Tenable Cloud Platform Service Description Guide

Last Revised: September 05, 2024

Table of Contents

Introduction

Last updated: September 05, 2024

The intention of this Tenable Cloud Platform Service Description Guide ("Service Description") is to provide customers with a comprehensive understanding of service definitions for all hosted products. These include Tenable One, Tenable Vulnerability Management, Tenable Identity Exposure, Legacy Tenable Cloud Security, Tenable Attack Surface Management, Tenable Web App Scanning, and may include future product(s). Tenable may update this document periodically.

> **Note:** This document does not cover Tenable's FedRAMP offering.

Service Terms and Policies

The following links access important term and policy documents that pertain to the Tenable Cloud Platform Services. Be sure to read these documents to understand the service clearly. If you have any questions, contact your Tenable sales representative.

- Tenable Software License Agreements, which includes the following:
  - Tenable Master Agreement
  - Tenable Data Processing Addendum
  - Service Level Agreement
- Tenable GDPR Alignment
- Pricing Model Definitions
- Tenable Technical Support Plans

Platform Regions

Users can find Supported Tenable Cloud Platform cloud regions and respective characteristics listed here.

Platform Network Connectivity

Access to the Tenable Cloud Platform is granted through publicly available endpoints. In all cases, customers are responsible for the required reliable connectivity complying with local and regional

regulations. If customers are unable to meet the connectivity requirements for accessing the Tenable Cloud Platform through agents, scanners, UI, and APIs, Tenable recommends collaborating with internal network resources to establish reliable and uninterrupted connectivity. Potential solutions may include using a proxy, configuring explicit firewall access control lists, utilizing alternative circuits or routes, or setting up VPNs as necessary to achieve the desired outcome.

Platform Authentication and Access

Customers can configure authentication using a SAML v2 identity provider. User access is controlled with a role-based access control (RBAC) feature set. To access our API, customers have the option to create a distinct set of API keys that are unique to their account. The keys allow external applications to make authorized API calls to the Tenable Cloud API, without creating a session. For more information, see Authorization.

Platform License Elasticity and Compliance

Currently, the Tenable Cloud Platform provides license elasticity for customers to burst up to 10% above their license. Overutilization of license may result in in-product and email notifications and/or loss of function and access. In addition, customers are liable for all actual license usage (including overages) in accordance with the Tenable Master Agreement. Tenable will use commercially reasonable efforts to communicate directly with account owners prior to functional impact.

To aid in license hygiene and compliance, Tenable provides several resources to help customers to comply with contracted licenses:

- Tenable Scan Best Practices
- Tenable Vulnerability Management Licenses
- Asset Ageout Feature Usage
- Manual Asset Delete

Tenable Cloud Platform Data

Data Isolation

Data is logically isolated from other customer data in the Tenable Cloud Platform. Data integrity is not affected by other platform users.

Data Encryption

All data in all states in the Tenable Cloud Platform is encrypted with at least one level of encryption, using no less than AES-256.

At Rest – Data is stored on encrypted media using at least one level of AES-256 encryption.

Some data classes include a second level of per-file encryption.

In Transport – Data is encrypted in transport using TLS v1.2 with a 4096-bit key (this includes internal transports).

Tenable Vulnerability Management Sensor Communication – Traffic from the sensors to the platform is always initiated by the sensor and is outbound only over port 443. Traffic is encrypted via SSL communication using TLS 1.2 with a 4096-bit key. This removes the need for firewall changes and allows customers to control the connections via firewall rules.

- Scanner-to-platform authentication
    - The platform generates a random key of 256-bit length for each scanner connected to the container and passes that key to the scanner during the linking process
    - Scanners uses this key to authenticate back to the controller when requesting jobs, plugin updates, and updates to the scanner binary
- Scanner-to-platform job communication
    - Unless congestion is observed, scanners contact the platform every 30 seconds.
    - If there is a job, the platform generates a random key of 128-bits
    - The scanner requests the policy from the platform
    - The controller uses the key to encrypt the policy, which includes the credentials to be used during the scan

In Backups / Replication – Volume snapshots and data replicas are stored with the same level of encryption as their source, no less than AES-256. All replication is done via the provider. Tenable does not back up any data to physical off-site media or physical systems.

