Licensing Tenable Products

Last Revised: August 20, 2025

Table of Contents

Licensing Tenable Products

This guide explains how to license Tenable products, which components are purchased separately, and what happens during license overages or expirations. To get the best experience, use it in collaboration with your Tenable representative, who can guide you on how Tenable customizes each license for your organization.

Note: This guide does not cover Tenable Cloud Security. For more information on licensing that product, contact your Tenable representative.

Tenable Licensing Overview

For all Tenable products except Tenable Nessus, which is subscription-based, you purchase licenses for *assets* in your environment: resources identified by—or managed in—your Tenable products.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

Tip: On the Tenable platform, assets are any data, device, or environmental component that supports information-related activities and needs to be protected from threats. Assets can be desktop computers, web servers, cloud resources, name servers, IoT devices, network printers, enabled users, or other items—and have elements such as hostnames, web application names, IP addresses, or DNS records. Assets are defined differently in each Tenable product.

Tenable Products

The following table lists Tenable's products and summarizes their licensing methods.

Product	Licensing Method
Tenable One	Purchase licenses and allocate them to your Tenable One products based on the asset types you want to scan or manage.
Tenable Vulnerability Management	Purchase licenses for assessed assets from the past 90 days and imported assets with vulnerabilities.

Tenable Web App Scanning	Purchase licenses for unique fully qualified domain names (FQDNs) assessed in the past 90 days. If you only scan IP addresses, the system licenses those instead.
Tenable Cloud Security	Purchase licenses for billable cloud resources. For more information, contact your Tenable representative.
Tenable Enclave Security	Purchase licenses for assessed container images in your environment.
Tenable Security Center	Purchase licenses for assessed hosts from Tenable Security Center or imported from other Tenable products.
Tenable Identity Exposure	Purchase licenses for enabled users in your directory services.
Tenable Attack Surface Management	Purchase licenses for observable objects, which include domain names, subdomains, or IP addresses for internet-connected or internal network devices.
Tenable OT Security	Purchase licenses for detected devices with IP addresses, one license for each IP address.
Tenable Nessus	Purchase a subscription to Tenable Nessus Expert or Tenable Nessus Professional.

What to Do Next

If you have already purchased your Tenable products, do one of the following:

- (Cloud products only) On the Tenable **License Information** page, check your license usage.
- In the Tenable documentation, learn more about each product.

Tenable One Licensing

This topic breaks down the Tenable One licensing process and lists the versions and components you can purchase. It also holds a license calculator with which you can estimate your license needs.

To learn how to use Tenable One, see Tenable One Platform.

Licensing Tenable One

To use Tenable One, you purchase licenses for *assets*: resources identified by—or managed in—your Tenable products. Some Tenable One products use different asset types. For example, in Tenable Web App Scanning, assets are unique fully qualified domain names (FQDNs), while in Tenable Identity Exposure, they are enabled users in your directory service. Once you have purchased licenses, your Tenable representative assigns them to your products based on the asset types you want to scan or manage.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

You can *reallocate* your licenses once per 90 days. For example, if you purchase 1,000 licenses and assign 500 each to Tenable Vulnerability Management and Tenable Security Center, you can switch 100 licenses to Tenable Vulnerability Management if your scan profile requires it. To reallocate licenses, contact your Tenable representative.

Tip: To view your current license count and available assets, in the Tenable top navigation bar, click ⚙ and then click **License Information**. To learn more, see License Information Page.

Note: Tenable offers simplified pricing to managed security service providers (MSSPs). To learn more, contact your Tenable representative.

Tenable One Components

You can customize Tenable One for your use case by adding components. Some components are add-ons that you purchase.

Tip: The latest version of the platform is called **Tenable One**, but there were previously two versions: *Enterprise* and *Standard*. The following table lists all versions, but if you are a new customer, you will purchase **Tenable One**. If you have a Tenable One Standard or Enterprise quote, Tenable will honor it through the end of 2024. If you are a current customer, you can upgrade, downgrade, or renew as follows:

- **Current Tenable One Standard customers** — You can upgrade, downgrade, or renew the same version through the end of 2025.

- **Current Tenable One Enterprise customers** — You can upgrade, downgrade or renew the same version for the foreseeable future.

Version	Version Type	Included with Purchase	Add-on Component
Tenable One	Current version	• Tenable Security Center+ companion license. • OT Security companion license. • Tenable Web App Scanning on-premises companion license.	• If using Tenable Security Center, purchase additional consoles when you need more than three. • Tenable Web App Scanning additional concurrency with Tenable cloud scanners. • Tenable Identity Exposure On-Premises. • Third-party Connectors.
Tenable One Standard	Legacy version	• Tenable Security Center+ companion license. • OT Security companion license. • Tenable Web App Scanning on-premises companion license.	• Tenable Web App Scanning additional concurrency with Tenable cloud scanners. • Tenable Identity Exposure On-Premises.
Tenable One Enterprise	Legacy version	• Tenable Security Center+	• If using Tenable Security Center, purchase additional

		companion license. • OT Security companion license. • Tenable Web App Scanning on-premises companion license.	consoles when you need more than three. • Tenable Web App Scanning additional concurrency with Tenable cloud scanners. • Tenable Attack Surface Management Daily Frequency. • Tenable Identity Exposure On-Premises.

Tenable One Asset Values

Tenable One has a centralized platform approach, collecting data from many asset types and providing domain-specific security teams (for example, Tenable Vulnerability Management, Tenable Cloud Security) with specialized domain-specific applications. These applications are similar to point products for managing cloud, web applications, OT assets, and so on, enhanced with context from the Tenable One platform.

The value customers derive from Tenable One varies by the type of resource being managed, as does the cost incurred by Tenable. To align Tenable One pricing to value, we convert the number of different resource types (for example, web servers, cloud resources, OT devices) to a number of Tenable One assets based on ratios defined in the following table. In this way we maintain a single price per Tenable One asset no matter the variety of resources being managed.

