



Nessus Agent Windows Installation and Scan Setup

Quick Reference Guide

Last Revised: August 07, 2025

Table of Contents

- Summary 3**
- Install a Nessus Agent 4**
- Create an Agent Group 6**
- Create a Tenable Agent Scan 9**

Summary

The purpose of this guide is to help you install a Tenable Agent on a Windows operating system and link it to your Tenable Vulnerability Management account. This guide covers the prerequisites, the agent installation process, and configuration of a Nessus Agent scan. Tenable does not recommend using this guide for larger Tenable Agent deployments, but rather for one-off testing scenarios against a small subset of assets.

Prerequisites

First, you need to download the agent, which is available on our [Tenable Downloads](#) site. There are many supported operating systems, but this guide focuses on a Windows installation.

You also need to know how to locate your Tenable Vulnerability Management linking key. You can find your linking key in your Tenable Vulnerability Management account in the **Sensors** section. For more information, see the [Tenable Vulnerability Management User Guide](#).

Note: Tenable Agents communicate outbound on port 443 to cloud.tenable.com. Agents update their own plugins and software automatically.

Install a Nessus Agent

Tip: To install an agent silently on Windows, see [Install a Tenable Nessus Agent on Windows](#) > [Deploy and Link via the Command Line](#) in the *Tenable Agent User Guide*.

To install an agent on Windows:

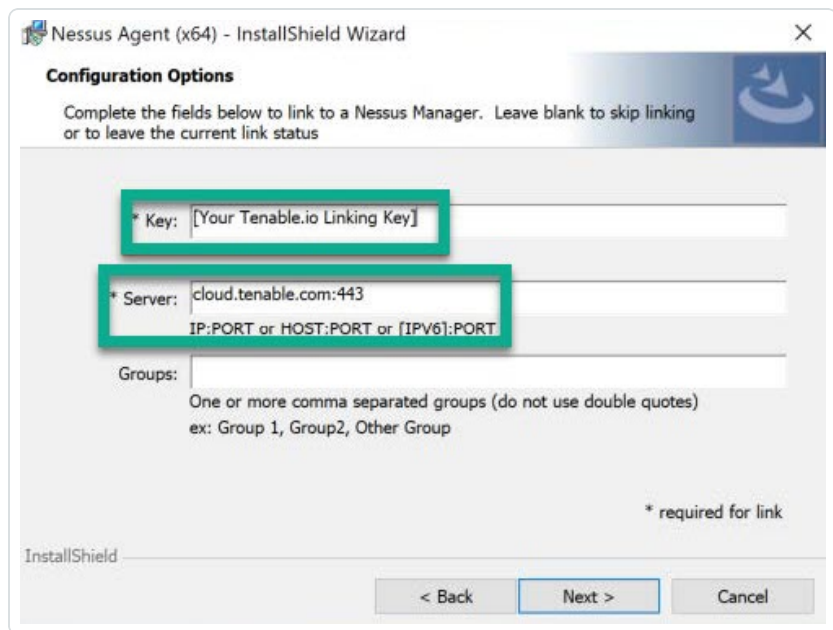
1. Open the agent installation file that you downloaded from the [Tenable Downloads](#) site.
2. Agree to the EULA.
3. Select the **Typical** installation method.

The installation wizard prompts you to enter in your Tenable Vulnerability Management linking key and a server for the agent to link to.

4. In the **Key** box, cut and paste your [Tenable Vulnerability Management linking key](#).
5. In the **Server** box, enter **cloud.tenable.com:443**.
6. (Optional) In the **Group** box, enter an agent group to add your agent to.

Tip: You can also add the agent to a group from the Tenable Vulnerability Management user interface. For more information, see the [Create an Agent Group](#) section of this guide.

