

Tenable Vulnerability Management vs. Tenable.sc

Quick Reference Guide

Last Revised: September 14, 2023

Copyright © 2023 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Welcome

This document exists to provide a high-level overview of the main differences between Tenable Vulnerability Management (formerly known as Tenable.io) and Tenable.sc (formerly known as Tenable.sc) functionality. Each individual section aims to answer the following questions:

Section	Questions Answered?
Product Architecture	What are the physical architecture differences between Tenable Vulnerability Management and Tenable.sc software?
Licensing	• How do assets count toward my license? • What are the limitations of my license(s)?
Scanning	• What types of scans can I perform? • What parts of my network can I scan?
Reporting	• Are there report templates? • Can I create a custom report?
Assets	• What is an asset? • What kind of assets does the software support? • How are assets identified?
Vulnerabilities / Findings	• What is a vulnerability? • What is a finding? • What is the difference? • What can I do with my vulnerabilities / findings?
Dashboards	• How can I view my data within the user interface? • How can I interact with, manage, and share this data using dashboards? • What dashboard templates are available?
Tenable Integrations / Data	• Does Tenable Vulnerability Management or Tenable.sc

Sharing	work with other Tenable products in any way? • Can I share vulnerability or scan data between Tenable products (for example, syncing vulnerability data between Tenable.sc and Tenable Vulnerability Management)?

Assumptions

This guide assumes you have basic familiarity with Vulnerability Management and at least one Tenable product (for example Tenable Vulnerability Management, Tenable.sc, or Tenable Nessus).

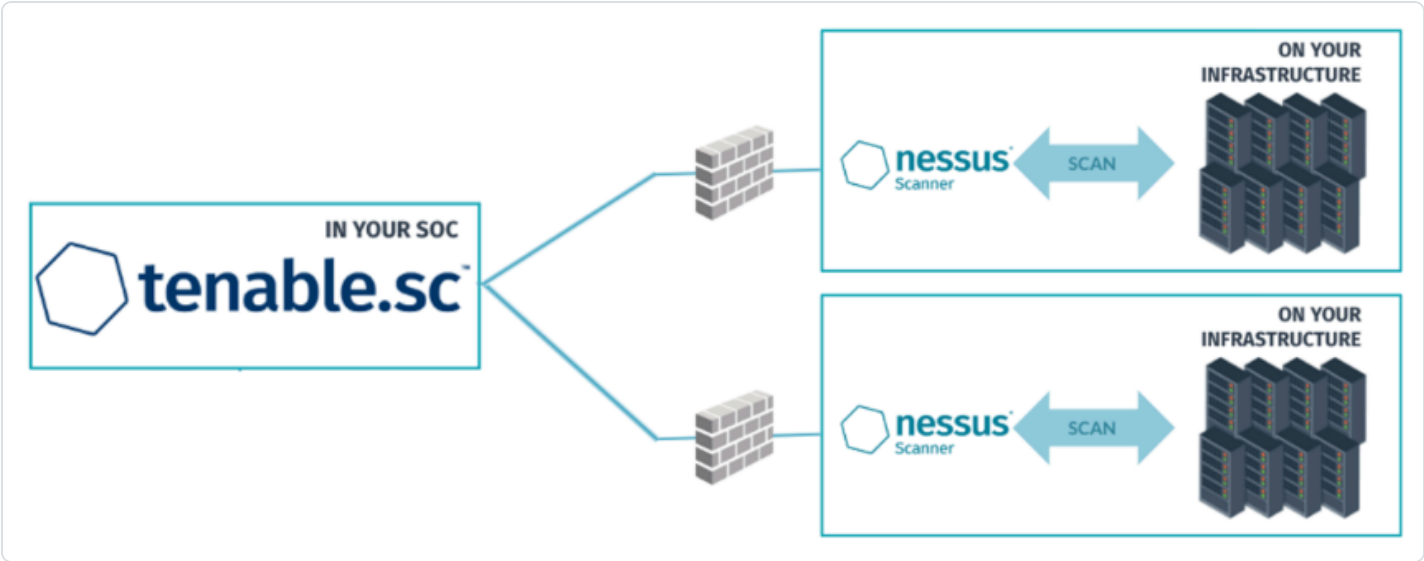
For more information, see

- The *Tenable Vulnerability Management User Guide*
- The *Tenable.sc User Guide*