The following table defines the Tenable One asset types in each product and compares them to their Tenable One *asset value*, which is the number of licenses you purchase from Tenable.

> **Note**: Tenable Lumin, Lumin Exposure View, Tenable Inventory, and Attack Path Analysis do not require licenses.

Product	Definition	Tenable One Asset Value
Tenable	Assets are scanned targets from the past 90 days,	1 of your assets

Vulnerability Management	discovery excluded, or imported assets with vulnerabilities. Examples include hosts, IP addresses, or other targets.	equals 1 Tenable One asset.
Tenable Security Center+		1 IP address in your environment equals 1 Tenable One asset.
Tenable Web App Scanning	Assets are fully qualified domain names (FQDNs) assessed in the past 90 days. If you only scan IP addresses, those are used instead.	1 FQDN or IP address in your environment equals 1 Tenable One asset.
Tenable Identity Exposure	Assets are human or machine identities in your identity service, for example: users, devices, applications, or systems.	1 identity asset in your environment equals 0.50 Tenable One assets.
Tenable Cloud Security CIEM	In Tenable Cloud Security, the assets you license are called *billable assets*. Billable assets are based on public cloud compute instances, public cloud container hosts or orchestrators, serverless assets, container repositories or on-premise container hosts.	1 Tenable Cloud Security CIEM billable asset equals 3 Tenable One assets.
Tenable Cloud Security Standard		1 Tenable Cloud Security Standard billable asset equals 5 Tenable One assets.

Tenable Cloud Security Enterprise		1 Tenable Cloud Security Enterprise billable asset equals 7.50 Tenable One assets.
Tenable OT Security	Assets are detected devices with IP addresses, a single license for each IP address.	1 detected device in your environment equals 1.50 Tenable One assets.
Tenable Attack Surface Management Fortnightly Frequency	Assets are observable objects, which are domain names, subdomains, or IP addresses for internet-connected or internal network devices.	1 observable object in your environment equals 0.25 Tenable One assets.
Tenable Attack Surface Management Daily Frequency		1 observable object in your environment equals 0.50 Tenable One assets.
Third-Party Application Assets	Third-party assets are defined as hosts, code projects, images, websites, or cloud resources ingested from a non-Tenable source.	1 third-party asset in your environment equals 0.50 Tenable One assets.

Tenable One Calculator

Use this calculator to estimate your license needs. In the **Licenses** column, enter your assets. The number of Tenable licenses to purchase appears in the **Assets** column. You must buy at least 300 licenses at a time.

Tip: *Licenses* is the number of assets in your environment that you want to manage in Tenable One. *Assets* is the number of Tenable One assets that you need to purchase.

Warning: This calculator provides an *estimate* and cannot be used for a sales quote. To get a sales quote, contact your Tenable representative.

Product	Type	Licenses	Ratio	Assets
Cloud Products				
Tenable Vulnerability Management	Assets		1.00	0
Tenable Web App Scanning	FQDNs		1.00	0
CIEM	Cloud resource workloads		3.00	0
Tenable Cloud Security Standard	Cloud resource workloads		5.00	0
Tenable Cloud Security Enterprise	Cloud resource workloads		7.50	0
Tenable Identity Exposure	Identities		0.50	0
Tenable Attack Surface	Observable objects		0.25	0

Management Fortnightly Frequency				
Tenable Attack Surface Management Daily Frequency	Observable objects		0.50	0
On-premise Products				
Tenable OT Security	Assets		1.50	0
Tenable Web App Scanning	FQDNs		1.00	0
Tenable Security Center+	IP addresses		1.00	0
Tenable Identity Exposure	In the context of Tenable One, **On-premise** versions of Tenable Identity Exposure are considered add-ons and do not follow a ratio-based model. They are priced the same as their ratio-based counterparts but tracked separately with their own counters. These values are **not included** in the Tenable One count and will **not affect** the calculator totals.			
Third-Party Applications				
Third-Party Application Assets	Assets		0.5	0
Totals				
Total Tenable One Cloud Assets		0		

Total Tenable One On-premise Assets		0		
Total Third-Party Application Assets		0		
Total Tenable One Assets		0		

Reclaiming Licenses

When you purchase Tenable licenses, your total license count is static for the length of your contract unless you purchase more licenses. However, Tenable One products reclaim licenses under some conditions—and then reassign them to new assets in the same product so that you do not run out of licenses.

The following table explains how each Tenable One product reclaims licenses.

Product	License Reclamation Process
Tenable Vulnerability Management	Licenses from deleted assets are reclaimed within 24 hours. Licenses for assets on a network with Asset Age Out enabled are reclaimed after not being scanned for a length of time you specify. Licenses for all other assets are reclaimed after not being scanned for 90 days.
Tenable Web App Scanning	Licenses from deleted assets are reclaimed within 24 hours. Licenses for assets that age out are reclaimed after a length of time you specify, or after 90 days.
Tenable Security Center	Licenses are reclaimed when you delete a repository, run a license report, or upload a new license. If you set assets to age out, licenses are reclaimed during nightly cleanup. If you configure your scan settings to remove unresponsive hosts, licenses are reclaimed at scan import. For more information, see License Count in the *Tenable Security Center Best Practices Guide*.

Tenable Identity Exposure	Licenses for enabled users you delete are reclaimed in real time when removed from your environment's directory service.
Tenable OT Security	Licenses for hidden assets are reclaimed in real time, as are licenses for assets that have been offline for more than 30 days. Licenses for assets you remove or hide in the user interface are also reclaimed.
Tenable Attack Surface Management	Licenses are reclaimed when individual assets are archived—or when asset sources are removed or age out. Your license count is updated daily.

Exceeding the License Limit

To allow for usage spikes due to hardware refreshes, sudden environment growth, or unanticipated threats, Tenable One licenses are elastic. However, when you scan more assets than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages.

