Data Ingestion in Tenable Vulnerability Management

Last Revised: August 07, 2025

Table of Contents

Overview

You can pull data into Tenable Vulnerability Management (formerly known as Tenable.io) through a number of methods. Depending on your business needs, you may want to ingest one or multiple data types, which you can then view and analyze within the user interface.

This document aims to describe each method of data ingestion supported by Tenable, and provides you with a series of steps to get your data up and running within Tenable Vulnerability Management.

For more information on each method of data ingestion, see the following topics:

- Linked Tenable Nessus Scanners
- Linked Tenable Network Monitor Sensors
- Tenable Nessus Cloud Scanners
- Tenable Agent Scans
- Connectors
- Integrations and Tenable Vulnerability Management API

Linked Tenable Nessus Scanners

To run network-based vulnerability scans of your internal networks, link one or more Tenable Nessus scanners to Tenable Vulnerability Management.

Before you Begin

Review the following Tenable Nessus documentation:

- Environments
- Install Tenable Nessus
- Deploy or Install Tenable Core + Nessus

Link a Tenable Nessus Scanner to Tenable Vulnerability Management

To link your Tenable Nessus scanner to Tenable Vulnerability Management, follow the steps outlined in the Tenable Vulnerability Management *User Guide*.

Configure Scans with the Tenable Nessus Scanner

Now that you've linked your Tenable Nessus scanner, you can select it as the scanner to use when configuring a scan. This allows Tenable Vulnerability Management to scan assets using the scanner (s) you linked. View your scans to see the scanner's status, manage the scanner and its scans, and view more information about the scanner. To increase efficiency and reduce scan times, you can also group multiple scanners and use them together in a scan.

> **Tip:** For more information about Tenable Nessus scanners in scan templates, see Nessus Scanner Templates in the *Tenable Vulnerability Management User Guide*.

View the Data in Tenable Vulnerability Management

Once your scan completes, you can view the scan details to see a summary of the results.

Additionally, you can utilize the Tenable Vulnerability Management interface to analyze scan data and make more informed business decisions based on your vulnerability findings and risk profile. For more information, see the following topics in the *Tenable Vulnerability Management User Guide*:

- Explore
- Findings
- Assets

Linked Tenable Network Monitor Sensors

For passive insight about your networks, you can link Tenable Network Monitor sensors to Tenable Vulnerability Management.

Before you Begin

Review the following Tenable Network Monitor documentation:

- Environments
- Install Tenable Network Monitor
- Deploy or Install Tenable Core + Nessus Network Monitor

Link an Tenable Network Monitor Sensor to Tenable Vulnerability Management

To link your Tenable Network Monitor sensor to Tenable Vulnerability Management, follow the steps outlined in the *Tenable Vulnerability Management User Guide*.

Configure Scans with the Tenable Network Monitor Sensor

Now that you've linked your Tenable Network Monitor sensor, passive data flows into Tenable Vulnerability Management based on how it is configured with Tenable Network Monitor.

View the Data in Tenable Vulnerability Management

Once your scan completes, you can view the scan details to see a summary of the results during each interval polled.

Additionally, you can utilize Tenable Vulnerability Management interface to analyze scan data and make more informed business decisions based on your vulnerability findings and risk profile. For more information, see the following topics in the *Tenable Vulnerability Management User Guide*:

- Explore
- Findings
- Assets

Tenable Nessus Cloud Scanners

By default, Tenable provides regional cloud sensors, which offer an external view of your attack surface. You can select these sensors when you create and launch scans of internet-facing targets within Tenable Vulnerability Management.

Tenable Nessus Cloud Scanners in Tenable Vulnerability Management

View the full list of each Tenable Vulnerability Management regional cloud sensor and, for allow list purposes, its IP address ranges in the *Tenable Vulnerability Management User Guide*. Be sure to review the additional considerations for allow lists and other specific business needs.

Configure Scans with the Tenable Nessus Cloud Scanner

Select the appropriate regional sensor when configuring a scan. This allows Tenable Vulnerability Management to scan assets using the Tenable Nessus Cloud Scanner. View your scans to see the scanner's status, manage the scanner and its scans, and view more information about the scanner.