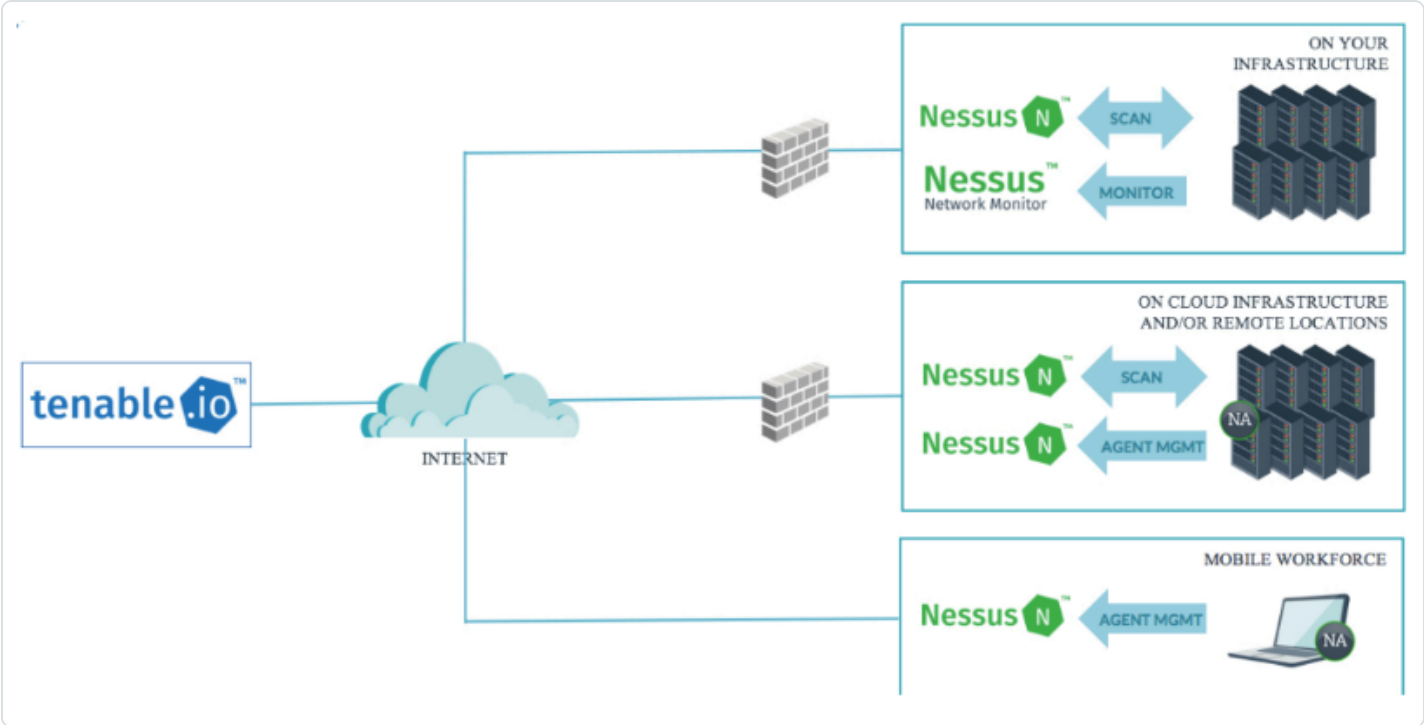
Product Architecture

The main difference between Tenable Vulnerability Management and Tenable.sc is the physical setup and location of the platforms.

Tenable.sc Architecture is hosted entirely on premise:



While the main Tenable Vulnerability Management interface is hosted in the cloud, and scanners are placed where needed:



Essentially, this means that Tenable.sc customers are responsible for the hardware for the entire infrastructure, including data storage. The Tenable Vulnerability Management “console” (and data storage) is hosted in the cloud and is therefore Tenable's responsibility.

Licensing

This topic describes the differences between licensing models in Tenable Vulnerability Management and Tenable.sc.