Scenario	Result
You scan more assets than are licensed for three consecutive days.	A message appears in Tenable One.
You scan more assets than are licensed for 15+ days.	A message and warning about reduced functionality appears in Tenable One.
You scan more assets than are licensed for 30+ days.	A message appears in Tenable One; scan and export features are disabled.

Tip: Improper scan hygiene or product misconfigurations can cause scan overages, which result in inflated asset counts. To learn more, see Scan Best Practices.

Expired Licenses

The Tenable One licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, you can no longer sign in to the Tenable platform.

Tenable Vulnerability Management Licensing

This topic breaks down the licensing process for Tenable Vulnerability Management as a standalone product. It also explains how assets are counted, lists add-on components you can purchase, explains how licenses are reclaimed, and notes plugins whose output is excluded from your license count. To learn how to use Tenable Vulnerability Management, see the Tenable Vulnerability Management User Guide.

Licensing Tenable Vulnerability Management

To use Tenable Vulnerability Management, you purchase licenses based on your organizational needs and environmental details. Tenable Vulnerability Management then assigns those licenses to your *assets*: assessed resources from the past 90 days, either identified on scans or imported with vulnerabilities (for example, servers, storage devices, network devices, virtual machines, or containers).

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

Tip: To view your current license count and available assets, in the Tenable top navigation bar, click  and then click **License Information**. To learn more, see License Information Page.

Note: Tenable offers simplified pricing to managed security service providers (MSSPs). To learn more, contact your Tenable representative.

How Assets Are Counted

When Tenable Vulnerability Management scans an asset, it compares it to previously discovered assets. In general, if the new asset does not match a previously discovered asset and has been assessed for vulnerabilities, it counts towards your license.

Tenable Vulnerability Management uses a complex algorithm to identify new assets without creating duplicates. The algorithm looks at the asset's BIOS UUID, MAC address, NetBIOS name, fully qualified domain name (FQDN), and more. Authenticated scanners or agents also assign a Tenable UUID to each asset to mark it as unique. For more information, see the Tenable Vulnerability Management FAQ.

The following table describes when assets count towards your license.

Counted Towards Your License	Not Counted Towards Your License
• An asset identified by an active scan. • An asset identified by an agent scan. • An asset import containing vulnerabilities (for example, a scan result from Tenable Nessus Professional). • Host and Tenable Web App Scanning asset types, if the last licensed scan was within the past 90 days. • An asset identified by a scan with plugin debugging enabled. To prevent such assets from counting against your license, delete them.	• A scan configured with the Host Discovery template or configured to use only the discovery plugins. • An asset import containing no vulnerabilities (for example, ServiceNow data). • A linked instance of Tenable Network Monitor running in discovery mode. • A discovery-only connector, until and unless the asset is scanned for vulnerabilities Scanned Mobile Device Management assets. • Some plugin output, as described in Excluded Plugin Output.

Tenable Vulnerability Management Components

You can customize Tenable Vulnerability Management for your use case by adding components. Some components are add-ons that you purchase.

Included with Purchase	Add-on Component
• Unlimited Tenable Nessus scanners. • Unlimited Tenable Agents. • Unlimited Tenable Network Monitors with vulnerability detection. • Access to the Tenable Vulnerability Management API.	• Tenable PCI ASV. • Tenable Attack Surface Management.

Reclaiming Licenses

When you purchase licenses, your total license count is static for the length of your contract unless you purchase more licenses. However, Tenable Vulnerability Management reclaims licenses under some conditions—and then reassigns them to new assets so that you do not run out of licenses.

The following table explains how Tenable Vulnerability Management reclaims licenses.

Asset Type	License Reclamation Process
Deleted assets	Tenable Vulnerability Management removes deleted assets from the **Assets** workbench and reclaims their licenses within 24 hours.
Aged out assets	In **Settings** > **Sensors** > **Networks**, if you enable **Asset Age Out**, Tenable Vulnerability Management reclaims assets after they have not been scanned for a period you specify.
Assets from connectors	Tenable Vulnerability Management reclaims assets from connectors the day after they are terminated. You can observe this event in each connector.
All other assets	Tenable Vulnerability Management reclaims all other assets—such as those imported from other products or assets with no age-out setting—after they have not been scanned for 90 days.

Exceeding the License Limit

To allow for usage spikes due to hardware refreshes, sudden environment growth, or unanticipated threats, Tenable licenses are elastic. However, when you scan more assets than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages.

Scenario	Result
You scan more assets than are licensed for three consecutive days.	A message appears in Tenable Vulnerability Management.
You scan more assets than are licensed for 15+ days.	A message and warning about reduced functionality appears in Tenable Vulnerability Management.
You scan more assets than are licensed for 30+ days.	A message appears in Tenable Vulnerability Management; scan and export features are disabled.

Tip: Improper scan hygiene or product misconfigurations can cause scan overages, which result in inflated asset counts. To learn more, see Scan Best Practices.

Expired Licenses

The Tenable Vulnerability Management licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, you can no longer sign in to the Tenable platform.

Excluded Plugin Output

The plugins listed in this section do not count towards your license limit.

Note: Plugin IDs are static, but Tenable products may sometimes update plugin names. For the latest information on plugins, see Tenable Plugins.

Tenable Nessus Plugins in Discovery Settings

Configure the following Tenable Nessus plugins in Discovery Settings. These plugins do not count towards your license.

Tenable Nessus Plugin ID	Plugin Name
10180	Ping the remote host
10335	Nessus TCP scanner
11219	Nessus SYN scanner
14274	Nessus SNMP Scanner
14272	Netstat Portscanner (SSH)
34220	Netstat Portscanner (WMI)
34277	Nessus UDP Scanner

Tenable Nessus Plugins on the Plugins Page

Configure the following Tenable Nessus plugins on the **Plugins** page. These plugins do not count towards your license.