In Indexes – Index data is stored on encrypted media using at least one level of AES-256 encryption.

Scan Credentials – Are stored inside of a policy which is encrypted within the container's AES-256 global key. When scans are launched, the policy is encrypted with a one-use random 128-bit key and transported using TLS v1.2 with a 4096-bit key.

Key Management – Keys are stored centrally, encrypted with a role-based key, and access is limited. All the encrypted data stored can be rotated to a new key. The datafile encryption keys are different on each regional site, as are the disk-level keys. Sharing of keys is prohibited, and key management procedures are reviewed on a yearly basis.

For more information, see How Tenable Encrypts Data.

Data Handling and Export

Data is kept in the region your container is deployed in. Customers may provision regional containers under a single license for multi-region requirements.

Data sent to the Tenable platform is analyzed, indexed and stored to provide functionality in the cloud. Data is ingested via Nessus Scanners of all types, product-specific connectors, integrations, and APIs. Additional details on current storage management and retention are below.

General Data Retention

- The default retention period for processed and indexed scan data is six months. Although not recommended, administrators can configure it for up to 15 months. This is configured via age-out time in the networks setting.
- Upon expiration or termination of a product subscription, customer data will be deleted. Currently, this data is retained for up to 30 days from the termination date.
- Raw data from individual scan results (ScanDB files) is retained for 45 days.

PCI Data Retention

Tenable's data retention policy concerning PCI scans will match then-current requirements set forth by the PCI Security Standards Council. Customers can also refer to the Tenable Master Agreement. (see Tenable Master Agreement).

Security Controls

Tenable security controls are described in our most recent Service Organization Control II, Type I Report. To receive a copy of the report, put in a request to compliance@tenable.com.

Platform Performance and Maximums Reference

The Tenable Cloud Platform is a multi-tenant architecture. Scanner and processing pools are shared and scaled to support demand. Rate and concurrency maximums may be activated when customer activity negatively impacts the platform, the products (the systems supporting the products), or other tenants. See the Tenable Master Agreement for additional details.

General platform performance varies based on platform conditions, resource utilization, global region, tenant traffic, license, and customer configuration of scan target volume and depth of assessment. The vast majority of customers experience individual end-to-end scan job duration within a maximum of a couple of hours; provided, however, this is subject to both platform conditions as well as customer-specific scan configurations. This is provided without guarantee and is to be used as a reference for troubleshooting customer environments and configurations. To learn how you can tune each aspect to make your scan faster or more data-inclusive, depending on your desired outcome, please view the Vulnerability Management Scan Tuning Guide. Also, to help improve this time, customers can leverage high-traffic plugin processing optimizations outlined in this FAQ.

Maximums and controls for major functions and services are described below:

API Maximums

The platform performs rate limiting on API requests to ensure that all customers experience the same level of service. The platform calculates the number of API requests it can accept from a single user per minute based on its current processing load. Users are uniquely identified by the API key utilized in every API request. Each user is limited to possessing only a single valid API key at any given time. For more information on the parameters and behaviors to adhere to, see API Rate Limiting.

Export Maximums

Note that there are limits on the number of concurrent export requests that can be made on the platform. Users are allowed a maximum of ten active concurrent export requests per customer container, depending on the endpoint being used. Additionally, the maximum storage capacity for

export job files is 500MB or 50GB depending on license. For more information, see Export Concurrency Limiting.

Cloud Scanner Maximums

Unless otherwise specified, each customer container has the following cloud scanner warnings or controls by default:

- Prior to scan execution, the maximum number of simultaneous cloud scanner jobs is 25. As a result, no additional cloud scanner scans will be launched or queued.
- Prior to scan execution, users are WARNED if any scan target list exceeds 10x license. This is intended to minimize mistakes in target definitions that may produce results that exceed customer license. Customers can tune scan target lists to remove warnings.
- During scan execution, the scan job will terminate when returned billable assets exceed 1.1x license (i.e. up to 10% elasticity over license per scan).
- Linked non-cloud scanners and agents will retry and be processed independent of the cloud scanner concurrency limit, in-line with API maximums.