Tenable Vulnerability Management

Your Tenable Vulnerability Management Tenable Vulnerability Management instance has a licensed asset limit, which determines the number of assets you can scan for vulnerabilities. If you exceed your license limit, you can temporarily continue to use Tenable Vulnerability Management to scan your assets before adjusting your license as needed.

Tenable Vulnerability Management licenses asset sand uses a “flexible” licensing model:

- Tenable Vulnerability Management attempts to resolve duplicates. For example, a file server with 5 IP addresses - all of which are being scanned – only consumes a single license.
- Users are not locked out of the product due to license overages

For more information, see Vulnerability Management Licenses in the *Tenable Vulnerability Management User Guide*.

Tenable.sc

Tenable.sc licenses are valid for a specific hostname and for a maximum number of active assets (identified by IP address or UUID). Assets are counted towards your license limit depending on how Tenable.sc discovers, or sees, the asset. In general, an asset does not count against your license limit unless it has been assessed for vulnerabilities.

Because Tenable.sc licenses IP addresses:

- A single asset with multiple IP addresses consumes multiple licenses.
- Users are locked out of the product if license usage exceeds the allotted number of licenses.

For more information, see License Requirements in the *Tenable.sc User Guide*.

Scanning

This topic describes the differences between how and what you can scan in Tenable Vulnerability Management and Tenable.sc.

Tenable Vulnerability Management

Tenable Vulnerability Management allows you to scan your environment for vulnerabilities. Unlike Tenable Nessus and Tenable.sc, Tenable Vulnerability Management is hosted in the cloud, and allows you to scan remotely with your Tenable Nessus scanners and Tenable Nessus Agents, or with Tenable's cloud scanners if you want to scan assets from an external network.

Most of the Tenable Vulnerability Management scan templates are meant to create assessment scans: scans that find vulnerabilities on your assets. However, some of the scan templates, such as Host Discovery, allow you to create discovery scans: scans that find assets on your network.

For more information, see Scanning Overview in the *Tenable Vulnerability Management User Guide*.

Tenable.sc

You can perform two types of scans using Tenable products: discovery scans and assessment scans. Tenable recommends performing discovery scans to get an accurate picture of the assets on your network and assessment scans to understand the vulnerabilities on your assets.

For more information, see Scanning Overview in the *Tenable.sc User Guide*.

Reporting

This topic describes the differences between reports in Tenable Vulnerability Management and Tenable.sc.

> **Note:** Broadly speaking, the reporting capabilities in Tenable.sc are much more mature than those within Tenable Vulnerability Management. This delta may be of consideration for users depending on their reporting needs.

Tenable Vulnerability Management

In Tenable Vulnerability Management, you can generate reports to view and share specific Tenable Vulnerability Management data. You can use templates or create custom reports. You can create report schedules and share report templates and details with other Tenable Vulnerability Management users.

For more information, see Reports in the *Tenable Vulnerability Management User Guide*.

Tenable.sc

You can generate reports in CSV or PDF format to share data with users who may not have access otherwise. You can use templates or create custom reports.

For more information, see Reports in the *Tenable.sc User Guide*.

Assets

This topic describes the differences between assets in Tenable Vulnerability Management and Tenable.sc.

Tenable Vulnerability Management

Tenable Vulnerability Management includes the ability to track assets that belong to your organization. Assets are entities of value on a network that can be exploited.

Tenable Vulnerability Management automatically creates or updates assets when a scan completes or scan results are imported. Tenable Vulnerability Management attempts to match incoming scan data to existing assets using a complex algorithm. This algorithm looks at attributes of the scanned hosts and employs a variety of heuristics to choose the best possible match. If Tenable Vulnerability Management cannot find a match, the system assumes this is the first time Tenable Vulnerability Management has encountered the asset and creates a new record for it. Otherwise, if Tenable Vulnerability Management finds a matching asset, the system updates any properties that have changed since the last time Tenable Vulnerability Management encountered the asset.

Tenable Vulnerability Management categorizes assets in the following categories:

- Host Assets
- Cloud Assets
- Web Application Assets
- Domain Inventory Assets

For more information, see Assets in the *Tenable Vulnerability Management User Guide*.