Tenable Nessus Plugin ID	Plugin Name
45590	Common Platform Enumeration (CPE)
54615	Device Type
12053	Host Fully Qualified Domain Name (FQDN)
11936	OS Identification
10287	Traceroute Information
22964	Service Detection
11933	Do not scan printers
87413	Host Tagging
19506	Nessus Scan Information
33812	Port scanners settings
33813	Port scanner dependency
209654	OS Fingerprints Detected
204872	Integration Status

Tenable Network Monitor Plugins

The following Tenable Network Monitor plugins do not count towards your license.

Tenable Network Monitor Plugin ID	Plugin Name
0	Open Ports
12	Host TTL discovered
18	Generic Protocol Detection
19	VLAN ID Detection

20	Generic IPv6 Tunnel Traffic Detection
113	VXLAN ID Detection
132	Host Attribute Enumeration

Tenable Web App Scanning Licensing

This topic breaks down the licensing process for Tenable Web App Scanning as a standalone product. It also explains how assets are counted, lists add-on components you can purchase, and describes what happens during license overages or expirations. To learn how to use Tenable Web App Scanning, see the Tenable Web App Scanning User Guide.

Licensing Tenable Web App Scanning

Tenable Web App Scanning has two versions: a cloud version and an on-premises version. For the cloud version, Tenable offers a subscription model. For the on-premises version, Tenable offers a subscription model as well as perpetual and maintenance licenses.

> **Note**: A Tenable Security Center license is required for the Tenable Web App Scanning on-premises version.

To use Tenable Web App Scanning, you purchase licenses based on your organizational needs and environmental details. Tenable Web App Scanning then assigns those licenses to *assets* in your environment: unique fully qualified domain names (FQDNs). If you only scan IP addresses, the system licenses those instead.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

> **Tip**: To view your current license count and available assets, in the Tenable top navigation bar, click and then click **License Information**. To learn more, see License Information Page.

How Assets are Counted

Tenable Web App Scanning determines your licensed asset count by scanning resources in your environment to identify FQDNs. FQDNs that have been scanned for vulnerabilities in the past 90 days count towards your license.

FQDNs are listed as complete URLs, as per the RFC-3986 internet standard. Under this standard, each FQDN has the following components and format:

```
hostname.parent-domain.top-level-domain
```

When you specify a web application target in a scan, Tenable Web App Scanning counts that target as a separate asset if any component of the FQDN differs from that of another scanned target or previously scanned asset. Multiple targets with different paths appended to the FQDN count as a single asset, as long as all components of the FQDNs match.

For example, the following targets count towards one asset:

```
hostname.parent-domain.top-level-domain/path1
hostname.parent-domain.top-level-domain/path2
hostname.parent-domain.top-level-domain/path2/path3
```

The following table shows when scan targets are considered to be the same asset and when they are considered to be separate assets, based on whether or not all the FQDN components match.

Same Asset	Separate Assets
• https://example.com • https://example.com/welcome • https://example.com/welcome/get-started • https://example.com/welcome/get-started/create-new-user • http://example.com	• *https://en.example.com (different hostname)* • *https://www.ex-ample.com (different parent domain)* • *https://www.example.org (different top-level domain)*

Tenable Tenable Web App Scanning Components

You can customize Tenable Web App Scanning for your use case by adding components. Some components are add-ons that you purchase.

Included with Purchase	Add-on Component
• External scanning functionality. • OWASP Top 10 Issues. • HTML5 crawling. • Integration with Tenable Vulnerability Management (if owned). • Use of the API.	Additional cloud scan concurrency. **Tip**: Concurrency is based on your licensed assets and determines how many Tenable-managed cloud scanners you can run simultaneously.

Reclaiming Licenses

When you purchase licenses, your total license count is static for the length of your contract unless you purchase more licenses. However, Tenable Web App Scanning reclaims licenses under some conditions. You can also delete assets or set them to age out so that you do not run out of licenses.

The following table explains how Tenable Web App Scanning reclaims licenses.

Asset Type	License Reclamation Process
Deleted assets	Tenable Web App Scanning removes deleted assets from the **Applications** and **Scanned** pages and reclaims their licenses within 24 hours.
Aged out assets	In **Settings** > **Sensors** > **Networks**, if you enable **Asset Age Out**, Tenable Web App Scanning reclaims assets after they have not been scanned for a period you specify.
All other assets	Tenable Web App Scanning reclaims all other assets—such as those imported from other products or assets with no age-out setting—after they have not been scanned for 90 days.

Exceeding the License Limit

To allow for usage spikes due to sudden environment growth or unanticipated threats, Tenable Web App Scanning licenses are elastic. However, when you scan more assets than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages.

Scenario	Result
You scan more assets than are licensed for three consecutive days.	A message appears in Tenable Web App Scanning.
You scan more assets than are licensed for 15+ days.	A message and warning about reduced functionality appears in Tenable Web App Scanning.
You scan more assets than are licensed for 30+ days.	A message appears in Tenable Web App Scanning; scan and export features are disabled.

Tip: Improper scan hygiene or product misconfigurations can cause scan overages, which result in inflated asset counts. To learn more, see Scan Best Practices.

Expired Licenses

The Tenable Web App Scanning licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, you can no longer sign in to the Tenable platform.

Tenable Enclave Security Licensing

This topic breaks down the licensing process for Tenable Enclave Security. It also explains how assets are counted, lists add-on components you can purchase, and describes what happens during license overages or expirations. To learn how to use Tenable Enclave Security, see the Tenable Enclave Security User Guide.

Licensing Tenable Enclave Security

To use Tenable Enclave Security, you purchase licenses based on your organizational needs and environmental details. Tenable Enclave Security assigns those licenses to your *assets*, which are assessed hosts from Container Security or Security Center.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

Note: Tenable offers simplified pricing to managed security service providers (MSSPs). To learn more, contact your Tenable representative.

Tenable Enclave Security Products

The following table lists Tenable Enclave Security products that require licenses, along with the asset type licensed.

Product	Asset Type
Tenable Security Center	Assessed hosts from Tenable Security Center or imported from other Tenable products.
Container Security	Assessed container images. For more information, contact your Tenable representative.

