



# Tenable On-Prem Connector Deployment Guide

---

## Quick Reference Guide

Last Revised: August 26, 2025



# Table of Contents

<b>Tenable On-Prem Connector Deployment Guide</b>	<b>1</b>
<b>Welcome to the Tenable On-Prem Connector Deployment Guide</b>	<b>3</b>
Process Overview	3
<b>Install the Tenable On-Prem Connector</b>	<b>3</b>
Prerequisites	4
Installation	5
Configuration	5
Finalize the Connection	8
<b>Troubleshooting</b>	<b>10</b>
Connectivity Issues	11
Authentication Issues	11
On-Prem Status	11
Data Fetching Issues	12
General Troubleshooting Steps	12
Tools	12



---

# Welcome to the Tenable On-Prem Connector Deployment Guide

---

**Last updated:** August 26, 2025

This document provides a comprehensive guide to deploying and configuring the Tenable On-Prem connector, an on-premises component that facilitates secure communication between the Tenable One platform and closed network environments. The Tenable On-Prem connector utilizes a WireGuard VPN tunnel over UDP port 51820 to establish this connection.

## Process Overview

The Tenable On-Prem connector allows Tenable One to pull data located from isolated networks without requiring direct inbound connections to those networks.

The workflow operates as follows:

1. **Establish a Secure Tunnel:** The Tenable On-Prem connector initiates an outbound connection to Tenable One, creating a secure, encrypted tunnel using the WireGuard VPN protocol over UDP port 51820.
2. **Communication Channel:** This tunnel establishes a secure communication channel between the Tenable One platform and the Tenable On-Prem connector.
3. **Data Scan Initiation:** When Tenable One launches a data sync, the data is securely transmitted through the tunnel to the Tenable On-Prem connector.
4. **Results Transmission:** The data results are then transmitted back to Tenable One through the secure WireGuard tunnel.
5. **Analysis and Reporting:** Tenable One processes the scan results and provides vulnerability data, compliance information, and other security insights.

In essence, the Tenable On-Prem connector acts as a secure intermediary, allowing Tenable One to reach into closed networks without compromising their security posture. The key is that the gateway initiates the connection to Tenable One, so no inbound connections to the closed network are required.

To get started, see [Install the Tenable On-Prem Connector](#).

---

## Install the Tenable On-Prem Connector

---



## Prerequisites

Before installing the Tenable On-Prem connector, ensure the following requirements are met:

- Within Tenable One, ensure you have a user with the appropriate permissions to manage third party connectors.

**Tip:** For more information on configuring user permissions, see [Permissions](#) in the *Tenable Vulnerability Management User Guide*.

- Confirm your Tenable Core environment supports your intended use of the instance as described in [System and License Requirements](#) in the *Tenable Core + Nessus User Guide*.
- Confirm your internet and port access supports your intended use of the instance as described in [Access Requirements](#) in the *Tenable Core + Nessus User Guide*.
- Hardware Requirements:

Requirement	Details
CPU	4 2GHz cores
Memory	4 GB RAM (8 GB RAM recommended)
Disk Space	30 GB, not including space used by the host operating system

- Network Requirements:

Port	Details
TCP 443	Outbound communications to the <code>appliance.cloud.tenable.com</code> and <code>sensor.cloud.tenable.com</code> servers for system updates.
UDP 53	Outbound DNS communications for Tenable Nessus, Tenable OT Security Enterprise Manager, and Tenable Core.
UDP 51820	The port must be open and pointing to your region-based server URL. <div><b>Tip:</b> You can find the region-based server URL on the Add Connector page when you <a href="#">create the Tenable On-Prem connector</a> within Tenable Exposure Management.</div>



TCP 8000	Inbound access to the web interface.
TCP XXX	An internal network with access to the systems you want Tenable to assess.

## Installation

To deploy Tenable Core as a VMware virtual machine, you must download the Tenable Core .ova file and deploy it on a hypervisor.

To deploy Tenable Core as a VMware virtual machine:

1. Download the **Tenable Core Nessus VMware Image** file from the [Tenable Downloads](#) page.
2. Open your VMware virtual machine in the hypervisor.
3. Import the Tenable Core VMware .ova file from your computer to your virtual machine.

**Tip:** For information about how to import a .ova file to your virtual machine, see the [VMware documentation](#).

4. In the setup prompt, configure the virtual machine to meet your organization's storage needs and requirements, and those described in [System and License Requirements](#) in the *Tenable Core + Nessus User Guide*.
5. Launch your Tenable Core instance.

The virtual machine boot process appears in a terminal window. The boot process may take several minutes to complete. When the virtual machine boot process finishes, the Tenable Core + Tenable Nessus deployment is complete.