Contact your Customer Success Manager to discuss your scan maximum needs or stagger jobs over time to reduce the chance of conflict. For more information, see Scan Concurrency Limiting and Scan Limitations.

Web Application Scan Maximum

Our platform has a standard for the number of concurrent Web Application Scans that can operate. The limit is based on the size of the purchased license, but it can be expanded as needed. By default, each customer instance can have a maximum of 5 ongoing web application scans (WAS), unless stated otherwise.

Plugin Search Maximum

The platform maintains a plugin output index to support plugin output search. This index maintains the previous 35 days of data. This feature is disabled by default. When enabled, if a container does not utilize the index for more than 35 days, it is disabled. Customer administrators can enable this feature at any time for all new scan data from that point forward.

Key Service Descriptions and Maximum Values

The Tenable Cloud Platform provides the following key services in support of Tenable products:

Category Service	Service Component	Maximum Value	Additional Information
Cloud Hosted Nessus Scanner	Scan Job	25 active, concurrent scans per container	Each container can have up to 25 active concurrent scans. For more information and the definition of an active scan, see Concurrent Active Scan Limits.
		10,000 scheduled scans per container	The maximum number of scheduled scans is 10,000 per container. For best practices on managing scans via the API, see Manage Scans.
		Target IP addresses and hostnames up to 1,000 times your licensed asset count per discovery scan	For example, if your organization has a licensed asset count of 1,000, the platform does not allow you to target more than 1,000,000 IP

			addresses or hostnames in a single discovery scan (for more information, see Discovery Scans vs. Assessment Scans in the *Tenable Vulnerability Management User Guide*).
		Live host scan results for up to 1.1 times your licensed assets per scan	A scan job aborts when it generates live host scan results for more than 1.1 times your licensed asset count.
		Dead host scan results for up to 100 times your licensed assets per scan	A scan job aborts when it generates dead host scan results for more than 100 times your licensed asset count.
		300,000 targeted IP addresses or ranges per scan	You cannot specify more than 300,000 comma-separated IP addresses or ranges when configuring a

			scan's targets.
		10,000 hosts, 150,000 findings, *or* 7 GB in total size per scan chunk	If a scan chunk exceeds any of the maximum values, Tenable Vulnerability Management does not process the scan and eventually aborts it. **Note:** This limits items like MDM assessments, importing Nessus files, and very large Auto Discovery scenarios (for example, VMware) to individual scans with less than 10,000 assessed targets.
Cloud Hosted Web Application Scanner	Scan Jobs	8 hours, 4 concurrent	Web Application scan jobs may take up to 8 hours to complete. Scans will run for a maximum time of 99:99:59 before aborting. Concurrency limits depend on

			your container license.
Agentless Scanners	Scan Jobs	24-hour scan completion	Agentless scan jobs may take up to 24 hours to complete.
	CSPM scans	6-hour max duration	CSPM scans, required by Agentless scans, have a maximum duration of 6 hours.
Bulk Delete	Query Endpoint	1,000 conditions in query object	Currently, Tenable supports up to 1,000 conditions (filters) within the query object.
	Bulk Delete Assets	1,000 filters per query	Currently, Tenable supports up to 1,000 conditions (filters) within the query object of the Bulk Delete Asset endpoint.
Export	Scan Results	400,000 individual scan results	Currently, Tenable can not export PDF files with more than 400,000 individual scan results.
	Scan DB	45 days	Currently, Tenable purges Scan DB

			exports 45 days after scan completion.
	Scan Results	Archived scan results older than 45 days are limited export types of .nessus and .csv files	
		Number of shown rows in the **Vulns by Asset** table is limited to 5,000	
	Concurrent Jobs	10 concurrent exports per container	For more information, see Concurrency Limiting.
Filtering	Filtering an Explore Table	Number of filters is limited to 18	Currently, the maximum number of filters that can be applied to any Explore > Findings or Assets views (including Group By tables) to 18.
	IPv4 Address filter on the Findings workbench	Number of IPv4 addresses limited to 256	On the **Findings** workbench, when using the **IPv4 Address** filter, the number of IPv4 addresses is limited to 256.
	Filtering a Report	Number of Custom Asset filter IP addresses you can specify is limited to 100	When filtering a report using the **Custom Asset**