Reclaiming Licenses

When you purchase Tenable licenses, your total license count is static for the length of your contract unless you purchase more licenses. However, Tenable Enclave Security products reclaim licenses under some conditions—and then reassign them to new assets in the same product so that you do not run out of licenses.

The following table explains how each Tenable Enclave Security product reclaims licenses.

Exceeding the License Limit

To allow for usage spikes due to hardware refreshes, sudden environment growth, or unanticipated threats, you can temporarily exceed your license limits in Tenable Enclave Security:

- **Tenable Security Center** - You can temporarily exceed your licensed IP address count by 10%. If you exceed this number, Tenable Security Center is disabled.
- **Tenable Enclave Security Container Security** - When you scan more assets than you have

licensed, Tenable clearly communicates the overage and then reduces functionality in three stages:

Scenario	Result
You scan more assets than are licensed for three consecutive days.	A message appears in Tenable Enclave Security.
You scan more assets than are licensed for 15+ days.	A message and warning about reduced functionality appears in Tenable Enclave Security.
You scan more assets than are licensed for 45+ days.	A message appears in Tenable Enclave Security; scan and export features are disabled.

Tenable Enclave Security generates a warning in the user interface when you approach or exceed the license limit.

Tip: Improper scan hygiene or product misconfigurations can cause scan overages, which result in inflated asset counts. To learn more, see Scan Best Practices.

Expired Licenses

The Tenable Enclave Security licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, you can no longer sign in to the Tenable platform.

Tenable Security Center Licensing

This topic breaks down the licensing process for Tenable Security Center as a standalone product. It also explains how assets are counted, lists add-on components you can purchase, and describes what happens during license overages or expiration. To learn how to use Tenable Security Center, see the Tenable Security Center User Guide.

Tenable Security Center Versions

Tenable Security Center has two versions:

- **Tenable Security Center** — Includes Tenable Network Monitor in discovery mode and unlimited Tenable Nessus scanners.
- **Tenable Security Center+** — Includes all of the above plus Tenable Network Monitor with vulnerability detection and metrics such as Asset Exposure Score (AES) and Asset Criticality Rating (ACR).

Tenable Security Center Director is available for both versions. Tenable Security Center Director is an add-on with which you can manage multiple Tenable Security Center instances from one location. For more information, see the Tenable Security Center Director User Guide.

> **Note**: You cannot upgrade a Tenable Security Center license to a Tenable Security Center Director license or downgrade a Tenable Tenable Security Center Director license to a Tenable Security Center license.

Licensing Tenable Security Center

To use any version of Tenable Security Center, you purchase licenses based on your organizational needs and environmental details. Tenable Security Center assigns those licenses to your *assets*, which are assessed hosts from Tenable Cloud Security or imported from other Tenable products.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

> **Note**: Tenable offers simplified pricing to managed security service providers (MSSPs). To learn more, contact your Tenable representative.

How Assets are Counted

Tenable Security Center licenses are valid for specific hosts and a maximum number of active assets identified by IP address or UUID. Assets count towards your license depending on how Tenable Security Center discovers them. In general, assets do not count unless they have been assessed for vulnerabilities.

For example, if you purchase a 500 asset license, you can perform host discovery on your network, but you cannot assess more than 500 assets. For more information about discovery and assessment scanning, see Scanning Overview in the *Tenable Security Center User Guide*.

The following table explains when assets count towards your license.

Counted Towards Your License	Not Counted Towards Your License
• Assets from active scans. • Assets from Log Correlation Engine instances. • Assets from Tenable Network Monitor instances not in discovery mode. • (Not available in Tenable Security Center Director) UUIDs from OT Security instances. • Assets in offline or remote repositories that you downloaded using the same Tenable Security Center instance or license. **Note**: In agent or IPv4 repositories, each single IP address or UUID counts once toward your license, even if it was scanned via multiple methods or stored in multiple repositories. In universal repositories, each asset with a UUID is counted toward your license. For example, if an asset in an IPv4 repository does not have a UUID, and the same asset is stored in a universal repository with a UUID, the asset is counted twice.	• Assets present only from imports to offline or remote repositories. • Assets present only from Tenable Network Monitor instances in discovery mode. • Assets in offline or remote repositories that you downloaded using the same Tenable Security Center instance with a different license. • Assets in offline or remote repositories that you downloaded using a different Tenable Security Center instance and license. • In the latest versions of Tenable Security Center and Tenable Security Center Director, the following excluded plugins: **Tenable Nessus** — 10180, 10287, 10335, 11219, 11933, 11936, 12053, 14272, 14274, 19506, 22964, 33812, 33813, 34220, 34277, 45590, 54615, 87413, 112154, 161455, 179042, 209654, and 204872. **Tenable Network Monitor** — 0, 12, 18, 19, 20, 113, and 132. **Tenable Log Correlation Engine** — 800000 through 800099.

Counted Towards Your License	Not Counted Towards Your License
Note: If you use an alternative port scanner, Tenable Security Center counts the detected IP addresses against your license.	**Note**: Older versions of Tenable Security Center may exclude different plugin output. To check excluded plugin output by product version, see License Requirements in the *Tenable Security Center User Guide*. From the drop-down in the upper right corner, select your version of Tenable Security Center.
Note: In the context of this table, assets are differentiated by the type of repository the data is stored in. For example: • in IPv4 and IPv6 repositories, *assets* are *IP addresses*. • in agent repositories, *assets* are *agents*. • in universal repositories, *assets* are *hosts*. For more information, see Asset Tracking in Tenable Security Center in the *Tenable Security Center User Guide*.	

Tenable Security Center Components

You can customize Tenable Security Center for your use case by adding components. Some components are add-ons that you purchase.

Note: Older versions of Tenable Security Center may not support all components. To check component support by product version, see License Requirements in the *Tenable Security Center User Guide*. From the drop-down in the upper right corner, select your version of Tenable Security Center.

