
    - Create a new dynamic tag for your OT assets, where:
        - Operator = **Host System Type**
        - Value = **PLC**
- In Lumin Exposure View:
    - Review the **Operational Technology** exposure card.
    - Configure the exposure view settings to seta customized card target, and to configure your **Remediation SLA** and **SLA Efficiency** based on your company policy.
    - Create a custom exposure card based on business context, and include the new tag you created in Asset Inventory.

Tenable Attack Surface Management (Tenable One Enterprise Only)

Tenable Attack Surface Management is part of the Tenable One Enterprise package. If you are a Tenable One Standard customer, you can skip this topic.

Deploy Tenable Attack Surface Management

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

Configure Tenable Attack Surface Management for Use in Tenable One Enterprise

Once you have installed Tenable Attack Surface Management, consider the following best practices for configuring the product for use:

- Configure Tenable Attack Surface Management with as many domains as possible, even if all domains are not relevant to your organization. Let this “run” for a week or so, ingesting and scraping the internet with more suggested domains while you continue your Tenable One deployment process.
- Once Tenable Attack Surface Management has "run" for a period of time, configure your data sets and confirm the entirety of your attack surface is present.

What to do next

Review how to best Realize the Value of Your Data.

Realize the Value of Your Data

Once you deploy and configure all of the Tenable One point products, you can use the Asset Inventory, Lumin Exposure View, and Attack Path Analysis to pull in data from these point products and get the most value out of that data.

Asset Inventory

To get the most out of your data within Asset Inventory:

- Join existing tags into new platform tags that reflect the aggregation of data types (for example, PCI scope assets can include Hosts, Web Applications, and Computing Resources).

For more information, see the *Asset Inventory User Guide*.

Lumin Exposure View

Here are some things you can do in Lumin Exposure View that can get you up and running with your newly imported data:

- Configure the general settings for Lumin Exposure View and its exposure cards:
  - Set your **Sparkline Timespan**
  - Set your default **Benchmark Industry**
  - Set your **Card Targets** and **Category Targets**
  - Set your default trend period
  - De-select the **Overall SLA** and **Low SLA** options
  - Adjust **Graph Range** SLA setting to see how it changes your scores
- Use the relevant tags that have been created in Asset Inventory to create new custom exposure cards:
  - For example, after consideration, you may find that you want to include 20 tags within custom exposure cards.
- Consider using custom SLAs for each tag within the exposure cards. This means each environment can be under different regulations requiring varying SLAs.

For more information, see the *Lumin Exposure View User Guide*.

Attack Path Analysis (Tenable One Enterprise Only)

To get the most out of your data within Attack Path Analysis:

- Gain insight from the Attack Path Analysis Dashboard:
  - Compare your data over time. How many critical assets are in your environment, and how many attack paths lead to these assets?
- Review your **Findings** within the Attack Path Analysis:
  - Are there any paths that are particularly troublesome in your environment?
- Interact with the Mitre Att&ck Heatmap to view a holistic view of your data based on the enterprise tactics and techniques from Mitre Att&ck.
- Discover potential threats by generating Attack Path queries:
  - Create **Blast Radius** queries based on assets of interest — Are there assets that have a high AES that could be mitigated and ultimately resolve more than one attack path?
  - Create **Asset Exposure Graph** queries for critical assets — What paths exist to critical assets?

For more information, see the *Attack Path Analysis User Guide*.

Additional Resources for Tenable One Deployment

The following resources can be useful as you deploy Tenable One and its product suite:

Tenable One Webinars

- Customer Update Session 1 (of 4)
- Customer Update Session 2 (of 4)
- Customer Update Session 3 (of 4)
- Customer Update Session 4 Coming Soon!
- Attack Path Analysis with AI

Supporting Documentation

- Tenable One Scoring Explained Quick Reference Guide