			report filter, you can filter by no more than 100 individual IP addresses.
		Number of filters you can apply to a Findings Report is 5	When filtering findings to generate a Findings Report, you can apply a maximum of 5 filters to each report.
Imports	Import Assets	Up to 50 individual assets per request	Currently, Tenable supports a maximum of 50 individual asset objects per request message with a total size limit of 15 MB.
Tags	Create Tag Rules	35 rules per tag	Tenable Vulnerability Management supports a maximum of 35 rules per tag. This limit means that you can specify a maximum of 35 **and** or **or** conditions for a single tag value.

	Create Tag Rules	25 values per individual rule/1,024 per individual tag rule	Tenable Vulnerability Management supports a default maximum of 25 values per individual tag rule. For IPv4, IPv6, and FQDNs, Tenable Vulnerability Management supports a maximum of 1,024 values per individual tag rule.
Recast/Accept Rules	Adding hosts to recast/accept rules	1,000 hosts per rule	Tenable limits the number of individual hosts you can target as part of a recast/accept rule to 1,000.
Activity Logs	Log Retention	3 years	Currently, Tenable retains activity log data for 3 years, after which it is deleted from the Tenable database.

Tenable Cloud Platform Licensing Policy

The Tenable Cloud Platform Licensing Policy provides customers an understanding of Tenable product definitions and their licensing policies. This policy may be updated periodically at Tenable's sole discretion.

Platform Licensing Breakdown

The Tenable Cloud Platform consists of multiple products. Products on the platform can be purchased via Tenable One or, alternatively, some may be purchased a-la-carte.

> Tip: For more information about how Tenable products are licensed, see the *Tenable Licensing Quick Reference Guide*.

- Tenable One: Single License structure for accessing all platform applications (a simplified "per asset" model).
- Tenable Vulnerability Management: Licensed per asset.
- Tenable Web App Scanning: Licensed per FQDN scanned.
- Tenable Cloud Security: Licensed per cloud resource/asset.
- Tenable Identity Exposure: Licensed per user.
- Tenable Attack Surface Management: Licensed per observable objects.
- Tenable PCI ASV: single license for unlimited scans/unlimited attestations (requires Tenable Vulnerability Management minimal license).

Definitions

Asset

The Tenable Master Agreement defines "Scan Target(s)" as the targets or subjects of a Scan. The purpose of this Policy is to set forth how Tenable defines, differentiates, and counts different types of Scan Targets for licensing purposes. For purposes of this Policy, an Asset is considered a Scan Target. For the purposes of this policy, an asset is considered a Scan Target.

An asset is defined as:

- A physical or virtual device with an operating system connected to a network.
- An active (non-terminated) cloud resource (including but not limited to containers, virtual devices, applications, native services, IaC etc.) that is monitored for policy violations and security risk.
- A web application with an FQDN.
- A user, under the constructs of Identity Security Products.

Example assets may include, but are not limited to:

- Laptops
- Desktops
- Servers
- Routers
- Firewalls
- Switches
- IoT Devices
- Mobile phones
- Virtual machines
- Software containers
- IaC
- Operational technology devices
- Cloud resources, including but not limited to AWS, GCP or MS Azure compute, database and networking services.
- User Accounts

Assessed Asset

An “assessed asset” is any asset that has been scanned for a vulnerability, configuration, or state.

Discovered Asset

A “discovered asset” is any asset that has been identified by discovery plugins, but not scanned for vulnerability, configuration or state.

Licensed Asset

A “licensed asset” is any asset that has been assessed within the product's specified metered billing term. Only billable cloud run time resources are considered as licensed assets and counted as such. Licenses are calculated by the number of scanner type(s) applied per resource.