Version	Included with Purchase	Add-on Component
Tenable Security Center	• One console (or more with additional IP addresses). • Tenable Network	• Cloud Tenable Agents. • Tenable Network Monitors in high-performance mode. • (Subscription-only) Additional consoles.

	Monitor in discovery mode. • Tenable Nessus scanners. • Vulnerability Probability Rating (VPR). • (Subscription-only) The same number of on-premises Tenable Agents as your licensed assets, provided on request.	• (Subscription-only) Security Center Lab License. • (Subscription-only) Tenable Lumin connector. Not available in Tenable Security Center Director. **Note:** The standalone Tenable Lumin SKU's will reach End of Sale (EOS) on March 31, 2025. Customers currently using Tenable Lumin and Tenable Lumin Connector will be upgraded to the Tenable One Platform for both new and renewal purchases. Contact your CSM if you want to migrate before this date to take advantage of all Tenable One capabilities. For more information, see the Tenable Lumin End of Sale Bulletin. • Tenable Web App Scanning, to scan web applications with a Tenable Nessus scanner in Tenable Security Center. Scan up to your number of licensed fully qualified domain names (FQDNs). For more information, see Web App Scans in the *Tenable Security Center User Guide*. **Note**: If you already have a Tenable Security Center license and you upgrade to Tenable Security Center version 6.2.x or later, there are two ways to enable web application scans. Either update your Tenable Web App Scanning plugins manually in Tenable Security Center or wait for the nightly plugin update to run. • (Subscription-only) Tenable Security Center Director.

		• (Perpetual-only) On-Premises Tenable Agents, which Perpetual customers must purchase separately. • Tenable Attack Surface Management. • Tenable Lumin, if you want to view your data in Tenable Vulnerability Management. Not available in Tenable Security Center Director. **Tip:** Synchronized assets that count toward your Tenable Security Center license also count toward your Tenable Vulnerability Management license. • Vulnerability Intelligence. • Log Correlation Engine. **Note:** Tenable no longer supports Log Correlation Engine and will deprecate it at the end of 2024.
Tenable Security Center+	• One console (or more with additional IP addresses). • Tenable Network Monitor in discovery mode. • Tenable Network Monitors with vulnerability detection. • Tenable Nessus scanners.	• Cloud Tenable Agents. • Tenable Network Monitors in high-performance mode. • (Subscription-only) Additional consoles. • (Subscription-only) Security Center Lab License. • (Subscription-only) Tenable Lumin connector. Not available in Tenable Security Center Director. **Note:** The standalone Tenable Lumin SKU's will reach End of Sale (EOS) on March 31, 2025. Customers currently using Tenable

	• Asset Exposure Score (AES). • (Not available in Tenable Security Center Director) Asset Criticality Rating (ACR). • Vulnerability Priority Rating (VPR). • (Subscription-only) The same number of on-premises Tenable Agents as your licensed assets, provided on request.	> Lumin and Tenable Lumin Connector will be upgraded to the Tenable One Platform for both new and renewal purchases. Contact your CSM if you want to migrate before this date to take advantage of all Tenable One capabilities. For more information, see the Tenable Lumin End of Sale Bulletin. • Tenable Web App Scanning, to scan web applications with a Tenable Nessus scanner in Tenable Security Center. Scan up to your number of licensed fully qualified domain names (FQDNs). For more information, see Web App Scans in the *Tenable Security Center User Guide*. > **Note**: If you already have a Tenable Security Center license and you upgrade to Tenable Security Center version 6.2.x or later, there are two ways to enable web application scans. Either update your Tenable Web App Scanning plugins manually in Tenable Security Center or wait for the nightly plugin update to run. • (Subscription-only) Tenable Security Center Director. • (Perpetual-only) On-Premises Tenable Agents, which Perpetual customers must purchase separately. • Tenable Attack Surface Management. • Tenable Lumin, if you want to view your data in Tenable Vulnerability Management. Not available in Tenable Security Center Director.

		Tip: Synchronized assets that count toward your Tenable Security Center license also count toward your Tenable Vulnerability Management license. • Vulnerability Intelligence. • Log Correlation Engine. **Note:** Tenable no longer supports Log Correlation Engine and will deprecate it at the end of 2024.

Reclaiming Licenses

Tenable Security Center's license count updates when you delete a repository, run a license report, or upload a new license. If you set assets to age out, they are removed during nightly cleanup. If you configure your scan settings to remove unresponsive hosts, they are removed at scan import.

For more information, see License Count in the *Tenable Security Center Best Practices Guide*.

Exceeding the License Limit

As you approach or exceed your license limit, a warning appears in the Tenable Security Center interface. If you exceed your limit, Tenable disables your access to Tenable Security Center. To monitor your license limit, use the **Licensing Status** widget, as described in Overview Dashboard. The Overview Dashboard is not available in Tenable Security Center Director. To upgrade your license, contact your Tenable representative.

Expired Licenses

The Tenable Security Center licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, your Tenable products and components are affected as follows:

- **Tenable Security Center Console (Perpetual license)** — The software remains fully functional. All user data is accessible.
- **Tenable Security Center Console (Subscription license)** — To access the console, you must enter a new license key. Once you enter a new license key, normal operation resumes.
- **Tenable Nessus (Perpetual license)** — When your maintenance period expires, plugin updates are no longer available. After 90 days, Tenable Nessus stops working and you cannot perform new scans. Because Tenable Security Center stops receiving feeds, the Tenable Nessus scanners managed by Tenable Security Centeror your managed Tenable Security Center instances no longer receive updates and also stop working.
- **Tenable Network Monitor (Perpetual license)** — After 30 days with no updates, new data is no longer processed.
- **Tenable Log Correlation Engine** — On the day of license expiration, new logs are no longer processed.

Working with License Keys

The following sections explain how to work with Tenable license keys and link to additional details.