7. Click **Next**.



The screenshot shows the 'Configuration Options' window of the 'Nessus Agent (x64) - InstallShield Wizard'. The window has a title bar with a close button. Below the title bar, the text reads: 'Complete the fields below to link to a Nessus Manager. Leave blank to skip linking or to leave the current link status'. There are three input fields: 1. '* Key: [Your Tenable.io Linking Key]' with a green rectangular highlight. 2. '* Server: cloud.tenable.com:443' with a green rectangular highlight. Below the server field, the text 'IP:PORT or HOST:PORT or [IPV6]:PORT' is displayed. 3. 'Groups:' with a text area below it containing the instruction 'One or more comma separated groups (do not use double quotes)' and an example 'ex: Group 1, Group2, Other Group'. At the bottom right, there is a note '* required for link'. At the bottom left, the 'InstallShield' logo is visible. At the bottom center, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

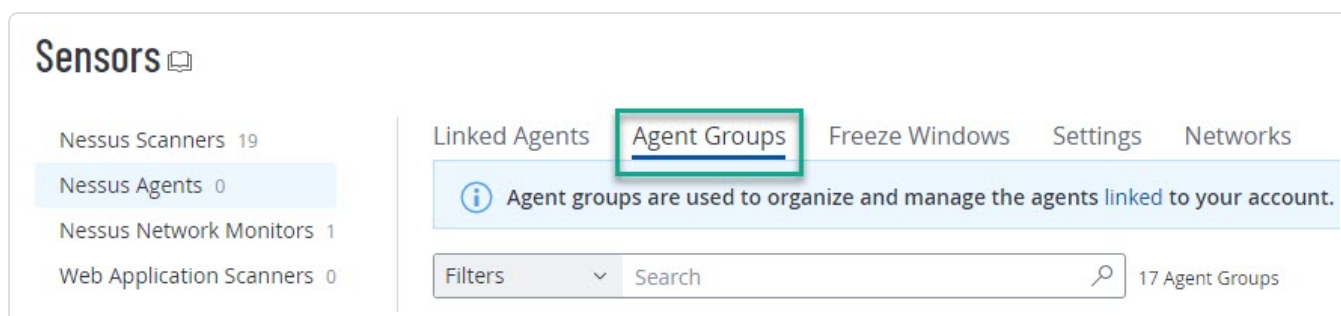
The agent should now show as linked in the Tenable Vulnerability Management user interface. You can confirm this in the **Settings > Sensors > Linked Agents** section of Tenable Vulnerability Management. The agent may go into an offline status as a result of the agent doing a plugin update and compilation. This is expected behavior, and the agent returns the online status once the process completes.

Create an Agent Group

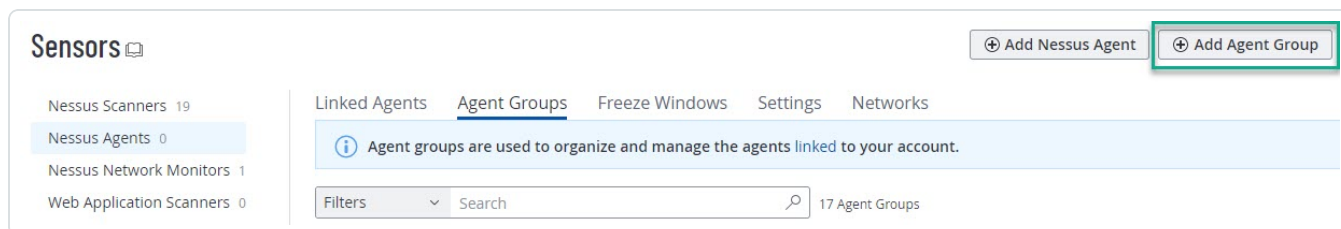
You can place agents into one or many agent groups, and you can link agents to agent groups at the time of installation or afterwards in the Tenable Vulnerability Management user interface. You can name agent groups based on characteristics of where you deploy the agent, the type of asset, or other similarities.

To create an agent group in Tenable Vulnerability Management:

1. Log in to Tenable Vulnerability Management.
2. Navigate to the **Sensors** page and select **Agent Groups** under the **Nessus Agents** section.



3. In the upper-right corner of the page, click the **+ Add Agent Group** button.



4. In the **Group Name** box, enter a name for the agent group.

Add Agent Group



Users & Groups ⊕

 All Users

Can Use ▼

Save

Cancel

- (Optional) In the **Users & Groups** section, configure which users can access the agent group.
- Click **Save**. Tenable Vulnerability Management saves the new agent group, and the **Agent Groups** table updates with your new agent group.