Unlicensed Asset

An “unlicensed asset” is any asset that has not been assessed within the metered billing term, and is within the data retention period noted in the Tenable Master Agreement. The Tenable Cloud Platform discovers ALL Resources in cloud accounts (Cloud Runtime) and in repositories/pipelines (IaC/Container Images). Local Scan/Repository/Pipelines (IaC, local container images) resources are NOT billable.

Terminated Asset

If an asset is terminated in a cloud platform, it is automatically terminated in Tenable Vulnerability Management via cloud connector. While the asset is not permanently deleted, it is flagged as “terminated”. Vulnerability data is permanently deleted and falls off of the license the next day (via a nightly job). Asset termination is known as a soft deletion.

Deleted Asset

Deleted assets are permanently removed from the Tenable Platform. Deleted assets and associated data cannot be restored. When deleting assets manually through the user interface or API (including bulk asset deletion), the asset is flagged as “DELETED” and remains licensed for the remainder of the specified metered billing term, and need to age-out to be reclaimed. Review the Tenable Vulnerability Management Scan Tuning Guide to ensure the assets that are counted as licensed are aligned with a scan and assessment strategy. The Asset age out feature deletes assets for hygiene purposes. If aged-out, both the asset and vulnerability data is permanently deleted.

Tenable Web App Scanning FQDN

Tenable Web App Scanning determines asset count by the number of fully qualified domain names (FQDNs) that Tenable Web App Scanning successfully scans for your user account. An asset does not count against your license limit until Tenable Web App Scanning has successfully scanned the asset for vulnerabilities.

License Size

License size references the number of assets you have purchased and that can be assessed or scanned. Tenable allows temporary elasticity to exceed the license size by 10%, but for no more than 45-days before it is considered a violation of the license agreement.

Elastic Licensing

On a temporary basis, customers can exceed their contracted license size. However, customers must true-up when license counts continue to be exceeded.

The primary benefits of Elastic Asset Licensing are:

- Compensates for imperfect scan hygiene
- Allows for temporary asset increases from activities such as hardware refreshes or sudden environment growth
- Compensates for modern cloud environments and ephemeral assets that don't have traditional life-spans
- Adapts to and is reflective of dynamic customer environments

If the license size exceeds 10% for more than 45 days, review the Tenable Overage Process.

Tenable Cloud Region Availability

Tenable's product suite provides cloud-based solutions that can be utilized in numerous regions across the world. To ensure deployment flexibility, Tenable cloud products include several out-of-the-box regions that you can use to customize your product deployments. Users can choose to deploy the products in any of the AWS or Azure regions where they are available. The table below displays these regions and the products in which they can be used.

Note: Tenable provisions hosting sites permanently based on order specification and requirements at the time of purchase.

Tenable Products	Deployment Regions
• Tenable Vulnerability Management • Tenable Web App Scanning	The following AWS regions are available for use: **AMER** • **US East**: us-east-1 and us-east-2 • **US West**: us-west-1 and us-west-2 • **Canada**: ca-central-1 • **Brazil**: sa-east-1 **APAC** • **Australia**: ap-southeast-1 • **India:** ap-south-1 • **Japan**: ap-northeast-1 • **Singapore**: ap-southeast-1 **EMEA** • **Germany**: eu-central-1 • **United Kingdom**: eu-west-2

	GovCloud • **AWS GovCloud**: (US-West) - us-gov-west-1 For use with Tenable FedRAMP containers.
• Tenable PCI ASV • Tenable Lumin Exposure View • Tenable Tenable Inventory • Tenable Attack Path Analysis • Tenable Attack Surface Management • Legacy Tenable Cloud Security	The following AWS regions are available for use: **AMER** • **US East**: us-east-1 and us-east-2 • **US West**: us-west-1 and us-west-2 • **Canada**: ca-central-1 • **Brazil**: sa-east-1 **APAC** • **Australia**: ap-southeast-1 • **India:** ap-south-1 • **Japan**: ap-northeast-1 • **Singapore**: ap-southeast-1 **EMEA** • **Germany**: eu-central-1 • **United Kingdom**: eu-west-2
Legacy Tenable Cloud Security	The following AWS regions are available for use: **AMER** • **United States**: US East (Ohio) - us-east-2 • **Canada**: Canada (Central) - ca-central-1 • **Brazil**: South America (São Paulo) - sa-east-1