## Configuration

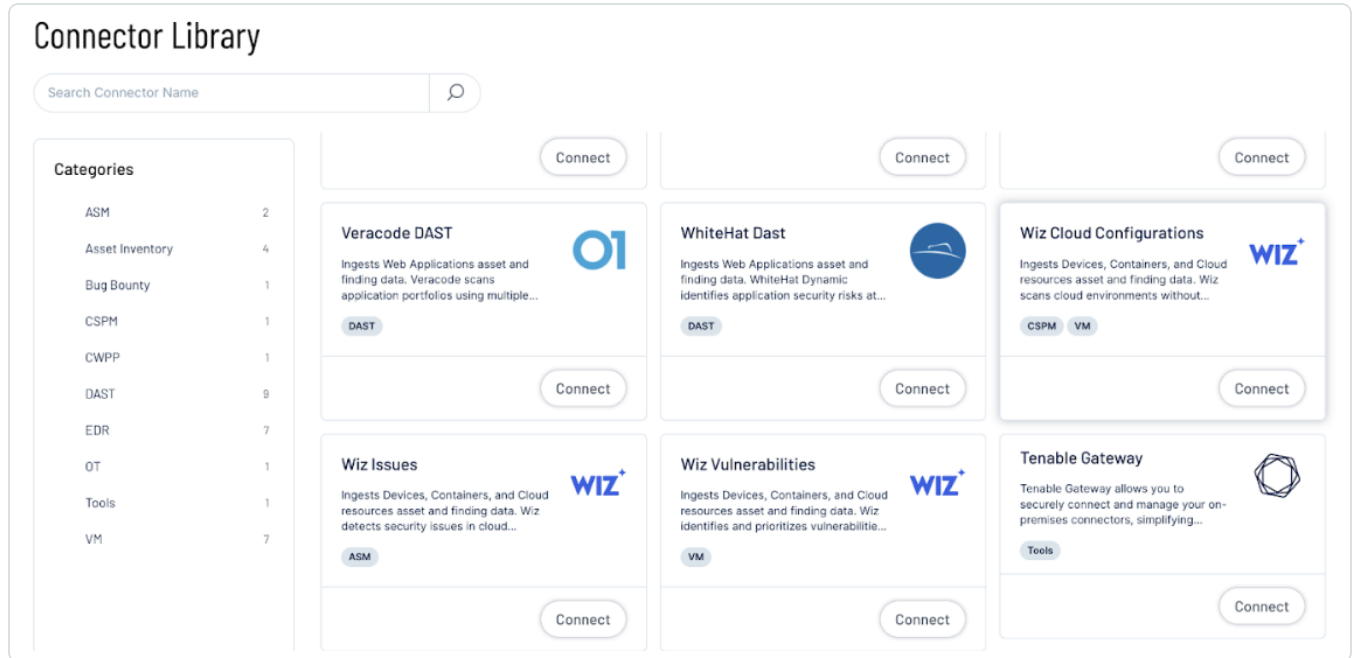
The Tenable On-Prem connector requires configuration to establish a connection with Tenable One. This procedure typically involves the generation of a pairing key within the Tenable One user interface, which is subsequently provided to the gateway during the setup phase.

To configure the Tenable On-Prem connector:



1. In Tenable Exposure Management, through the Connector Library, add a new **Tenable On-Prem** connector.

**Tip:** For more information on adding connectors within Tenable Exposure Management, see [Manage Connectors](#) in the *Tenable Exposure Management User Guide*.



The add connector page appears.



## Tenable Gateway

### Gateway Name

Tenable Gateway

### Connecting TenableOne Gateway


Download the Tenable Core OVA file from the following link: <https://www.tenable.com/downloads/tenable-appliance>

Ensure UDP port 51820 is open to site\_url

Log In to Tenable Core Once the installation is complete, log in to Tenable Core.

Locate the private key provided here and copy it. In the Tenable Core setup, paste the copied private key into the dedicated field.

### Private Key

[Redacted Private Key] 

 **Please note:** Make sure to copy and securely save the pairing key. This key will not be available again after saving

### UID


[Redacted UID] 

**Tip:** Here you can find your region-based server URL [required for your network configuration](#).

2. In the **On-Prem Name** text box, type a descriptive name for the connector.
3. Copy and save the **Pairing Key** for later use.
4. Click **Save**.

You return to the **Connector Library**.

5. Follow the steps to [Add a Connector](#) for your desired connector type, for example, Rapid7.
6. From the **On-Prem** drop-down, select the Tenable On-Prem connector you previously configured.