Get a Tenable Security Center License Key

To get a Tenable Security Center license key, enter the hostname of the installation machine in a form on the Tenable Community site, as described in the Tenable Community Guide. You can also email the key to licenses@tenable.com. In both cases, you receive a Tenable Security Center license key to use when activating your products.

> **Tip**: To obtain the hostname of the installation machine, in a system shell prompt, type hostname.
>
> You can also use the install UUID in place of the hostname. The install UUID appears on the license activation page of the initial setup wizard, and is also available on disk in the install log and in the `install-uuid.txt` file.

Add or Update a Tenable Security Center License Key

In most cases, adding a license key to Tenable Security Center or its attached products requires the Tenable Security Center console to contact a product registration server. The server connection is encrypted, as described in Encryption Strength.

Tip: To learn which Tenable sites to allow through your firewall, see the Tenable Knowledge Base.

Note: For instructions to use in offline or air-gapped environments, see Offline Plugin and Feed Updates for Tenable Security Center.

See the following topics for instructions to upload a new license key or update an existing one:

- Quick Setup — Upload a new Tenable Security Center license and add activation codes for any attached products.
- Apply a New License — Upload a new license for attached Tenable products only.
- Update an Existing License — Update an existing Tenable Security Center license or existing attached Tenable product licenses.

Tenable Identity Exposure Licensing

This topic breaks down the licensing process for Tenable Identity Exposure as a standalone product. It also explains how assets are counted and describes what happens during license overages or expirations. To learn how to use Tenable Identity Exposure, see the Tenable Identity Exposure User Guide.

Licensing Tenable Identity Exposure

Tenable Identity Exposure has two versions: a cloud version and an on-premises version. Tenable also offers subscription pricing in some cases.

To use Tenable Identity Exposure, you purchase licenses based on your organizational needs and environmental details. Tenable Identity Exposure then assigns those licenses to your *assets*: enabled users in your directory services.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

Tip: To view your current license count and available assets, in the Tenable top navigation bar, click and then click **License Information**. To learn more, see License Information Page.

Note: Tenable offers simplified pricing to managed security service providers (MSSPs). To learn more, contact your Tenable representative.

How Assets are Counted

Each Tenable Identity Exposure license you purchase entitles you to scan one unique identity or digital representation of a user. Tenable does not double count identities. For example, enabled user accounts for the same identity in both Microsoft Active Directory and Microsoft Entra ID count as one Tenable license.

Use this PowerShell script to trace enabled user accounts in AD:

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

Use this PowerShell script to trace enabled user accounts in Entra ID:

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

Tenable Identity Exposure Components

Both versions of Tenable Identity Exposure come with the following components:

- Trail Flow
- Topology
- Indicators of Exposure
- Indicators of Attacks
- Attack Paths
- Exposure Center
- Microsoft Entra ID Support

Reclaiming Licenses

When you purchase licenses, your total license count remains static for the length of your contract unless you purchase more licenses. However, Tenable Identity Exposure reclaims licenses in real time when you delete enabled users from your environment's directory service.

Exceeding the License Limit

To allow for usage spikes due to hardware refreshes, sudden environment growth, or unanticipated threats, Tenable licenses are elastic. You can temporarily exceed your licensed identity count. However, when you scan more identities than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages.

Note: For on-premises environments using Tenable Identity Exposure 3.77 or later, the license enforcement is immediate.

Scenario	Result
You have more enabled identities than are licensed for three consecutive days	A message appears in Tenable Identity Exposure.
You have more enabled identities than are licensed for 15+ days	A message and a warning about reduced functionality appears in Tenable Identity Exposure.
You have more enabled identities than are licensed for 30+ days	A message appears in Tenable Identity Exposure and you cannot use the Indicator of Exposure feature in the user interface or API.

Expired Licenses

The Tenable Identity Exposure licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, you can no longer sign in to the Tenable platform.

Tenable Attack Surface Management Licensing

This topic breaks down the licensing process for Tenable Attack Surface Management as a standalone product. It also explains how assets are counted and describes what happens during license overages or expirations. To learn how to use Tenable Attack Surface Management, see the Tenable Attack Surface Management User Guide.

Tenable Attack Surface Management Versions

You can purchase Tenable Attack Surface Management in two versions:

- **Tenable Attack Surface Management Fortnightly Frequency**
- **Tenable Attack Surface Management Daily Frequency**

Licensing Tenable Attack Surface Management

To use any version of Tenable Attack Surface Management, you purchase licenses based on your organizational needs and environmental details. Tenable Attack Surface Management then assigns those licenses to your *assets*: observable objects, which include domain names, subdomains, or IP addresses for internet-connected or internal network devices.

> **Tip**: An observable object is a unique quadruple of DNS record name, DNS record type, DNS record value, and IP address.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

> **Note**: Tenable offers simplified pricing to managed security service providers (MSSPs). To learn more, contact your Tenable representative.

> **Note**: When you purchase a Tenable Attack Surface Management license, inventory is set to 10% of the purchase limit by default. You can increase this limit on the **Inventory Settings** page. For more information, see Inventory Settings.

How Assets are Counted

All assets in all inventories are counted towards your license, except archived assets.

Reclaiming Licenses

Tenable Attack Surface Management's license count updates daily. The license count updates when you archive individual assets or remove asset sources—and it also updates when assets age out. Removed assets are only counted when restored.

Exceeding the License Limit

In Tenable Attack Surface Management, when your asset count exceeds your license limit, Tenable clearly communicates the overage as follows.

Scenario	Result
You add a source that is greater than your inventory limit.	A message appears in the Source column: *"We could not add all of the subdomains for this domain because your inventory is full."*
You reach your inventory asset limit.	When you click the inventory, a message appears: *"You have reached your limit of # assets. Please contact us to increase your limit."*
You reach your business limit, which is related to your licensed asset purchase.	A message appears in Tenable Attack Surface Management: *"Business Asset limit reached. Please contact support to increase the Business Asset limit."*

Expired Licenses

The Tenable Attack Surface Management licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, you can no longer sign in to the Tenable platform.