	APAC • **Australia**: Asia Pacific (Sydney) -ap-southeast-2 • **India**: Asia Pacific (Mumbai) - ap-south-1 • **Japan**: Asia Pacific (Tokyo) - ap-northeast-1 • **Singapore**: Asia Pacific (Singapore) - ap-southeast-1 • **South Korea**: Asia Pacific (Seoul) - ap-northeast-2 **EMEA** • **Europe**: Europe (Frankfurt) - eu-central-1 • **United Kingdom**: Europe (London) - eu-west-2 • **United Arab Emirates**: Middle East (UAE) - me-central-1 **GovCloud** • **AWS GovCloud**: (US-West) - us-gov-west-1 For use with Tenable FedRAMP containers.
Tenable Identity Exposure	The following Azure regions are available for use: **AMER** • **Brazil — Sao Paulo**: Brazil South • **Canada — Quebec City**: Canada East • **Canada — Toronto**: Canada Central • **United States — California**: West US • **United States — Iowa**: Central US • **United States — Virginia**: East US 2 **APAC**

	• **Australia — New South Wales**: Australia East • **Australia — Victoria**: Australia Southeast • **Hong Kong**: East Asia • **India — Pune**: Central India • **Japan — Osaka**: Japan West • **Singapore**: Southeast Asia **EMEA** • **France — Paris**: France Central • **Ireland**: North Europe • **Netherlands**: West Europe • **South Africa — Johannesburg**: South Africa North • **Switzerland — Zurich**: Switzerland North • **United Arab Emirates — Dubai** UAE North • **United Kingdom — London** UK South
Tenable MSSP Portal	**AMER** • **US West**: us-west-1 and us-west-2 The Tenable MSSP Portal is hosted in the **US West** region, but Tenable Products managed by the Tenable MSSP Portal can be deployed in multiple regions as detailed on this page. For more information, see the Tenable MSSP User Guide.

Additional Resources

- For more information about Tenable Vulnerability Management sensors and regions, see Cloud Sensors in the Tenable Vulnerability Management User Guide.

- For more information about Tenable Identity Exposure sensors and regions, see Deployment Regions in the Tenable Identity Exposure User Guide.
- For more information about Tenable Attack Surface Management sensors and regions, see Cloud Sensors in the Tenable Attack Surface Management User Guide.
- For more information about FedRAMP sensors and regions, see Cloud Sensors in the Tenable Vulnerability Management FedRAMP Moderate User Guide.

Platform Certifications, Maintenance, and Support

Platform Certifications

Tenable Cloud Platform has attained compliance attestations and certifications as part of Tenable's commitment to global security standards and data protection. These are as follows:

FedRAMP

Tenable Vulnerability Management and Tenable Web App Scanning received FedRAMP Authorization to Operate (ATO) in 2021.

> **Note:** This document does not cover Tenable's FedRAMP offering. Please refer to the FedRAMP Product Offering to view the authorized and supported features.

StateRAMP

Tenable Vulnerability Management is StateRAMP Authorized.

Cloud Security Alliance (CSA) STAR

Tenable is a member of the CSA STAR program. CSA STAR is an industry-leading program for security assurance in the cloud. To view the security controls for Tenable Vulnerability Management, visit the CSA website.

ISO 27001

Tenable's ISO/IEC 27001:2013 certification covers the ISMS supporting Tenable's legal areas, human resources, information technology, software development, executive leadership, and customer support functions. Details are publicly available in the Schellman Certificate Directory.

For more information, see Tenable Trust and Assurance.

Platform Assistance and Technical Support

Useful links for Tenable Cloud Platform technical support are:

- Customer Technical Support
- Tenable Community
- Technical Support Plans

Platform Maintenance

For information about Tenable network statuses and scheduled platform maintenance windows, see the Tenable Status website.

> **Tip:** You can subscribe to get the latest Tenable status updates.

Customer Responsibilities

Refer to the Tenable Master Agreement for details on customer responsibilities when using the Tenable Cloud Platform.