Tenable.sc

Tenable.sc assets are lists of devices (for example, laptops, servers, tablets, or phones) within a Tenable.sc organization. Assets can be shared with one or more users based on local security policy requirements.

You can add an asset to group devices that share common attributes (IP address ranges, hardware types, vulnerabilities, outdated software versions, operating systems, etc.). Then, you can use the asset during scan configuration to target the devices in the asset.

Tenable provides asset templates that you can customize for your environment. Tenable-provided asset templates are updated via the Tenable.sc feed and visible depending on other configurations.

Tenable.sc supports the following custom asset types:

- Static Assets
- DNS Name List Assets
- LDAP Query Assets
- Combination Assets
- Dynamic Assets
- Watchlist Assets
- Import Assets

For more information, see Assets in the *Tenable.sc User Guide*.

Vulnerabilities / Findings

This topic describes the differences between vulnerabilities in Tenable Vulnerability Management and Tenable.sc.

Tenable Vulnerability Management

A finding is a single instance of a vulnerability appearing on an asset, identified uniquely by plugin ID, port, and protocol.

In Tenable Vulnerability Management, you can view and manage the following types of findings:

- Vulnerabilities
- Cloud Misconfigurations
- Host Audits
- Web Application Findings

For more information, see Findings in the *Tenable Vulnerability Management User Guide*.

Tenable.sc

In Tenable.sc, vulnerabilities are categorized as Cumulative or Mitigated and stored in two databases. The cumulative database contains currently vulnerable vulnerabilities, including recast, accepted, or previously mitigated vulnerabilities. The mitigated database contains vulnerabilities that Tenable.sc determines are not vulnerable, based on the scan definition, the results of the scan, the current state of the cumulative view, and authentication information.

For more information, see Vulnerability Analysis in the *Tenable.sc User Guide*.

Dashboards

This topic describes the differences between dashboards in Tenable Vulnerability Management and Tenable.sc.

Tenable Vulnerability Management

Dashboards are interactive, graphical interfaces that often provide at-a-glance views of key performance indicators (KPIs) relevant to a particular objective or business process. You can view, manage, and share dashboards within Tenable Vulnerability Management.

Tenable Vulnerability Management includes Tenable-provided dashboards, user-created dashboards, and dashboards that other users have shared with you.

For more information, see Dashboards in the *Tenable Vulnerability Management User Guide*.

Tenable.sc

In Tenable.sc, administrator users can view Tenable-provided default dashboards. Organizational users can configure custom or template-based dashboards that contain dashboard components, which display vulnerability, event, ticket, user, and alert data for analysis. When viewing vulnerability or event data, you can drill into the underlying dataset for further evaluation.

Dashboards allow you to organize similar dashboard components to streamline your analysis. Instead of creating a single dashboard with several dozen dashboard components, you can create several dashboards that group similar dashboard components together. For example, you can create two separate dashboards to view active scanning data and passive scanning data.

For more information, see Dashboards in the *Tenable.sc User Guide*.

Tenable Integrations / Data Sharing

This topic describes which Tenable Products you can use with Tenable Vulnerability Management and Tenable.sc.

For information about third-party integrations, see Integrations.

Tenable Vulnerability Management

Tenable Vulnerability Management data can be shared with the following Tenable Products:

- Lumin Exposure View
- Asset Inventory
- Attack Path Analysis
- Tenable Lumin

You can use the following Tenable products as scanners in Tenable Vulnerability Management:

- Tenable Nessus
- Tenable Nessus Agent
- Tenable Nessus Network Monitor
- Tenable Web App Scanning

Tenable.sc

Tenable.sc data can be shared with the following Tenable Products:

- Lumin Exposure View (Tenable One)

Tenable.sc can receive data from the following Tenable products:

- Tenable OT Security

You can use the following Tenable products as scanners in Tenable.sc:

- Tenable Nessus
- Tenable Vulnerability Management (as a Tenable Nessus scanner)

- Tenable Nessus Network Monitor
- Log Correlation Engine Server
- Log Correlation Engine clients