Tenable OT Security Licensing

This topic breaks down the licensing process for Tenable OT Security as a standalone product. It also explains how assets are counted, lists add-on components you can purchase, explains how licenses are reclaimed, and describes what happens during license overages or expirations. To learn how to use Tenable OT Security, see the Tenable OT Security User Guide.

Tip: To update or reinitialize your license, see OT Security License Workflow.

Licensing Tenable OT Security

You can purchase Tenable OT Security in subscription or perpetual/maintenance versions.

To license Tenable OT Security, you purchase licenses based on your organizational needs and environmental details. Tenable OT Security then assigns those licenses to your *assets*: all detected devices with IP addresses, one license for each IP address.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

How Assets are Counted

In Tenable OT Security, your license count is based on the number of unique IP addresses in your environment. Assets are licensed from the moment they are detected.

Note: Assets on internal networks behind live IP addresses do not count towards your license. For example, in a redundantly connected Programmable Logic Controller (PLC) chassis with two live IP addresses and 10 modules behind these, only the two live IP addresses count towards your license.

Note: While you can connect a standalone purchase of OT Security to your instance of Tenable One, that does not handle the licensing of those assets. Tenable One customers have a plethora of Tenable solutions that are licensed to them, including OT Security, but the licenses must be part of the Tenable One license first. You can work with your customer success managers (CSM) to update the account accordingly.

Tenable OT Security Components

You can customize Tenable OT Security for your use case by adding components. Some components are add-ons that you purchase.

Included with Purchase	Add-on Component
• Virtual Core Appliance. • Tenable Security Center.	• Tenable OT Security Enterprise Manager. • Tenable OT Security Configurable Sensor. • Tenable OT Security Certified Configurable Sensor.

	• Tenable OT Security Certified Core Platform. • Tenable OT Security Core Platform. • Tenable OT Security XL Core Platform.

Reclaiming Licenses

When you purchase licenses, your total license count is static for the length of your contract unless you purchase more licenses. However, Tenable OT Security reclaims licenses in real time as your asset count changes.

Tenable OT Security reclaims the following assets:

- Hidden assets
- Assets that have been offline for more than 30 days
- Assets you remove or hide in the user interface

Exceeding the License Limit

In Tenable OT Security, you can only use your allocated number of licenses unless you purchase more licenses.

When you exceed your license limit:

- Non-administrators can no longer access Tenable OT Security.
- A message that your license has been exceeded appears in the user interface.
- You can no longer restore assets from the Tenable OT Security Settings.
- You can no longer update vulnerability plugins or IDS Signatures (Feed updates).

Note: When you exceed your license limit, Tenable OT Security can still detect and add new assets.

Expired Licenses

The Tenable OT Security licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, Tenable OT Security is disabled and you cannot use it.

Tenable Nessus Licensing

This topic explains how to license Tenable Nessus and lists its features. To learn how to use Tenable Nessus, see the Tenable Nessus User Guide.

Licensing Tenable Nessus

You can manage Tenable Nessus in Tenable Security Center or run it as a a standalone subscription product. To purchase a subscription, go to the Tenable website or work with a Tenable partner.

Tenable Nessus has two versions:

- **Tenable Nessus Professional** — A single subscription price.
- **Tenable Nessus Expert** — A subscription price plus any additional web application scanning or external attack surface scanning (EASM) domains beyond five per quarter.

Plugin Feed Activation Code

Wherever you manage Tenable Nessus, you need a *plugin feed activation code*, which identifies which version you are licensed for—and, if applicable, how many IP addresses you can scan, how many remote scanners you can link, and how many Tenable Agents you can link to Tenable Nessus Manager. Where you enter this code depends on how you manage Tenable Nessus.

- **Tenable Nessus Subscription** — Manage your activation code in Tenable Nessus, as described in Manage Activation Code.

  > **Tip**: To set up Tenable Nessus offline, see Manage Tenable Nessus Offline.

- **Tenable Nessus in Tenable Security Center** — Manage your activation code (and plugin updates) in Tenable Security Center. When you register Tenable Nessus, start it before Tenable Security Center and select **Managed by SecurityCenter**. For more information, see Apply a New License in the *Tenable Security Center User Guide*.

Manage Tenable Nessus with Tenable Vulnerability Management

If you are using Tenable Vulnerability Management to manage your Tenable Nessus scanners, the plugin and software updates are managed from Tenable Vulnerability Management. For more information, see Tenable Nessus Plugin and Software Updates in the *Tenable Nessus User Guide*.

Tenable Vulnerability Management includes the ability to link unlimited Tenable Nessus scanners as a default component.

For more information about Tenable Vulnerability Management licensing, see Tenable Vulnerability Management Licensing in the *Tenable Licensing Guide*.

Manage Tenable Nessus with Tenable Security Center

If you are using Tenable Security Center to manage your Tenable Nessus scanners, the activation code and plugin updates are managed from Tenable Security Center. For more information, see Tenable Nessus Plugin and Software Updates in the *Tenable Nessus User Guide*.

You must start Tenable Nessus before it communicates with Tenable Security Center, which it normally does not do without a valid activation code and plugins. To have Tenable Nessus ignore this requirement and start (so that it can get the information from Tenable Security Center), when you register your scanner, select **Managed by SecurityCenter**.

For more information about Tenable Security Center licensing, see Tenable Security Center Licensing in the *Tenable Licensing Guide*.

Tenable Nessus Versions

Tenable Nessus Professional and Tenable Nessus Expert have the following features.

Feature	Tenable Nessus Professional	Tenable Nessus Expert
Nessus Live Results	Yes	Yes
Vulnerability scanning	Yes	Yes
Compliance scanning	Yes	Yes
Dynamic Application Security Testing (DAST) web application scanning	No	Five web applications per quarter (purchase more as needed)
External attack surface scanning	No	Five domains per quarter (purchase more as needed)
Scan Infrastructure as Code	No	Yes