Now that you create the agent group, you can begin assigning your linked agent or agents to the group:

- In the **Agent Groups** table, click your new agent group.

The agent group details page opens.

- Click the ⊕ **Assign Agents** button.

Sensors

- Nessus Scanners 19
- Nessus Agents 0
- Nessus Network Monitors 1
- Web Application Scanners 0

Remote Agents

0 Agents

☐ 0 Linked Agents

1 to 0 of 0 ⏪ ⏩ Page 1 of 0 ⏪ ⏩

NAME ↑	STATUS	IP ADDRESS	PLATFORM (DISTRO)	VERSION	GROUPS	LAST PLUGIN UPDATE	LAST SCANNED	ACTIONS
--------	--------	------------	-------------------	---------	--------	--------------------	--------------	---------

The **Assign Agents** page opens.

- Select the linked agent or agents that you want to add to the agent group.
- Click the **Assign** button.

Tenable Vulnerability Management adds the selected agent or agents to the agent group.

Now that you populated your agent group, you can set up and run a scan targeting that agent group.

Create a Tenable Agent Scan

Now that you installed, linked, and assigned your agent or agents to an agent group, you can now create a scan that targets your new agent group. This process is similar to creating a vulnerability scan that uses a Tenable Nessus scanner. The main difference is that your targets for the scan are based on the new agent group.

To create a Tenable Agent scan in Tenable Vulnerability Management:

1. In the upper-left corner, click the ☰ button.

The left navigation plane appears.

2. In the left navigation plane, click **Scans**.

The **Scans** page appears with the **Vulnerability Management Scans** tab open.

3. In the upper-right corner of the page, click ⊕ **Create Scan**.

The **Select a Scan Template** page appears.

4. Click the **Nessus Agent** tab to view available templates for your scan.

Select a Scan Template

Nessus Scanner **Nessus Agent** User Defined

 32 Results

Vulnerability Scans (Common)

**Advanced Network Scan**
Configure a scan without using any recommendations.

**Basic Network Scan**
A full system scan suitable

A list of different scan templates that you can use with agents appears.

5. For this particular scenario, select the **Basic Agent Scan**: a comprehensive vulnerability template that scans the agent or agents for all known plugins.

Select a Scan Template

Nessus Scanner Nessus Agent User Defined

 7 Results

Vulnerability Scans

**Advanced Agent Scan**
Configure an agent scan without using any recommendations.

**Agent Log4Shell**
Agent Detection of Apache Log4j CVE-2021-44228

**Basic Agent Scan**
Scan systems connected via Nessus Agents.

6. Configure the scan settings.

Basic

General

NAME

Remote Windows Agent Scan

SCAN RESULTS

Show in dashboard

DESCRIPTION

FOLDER

My Scans

AGENT GROUPS

Remote Agents x

Scan Type ⓘ

☒ Scan Window

☐ Triggered Scan

3 Hours

The scan will be automatically stopped when the scan windows expires.

The three main template settings are a descriptive name, the agent group or groups that you want to target during the scan, and the **Scan Type**:

- A Scan Window is the duration of time that an agent has from the scheduled scan start time to check into Tenable Vulnerability Management, receive the scan job, run the vulnerability scan, and upload those results to Tenable Vulnerability Management. For testing purposes, you can leave the scan window at the default three hours.
- A Triggered Scan configuration allows the agent or agent group to launch the scan without any FedRAMP or user intervention. Agents can launch triggered scans using three different methods:

- Interval trigger – Configure agents to scan at a certain time interval (for example, every 12 hours or every 24 hours).
- File Name trigger – Configure agents to scan whenever a file with a specific file name is added to the agent trigger directory.
- Nessuscli trigger – Launch an existing triggered scan manually by running the following command in the Tenable Agentnessuscli utility:

```
# nessuscli scan-triggers --start --UUID=<scan-uuid>
```

You can also set multiple triggers for a single scan, and the scan searches for the triggers in their listed order (in other words, if the first trigger does not trigger the scan, it searches for the second trigger). For more information about triggered scans, see [Triggered Agent Scans](#) in the *Tenable Vulnerability Management User Guide*.

7. Once you configure those three settings, and any additional optional settings, click either **Save** or **Save and Launch** if you are ready to start the scan immediately.