View the Data in Tenable Vulnerability Management

Once your scan completes, you can view the scan details to see a summary of the results.

Additionally, you can utilize the Tenable Vulnerability Management interface to analyze scan data and make more informed business decisions based on your vulnerability findings and risk profile. For more information, see the following topics in the *Tenable Vulnerability Management User Guide*:

- Explore
- Findings
- Assets

Tenable Agent Scans

Some system types may benefit from assessments via locally installed Tenable Agents that link back to Tenable Vulnerability Management.

Before you Begin

Review the following Tenable Agent documentation:

- Environments
- Install Tenable Agent

Link a Tenable Agent to Tenable Vulnerability Management

To link your Tenable Agent to Tenable Vulnerability Management, follow the steps outlined in the *Tenable Vulnerability Management User Guide*.

Configure Scans with the Tenable Agent

Now that you've linked your Tenable Agent, you can scan that agent group by configuring either a Scan Window or Triggered Scan. This allows Tenable Vulnerability Management to scan assets using Tenable Agent. View your scans to see the scan status, manage the scans, and view more scan information. To increase efficiency and reduce scan times, you can also group multiple agents and use them together in a scan.

> **Tip:** For more information about Tenable Nessus scanners in scan templates, see Nessus Agent Scanner Templates in the *Tenable Vulnerability Management User Guide*.

View the Data in Tenable Vulnerability Management

Once your scan completes, you can view the scan details to see a summary of the results.

Additionally, you can utilize the Tenable Vulnerability Management interface to analyze scan data and make more informed business decisions based on your vulnerability findings and risk profile. For more information, see the following topics in the *Tenable Vulnerability Management User Guide*:

- Explore
- Findings
- Assets

Connectors

Tenable Vulnerability Management uses connectors, including third-party data connectors, to import assets from other platforms. Tenable Vulnerability Management includes connectors for the following platforms:

- **Amazon Web Service (AWS)** — The Amazon Web Services (AWS) connector provides real-time visibility and inventory of EC2 instances in your AWS account. To import and analyze information about EC2 instances in AWS, you must first configure AWS to support your connector configuration, then create an AWS connector in Tenable Vulnerability Management.
- **Google Cloud Platform (GCP)** — The Google Cloud Platform (GCP) Connector provides real-time visibility and inventory of assets in Google Cloud Platform. The GCP connector refreshes according to a schedule set by the user. To import and analyze information about assets in Google Cloud Platform, you must configure GCP to support connectors and then create a GCP connector in Tenable Vulnerability Management.
- **Microsoft Azure** — The Microsoft Azure Connector provides real-time visibility and inventory of assets in Microsoft Azure accounts. To import and analyze information about assets in Microsoft Azure, you must configure Azure to support connectors and then create an Azure connector in Tenable Vulnerability Management.

Configure the Platform

To use connectors to identify your assets, you must first configure the platform the connector integrates with, then create the connector.

For more information, see the following topics in the *Tenable Vulnerability Management User Guide*:

- Amazon Web Service (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

Manage your Connectors

After you configure platforms and create connectors, you can manage connectors from the **Settings** page in Tenable Vulnerability Management.

> **Tip:** For descriptions of common connector errors, see Connectors in the (missing or bad snippet).

Integrations and Tenable Vulnerability Management API

You can import data into Tenable Vulnerability Management outside the user interface. To do this, use third-party integrations or the API Explorer.

Third-party Integrations

Tenable Vulnerability Management supports a number of third-party integrations. For more information, see the following resources:

- Tenable Integration Partners
- Tenable Vulnerability Management Integrations documentation

API Explorer

You can use the API Explorer within the Tenable Developer Portal to ingest data into Tenable Vulnerability Management directly from the API. Here, you can:

- Create and manage connectors
- Create, manage, and run scans
- View and manage scanners
- Import data from third-party integrations

Tip: Check out the API documentation for more information on using the API Explorer.