[Back to Connectors](#)

Connector credentials

Data pulling configuration

Test connectivity

Connector scheduling

Connector's log

## Rapid7

**Connector's Name**

**Gateway**

Dont use gateway

Dont use gateway

Tenable Gateway

**Username \***

**Password \***

**Data pulling configuration**

Set the integration data pulling

**Asset Retention**

Remove assets when their last seen date is more than  days ago

7. Click **Save**.

## Finalize the Connection

Lastly, you must link the connector to your Tenable Core on-premise installation.

To finalize the connection:

1. In your browser, navigate to the following URL, where *tenable-ip* is your Tenable IP address.

`https://<tenable-ip>:8000`

Your Tenable Core on-premise installation appears.

2. In the navigation menu, select **Tenable One On-Prem Connector**.





A prompt appears.

TENABLE ONE CONNECTOR PAIRING

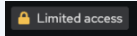
This connector is not currently paired with Tenable One.  
Enter the following information to complete pairing:

\* Pairing Key:

\* - Field is required to continue. Pairing key is required to continue.

Complete Pairing Close

3. Paste the **Pairing Key** that you generated within Tenable Exposure Management.
4. Click **Complete Pairing**.

**Note:** In some instances, you may need to allow administrative access by clicking the  button.


Upon successful establishment of communication via UDP port 51820, a new network interface named **wg0** appears in the Connectors table. Additionally, you should see evidence of received packets.



#### CONNECTOR STATUS:

Connector	Status
▶ try1	waiting for connection

#### Interface wg0

Peer	Last Handshake	Transmitted	Received
	5/12/2025, 9:53:25 AM	5.79 MB	4.52 MB

Within the connector table, each connector is represented by an expandable entry detailing the internal IP address and port necessary for data acquisition. The table presents an expandable line for each connector, specifying the internal IP address and port essential for retrieving data.

#### CONNECTOR STATUS:

Connector	Status
▼ try1	waiting for connection
Server Url	cloud.tenable.com
Server Port	443
Listening Port	13405

**Tip:** If only transmitted data is visible and received data is absent, the UDP connection is not established and therefore requires further [troubleshooting](#).

## Troubleshooting



This section provides guidance on troubleshooting common issues with Tenable On-Prem connector deployments.

## Connectivity Issues

- **Verify network connectivity:** Ensure the gateway server can reach Tenable One over HTTPS (port 443) and UDP port 51820. Use tools like ping, traceroute, and telnet or nc to test connectivity:

```
nc -v -u -z -w 3 site.url.com 51820
```

- **Check firewall rules:** Verify that the necessary firewall rules are in place on the gateway server, any intermediate firewalls, and the network perimeter. Specifically, ensure that outbound HTTPS and UDP/51820 traffic is allowed, and that inbound UDP/51820 traffic to the gateway's public IP address is permitted.
- **DNS resolution:** Ensure the gateway server can resolve the Tenable One hostname (e.g., gateway.TenableOne).

## Authentication Issues

- **Verify the activation key:** Double-check that the activation key was entered correctly during the gateway configuration.
- **Check gateway:** Ensure the gateway is properly registered and activated within the Tenable Exposure Management application.

## On-Prem Status

- **Check gateway status in Tenable Exposure Management:** The Tenable Exposure Management interface provides information about the status of connected gateways. Check for any error messages or alerts.

**Tip:** For more information, see [Connector Status](#) in the *Tenable Exposure Management User Guide*.

- **Check gateway logs:** Examine the Tenable On-Prem connector logs on the server for any error messages. The location of these logs are available through the Tenable Core user interface (port 8000).



## Data Fetching Issues

- **Verify scanner connectivity:** Ensure that the Tenable scanner used by the gateway can communicate with the target assets.
- **Check network segmentation:** Ensure that the gateway and scanner are located in a network segment that can reach the target assets.
- **Check credentials:** Ensure that the provided credentials are correct and have the correct role associated with them.

## General Troubleshooting Steps

For general help, do the following:

- Consult the Tenable documentation and support resources.
- Contact Tenable Support for assistance.

## Tools

The following are some tools that can help you troubleshoot issues with your Tenable On-Prem connector configuration:

- **ping:** Test basic network connectivity.
- **traceroute / tracert:** Trace the route that packets take to reach a destination.
- **telnet / nc:** Test connectivity to a specific port on a host. nc (netcat) is generally preferred over telnet.
- **nslookup / dig:** Query DNS servers to troubleshoot name resolution.
- **ifconfig / ip addr:** Display network interface configuration.
- **netstat / ss:** Display network connections and listening ports.
- **docker logs:** View the logs of a Docker container.
- **Firewall tools** (e.g., iptables, firewall-cmd, ufw): Inspect and modify firewall rules.